de Gruyter Expositions in Mathematics 45

Distribution Theory of Algebraic Numbers

by

Pei-Chu Hu and Chung-Chun Yang

Walter de Gruyter · Berlin · New York

Authors

Pei-Chu Hu
Department of Mathematics
Shandong University
Shandong
China
E-Mail: pchu@sdu.edu.cn

Chung-Chun Yang
Department of Mathematics
The Hong Kong University of Science and Technology
Hong Kong
China
E-Mail: mayang@ust.hk

Mathematics Subject Classification 2000: 11-02, 11Jxx, 11J68, 11J97, 11Mxx, 11Rxx

Key words: Number theory, Diophantine approximation, field extensions, algebraic numbers, algebraic geometry, height functions, *abc*-conjecture, Roth's theorem, subspace theorems, Vojta's conjectures, *L*-functions

♾ Printed on acid-free paper which falls within the guidelines
of the ANSI to ensure permanence and durability.

ISSN 0938-6572
ISBN 978-3-11-020536-7

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Typeset using the authors' LaTeX files: Florian Platzek, Berlin.
Printing and binding: Hubert & Co. GmbH & Co. KG, Göttingen.
Cover design: Thomas Bonnie, Hamburg.

Preface

More recently, it has been found that there are profound relations between Nevanlinna theory and Diophantine approximation. C. F. Osgood first noticed a similarity between the number 2 in the Nevanlinna's defect relation and the number 2 in Roth's theorem. S. Lang pointed to the existence of a structure to the error term in Nevanlinna's second main theorem, conjectured what could be essentially the best possible form of this error term in general based on his conjecture on the error term in Roth's theorem. P. M. Wong used a method of Ahlfors to prove Lang's conjecture in one dimensional case. As for higher dimension, this problem was studied by S. Lang and W. Cherry, A. Hinkkanen, and was finally completed by Z. Ye. Lately, P. Vojta gave a much deeper analysis of the situation, and compared the theory of heights in number theory with the characteristic functions of Nevanlinna theory. In his dictionary, the second main theorem due to H. Cartan corresponds to the Schmidt's subspace theorem. Further, he proposed the general conjecture in number theory by comparing the second main theorem in Carlson–Griffiths–King's theory. Along this route, the Shiffman's conjecture on hypersurface targets in value distribution theory corresponds to a subspace theorem for homogeneous polynomial forms in Diophantine approximation. Vojta's $(1,1)$-form conjecture is an analogue of an inequality of characteristic functions of holomorphic curves for line bundles. Being influenced by Mason's theorem, Oesterlé and Masser formulated the abc-conjecture. The generalized abc-conjectures for integers are counterparts of Nevanlinna's third main theorem and its variations in value distribution theory, and so on.

In this book, we will introduce the analogues of Nevanlinna theory in Diophantine approximation, which are named "distribution theory of algebraic numbers" corresponded to another name "value distribution theory" of Nevanlinna theory. In other words, we will introduce some qualitative and quantitative relations of algebraic numbers distributed in spaces. The book consists of nine chapters: In Chapter 1, we introduce some basic notations, terminologies and propositions on groups, ideals in rings, fields, field extensions, valuations and absolute values, which are often used in this book. In particular, we hope to explain clearly the corresponding relation between prime ideals and places in Dedekind domains. It will help us to understand well some contents related to absolute values, say, product formula and its derivatives.

Some foundational properties of algebraic numbers will be discussed in Chapter 2, which contains factorizations and norms of ideals, product formula and discriminants on number fields, and Minkowski's geometry of numbers.

In Chapter 3, we introduce basic notations and facts in algebraic geometry. This is

the part of spaces carrying algebraic numbers in this book. First of all, we discuss carefully operations, norms and some properties in projective spaces which play important role in this book, and then we introduce varieties, divisors, linear systems, algebraic curves, sheaves, vector bundles, schemes and Kobayashi hyperbolicity.

We will discuss height functions in Chapter 4. This is the part of quantitative tools studying distribution of algebraic numbers in this book. Height functions share many general character with Nevanlinna's order functions, say, they all satisfy first main theorem of Nevanlinna type, which establishes an important connection among height, proximity and valence (or counting by some authors) functions. This chapter also contains some introduction on Weil functions, Aralelov theory and canonical heights over Abelian varieties.

In Chapter 5, we introduce the abc-conjecture and its generalizations in detail. To understand these conjectures well, we also introduce their analogues for polynomials.

In Chapter 6, we discuss the Roth's theorem and its generations. The Roth's theorem is corresponding to Nevanlinna's second main theorem on meromorphic functions on $\mathbb{C}$. In order to make reader convenience, we also introduce its proof and connection with the abc-conjecture.

In Chapter 7, we introduce the Schmidt subspace theorem and its generalization. Schmidt subspace theorem is corresponding to Cartan's second main theorem in value distribution of holomorphic curves into complex projective spaces. We also give a subspace theorem on hypersurfaces which is regarded as an analogue of Shiffman conjecture (proved by Hu and Yang for non-Archimedean cases and Ru for complex cases) in value distribution.

In Chapter 8, we introduce Mordell–Faltings theorem, Bombieri–Lang's conjecture related to pseudo canonical varieties, and Vojta's conjectures on height inequalities.

In Chapter 9, we introduce a few of L-functions. Hopefully, the methods proving prime number theorem by using the Riemann zeta-function and Dirichlet L-functions can be applied to study similar problems of other L-functions derived from number fields, modular forms, geometric analysis and so on.

Each chapter of this book is self-contained and this book is appended with a comprehensive and up-dated list of references. The book will provide not just some new research results and directions but challenging open problems in studying Diophantine approximation. One of the aims of this book is to make timely surveys on these new results and their related developments; some of which are newly obtained by the authors and have not been published yet. It is hoped that the publication of this book will stimulate, among the peers, further the researches on Diophantine approximation and their applications.

We gratefully acknowledge the supports of the related research and writing of the present book from Natural Science Fund of China (NSFC) and Research Grant Council of Hong Kong during the past years.

Pei-Chu Hu
Chung-Chun Yang

Contents

Preface v

1 Field extensions 1
1.1 Groups 1
1.1.1 Abelian groups 1
1.1.2 Galois cohomology 7
1.2 Rings and ideals 9
1.2.1 Ideals 9
1.2.2 Completion of topological groups 16
1.2.3 Fractional ideals 18
1.2.4 Relative differentials 19
1.3 Integral elements and valuations 21
1.3.1 Integral elements 21
1.3.2 Valuation rings 23
1.3.3 Discrete valuation rings 27
1.4 Polynomials 32
1.5 Algebraic extension fields 36
1.6 Separable extension fields 41
1.6.1 Separable algebraic extensions 41
1.6.2 Ramification indices 45
1.7 Norm and trace 47
1.8 Discriminant of field extensions 52
1.9 Absolute values on fields 55
1.9.1 Absolute values 55
1.9.2 Extensions of absolute values 58
1.9.3 Extensions of valuations 60
1.10 Divisor groups 71
1.10.1 Valuation properties of Dedekind domains 71
1.10.2 Local degrees in field extensions 78
1.11 Different 84

2 Algebraic numbers 91
2.1 Integral ideals 91
2.1.1 Factorization of ideals 91
2.1.2 The norm of an ideal 99

2.2 Absolute values on number fields . . . 101
2.2.1 Archimedean absolute values . . . 102
2.2.2 Product formula . . . 103
2.2.3 Galois extensions of number fields . . . 108
2.3 Discriminant of number fields . . . 109
2.4 Minkowski's geometry of numbers . . . 112
2.4.1 Minkowski's first theorem . . . 112
2.4.2 Minkowski's bound . . . 116
2.4.3 Dirichlet's unit theorem . . . 120
2.4.4 Minkowski's second theorem . . . 123
2.5 Different of number fields . . . 124

3 Algebraic geometry . . . 130
3.1 Hermitian geometry . . . 130
3.1.1 Exterior product . . . 130
3.1.2 Norms of vector spaces . . . 132
3.1.3 Schwarz inequalities . . . 136
3.1.4 General position . . . 140
3.1.5 Hypersurfaces . . . 144
3.2 Varieties . . . 150
3.2.1 Affine varieties . . . 150
3.2.2 Projective varieties . . . 154
3.2.3 Local rings of varieties . . . 156
3.2.4 Dimensions . . . 160
3.2.5 Differential forms . . . 162
3.2.6 Abelian varieties . . . 165
3.3 Divisors . . . 167
3.4 Linear systems . . . 173
3.5 Algebraic curves . . . 177
3.5.1 Bézout's theorem . . . 177
3.5.2 Riemann–Roch theorem . . . 181
3.5.3 Rational curves . . . 184
3.5.4 Elliptic curves . . . 186
3.5.5 Hyperelliptic curves . . . 194
3.5.6 Jacobian of curves . . . 196
3.6 Sheaves and vector bundles . . . 197
3.6.1 Sheaves . . . 197
3.6.2 Vector bundles . . . 202
3.6.3 Line bundles . . . 206
3.6.4 Intersection multiplicity . . . 209
3.7 Schemes . . . 212
3.7.1 Schemes . . . 212

3.7.2 Basic properties of schemes . . . 219
3.7.3 Sheaves of modules . . . 224
3.7.4 Differentials over schemes . . . 224
3.7.5 Ramification divisors . . . 226
3.8 Kobayashi hyperbolicity . . . 229
3.8.1 Hyperbolicity . . . 229
3.8.2 Measure hyperbolicity . . . 232
3.8.3 Open problems . . . 237

4 Height functions . . . 239
4.1 Heights on projective spaces . . . 239
4.1.1 Basic properties . . . 239
4.1.2 Heights on number fields . . . 242
4.1.3 Functional properties of heights . . . 247
4.2 Heights of polynomials . . . 250
4.2.1 Coefficients for polynomials . . . 250
4.2.2 Gelfand's inequality . . . 255
4.2.3 Finiteness theorems . . . 259
4.3 Heights on varieties . . . 264
4.4 Heights and Weil functions . . . 274
4.4.1 Weil functions . . . 274
4.4.2 Heights expand Weil functions . . . 278
4.4.3 Proximity functions . . . 280
4.5 Arakelov theory . . . 283
4.5.1 Function fields . . . 283
4.5.2 Number fields . . . 286
4.6 Canonical heights on Abelian varieties . . . 294
4.6.1 Periodic points . . . 294
4.6.2 Canonical heights . . . 297
4.6.3 Tate–Shafarevich groups . . . 299
4.6.4 Mordell–Weil theorem . . . 301

5 The abc-conjecture . . . 304
5.1 The abc-theorem for function fields . . . 304
5.2 The abc-conjecture for integers . . . 306
5.3 Equivalent abc-conjecture . . . 308
5.4 Generalized abc-conjecture . . . 312
5.5 Generalized Hall's conjecture . . . 315
5.6 The abc-conjecture for number fields . . . 318
5.6.1 Generalizations of the abc-conjecture . . . 318
5.6.2 Further formulations of the abc-conjecture . . . 321
5.7 Fermat equations . . . 323

6 Roth's theorem . . . 328
6.1 Statement of the theorem . . . 328
6.2 Siegel's lemma . . . 331
6.3 Indices of polynomials . . . 335
6.4 Roth's lemma . . . 340
6.5 Proof of Roth's theorem . . . 346
6.6 Formulation of Roth's theorem . . . 351
6.6.1 A generalization . . . 351
6.6.2 Approach infinity . . . 352
6.6.3 Ramification term . . . 354
6.6.4 Roth's theorem and abc-conjecture . . . 358

7 Subspace theorems . . . 360
7.1 p-adic Minkowski's second theorem . . . 360
7.2 Adelic Minkowski's second theorem . . . 366
7.2.1 Haar measures . . . 366
7.2.2 Adèle rings . . . 368
7.2.3 Minkowski's second theorem . . . 371
7.3 Successive minima of a length function . . . 379
7.4 Vojta's estimate . . . 386
7.5 Schmidt subspace theorem . . . 392
7.5.1 Subspace theorem . . . 392
7.5.2 Proof of subspace theorem . . . 395
7.6 Cartan's method . . . 399
7.7 Subspace theorems on hypersurfaces . . . 403
7.7.1 Statements of theorems . . . 404
7.7.2 Proof of Theorem 7.35 . . . 406

8 Vojta's conjectures . . . 415
8.1 Mordellic varieties . . . 415
8.2 Main conjecture . . . 420
8.3 General conjecture . . . 424
8.4 Vojta's $(1,1)$-form conjecture . . . 429
8.5 abc-conjecture implies Vojta's height inequality . . . 432

9 *L*-functions . . . 434
9.1 Dirichlet series . . . 434
9.1.1 Abscissa of convergence . . . 434
9.1.2 Riemann's ζ-function . . . 436
9.1.3 Dirichlet's characters . . . 443
9.1.4 Dirichlet's L-functions . . . 446
9.1.5 Zeros of Dirichlet's L-functions . . . 449
9.2 The Dedekind zeta-function . . . 454

9.2.1 The ζ-functions of number fields . . . 454
9.2.2 Selberg class . . . 456
9.3 Special linear groups . . . 459
9.3.1 General linear groups . . . 459
9.3.2 Modular groups . . . 461
9.4 Modular functions . . . 464
9.4.1 Automorphic forms . . . 464
9.4.2 Weierstrass $\wp$ function . . . 466
9.4.3 Elliptic modular functions . . . 468
9.4.4 Hecke's theorem . . . 470
9.5 Modular forms . . . 475
9.5.1 Modular forms for $\mathrm{SL}(2,\mathbb{Z})$ . . . 475
9.5.2 Modular forms for congruence subgroups . . . 478
9.5.3 Hecke operator . . . 480
9.5.4 Hecke's L-series . . . 483
9.5.5 Modular representations . . . 484
9.6 Hasse–Weil L-functions . . . 485
9.7 L-functions of varieties . . . 490
9.7.1 L-functions of $\mathbb{P}^N$ . . . 492
9.7.2 L-functions of Abelian varieties . . . 493

Bibliography . . . 495

Symbols . . . 511

Index . . . 515

Chapter 1

Field extensions

In this chapter, we will introduce some basic notations, terminologies and theorems about fields and algebraic geometry, which will be used in this book.

1.1 Groups

We denote the fields of complex, real, and rational numbers by $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Q}$, respectively, and let $\mathbb{Z}$ be the ring of integers. If κ is a set, we write

$$\kappa^n = \{(x_1, \ldots, x_n) \mid x_i \in \kappa\} = \kappa \times \cdots \times \kappa \ (n \text{ times}).$$

If κ is partially ordered, denote

$$\kappa(s,r) = \{x \in \kappa \,|s < x < r\}, \quad \kappa(s,r] = \{x \in k|s < x \leq r\},$$
$$\kappa[s,r) = \{x \in \kappa \,|s \leq x < r\}, \quad \kappa[s,r] = \{x \in \kappa \,|s \leq x \leq r\},$$

$$\kappa_+ = \kappa[0,\infty), \quad \kappa^+ = \kappa(0,\infty).$$

For example, $\mathbb{Z}[s,r]$ means the set of integers i satisfying $s \leq i \leq r$, $\mathbb{R}^+$ is the set of positive real numbers, and so on.

1.1.1 Abelian groups

Let G be an Abelian group with a rule of composition by multiplication. If the group contains infinitely many different elements it is called an *infinite group*; otherwise it is called a *finite group of order* $\mathbf{h}$, where $\mathbf{h}$ is the number of its elements. Now in case G is a finite group of order $\mathbf{h}$, then the order N of a subgroup H is also finite and then the number of different cosets gH for each $g \in G$ is also finite, say $= j$. Since each element of G occurs in exactly one coset and exactly N different elements are contained in each coset, we have $\mathbf{h} = jN$, and thus we have shown

Proposition 1.1. *In a finite group of order* $\mathbf{h}$*, the order* N *of each subgroup is a divisor of* $\mathbf{h}$.

The quotient $\mathbf{h}/N = j$ is called the *index* of the subgroup relative to G. In case G is an infinite group, then the order of H as well as the number of different cosets can be infinite and at least one of these cases must obviously occur. Furthermore, the number of different cosets in a group G determined by a subgroup H of G is called the *index* of H in G whether this index is finite or not.

If G is a finite group of order $\mathbf{h}$, all powers of an element g with a positive exponent always form a subgroup of G. These powers cannot all be different. From $g^m = g^n$ it follows that $g^{m-n} = 1$ (unit of G). Hence a certain power of g with exponent different from zero is always $= 1$, say $g^l = 1$. These l are identical with all multiples of an integer t (> 0). This exponent t, uniquely determined by g, is called the *order of* g. Consequently among the powers of g there are only t different ones, say, $g^0 = 1, g^1, \ldots, g^{t-1}$, and by the above these form a subgroup of G of order t. Moreover from Proposition 1.1 we obtain

Theorem 1.2. *The order a of each element of a finite group G is a divisor of the order $\mathbf{h}$ of G and hence $g^{\mathbf{h}} = 1$ for each element $g \in G$.*

Now we state the *fundamental theorem of Abelian groups* which gives us full information about the structure of the finite Abelian group (cf. [95]).

Theorem 1.3. *In each Abelian group G of order $\mathbf{h}$ (> 1) there are certain elements $w_1, \ldots, w_n$ with orders $h_1, \ldots, h_n$ respectively $(h_i > 1)$ such that each element of G is obtained in exactly one way in the form*

$$v = w_1^{k_1} w_2^{k_2} \cdots w_n^{k_n},$$

where the integers k_i each run through a complete system of residue $\bmod h_i$ *independently of one another. Moreover the $h_i = p^{l_i}$ are prime powers and $\mathbf{h} = h_1 h_2 \cdots h_n$.*

The n elements of this kind are called a *basis of* G. To prove next theorem, we need a fact from number theory. A system S of integers is a *module* if it contains at least one number different from 0 and if among with m and n, $m+n$ and $m-n$ also always belong to S. A general theorem about modules states that the numbers in a module S are identical with the multiples of certain number d. The number d is determined by S up to the factor ± 1.

Theorem 1.4. *If an infinite Abelian group G has a finite basis, then each subgroup of G also has a finite basis.*

Proof. Let $w_1, w_2, \ldots, w_n$ be a basis of G where $w_1, \ldots, w_m$ are the elements of infinite order and $w_{m+1}, \ldots, w_n$ are those of order $h_1, \ldots, h_{n-m}$. We consider the set I of exponents $(k_1, \ldots, k_n)$ of all products of powers

$$v = w_1^{k_1} \cdots w_n^{k_n}$$

which belong to a subgroup H of G, where, in addition, the last $k_{m+1}, \ldots, k_n$ are to run through all numbers, not just the numbers which are distinct mod h_i, as long as the product belongs to H. By the group property of H, however, we obviously have that for exponents $(k_1, \ldots, k_n)$ and $(k'_1, \ldots, k'_n)$ in I, the exponents $(k_1 + k'_1, \ldots, k_n + k'_n)$ and $(k_1 - k'_1, \ldots, k_n - k'_n)$ also correspond to elements v in H. In particular, we keep in mind the elements

$$v = w_i^{k_i} w_{i+1}^{k_{i+1}} \cdots w_n^{k_n} \quad (1 \leq i \leq n) \tag{1.1}$$

belonging to H for a definite i, thus for which $k_1 = \cdots = k_{i-1} = 0$. There are such elements, since if all $k_i = 0$ the unit element of H is obtained. The totality of possible first exponents k_i in (1.1) forms a module of integers, as long as we do not always have $k_i = 0$. However, all numbers of this module are identical with the multiples of a certain integer; consequently, if we do not always have $k_i = 0$, there is an element v_i in H with one such $r_{ii} \neq 0$,

$$v_i = w_i^{r_{ii}} w_{i+1}^{r_{i,i+1}} \cdots w_n^{r_{in}},$$

such that k_i in (1.1) is a multiple of this r_{ii}. From the v_i with this r_{ii} (possibly infinite in number), we pick out a definite one for each $i = 1, \ldots, n$, where we set $v_i = 1$ and $r_{ii} = 0$ in case we always have $k_i = 0$ for this i in (1.1).

We show that each element in H is representable as a product of these elements $v_1, \ldots, v_n$. Let $v = w_1^{k_1} \cdots w_n^{k_n}$ be an element of H. By the preceding discussion, k_1 is a multiple of r_{11}, $k_1 = j_1 r_{11}$, and hence

$$v v_1^{-j_1} = w_2^{k'_2} w_3^{k'_3} \cdots w_n^{k'_n} \tag{1.2}$$

is a product only of powers of $w_2, \ldots, w_n$, which also belongs to H by the group property. If we should have $r_{11} = 0$ and $v_1 = 1$, then we should take $j_1 = 0$. Likewise, in (1.2), k'_2 must be a multiple of r_{22} in case this element is $\neq 0$, $k'_2 = j_2 r_{22}$. Moreover if $r_{22} = 0$ then k'_2 must be $= 0$ and we take $j_2 = 0$. In any case then $v v_1^{-j_1} v_2^{-j_2}$ is an element of H and representable as product of powers only of $w_3, \ldots, w_n$ etc. until we arrive at the unit element and obtain a representation

$$v = v_1^{j_1} v_2^{j_2} \cdots v_n^{j_n}.$$

The $v_1, \ldots, v_m$ are of infinite order if they are $\neq 1$, the other v's are of finite order.

The products of powers of the $v_{m+1}, \ldots, v_n$ form a finite Abelian group and can hence be represented by a basis $u_1, \ldots, u_q$, by Theorem 1.3. We assert that $v_1, \ldots, v_m$, $u_1, \ldots, u_q$ form a basis for H if we omit the elements $v_i = 1$. First, each element can be represented by the $v_1, \ldots, v_n$, hence also by the $v_1, \ldots, v_m, u_1, \ldots, u_q$. Now if

$$v_1^{a_1} v_2^{a_2} \cdots v_m^{a_m} u_1^{b_1} \cdots u_q^{b_q} = 1 \tag{1.3}$$

is a representation of the unit element where $a_i = 0$ is assumed for $v_i = 1$ (i.e., $r_{ii} = 0$), then by substitution of the w_i in place of the v_i and u_j, it follows that $a_1 r_{11} = 0$; hence either $a_1 = 0$ or $r_{11} = 0$. However, in the latter case we also have $a_1 = 0$ as a consequence of our convention. Likewise $a_2 = 0, \ldots, a_m = 0$. Furthermore, since the u_j form a basis of the finite group, then in (1.3) each b_j must be a multiple of the order of u_j. Now since each element is represented the same number of times by the v_i as by the u_i, hence the same number of times as the unit element, these elements actually form a basis for H as was to be proved. □

Those infinite Abelian groups in which no element of finite order except the unit 1 appears are of chief interest. We call such groups *torsion-free groups*, the others *mixed groups*. Along with a torsion-free group G, each subgroup of G is also torsion-free. In particular, let H be a subgroup of G of finite index. Then a certain power of each element of G with exponent different from zero must always belong to H. For if g is an element of G, then the cosets

$$gH,\ g^2H,\ \ldots,\ g^mH,\ \ldots$$

are not all distinct, since the index is assumed to be finite. Thus for some n, $g^nH = g^mH$, that is, $g^{n-m} \in H$ with $n - m \neq 0$. Hence in the proof of Theorem 1.4 applied to G and H, the case $r_{ii} = 0$, $v_i = 1$ can obviously never occur, since, in fact, a system of values $k_i \neq 0$, $k_{i+1} = \cdots = k_n = 0$ always exists, so that $v_i = w_i^{k_i} \in H$. From this we have immediately

Theorem 1.5. *If G is a torsion-free Abelian group with finite basis $w_1, \ldots, w_n$, then every subgroup H of G with finite index has a basis $v_1, \ldots, v_n$ of the form*

$$v_i = \prod_{j=i}^{n} w_j^{r_{ij}},$$

with $r_{ii} \neq 0$ for $i = 1, 2, \ldots, n$.

It is not difficult to show that the index of H in G is just $j = |r_{11} r_{22} \cdots r_{nn}|$ (see [95], Theorem 36).

Theorem 1.6. *If a torsion-free Abelian group G has a finite basis of n elements w_1, $\ldots, w_n$, then n is the maximal number of independent elements of G, independent of the choice of basis.*

Proof. Since the $w_1, \ldots, w_n$ are independent in any case, there are n independent elements in G and thus we need only show that $n + 1$ elements in G are not independent. In fact, between $n + 1$ arbitrary elements

$$v_i = w_1^{a_{i1}} w_2^{a_{i2}} \cdots w_n^{a_{in}} \quad (i = 1, 2, \ldots, n + 1),$$

there is the relation

$$v_1^{x_1} v_2^{x_2} \cdots v_{n+1}^{x_{n+1}} = 1,$$

if we choose the $n+1$ integers x_i so that they satisfy the n linear homogeneous equations

$$\sum_{i=1}^{n+1} a_{ij} x_i = 0 \ \ (j = 1, 2, \ldots, n).$$

As is known this is always possible since the coefficients a_{ij} are integers. □

Theorem 1.7. *From a basis $w_1, \ldots, w_n$ of a torsion-free Abelian group G one can obtain all systems of bases $w_1', \ldots, w_n'$ of G in the form*

$$w_i' = \prod_{j=1}^{n} w_j^{a_{ij}}, \ i = 1, 2, \ldots, n$$

where the system of the exponents are arbitrary integers a_{ij} with determinant ± 1.

Proof. Note that the w_i' always form a basis. To see this we need only show that the w_i can be represented through the w_i'. The equation

$$w_j = w_1'^{x_{j1}} w_2'^{x_{j2}} \cdots w_n'^{x_{jn}}$$

is satisfied if the integers x_{jk} are chosen so that the n equations

$$\sum_{j=1}^{n} a_{ij} x_{jk} = \begin{cases} 0, & \text{if } i \neq k, \\ 1, & \text{if } i = k \end{cases}$$

hold. Since the determinant of the (integral) coefficients is $= \pm 1$ and the right side is also integral, the x_{jk} are uniquely determined integers.

Secondly, if n elements

$$w_i' = \prod_{j=1}^{n} w_j^{a_{ij}}, \ i = 1, 2, \ldots, n$$

form a basis, then w_j must be represented through the w_i',

$$w_j = w_1'^{b_{j1}} w_2'^{b_{j2}} \cdots w_n'^{b_{jn}}, \ \ j = 1, 2, \ldots, n,$$

if the w_j are substituted for the w_i', then the n^2 equations

$$\sum_{j=1}^{n} a_{ij} b_{jk} = \begin{cases} 0, & \text{if } i \neq k, \\ 1, & \text{if } i = k \end{cases}$$

are obtained, by the basis property of the w_i'. The determinant of this array is thus $= 1$; on the other hand, however, by the multiplication theorem of determinant theory, the determinant is equal to the product of the two determinant $\det(a_{ij})$ and $\det(b_{jk})$. Hence each of these integers must divide 1, and therefore each integer is itself $= \pm 1$; thus $\det(a_{ij}) = \pm 1$. □

By Theorem 1.7 and the remark after Theorem 1.5, we obtain

Theorem 1.8. *If G is a torsion-free Abelian group with a finite basis $w_1, \ldots, w_n$, then every subgroup H of G with finite index j has a basis $v_1, \ldots, v_n$, and the determinant $\det(a_{ij})$ in the n equations*

$$v_i = \prod_{j=1}^{n} w_j^{a_{ij}}, \quad i = 1, 2, \ldots, n$$

is always equal to j in absolute value.

Theorem 1.9. *If G is a group with a finite basis $w_1, \ldots, w_n$, then a subgroup H is of finite index if and only if a power of each element of G belongs to H.*

Proof. If the h_i-th power $(h_i > 0)$ of w_i belongs to H and if we set

$$h = h_1 h_2 \cdots h_n,$$

then w_i^h also belongs to H and consequently the h-th power of each element likewise belongs to H. Hence each element of G differs from some

$$w_1^{x_1} w_2^{x_2} \cdots w_n^{x_n} \quad (0 \leq x_i < h)$$

by a factor in H; therefore there are at most h^n different cosets, represented by the above elements. Thus the index of H is finite.

Conversely, in the case of a finite index the infinitely many cosets

$$gH, \ g^2H, \ g^3H, \ \ldots$$

cannot all be distinct for each $g \in G$, thus a power of g must belong to H. □

Let $\Gamma = (\Gamma, +, \leq)$ be a *totally ordered* Abelian additive group. This means that the order relation $\leq$ on Γ satisfies:

(1) $\alpha \leq \beta$ implies $\alpha + \gamma \leq \beta + \gamma$ for any $\alpha, \beta, \gamma \in \Gamma$.

(2) For each $\alpha, \beta \in \Gamma$ either $\alpha \leq \beta$ or $\beta \leq \alpha$.

Special cases occur when Γ is a subgroup of $\mathbb{R}$. This happens if and only if the *Archimedean property* holds:

(3) If $\alpha > 0$, for every $\beta \in \Gamma$ there exists a natural number n such that $n\alpha > \beta$.

Lemma 1.10. *If Γ is a totally ordered Abelian additive group satisfying the Archimedean property, then it is order-isomorphic to a subgroup of the ordered additive group $\mathbb{R}$.*

Proof. See P. Ribenboim [215], Lemma 1 on page 60. □

1.1.2 Galois cohomology

Let G be a (finite or topological) group acting on another Abelian group A (endowed with the discrete topology). Denote the action of G on A by

$$G \times A \longrightarrow A, \ \ (\sigma, a) \longmapsto \sigma(a).$$

By the definition, we have the relations

$$(\sigma\tau)(a) = \sigma(\tau(a)), \quad 1(a) = a$$

for $\sigma, \tau \in G$, $a \in A$, where 1 is the unit of G.

The cohomology groups of G with coefficients in A are defined with the help of the complex of cochains. Consider the following Abelian groups:

$$C^0(G, A) = A,$$

and for $n \geq 1$,

$$C^n(G, A) = \{f : G^n \longrightarrow A \mid f \text{ is continuous}\},$$

where the continuity of $f \in C^n(G, A)$ means that the function $f(\sigma_1, \ldots, \sigma_n)$ depends only on a coset of σ_i modulo some open subgroup of G. More precisely, if $f, g : G^n \longrightarrow A$ are two continuous mappings, we define their sum by the rule

$$(f + g)(\sigma_1, \ldots, \sigma_n) = f(\sigma_1, \ldots, \sigma_n) + g(\sigma_1, \ldots, \sigma_n).$$

It is clear from the commutativity of A that $f + g$ is again an element of $C^n(G, A)$, so it forms a group.

We define a homomorphism $d_n : C^n(G, A) \longrightarrow C^{n+1}(G, A)$ by the formula

$$\begin{aligned}(d_n f)(\sigma_1, \ldots, \sigma_{n+1}) \ &= \ \sigma_1(f(\sigma_2, \ldots, \sigma_{n+1})) + (-1)^{n+1} f(\sigma_1, \ldots, \sigma_n) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{n+1})\end{aligned}$$

such that $d_{n+1} \circ d_n = 0$. The group

$$Z^n(G, A) = \mathrm{Ker}(d_n)$$

is called the group of n-*cocycles*, and the group

$$B^n(G, A) = \mathrm{Im}(d_{n-1})$$

is called the group of n-*coboundaries*. The property $d_{n+1} \circ d_n = 0$ implies that

$$B^n(G, A) \subseteq Z^n(G, A).$$

The n-*th cohomology group of* G *acting on* A is then defined by

$$H^n(G, A) = Z^n(G, A)/B^n(G, A).$$

If $n = 0$, the 0-th cohomology group of G is the group

$$H^0(G, A) = \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in G\}$$

of elements of A that is fixed by every element of G. For $n = 1$, we find that a continuous mapping $f : G \longrightarrow A$ is a 1-cocycle if and only if for all $\sigma, \tau \in G$ one has

$$f(\sigma\tau) = f(\sigma) + \sigma(f(\tau)).$$

Obviously, we have

$$B^1(G, A) = \mathrm{Im}(d_0) = \{d_0 a \mid a \in A\},$$

where, by the definition,

$$(d_0 a)(\sigma) = \sigma(a) - a, \;\; \sigma \in G.$$

Two 1-cocycles f, g from G to A are said to be *cohomologous* if there exists an $a \in A$ such that each $\sigma \in G$ satisfies

$$g(\sigma) - f(\sigma) = \sigma(a) - a.$$

This is an equivalence relation, and 1-th cohomology group $H^1(G, A)$ of G acting on A is just the set of cohomology classes of 1-cocycles.

Let A' be other Abelian group on which G acts and let $\varphi : A \longrightarrow A'$ be a G-homomorphism, that is, a homomorphism that commutes with the action of G. Then φ induces a natural homomorphism

$$\varphi_* : H^1(G, A) \longrightarrow H^1(G, A')$$

defined by $\varphi_*([f]) = [\varphi \circ f]$ for any $[f] \in H^1(G, A)$.

Let $\Phi : G' \longrightarrow G$ be a homomorphism. Then G' acts on A via Φ, and this induces a natural homomorphism

$$\Phi^* : H^1(G, A) \longrightarrow H^1(G', A)$$

defined by $\Phi^*([f]) = [f \circ \Phi]$ for any $[f] \in H^1(G, A)$.

1.2 Rings and ideals

1.2.1 Ideals

For later discussions, we will need some notions of rings. When we speak of a *ring*, we shall always mean a commutative ring with a multiplicative identity element (denoted by 1). Elements x, y of a ring A are said to be *zero divisors* if $x \neq 0,\ y \neq 0$, and $xy = 0$. We define a ring to be *entire* (or *domain*, or *integral domain*) if $1 \neq 0$, and if there are no zero divisors in the ring. A *unit* in A is an element x which divides 1, i.e., an element x such that $xy = 1$ for some $y \in A$. The element y is then uniquely determined by x, and is written x^{-1}. The units in A form a (multiplicative) Abelian group. A *field* is a domain in which every non-zero element is a *unit*.

Let A be a domain. Then A has a *quotient field* or *field of fractions* κ, which is a field containing A as a subring, and any element in κ may be written (not necessarily uniquely) as a ratio of two elements of A. If $a, b \in A$ with $ab \neq 0$, we say that a *divides* b and write $a|b$ if there exists $c \in A$ such that $b = ac$. We say that $d \in A - \{0\}$ is a *greatest common divisor* of a and b if $d|a$, $d|b$, and if any element $e \in A - \{0\}$ which divides both a and b also divides d.

An element x in a ring A is *irreducible* if for any factorization $x = ab$, $a, b \in A$, either a or b is a unit. A domain A is a *unique factorization domain* (or *factorial*) if every non-zero element in A can be factored uniquely, up to units and the ordering of the factors, into a product of irreducible elements.

An *ideal* $\mathfrak{a}$ of a ring A is a subset of A which is an additive subgroup and is such that $A\mathfrak{a} \subseteq \mathfrak{a}$, that is, if $xy \in \mathfrak{a}$ for all $x \in A$ and $y \in \mathfrak{a}$. The quotient group $A/\mathfrak{a}$ inherits a uniquely defined multiplication from A which makes it into a ring, called the *quotient ring* (or *residue-class ring*). The elements of $A/\mathfrak{a}$ are the cosets of $\mathfrak{a}$ in A, and the mapping $p : A \longrightarrow A/\mathfrak{a}$ which maps each $x \in A$ to its coset $x + \mathfrak{a}$ is a surjective ring homomorphism.

If $f : A \longrightarrow B$ is any ring homomorphism, the *kernel* of f $(= f^{-1}(0))$ is an ideal $\mathfrak{a}$, and the *image* of f $(= f(A))$ is a subring C of B; and f induces a ring isomorphism $A/\mathfrak{a} \cong C$.

We shall sometimes use the notation $x \equiv y \pmod{\mathfrak{a}}$; this means that $x - y \in \mathfrak{a}$.

The set of multiples of a particular element $a \in A$, or equivalently, the set of elements divisible by a, forms an ideal called the *principal ideal* generated by a, denoted by (a) or Aa. x is a unit if and only if $(x) = A = (1)$. The *zero ideal* (0) is usually denoted by 0.

We say that the an ideal $\mathfrak{a}$ of a ring A is *proper* if $\mathfrak{a} \neq A$. A proper ideal $\mathfrak{p}$ in A is said to be *prime* if $xy \in \mathfrak{p}$ for $x, y \in A$ means $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. It is easy to show that $x \in A - \{0\}$ is irreducible if the principal ideal (x) is prime. A proper ideal $\mathfrak{q}$ in A is said to be *primary* if $xy \in \mathfrak{q}$ for $x, y \in A$ means $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$. By a *chain* of prime ideals of the ring A we mean a finite strictly increasing sequence

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n;$$

the *length* of the chain is n. The *height* of a prime ideal $\mathfrak{p}$ in A is the supremum of all integers n such that there exists a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ of distinct prime ideals. We define the *dimension* (or *Krull dimension*) of A to be the supremum of the lengths of all chains of prime ideals in A; it is an integer ≥ 0, or $+\infty$ (assuming $A \neq 0$). An ideal $\mathbf{m}$ in A is *maximal* if $m \neq (1)$ and if there is no ideal $\mathfrak{a}$ such that $\mathbf{m} \subset \mathfrak{a} \subset (1)$ (*strict* inclusions). Equivalently:

$\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is an integral domain;

$\mathbf{m}$ is maximal if and only if $A/\mathbf{m}$ is a field.

Hence a maximal ideal is prime. A standard application of Zorn's lemma shows that every ring $A \neq 0$ has at least one maximal ideal.

Proposition 1.11. *The following conditions on a ring A are equivalent:*

(i) *The set of non-units in A forms an ideal $\mathbf{m}$.*

(ii) *A has a unique maximal ideal $\mathbf{m}$ which contains every proper ideal of A.*

Proof. (i)⇒(ii). Every ideal $\neq (1)$ consists of non-units, hence is contained in $\mathbf{m}$. Thus $\mathbf{m}$ is the only maximal ideal of A.

(ii)⇒(i). Take $x \in A - \mathbf{m}$. If x is not a unit, the principal ideal (x) is not (1). Then there exists a maximal ideal $\mathbf{m}'$ of A containing (x). Since $\mathbf{m}$ is unique, it follows $\mathbf{m}' = \mathbf{m}$, and so $(x) \subseteq \mathbf{m}$. This is a contradiction. Hence x must be a unit, that is, $\mathbf{m}$ consists of all non-units in A. □

A ring satisfying the conditions of Proposition 1.11 is called a *local ring*. The field $A/\mathbf{m}$ is called the *residue field* of A.

Let A be any ring. A *multiplicatively closed subset* of A is a subset S of A such that $1 \in S, 0 \notin S$ and S is closed under multiplication: in other words S is a subsemigroup of the multiplicative semigroup of A. Let S be a multiplicatively closed subset of A and define an equivalence relation on the set $A \times S$ by calling two pairs (a, s) and (b, t) equivalent if $at = bs$. It is an exercise to show that this is an equivalence relation. Let a/s denote the equivalence class containing the pair (a, s). Write

$$S^{-1}A = \{a/s \mid a \in A, s \in S\}.$$

We put a ring structure on $S^{-1}A$ by defining addition and multiplication of these fractions a/s in the same way as in elementary algebra: that is,

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

The ring $S^{-1}A$ is called the *ring of fractions* of A with respect to S. If A is an integral domain and $S = A - \{0\}$, then $S^{-1}A$ is the field of fractions of A.

Let $\mathfrak{p}$ be a prime ideal of a ring A. Then $S = A - \mathfrak{p}$ is multiplicatively closed (in fact $A - \mathfrak{p}$ is multiplicatively closed if and only if $\mathfrak{p}$ is prime). We write $A_\mathfrak{p}$ for $S^{-1}A$ in this case, and so we obtain the *ring of fractions* of A with respect to $A - \mathfrak{p}$

$$A_\mathfrak{p} = \{a/b \mid a \in A, b \in A - \mathfrak{p}\}.$$

The set

$$\mathbf{m} = \{a/b \in A_\mathfrak{p} \mid a \in \mathfrak{p}, b \in A - \mathfrak{p}\}$$

form an ideal in $A_\mathfrak{p}$. If $c/d \notin \mathbf{m}$, then $c \notin \mathfrak{p}$, hence c/d is a unit in $A_\mathfrak{p}$. It follows that if $\mathfrak{a}$ is an ideal in $A_\mathfrak{p}$ and $\mathfrak{a} \nsubseteq \mathbf{m}$, then $\mathfrak{a}$ contains a unit and is therefore the whole ring. Hence $\mathbf{m}$ is the only maximal ideal in $A_\mathfrak{p}$; in other words, $A_\mathfrak{p}$ is a local ring. The ring $A_\mathfrak{p}$ is called *localization* of A at $\mathfrak{p}$.

If $\mathfrak{a}$, $\mathfrak{b}$ are ideals in a ring A, their *sum* $\mathfrak{a} + \mathfrak{b}$ is the set of all $x + y$ where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. It is the smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b}$. The *intersection* of any family $\{\mathfrak{a}_i\}_{i \in I}$ of ideals is an ideal. The *product* of two ideals $\mathfrak{a}$, $\mathfrak{b}$ in A is the ideal $\mathfrak{ab}$ generated by all products xy, where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. We set $\mathfrak{a}^0 = (1)$, $\mathfrak{a}^1 = \mathfrak{a}$ and for each positive rational integer m we set $\mathfrak{a}^{m+1} = \mathfrak{a}^m\mathfrak{a}$ so that $\mathfrak{a}^{p+q} = \mathfrak{a}^p\mathfrak{a}^q$ as with ordinary powers. It follows directly from this definition that multiplication of ideals is commutative and associative

$$\mathfrak{ab} = \mathfrak{ba}, \quad \mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\mathfrak{c}.$$

Also there is the distributive law

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}.$$

Two ideals $\mathfrak{a}$, $\mathfrak{b}$ in a ring A are said to be *coprime* if $\mathfrak{a} + \mathfrak{b} = (1)$. Thus for coprime ideals we have $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$. Clearly two ideals $\mathfrak{a}$, $\mathfrak{b}$ are coprime if and only if there exist $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ such that $x + y = 1$.

Proposition 1.12. *Let A be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals of A. If $\mathfrak{a}_i$, $\mathfrak{a}_j$ are coprime whenever $i \neq j$, then $\prod \mathfrak{a}_i = \cap \mathfrak{a}_i$.*

Proof. By induction on n, the case $n = 2$ is dealt with above. Suppose $n > 2$ and the result true for $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}$, and let

$$\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i.$$

Since $\mathfrak{a}_i + \mathfrak{a}_n = (1)$ $(1 \leq i \leq n-1)$, we have equations

$$x_i + y_i = 1 \ \ (x_i \in \mathfrak{a}_i, \ y_i \in \mathfrak{a}_n),$$

and therefore

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1}(1-y_i) \equiv 1 \pmod{\mathfrak{a}_n}.$$

Hence $\mathfrak{a}_n + \mathfrak{b} = (1)$ and so

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i. \qquad \square$$

Theorem 1.13 (Chinese Remainder Theorem). *Let A be a ring with identity and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ a set of ideals in A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for $i \neq j$. Let $\mathfrak{A} = \bigcap \mathfrak{a}_i$. Then the diagonal mapping*

$$x \longmapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$$

induces an isomorphism of rings

$$A/\mathfrak{A} \cong A/\mathfrak{a}_1 \oplus \cdots \oplus A/\mathfrak{a}_n.$$

If $\mathfrak{a}$, $\mathfrak{b}$ are ideals in a ring A, their *ideal quotient* is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\},$$

which is an ideal such that $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$, and

$$(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}. \tag{1.4}$$

If the equality in (1.4) holds, we also write $\mathfrak{a}/\mathfrak{b}$ in place of $(\mathfrak{a} : \mathfrak{b})$. In particular, $(0 : \mathfrak{b})$ is called the *annihilator* of $\mathfrak{b}$ and is also denoted by $\mathrm{Ann}(\mathfrak{b})$: it is the set of all $x \in A$ such that $x\mathfrak{b} = 0$. Also $(A : \mathfrak{b})$ is called the *generalized inverse* of $\mathfrak{b}$. Further, if $(A : \mathfrak{b})\mathfrak{b} = A$, we also write $\mathfrak{b}^{-1}$ or $1/\mathfrak{b}$ in place of $(A : \mathfrak{b})$ and call $\mathfrak{b}$ *invertible*.

An element x of A is Nilpotent if $x^n = 0$ for some $n > 0$. The set $\mathrm{Nil}(A)$ of all Nilpotent elements in A, called the *nilradical* of A, is an ideal, and

$$A_{\mathrm{red}} = A/\mathrm{Nil}(A)$$

has no Nilpotent element $\neq 0$. Also $\mathrm{Nil}(A)$ is the intersection of all prime ideals of A. The *Jacobson radical* $\mathrm{Jac}(A)$ of A is defined to be the intersection of all the maximal ideals of A. It can be characterized as follows: $x \in \mathrm{Jac}(A)$ if and only if $1 - xy$ is a unit in A for all $y \in A$.

If $\mathfrak{a}$ is any ideal of A, the *radical* of $\mathfrak{a}$ is defined to be the ideal

$$\sqrt{\mathfrak{a}} = \{x \in A \mid x^r \in \mathfrak{a} \text{ for some } r > 0\}.$$

Proposition 1.14. *Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals in a ring A such that $\sqrt{\mathfrak{a}}$, $\sqrt{\mathfrak{b}}$ are coprime. Then $\mathfrak{a}$, $\mathfrak{b}$ are coprime.*

Proof. It is easy to show

$$\sqrt{\mathfrak{a}+\mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}} = \sqrt{1} = (1),$$

and hence $\mathfrak{a}+\mathfrak{b} = (1)$. □

A ring is called *Noetherian* if every ideal in the ring is finitely generated. Fields are Noetherian rings. A basic fact is the following *Hilbert basis theorem*:

Theorem 1.15. *If A is a Noetherian ring, then the ring $A[X_1, \ldots, X_n]$ of polynomials in n variables over A is a Noetherian ring.*

Proof. See Fulton [71], Atiyah–Macdonald [2], Theorem 7.5 or Lang [146], Section 6.2. □

Theorem 1.16 (Krull's Hauptidealsatz). *Let A be a Noetherian ring, and let $f \in A$ be an element which is neither a zero divisor nor a unit. Then every minimal prime ideal $\mathfrak{p}$ containing f has height* 1.

Proof. Atiyah–Macdonald [2], p. 122. □

Proposition 1.17. *A Noetherian integral domain A is a unique factorization domain if and only if every prime ideal of height* 1 *is principal.*

Proof. Matsumura [173], p. 141. □

A sequence $x_1, \ldots, x_r$ of elements of a ring A is called a *regular sequence* for A if x_1 is not a zero divisor in A, and for all $i = 2, \ldots, r$, x_i is not a zero divisor in the ring $A/(x_1, \ldots, x_{i-1})$, where

$$(x_1, \ldots, x_{i-1}) = \{a_1x_1 + \cdots + a_{i-1}x_{i-1} \mid a_j \in A\}$$

is the ideal generated by $x_1, \ldots, x_{i-1}$. If A is a local ring with maximal ideal $\mathbf{m}$, then the *depth* of A is the maximum length of a regular sequence $x_1, \ldots, x_r$ for A with all $x_i \in \mathbf{m}$. We say that a local Noetherian ring A is *Cohen–Macaulay* if $\operatorname{depth} A = \dim A$. Now we list some properties of Cohen–Macaulay rings.

Proposition 1.18. *Let A be a local Noetherian ring with maximal ideal $\mathbf{m}$.*

(a) *If A is regular, that is, $\dim_\kappa \mathbf{m}/\mathbf{m}^2 = \dim A$, where $\kappa = A/\mathbf{m}$ is the residue class field, then it is Cohen–Macaulay.*

(b) *If A is Cohen–Macaulay, then any localization $A_\mathfrak{p}$ of A at a prime ideal $\mathfrak{p}$ is also Cohen–Macaulay.*

(c) *If A is Cohen–Macaulay, then a set of elements $x_1, \ldots, x_r \in \mathbf{m}$ forms a regular sequence for A if and only if $\dim A/(x_1, \ldots, x_r) = \dim A - r$.*

(d) *If A is Cohen–Macaulay, and $x_1, \dots, x_r \in \mathbf{m}$ is a regular sequence for A, then $A/(x_1, \dots, x_r)$ is also Cohen–Macaulay.*

(e) *If A is Cohen–Macaulay, and $x_1, \dots, x_r \in \mathbf{m}$ is a regular sequence, let $\mathfrak{x}$ be the ideal $(x_1, \dots, x_r)$. Then the natural mapping $(A/\mathfrak{x})[t_1, \dots, t_r] \to \oplus_{n\geq 0}\mathfrak{x}^n/\mathfrak{x}^{n+1}$, defined by sending $t_i \mapsto x_i$, is an isomorphism. In other words, $\mathfrak{x}/\mathfrak{x}^2$ is a free $A/\mathfrak{x}$-module of rank r, and for each $n \geq 1$, the natural mapping $S^n(\mathfrak{x}/\mathfrak{x}^2) \to \mathfrak{x}^n/\mathfrak{x}^{n+1}$ is an isomorphism, where S^n denotes the n-th symmetric power.*

Proof. Matsumura [173]: (a) p. 121; (b) p. 104; (c) p. 105; (d) p. 104; (e) p. 110 or Hartshorne [90], Theorem 8.21A. □

Proposition 1.19. *Let Σ be the set of submodules of a module M, ordered by the relation $\subseteq$. The following conditions on Σ are equivalent:*

(I) *Every increasing sequence $M_1 \subseteq M_2 \subseteq \cdots$ in Σ is stationary (i.e., there exists n such that $M_n = M_{n+1} = \cdots$).*

(II) *Every non-empty subset of Σ has a maximal element.*

Proof. (I) $\Rightarrow$ (II). If (II) is false, there is a non-empty subset Λ of Σ with no maximal element, and we can construct inductively a non-terminating strictly increasing sequence in Λ.

(II) $\Rightarrow$ (I). The set $\{M_i\}_{i\geq 1}$ has a maximal element, say M_n. □

The condition (I) is called the *ascending chain condition*, and (II) the *maximal condition*. A module M satisfying either of these equivalent conditions is said to be *Noetherian*.

Proposition 1.20. *M is a Noetherian A-module if and only if every submodule of M is finitely generated.*

Proof. Suppose that M is Noetherian. Let N be a submodule of M, and let Σ be the set of all finitely generated submodules of N. Since $0 \in \Sigma$, then Σ is not empty and therefore has a maximal element, say N_0. If $N_0 \neq N$, consider the submodule $N_0 + Ax$, where $x \in N$, $x \notin N_0$; this is finitely generated and strictly contains N_0, so we have a contradiction. Hence $N = N_0$ and therefore N is finitely generated.

Next assume that every submodule of M is finitely generated. Let $M_1 \subseteq M_2 \subseteq \cdots$ be an ascending chain of submodules of M. Then $N = \bigcup_{i=1}^{\infty} M_i$ is a submodule of M, hence is finitely generated, say by $w_1, \dots, w_r$. Say $w_i \in M_{n_i}$ and let

$$n = \max_{1\leq i\leq r} n_i;$$

then each $w_i \in M_n$, hence $M_n = N$ and therefore the chain is stationary. □

An ideal $\mathfrak{a}$ is said to be *irreducible* if $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ means either $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$.

Proposition 1.21. *In a Noetherian ring A every ideal is a finite intersection of irreducible ideals.*

Proof. Suppose not; then the set of ideals in A for which the proposition is false is not empty, hence has a maximal element $\mathfrak{a}$. Since $\mathfrak{a}$ is not irreducible, we have $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ where $\mathfrak{a} \subset \mathfrak{b}$ and $\mathfrak{a} \subset \mathfrak{c}$. Hence each of $\mathfrak{b}, \mathfrak{c}$ is a finite intersection of irreducible ideals and therefore so is $\mathfrak{a}$: contradiction. □

Proposition 1.22. *In a Noetherian ring A every irreducible ideal is primary.*

Proof. By passing to the quotient ring, it is enough to show that if the zero ideal is irreducible then it is primary. Let $xy = 0$ with $y \neq 0$, and consider the chain of ideals

$$\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \cdots .$$

By the ascending chain condition, this chain is stationary, i.e., we have

$$\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) = \cdots$$

for some n. It follows that $(x^n) \cap (y) = 0$; for if $a \in (y)$ then $ax = 0$, and if $a \in (x^n)$ then $a = bx^n$, hence $bx^{n+1} = 0$, hence $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$, hence $bx^n = 0$; that is, $a = 0$. Since (0) is irreducible and $(y) \neq 0$ we must therefore have $x^n = 0$, and this shows that (0) is primary. □

A *primary decomposition* of an ideal $\mathfrak{a}$ in A is an expression of $\mathfrak{a}$ as a finite intersection of primary ideals, say

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i. \tag{1.5}$$

We shall say that $\mathfrak{a}$ is *decomposable* if it has a primary decomposition. If moreover the $\sqrt{\mathfrak{q}_i}$ are all distinct, and we have

$$\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i \ \ (1 \leq i \leq n)$$

the primary decomposition (1.5) is said to be *minimal*. It is easy to show that any primary decomposition can be reduced to a minimal one. If the primary decomposition (1.5) is minimal, the minimal elements of the set $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$ are called the *minimal prime ideals* belonging to $\mathfrak{a}$.

Proposition 1.23. *Let $\mathfrak{a}$ be a decomposable ideal with a minimal primary decomposition* (1.5)*. Then the primary components $\mathfrak{q}_i$ corresponding to minimal prime ideals belonging to $\mathfrak{a}$ are uniquely determined by $\mathfrak{a}$.*

Proof. See M. F. Atiyah and I. G. Macdonald [2], Chapter 4. □

From Proposition 1.21 and Proposition 1.22 we have at once:

Theorem 1.24. *In a Noetherian ring A every ideal has a primary decomposition.*

Theorem 1.25. *Let A be a Noetherian domain of dimension* 1. *Then every non-zero ideal $\mathfrak{a}$ in A can be uniquely expressed as a product of primary ideals whose radicals are all distinct.*

Proof. Since A is Noetherian, $\mathfrak{a}$ has a minimal primary decomposition (1.5) by Theorem 1.24. Since $\dim A = 1$ and A is an integral domain, each non-zero prime ideal of A is maximal, hence the prime ideals $\sqrt{\mathfrak{q}_i}$ are distinct maximal ideals (since $\sqrt{\mathfrak{q}_i} \supseteq \mathfrak{q}_i \supseteq \mathfrak{a} \neq 0$), and are therefore pairwise coprime. Hence by Proposition 1.14, the $\mathfrak{q}_i$ are pairwise coprime and therefore by Proposition 1.12 we have

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i = \prod_{i=1}^{n} \mathfrak{q}_i.$$

Conversely, if $\mathfrak{a} = \prod \mathfrak{q}_i$, the same argument shows that $\mathfrak{a} = \bigcap \mathfrak{q}_i$; this is a minimal primary decomposition of $\mathfrak{a}$, in which each $\mathfrak{q}_i$ is an minimal primary component (i.e., the primary component $\mathfrak{q}_i$ corresponding to a minimal prime ideal belonging to $\mathfrak{a}$), and is therefore unique by Proposition 1.23. □

1.2.2 Completion of topological groups

We simply introduce the completion of a topological Abelian group under a fixed topology. Let G be a topological Abelian group (written additively): thus G is both a topological space and an Abelian group, and the two structures on G are compatible in the sense that the mappings

$$G \times G \longrightarrow G, \ \ (x, y) \mapsto x + y$$

and

$$G \longrightarrow G, \ \ x \mapsto -x$$

are continuous. If $\{0\}$ is closed in G, then the diagonal is closed in $G \times G$ (being the inverse image of $\{0\}$ under the mapping $(x, y) \mapsto x - y$) and so G is Hausdorff. If a is a fixed element of G, the translation T_a defined by $T_a(x) = x + a$ is a homeomorphism of G onto G (for T_a is continuous, and its inverse is T_{-a}); hence if U is any neighborhood of 0 in G, then $U + a$ is a neighborhood of a in G, and conversely every neighborhood of a appears in this form. Thus the topology of G is uniquely determined by the neighborhoods of 0 in G. Obviously, G is Hausdorff if and only if the intersection of all neighborhoods of 0 in G is equal to 0.

Assume for simplicity that $0 \in G$ has a countable fundamental system of neighborhoods. Then the *completion* $\hat{G}$ of G may be defined in the usual way by means

of Cauchy sequences. A *Cauchy sequence* in G is defined to be a sequence $\{x_n\}$ of elements of G such that, for any neighborhood U of 0, there exists an integer $N(U)$ with the property that $x_m - x_n \in U$ for all $m, n \geq N(U)$. Two Cauchy sequences $\{x_n\}$ and $\{y_n\}$ are *equivalent* if $x_n - y_n \to 0$ in G. The set of all equivalence classes of Cauchy sequences is denoted by $\hat{G}$. If $\{x_n\}$ and $\{y_n\}$ are Cauchy sequences, so is $\{x_n + y_n\}$, and its class in $\hat{G}$ depends only on the classes of $\{x_n\}$ and $\{y_n\}$. Hence we have an addition in $\hat{G}$ with respect to which $\hat{G}$ is an Abelian group. For each $x \in G$, the class of the constant sequence $\{x\}$ is an element $\phi(x)$ of $\hat{G}$, and $\phi : G \longrightarrow \hat{G}$ is a homomorphism of Abelian groups. Note that

$$\mathrm{Ker}(\phi) = \bigcap U,$$

where U runs through all neighborhoods of 0 in G, and so ϕ is injective if and only if G is Hausdorff. If $\phi : G \longrightarrow \hat{G}$ is an isomorphism, we shall say that G is *complete*.

Now we restrict ourselves to the special kind of topologies occurring in commutative algebra, namely we assume that $0 \in G$ has a fundamental system of neighborhoods consisting of subgroups. Thus we have a sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n \supseteq \cdots$$

and $U \subseteq G$ is a neighborhood of 0 if and only if it contains some G_n. A typical example is the p-adic topology on $\mathbb{Z}$, in which $G_n = p^n\mathbb{Z}$. For topologies given by sequences of subgroups there is an alternative purely algebraic definition of the completion. Suppose $\{x_m\}$ is a Cauchy sequence in G. Then the image of x_m in G/G_n is ultimately constant, equal say to ξ_n. If we pass from $n+1$ to n it is clear that $\xi_{n+1} \mapsto \xi_n$ under the projection

$$\theta_{n+1} : G/G_{n+1} \longrightarrow G/G_n.$$

Thus a Cauchy sequence $\{x_m\}$ in G defines a *coherent sequence* $\{\xi_n\}$ in the sense that

$$\theta_{n+1}(\xi_{n+1}) = \xi_n, \;\; n \geq 0.$$

Moreover it is clear that Cauchy sequences which are equivalent to $\{x_m\}$ define the same sequence $\{\xi_n\}$. Finally, given any coherent sequence $\{\xi_n\}$, we can construct a Cauchy sequence $\{x_n\}$ giving rise to it by taking x_n to be any element in the coset ξ_n (so that $x_{n+1} - x_n \in G_n$). Thus $\hat{G}$ can equally well be defined as the set of coherent sequences $\{\xi_n\}$ with the obvious group structure.

We have now arrived at a special case of inverse limits. More generally, consider any sequence of groups $\{A_n\}$ and homomorphism

$$\theta_{n+1} : A_{n+1} \longrightarrow A_n.$$

We call this an *inverse system*, and the group of all coherent sequences $\{a_n\}$ (i.e., $a_n \in A_n$ and $\theta_{n+1}(a_{n+1}) = a_n$) is called the *inverse limit* of the system. It is usually

written $\varprojlim A_n$. If the homomorphisms θ_n are always surjective, the inverse system $\{A_n\}$ is called a *surjective system*. With this notation we have

$$\hat{G} \cong \lim_{\leftarrow} G/G_n.$$

The most important class of examples of topological groups of the kind we are considering are given by taking

$$G = A, \quad G_n = \mathfrak{a}^n,$$

where $\mathfrak{a}$ is an ideal in a ring A. The topology so defined on A is called the $\mathfrak{a}$-*adic topology*, or just the $\mathfrak{a}$-*topology*. Since the $\mathfrak{a}^n$ are ideals, it is not hard to check that with this topology A is a *topological ring*, i.e. that the ring operations are continuous. The topology is Hausdorff if and only if $\bigcap \mathfrak{a}^n = (0)$. The completion $\hat{A}$ of A is again a topological ring; $\phi : A \longrightarrow \hat{A}$ is a continuous ring homomorphism, whose kernel is $\bigcap \mathfrak{a}^n$.

Similarly, if M is any A-module, we define

$$\hat{M} = \lim_{\leftarrow} M/\mathfrak{a}^n M,$$

and call it the $\mathfrak{a}$-*adic completion* of M. It has a nature structure of $\hat{A}$-module.

Proposition 1.26. *If A is a Noetherian ring, $\mathfrak{a}$ an ideal of A, $\hat{A}$ its $\mathfrak{a}$-adic completion, then*

⟨1⟩ $\hat{\mathfrak{a}} = \hat{A}\mathfrak{a}$; $\hat{\mathfrak{a}^n} = \hat{\mathfrak{a}}^n = \hat{A}\mathfrak{a}^n$; $\hat{A}/\hat{\mathfrak{a}}^n \cong A/\mathfrak{a}^n$;

⟨2⟩ $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$;

⟨3⟩ $\hat{\mathfrak{a}}$ *is contained in the Jacobson radical of* $\hat{A}$;

⟨4⟩ $\hat{A}$ *is Noetherian;*

⟨5⟩ *If A is a Noetherian domain, $\mathfrak{a} \neq (1)$, then $\bigcap \mathfrak{a}^n = 0$;*

⟨6⟩ *If A is a Noetherian local ring, $\mathfrak{a}$ its maximal ideal, then $\hat{A}$ is a local ring with maximal ideal $\hat{\mathfrak{a}}$; the $\mathfrak{a}$-topology of A is Hausdorff;*

⟨7⟩ *If M is a finitely generated A-module, then $\hat{M} \cong M \otimes_A \hat{A}$.*

Proof. See M. F. Atiyah and I. G. Macdonald [2], Chapter 10. □

1.2.3 Fractional ideals

Let A be an integral domain, κ its field of fractions. An A-submodule $\mathfrak{g}$ of κ is to be called a *fractional ideal* of A if $\omega\mathfrak{g} \subseteq A$ for some $\omega \neq 0$ in A. If $\mathfrak{g}$ is an A-submodule of κ, we also define the *generalized inverse* of $\mathfrak{g}$

$$(A : \mathfrak{g}) = \{\alpha \in \kappa \mid \alpha\mathfrak{g} \subseteq A\}.$$

Every ideal $\mathfrak{g}$ of A is a fractional ideal (take $\omega = 1$). If we wish to emphasize that the fractional ideal $\mathfrak{g}$ is actually contained in A, we say $\mathfrak{g}$ is an *integral ideal*. Any element $\alpha \in \kappa$ generates a fractional ideal, denoted by (α) or αA, and called *principal*.

Every finitely generated A-submodule $\mathfrak{g}$ of κ is a fractional ideal. For if $\mathfrak{g}$ is generated by $\beta_1, \ldots, \beta_r \in \kappa$, we can write

$$\beta_i = \frac{\alpha_i}{\omega}, \;\; i = 1, 2, \ldots, r,$$

where α_i and ω are in A, and then $\omega\mathfrak{g} \subseteq A$. Conversely, if A is Noetherian, every fractional ideal $\mathfrak{g}$ is finitely generated, for it of the form $\omega^{-1}\mathfrak{a}$ for some integral ideal $\mathfrak{a}$.

Let $\mathfrak{I}_A$ denote the set of nonzero fractional ideals of A. If $\mathfrak{g}$ and $\mathfrak{h}$ are A-submodules of κ, their *product* $\mathfrak{g}\mathfrak{h}$ is the collection of all sums $\sum g_i h_i$ with $g_i \in \mathfrak{g}$ and $h_i \in \mathfrak{h}$. Then it is easy to see that $\mathfrak{I}_A$ is a commutative semigroup.

An A-submodule $\mathfrak{g}$ of κ is called *invertible* if there exists a A-submodule $\mathfrak{h}$ of κ such that $\mathfrak{g}\mathfrak{h} = A$. The module $\mathfrak{h}$ is then unique and equal to $(A : \mathfrak{g})$ for we have

$$\mathfrak{h} \subseteq (A : \mathfrak{g}) = (A : \mathfrak{g})\mathfrak{g}\mathfrak{h} \subseteq A\mathfrak{h} = \mathfrak{h}.$$

If $\mathfrak{g}$ is invertible, it follows that $\mathfrak{g}$ is finitely generated, and therefore a fractional ideal: for since $\mathfrak{g}(A : \mathfrak{g}) = A$, there exist $\beta_i \in \mathfrak{g}$ and $\gamma_i \in (A : \mathfrak{g})$ $(1 \leq i \leq r)$ such that

$$\beta_1\gamma_1 + \beta_2\gamma_2 + \cdots + \beta_r\gamma_r = 1,$$

and hence for any $\alpha \in \mathfrak{g}$ we have

$$\alpha = \sum_{i=1}^{r} (\gamma_i\alpha)\beta_i,$$

with each $\gamma_i\alpha \in A$, so that $\mathfrak{g}$ is generated by $\beta_1, \ldots, \beta_r$. Clearly every non-zero principal factional ideal (α) is invertible, its inverse being (α^{-1}). The invertible ideals form a group with respect to multiplication, whose identity element is $A = (1)$. Invertibility is a local property, that is, a fractional ideal $\mathfrak{g}$ is invertible if and only if $\mathfrak{g}$ is finitely generated and, for each prime ideal $\mathfrak{p}$, $\mathfrak{g}_\mathfrak{p}$ is invertible, equivalently, $\mathfrak{g}$ is finitely generated and, for each maximal ideal $\mathbf{m}$, $\mathfrak{g}_\mathbf{m}$ is invertible.

1.2.4 Relative differentials

Here we review the algebraic theory of E. Kähler differentials. Let A be a ring (commutative with identity as always), let B be an A-algebra, and let M be a B-module. An *A-derivation* of B into M is a mapping $d : B \longrightarrow M$ such that d is additive,

$$d(xy) = x\,dy + y\,dx, \;\; \{x, y\} \subset B,$$

and $da = 0$ for all $a \in A$. We define the *module of relative differential forms* of B over A to be a B-module $\Omega_{B/A}$, together with an A-derivation $d : B \longrightarrow \Omega_{B/A}$, which satisfies the following universal property: for any B-module M, and for any A-derivation $d' : B \longrightarrow M$, there exists a unique B-module homomorphism $f : \Omega_{B/A} \longrightarrow M$ such that $d' = f \circ d$. The elements in $\Omega_{B/A}$ are called *Kähler differentials*.

Clearly one way to construct such a module $\Omega_{B/A}$ is to take the free B-module F generated by the symbols $\{dx \mid x \in B\}$, and to divide out by the submodule generated by all expressions of the form (1) $d(x+y)-dx-dy$ for $x, y \in B$, (2) $d(xy)-xdy-ydx$ for $x, y \in B$, and (3) da for $a \in A$. The derivation $d : B \longrightarrow \Omega_{B/A}$ is defined by sending x to dx. Thus we see that $\Omega_{B/A}$ exists. It follows from the definition that the pair $(\Omega_{B/A}, d)$ is unique up to unique isomorphism. As a corollary of this construction, we see that $\Omega_{B/A}$ is generated as a B-module by $\{dx \mid x \in B\}$.

Concretely, we may consider the homomorphism

$$m : B \otimes_A B \longrightarrow B, \;\; x \otimes y \mapsto xy,$$

whose kernel we denote by I. Then

$$\Omega_{B/A} := I/I^2 = I \otimes_{B \otimes B} B \tag{1.6}$$

is a $B \otimes B$-module, and hence in particular also a B-module, via the embedding

$$B \longrightarrow B \otimes B, \;\; x \mapsto x \otimes 1.$$

If we put

$$dx = x \otimes 1 - 1 \otimes x \bmod I^2,$$

then we obtain an A-derivation

$$d : B \longrightarrow \Omega_{B/A}.$$

One can show that d is universal among all A-derivation of B with values in B-modules. Hence $\Omega_{B/A}$ is a module of relative differential forms of B over A, and its elements are the linear combinations $\sum y_i dx_i$.

If A' is any commutative A-algebra and $B' = B \otimes_A A'$, then it is easy to see that

$$\Omega_{B'/A'} = \Omega_{B/A} \otimes_A A'. \tag{1.7}$$

Furthermore, if S is a multiplicative system in B, then

$$\Omega_{S^{-1}B/A} \cong S^{-1}\Omega_{B/A}.$$

Thus the module of relative differential forms is preserved under completion and localization.

Let $A \longrightarrow B \longrightarrow C$ be rings and homomorphisms. Then there is a nature exact sequence of C-modules

$$\Omega_{B/A} \otimes_B C \longrightarrow \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0, \tag{1.8}$$

called *first exact sequence*.

1.3 Integral elements and valuations

1.3.1 Integral elements

Let B be a ring and A a subring of B (so that $1 \in A$). An element α of B is said to be *integral* over A if it satisfies a monic equation over A:

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \tag{1.9}$$

where $a_i \in A$ for $i = 1, \ldots, n$. Clearly every element of A is integral over A.

Proposition 1.27. *The following are equivalent:*

(1) $\alpha \in B$ *is integral over* A*;*

(2) $A[\alpha]$ *is a finitely generated* A*-module;*

(3) $A[\alpha]$ *is contained in a subring* C *of* B *such that* C *is a finitely generated* A*-module;*

(4) *There exists a faithful* $A[\alpha]$*-module* M *(that is,* $\mathrm{Ann}(M) = 0$*) which is finitely generated as an* A*-module.*

Proof. (1)⇒(2). From (1.9) we have

$$\alpha^{n+r} = -a_1\alpha^{n+r-1} - \cdots - a_n x^r$$

for all $r \geq 0$; hence, by induction, all positive powers of α lie in the A-module generated by $1, \alpha, \ldots, \alpha^{n-1}$. Hence $A[\alpha]$ is generated (as an A-module) by $1, \alpha, \ldots, \alpha^{n-1}$.

(2)⇒(3). Take $C = A[\alpha]$.

(3)⇒(4). Take $M = C$, which is a faithful $A[\alpha]$-module since $yC = 0$ implies $y \cdot 1 = 0$.

(4)⇒(1). We consider an $A[\alpha]$-module endomorphism ϕ of M defined by $\phi(x) = \alpha x$ for $x \in M$. Obviously, $\phi(M) = \alpha M \subseteq M$ since M is an $A[\alpha]$-module. We claim that ϕ satisfies an equation of the form

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0,$$

where the a_i are in A. Let $x_1, \ldots, x_n$ be a set of generators of M. Then each $\phi(x_i) \in M$, so that we have

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j \ \ (1 \leq i \leq n;\ a_{ij} \in A),$$

i.e.,

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij})x_j = 0$$

where δ_{ij} is the Kronecker delta. By multiplying on the left by the adjoint of the matrix $(\delta_{ij}\phi - a_{ij})$ it follows that $\det(\delta_{ij}\phi - a_{ij})$ annihilates each x_i, hence is the zero endomorphism of M. Expanding out the determinant, we have an equation of the required form. Since M is faithful, we obtain an equation of the form (1.9). □

Proposition 1.28. *Let α_i $(1 \leq i \leq n)$ be elements of B, each integral over A. Then the ring $A[\alpha_1, \ldots, \alpha_n]$ is a finitely generated A-module.*

Proof. In fact, by induction on n, the case $n = 1$ is part of Proposition 1.27. Assume $n > 1$, let $A_r = A[\alpha_1, \ldots, \alpha_r]$; then by the inductive hypothesis A_{n-1} is a finitely generated A-module. By the case $n = 1$, $A_n = A_{n-1}[\alpha_n]$ is a finitely generated A_{n-1}-module since α_n is integral over A_{n-1}. Hence A_n is finitely generated as an A-module. □

In particular, the set $\bar{A}$ of elements of B which are integral over A is a subring of B containing A, since, if $\alpha, \beta \in \bar{A}$, then $A[\alpha, \beta]$ is a finitely generated A-module by the above fact, and hence $\alpha \pm \beta$ and $\alpha\beta$ are integral over A, by (3) of Proposition 1.27. The ring $\bar{A}$ is called the *integral closure* of A in B. If $\bar{A} = A$, that is, every element of B integral over A lies in A, then A is said to be *integrally closed* in B. If $\bar{A} = B$, the ring B is said to be *integral over* A.

Further, if $A \subseteq B \subseteq C$ are rings and if B is integral over A, and C is integral over B, then C is integral over A (*transitivity of integral dependence*). In fact, if $\alpha \in C$, then we have an equation

$$\alpha^n + b_1\alpha^{n-1} + \cdots + b_n = 0 \ \ (b_i \in B).$$

The ring $B' = A[b_1, \ldots, b_n]$ is a finitely generated A-module, and $B'[\alpha]$ is a finitely generated B'-module since α is integral over B'. Hence $B'[\alpha]$ is a finitely generated A-module, and therefore α is integral over A by (3) of Proposition 1.27. Moreover, a prime ideal $\mathfrak{p}$ of B is maximal if and only if $\mathfrak{p} \cap A$ is maximal in A.

An integral domain A is called *integrally closed* if it is integrally closed in its field of fractions. Integral closure is a local property, that is, an integral domain A is integrally closed if and only if $A_\mathfrak{p}$ is integrally closed, for each prime ideal $\mathfrak{p}$, equivalently, $A_\mathbf{m}$ is integrally closed, for each maximal ideal $\mathbf{m}$. An integral element ε over A is called a *unit* of A if $1/\varepsilon$ is also an integral element over A. An integral element α over A is said to be *divisible* by an integral element β $(\neq 0)$ over A, if α/β is integral over A; in symbols we write $\beta|\alpha$. We say that $d \in A - \{0\}$ is a *greatest common divisor* of α and β if $d|\alpha$, $d|\beta$, and if any element e of $A - \{0\}$ which divides both α and β also divides d.

Let A be an integrally closed Noetherian domain. We call an ideal $\mathfrak{a}$ of A *divisible* by an ideal $\mathfrak{c}$ or $\mathfrak{c}$ a factor (divisor) of $\mathfrak{a}$ if $\mathfrak{c} \neq (0)$ and there is an ideal $\mathfrak{b}$ such that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. In symbols we write $\mathfrak{c}|\mathfrak{a}$. The connection between divisibility of elements and of ideals is made by the following fact: The principal ideal (α) is divisible by the

principal ideal $(\beta) \neq (0)$ if and only if the element α is divisible by the element β. This follows since

$$(\alpha) = (\beta)(\gamma_1, \ldots, \gamma_r) = (\beta\gamma_1, \ldots, \beta\gamma_r)$$

implies

$$\alpha = \sum_i \lambda_i \beta\gamma_i = \beta \sum_i \lambda_i \gamma_i$$

with algebraic integers λ_i; hence $\beta|\alpha$. Conversely, if $\beta|\alpha$, then for some algebraic integer γ, $\alpha = \beta\gamma$, and we also have $(\alpha) = (\beta)(\gamma)$ and $(\beta)|(\alpha)$.

In all statements which concern the divisibility of an principal ideal (α), we replace the ideal by the element α. Thus α is divisible by $\mathfrak{a}$ means that (α) is divisible by $\mathfrak{a}$. The statement $\beta|\alpha$ has meaning, it actually agrees with $(\beta)|(\alpha)$.

The unit ideal (1) consists of integral elements of the field of fractions. If an ideal contains the element 1, then it contains all algebraic integers, and is thus $= (1)$. For each ideal $\mathfrak{a} \neq (0)$,

$$\mathfrak{a} = \mathfrak{a}(1),\ \mathfrak{a}|\mathfrak{a},\ (1)|\mathfrak{a},\ \mathfrak{a}|(0).$$

Each ideal $\mathfrak{a}$ has the trivial factors $\mathfrak{a}$ and (1).

1.3.2 Valuation rings

An integral domain A with its field of fractions κ is called a *valuation ring* of κ if it has the property that for any $x \in \kappa$ we have $x \in A$ or $x^{-1} \in A$ (or both). Obviously, if A is a valuation ring of κ such that there exists a ring B with $A \subseteq B \subseteq \kappa$, then B is a valuation ring of κ.

Proposition 1.29. *Let A be a valuation ring of κ. Then A is a local ring, and integrally closed in κ.*

Proof. Let $\mathbf{m}$ be the set of non-units of A, so that $x \in \mathbf{m}$ if and only if $x = 0$ or $x^{-1} \notin A$. If $a \in A$ and $x \in \mathbf{m}$ we have $ax \in \mathbf{m}$, for otherwise $(ax)^{-1} \in A$ and therefore $x^{-1} = a(ax)^{-1} \in A$. Next let x, y be non-zero elements of $\mathbf{m}$. Then either $xy^{-1} \in A$ or $x^{-1}y \in A$. If $xy^{-1} \in A$, then $x + y = (1 + xy^{-1})y \in A\mathbf{m} \subseteq \mathbf{m}$, and similarly if $x^{-1}y \in A$. Hence $\mathbf{m}$ is an ideal and therefore A is a local ring by Proposition 1.11.

Let $\alpha \in \kappa$ be integral over A. Then we have, say,

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

with the $a_i \in A$. If $\alpha \in A$ there is nothing to prove. If not, then $\alpha^{-1} \in A$, hence

$$\alpha = -(a_1 + a_2\alpha^{-1} + \cdots + a_n\alpha^{1-n}) \in A.$$

This is a contradiction. Hence we always have $\alpha \in A$, that is, A is integrally closed.□

Generally, if A is a subring of a field κ, then the integral closure $\bar{A}$ of A in κ is the intersection of all the valuation rings of κ which contain A.

Definition 1.30. A valuation on a field κ is a function v from κ into $\mathbb{R} \cup \{+\infty\}$ satisfying:

(1) $v(x) = +\infty$ if and only if $x = 0$.

(2) $v(xy) = v(x) + v(y)$ for all $x, y \in \kappa$.

(3) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in \kappa$.

Set $\kappa_* = \kappa - \{0\}$. A valuation v is said to be *trivial* if

$$v(x) = \begin{cases} 0, & x \in \kappa_*, \\ +\infty, & x = 0. \end{cases}$$

Two valuations v and v' are *equivalent* if and only if there is a positive real constant λ such that $v'(x) = \lambda v(x)$ for all $x \in \kappa$. The equivalence class of a non-trivial valuation v on κ, denoted usually by $[v]$ or simply by its representatives, say v, will be called a *prime* (*divisor*) or *place* of κ. Let M_κ^0 denote the set of places of κ.

Example 1.31. Let $p \in \mathbb{Z}^+$ be a prime number. For $x = a/b \in \mathbb{Q}_*$ with $a, b \in \mathbb{Z}$, there exist integers $\mathrm{ord}_p(x), a', b'$ such that

$$x = p^{\mathrm{ord}_p(x)} \frac{a'}{b'}, \quad p \nmid a'b'.$$

Further, set $\mathrm{ord}_p(0) = +\infty$. The function $\mathrm{ord}_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{+\infty\}$ is a valuation on $\mathbb{Q}$, called the *p-adic valuation* on $\mathbb{Q}$.

If v is a valuation on a field κ, the subset

$$\mathcal{O}_{\kappa,v} = \{x \in \kappa \mid v(x) \geq 0\}$$

is a subring of κ, called the *valuation ring* of v, which has κ as field of quotients; because if $x \in \kappa$, $x \notin \mathcal{O}_{\kappa,v}$, then $v(x) < 0$ so $v(x^{-1}) > 0$ since $v(1) = 0$, and so $x = 1/y$, where $y = x^{-1} \in A$. Let us note that $\mathcal{O}_{\kappa,v} = \kappa$ exactly when v is the trivial valuation. It is easy to show that two valuations v', v of κ have the same valuation ring $\mathcal{O}_{\kappa,v'} = \mathcal{O}_{\kappa,v}$ if and only if v', v are equivalent. In view of this fact, the study of the rings of valuations is equivalent to that of the equivalence classes of valuations.

Now, we may formulate the *main theorem* on valuation rings:

Theorem 1.32. *Let A be a domain, κ its field of quotients, and U the group of units of A. Then the following statements are equivalent:*

(i) *$A = \mathcal{O}_{\kappa,v}$ for a nontrivial valuation v of κ.*

(ii) *A is a maximal proper subring of κ.*

(iii) *The following properties are satisfied:*

(iii.1) *If $x \in \kappa$, $x \notin A$, then $x^{-1} \in A$.*

(iii.2) *If $x \in A$, $x^{-1} \notin A$, if $y \in \kappa_*$, there exists an integer $n > 0$ such that $x^n \in Ay$.*

(iv) *κ_*/U is a totally ordered Archimedean group.*

Proof. (i)⇒(ii) Since A is the valuation ring of a nontrivial valuation v of κ, we have $A \neq \kappa$. Let B be a subring of κ such that $A \subseteq B \subseteq \kappa$, $A \neq B$. We will prove that $B = \kappa$. Take $x \in B$ with $x \notin A$. Then $v(x) < 0$, and so $v(x^{-1}) > 0$. If $y \in \kappa_*$, there exists an integer $n > 0$ such that

$$nv(x^{-1}) \geq v(y^{-1}),$$

and hence $v(y) \geq v(x^n)$, which means

$$y \in Ax^n \subseteq AB \subseteq B.$$

(ii)⇒(iii) First of all, we show (iii.1). Let $x \in \kappa$, $x \notin A$, and let us assume that $x^{-1} \notin A$. It follows that $A[x^{-1}] = \kappa$ from the maximality of the subring A. Hence we may write

$$x = a_0 + a_1 x^{-1} + \cdots + a_n x^{-n}$$

with $a_i \in A$, and therefore

$$x^{n+1} = a_0 x^n + a_1 x^{n-1} + \cdots + a_n.$$

Similarly, for every $j \geq 1$ we may express x^{n+j} as a linear combination of the elements $1, x, \ldots, x^n$ with coefficients in A. Thus $\kappa = A[x]$ is a finitely generated A-module. Since κ is the field of quotients of A and $\kappa \neq A$, this is not possible, because κ is not a fractional ideal.

To prove (iii.2), let $x \in A$, $x^{-1} \notin A$, then $\kappa = A[x^{-1}]$ by the maximality of A. If $y \in \kappa_*$, then y^{-1} may be written as

$$y^{-1} = a_0 + a_1 x^{-1} + \cdots + a_n x^{-n}$$

with $a_i \in A$, thus $y^{-1} = ax^{-n}$ with

$$a = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in A$$

and so $x^n = ay \in Ay$.

(iii)⇒(iv) First of all, we define a relation on κ_*/U as follows: $xU \leq yU$ when $Ax \supseteq Ay$. This is an order relation on κ_*/U compatible with multiplication: if $xU \leq yU$, for every $z \in A$, we have $xU \cdot zU \leq yU \cdot zU$.

If $x, y \in \kappa_*$ and $xU \not\leq yU$, then $Ax \not\supseteq Ay$, so $yx^{-1} \notin A$. By (iii.1), $xy^{-1} \in A$ so $yU \leq xU$. This shows that κ_*/U is a totally ordered multiplication group.

If $U \leq xU$, $U \neq xU$, that is, $x \in A$, $x \notin U$, so $x^{-1} \notin A$. If $yU \in \kappa_*/U$, by (iii.2) there exists an integer $n > 0$ such that $x^n \in Ay$, and therefore $yU \leq x^n U = (xU)^n$. This proves that κ_*/U satisfies the Archimedean property.

(iv)⇒(i) By Lemma 1.10, κ_*/U is order-isomorphic to a subgroup Γ of the ordered additive group $\mathbb{R}$. We define a mapping $v : \kappa \longrightarrow \Gamma \cup \{+\infty\}$ as follows: $v(0) = +\infty$; if $x \in \kappa_*$, let $\xi \in \Gamma$ correspond to $xU \in \kappa_*/U$, then we put $v(x) = \xi$.

We now verify that v is a valuation of κ. If $\xi, \eta \in \Gamma$ correspond respectively to xU, yU, then $\xi + \eta$ corresponds to $xyU = xU \cdot yU$; thus

$$v(xy) = v(x) + v(y).$$

Similarly, if $\xi = v(x) \leq v(y) = \eta$, then $xU \leq yU$, that is, $Ax \supseteq Ay$, hence $Ax \supseteq A(x + y)$, therefore

$$v(x + y) \geq v(x) = \min\{v(x), v(y)\}.$$

To conclude the proof, we just note that $x \in A$ if and only if $U \leq xU$, that is $0 \leq v(x)$, so A is the valuation ring of v. □

If v is a non-trivial valuation on a field κ, then $\mathcal{O}_{\kappa,v}$ is maximal among subrings of κ different from κ (or see [33], Corollary 7.3 in Chapter 1). Elements of $\mathcal{O}_{\kappa,v}$ are the *valuation integers* or *v-integers*. Obviously, $\mathcal{O}_{\kappa,v}$ is a valuation ring of the field κ. By Proposition 1.29, $\mathcal{O}_{\kappa,v}$ is a local ring, and its maximal ideal $\mathbf{m}$ is the set

$$\mathbf{m} = \mathbf{m}_{\kappa,v} = \{x \in \kappa \mid v(x) > 0\},$$

which is called the *valuation ideal* of v. The field

$$\mathbb{F}_v(\kappa) = \mathcal{O}_{\kappa,v}/\mathbf{m}$$

is called the *residue class field* of v. The characteristic of $\mathbb{F}_v(\kappa)$ is named the *residue characteristic* of κ. Further, if $\mathfrak{p} = [v]$ is the place of κ determined by the valuation v, then

$$\mathcal{O}_{\kappa,\mathfrak{p}} = \mathcal{O}_{\kappa,v},\ \mathbb{F}_{\mathfrak{p}}(\kappa) = \mathbb{F}_v(\kappa)$$

are independent of the choice of the representative v in $\mathfrak{p}$.

Example 1.33. If we consider the p-adic valuation $v = \mathrm{ord}_p$ of $\mathbb{Q}$, the residue class field $\mathbb{F}_v(\mathbb{Q})$ is the field $\mathbb{F}_p$ with p elements.

In fact, we have

$$\mathbb{Z} \subseteq \mathcal{O}_{\mathbb{Q},v}, \quad \mathbf{m}_{\mathbb{Q},v} \cap \mathbb{Z} = \mathbb{Z}p.$$

Let $\varphi : \mathcal{O}_{\mathbb{Q},v} \longrightarrow \mathbb{F}_v(\mathbb{Q})$ be the canonical mapping, and let φ_0 be its restriction to $\mathbb{Z}$. Then the kernel of φ_0 is $\mathbf{m}_{\mathbb{Q},v} \cap \mathbb{Z} = \mathbb{Z}p$, and so

$$\varphi_0(\mathbb{Z}) = \mathbb{Z}/\mathbb{Z}p = \mathbb{F}_p.$$

It is enough to show that $\varphi_0(\mathbb{Z}) = \varphi(\mathcal{O}_{\mathbb{Q},v})$, that is, given $a/b \in \mathcal{O}_{\mathbb{Q},v}$, there exists $n \in \mathbb{Z}$ such that $a/b - n \in \mathbf{m}_{\mathbb{Q},v}$. Now, since p does not divide b, there exist integers r, s such that $rp + sb = 1$. Take $n = as$. Then

$$\frac{a}{b} - n = \frac{a}{b}\left(1 - \frac{nb}{a}\right) = \frac{arp}{b} \in \mathbf{m}_{\mathbb{Q},v}.$$

1.3.3 Discrete valuation rings

Let v be a valuation on a field κ. The image of κ_* by v is a subgroup of the additive group $\mathbb{R}$ called the *valuation group of* v. The valuation of κ is said to be *discrete* (resp., *dense*) if its valuation group is a discrete (resp., dense) subgroup of $\mathbb{R}$. For the trivial valuation, the valuation group consists of 0 alone. If v is a non-trivial valuation, its valuation group Γ either has a least positive element λ or Γ has no least positive element. For the former, $\Gamma = \lambda\mathbb{Z}$. For the latter, Γ is clearly dense in $\mathbb{R}$. For a discrete valuation we can always find an equivalent one with precise valuation group $\mathbb{Z}$; such a valuation is said to be *normalized* or an *order function* on κ.

An integral domain A is a *discrete valuation ring* if there is an order function of its field of fractions κ such that A is the valuation ring $\mathcal{O}_{\kappa,\mathrm{ord}}$. If two elements $x, y \in A$ have the same value, that is, $\mathrm{ord}(x) = \mathrm{ord}(y)$, then $\mathrm{ord}(xy^{-1}) = 0$ and therefore $u = xy^{-1}$ is a unit in A. Hence $(x) = (y)$. If $\mathfrak{a} \neq 0$ is an ideal in A, there is a least integer n such that $\mathrm{ord}(x) = n$ for some $x \in \mathfrak{a}$. It follows that $\mathfrak{a}$ contains every $y \in A$ with $\mathrm{ord}(y) \geq n$, and therefore the only ideals $\neq 0$ in A are the ideals

$$\mathbf{m}_n = \{y \in A \mid \mathrm{ord}(y) \geq n\}.$$

These form a single chain

$$\mathbf{m} = \mathbf{m}_1 \supset \mathbf{m}_2 \supset \mathbf{m}_3 \supset \cdots,$$

and therefore A is Noetherian. Moreover, since $\mathrm{ord} : \kappa_* \longrightarrow \mathbb{Z}$ is surjective, there exists $t \in \mathbf{m}$ such that $\mathrm{ord}(t) = 1$, and then

$$\mathbf{m}_n = (t^n), \;\; n \geq 1.$$

Hence $\mathbf{m}$ is the only non-zero prime ideal of A, and A is thus a Noetherian local domain of dimension one in which every non-zero ideal is a power of the maximal ideal. In fact many of these properties are characteristic of discrete valuation rings.

Proposition 1.34. *Let A be a Noetherian local domain of dimension one, $\mathbf{m}$ its maximal ideal, $\mathbb{F} = A/\mathbf{m}$ its residue field. Then the following conditions are equivalent:*

(I) *A is a discrete valuation ring;*

(II) *A is integrally closed;*

(III) *$\mathbf{m}$ is a principal ideal;*

(IV) $\dim_{\mathbb{F}} \mathbf{m}/\mathbf{m}^2 = 1$*;*

(V) *Every non-zero ideal is a power of* $\mathbf{m}$*;*

(VI) *There exists* $t \in A$ *such that every non-zero ideal is of the form* (t^n)*,* n *a non-negative integer.*

Proof. See M. F. Atiyah and I. G. Macdonald [2], Proposition 9.2. □

An element t as in Proposition 1.34 is called a *uniformizing parameter* for A; any other uniformizing parameter is of the form ut, u a unit in A. Let κ be the quotient field of A. Then any non-zero element $z \in \kappa$ has a uniquely expression $z = ut^n$, u a unit in A, $n \in \mathbb{Z}$. The exponent $n = \mathrm{ord}(z)$ is called the *order* of z.

Proposition 1.35. *Let* A *be a Noetherian domain of dimension one. Then the following are equivalent:*

(α**)** A *is integrally closed;*

(β**)** *Every primary ideal in* A *is a prime power;*

(γ**)** *Every local ring* $A_{\mathfrak{p}}$ $(\mathfrak{p} \neq 0)$ *is a discrete valuation ring.*

Proof. $(\alpha) \Leftrightarrow (\gamma)$. Since A is integrally closed if and only if $A_{\mathfrak{p}}$ is integrally closed, for each prime ideal $\mathfrak{p}$, then it follows from Proposition 1.34.

$(\beta) \Leftrightarrow (\gamma)$. See M. F. Atiyah and I. G. Macdonald [2], Theorem 9.3. □

A Noetherian domain of dimension one satisfying the conditions of Proposition 1.35 is called a *Dedekind domain*. The first result is that in such a domain we have a *unique factorization theorem* for ideals:

Theorem 1.36. *Let* A *be an integral domain. Then* A *is a Dedekind domain if and only if every non-zero ideal of* A *has a unique factorization as a product of prime ideals.*

Proof. Theorem 1.25 and Proposition 1.35, or see [215], Section 10.2, Theorem 2. □

Proposition 1.37. *Let* A *be a local domain. Then* A *is a discrete valuation ring if and only if every non-zero fractional ideal of* A *is invertible.*

Proof. Assume that A is a discrete valuation ring. Let t be a generator of the maximal ideal $\mathbf{m}$ of A, and let $\mathfrak{g} \neq 0$ be a fractional ideal. Then there exists $\omega \in A$ such that $\omega\mathfrak{g} \subseteq A$: thus $\omega\mathfrak{g}$ is an integral ideal, say (t^n), and therefore $\mathfrak{g} = (t^{n-l})$, where $l = v(\omega)$.

Conversely, every non-zero fractional ideal of A is invertible and therefore finitely generated, so that A is Noetherian. By Proposition 1.34, it is therefore enough to prove that every non-zero ideal is a power of $\mathbf{m}$. Suppose this is false. Let Σ be the set of

non-zero ideals which are not powers of $\mathbf{m}$, and let $\mathfrak{m}$ be a maximal element of Σ. Then $\mathfrak{m} \neq \mathbf{m}$, hence $\mathfrak{m} \subset \mathbf{m}$, and so

$$\mathbf{m}^{-1}\mathfrak{m} \subset \mathbf{m}^{-1}\mathbf{m} = A$$

is a proper integral ideal, and $\mathbf{m}^{-1}\mathfrak{m} \supseteq \mathfrak{m}$. If $\mathbf{m}^{-1}\mathfrak{m} = \mathfrak{m}$, then $\mathfrak{m} = \mathbf{m}\mathfrak{m}$ and therefore $\mathfrak{m} = 0$ by a Nakayama's lemma, hence $\mathbf{m}^{-1}\mathfrak{m} \supset \mathfrak{m}$, and hence $\mathbf{m}^{-1}\mathfrak{m}$ is a power of $\mathbf{m}$ (by the maximality of $\mathfrak{m}$). Hence $\mathfrak{m}$ is a power of $\mathbf{m}$: contradiction. □

Proposition 1.38. *Let A be an integral domain. Then A is a Dedekind domain if and only if every non-zero fractional ideal of A is invertible.*

Proof. Let A be a Dedekind domain and let $\mathfrak{g} \neq (0)$ be a fractional ideal. Since A is Noetherian, $\mathfrak{g}$ is finitely generated. For each prime ideal $\mathfrak{p}$, $\mathfrak{g}_\mathfrak{p}$ is a fractional ideal $\neq 0$ of the discrete valuation ring $A_\mathfrak{p}$, hence is invertible by Proposition 1.37. Hence $\mathfrak{g}$ is invertible by the local property of invertibility.

Conversely, every non-zero integral ideal of A is invertible, hence finitely generated, and so A is Noetherian. We shall show that each $A_\mathfrak{p}$ ($\mathfrak{p} \neq 0$) is a discrete valuation ring. For this it is enough to show that each integral ideal $\neq 0$ in $A_\mathfrak{p}$ is invertible, and then use Proposition 1.37. Let $\mathfrak{a} \neq 0$ be an integral ideal in $A_\mathfrak{p}$, and let $\mathfrak{b} = \mathfrak{a} \cap A$. Then $\mathfrak{b}$ is invertible, hence $\mathfrak{a} = \mathfrak{b}_\mathfrak{p}$ is invertible by Proposition 1.37. □

Theorem 1.39. *Any non-zero fractional ideal $\mathfrak{g}$ of a Dedekind domain A can be uniquely expressed as a product*

$$\mathfrak{g} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_r^{a_r}$$

with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ distinct prime ideals and $a_1, \ldots, a_r$ positive or negative integers.

Proof. Since $\omega\mathfrak{g} \subseteq A$ for some $\omega \in A - \{0\}$, each of the ideals $\omega\mathfrak{g}$ and ωA in A has a factorization as a product of prime ideals with nonnegative exponents as

$$\omega\mathfrak{g} = \prod \mathfrak{p}_i^{b_i}, \quad \omega A = \prod \mathfrak{q}_j^{c_j},$$

with $\mathfrak{p}_i$ and $\mathfrak{q}_j$ maximal ideals of A in which the exponents b_i and c_j positive integers (cf. Theorem 1.36). It follows that

$$\prod \mathfrak{p}_i^{b_i} = \omega\mathfrak{g} = (\omega A)\mathfrak{g} = \left(\prod \mathfrak{q}_j^{c_j}\right)\mathfrak{g}.$$

We have just proved that ideals of A are invertible, so it follows that

$$\mathfrak{g} = \prod \mathfrak{p}_i^{b_i} \prod \mathfrak{q}_j^{-c_j}$$

which is a factorization of $\mathfrak{g}$.

To establish the uniqueness of the factorization, suppose

$$\mathfrak{g} = \prod \mathfrak{p}_i^{b_i} \prod \mathfrak{q}_j^{-c_j} = \prod \mathfrak{r}_k^{d_k} \prod \mathfrak{s}_l^{-e_l},$$

where all $\mathfrak{p}_i$, $\mathfrak{q}_j$, $\mathfrak{r}_k$, and $\mathfrak{s}_l$ are maximal ideals of A and the numbers b_i, c_j, d_k, e_l are positive integers. We may assume further that all the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are distinct as are all the $\mathfrak{r}_k$ and $\mathfrak{s}_l$. Since ideals of A are invertible, we may clear the negative exponents by multiplication to get

$$\prod \mathfrak{p}_i^{b_i} \prod \mathfrak{s}_l^{e_l} = \prod \mathfrak{q}_j^{c_j} \prod \mathfrak{r}_k^{d_k}.$$

Each side is an ideal of A and we already know the uniqueness of the expression of an ideal of A as a product of maximal ideals by Theorem 1.36. It follows, after suitable renumbering, that

$$\mathfrak{p}_i^{b_i} = \mathfrak{r}_k^{d_k}, \quad \mathfrak{q}_j^{c_j} = \mathfrak{s}_l^{e_l},$$

which yields the uniqueness of the factorization for $\mathfrak{g}$. □

Thus if A is a Dedekind domain, the non-zero fractional ideals of A form a group with respect to multiplication. This group is called the *group of ideals* of A; we denote it by $\mathfrak{I}_A$. In this terminology Theorem 1.39 says that $\mathfrak{I}_A$ is a free Abelian group, generated by the non-zero prime ideals of A.

Let A be a Dedekind domain, κ its field of fractions. We consider the homomorphism

$$\vartheta : \kappa_* \longrightarrow \mathfrak{I}_A, \ \ \vartheta(\alpha) = (\alpha).$$

The image $\vartheta(\kappa_*)$ of ϑ is the group of *principal* fractional ideals. The quotient

$$I_A = \mathfrak{I}_A / \vartheta(\kappa_*)$$

can be made into an Abelian group, called *ideal class group* of A (or κ). For each element $\mathfrak{a} \in \mathfrak{I}_A$, the equivalence class $[\mathfrak{a}]$ of all ideals equivalent to $\mathfrak{a}$ is called an *ideal class*. Here two elements $\mathfrak{a}, \mathfrak{b}$ of $\mathfrak{I}_A$ are said to be *equivalent*, in symbols $\mathfrak{a} \sim \mathfrak{b}$, if they differ only by a factor which is a principal ideal, that is, if there is a (integral or fractional) principal ideal $(\omega) \neq (0)$ such that $\mathfrak{a} = \omega\mathfrak{b}$. In particular, all principal ideals $(\neq 0)$ are equivalent to each other. They form the *principal class*, which is the unit element in I_A. The kernel $\mathrm{Ker}(\vartheta)$ of ϑ is the set of all $\alpha \in \kappa_*$ such that $(\alpha) = (1)$, so that it is the *group of units* of A. We have an exact sequence

$$1 \to \mathrm{Ker}(\vartheta) \to \kappa_* \xrightarrow{\vartheta} \mathfrak{I}_A \to I_A \to 1. \tag{1.10}$$

A family of valuations S on a field κ is said to satisfy the *strong approximation property* if the following conditions hold:

⟨1⟩ each valuation in S is discrete;

⟨2⟩ for any $x \in \kappa_*$, $v(x) = 0$ except at most for finitely many valuations $v \in S$;

$\langle 3\rangle$ given $v, v' \in S$ and $N > 0$, there exists $x \in \kappa$ such that $v(x-1) > N$, $v'(x) > N$ and $w(x) \geq 0$ for all $w \neq v, v'$ in S.

Theorem 1.40. *If A is a Dedekind domain with field of fractions κ, then A can be defined as the intersection of valuation rings for a family S of non-trivial inequivalent valuations on κ with the strong approximation property.*

Proof. If the different maximal ideals of A are $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$, then we have

$$\prod_i \mathfrak{p}_i^{\alpha_i} \subseteq A$$

for any $\alpha_i \geq 0$, with equality if and only if $\alpha_i = 0$ for all i. Thus the $\mathfrak{p}_i$ generate a free Abelian group $\mathfrak{I}_0$ say. If some integral ideal is not in $\mathfrak{I}_0$, then because A is Noetherian we can find an ideal $\mathfrak{a}$ which is maximal among ideals not in $\mathfrak{I}_0$. We have $\mathfrak{a} \subseteq \mathfrak{p}_i \subset A$ for some maximal ideal $\mathfrak{p}_i$, hence $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}_i^{-1} \subseteq A$. By the maximality of $\mathfrak{a}$ it follows that $\mathfrak{a}\mathfrak{p}_i^{-1} \in \mathfrak{I}_0$ and so $\mathfrak{a} = \mathfrak{a}\mathfrak{p}_i^{-1}\mathfrak{p}_i \in \mathfrak{I}_0$, which is a contradiction. Thus $\mathfrak{I}_0$ contains every integral ideal and hence every principal ideal, for if $u = ab^{-1}$, then $aA, bA \in \mathfrak{I}_0$, hence also $uA = (aA)(bA)^{-1}$. If $\mathfrak{g}$ is any fractional ideal, then there exists $\omega \in A - \{0\}$ such that $\omega\mathfrak{g} \subseteq A$, and hence $\mathfrak{f} = \omega\mathfrak{g} \in \mathfrak{I}_0$; therefore $\mathfrak{g} = \mathfrak{f}\omega^{-1} \in \mathfrak{I}_0$ and this shows that $\mathfrak{I}_0$ includes all fractional ideals.

Given $a \in \kappa_*$, the principal ideal aA is a fractional ideal and so we have a representation

$$aA = \prod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(a)}. \tag{1.11}$$

For each maximal ideal $\mathfrak{p}$, the function $\mathrm{ord}_\mathfrak{p}(a)$ is a discrete valuation on κ, where we think $\mathrm{ord}_\mathfrak{p}(0) = +\infty$. Let S be the set of equivalence classes defined by these valuations. We have just see that $\langle 1\rangle$ holds and $\langle 2\rangle$ follows because in (1.11) almost all the $\mathrm{ord}_\mathfrak{p}(a)$ vanish. To prove $\langle 3\rangle$, take distinct maximal ideals $\mathfrak{p}$, $\mathfrak{q}$. Then $\mathfrak{p} + \mathfrak{q} = A$, hence $(\mathfrak{p} + \mathfrak{q})^{2N} = A$ for any $N > 0$, and so

$$A = (\mathfrak{p} + \mathfrak{q})^{2N} \subseteq \mathfrak{p}^{2N} + \mathfrak{p}^{2N-1}\mathfrak{q} + \cdots + \mathfrak{q}^{2N} \subseteq \mathfrak{p}^N + \mathfrak{q}^N.$$

It follows that we can write $1 = a + b$, where $a \in \mathfrak{p}^N$, $b \in \mathfrak{q}^N$ and $a, b \in A$. Thus a satisfies

$$\mathrm{ord}_\mathfrak{p}(a) \geq N, \ \ \mathrm{ord}_\mathfrak{q}(1-a) \geq N, \ \ a \in A,$$

and so $\langle 3\rangle$ holds. □

For every nonzero prime ideal $\mathfrak{p}$ of A, the mapping $\mathrm{ord}_\mathfrak{p}$ defined in (1.11) is called the $\mathfrak{p}$-*adic valuation*. In fact, Theorem 1.40 exhibits a characterization of Dedekind domains by means of valuations:

Proposition 1.41. *Let A be an integral domain. Then A is a Dedekind domain if and only if A satisfies the conditions:*

(a) *there exists a family S of discrete normalized valuations of the field of quotients κ of A such that*

$$A = \bigcap_{v \in S} \mathcal{O}_{\kappa,v};$$

(b) *for every $x \in \kappa_*$, the set $\{v \in S \mid v(x) \neq 0\}$ is finite;*

(c) *every nonzero prime ideal of A is maximal.*

Proof. See [215], Section 10.2, Theorem 2. □

By using Proposition 1.41, one can prove that if A is a Dedekind domain with the field κ of quotients of A, the following sets of rings coincide:

$$\Omega = \{\mathcal{O}_{\kappa,v} \mid \ v \text{ is discrete such that } A \subseteq \mathcal{O}_{\kappa,v}\},$$

$$\Omega' = \{A_{\mathfrak{p}} \mid \mathfrak{p} \neq 0, \ \mathfrak{p} \text{ prime ideal}\},$$

and

$$\Omega'' = \{\mathcal{O}_{\kappa,v} \mid \ v \text{ is a nontrivial valuation of } \kappa \text{ such that } A \subseteq \mathcal{O}_{\kappa,v}\},$$

see [215], Section 10.1, (B).

Proposition 1.42. *Let A be an integrally closed Noetherian domain. Then*

$$A = \bigcap_{\text{ht } \mathfrak{p}=1} A_{\mathfrak{p}},$$

where the intersection is taken over all prime ideals of height 1.

Proof. See Matsumura [173], Theorem 38, p. 124. □

1.4 Polynomials

For further investigation we need the *symmetric polynomial theorem* from algebra, which we formulate as follows:

Theorem 1.43. *Let $x_1, \ldots, x_n$ be n independent variables and let $\sigma_1, \ldots, \sigma_n$ be their n elementary symmetric polynomials which are the coefficients of the polynomial in x:*

$$(x - x_1) \cdots (x - x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \cdots + (-1)^n \sigma_n.$$

Then every symmetric polynomial $S(x_1, \ldots, x_n)$ in $x_1, \ldots, x_n$ can be represented uniquely as a polynomial G of $\sigma_1, \ldots, \sigma_n$:

$$S(x_1, \ldots, x_n) = G(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)).$$

The coefficients of G can be calculated from those of S entirely by the operations of addition, subtraction, and multiplication.

If the theorem is applied twice in succession, then we obtain: If $y_1, \ldots, y_m$ are m additional independent variables and $\rho_1, \ldots, \rho_m$ are their elementary symmetric polynomials, and if $S(x_1, \ldots, x_n; y_1, \ldots, y_m)$ is a polynomial of the $n+m$ arguments which remains unchanged under each permutation of the x among themselves and under each permutation of the y among themselves, then S can be represented as a polynomial G of the $\sigma_1, \ldots, \sigma_n$ and $\rho_1, \ldots, \rho_m$:

$$S(x_1, \ldots, x_n; y_1, \ldots, y_m) = G(\sigma_1, \ldots, \sigma_n, \rho_1, \ldots, \rho_m).$$

The coefficients of G can be calculated from those of S entirely by the operations of addition, subtraction, and multiplication.

The most important fact concerning polynomials over a field κ is stated in the following theorem:

Theorem 1.44. *Two nonzero polynomials $f_1(x)$ and $f_2(x)$ over κ have a uniquely determined greatest common divisor $d(x)$, that is, there is a polynomial $d(x)$ with leading coefficient 1, such that $d(x)|f_1(x)$, $d(x)|f_2(x)$, and every polynomial which divides $f_1(x)$ and $f_2(x)$, also divides $d(x)$. Moreover, $d(x)$ can be represented in the form*

$$d(x) = g_1(x)f_1(x) + g_2(x)f_2(x), \tag{1.12}$$

where $g_1(x)$ and $g_2(x)$ are polynomials over κ, and thus $d(x)$ is also a polynomial over κ.

Proof. Among the polynomials

$$P(x) = u_1(x)f_1(x) + u_2(x)f_2(x),$$

where $u_1(x)$ and $u_2(x)$ run through all polynomials over κ, we consider such a polynomial with leading coefficient 1 whose degree is as small as possible. Let $d(x)$ be such a polynomial and suppose that (1.12) holds. If $d(x)$ is of degree 0, then it is $= 1$ and hence it divides $f_1(x)$ and $f_2(x)$. But even if it is of higher degree, it must divide $f_1(x)$, for let the remainder $r(x)$ of $f_1(x) \bmod d(x)$ be determined

$$f_1 = qd + r,$$

that is,

$$r = f_1 - qd = f_1 - q(g_1f_1 + g_2f_2) = (1 - qg_1)f_1 - qg_2f_2.$$

Thus this $r(x)$ also has the form $P(x)$, while its degree (as a remainder $\bmod d(x)$) is less than the degree of $d(x)$. Consequently it cannot have coefficients different from 0, hence it is 0. Thus $d(x)|f_1(x)$; similarly we also have $d(x)|f_2(x)$.

However, by (1.12) each common divisor of $f_1(x)$ and $f_2(x)$ divides $d(x)$. If a polynomial $d_0(x)$ has the property stated in the first part of the theorem, then $d(x)|d_0(x)$ holds as well as $d_0(x)|d(x)$, consequently $d(x)$ and $d_0(x)$ differ by only a constant factor; since their leading coefficients are 1, $d_0(x) = d(x)$. □

We write $(f_1(x), f_2(x)) = d(x)$ and call $f_1(x)$ and $f_2(x)$ relatively prime if $d = 1$. We have immediately from Theorem 1.44:

Theorem 1.45. *If a polynomial $f(x)$, irreducible over κ, has a common zero $x = \alpha$ with a polynomial $g(x)$ over κ, then $f(x)$ is a divisor of $g(x)$ and hence all zeros of $f(x)$ are zeros of $g(x)$.*

Theorem 1.46. *Let p be a prime. If for two rational integral polynomials $f(x)$ and $g(x)$*

$$f(x)g(x) \equiv 0 \pmod{p},$$

then either $f(x) \equiv 0 \pmod{p}$ or $g(x) \equiv 0 \pmod{p}$ or both.

Proof. Suppose the theorem is false, i.e., neither $f(x)$ nor $g(x)$ is $\equiv 0 \pmod{p}$. Then let all terms of $f(x)$ and $g(x)$ which are divisible by p be omitted and two nonvanishing polynomials $\bar{f}(x)$, $\bar{g}(x)$ are obtained, all of whose coefficients are not divisible by p, while at the same time

$$f(x) \equiv \bar{f}(x) \pmod{p},$$

$$g(x) \equiv \bar{g}(x) \pmod{p},$$

it follows that

$$\bar{f}(x)\bar{g}(x) \equiv 0 \pmod{p}.$$

The highest-degree term in $\bar{f}(x)\bar{g}(x)$ must be $\equiv 0 \pmod{p}$ on the one hand, on the other hand however it is equal to the product of the highest terms of $\bar{f}(x)$ and $\bar{g}(x)$. Since p is a prime and all terms of $\bar{f}(x)$ and $\bar{g}(x)$ are not divisible by p, such product of such terms is also not divisible by p. Consequently the hypothesis is false, and the theorem is proved. □

A rational integral polynomial is called *primitive* if its coefficients are relatively prime. Then Theorem 1.46 obviously allows the following formulation:

Theorem 1.47 (Theorem of Gauss). *The product of two primitive polynomials is again a primitive polynomial.*

We will need *Hilbert's Nullstellensatz*:

Theorem 1.48. *Take polynomials $P_1, \ldots, P_r$ and P in $K[X_0, \ldots, X_m]$, where K is an algebraically closed field. If P vanishes at all the common zeros of $P_1, \ldots, P_r$, then there exist polynomials $Q_1, \ldots, Q_r$ in $K[X_0, \ldots, X_m]$ such that*

$$P^s = Q_1P_1 + \cdots + Q_rP_r$$

holds for some natural number s.

Proof. Van der Waerden [282] or Lang [152] or Atiyah–Macdonald [2], p. 85 or Zariski–Samuel [307], vol. 2, p. 164. □

Let v be a valuation of a field κ. The first result concerns the extension of the valuation v of κ to a valuation w of $\kappa(x)$. Given a polynomial

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \kappa[x],$$

we usually write

$$\deg(f) = n$$

when $a_n \neq 0$, and define

$$w(f) = \min_{0 \leq i \leq n} v(a_i). \tag{1.13}$$

It is clear that this reduces to v on κ, and moreover satisfies

$$w(f+g) \geq \min\{w(f), w(g)\};$$

further, the argument used to prove Gauss' lemma shows that

$$w(fg) = w(f) + w(g),$$

cf. Lemma 4.17. Hence we obtain a valuation w on $\kappa[x]$; it extends in a unique way to a valuation on $\kappa(x)$, still denoted w, by the rule

$$w\left(\frac{f}{g}\right) = w(f) - w(g), \quad f, g \in \kappa[x]. \tag{1.14}$$

The valuation thus defined is called the *Gaussian extension* or *canonical extension* of v to $\kappa(x)$; its value group is the same as that of v. A polynomial $f \in \kappa[x]$ is said to be *primitive* (with respect to v) if $w(f) = 0$. Obviously, a product of two primitive polynomials is again primitive. This is the analogue of Theorem 1.47.

Consider the canonical homomorphism

$$a \in \mathcal{O}_{\kappa,v} \longmapsto \bar{a} \in \mathbb{F}_v(\kappa) = \mathcal{O}_{\kappa,v}/\mathbf{m}.$$

For a polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathcal{O}_{\kappa,v}[x],$$

we will write

$$\bar{f}(x) = \bar{a}_n x^n + \bar{a}_{n-1} x^{n-1} + \cdots + \bar{a}_0 \in \mathbb{F}_v(\kappa)[x],$$

which is said to be obtained from f by *reduction modulo* $\mathbf{m}$. Any $g \in \mathcal{O}_{\kappa,v}[x]$ such that $\bar{g} = \bar{f}$ is called a *lifting* of $\bar{f}$.

The field κ is called *Henselian* for v when it satisfies the property: if $f \in \mathcal{O}_{\kappa,v}[x]$ is a primitive polynomial, if $\gamma, \eta \in \mathbb{F}_v(\kappa)[x]$ are relatively prime polynomials such that γ is nonconstant and $\bar{f} = \gamma\eta$, then there exist polynomials $g, h \in \mathcal{O}_{\kappa,v}[x]$ such that

$$\bar{g} = \gamma, \ \bar{h} = \eta, \ \deg(g) = \deg(\gamma), \ f = gh.$$

Proposition 1.49. *A field κ is Henselian for a valuation v if and only if the following property holds: if $f \in \mathcal{O}_{\kappa,v}[x]$ is a primitive irreducible polynomial, then either $\bar{f}$ is a constant or*

$$\deg(\bar{f}) = \deg(f), \quad \bar{f} = \bar{a}\gamma^s,$$

where $\bar{a} \in \mathbb{F}_v(\kappa)$, $\bar{a} \neq 0$, $s \geq 1$, and $\gamma \in \mathbb{F}_v(\kappa)[x]$ is an irreducible monic polynomial.

Proof. See [215], Section 3.2. □

A basic fact on Henselian fields are the following *Hensel's lemma*:

Lemma 1.50. *If κ is a complete field with respect to a valuation v, then it is Henselian for v.*

Proof. See [215], Section 3.2. □

1.5 Algebraic extension fields

Let κ be a field. If κ is a subfield of a field K, then we also say that K is an *extension field* of κ, which will be denoted by K/κ. The field K can always be regarded as a vector space over κ. The dimension $\dim_\kappa K$ of K as an κ-vector space is called the *degree* of K over κ. It will be denoted by

$$[K : \kappa] = \dim_\kappa K.$$

If $[K : \kappa] < \infty$, K is called a *finite extension* of κ, otherwise, an *infinite extension* of κ. The following proposition is a basic fact of extension fields:

Proposition 1.51. *Let κ be a field and $F \subset K$ extension fields of κ. Then*

$$[K : \kappa] = [K : F][F : \kappa]. \tag{1.15}$$

If $\{x_i\}_{i\in I}$ is a basis for F over κ and $\{y_j\}_{j\in J}$ is a basis for K over F, then $\{x_i y_j\}_{(i,j)\in I\times J}$ is a basis for K over κ.

Let κ be a subfield of a field K. Take an element α in K. The field extension of κ, which is generated by α, will be denoted by $\kappa(\alpha)$, that is, $\kappa(\alpha)$ is the smallest field containing κ and α. We denote the ring generated by α over κ by $\kappa[\alpha]$. It consists of all elements of K that can be written as polynomials in α with coefficients in κ:

$$a_n\alpha^n + \cdots + a_1\alpha + a_0, \;\; a_i \in \kappa. \tag{1.16}$$

The field $\kappa(\alpha)$ is isomorphic to the field of fractions of $\kappa[\alpha]$. Its elements are ratios of elements of the form (1.16). The element α is said to be *algebraic over κ* if it is the root of some nonzero polynomial with coefficients in κ, otherwise, *transcendental over κ*. The lowest degree irreducible monic polynomial P_α with coefficients in κ such that $P_\alpha(\alpha) = 0$ is called the *minimal polynomial of α over κ*. The degree of the polynomial P_α is also called the *degree of α over κ*, which is determined as follows:

Proposition 1.52. *Let α be algebraic over κ. Then $\kappa(\alpha) = \kappa[\alpha]$, and $\kappa(\alpha)$ is finite over κ. The degree $[\kappa(\alpha) : \kappa]$ is equal to the degree of the minimal polynomial for α over κ.*

Proof. Take $\beta \in \kappa(\alpha)$. Then there are two polynomials Q and R satisfying

$$\beta = \frac{Q(\alpha)}{R(\alpha)}, \ \ R(\alpha) \neq 0.$$

Then $R(x)$ does not have the root α in common with the polynomial $P_\alpha(x)$ belonging to α which is irreducible over κ; and hence $R(x)$ is relatively prime to $P_\alpha(x)$, otherwise, $P_\alpha(x)|R(x)$. Thus there are two polynomials $S(x)$ and $T(x)$ over κ such that

$$P_\alpha(x)S(x) + R(x)T(x) = 1,$$

and since $P_\alpha(\alpha) = 0$,

$$R(\alpha)T(\alpha) = 1, \quad \beta = \frac{Q(\alpha)}{R(\alpha)} = Q(\alpha)T(\alpha) = f(\alpha),$$

where $f(x) = Q(x)T(x)$ is again a polynomial over κ. Finally, let $g(x)$ be the remainder of $f(x)$ mod $P_\alpha(x)$, which is also a polynomial over κ of degree $\leq n-1$, where $n = \deg(P_\alpha)$. Then

$$f(x) = q(x)P_\alpha(x) + g(x), \quad f(\alpha) = g(\alpha),$$

so that β is put into the form

$$\beta = g(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}. \tag{1.17}$$

If there are two polynomials $g(x)$ and $g_1(x)$ over κ, of degree at most $n-1$, such that $g(\alpha) = g_1(\alpha)$, then $g(x) - g_1(x)$ is a polynomial over κ with the root α, whose degree is $< n$. Thus $g(x) - g_1(x) = 0$, that is, the coefficients of $g(x)$ and $g_1(x)$ agree. Obviously, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent over κ, that is, $[\kappa(\alpha) : \kappa] = n$. □

A field extension K of κ is said to be an *algebraic closure* of κ if all elements of K are algebraic over κ, and K is *algebraically closed*, that is, every polynomial $f(x) \in K[x]$ of positive degree has a root in K.

Proposition 1.53. *Every field κ has an algebraic closure.*

Let K be an algebraic closure of a field κ. Take $\alpha \in K$. The roots of the minimal polynomial P_α of α over κ, surely distinct from one another, are called the *conjugates* of α with respect to κ.

Proposition 1.54. *If α, β are algebraic over κ, then the same is true for $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, and if $\beta \neq 0$, for α/β.*

Proof. If $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are the conjugates of α and $\beta^{(1)}, \ldots, \beta^{(m)}$ are those of β with respect to κ, then the elementary symmetric polynomials of α, as well as those of β, are elements in κ. The product

$$H(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} \left\{ x - \left(\alpha^{(i)} + \beta^{(j)} \right) \right\}$$

as a symmetric function in the α, and in the β, is then a polynomial over κ by reason of the symmetric polynomial fundamental theorem, and $\alpha+\beta$ is to be found among its roots, which accordingly is algebraic over κ. This likewise follows for $\alpha-\beta$ and $\alpha\beta$.

If $\beta \neq 0$, let us set $x = 1/y$ in the irreducible equation for β over κ

$$x^m + b_1 x^{m-1} + \cdots + b_m = 0,$$

and let us multiply by y^m

$$b_m y^m + b_{m-1} y^{m-1} + \cdots + b_1 y + 1 = 0.$$

The polynomial then has the root $1/\beta$, and this element is thus likewise algebraic over κ; consequently by what has gone before, the product α/β is also algebraic over κ. □

Proposition 1.55. *Let α be an algebraic element over κ of degree n with conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$. Then every element $\beta = g(\alpha) \in \kappa[\alpha]$ is likewise an algebraic element over κ of degree at most n. The conjugates of β are the distinct elements among the elements $\left\{ g\left(\alpha^{(i)}\right) \right\}$. Each conjugate of β appears equally often among $\left\{ g\left(\alpha^{(i)}\right) \right\}$.*

Proof. We consider the product

$$f(x) = \prod_{i=1}^{n} \left\{ x - g\left(\alpha^{(i)}\right) \right\}.$$

The coefficients of this polynomial are integral rational combinations of $\alpha^{(1)}, \ldots, \alpha^{(n)}$, which are moreover symmetric in $\alpha^{(1)}, \ldots, \alpha^{(n)}$ and whose coefficients belong to κ. Consequently, $f(x)$ is a polynomial over κ and thus every element $g\left(\alpha^{(i)}\right)$ is algebraic over κ.

Further, if $\varphi(x)$ is a polynomial, among whose roots just one of the elements $\beta^{(i)} = g\left(\alpha^{(i)}\right)$ occurs, then all $\beta^{(i)}$ are roots of $\varphi(x)$. Namely the polynomial $\varphi(g(x))$ over κ has a root $x = \alpha^{(i)}$ in common with the minimal polynomial $P_\alpha(x)$ of α over κ, and hence it vanishes for all $x = \alpha^{(1)}, \ldots, \alpha^{(n)}$ since P_α is irreducible; consequently, $\varphi(x)$ vanishes for each $x = \beta^{(1)}, \ldots, \beta^{(n)}$.

Moreover, if $P_\beta(x)$ is the irreducible polynomial over κ with leading coefficient 1 which has β as a root, then $P_\beta(x)$ is a divisor of $f(x)$. Let $P_\beta(x)^q$ be the highest power of $P_\beta(x)$ dividing $f(x)$. Now if $f(x)/P_\beta(x)^q$ were not constant, then it would have a $\beta^{(i)}$, a root of f, as a root; consequently, it would still be divisible by $P_\beta(x)$, contrary to the assumption about q. Hence for a certain integer q,

$$f(x) = P_\beta(x)^q,$$

that is, the n elements

$$\beta^{(i)} = g\big(\alpha^{(i)}\big), \;\; i = 1, 2, \ldots, n$$

represent all conjugates of β; however they represent q times for each conjugate of β. Thus β has the degree n/q. □

We now modify the concept of the conjugate, keeping in mind the above proposition, by the following: if α is an algebraic element over κ of degree n with conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$, and if $\beta = g(\alpha) \in \kappa[\alpha]$ is an algebraic element over κ of degree n/q, then the system of n elements $\beta^{(i)} = g\left(\alpha^{(i)}\right)$ $(i = 1, 2, \ldots, n)$ will be called the *conjugates of β in $\kappa(\alpha)$ with respect to κ*. These are the conjugates of β with respect to κ, each one taken q times.

Proposition 1.56. *Let α be an algebraic element over κ of degree n. An element β in $\kappa(\alpha)$ belongs to κ if and only if it is equal to its n conjugates in $\kappa(\alpha)$. An element β in $\kappa(\alpha)$ has degree n over κ if and only if it is distinct from all its conjugates. The latter condition is at the same time necessary and sufficient for the number β to generate the field $\kappa(\alpha)$.*

Proposition 1.57. *Each rational equation $R(\beta_1, \ldots, \beta_m) = 0$ between numbers $\beta_1, \ldots, \beta_m$ in $\kappa(\alpha)$ with coefficients in κ remains true if $\beta_1, \ldots, \beta_m$ are replaced by the conjugates with the same index.*

Proof. We can write R as the quotient of two polynomials P and Q

$$R(x_1, \ldots, x_m) = \frac{P(x_1, \ldots, x_m)}{Q(x_1, \ldots, x_m)}.$$

If we substitute for $\beta_1, \ldots, \beta_m$ in R their representations as polynomials in α,

$$\beta_i = g_i(\alpha) \in \kappa[\alpha], \;\; i = 1, 2, \ldots, m,$$

then $Q(\beta_1, \ldots, \beta_m)$ becomes a polynomial in α, which does not vanish for the value α. Consequently, it does not vanish for any of the conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$ of α with respect to κ. However,

$$P(\beta_1, \ldots, \beta_m) = P(g_1(\alpha), \ldots, g_m(\alpha)) = 0.$$

Hence this polynomial in α must vanish for all conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$, i.e.,

$$P\Big(\beta_1^{(i)}, \ldots, \beta_m^{(i)}\Big) = P\Big(g_1\big(\alpha^{(i)}\big), \ldots, g_m\big(\alpha^{(i)}\big)\Big) = 0, \;\; i = 1, 2, \ldots, n,$$

and hence

$$R\left(\beta_1^{(i)}, \ldots, \beta_m^{(i)}\right) = 0, \;\; i = 1, 2, \ldots, n$$

since $Q\left(\beta_1^{(i)}, \ldots, \beta_m^{(i)}\right) \neq 0$. □

In particular, it follows for each two elements β, γ in $\kappa(\alpha)$

$$\beta^{(i)} \pm \gamma^{(i)} = (\beta \pm \gamma)^{(i)}, \;\; \beta^{(i)}\gamma^{(i)} = (\beta\gamma)^{(i)}, \;\; \frac{\beta^{(i)}}{\gamma^{(i)}} = \left(\frac{\beta}{\gamma}\right)^{(i)},$$

since, for example, for $\beta = g(\alpha) \in \kappa[\alpha]$ and $\gamma = h(\alpha) \in \kappa[\alpha]$,

$$\beta\gamma = g(\alpha)h(\alpha) = r(\alpha) \in \kappa[\alpha].$$

By the above theorem, from this one equation of α, the n equations

$$g\big(\alpha^{(i)}\big)h\big(\alpha^{(i)}\big) = r\big(\alpha^{(i)}\big)$$

follows, that is,

$$\beta^{(i)}\gamma^{(i)} = (\beta\gamma)^{(i)}, \;\; i = 1, 2, \ldots, n.$$

A field extension K of κ is called an *algebraic extension*, or K is said to be *algebraic over* κ, if all its elements are algebraic over κ. One important case of a tower of field extensions is that K is a given extension of κ and α is an element of K. The field $\kappa(\alpha)$ is an intermediate field:

$$\kappa \subset \kappa(\alpha) \subset K.$$

Thus, one has

$$[K : \kappa] = [K : \kappa(\alpha)][\kappa(\alpha) : \kappa].$$

Note that $[\kappa(\alpha) : \kappa]$ is the degree of α over κ if α is algebraic, otherwise $[\kappa(\alpha) : \kappa] = \infty$. Hence one shows the property:

Proposition 1.58. *If K is a finite extension of κ, then K is algebraic over κ.*

Let κ be a subfield of K and let $\alpha_1, \ldots, \alpha_n$ be elements of K. We denote by $\kappa(\alpha_1, \ldots, \alpha_n)$ the smallest subfield of K containing κ and $\alpha_1, \ldots, \alpha_n$. Its elements consists of all quotients

$$\frac{P(\alpha_1, \ldots, \alpha_n)}{Q(\alpha_1, \ldots, \alpha_n)}$$

where P, Q are polynomials in n variables with coefficients in κ, and $Q(\alpha_1, \ldots, \alpha_n) \neq 0$. We say that K is *finitely generated* over κ if there is a finite family of elements $\alpha_1, \ldots, \alpha_n$ of K such that $K = \kappa(\alpha_1, \ldots, \alpha_n)$. We exhibit an example of such fields as follows:

Proposition 1.59. *If K is a finite extension of κ, then K is finitely generated over κ.*

Proposition 1.60. *Let A be a ring. Then every algebraic element α in its field of fractions κ can be transformed into an integral element by multiplication by a suitable nonzero element in A.*

Proof. To prove this assume that

$$c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n = 0$$

is an equation for α with coefficients in A and $c_0 \neq 0$. Then by multiplication by c_0^{n-1} we obtain an equation of A-coefficients for $y = c_0x$ with leading coefficient 1, which has the root $c_0\alpha$. □

1.6 Separable extension fields

1.6.1 Separable algebraic extensions

Let K be an extension of a field κ and let

$$\sigma : \kappa \longrightarrow L$$

be an *embedding* (i.e. an injective homomorphism) of κ into a field L. Then σ induces an isomorphism of κ with its image $\sigma(\kappa)$. An embedding τ of K in L will be said to be *over* σ if the restriction of τ to κ is equal to σ. We also say that τ *extends* σ. If $\kappa \subset L$ and if σ is the identity, then an embedding τ of K in L over σ is called an *embedding of K over κ*. In particular, an embedding of K into itself over κ usually is called an *automorphism of K over κ*.

Assume that L is algebraically closed. We analyze the extensions of σ to algebraic extensions K of κ. First of all, we consider the special case $K = \kappa(\alpha)$, where α is algebraic over κ of degree n. Let P_α be the minimal polynomial of α over κ. Let $\alpha^{(i)}$ be a root of $\sigma(P_\alpha)$ in L. Given an element β of $\kappa(\alpha) = \kappa[\alpha]$, we can write it in the form $\beta = g(\alpha)$ with some polynomial g over κ of degree $\leq n - 1$. We define an extension of σ by the mapping

$$g(\alpha) \mapsto \sigma(g)\big(\alpha^{(i)}\big).$$

This is in fact well defined, i.e. independent of the choice of polynomial g used to express our element in $\kappa[\alpha]$. Indeed, if $f(X)$ is in $\kappa[X]$ such that $g(\alpha) = f(\alpha)$, then $(g - f)(\alpha) = 0$, whence $P_\alpha(X)$ divides $g(X) - f(X)$. Hence $\sigma(P_\alpha)(X)$ divides $\sigma(g)(X) - \sigma(f)(X)$, and thus $\sigma(g)\left(\alpha^{(i)}\right) = \sigma(f)\left(\alpha^{(i)}\right)$. It is clear that the mapping is a homomorphism inducing σ on κ, and that it is an extension of σ to $\kappa(\alpha)$. Hence we get:

Proposition 1.61. *The number of possible extensions of σ to $\kappa(\alpha)$ is $\leq$ the number of roots of P_α, and is equal to the number of distinct roots of P_α.*

We are interested in extensions of σ to arbitrary algebraic extensions of κ. By using Zorn's lemma, one can prove the following result:

Proposition 1.62. *Let κ be a field, K an algebraic extension of κ, and $\sigma : \kappa \longrightarrow L$ an embedding of κ into an algebraically closed field L. Then there exists an extension of σ to an embedding of K in L. If K is algebraically closed and L is algebraic over $\sigma(\kappa)$, then any such extension of σ is an isomorphism of K onto L.*

As a corollary, we have a certain uniqueness for an algebraic closure of a field κ.

Corollary 1.63. *If L, L' are two algebraic closures of a field κ, there is an isomorphism $\lambda : L \longrightarrow L'$, which is the identity mapping on κ.*

Let K be an algebraic extension of a field κ and let

$$\sigma : \kappa \longrightarrow L$$

be an embedding of κ into an algebraically closed field L. Let S_σ be the set of extensions of σ to an embedding of K in L. Assume that L is algebraic over $\sigma(\kappa)$, hence is equal to an algebraic closure of $\sigma(\kappa)$. Let L' be another algebraically closed field, and let $\tau : \kappa \longrightarrow L'$ be an embedding. Let S_τ be the set of embeddings of K in L' extending τ. We also assume that L' is an algebraic closure of $\tau(\kappa)$. By Proposition 1.62, there exists an isomorphism $\lambda : L \longrightarrow L'$ extending the mapping $\tau \circ \sigma^{-1}$ applied to the field $\sigma(\kappa)$. If $\sigma^* \in S_\sigma$ is an extension of σ to an embedding of K in L, then $\lambda \circ \sigma^*$ is an extension of τ to an embedding of K in L', because for the restriction to κ we have

$$\lambda \circ \sigma^* = \tau \circ \sigma^{-1} \circ \sigma = \tau.$$

Thus λ induces a mapping from S_σ into S_τ. It is clear that the inverse mapping is induced by λ^{-1}, and hence that $S_\sigma,\ S_\tau$ are in bijection under the mapping $\sigma^* \mapsto \lambda \circ \sigma^*$. In particular, the cardinality of $S_\sigma,\ S_\tau$ are the same. Thus this cardinality depends only on the extension K/κ, and will be denoted by $[K : \kappa]_s$. We shall call it the *separable degree* of K over κ. A basic fact is listed as follows:

Proposition 1.64. *Let κ be a field and $F \subset K$ be algebraic extensions of κ. Then*

$$[K : \kappa]_s = [K : F]_s [F : \kappa]_s.$$

Furthermore, if K is finite over κ, then $[K : \kappa]_s$ is finite and divides $[K : \kappa]$.

Let κ be a field and let f be a polynomial over κ of degree ≥ 1. By a *splitting field* K of f we shall mean an extension K of κ such that f splits into linear factors in K, i.e.

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$$

with $\alpha_i \in K,\ i = 1, \ldots, n$, and such that

$$K = \kappa(\alpha_1, \ldots, \alpha_n)$$

is generated by all roots of f. A splitting field of a polynomial f over κ is unique in the sense of isomorphism:

Proposition 1.65. *Let K be a splitting field of a polynomial f over κ. If F is another splitting field of f, there is an isomorphism $\sigma : F \longrightarrow K$, which is the identity mapping on κ. If $\kappa \subset K \subset \overline{\kappa}$, where $\overline{\kappa}$ is an algebraic closure of κ, then any embedding of F in $\overline{\kappa}$ inducing the identity on κ must be an isomorphism of F onto K.*

Let I be a set of indices and let $\{f_i\}_{i\in I}$ be a family of polynomials over κ of degrees ≥ 1. By a *splitting field* for this family we shall mean an extension K of κ such that every f_i splits into linear factors in K, and K is generated by total roots of the polynomials $f_i,\ i \in I$. Let $\overline{\kappa}$ be an algebraic closure of κ, and let K_i be a splitting field of f_i in $\overline{\kappa}$. Then the smallest subfield of $\overline{\kappa}$ containing all fields $K_i,\ i \in I$ is a splitting field for the family $\{f_i\}_{i\in I}$.

Corollary 1.66. *Let K be a splitting field for the family $\{f_i\}_{i\in I}$. If F is another splitting field for $\{f_i\}_{i\in I}$, any embedding of F into $\overline{\kappa}$ inducing the identity on κ gives an isomorphism of F onto K.*

The following result gives characteristic conditions that an algebraic extension of κ is a splitting field of a family of polynomials over κ.

Theorem 1.67 (cf. [146]). *Let K be an algebraic extension of κ, contained in an algebraic closure $\overline{\kappa}$ of κ. Then the following conditions are equivalent:*

(1) *K is the splitting field of a family of polynomials over κ.*

(2) *Every embedding σ of K in $\overline{\kappa}$ over κ is an automorphism of K.*

(3) *Every irreducible polynomial over κ which has a root in K splits into linear factors in K.*

An extension K of κ satisfying one of the hypotheses (1)–(3) in Theorem 1.67 will be said to be *normal*. If K is an algebraic extension of κ, then there exists a smallest normal extension E of κ containing K. The field E can be given by taking the intersection of all normal extensions of κ containing K.

Let κ be a field, and $0 \neq f(x) \in \kappa[x]$. If $f(x)$ has no multiple root in an algebraic closure $\overline{\kappa}$ of κ, then f is called a *separable polynomial*. Let K be an extension of κ, and let $\alpha \in K$ be algebraic over κ. If the minimal polynomial of α over κ is separable, then α is called a *separable algebraic element* over κ, otherwise, α is *inseparable* over κ. If an inseparable element over κ exists, then $\mathrm{char}(\kappa) \neq 0$, where $\mathrm{char}(\kappa)$ denotes the characteristic of κ. We see that the separable condition is equivalent to saying that $[\kappa(\alpha) : \kappa]_s = [\kappa(\alpha) : \kappa]$ according to the following criterion:

Proposition 1.68. *Let K be an algebraic closure of κ. Take $\alpha \in K$ and let P_α be the minimal polynomial of α over κ. If $\mathrm{char}(\kappa) = 0$, then all roots of P_α have multiplicity 1 (P_α is separable). If $\mathrm{char}(\kappa) = p > 0$, then there exists an integer $\mu \geq 0$ such that every root of P_α has multiplicity p^μ. We have*

$$[\kappa(\alpha) : \kappa] = p^\mu [\kappa(\alpha) : \kappa]_s,$$

and α^{p^μ} is separable over κ.

If all elements in K are separable algebraic over κ, then K is called a *separable algebraic extension* of κ. An algebraic extension K of κ is said to be *purely inseparable* if every element in $K - \kappa$ is inseparable over κ. If K/κ is purely inseparable of finite degree, then $[K : \kappa]$ is a power of the characteristic p of κ. If K is separable over κ, we can choose a smallest normal extension E of κ containing K such that E is separable over κ. One has the following condition determining a separable algebraic extension:

Proposition 1.69. *Let K be a finite extension of a field κ. Then K is separable over κ if and only if $[K : \kappa]_s = [K : \kappa]$.*

Let K be an extension of a field κ. If $\alpha \in K$ is a separable algebraic element over κ, then $\kappa[\alpha]$ is a separable algebraic extension of κ. Further, if K is generated by a family of separable algebraic elements $\{\alpha_i\}_{i \in I}$ over κ, then K is separable over κ. Then one has the *theorem of the primitive element*:

Theorem 1.70. *Let K be a finite extension of a field κ. There exists an element $\alpha \in K$ such that $K = \kappa(\alpha)$ if and only if there exists only a finite number of fields F such that $\kappa \subset F \subset K$. If K is separable over κ, then there exists such an element α.*

Proof. Zariski and Samuel [307], Ch. II, Theorem 19, p. 84. □

Let K be any algebraic extension field of κ, and let S be the set of all elements of K which are separable over κ. Clearly, S is a field and S/κ is a separable extension. Then K/S is a purely inseparable extension.

A field κ of characteristic $p > 0$ is called *perfect* if $\{x^p \mid x \in \kappa\} = \kappa$. Every field of characteristic zero is also called perfect. It is well known that if κ is perfect, every algebraic extension of κ is separable and perfect (cf. [146]). If K is an extension field of κ which is not algebraic, the *transcendence degree* of K/κ is the maximum number of elements of K that are algebraically independent over κ. A subset S of K which is algebraically independent over κ and is maximal with respect to the inclusion ordering will be called a *transcendence base* of K over κ. If K is a finitely generated extension of κ, $K = \kappa(x)$, it is said to be *separably generated* if we can find a transcendence base $t = (t_1, \ldots, t_r)$ of K/κ such that K is separably algebraic over $\kappa(t)$. Such a transcendence base is said to be a *separating transcendence base* for K over κ.

Proposition 1.71 (cf. [33]). *Let κ be a perfect field and K an extension of κ of transcendence degree* 1. *Then there exists $x \in K$ such that $K/\kappa(x)$ is a separable extension. The element x is called a separating element of the extension.*

Let κ be a field and let G be a group of automorphisms of κ. Let $F(G)$ be the set of invariants of G, namely,

$$F(G) = \{x \mid x \in \kappa,\ \sigma(x) = x \text{ for all } \sigma \in G\}.$$

Then the set $F(G)$ is a subfield of κ, which is called the *invariant field* of G, or the *fixed field* of G. Let K be an algebraic extension of κ and let $G_{K/\kappa}$ be the group of automorphisms of K over κ. The field K is called a *Galois extension* of κ if K is a normal separable extension of κ. If K is a Galois extension of κ, then $G_{K/\kappa}$ is called the *Galois group* of K over κ. For the convenience of the reader, we shall now state the *main theorem of Galois theory* for finite Galois extensions.

Theorem 1.72 (cf. [187]). *Let K be a finite Galois extension of κ. Then we have*

(1) *Let E be an intermediate field between K and κ, namely $\kappa \subset E \subset K$. Then*

- **(α)** *K is a Galois extension of E. $G_{K/E}$ is a subgroup of $G_{K/\kappa}$.*
- **(β)** *The order of the group $G_{K/E}$ is $[K : E]$.*
- **(γ)** *The invariant field $F(G_{K/E})$ of $G_{K/E}$ is E.*

(2) *Let H be a subgroup of $G_{K/\kappa}$. Then*

- **(δ)** *The invariant field $F(H)$ is an intermediate field between K and κ.*
- **(ε)** *The order of H is $[K : F(H)]$.*
- **(ζ)** *The Galois group $G_{K/F(H)} = H$.*

Therefore, there is a bijective mapping between the set of subfields E of K containing κ, and the set of subgroups H of $G_{K/\kappa}$, given by $E = F(H)$ (resp., $H = G_{K/E}$). The E is Galois over κ if and only if H is normal in $G_{K/\kappa}$, and if that is the case, then the mapping $\sigma \mapsto \sigma|E$ induces an isomorphism of $G_{K/\kappa}/H$ onto the Galois group $G_{E/\kappa}$ of E over κ.

1.6.2 Ramification indices

The following theorem shows an important reason for considering Dedekind domains rather than some other kinds of integral domains.

Theorem 1.73. *Let A be a Dedekind domain with quotient field κ and let K be a finite dimensional extension field of κ. Then the integral closure of A in K is a Dedekind domain.*

Proof. See G. J. Janusz [119], Theorem 6.1, or P. M. Cohn [33], Chapter 2, Theorem 5.1. □

Let $A \subseteq B$ be Dedekind domains with quotient fields κ and K respectively. Let $\mathfrak{p}$ be a nonzero prime ideal of A. Then $B\mathfrak{p}$ is an ideal of B and it has a factorization

$$B\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \tag{1.18}$$

in which $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are distinct prime ideals of B and $e_1, \ldots, e_g$ are positive integers. Since $\mathfrak{p} \subseteq \mathfrak{P}_i$ and $\mathfrak{p}$ is a maximal ideal of A, then $\mathfrak{P}_i \cap A = \mathfrak{p}$ for each i. Thus the integer e_i is completely determined by $\mathfrak{P}_i$.

If $A \subseteq B$ are Dedekind domains and $\mathfrak{P}$ is a nonzero prime ideal of B and $\mathfrak{p} = A \cap \mathfrak{P}$, then the *ramification index* of $\mathfrak{P}$ over A is the power of $\mathfrak{P}$ that appears in the prime factorization of $B\mathfrak{p}$. We write the ramification index as either $e_{\mathfrak{P}/A}$ or $e_{\mathfrak{P}/\mathfrak{p}}$. We say $\mathfrak{P}$ is *ramified* over A if either the ramification index $e_{\mathfrak{P}/A}$ is greater than 1 or the field $B/\mathfrak{P}$ is not separable over $A/\mathfrak{p}$, *unramified* otherwise.

We say the prime ideal $\mathfrak{p}$ is *ramified* in B if $B\mathfrak{p}$ is divisible by some ramified prime ideal of B, *unramified* otherwise. The extension K/κ itself is called *unramified* if all prime ideals $\mathfrak{p}$ of A are unramified in B.

Exercise 1.74. *If $A \subseteq B \subseteq C$ are Dedekind domains and $\mathfrak{P}$ is a nonzero prime ideal of C, then one has the multiplicative property of the ramification indices*

$$e_{\mathfrak{P}/A} = e_{\mathfrak{P}/B} e_{\mathfrak{P}\cap B/A}.$$

If $\mathfrak{P}$ is a nonzero prime ideal of B with $A \cap \mathfrak{P} = \mathfrak{p}$, then $B/\mathfrak{P}$ is a field containing an isomorphic copy of $A/\mathfrak{p}$, which is also a field. The following property can be used to ensure that $B/\mathfrak{P}$ is finite dimensional over $A/\mathfrak{p}$.

Proposition 1.75. *Let $A \subseteq B$ be Dedekind domains with quotient fields κ and K respectively and let $\mathfrak{A}$ be an ideal of B such that $A \cap \mathfrak{A} = \mathfrak{p}$ is a nonzero prime ideal of A. Then $B/\mathfrak{A}$ is a vector space over $A/\mathfrak{p}$ and the dimension satisfy the inequality*

$$[B/\mathfrak{A} : A/\mathfrak{p}] \leq [K : \kappa].$$

Proof. See G. J. Janusz [119], Lemma 6.5. □

Let $A \subseteq B$ be Dedekind domains, $\mathfrak{P}$ a nonzero prime ideal of B and $\mathfrak{p} = A \cap \mathfrak{P}$. The dimension $[B/\mathfrak{P} : A/\mathfrak{p}]$ is called the *relative degree* (or *inertial degree*) of $\mathfrak{P}$ over $\mathfrak{p}$. We will sometimes write either $f_{\mathfrak{P}/\mathfrak{p}}$ or $f_{\mathfrak{P}/A}$ for this relative degree. If $\mathfrak{P}$ is ramified over A with $f_{\mathfrak{P}/\mathfrak{p}} = 1$, then $\mathfrak{P}$ also is said to be *totally ramified* over A.

Exercise 1.76. *If $A \subseteq B \subseteq C$ are Dedekind domains and $\mathfrak{P}$ is a nonzero prime ideal of C, then one has the multiplicative property of the relative degrees*

$$f_{\mathfrak{P}/A} = f_{\mathfrak{P}/B} f_{\mathfrak{P}\cap B/A}.$$

In the next theorem we make a connection between the ramification indices, relative degrees and the dimensions of the quotient fields of a pair of Dedekind domains.

Theorem 1.77. *Let $A \subseteq B$ be Dedekind domains with B integral over A and $\mathfrak{p}$ a nonzero prime ideal of A. Let $B\mathfrak{p}$ have the factorization given in Equation* (1.18) *and let $f_i = f_{\mathfrak{P}_i/A}$. Then*

(i)

$$\sum_{i=1}^{g} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}].$$

(ii) *If κ and K are the quotient fields of A and B respectively and the dimension $[K : \kappa]$ is finite, then*

$$\sum_{i=1}^{g} e_i f_i \leq [K : \kappa].$$

In particular, if K is separable, the equality holds.

(iii) *If $(A - \mathfrak{p})^{-1}B$ is finitely generated as a module over $A_{\mathfrak{p}}$, then*

$$\sum_{i=1}^{g} e_i f_i = [K : \kappa].$$

Proof. See G. J. Janusz [119], Theorem 6.6, Corollary 6.7 in Chapter I. □

Theorem 1.78. *Let A be a Dedekind domain with quotient field κ and let B be the integral closure of A in a finite dimensional Galois extension K of κ. For a nonzero prime ideal $\mathfrak{p}$ of A, the ideal $B\mathfrak{p}$ has the factorization*

$$B\mathfrak{p} = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e, \tag{1.19}$$

in which $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are distinct prime ideals of B. All relative degrees $f_{\mathfrak{P}_i/A}$ are equal (to f say) and we have

$$efg = [K : \kappa].$$

Moreover the action of Galois group $G_{K/\kappa}$ transitively permutes the prime ideals $\mathfrak{P}_i$ of B containing $\mathfrak{p}$.

Proof. See G. J. Janusz [119], Theorem 6.8 in Chapter I. □

1.7 Norm and trace

Let K be a finite field extension of a field κ. Take $\alpha \in K$. Then α induces a κ-linear mapping

$$\mathbf{A}_\alpha : K \longrightarrow K$$

defined by $\mathbf{A}_\alpha(x) = \alpha x$. Let $\{w_1, \ldots, w_n\}$ be a base of K over κ. Write

$$\mathbf{A}_\alpha(w_i) = \alpha w_i = \sum_{j=1}^{n} a_{ij} w_j.$$

The characteristic polynomial

$$\chi_\alpha(x) = \det(xI - A_\alpha)$$

of the matrix form $A_\alpha = (a_{ij})$ of $\mathbf{A}_\alpha$ is called the *field polynomial* of α. The field polynomial χ_α is independent of the base $\{w_1, \ldots, w_n\}$ selected for K over κ. Obviously, α is a root of its field polynomial.

Lemma 1.79. *Let K be a finite field extension of a field F which is a finite field extension of κ, and $\alpha \in F$. Let the field polynomial of α as an element of K be $\chi_\alpha(x)$, the field polynomial of α as an element of F be $G(x)$, and the minimal polynomial of α over κ be $P_\alpha(x)$. Then we have*

(A) *$K = \kappa(\alpha)$ if and only if $\chi_\alpha(x) = P_\alpha(x)$.*

(B) *$\chi_\alpha(x) = G(x)^{[K:F]}$.*

Proof. (A) Since α is a root of χ_α, therefore we have $P_\alpha(x) \mid \chi_\alpha(x)$. Since their degrees are equal, and both are monic polynomials, then they must be equal.

(B) Let $[F : \kappa] = s$. Let $\{u_1, \ldots, u_s\}$ be a basis for F over κ, and $\{v_1, \ldots, v_m\}$ be a basis for K over F. Let K_i be the following subspace

$$K_i = \overset{s}{\underset{j=1}{\oplus}} u_j v_i \kappa.$$

Then we have

$$K = \overset{m}{\underset{i=1}{\oplus}} K_i.$$

Each K_i is an invariant subspace of $\mathbf{A}_\alpha$ with the characteristic polynomial of the restriction of $\mathbf{A}_\alpha$ to K_i equaling $G(x)$. Therefore, we have $\chi_\alpha(x) = G(x)^{[K:F]}$. □

Let $P_\alpha \in \kappa[x]$ be the minimal polynomial of α over κ. Let χ_α be the field polynomial of α. Then one has

$$\chi_\alpha(0) = (-1)^{[K:\kappa]} \det(A_\alpha) = P_\alpha(0)^{[K:\kappa(\alpha)]},$$

and hence

$$\det(A_\alpha) = \Big\{(-1)^d P_\alpha(0)\Big\}^{[K:\kappa(\alpha)]} = \Big\{(-1)^d P_\alpha(0)\Big\}^{\frac{[K:\kappa]}{d}},$$

where $d = \deg(P_\alpha) = [\kappa(\alpha) : \kappa]$. We will denote the element of κ by $\mathbf{N}_{K/\kappa}(\alpha)$, called the *norm of α over κ*. Define the *trace* $\mathbf{Tr}_{K/\kappa}(\alpha)$ of α over κ as $\text{trace}(A_\alpha) = \sum a_{ii}$. In other words, in the following field polynomial χ_α of α, we have

$$\chi_\alpha(x) = x^n - \mathbf{Tr}_{K/\kappa}(\alpha) x^{n-1} + \cdots + (-1)^n \mathbf{N}_{K/\kappa}(\alpha),$$

where $n = [K : \kappa]$. The norm of K over κ

$$\mathbf{N}_{K/\kappa} : K \longrightarrow \kappa$$

is a multiplicative homomorphism of K_* into κ_*, namely

$$\mathbf{N}_{K/\kappa}(\alpha\beta) = \mathbf{N}_{K/\kappa}(\alpha)\mathbf{N}_{K/\kappa}(\beta) \in \kappa_*, \ \ \alpha, \beta \in K_*.$$

The trace of K over κ

$$\mathbf{Tr}_{K/\kappa} : K \longrightarrow \kappa$$

determines a κ-linear mapping of K to κ, namely, for $\alpha, \beta \in K$, $a \in \kappa$,

$$\mathbf{Tr}_{K/\kappa}(\alpha + \beta) = \mathbf{Tr}_{K/\kappa}(\alpha) + \mathbf{Tr}_{K/\kappa}(\beta), \quad \mathbf{Tr}_{K/\kappa}(a\alpha) = a\mathbf{Tr}_{K/\kappa}(\alpha).$$

When $\alpha \in \kappa$, the following formulas

$$\mathbf{Tr}_{K/\kappa}(\alpha) = [K : \kappa]\alpha, \quad \mathbf{N}_{K/\kappa}(\alpha) = \alpha^{[K:\kappa]} \tag{1.20}$$

are trivial. By Lemma 1.79, if K is a finite field extension of a field F which is a finite field extension of κ, and $\alpha \in F$, then we have

$$\mathbf{Tr}_{K/\kappa}(\alpha) = [K : F]\mathbf{Tr}_{F/\kappa}(\alpha), \quad \mathbf{N}_{K/\kappa}(\alpha) = \mathbf{N}_{F/\kappa}(\alpha)^{[K:F]}. \tag{1.21}$$

Let K be a finite extension of a field κ. Let $[K : \kappa]_s = r$, and let

$$p^\mu = \frac{[K : \kappa]}{[K : \kappa]_s}$$

if the characteristic of κ is $p > 0$, and 1 otherwise. Let $\overline{\kappa}$ be an algebraic closure of κ and let $\sigma_1, \ldots, \sigma_r$ be the distinct embeddings of K in $\overline{\kappa}$. Then for $\alpha \in K$, one has

$$\mathbf{N}_{K/\kappa}(\alpha) = \prod_{i=1}^{r} \sigma_i\left(\alpha^{p^\mu}\right), \quad \mathbf{Tr}_{K/\kappa}(\alpha) = p^\mu \sum_{i=1}^{r} \sigma_i(\alpha). \tag{1.22}$$

When $K = \kappa(\alpha)$, it is easy to show that (1.22) holds by using Proposition 1.61. Generally, the mappings of K into κ defined by (1.22) are transitive, in other words, if we have three fields $\kappa \subset F \subset K$, then (cf. [146])

$$\mathbf{Tr}_{F/\kappa} \circ \mathbf{Tr}_{K/F} = \mathbf{Tr}_{K/\kappa}, \quad \mathbf{N}_{F/\kappa} \circ \mathbf{N}_{K/F} = \mathbf{N}_{K/\kappa}. \tag{1.23}$$

Thus (1.22) follows from (1.21) and (1.23) applied to $F = \kappa(\alpha)$.

Theorem 1.80. *Let K be a finite separable extension of a field κ. Then $\mathbf{Tr}_{K/\kappa} : K \longrightarrow \kappa$ is a non-zero functional. The mapping $(x, y) \mapsto \mathbf{Tr}_{K/\kappa}(xy)$ of $K \times K \longrightarrow \kappa$ is bilinear, and identifies K with its dual space.*

Proof. Trivially, $\mathbf{Tr}_{K/\kappa} : K \longrightarrow \kappa$ is a non-zero functional. For each $x \in K$, the mapping

$$\mathbf{Tr}_{K/\kappa,x} : K \longrightarrow \kappa$$

such that $\mathbf{Tr}_{K/\kappa,x}(y) = \mathbf{Tr}_{K/\kappa}(xy)$ is obviously a κ-linear mapping, and the mapping

$$x \mapsto \mathbf{Tr}_{K/\kappa,x}$$

is a κ-homomorphism of K into its dual space K^*. If $\mathbf{Tr}_{K/\kappa,x}$ is the zero mapping, then $\mathbf{Tr}_{K/\kappa}(xK) = 0$. If $x \neq 0$ then $xK = K$. Hence the kernel of $x \mapsto \mathbf{Tr}_{K/\kappa,x}$ is 0. Hence we get an injective homomorphism of K into K^*. Since these spaces have the same finite dimension, it follows that we get an isomorphism. □

Let $w_1, \ldots, w_n$ be a basis of K over κ. Then $\mathbf{Tr}_{K/\kappa,w_1}, \ldots, \mathbf{Tr}_{K/\kappa,w_n}$ is a basis of K^*. Thus we can find $v_1, \ldots, v_n \in K$ to satisfy

$$\mathbf{Tr}_{K/\kappa}(w_i v_j) = \delta_{ij},$$

where $\delta_{ij} = 1$ if $i = j$, otherwise $\delta_{ij} = 0$. Obviously, $v_1, \ldots, v_n$ forms a basis of K over κ.

Proposition 1.81. *Let A be an integrally closed domain, κ its field of fractions, K a finite separable algebraic extension of κ, B the integral closure of A in K. Then there exists a basis $v_1, \ldots, v_n$ of K over κ such that $B \subseteq \sum_{j=1}^{n} Av_j$.*

Proof. By Proposition 1.60, given any basis of K over κ we may multiply the basis elements by suitable elements of A to get a basis $w_1, \ldots, w_n$ such that each $w_i \in B$. Since K/κ is separable, the bilinear form $(x, y) \mapsto \mathbf{Tr}_{K/\kappa}(xy)$ on K is non-degenerate, and hence we have a dual basis $v_1, \ldots, v_n$ of K over κ, defined by $\mathbf{Tr}_{K/\kappa}(w_i v_j) = \delta_{ij}$. Let $x \in B$, say

$$x = x_1 v_1 + x_2 v_2 + \cdots + x_n v_n \ (x_i \in \kappa).$$

We have $xw_i \in B$ since $w_i \in B$, and therefore $\mathbf{Tr}_{K/\kappa}(xw_i) \in A$. But,

$$\mathbf{Tr}_{K/\kappa}(xw_i) = \sum_{j=1}^{n} \mathbf{Tr}_{K/\kappa}(x_j w_i v_j) = \sum_{j=1}^{n} x_j \mathbf{Tr}_{K/\kappa}(w_i v_j) = x_i,$$

hence $x_i \in A$. Consequently, Proposition 1.81 is proved. □

Let A be a Dedekind domain with quotient field κ, B be the integral closure of A in a finite dimensional separable field extension K of κ. If $\alpha \in B$, then $\mathbf{N}_{K/\kappa}(\alpha) \in A$. We see this by considering the minimum and field polynomials of α. The minimum polynomial of α has coefficients in A and the field polynomial is a power of the minimum polynomial. Then $\pm\mathbf{N}_{K/\kappa}(\alpha)$ is the constant term of the field polynomial, so $\mathbf{N}_{K/\kappa}(\alpha) \in A$.

Let $\mathfrak{B}$ be an ideal of B. The *norm* of $\mathfrak{B}$ is the ideal of A generated by all elements $\mathbf{N}_{K/\kappa}(\alpha)$ with $\alpha \in \mathfrak{B}$; that is,

$$\mathbf{N}_{K/\kappa}(\mathfrak{B}) = \sum_{\alpha\in\mathfrak{B}} A\mathbf{N}_{K/\kappa}(\alpha). \tag{1.24}$$

One has the following simple property

$$\mathbf{N}_{K/\kappa}(B\alpha) = A\mathbf{N}_{K/\kappa}(\alpha),\ \ \alpha \in B. \tag{1.25}$$

In fact, since

$$1 \in B, \quad \mathbf{N}_{K/\kappa}(1) = 1 \in \mathbf{N}_{K/\kappa}(B) = A,$$

then

$$\begin{aligned}\mathbf{N}_{K/\kappa}(B\alpha) &= \sum_{x\in B} A\mathbf{N}_{K/\kappa}(x\alpha) = \sum_{x\in B} A\mathbf{N}_{K/\kappa}(x)\mathbf{N}_{K/\kappa}(\alpha)\\ &= \mathbf{N}_{K/\kappa}(B)\mathbf{N}_{K/\kappa}(\alpha) = A\mathbf{N}_{K/\kappa}(\alpha).\end{aligned}$$

If S is a multiplicatively closed subset of A and $\mathfrak{B}$ an ideal of B, then

$$S^{-1}\mathbf{N}_{K/\kappa}(\mathfrak{B}) = \mathbf{N}_{K/\kappa}(S^{-1}\mathfrak{B}). \tag{1.26}$$

In fact, any element of $S^{-1}\mathfrak{B}$ has the form b/s with $b \in \mathfrak{B}$ and $s \in S$. Then

$$\mathbf{N}_{K/\kappa}(b/s) = \mathbf{N}_{K/\kappa}(b)/s^{[K:\kappa]}.$$

It follows that $\mathbf{N}_{K/\kappa}(S^{-1}\mathfrak{B}) \subseteq S^{-1}\mathbf{N}_{K/\kappa}(\mathfrak{B})$. Conversely, the ideal $S^{-1}\mathbf{N}_{K/\kappa}(\mathfrak{B})$ is generated over $S^{-1}A$ by elements $\mathbf{N}_{K/\kappa}(\alpha)$ with $\alpha \in \mathfrak{B}$. All such elements are in $\mathbf{N}_{K/\kappa}(S^{-1}\mathfrak{B})$, so the other inclusion also holds.

Proposition 1.82. *For ideals $\mathfrak{A}$ and $\mathfrak{B}$ of B, one has*

$$\mathbf{N}_{K/\kappa}(\mathfrak{A}\mathfrak{B}) = \mathbf{N}_{K/\kappa}(\mathfrak{A})\mathbf{N}_{K/\kappa}(\mathfrak{B}). \tag{1.27}$$

Proof. For a maximal ideal $\mathfrak{p}$ of A let $S = A - \mathfrak{p}$. Then $A_{\mathfrak{p}} = S^{-1}A$ is a discrete valuation ring and $S^{-1}B$ is a Dedekind domain with only finite number of maximal ideals, namely those corresponding to the ideals of B that contain $\mathfrak{p}$. Hence $S^{-1}B$ is a principal ideal domain. Then

$$(S^{-1}B)\mathfrak{A} = S^{-1}\mathfrak{A} = (S^{-1}B)a, \quad (S^{-1}B)\mathfrak{B} = S^{-1}\mathfrak{B} = (S^{-1}B)b$$

for some $a, b \in S^{-1}B$, and so

$$\begin{aligned}S^{-1}\mathbf{N}_{K/\kappa}(\mathfrak{A}\mathfrak{B}) &= \mathbf{N}_{K/\kappa}((S^{-1}\mathfrak{A})\cdot(S^{-1}\mathfrak{B})) = \mathbf{N}_{K/\kappa}((S^{-1}B)a\cdot(S^{-1}B)b)\\ &= \mathbf{N}_{K/\kappa}((S^{-1}B)ab) = (S^{-1}B)\mathbf{N}_{K/\kappa}(ab)\\ &= \mathbf{N}_{K/\kappa}(S^{-1}\mathfrak{A})\mathbf{N}_{K/\kappa}(S^{-1}\mathfrak{B}) = S^{-1}(\mathbf{N}_{K/\kappa}(\mathfrak{A})\mathbf{N}_{K/\kappa}(\mathfrak{B})).\end{aligned}$$

This holds for every maximal ideal $\mathfrak{p}$ so the claim is proved. □

Since each fractional ideal can be written as the quotient of two integral ideals, we may extend the definition (1.24) to fractional ideals by

$$\mathbf{N}_{K/\kappa}\left(\frac{\mathfrak{A}}{\mathfrak{B}}\right) = \frac{\mathbf{N}_{K/\kappa}(\mathfrak{A})}{\mathbf{N}_{K/\kappa}(\mathfrak{B})}.$$

Obviously, the formula (1.27) is true for fractional ideals.

Proposition 1.83. *For each prime ideal $\mathfrak{P}$ of B there is exactly one prime ideal $\mathfrak{p}$ of A which is divisible by $\mathfrak{P}$. Then*

$$\mathbf{N}_{K/\kappa}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}/\mathfrak{p}}}.$$

Proof. If $\mathbf{N}_{K/\kappa}(\mathfrak{P})$ is decomposed into its prime factors, then by Theorem 1.39, $\mathfrak{P}$ must divide at least one of these prime ideals of A. If $\mathfrak{P}$ were to divide two distinct prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ of A, then it would also have to be a divisor of $(\mathfrak{p}_1, \mathfrak{p}_2) = 1$, which, however, cannot be the case. Thus there exists exactly one prime ideal $\mathfrak{p}$ of A which is divisible by $\mathfrak{P}$. If the decomposition of $\mathfrak{p}$ into prime ideals of B is

$$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_s,$$

then it follows that

$$\mathbf{N}_{K/\kappa}(\mathfrak{P}_1)\mathbf{N}_{K/\kappa}(\mathfrak{P}_2)\cdots\mathbf{N}_{K/\kappa}(\mathfrak{P}_s) = \mathbf{N}_{K/\kappa}(\mathfrak{p}) = \mathfrak{p}^m.$$

Each factor on the left is an ideal of A and by this equation each factor must be a power of $\mathfrak{p}$. Therefore

$$\mathbf{N}_{K/\kappa}(\mathfrak{P}_i) = \mathfrak{p}^{f_{\mathfrak{P}_i/\mathfrak{p}}}. \qquad \square$$

For the proof, see Gerald J. Janusz [119], Proposition 8.2.

1.8 Discriminant of field extensions

In this section, discriminants of field extensions will be defined. Mainly, we will show an important formula of discriminants on a tower of field extensions.

Let κ be a field, and let K be a finite field extension of κ with a basis $\{w_1, \ldots, w_n\}$. Then the *discriminant* $D_{K/\kappa}(w_1, \ldots, w_n)$ of the basis $\{w_1, \ldots, w_n\}$ is defined as

$$D_{K/\kappa}(w_1, \ldots, w_n) = \det(\mathbf{Tr}_{K/\kappa}(w_i w_j)). \tag{1.28}$$

Let $\{w'_1, \ldots, w'_n\}$ be another basis of K over κ. Set

$$w'_i = \sum_{k=1}^{n} b_{ik} w_k.$$

Then we have

$$\begin{aligned} D_{K/\kappa}(w_1', \ldots, w_n') &= \det\left(\mathbf{Tr}_{K/\kappa}(w_i' w_j')\right) \\ &= \det\left(\sum_{k,l} b_{ik} b_{jl} \mathbf{Tr}_{K/\kappa}(w_k w_l)\right) \\ &= \{\det(b_{ik})\}^2 \det(\mathbf{Tr}_{K/\kappa}(w_k w_l)), \end{aligned}$$

that is

$$D_{K/\kappa}(w_1', \ldots, w_n') = \{\det(b_{ik})\}^2 D_{K/\kappa}(w_1, \ldots, w_n). \tag{1.29}$$

Let K be a finite separable algebraic extension of κ, of degree n. Let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of K in $\overline{\kappa}$ over κ, where $\overline{\kappa}$ is an algebraic closure of κ. Then the discriminant of a basis $\{w_1, \ldots, w_n\}$ of K over κ satisfies

$$D_{K/\kappa}(w_1, \ldots, w_n) = \{\det(\sigma_i(w_j))\}^2. \tag{1.30}$$

In fact, by (1.22), we have

$$\mathbf{Tr}_{K/\kappa}(w_i w_j) = \sum_{m=1}^{n} \sigma_m(w_i w_j) = \sum_{m=1}^{n} \sigma_m(w_i)\sigma_m(w_j),$$

which means

$$(\mathbf{Tr}_{K/\kappa}(w_i w_j)) = {}^t((\sigma_i(w_j))((\sigma_i(w_j)),$$

and hence the claim follows.

Theorem 1.84. *Let K be a finite extension of κ, and $\{w_1, \ldots, w_n\}$ a basis of K over κ. Then $D_{K/\kappa}(w_1, \ldots, w_n) \neq 0$ if and only if K is a separable algebraic extension of κ.*

Proof. ($\Rightarrow$) Let κ_K^S be a separable closure of κ in K. If $\kappa_K^S = K$, then K is separable algebraic over κ, and we are done. Otherwise, $\kappa_K^S \neq K$, K is purely inseparable over κ_K^S, and

$$[K : \kappa_K^S] = p^r, \ \ r \geq 1.$$

Let α be any element in K. We claim that $\mathbf{Tr}_{K/\kappa}(\alpha) = 0$, and so $D_{K/\kappa}(w_1, \ldots, w_n) = 0$. We distinguish two cases, (i) $\alpha \in \kappa_K^S$, (ii) $\alpha \notin \kappa_K^S$.

Case (i). Let the field polynomial of α as an element in κ_K^S (resp. K) be $G(x)$ (resp. $\chi_\alpha(x)$), and write

$$G(x) = x^m + a_1 x^{m-1} + \cdots + a_m.$$

It follows from Lemma 1.79, that

$$\chi_\alpha(x) = G(x)^{p^r} = x^{mp^r} + 0x^{mp^r - 1} + \cdots .$$

Therefore, $\mathbf{Tr}_{K/\kappa}(\alpha) = 0$.

Case (ii). There is an integer $l \geq 1$ such that the minimal polynomial $P_\alpha(x)$ of α over κ is in $\kappa[x^{p^l}]$. It follows from Lemma 1.79 that the field polynomial $\chi_\alpha(x)$ of α as an element in K is of the following form

$$\chi_\alpha(x) = P_\alpha(x)^s \in \kappa[x^{p^l}].$$

Therefore, $\mathbf{Tr}_{K/\kappa}(\alpha) = 0$.

($\Leftarrow$) Since K is a finite separable algebraic extension of κ, then there exists an element $\alpha \in K$ such that $K = \kappa[\alpha]$. Let us take $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ as a basis of K over κ. Let $\overline{K}$ be an algebraic closure of K, and $P_\alpha(x)$ be the minimal polynomial of α over κ. Note that the filed polynomial of α is $P_\alpha(x)$. Let $P_\alpha(x)$ be split completely in $\overline{K}$ as follows

$$P_\alpha(x) = \prod_{i=1}^{n}(x - \alpha_i), \;\; \alpha_1 = \alpha, \;\; \alpha_i \neq \alpha_j \;\; (i \neq j).$$

Then we have

$$\mathbf{Tr}_{K/\kappa}(\alpha) = \sum_{i=1}^{n} \alpha_i.$$

Further, we claim

$$\mathbf{Tr}_{K/\kappa}(\alpha^j) = \sum_{i=1}^{n} \alpha_i^j.$$

Let the splitting field of $P_\alpha(x)$ in $\overline{K}$ be E which is a Galois extension of κ with Galois group $G_{E/\kappa}$. In the collection $\{\alpha_1^j, \alpha_2^j, \ldots, \alpha_n^j\}$, some elements may be identical. It is easy to see that each element appears with the same multiplicities. Picking all distinct elements from it to form a set $\{\beta_1, \ldots, \beta_m\}$. Then we have that $m \mid n$, and the polynomial $Q(x)$ defined as

$$Q(x) = \prod_{i=1}^{m}(x - \beta_i)$$

is the minimal polynomial of α^j over κ. Then we have

$$\mathbf{Tr}_{k[\alpha^j]/\kappa}(\alpha^j) = \sum_{i=1}^{m} \beta_i,$$

$$\mathbf{Tr}_{K/\kappa}(\alpha^j) = \frac{n}{m} \sum_{i=1}^{m} \beta_i = \sum_{i=1}^{n} \alpha_i^j.$$

Therefore, the discriminant is related the *van der Monde determinant* as follows:

$$D_{K/\kappa}(1,\alpha,\ldots,\alpha^{n-1}) = \begin{vmatrix} n & \sum\alpha_i & \cdots & \sum\alpha_i^{n-1} \\ \sum\alpha_i & \sum\alpha_i^2 & \cdots & \sum\alpha_i^n \\ \cdots & \cdots & \cdots & \cdots \\ \sum\alpha_i^{n-1} & \sum\alpha_i^n & \cdots & \sum\alpha_i^{2n-2} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{vmatrix}$$

$$= \left\{ \prod_{i>j} (\alpha_i - \alpha_j) \right\}^2 \neq 0,$$

and hence the theorem is proved. □

In the proof of Theorem 1.84, since the derivative of P_α at α_i is easily computed to be

$$P'_\alpha(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j),$$

it follows that

$$D_{K/\kappa}(1,\alpha,\ldots,\alpha^{n-1}) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} P'_\alpha(\alpha_i),$$

and hence

$$D_{K/\kappa}(1,\alpha,\ldots,\alpha^{n-1}) = (-1)^{n(n-1)/2} \mathbf{N}_{K/\kappa}(P'_\alpha(\alpha)) \tag{1.31}$$

which is just the discriminant of the element α.

Recall that a symmetric bilinear form $(\,,\,) : K \times K \longrightarrow \kappa$ is *nondegenerate* if $(K, x) = 0$ implies $x = 0$. Theorem 1.84 immediately yields the following result (or cf. Gerald J. Janusz [119], Theorem 5.2):

Theorem 1.85. *The finite dimensional field extension K of κ is separable if and only if the symmetric bilinear form $(x, y) = \mathbf{Tr}_{K/\kappa}(xy)$ from $K \times K$ to κ is nondegenerate.*

1.9 Absolute values on fields

1.9.1 Absolute values

Definition 1.86. An absolute value on a field κ is a function $|\cdot| : \kappa \longrightarrow \mathbb{R}_+$ that satisfies the following conditions:

(1) $|x| = 0$ if and only if $x = 0$;

(2) $|xy| = |x||y|$ for all $x, y \in \kappa$;

(3) $|x + y| \leq |x| + |y|$ for all $x, y \in \kappa$.

If instead of (3) the absolute value satisfies the stronger condition

(4) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in \kappa$,

then the absolute value is called ultrametric or non-Archimedean. Otherwise, it is called Archimedean. The absolute value $|\cdot|$ is said to be *trivial* if

$$|x| = \begin{cases} 1, & x \in \kappa_*, \\ 0, & x = 0. \end{cases}$$

An absolute value $|\cdot|$ on a field κ induces a *distance function* d defined by

$$d(x, y) = |x - y|,$$

for any two elements $x, y \in \kappa$, and hence induces a topology on κ. A field κ with an absolute value is said to be *complete* if every Cauchy sequence in κ has a limit in κ under the induced topology. Two absolute values on a field κ are said to be *equivalent* (or *dependent*) if they induce the same topology (i.e., the same sets of convergent sequences) on κ. We have the following more accessible criterion:

Lemma 1.87. *Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on a field κ. The following statements are equivalent:*

(i) *$|\cdot|_1$ and $|\cdot|_2$ are equivalent absolute values;*

(ii) *$|x|_1 < 1$ if and only if $|x|_2 < 1$ for any $x \in \kappa$;*

(iii) *there exists a positive real number α such that for each $x \in \kappa$, one has $|x|_1 = |x|_2^{\alpha}$.*

Proof. See [33], Theorem 2.1 in Chapter 1; or [77], [215]. □

Inequivalent absolute values satisfy a rather strong independence property showed by the following fundamental *approximation theorem* of Mahler, reminiscent of the Chinese Remainder Theorem.

Theorem 1.88. *Let $|\cdot|_1, \ldots, |\cdot|_r$ be non-trivial absolute values on a field κ which are pairwise inequivalent. Then any r-tuple over κ can be simultaneously approximated; thus for any $\alpha_1, \ldots, \alpha_r \in \kappa$ and $\varepsilon > 0$ there exists $\alpha \in \kappa$ such that*

$$|\alpha - \alpha_i|_i < \varepsilon, \;\; i = 1, \ldots, r. \tag{1.32}$$

Proof. See [33], Theorem 2.3 in Chapter 1, or [215], Theorem 2 in Section 1.4. □

Let $p \in \mathbb{Z}^+$ be a prime number and let ord_p be the p-adic valuation on $\mathbb{Q}$. The function

$$|x|_p = p^{-\mathrm{ord}_p(x)}$$

of $x \in \mathbb{Q}$ is a non-Archimedean absolute value on $\mathbb{Q}$, called the *p-adic absolute value*, which was first introduced by Hensel in 1904. Let $|\cdot|_\infty$ denote the ordinary Archimedean absolute value on $\mathbb{Q}$. These absolute values are related by the *product formula*

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1, \ \ x \in \mathbb{Q}_*, \tag{1.33}$$

where

$$M_{\mathbb{Q}} = \{\infty\} \cup \{\text{primes}\}.$$

Further, we have *Ostrowski's first theorem*:

Theorem 1.89 (Ostrowski [211]). *Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. If $|\cdot|$ is Archimedean, then there exists α with $0 < \alpha \leq 1$ such that*

$$|x| = |x|_\infty^\alpha, \ \ x \in \mathbb{Q}.$$

If $|\cdot|$ is non-Archimedean, then there exist a prime p and real $\beta > 0$ such that

$$|x| = |x|_p^\beta, \ \ x \in \mathbb{Q}.$$

Proof. See [232]; or [33], Theorem 3.4 and Proposition 4.3 in Chapter 1. □

According to Lemma 1.87 and Theorem 1.89, the set $M_{\mathbb{Q}}$ is one-to-one with the set of equivalence classes of all absolute values in $\mathbb{Q}$.

Let κ be a field with an absolute value $|\cdot|$. A field $\hat{\kappa}$ with an absolute value $|\cdot|_\wedge$ is said to be a *completion* of κ when the following properties are satisfied:

(I) κ is a subfield of $\hat{\kappa}$, $|\cdot|$ is the restriction of $|\cdot|_\wedge$ to κ;

(II) $\hat{\kappa}$ is complete;

(III) Each elements of $\hat{\kappa}$ is the limit of a Cauchy sequence of elements in κ.

A basic fact is that the field κ has a completion $\hat{\kappa}$. If $\tilde{\kappa}$ is any other completion of κ, there exists a κ-isomorphism $\varphi : \tilde{\kappa} \longrightarrow \hat{\kappa}$, i.e., φ leaves invariant every element of κ and

$$|\varphi(x)|_\wedge = |x|_\sim, \ \ x \in \tilde{\kappa}.$$

The completion of $\mathbb{Q}$ with the usual absolute value is $\mathbb{R}$. According to the standard theory in p-adic analysis, the completion of $\mathbb{Q}$ relative to the topology induced by the p-adic absolute value $|\cdot|_p$ is just the field $\mathbb{Q}_p$ of *p-adic numbers*, and the absolute value $|\cdot|_p$ on $\mathbb{Q}$ extends to a non-Archimedean absolute value on $\mathbb{Q}_p$, which is also denoted by $|\cdot|_p$. The set of values of $\mathbb{Q}$ and $\mathbb{Q}_p$ under $|\cdot|_p$ is the same, which is equal to the set

$$\{p^n \mid n \in \mathbb{Z}\} \cup \{0\}.$$

In particular, the valuation ring of p-adic valuation ord_p

$$\mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p, \mathrm{ord}_p}$$

is both open and closed, which is called the ring of *p-adic integers*.

It is possible to determine all fields which are complete under an Archimedean absolute value: the only cases are $\mathbb{R}$ and $\mathbb{C}$, which is just contents of the *Ostrowski's second theorem*:

Theorem 1.90. *Let κ be a field with an Archimedean absolute value $|\cdot|$ for which it is complete. Then there exists a real number α with $0 < \alpha \leq 1$, and an isomorphism φ from κ onto $\mathbb{R}$ or $\mathbb{C}$ such that*

$$|x| = |\varphi(x)|_\infty^\alpha, \ \ x \in \kappa.$$

Proof. See [33], Theorem 3.5 in Chapter 1, or [215], Section 1.6. □

1.9.2 Extensions of absolute values

Definition 1.91. Let V be a vector space over a field κ and let $|\cdot|$ be a non-trivial absolute value on κ. A function $f : V \longrightarrow \mathbb{R}_+$ is called a norm or distance function on V (compatible with the absolute value of κ) if it satisfies the following conditions:

(α) $f(\mathbf{x}) = 0$ if and only if $\mathbf{x} = 0$;

(β) $f(a\mathbf{x}) = |a|f(\mathbf{x})$ for all $a \in \kappa$ and all $\mathbf{x} \in V$;

(γ) $f(\mathbf{x} + \mathbf{y}) \leq f(\mathbf{x}) + f(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in V$.

A vector space V with a norm is called a normed vector space over κ.

Let V be a normed vector space. Then any norm f induces a metric d as follows

$$d(\mathbf{x}, \mathbf{y}) = f(\mathbf{x} - \mathbf{y}),$$

which makes V a topological space. Two norms f_1 and f_2 on V are said to be *equivalent* if there are positive real numbers c_1 and c_2 such that

$$c_1 f_1 \leq f_2 \leq c_2 f_1.$$

Equivalently, they define the same topology on V (i.e., a set is open with respect to one norm if and only if it is open with respect to the other).

Proposition 1.92. *If V is a finite-dimensional and if κ is complete under a non-trivial absolute value, then any two norms on V are equivalent, and V is complete with respect to the metric induced by any norm.*

Proof. Fix a basis $\{e_1, \ldots, e_n\}$ of V. Any vector $\mathbf{x}$ in V can then be written (uniquely) in the form

$$\mathbf{x} = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$$

with $x_i \in \kappa$. We can define a norm on V by putting

$$f(\mathbf{x}) = \max_{1 \leq i \leq n} |x_i|.$$

To prove that V is complete in the norm f, let

$$\mathbf{x}^{(j)} = \sum_{i=1}^{n} x_i^{(j)} e_i$$

be a Cauchy sequence. Then $\mathbf{x}^{(j)} - \mathbf{x}^{(l)} \to 0$ and so $|x_i^{(j)} - x_i^{(l)}| \to 0$ as $j, l \to \infty$, for $i = 1, \ldots, n$. Hence $x_i^{(j)}$ converges to x_i say, by the completeness of κ. Write $\mathbf{x} = \sum x_i e_i$; then

$$f(\mathbf{x}^{(j)} - \mathbf{x}) = \max_{1 \le i \le n} |x_i^{(j)} - x_i| \to 0,$$

hence $\mathbf{x}^{(j)} \to \mathbf{x}$ and this shows V to be complete.

If g is any other norm on V, we have to show that this defines the same topology as the norm f. Given $\mathbf{x} = \sum x_i e_i \in V$, we have

$$g(\mathbf{x}) \le \max_{1 \le i \le n} |x_i| \sum_{i=1}^{n} g(e_i) = c_2 f(\mathbf{x})$$

for some $c_2 > 0$ independent of $\mathbf{x}$, so the norm f is finer than the g-topology (i.e. $f(\mathbf{x}^{(j)}) \to 0$ implies $g(\mathbf{x}^{(j)}) \to 0$).

The converse implication takes a lot more proving. We will do it by induction on the dimension of V, noting first that the converse implication is trivial true for spaces of dimension 1. By combining the above proof, this shows that the proposition is true for the case of dimension 1. Thus, we only need to prove the induction step: assume that the proposition is true for spaces of dimension $n - 1$, and show that it is then also true for spaces of dimension n. Let V, then, be a space of dimension n. To prove the proposition, according to the above arguments, it is enough to show the converse implication of the topologies.

Suppose that $\{\mathbf{x}^{(j)}\}$ is a sequence such that $g(\mathbf{x}^{(j)}) \to 0$ but $f(\mathbf{x}^{(j)}) \not\to 0$, so for some i, say $i = 1$, $|x_1^{(j)}| \not\to 0$. By passing to a subsequence we may assume that $|x_1^{(j)}| \ge \varepsilon$ for some $\varepsilon > 0$ and all j. Put

$$\mathbf{y}^{(j)} = \mathbf{x}^{(j)} / x_1^{(j)} = \sum_{i=1}^{n} y_i^{(j)} e_i;$$

then

$$y_1^{(j)} = 1, \; g(\mathbf{y}^{(j)}) \le \varepsilon^{-1} g(\mathbf{x}^{(j)}) \to 0,$$

thus

$$\sum_{i=2}^{n} y_i^{(j)} e_i \to -e_1$$

in the g-topology. Let W be the subspace spanned by $e_2, \ldots, e_n$; it is $(n-1)$-dimensional and so by the induction hypothesis has a unique topology and is complete, hence closed. Therefore W contains e_1, which is a contradiction; it follows that $f(\mathbf{x}^{(j)}) \to 0$ and the g-topology is just the f-topology. □

Let K be an extension of a field κ. We will consider extensions of absolute values on κ to K. An absolute value $|\cdot|_1$ of K is said to be an *extension* of an absolute value $|\cdot|$ of κ if $|x|_1 = |x|$ for each $x \in \kappa$.

Theorem 1.93. *Let κ be a complete field induced by an absolute value. Then any algebraic extension K of κ has at most one extension of the absolute value and it is complete for the induced topology.*

Proof. Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on K that extend the absolute value $|\cdot|$ of κ. We have to show that $|\alpha|_1 = |\alpha|_2$ for all $\alpha \in K$, so on replacing K by $\kappa(\alpha)$ we may take K to be of finite degree over κ. By Proposition 1.92, both absolute values determine the same topology and K is complete in this topology. Hence $|\cdot|_1$ and $|\cdot|_2$ also are two equivalent absolute values. Thus, there exists a positive real number α such that for each $x \in K$, one has $|x|_1 = |x|_2^{\alpha}$, and hence $\alpha = 1$ since $|x|_1 = |x|_2 = |x|$ when $x \in \kappa$, i.e., the two absolute values are the same. □

Theorem 1.93 answers uniqueness of the extended absolute value. However, we also have the following existence of the extended absolute value:

Theorem 1.94. *If κ is a complete field induced by a non-trivial absolute value $|\cdot|$ and K is any finite dimensional separable extension of κ, then there is a unique extension of the absolute value $|\cdot|$ to a absolute value $|\cdot|_1$ of K and it is given by the formula*

$$|x|_1 = |\mathbf{N}_{K/\kappa}(x)|^{1/[K:\kappa]}.$$

Proof. See Janusz [119], Corollary 3.4; Neukirch [202], Chapter II, Theorem 4.8. □

1.9.3 Extensions of valuations

Let c be a real constant with $c > 1$. If v is a valuation on a field κ, then a non-Archimedean absolute value

$$|x|_v = c^{-v(x)}, \ \ x \in \kappa$$

is well defined. Conversely, if $|\cdot|$ is a non-Archimedean absolute value on κ, a valuation $v : \kappa \longrightarrow \mathbb{R} \cup \{+\infty\}$ is defined by

$$v(x) = \begin{cases} -\log_c |x|, & x \in \kappa_*, \\ +\infty, & x = 0, \end{cases}$$

and is named the (*additive*) *valuation associated to the absolute value*, where $\log_c$ is the real logarithm function of base c.

By Lemma 1.87, it follows that two non-Archimedean absolute values on κ are equivalent if and only if the valuations associated to them are equivalent. We may express this relationship in a more precise way by considering equivalence classes of valuations and of non-Archimedean absolute values:

Proposition 1.95. *Let κ be a field. There is a natural one-to-one correspondence between the set of equivalence classes of valuations of κ and the set of equivalence classes of non-Archimedean absolute values of κ.*

We will identify an equivalence class of non-trivial non-Archimedean absolute values on κ with the place of κ, i.e., an element of M_κ^0, which is the equivalence class of valuations associated to the absolute values. To make notation consistent, an equivalence class of non-trivial Archimedean absolute values also is called a *place* of κ. A place is called *non-Archimedean* or *finite* (resp., *Archimedean* or *infinite*) if its absolute value is non-Archimedean (resp., Archimedean). Usually, let M_κ^∞ be all infinite places of κ, and set

$$M_\kappa = M_\kappa^0 \cup M_\kappa^\infty.$$

To ease notation, we frequently write the absolute values corresponding to a place $\mathfrak{p}$ of κ as $|\cdot|_\mathfrak{p}$ or $|\cdot|_v$ if $[v] = \mathfrak{p}$.

Let K be an extension of a field κ. Let v and w be valuations of κ and K respectively. If the absolute value $|\cdot|_w$ of K is an extension of the absolute value $|\cdot|_v$ of κ, we say that w *divides* v (or w *lies over* v) and denote the relation between v and w by $w|v$. We say that v is *p-adic* if it lies over the p-adic absolute value of $\mathbb{Q}$. Obviously, if $w|v$, then $|\cdot|_w$ is also a norm on K as a κ-vector space.

The topology defined by a valuation v of κ is the one defined by the corresponding absolute value. It is obvious that the topology depends only on the equivalence class of v. The completion of κ relative to the topology induced by v is a field which is denoted by κ_v. Obviously, there is a valuation w of κ_v with $w|v$, $w(\kappa_v) = v(\kappa)$. By Proposition 1.26, $\mathcal{O}_{\kappa_v,w}$ is the closure of $\mathcal{O}_{\kappa,v}$ in κ_v satisfying

$$\mathcal{O}_{\kappa,v} = \mathcal{O}_{\kappa_v,w} \cap \kappa.$$

Let $\mathfrak{m}$ and $\mathbf{m}$ be the maximal ideal of the valuation rings $\mathcal{O}_{\kappa,v}$ and $\mathcal{O}_{\kappa_v,w}$, respectively. Then $\mathbf{m}$ is the closure of $\mathfrak{m}$ in κ_v with $\mathfrak{m} = \mathbf{m} \cap \kappa$. Thus there is the canonical isomorphism

$$\mathbb{F}_w(\kappa_v) \cong \mathbb{F}_v(\kappa).$$

Theorem 1.96. *A field κ is Henselian for a valuation v if and only if the valuation v can be uniquely extended to any algebraic extension.*

Proof. Neukirch [202], Chapter II, Theorem 6.6. □

Lemma 1.97. *If K is a purely inseparable extension of a field κ of characteristic p, then every valuation v of κ has exactly one extension to K.*

Proof. Given $x \in K_*$, there exists p^m such that $x^{p^m} = a \in \kappa$. If p^n is also such that $x^{p^n} = b \in \kappa$, with $m > n$, then

$$\left(x^{p^n}\right)^{p^{m-n}} = b^{p^{m-n}} = a;$$

then $p^{m-n}v(b) = v(a)$, and so

$$\frac{v(b)}{p^n} = \frac{v(a)}{p^m}.$$

We define w on K by $w(0) = +\infty$, and

$$w(x) = \frac{v(a)}{p^m}$$

when $x^{p^m} = a \in \kappa$. This is a well-defined mapping satisfying the following properties: if

$$x^{p^m} = a, \quad y^{p^n} = b, \quad m \leq n,$$

then

$$(xy)^{p^n} = a^{p^{n-m}}b,$$

hence

$$w(xy) = \frac{v\big(a^{p^{n-m}}b\big)}{p^n} = \frac{v(a)}{p^m} + \frac{v(b)}{p^n} = w(x) + w(y).$$

Similarly,

$$(x+y)^{p^n} = x^{p^n} + y^{p^n} = a^{p^{n-m}} + b,$$

and so

$$\begin{aligned} w(x+y) &= \frac{1}{p^n}v\big(a^{p^{n-m}} + b\big) \geq \min\left\{\frac{v(a)}{p^m}, \frac{v(b)}{p^n}\right\} \\ &= \min\{w(x), w(y)\}. \end{aligned}$$

This shows that w is a valuation of K, which clearly extends v. Finally, any valuation w' of K extending v must be such that if $x^{p^m} = a$, then $p^m w'(x) = v(a)$, so w' coincides with w. □

Theorem 1.98. *Let K/κ be an algebraic extension field. Than any valuation v on κ has an extension to K.*

Proof. As it is well known, if K be an algebraic extension field of κ, and if S denotes the set of all elements of K which are separable over κ, then S is a field, S/κ is a separable extension, and K/S is a purely inseparable extension. In view of Lemma 1.97 we may assume that K/κ is a separable extension.

First of all, we assume that κ is Henselian for v. Take $\alpha \in K_*$. Let F be any field such that $\alpha \in F$ and F/κ is of finite degree; let

$$P_\alpha(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \kappa[x]$$

be the minimal polynomial of α over κ. Then

$$\mathbf{N}_{F/\kappa}(\alpha) = \{(-1)^n a_n\}^{[F:\kappa(\alpha)]}.$$

Note that if F' is any other field such that $\alpha \in F \subseteq F'$, F'/κ also of finite degree, then also

$$\mathbf{N}_{F'/\kappa}(\alpha) = \{(-1)^n a_n\}^{[F':\kappa(\alpha)]},$$

hence

$$\mathbf{N}_{F'/\kappa}(\alpha)^{1/[F':\kappa]} = \{(-1)^n a_n\}^{1/n} = \mathbf{N}_{F/\kappa}(\alpha)^{1/[F:\kappa]}. \tag{1.34}$$

If F_1 is any field such that $\alpha \in F_1$, F_1/κ of finite degree, let F' be of finite degree and contain both F and F_1; then (1.34) holds also for F_1, F', and therefore (1.34) holds for F, F_1. It follows that

$$\frac{1}{[F_1:\kappa]} v\left(\mathbf{N}_{F_1/\kappa}(\alpha)\right) = \frac{1}{n} v(a_n) = \frac{1}{[F:\kappa]} v\left(\mathbf{N}_{F/\kappa}(\alpha)\right). \tag{1.35}$$

Now we are ready to define the mapping w on K: $w(0) = +\infty$ and if $\alpha \in K_*$, if F is any finite extension of κ such that $\alpha \in F \subseteq K$, we put

$$w(\alpha) = \frac{1}{[F:\kappa]} v\left(\mathbf{N}_{F/\kappa}(\alpha)\right) = \frac{1}{n} v(a_n). \tag{1.36}$$

By (1.35), w is well defined. We now verify that w is a valuation of K, which obviously extends v. Let $\alpha, \beta \in K$, so there exists a finite field extension F/κ such that $\alpha, \beta \in F$, $F \subseteq K$; thus

$$\begin{aligned} w(\alpha\beta) &= \frac{1}{[F:\kappa]} v\left(\mathbf{N}_{F/\kappa}(\alpha\beta)\right) = \frac{1}{[F:\kappa]} v\left(\mathbf{N}_{F/\kappa}(\alpha)\mathbf{N}_{F/\kappa}(\beta)\right) \\ &= \frac{1}{[F:\kappa]} v\left(\mathbf{N}_{F/\kappa}(\alpha)\right) + \frac{1}{[F:\kappa]} v\left(\mathbf{N}_{F/\kappa}(\beta)\right) = w(\alpha) + w(\beta). \end{aligned}$$

To prove that

$$w(\alpha+\beta) \geq \min\{w(\alpha), w(\beta)\},$$

let us assume that $w(\alpha) \leq w(\beta)$; putting $\gamma = \beta\alpha^{-1}$, then $w(\gamma) \geq 0$ and

$$w(\alpha+\beta) = w(\alpha+\alpha\gamma) = w(\alpha) + w(1+\gamma);$$

it will be enough to prove that if $w(\gamma) \geq 0$, then $w(1+\gamma) \geq 0$. Let

$$P_\gamma(x) = x^m + b_1 x^{m-1} + \cdots + b_m \in \kappa[x]$$

be the minimal polynomial of γ over κ, so $P = P_\gamma(x-1)$ is the minimal polynomial of $1+\gamma$ over κ because $P(1+\gamma) = 0$ and P is irreducible; its constant term is

$$P(0) = P_\gamma(-1) = (-1)^m + b_1(-1)^{m-1} + \cdots + b_m,$$

thus $w(\gamma) = v(b_m)/m$, and

$$\begin{aligned} w(1+\gamma) &= \frac{1}{[F:\kappa]} v\left(\mathbf{N}_{F/\kappa}(1+\gamma)\right) = \frac{1}{m} v(P(0)) \\ &= \frac{1}{m} v\left((-1)^m + b_1(-1)^{m-1} + \cdots + b_m\right); \end{aligned}$$

it suffices to show that $v(b_m) \geq 0$ implies $v(b_1) \geq 0, \ldots, v(b_{m-1}) \geq 0$, hence $w(1+\gamma) \geq 0$.

Assume, to the contrary, that

$$\min\{v(b_1), v(b_2), \ldots, v(b_m)\} = \lambda < 0.$$

Let r be the largest index such that $v(b_r) = \lambda$. Then we have $1 \leq r < m$. Consider the polynomial $b_r^{-1} P_\gamma$ which belongs to $\mathcal{O}_{\kappa,v}[x]$. Since

$$v(b_{r+i}) > \lambda, \;\; i = 1, \ldots, m-r,$$

we obtain

$$b_r^{-1} P_\gamma(x) \equiv b_r^{-1} x^m + b_r^{-1} b_1 x^{m-1} + \cdots + x^{m-r} \pmod{\mathbf{m}[x]},$$

where $\mathbf{m}$ is the maximal ideal of $\mathcal{O}_{\kappa,v}$; thus

$$b_r^{-1} P_\gamma(x) \equiv \left(b_r^{-1} x^r + b_r^{-1} b_1 x^{r-1} + \cdots + 1\right) x^{m-r} \pmod{\mathbf{m}[x]}.$$

Since κ is Henselian for v, then $b_r^{-1} P_\gamma$ is reducible and is P_γ, which is contrary to the fact that it is the minimal polynomial of γ. This proves that $\lambda \geq 0$, hence $w(1+\gamma) \geq 0$ and w is a valuation.

Finally, let $(\hat{\kappa}, \hat{v})$ be a completion of (κ, v). By Lemma 1.50, $(\hat{\kappa}, \hat{v})$ is Henselian. Let $K\hat{\kappa}$ denote the *compositum* of K and $\hat{\kappa}$ (the smallest field containing K and $\hat{\kappa}$), which is an algebraic extension of $\hat{\kappa}$. By the first case, $\hat{v}$ has an extension w' to $K\hat{\kappa}$; the restriction w of w' to K is therefore an extension of v. □

Let κ be a field with a valuation v. Let K be an extension of κ, and let w be a valuation of K with $w|v$. Let $\mathfrak{m}$ and $\mathbf{m}$ be the maximal ideal of the valuation rings $\mathcal{O}_{\kappa,v}$ and $\mathcal{O}_{K,w}$, respectively. Obviously,

$$\mathcal{O}_{\kappa,v} = \mathcal{O}_{K,w} \cap \kappa, \quad \mathfrak{m} = \mathbf{m} \cap \kappa = \mathbf{m} \cap \mathcal{O}_{\kappa,v},$$

and therefore

$$\mathbb{F}_v(\kappa) = \mathcal{O}_{\kappa,v}/(\mathcal{O}_{\kappa,v} \cap \mathbf{m}) \cong (\mathcal{O}_{\kappa,v} + \mathbf{m})/\mathbf{m} \subseteq \mathcal{O}_{K,w}/\mathbf{m} = \mathbb{F}_w(K).$$

Thus we may regard the residue class field $\mathbb{F}_w(K)$ as an extension of $\mathbb{F}_v(\kappa)$.

Lemma 1.99. *Let K/κ be an algebraic extension, w an extension of the valuation v from κ to K. Then*

(1) *$w(K_*)$ is a subgroup of the divisible group generated by $v(\kappa_*)$;*

(2) *$\mathbb{F}_w(K)$ is an algebraic extension of $\mathbb{F}_v(\kappa)$;*

(3) *there exists $\alpha \in \mathcal{O}_{K,w}$ satisfying $\mathcal{O}_{K,w} = \mathcal{O}_{\kappa,v}[\alpha]$ if $\mathbb{F}_w(K)/\mathbb{F}_v(\kappa)$ is separable.*

Proof. (1) Take $\alpha \in K_*$. Then α satisfies a relation

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

with $a_i \in \kappa$, $a_0 \neq 0$. Thus

$$w(a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n) = w(0) = +\infty,$$

and hence there exist distinct indices i, j such that

$$w\left(a_i\alpha^{n-i}\right) = w\left(a_j\alpha^{n-j}\right).$$

It follows that

$$w(\alpha) = \frac{v(a_i) - v(a_j)}{i - j},$$

so $w(\alpha)$ belongs to the divisible group generated by $v(\kappa_*)$.

(2) Let $\varphi : \mathcal{O}_{K,w} \longrightarrow \mathbb{F}_w(K)$ be the natural homomorphism; its restriction to $\mathcal{O}_{\kappa,v}$ maps it onto $\mathbb{F}_v(\kappa)$. If $\beta \in \mathbb{F}_w(K)$, $\beta \neq 0$, let $x \in \mathcal{O}_{K,w}$ be such that $\varphi(x) = \beta$. Since x is algebraic over κ, it satisfies a relation

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

with $a_i \in \kappa$, $a_0 \neq 0$. Let $a \in \kappa$ be such that

$$v(a) = -\min_{0\leq i\leq n} v(a_i).$$

Hence $aa_i \in \mathcal{O}_{\kappa,v}$ for every index i, and there exists j such that $v(aa_j) = 0$, so $aa_j \notin \mathfrak{m}$. Therefore, the elements

$$b_i = \varphi(aa_i) \in \mathbb{F}_v(\kappa), \;\; i = 0, \ldots, n$$

satisfy a relation

$$b_0\beta^n + b_1\beta^{n-1} + \cdots + b_n = 0$$

with $b_j \neq 0$. Hence β is algebraic over $\mathbb{F}_v(\kappa)$.

(3) see Neukirch [202], Chapter II, Lemma 10.4. □

From (1) of Lemma 1.99, it follows that if v is the trivial valuation of κ and K/κ is an algebraic extension, then the only extension of v to K is the trivial valuation since the divisible subgroup generated by $\{0\}$ is $\{0\}$. We may use this fact to derive easily that a field κ has only the trivial valuation if and only if κ has positive characteristic p and it is algebraic over $\mathbb{F}_p$. In every other case, κ has at least two nonequivalent nontrivial valuations (cf. [215], Section 4.1).

Lemma 1.100. *Let K/κ be a field extension, w an extension of the valuation v from κ to K. Suppose $\beta_1, \ldots, \beta_m \in \mathbb{F}_w(K)$ are linearly independent over $\mathbb{F}_v(\kappa)$ and $x_1, \ldots, x_m \in \mathcal{O}_{K,w}$ are elements such that $\varphi(x_i) = \beta_i$ for $i = 1, \ldots, m$. Then*

(a) *for any elements $a_i \in \kappa$,*

$$w\left(\sum_{i=1}^{m} a_i x_i\right) = \min_{1\le i\le m} v(a_i);$$

(b) *$x_1, \ldots, x_m$ are linearly independent over κ.*

Proof. (a) We may assume that all coefficients a_i are nonzero. Let j be an index such that

$$v(a_j) = \min_{1\le i\le m} v(a_i) < \infty.$$

Since $a_j^{-1} a_i \in \mathcal{O}_{K,w}$, then

$$w\left(\sum_{i=1}^{m} a_j^{-1} a_i x_i\right) \ge 0.$$

If the number in above inequality is positive, then

$$\varphi\left(\sum_{i=1}^{m} a_j^{-1} a_i x_i\right) = 0,$$

that is,

$$\sum_{i=1}^{m} \varphi\big(a_j^{-1} a_i\big)\beta_i = 0,\ \varphi\big(a_j^{-1} a_j\big) = \varphi(1) = 1;$$

this contradicts the hypothesis of linear independence of $\beta_1, \ldots, \beta_m$ over $\mathbb{F}_v(\kappa)$. Hence it follows that

$$w\left(\sum_{i=1}^{m} a_j^{-1} a_i x_i\right) = 0,$$

that is

$$w\left(\sum_{i=1}^{m} a_i x_i\right) = v(a_j)$$

as required.

(b) If there exist $a_1, \ldots, a_m \in \kappa$ such that

$$\sum_{i=1}^{m} a_i x_i = 0,$$

then

$$+\infty = w(0) = w\left(\sum_{i=1}^{m} a_i x_i\right) = \min_{1 \le i \le m} v(a_i)$$

and so each a_i is zero. □

Let K/κ be an algebraic extension, let w be a valuation of K and v its restriction to κ. The valuation group $v(\kappa_*)$ of κ is a subgroup of the valuation group $w(K_*)$ of K, whose index $e = e_{K/\kappa}(w)$ is called the *ramification index* of w in the extension K/κ. By the definition, the index is the number of cosets of the subgroup $v(\kappa_*)$ in $w(K_*)$. The extension w is said to be *ramified* if its ramification index > 1, *unramified* otherwise. The degree of $\mathbb{F}_w(K)$ over $\mathbb{F}_v(\kappa)$, i.e. the dimension of $\mathbb{F}_w(K)$ as $\mathbb{F}_v(\kappa)$-space:

$$f = f_{K/\kappa}(w) = [\mathbb{F}_w(K) : \mathbb{F}_v(\kappa)]$$

is called the *residue class degree* (or *inertial degree*) of w in the extension K/κ. It is clear that under repeated extensions, f and e are all multiplicative. Thus if $\kappa \subseteq K \subseteq L$, then

$$f_{L/\kappa}(u) = f_{L/K}(u) f_{K/\kappa}(w), \quad e_{L/\kappa}(u) = e_{L/K}(u) e_{K/\kappa}(w),$$

where u is a valuation of L and w is its restriction to K.

Theorem 1.101. *Let K/κ be an extension of valuated fields with ramification index e and residue class degree f, where the valuation w of K extends that of κ, v say. If K/κ is finite, then*

$$ef \le [K : \kappa], \tag{1.37}$$

and if v is discrete, then so is w. If v is discrete and κ is complete, then equality holds in (1.37).

Proof. See [33], Theorem 1.1 in Chapter 2; or [144]. Here we introduce a proof in [215]. Let $\beta_1, \ldots, \beta_m \in \mathbb{F}_w(K)$ are linearly independent over $\mathbb{F}_v(\kappa)$. Let $t_1, \ldots, t_r \in K$ be elements such that the cosets

$$w(t_1) + v(\kappa_*), \ldots, w(t_r) + v(\kappa_*)$$

are distinct. Let $x_1, \ldots, x_m \in \mathcal{O}_{K,w}$ be elements having images $\beta_1, \ldots, \beta_m$ in $\mathbb{F}_w(K)$. We will show that

$$\{x_i t_j \mid i = 1, \ldots, m;\ j = 1, \ldots, r\}$$

is a linearly independent set over κ, and therefore $mr \leq [K : \kappa]$. Since m, r are arbitrary positive integers such that

$$m \leq f_{K/\kappa}(w) = f, \quad r \leq e_{K/\kappa}(w) = e,$$

then (1.37) will hold.

To prove the linear independence of the elements $x_i t_j$, let

$$\sum_{i=1}^{m} \sum_{j=1}^{r} a_{ij} x_i t_j = 0.$$

In particular, if

$$\sum_{i=1}^{m} a_{ij} x_i = 0, \ \ j = 1, \ldots, r,$$

then by Lemma 1.100 we have $a_{ij} = 0$ for all indices i, j. If there exists an index j such that

$$\sum_{i=1}^{m} a_{ij} x_i \neq 0,$$

noting that

$$+\infty = w(0) = w\left(\sum_{i=1}^{m} \sum_{j=1}^{r} a_{ij} x_i t_j \right),$$

there must exist two distinct indices j, k such that

$$w\left(\sum_{i=1}^{m} a_{ij} x_i \right) + w(t_j) = w\left(\sum_{i=1}^{m} a_{ik} x_i \right) + w(t_k);$$

by Lemma 1.100,

$$\begin{aligned} w\left(\sum_{i=1}^{m} a_{ij} x_i \right) &= \min_{1 \leq i \leq m} v(a_{ij}) \in v(\kappa_*), \\ w\left(\sum_{i=1}^{m} a_{ik} x_i \right) &= \min_{1 \leq i \leq m} v(a_{ik}) \in v(\kappa_*), \end{aligned}$$

hence

$$w(t_j) + v(\kappa_*) = w(t_k) + v(\kappa_*),$$

which is contrary to the choice of the elements $t_1, \ldots, t_r$. Therefore, this case cannot occur, proving our assertion.

Further, if v is discrete, we have $e < \infty$, and hence if $v(\kappa_*) \simeq \mathbb{Z}$, then $w(K_*) \simeq \frac{1}{e}\mathbb{Z}$, so w is discrete.

Here we omit the proof of the equality in (1.37) when κ is complete. For more detail, see [215], Section 6.1, Theorem 1. □

Any algebraic extension K/κ can be written as a union of finite extensions, and applying Theorem 1.101 to these extensions we obtain the following conditions:

Corollary 1.102. *If K/κ is an algebraic extension and κ has a valuation v with extension w to K, then $w(K_*)/v(\kappa_*)$ is a torsion group and $\mathbb{F}_w(K)/\mathbb{F}_v(\kappa)$ is algebraic.*

Now we can describe the set of extensions of a valuation.

Theorem 1.103. *Let K/κ be an algebraic extension of finite degree, let v be a valuation of κ, B the integral closure of $\mathcal{O}_{\kappa,v}$ in K.*

(A) *If K/κ is a normal extension, then all the valuations of K extending v are conjugate (i.e., equal to $w \circ \sigma$ for some fixed w extending v and a κ-automorphism of K).*

(B) *There exist only finitely many valuations of K extending v.*

(C) $B = \bigcap_w \mathcal{O}_{K,w}$ *(intersection of all the rings of the valuations of K extending v).*

Proof. (A) Let w be a valuation of K extending v. Obviously, $w \circ \sigma$ is a valuation of K extending v for every κ-automorphism σ of K. Now let w' be any extension of v to K. Since $\mathcal{O}_{K,w'}$ is integrally closed and

$$\mathcal{O}_{\kappa,v} = \mathcal{O}_{K,w'} \cap \kappa,$$

then $\mathcal{O}_{K,w'}$ contains the integral closure of $\mathcal{O}_{\kappa,v}$ in K, which is just

$$B = \bigcap_{\sigma \in G_{K/\kappa}} \mathcal{O}_{K,w\circ\sigma}.$$

In fact, if $x \in B$, it is integral over $\mathcal{O}_{\kappa,v}$, hence also over the larger ring $\mathcal{O}_{K,w\circ\sigma}$; so $x \in \mathcal{O}_{K,w\circ\sigma}$, because this ring is integrally closed. Conversely, if $x \in \mathcal{O}_{K,w\circ\sigma}$ for every $\sigma \in G_{K/\kappa}$, then $w(\sigma(x)) \geq 0$ for every conjugate $\sigma(x)$ of x, so the minimal polynomial of x over κ has coefficients in $\mathcal{O}_{K,w} \cap \kappa = \mathcal{O}_{\kappa,v}$, showing that x is integral over $\mathcal{O}_{\kappa,v}$.

Since $G_{K/\kappa}$ is finite, say, $G_{K/\kappa} = \{\sigma_1, \ldots, \sigma_n\}$, we may assume that $w \circ \sigma_1, \ldots, w \circ \sigma_n$ are pairwise inequivalent. If $w' \neq w \circ \sigma_i$ for every $i = 1, \ldots, n$, then there exists $x \in K$ such that

$$w'(x) < 0, \quad w(\sigma_i(x)) \geq 0 \ \ (1 \leq i \leq n);$$

this is however contrary to the fact

$$\mathcal{O}_{K,w'} \supseteq \bigcap_{i=1}^{n} \mathcal{O}_{K,w\circ\sigma_i}.$$

(B) This is obvious when K/κ is a normal extension since $G_{K/\kappa}$ is finite. Generally, if L is the smallest normal extension of κ containing K, noting that $[L : \kappa] < \infty$, then

v has only finitely many extensions to L. Since every valuation of K may be extended to L, then v has only finitely many extensions to K.

(C) If K/κ is a normal extension, it follows from (A) and its proof. In general, let L be as above and let C be the integral closure of $\mathcal{O}_{\kappa,v}$ in L. Thus

$$C = \bigcap_u \mathcal{O}_{L,u}$$

for all extensions u of v to L. Since $C \cap K = B$, and all valuations of K may be extended to L, then

$$B = C \cap K = \bigcap_u (\mathcal{O}_{L,u} \cap K) = \bigcap_w \mathcal{O}_{K,w}$$

for all extensions w of v to K. □

Let $(\kappa_v, \hat{v})$ be the completion of κ with respect to a valuation v, where $\hat{v}|v$. Let $\bar{\kappa}_v$ be an algebraic closure of κ_v and let $\bar{v}$ be the unique extension of $\hat{v}$ to $\bar{\kappa}_v$.

Corollary 1.104. *Let K/κ be an algebraic extension of finite degree, and let v be a valuation of κ. If w is any extension of v to K, there exists a κ-embedding $\sigma : K \longrightarrow \bar{\kappa}_v$ such that $w = \bar{v} \circ \sigma$. Thus the number of extensions of v to K is at most equal to $[K : \kappa]$.*

Proof. We assume first that K is a normal extension of κ, let $\rho : K \longrightarrow \bar{\kappa}_v$ be a κ-isomorphism. Then $\bar{v} \circ \rho$ is a valuation of K. By Theorem 1.103, all other valuations of K are conjugate to $\bar{v} \circ \rho$, that is, of type $\bar{v} \circ \rho \circ \tau$, where τ is a κ-automorphism of K.

Generally, let L be the smallest normal extension of κ containing K. If w is any valuation of v to K, let u be any extension of w to L and let $\rho : L \longrightarrow \bar{\kappa}_v$ be a κ-isomorphism. By the above arguments, $u = \bar{v} \circ \rho \circ \tau$, for some κ-automorphism τ of L. Let σ be the restriction of $\rho \circ \tau$ to K, hence $\sigma(K) \subseteq \rho(L)$. It follows that

$$w = u|_K = (\bar{v} \circ \rho \circ \tau)|_K = \bar{v} \circ \sigma.$$ □

Let v be a valuation of κ which is extended uniquely to a valuation w of K. A finite extension K/κ is called *unramified* if the extension $\mathbb{F}_w(K)/\mathbb{F}_v(\kappa)$ of the residue class field is separable and one has

$$[\mathbb{F}_w(K) : \mathbb{F}_v(\kappa)] = [K : \kappa].$$

An algebraic extension K/κ is called *unramified* if it is a union of finite unramified subextensions. If K/κ is an algebraic extension, then the composite T/κ of all unramified subextensions is called the *maximal unramified* subextension. If $T = \kappa$, the extension K/κ is called *totally* (or *purely*) *ramified*.

Proposition 1.105. *The residue class field of T is the separable closure of $\mathbb{F}_v(\kappa)$ in the residue class field extension $\mathbb{F}_w(K)/\mathbb{F}_v(\kappa)$ of K/κ, whereas the valuation group of T equals that of κ.*

Proof. Neukirch [202], Chapter II, Proposition 7.5. □

If the characteristic $p = \mathrm{char}(\mathbb{F}_v(\kappa))$ is positive, then one has the following weaker notion accompanying that of an unramified extension. An algebraic extension K/κ is called *tamely ramified* if the extension $\mathbb{F}_w(K)/\mathbb{F}_v(\kappa)$ of the residue class fields is separable and one has $([K : T], p) = 1$. In the infinite case this latter condition is taken to mean that the degree of each finite subextension of K/T is prime to p. When the fundamental identity

$$e_{K/\kappa}(w) f_{K/\kappa}(w) = [K : \kappa] \tag{1.38}$$

holds and $\mathbb{F}_w(K)/\mathbb{F}_v(\kappa)$ is separable, to say that the extension is unramified, resp. tamely ramified, simply amounts to saying that $e_{K/\kappa}(w) = 1$, resp. $(e_{K/\kappa}(w), p) = 1$. However, the fundamental identity (1.38) always holds when a finite extension K/κ is tamely ramified (cf. [202], Chapter II, Proposition 7.7).

Note that the composite of tamely ramified extensions is tamely ramified. If K/κ is an algebraic extension, then the composite V/κ of all tamely ramified subextensions is called the *maximal tamely ramified* subextension. The extension K/κ is called *wildly ramified* if it is not tamely ramified, i.e., if $V \neq K$.

1.10 Divisor groups

1.10.1 Valuation properties of Dedekind domains

Let κ be a field with a family S of discrete valuations defined on it. We will assume that S satisfies the strong approximation property. We may as well take the members of S to be non-trivial and pairwise inequivalent, thus the members of S are places of κ. We shall denote the members of S by small letters: $v, w, \ldots$ and write $\mathrm{ord}_v, \mathrm{ord}_w$ for the corresponding normalized valuations. With each $v \in S$ we associate its valuation ring

$$\mathcal{O}_{\kappa,v} = \{x \in \kappa \mid \mathrm{ord}_v(x) \geq 0\},$$

and we set the *ring of integers* (with respect to S)

$$A = \bigcap_{v \in S} \mathcal{O}_{\kappa,v}. \tag{1.39}$$

It follows that divisibility relative to A is described by the rule $x|y$ if and only if $\mathrm{ord}_v(x) \leq \mathrm{ord}_v(y)$ for all $v \in S$. An element x of κ is said to be *integral at* v if $\mathrm{ord}_v(x) \geq 0$.

Theorem 1.106. *Let κ be a field with a set S of valuations satisfying the strong approximation property. Then for any distinct $v_1, \dots, v_n \in S$, any $a_1, \dots, a_n \in \kappa$ and any $N > 0$ there exists $a \in \kappa$ such that*

$$\mathrm{ord}_{v_i}(a - a_i) > N, \;\; i = 1, 2, \dots, n, \tag{1.40}$$

$$\mathrm{ord}_w(a) \geq 0, \;\; w \in S - \{v_1, \dots, v_n\}. \tag{1.41}$$

Proof. When S is finite, this is essentially Theorem 1.88 and there is nothing more to prove; so we may take S to be infinite and we may also assume that

$$\mathrm{ord}_w(a_i) \geq 0, \;\; w \neq v_1, \dots, v_n.$$

For this can only fail to hold at finitely many w, which we can add to $v_1, \dots, v_n$, putting the corresponding a_i equal to 0. We may also assume, without loss of generality, that $n > 1$. Let M be a positive constant; our aim is to construct b_1 integral such that

$$\mathrm{ord}_{v_1}(b_1 - 1) > M; \quad \mathrm{ord}_{v_i}(b_1) > M, \;\; i = 2, \dots, n. \tag{1.42}$$

By $\langle 3 \rangle$ in Subsection 1.3.3, for each $i = 2, \dots, n$ there exists c_i integral at all $w \neq v_1, v_i$ (i.e., $\mathrm{ord}_w(c_i) \geq 0$) such that

$$\mathrm{ord}_{v_1}(c_i - 1) > M; \quad \mathrm{ord}_{v_i}(c_i) > M.$$

Since $M > 0$, c_i is also integral at v_1, v_i and so $c_i \in A$. Putting $b_1 = c_2 \cdots c_n$, we have $b_1 \in A$ and

$$\mathrm{ord}_{v_i}(b_1) = \sum_{j=2}^{n} \mathrm{ord}_{v_i}(c_j) > M.$$

Further, we have

$$b_1 - 1 = (c_2 - 1)c_3 \cdots c_n + (c_3 - 1)c_4 \cdots c_n + \cdots + c_n - 1,$$

hence

$$\mathrm{ord}_{v_1}(b_1 - 1) \geq \min\{\mathrm{ord}_{v_1}(c_2 - 1), \dots, \mathrm{ord}_{v_1}(c_n - 1)\} > M.$$

Thus b_1 satisfying (1.42) has been found. If we define $b_2, \dots, b_n$ similarly and then put $a = \sum a_i b_i$, we find that

$$\mathrm{ord}_{v_1}(a - a_1) = \mathrm{ord}_{v_1}\Big(a_1(b_1 - 1) + \sum_{i=2}^{n} a_i b_i\Big) \geq \min_i\{\mathrm{ord}_{v_1}(a_i) + M\},$$

and it follows that $\mathrm{ord}_{v_1}(a - a_1) > N$, provided we choose M to satisfy

$$M > N - \min_i\{\mathrm{ord}_{v_1}(a_i)\}.$$

Similarly $\mathrm{ord}_{v_i}(a - a_i) > N$ and for $w \neq v_i$,

$$\mathrm{ord}_w(a) \geq \min\{\mathrm{ord}_w(a_i) + \mathrm{ord}_w(b_i)\} \geq 0,$$

so a satisfies all the conditions. □

Corollary 1.107. *Let κ be a field and S a family of places with the strong approximation property. Given any finite subset $\{v_1, \dots, v_n\}$ of S and any rational integers $\alpha_1, \dots, \alpha_n$, there exists $a \in \kappa$ such that*

$$\begin{aligned} &\mathrm{ord}_{v_i}(a) = \alpha_i, \;\; i = 1, \dots, n; \\ &\mathrm{ord}_w(a) \geq 0, \;\; w \in S - \{v_1, \dots, v_n\}. \end{aligned} \tag{1.43}$$

Proof. Let $a_i \in \kappa$ be such that

$$\mathrm{ord}_{v_i}(a_i) = \alpha_i, \;\; i = 1, \dots, n;$$

such a_i exists because ord_{v_i} is normalized. By Theorem 1.106, there exists $a \in \kappa$ such that

$$\mathrm{ord}_{v_i}(a - a_i) > \alpha_i; \quad \mathrm{ord}_w(a) \geq 0, \;\; w \in S - \{v_1, \dots, v_n\}.$$

Hence

$$\mathrm{ord}_{v_i}(a) \geq \min\{\mathrm{ord}_{v_i}(a_i), \mathrm{ord}_{v_i}(a - a_i)\},$$

and here equality holds; thus (1.43) is satisfied. □

We define the *divisor group* $\mathcal{D}_\kappa$ of κ with respect of S as the free Abelian group on S as generating set. The typical element is written:

$$D = \prod_{v \in S} v^{\alpha_v},$$

where the α_v are integers, almost all zero, and D is called a *divisor*. If $\alpha_v \geq 0$ for all $v \in S$, then D is said to be an *integral divisor*. Denote the set of all nonzero fractional ideals of A by $\mathfrak{I}_\kappa$. Our aim will be to explore the relations between $\mathcal{D}_\kappa$ and $\mathfrak{I}_\kappa$.

For any $\mathfrak{g} \in \mathfrak{I}_\kappa$ we put

$$\mathrm{ord}_v(\mathfrak{g}) = \min\{\mathrm{ord}_v(x) \mid x \in \mathfrak{g}\}. \tag{1.44}$$

Since there exists $\omega \in A - \{0\}$ such that $\omega\mathfrak{g} \subseteq A$, we have $\mathrm{ord}_v(x) \geq -\mathrm{ord}_v(\omega)$ for all $x \in \mathfrak{g}$, and so $\mathrm{ord}_v(\mathfrak{g})$ is well defined. On another hand, there are $a \in \mathfrak{g}$, $b \in \mathfrak{g}^{-1}$ such that $ab = 1$, hence

$$-\mathrm{ord}_v(\omega) \leq \mathrm{ord}_v(\mathfrak{g}) \leq \mathrm{ord}_v(a) = -\mathrm{ord}_v(b)$$

for all v. This shows that $\mathrm{ord}_v(\mathfrak{g}) = 0$ for almost all v.

The mapping $\mathrm{ord}_v : \mathfrak{I}_\kappa \longrightarrow \mathbb{Z}$ is a homomorphism. For if $c \in \mathfrak{gh}$, say,

$$c = \sum a_i b_i, \;\; a_i \in \mathfrak{g}, \;\; b_i \in \mathfrak{h},$$

then

$$\mathrm{ord}_v(c) \geq \min_i\{\mathrm{ord}_v(a_i) + \mathrm{ord}_v(b_i)\} \geq \mathrm{ord}_v(\mathfrak{g}) + \mathrm{ord}_v(\mathfrak{h}).$$

Therefore

$$\mathrm{ord}_v(\mathfrak{gh}) \geq \mathrm{ord}_v(\mathfrak{g}) + \mathrm{ord}_v(\mathfrak{h}),$$

and here equality holds, as we see by taking $c = ab$, where a, b are chosen in $\mathfrak{g}, \mathfrak{h}$ so as to attain the minimum in (1.44). Hence

$$\mathrm{ord}_v(\mathfrak{gh}) = \mathrm{ord}_v(\mathfrak{g}) + \mathrm{ord}_v(\mathfrak{h}),$$

and it follows that (1.44) is a homomorphism. Further, we obtain a homomorphism $\phi : \mathfrak{I}_\kappa \longrightarrow \mathcal{D}_\kappa$ defined

$$\phi(\mathfrak{g}) = \prod_{v \in S} v^{\mathrm{ord}_v(\mathfrak{g})}. \tag{1.45}$$

In this homomorphism, integral ideals correspond to integral divisors.

Lemma 1.108. *Let κ be a field and S a family of places with the strong approximation property, and let A be the associated ring of integers. Given a fractional ideal $\mathfrak{g}$ in κ, if $\mathrm{ord}_v(\mathfrak{g})$ is defined by* (1.44)*, then for all $x \in \kappa$, $x \in \mathfrak{g}$ if and only if $\mathrm{ord}_v(x) \geq \mathrm{ord}_v(\mathfrak{g})$ for all $v \in S$.*

Proof. By definition, $\mathrm{ord}_v(x) \geq \mathrm{ord}_v(\mathfrak{g})$ for all $v \in S$ if $x \in \mathfrak{g}$. Conversely, let us fix x in κ and replace $\mathfrak{g}$ by $x^{-1}\mathfrak{g}$; then we have to show $1 \in \mathfrak{g}$ if $\mathrm{ord}_v(\mathfrak{g}) \leq 0$. If we replace $\mathfrak{g}$ by $\mathfrak{g} \cap A$, then $\mathfrak{g} \subseteq A$ and the hypothesis becomes $\mathrm{ord}_v(\mathfrak{g}) = 0$. Take $c \in \mathfrak{g} - \{0\}$; if c is a unit, then $1 = cc^{-1} \in \mathfrak{g}$. Otherewise $\mathrm{ord}_v(c) \neq 0$ for only finitely many places, say $v = v_1, \ldots, v_n$. Let us take $a_i \in \mathfrak{g}$ such that $\mathrm{ord}_{v_i}(a_i) = 0$. Now fix j with $1 \leq j \leq n$, and by Theorem 1.106 choose $b_j \in \kappa$ such that

$$\mathrm{ord}_{v_j}\left(a_j^{-1} - b_j\right) \geq \mathrm{ord}_{v_j}(c); \quad \mathrm{ord}_w(b_j) \geq \mathrm{ord}_w(c), \;\; w \neq v_1, \ldots, v_n.$$

Since $\mathrm{ord}_w(c) = 0$ at almost all places, this is possible, and in fact $b_j \in A$ because $c \in A$ and $\mathrm{ord}_{v_j}(a_j) = 0$. If we carry out this construction for $j = 1, \ldots, n$ and put $a = \sum a_i b_i$, we find that $a \in \mathfrak{g}$, because $a_i \in \mathfrak{g}$ and $b_i \in A$. Further, by the choice of b_i we have

$$\mathrm{ord}_{v_j}(1 - a) = \mathrm{ord}_{v_j}\Big(1 - a_j b_j - \sum_{i \neq j} a_i b_i\Big) \geq \mathrm{ord}_{v_j}(c), \;\; j = 1, \ldots, n,$$

and $1 - a \in A$, so for $w \neq v_1, \ldots, v_n$,

$$\mathrm{ord}_w(1 - a) \geq 0 = \mathrm{ord}_w(c).$$

Hence $c^{-1}(1 - a) = d \in A$ and $1 = a + cd \in \mathfrak{g}$, as claimed. □

The theorem which follows is important because it establishes the link between the valuations and the ideals of A. In the case where A is the ring of algebraic integers of an algebraic number field κ, the theorem is due to Dedekind.

Theorem 1.109. *Let κ be a field and S a family of places with the strong approximation property, and let A be the ring of integers. The mapping ϕ from the fractional ideals to the divisors is an isomorphism, and so the nonzero fractional ideals form a group. In this isomorphism, a fractional ideal corresponds to a place v in S if and only if the ideal, say $\mathfrak{p}$, is a nonzero prime ideal, and in this case $\mathfrak{p} = A \cap \mathbf{m}_{\kappa,v}$, while $A_{\mathfrak{p}} = \mathcal{O}_{\kappa,v}$.*

Proof. In order to show ϕ is an isomorphism we shall define a mapping $\Phi : \mathcal{D}_\kappa \longrightarrow \mathfrak{I}_\kappa$ which will turn out to be the inver of ϕ. It is defined by the rule, if

$$D = \prod_{v \in S} v^{\alpha_v} \in \mathcal{D}_\kappa,$$

then

$$\Phi(D) = \{x \in \kappa \mid \mathrm{ord}_v(x) \geq \alpha_v,\ v \in S\}.$$

If $x, y \in \Phi(D)$, $a \in A$, then for $v \in S$,

$$\mathrm{ord}_v(x+y) \geq \min\{\mathrm{ord}_v(x), \mathrm{ord}_v(y)\} \geq \alpha_v$$

and

$$\mathrm{ord}_v(ax) = \mathrm{ord}_v(a) + \mathrm{ord}_v(x) \geq \mathrm{ord}_v(x) \geq \alpha_v,$$

hence $x + y, ax \in \Phi(D)$, showing that $\Phi(D)$ is an A-module contained in κ.

To show that it is a fractional ideal, let $v_1, \ldots, v_r$ be the places for which $\alpha_v \neq 0$, take $\omega \in \kappa$ such that

$$\mathrm{ord}_v(\omega) = -\alpha_v,\ \ v \in \{v_1, \ldots, v_r\}; \quad \mathrm{ord}_w(\omega) \geq 0,\ \ w \notin \{v_1, \ldots, v_r\}.$$

Then it is clear that $\omega\Phi(D) \subseteq A$; this shows $\Phi(D)$ to be a fractional ideal.

Now it is clear from the definition that for any fractional ideal $\mathfrak{g}$ we have $\Phi(\phi(\mathfrak{g})) \supseteq \mathfrak{g}$ and by Lemma 1.108 equality holds, so that $\Phi(\phi(\mathfrak{g})) = \mathfrak{g}$.

Next, if $D = \prod v^{\alpha_v} \in \mathcal{D}_\kappa$ and $\Phi(D) = \mathfrak{g}$, then by Corollary 1.107, for any fixed $v \in S$ we can find $x \in \mathfrak{g}$ such that $\mathrm{ord}_v(x) = \alpha_v$. It follows that $\mathrm{ord}_v(\mathfrak{g}) = \alpha_v$ and so $\phi(\Phi(D)) = D$. Thus ϕ has the inverse Φ and hence is an isomorphism; in particular, it follows that $\mathfrak{I}_\kappa$ is a group.

Let $\mathfrak{p}$ be a nonzero prime ideal of A. By the definition, we have

$$\phi(\mathfrak{p}) = \prod_{v \in S} v^{\mathrm{ord}_v(\mathfrak{p})}.$$

Let $v_1, \ldots, v_r \in S$ be those valuations such that $\mathrm{ord}_{v_i}(\mathfrak{p}) \neq 0$. Since $\phi(\mathfrak{p})$ is integral, then

$$\mathrm{ord}_{v_i}(\mathfrak{p}) > 0,\ \ i = 1, \ldots, r.$$

Let us assume that $r \geq 2$. By Corollary 1.107, there exist elements a_1, $a_2 \in \kappa$ such

that

$$\mathrm{ord}_{v_1}(a_1) = \mathrm{ord}_{v_1}(\mathfrak{p}); \quad \mathrm{ord}_{v_2}(a_1) = 0;$$
$$\mathrm{ord}_w(a_1) \geq \mathrm{ord}_w(\mathfrak{p}), \ \ w \in S - \{v_1, v_2\},$$

and similarly,

$$\mathrm{ord}_{v_1}(a_2) = 0; \quad \mathrm{ord}_{v_2}(a_2) = \mathrm{ord}_{v_2}(\mathfrak{p});$$
$$\mathrm{ord}_w(a_2) \geq \mathrm{ord}_w(\mathfrak{p}), \ \ w \in S - \{v_1, v_2\}.$$

Thus $a_1, a_2 \in A - \mathfrak{p}$, however $a_1 a_2 \in \mathfrak{p}$ since $\mathrm{ord}_v(a_1 a_2) \geq \mathrm{ord}_v(\mathfrak{p})$ for all $v \in S$. This is impossible since $\mathfrak{p}$ is a prime ideal, and so $r = 1$. Now we show that $\mathrm{ord}_{v_1}(\mathfrak{p}) = 1$, for if $\mathrm{ord}_{v_1}(\mathfrak{p}) > 1$, by Corollary 1.107, there exists an element $a \in \kappa$ such that

$$\mathrm{ord}_{v_1}(a) = \mathrm{ord}_{v_1}(\mathfrak{p}) - 1; \quad \mathrm{ord}_w(a) \geq 0, \ \ w \in S - \{v_1\},$$

thus $a \in A - \mathfrak{p}$, but $a^2 \in \mathfrak{p}$, which is again impossible. We have shown that if $\mathfrak{p}$ is a prime ideal, then $\phi(\mathfrak{p}) \in S$.

Conversely, if $v \in S$, then $\mathfrak{p} = \phi^{-1}(v)$ is a prime ideal. In fact, take $a, b \in A - \mathfrak{p}$, hence necessarily

$$\mathrm{ord}_v(a) = \mathrm{ord}_v(b) = 0$$

and so $\mathrm{ord}_v(ab) = 0$, proving that $ab \notin \mathfrak{p}$ and $\mathfrak{p}$ is a prime ideal.

From $\phi(\mathfrak{p}) = v$, we deduce that

$$\mathfrak{p} = A \cap \mathbf{m}_{\kappa,v}.$$

Similarly,

$$\mathcal{O}_{\kappa,v} = A_{\mathfrak{p}} = \left\{ \frac{a}{b} \mid a, b \in A, \ b \notin \mathfrak{p} \right\}.$$

In fact, if $x \in \mathcal{O}_{\kappa,v}$, we may write $x = c/d$, with $c, d \in A$. Further, if $\mathrm{ord}_v(d) > 0$, let $b \in \kappa$ be such that $\mathrm{ord}_v(b) = -\mathrm{ord}_v(d)$, $\mathrm{ord}_w(b) \geq 0$ for every other place $w \in S$, so $x = bc/(bd)$ with $bd \in A$, $bd \notin \mathfrak{p}$, and $bc \in A$ because

$$\mathrm{ord}_v(bc) = \mathrm{ord}_v(bc) - \mathrm{ord}_v(bd) = \mathrm{ord}_v(x) \geq 0,$$

and $\mathrm{ord}_w(bc) \geq 0$ for every other place $w \in S$. Conversely, if $x = a/b$ with $a, b \in A$, $b \notin \mathfrak{p}$, then

$$\mathrm{ord}_v(a) \geq 0, \quad \mathrm{ord}_v(b) = 0,$$

so $x \in \mathcal{O}_{\kappa,v}$. □

Let A be a Dedekind domain, κ its field of fractions. By Theorem 1.40, A can be defined as the intersection of discrete valuation rings for a family S of places on κ with the strong approximation property. We also have a homomorphism $\theta = \theta_\kappa$ of κ_* into the divisor group $\mathcal{D}_\kappa$ of κ given by

$$\theta(x) = \prod v^{\mathrm{ord}_v(x)}. \tag{1.46}$$

The kernel $\mathrm{Ker}(\theta)$ of θ is the set of all $x \in \kappa_*$ such that $\mathrm{ord}_v(x) = 0$ for all $v \in S$, so that it is the *group of units* of A, because the mapping from the fractional ideals to the divisors is an isomorphism, by Theorem 1.109. The quotient

$$C_\kappa = \mathcal{D}_\kappa / \theta(\kappa_*)$$

can be made into an Abelian group, called *divisor class group* of A (or κ). We have an exact sequence

$$1 \to \mathrm{Ker}(\theta) \to \kappa_* \xrightarrow{\theta} \mathcal{D}_\kappa \to C_\kappa \to 1. \tag{1.47}$$

Corollary 1.110. *Let A be a Dedekind domain, κ its field of fractions. Then every nontrivial valuation of κ is equivalent to a $\mathfrak{p}$-adic valuation for some nonzero prime ideal $\mathfrak{p}$ of A.*

Proof. Since A is a Dedekind domain, by the remark after Proposition 1.41 if $A \subseteq \mathcal{O}_{\kappa,v}$ (v nontrivial), then $\mathcal{O}_{\kappa,v} = A_\mathfrak{p}$ for some nonzero prime ideal $\mathfrak{p}$. It remains to show that $A_\mathfrak{p}$ is the ring of the $\mathfrak{p}$-adic valuation, which we denote temporarily by B. It suffices to show that $A_\mathfrak{p} \subseteq B$, hence $\mathcal{O}_{\kappa,v} = A_\mathfrak{p}$ being a maximal subring of κ (by Theorem 1.32), then $A_\mathfrak{p} = B$. If $x \in A_\mathfrak{p}$, then $x = a/b$ with $a, b \in A$, $b \notin \mathfrak{p}$. Then $\mathfrak{p}$ does not divide Ab and may, or may not, divide Aa. Thus the $\mathfrak{p}$-adic value of x is not negative, that is, $x \in B$, which concludes the proof. □

Lemma 1.111. *Let A be an integral domain and let $\mathfrak{p}$ be a nonzero prime ideal of A.*

(i) *$A_\mathfrak{p}\mathfrak{p}$ is the only maximal ideal of A and for every $e \geq 1$, $A_\mathfrak{p}\mathfrak{p}^e = (A_\mathfrak{p}\mathfrak{p})^e$.*

(ii) *If $\mathfrak{p}$ does not contain an ideal $\mathfrak{a}$, and $e \geq 0$, then $A_\mathfrak{p}(\mathfrak{p}^e\mathfrak{a}) = A_\mathfrak{p}\mathfrak{p}^e$.*

Proof. (i) Take $a/b \in A_\mathfrak{p} - A_\mathfrak{p}\mathfrak{p}$, so $a, b \in A - \mathfrak{p}$. Then $b/a \in A_\mathfrak{p}$. This shows that every element of $A_\mathfrak{p}$ not in $A_\mathfrak{p}\mathfrak{p}$ is a unit, so $A_\mathfrak{p}\mathfrak{p}$ is the only maximal ideal of $A_\mathfrak{p}$. The verification that $A_\mathfrak{p}\mathfrak{p}^e = (A_\mathfrak{p}\mathfrak{p})^e$ is trivial.

(ii) It is obvious that $A_\mathfrak{p}(\mathfrak{p}^e\mathfrak{a}) \subseteq A_\mathfrak{p}\mathfrak{p}^e$. Conversely, take $x = a/b \in A_\mathfrak{p}\mathfrak{p}^e$ with $a \in \mathfrak{p}^e, b \in A - \mathfrak{p}$. By hypothesis, there exists $c \in \mathfrak{a} - \mathfrak{p}$. Thus $x = ac/(bc)$ with $bc \notin \mathfrak{p}$, $ac \in \mathfrak{p}^e\mathfrak{a}$, showing that $x \in A_\mathfrak{p}(\mathfrak{p}^e\mathfrak{a})$. □

Proposition 1.112. *Let $A \subseteq B$ be Dedekind domains with quotient fields κ and K respectively and let $\mathfrak{p}$ be a nonzero prime ideal of A, and let $\mathfrak{P}$ be a prime ideal of B such that $\mathfrak{P} \cap A = \mathfrak{p}$. The ramification index and the relative degree of $\mathfrak{P}$ over $\mathfrak{p}$ are respectively equal to the ramification index and residue class degree of the $\mathfrak{P}$-adic valuation in K/κ.*

Proof. We can write

$$B\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

where $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ are prime ideals of B, and $e_1 \geq 1, \ldots, e_g \geq 1$. By definition, e_1 is the ramification index of $\mathfrak{P}$ in K/κ.

By Lemma 1.111, one has

$$B_{\mathfrak{P}}(B\mathfrak{p}) = B_{\mathfrak{P}}\mathfrak{P}^{e_1} = (B_{\mathfrak{P}}\mathfrak{P})^{e_1},$$

since $\mathfrak{P}_2, \ldots, \mathfrak{P}_g$ are not contained in $\mathfrak{P}$. On the other hand, since the valuation $\mathrm{ord}_{\mathfrak{p}}$ is discrete, the prime ideal of $A_{\mathfrak{p}}$ is principal, so there exists an element t such that $A_{\mathfrak{p}}\mathfrak{p} = A_{\mathfrak{p}}t$. The ramification index of $\mathrm{ord}_{\mathfrak{P}}$ in K/κ is equal to the value of t, that is, $\mathrm{ord}_{\mathfrak{P}}(t) = e$, and this means that $B_{\mathfrak{P}}t = (B_{\mathfrak{P}}\mathfrak{P})^e$. Now,

$$B_{\mathfrak{P}}t = B_{\mathfrak{P}}(A_{\mathfrak{p}}t) = B_{\mathfrak{P}}(A_{\mathfrak{p}}\mathfrak{p}) = B_{\mathfrak{P}}(B\mathfrak{p}) = (B_{\mathfrak{P}}\mathfrak{P})^{e_1}$$

by the above. Hence $e = e_1$.

By definition, the relative degree of $\mathfrak{P}$ over $\mathfrak{p}$ is the degree of $B/\mathfrak{P}$ over $A/\mathfrak{p}$. Similarly, the residue class degree of $\mathrm{ord}_{\mathfrak{P}}$ in K/κ is the degree of the residue class field $\mathbb{F}_{\mathfrak{P}}(K)$ over $\mathbb{F}_{\mathfrak{p}}(\kappa)$. Now

$$\mathbb{F}_{\mathfrak{P}}(K) = B_{\mathfrak{P}}/B_{\mathfrak{P}}\mathfrak{P}, \quad \mathbb{F}_{\mathfrak{p}}(\kappa) = A_{\mathfrak{p}}/A_{\mathfrak{p}}\mathfrak{p}.$$

We will show that $A_{\mathfrak{p}}/A_{\mathfrak{p}}\mathfrak{p} \simeq A/\mathfrak{p}$ and similarly for the other residue field, and this implies the equality between residue class degree and relative degree. The stated isomorphism has been given for the particular case where $A = \mathbb{Z}$ (cf. Example 1.33). The proof in the general case is completely analogous, and may be left to the reader. □

1.10.2 Local degrees in field extensions

Let κ be a field with a nontrivial valuation v. Let $(\kappa_v, \hat{v})$ be the completion of κ with respect to v. Let $\bar{\kappa}_v$ be an algebraic closure of κ_v and let $\bar{v}$ be the unique extension of $\hat{v}$ to $\bar{\kappa}_v$. Let K be a field extension of κ.

First of all, we consider the case that there exists $t \in K$ such that $K = \kappa(t)$. Let P_t be the minimal polynomial of t over κ and let $P_t = h_1 \cdots h_g$ $(g \geq 1)$ be the decomposition of P_t as a product of irreducible polynomials over κ_v. Note that since P_t has no multiple roots, the polynomials $h_1, \ldots, h_g$ are all distinct. By Corollary 1.104, every valuation w of K extending v is of the form $w = \bar{v} \circ \sigma$, where σ is a κ-isomorphism from K into $\bar{\kappa}_v$. We will determine conditions on the κ-isomorphisms ρ, σ of K into $\bar{\kappa}_v$ so that $w_\rho = \bar{v} \circ \rho$ and $w_\sigma = \bar{v} \circ \sigma$ coincide.

Proposition 1.113. *With the above hypotheses and notations, the following conditions are equivalent:*

(1) $w_\rho = w_\sigma$;

(2) *the mapping* $\sigma\rho^{-1} : \kappa(\rho(t)) \longrightarrow \kappa(\sigma(t))$ *is continuous in the topology defined by* $\bar{v}$;

(3) *the fields* $\kappa_v(\rho(t))$, $\kappa_v(\sigma(t))$ *are conjugate over* κ_v *under an extension of* $\sigma\rho^{-1}$*;*

(4) $\rho(t)$, $\sigma(t)$ *are roots of the same factor* h_i.

In particular, $(\kappa_v(\rho(t)), \bar{v})$ *is the completion of* (K, w_ρ).

Proof. (1) $\Rightarrow$ (2) Given $x \in K$, let $\varepsilon > 0$ be a real number and let V_ε be the neighborhood of $\sigma(x)$ consisting of all elements $\sigma(y) \in \sigma(K) = K(\sigma(t))$ such that $\bar{v}(\sigma(y) - \sigma(x)) > \varepsilon$. By hypothesis $w_\rho = w_\sigma$, hence the image by $\sigma\rho^{-1}$ of the neighborhood

$$U_\varepsilon = \{\rho(y) \in \rho(K) \mid \bar{v}(\rho(y) - \rho(x)) > \varepsilon\}$$

of $\rho(x)$ is V_ε. This shows the continuity of $\sigma\rho^{-1}$.

(2) $\Rightarrow$ (3) By hypothesis $\sigma\rho^{-1}$ is a continuous κ-isomorphism of $\kappa(\rho(t))$ to $\kappa(\sigma(t))$. It may be extended naturally to a κ_v-isomorphism of $\kappa_v(\rho(t))$ to $\kappa_v(\sigma(t))$ because κ is dense in κ_v and $\sigma\rho^{-1}$ leaves fixed every element of κ.

(3) $\Rightarrow$ (4) Let Φ be a κ_v-isomorphism from $\kappa_v(\rho(t))$ to $\kappa_v(\sigma(t))$ extending $\sigma\rho^{-1}$. Then $\rho(t)$, $\sigma(t)$ are conjugate over κ_v, and so they are roots of the same irreducible polynomial h_i for some i.

(4) $\Rightarrow$ (1) By hypothesis, there exists a κ_v-automorphism Φ of $\bar{\kappa}_v$ such that $\Phi(\rho(t)) = \Phi(\sigma(t))$. The restriction of Φ to $\rho(K)$ is $\sigma\rho^{-1}$, hence $\Phi(\rho(x)) = \sigma(x)$ for every $x \in K$, which means that $\rho(x)$, $\sigma(x)$ are conjugate over κ_v. Since $\bar{v}$ is the only extension of $\hat{v}$ to $\bar{\kappa}_v$, then $\bar{v} \circ \Phi = \bar{v}$ so

$$w_\rho(x) = (\bar{v} \circ \Phi) \circ \rho(x) = \bar{v}(\sigma(x)) = w_\sigma(x)$$

for every $x \in K$.

In particular, the fields (K, w_ρ) and $(\kappa(\rho(t)), \bar{v})$ are isomorphic. The completion of $(\kappa(\rho(t)), \bar{v})$ must contain $\kappa_v(\rho(t))$. On the other hand, $(\kappa_v(\rho(t)), \bar{v})$ is complete because $\kappa_v(\rho(t))$ is of finite degree over κ_v and $\bar{v}$ extends $\hat{v}$. So $(\kappa_v(\rho(t)), \bar{v})$ is the completion of (K, w_ρ). □

Proposition 1.114. *If* K *is a finite separable extension of* κ*, then*

$$[K : \kappa] = \sum_{w|v} [K_w : \kappa_v].$$

Proof. Since K is separable, there exists $t \in K$ such that $K = \kappa(t)$ (by Theorem 1.70). Using the same notations, we have

$$P_t = h_1 \cdots h_g \ \ (g \geq 1),$$

where $h_1, \ldots, h_g$ are the irreducible factors of P_t over κ_v, and hence

$$\deg(P_t) = \sum_{i=1}^{g} \deg(h_i).$$

By Proposition 1.113, v has g distinct extensions to K, which are of the form $w_\rho = \bar{v} \circ \rho$. In particular, one has

$$[K_{w_\rho} : \kappa_v] = [k_v(\rho(t)) : k_v] = \deg(h_i),$$

where $\rho(t)$ is a root of h_i. Therefore

$$\sum_{w|v} [K_w : \kappa_v] = \sum_{i=1}^{g} \deg(h_i) = \deg(P_t) = [\kappa(t) : \kappa] = [K : \kappa].$$

See [144], or Serre [236], I, Proposition 10 and II, Théorème 1. □

If w is a valuation on K extending v, we shall call $[K_w : \kappa_v]$ the *local degree* in K/κ, which satisfy

$$\sum_{w|v} [K_w : \kappa_v] \leq [K : \kappa].$$

It is immediate that the local degree satisfies the following transitivity relation: if $\kappa \subseteq K \subseteq E$ are fields, E/κ being separable of finite degree, then

$$[E_u : \kappa_v] = [E_u : K_w][K_w : \kappa_v],$$

where u is an extension of w to E.

For any two algebras A, B over a field κ, their *tensor product* $A \otimes_\kappa B$ is defined by the property that the bilinear mappings on $A \times B$ correspond to the linear mappings of $A \otimes_\kappa B$. Explicitly, if A, B have respectively bases $\{u_i\}$, $\{v_j\}$ over κ, then $A \otimes_\kappa B$ has the basis $\{u_i \otimes v_j\}$.

Theorem 1.115. *Let κ be a field with a valuation v and let K/κ be a separable extension of degree n. Then there are at most n extensions of v to K, say $w_1, \ldots, w_g$, where $g \leq n$. If e_i denotes the ramification index and f_i the residue class degree of w_i, then*

$$\sum_{i=1}^{g} e_i f_i \leq n.$$

If v is discrete, the equality holds. If the completion of κ under v is κ_v and that of K under w_i is K_{w_i}, then

$$K \otimes_\kappa \kappa_v \cong K_{w_1} \times \cdots \times K_{w_g}.$$

Proof. By Proposition 1.114, we have

$$n = \sum_{i=1}^{g} [K_{w_i} : \kappa_v].$$

According to the arguments in Subsection 1.9.3, the residue class field and valuation group are unchanged by completion, and hence so are the residue class degree and ramification index. Thus the fundamental inequality follows from Theorem 1.101.

Take $t \in K$ with $K = \kappa(t)$. We select κ-isomorphisms $\rho_1, \ldots, \rho_g$ of K into $\bar{\kappa}_v$ such that

$$w_1 = \bar{v} \circ \rho_1, \ldots, w_g = \bar{v} \circ \rho_g$$

are the distinct extensions of v to K; hence these valuations are pairwise inequivalent. Since a κ-basis $\{y_1, \ldots, y_n\}$ of K gives rise to a κ_v-basis $\{y_1 \otimes 1, \ldots, y_n \otimes 1\}$ of $K \otimes_\kappa \kappa_v$, then $K \otimes_\kappa \kappa_v$ is a κ_v-vector space of dimension $n = [K : \kappa]$. Note that the dimension of the κ_v-vector space $\prod_{i=1}^g K_{w_i}$ is the sum of the local degrees of all the w_i, hence it is also equal to n (by Proposition 1.114).

The mapping

$$K \times \kappa_v \longrightarrow \prod_{i=1}^{g} \rho_i(K) \cdot \kappa_v, \ \ (y, z) \mapsto (\rho_1(y) \cdot z, \ldots, \rho_g(y) \cdot z)$$

is κ-bilinear. Hence it yields a κ-linear mapping

$$\varphi : K \otimes_\kappa \kappa_v \longrightarrow \prod_{i=1}^{g} \rho_i(K) \cdot \kappa_v;$$

namely,

$$\varphi(y \otimes z) = (\rho_1(y) \cdot z, \ldots, \rho_g(y) \cdot z), \ \ y \in K, \ z \in \kappa_v.$$

Further, φ is a homomorphism of κ_v-algebra and its image is dense in $\prod_{i=1}^g \rho_i(K) \cdot \kappa_v$, relative to the product topology. In fact, given any element

$$(x_1, \ldots, x_g) \in \prod_{i=1}^{g} \rho_i(K) \cdot \kappa_v,$$

since $\rho_i(K) \cdot \kappa_v$ is the completion K_{w_i} of (K, w_i), there exists some element

$$(y_1, \ldots, y_g) \in K \times \cdots \times K$$

which is arbitrarily close to $(x_1, \ldots, x_g)$ in the product topology, and by the approximation theorem in K, there exists $y \in K$ arbitrarily close to each element y_i in the topology of w_i.

The image of φ is a finite-dimensional vector space over the complete valued field κ_v, and so the image of φ is also complete. Hence it must be a closed subspace, and by density, it must coincide with $\prod_{i=1}^g \rho_i(K) \cdot \kappa_v$. Since the κ_v-spaces $K \otimes_\kappa \kappa_v$ and $\prod_{i=1}^g \rho_i(K) \cdot \kappa_v$ have the same dimension, φ must be an isomorphism. □

Proposition 1.116. *Let K be a finite separable extension of κ. For every $\alpha \in K$, one has*

$$\mathbf{N}_{K/\kappa}(\alpha) = \prod_{w|v} \mathbf{N}_{K_w/\kappa_v}(\alpha),$$

$$\mathbf{Tr}_{K/\kappa}(\alpha) = \sum_{w|v} \mathbf{Tr}_{K_w/\kappa_v}(\alpha).$$

Proof. Set $n = [K : \kappa]$. We will use the notations in the proof of Theorem 1.115. Let χ_α be the field polynomial of α in K/κ defined by the κ-linear mapping

$$\mathbf{A}_\alpha : K \longrightarrow K, \ \ \mathbf{A}_\alpha(x) = \alpha x.$$

By the theorem of Cayley and Hamilton, $\chi_\alpha(\mathbf{A}_\alpha)$ is the zero linear transformation. The minimal polynomial of $\mathbf{A}_\alpha$ over κ is P_α, defined as being the monic polynomial of smallest degree such that $P_\alpha(\mathbf{A}_\alpha) = 0$; then P_α is irreducible over κ and coincides with the minimal polynomial of α over κ. Moreover χ_α is a power of P_α, that is, $\chi_\alpha = P_\alpha^r$, hence

$$n = \deg(\chi_\alpha) = r \deg(P_\alpha), \quad [K : \kappa] = r[\kappa(\alpha) : \kappa].$$

Write

$$P_\alpha(x) = \prod_\sigma (x - \sigma(\alpha)),$$

where σ runs through the set of κ-isomorphisms of $\kappa(\alpha)$ into $\bar{\kappa}_v$. Noting that each σ has r distinct extensions to κ-isomorphisms of K into $\bar{\kappa}_v$, we have

$$\chi_\alpha(x) = P_\alpha(x)^r = \prod_\sigma (x - \sigma(\alpha))^r = \prod_\rho (x - \rho(\alpha)),$$

where ρ runs through the set of κ-isomorphisms of K into $\bar{\kappa}_v$. A similar argument shows that for each κ-isomorphism ρ of K into $\bar{\kappa}_v$, the field polynomial of $\rho(\alpha)$ in $\rho(K) \cdot \kappa_v/\kappa_v$ is equal to

$$\chi_{\alpha,\rho}(x) = \prod_\tau (x - \tau(\rho(\alpha))),$$

where τ runs through the set of κ_v-isomorphisms of $\rho(K) \cdot \kappa_v$ into $\bar{\kappa}_v$.

We will write $\rho = \sigma$ when $\sigma \circ \rho^{-1}$ leaves κ_v fixed. By Proposition 1.113, the set of κ-isomorphisms of K into $\bar{\kappa}_v$ has exactly g equivalence classes, and $\rho_1, \ldots, \rho_g$ are representatives. The elements in the class of ρ_i are $\tau\rho_i$, where τ runs through the set of all κ_v-isomorphisms of $\rho_i(K) \cdot \kappa_v$ into $\bar{\kappa}_v$. Grouping the roots of χ_α according to the equivalence classes, we have

$$\chi_\alpha = \prod_{i=1}^{g} \chi_{\alpha,\rho_i},$$

where χ_{α,ρ_i} is just the field polynomial of $\rho_i(\alpha)$ in $\rho_i(K)\cdot\kappa_v/\kappa_v$. Note that $\rho_i(K)\cdot\kappa_v$ is the completion K_{w_i} of (K, w_i). From the definition of trace and norm, it follows immediately that the global trace is the sum of local traces, while the global norm is the product of the local norms. □

Let K be a finite separable extension of κ. Let v be a valuation on κ with an extension w to K. By Theorem 1.115, there are only a finite number of w dividing a given place v. Let θ_K be the corresponding mapping defined by (1.46) for K. Then for $w|v$ we have

$$\mathrm{ord}_w(x) = e_{K/\kappa}(w)\mathrm{ord}_v(x),\ \ x \in K,$$

where $e_{K/\kappa}(w)$ is the ramification index for w. Hence for any $x \in K$ we have

$$\theta_K(x) = \prod_w w^{\mathrm{ord}_w(x)} = \prod_v \Big(\prod_{w|v} w^{\mathrm{ord}_w(x)} \Big) = \prod_v \Big(\prod_{w|v} w^{e_{K/\kappa}(w)} \Big)^{\mathrm{ord}_v(x)}.$$

Thus we obtain a commutative diagram $\gamma \circ \theta_\kappa = \theta_K \circ \iota$ as shown below by defining a mapping $\gamma : \mathcal{D}_\kappa \longrightarrow \mathcal{D}_K$,

$$\gamma(v) = \prod_{w|v} w^{e_{K/\kappa}(w)}, \tag{1.48}$$

where $\iota : \kappa \longrightarrow K$ is the inclusion. The mapping (1.48) is an embedding of $\mathcal{D}_\kappa$ in $\mathcal{D}_K$, sometimes called the *conorm mapping*.

Given a place v of κ, let the divisors of v in K be $w_1, \ldots, w_g$ and let $K_{w_1}, \ldots, K_{w_g}$ be the corresponding extensions of κ_v, the completion of κ (cf. Theorem 1.115). As we saw, we have

$$[K_{w_i} : \kappa_v] = n_{w_i} = e(w_i)f(w_i),$$

hence

$$\mathrm{ord}_{w_i}(x) = \frac{1}{n_{w_i}}\mathrm{ord}_{w_i}\big(\mathbf{N}_{K_{w_i}/\kappa_v}(x)\big) = \frac{e(w_i)}{n_{w_i}}\mathrm{ord}_v\big(\mathbf{N}_{K_{w_i}/\kappa_v}(x)\big),$$

and so we obtain

$$\mathrm{ord}_v\left(\mathbf{N}_{K/\kappa}(x)\right) = \sum \mathrm{ord}_v\big(\mathbf{N}_{K_{w_i}/\kappa_v}(x)\big) = \sum f(w_i)\mathrm{ord}_{w_i}(x). \tag{1.49}$$

In the other direction we have the norm mapping. If a valuation v on κ corresponds to a prime divisor $\mathfrak{p}$ and v has an extension w to K, with corresponding prime divisor $\mathfrak{P}$, then we shall write $\mathfrak{P}|\mathfrak{p}$ and say that $\mathfrak{P}$ *divides* $\mathfrak{p}$. The reason for this notation is that in terms of the corresponding fractional ideals we have $\mathfrak{p} \subseteq \mathfrak{P}$. Then γ induces a mapping $\gamma : \mathfrak{I}_\kappa \longrightarrow \mathfrak{I}_K$ such that (1.48) becomes

$$\gamma(\mathfrak{p}) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}/\mathfrak{p}}}. \tag{1.50}$$

Note that

$$\mathbf{N}_{K/\kappa}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}/\mathfrak{p}}}. \tag{1.51}$$

Hence we find that

$$\mathbf{N}_{K/\kappa}(\gamma(\mathfrak{p})) = \mathbf{N}_{K/\kappa}(\mathfrak{P}_1^{e_{\mathfrak{P}_1/\mathfrak{p}}} \cdots \mathfrak{P}_g^{e_{\mathfrak{P}_g/\mathfrak{p}}}) = \mathfrak{p}^{\sum e_{\mathfrak{P}_i/\mathfrak{p}} f_{\mathfrak{P}_i/\mathfrak{p}}} = \mathfrak{p}^{[K:\kappa]},$$

where we have used Theorem 1.115.

1.11 Different

Let K be an algebraic extension of a field κ of degree n. Take $\alpha \in K$ and let $\alpha^{(1)}(= \alpha), \alpha^{(2)}, \ldots, \alpha^{(n)}$ be the conjugates of α with respect to κ. Define the *different of* α *in* K as the element

$$\delta(\alpha) = \prod_{i=2}^{n}(\alpha - \alpha^{(i)}) \in K.$$

If $g(x)$ is the polynomial of degree n with κ-coefficients and leading coefficient 1 which has the n elements $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ as roots, then obviously

$$\delta(\alpha) = g'(\alpha). \tag{1.52}$$

By Proposition 1.55, $\delta(\alpha)$ vanishes if and only if α is a number of lower degree than n. We then find the value

$$\prod_{i>j}(\alpha^{(i)} - \alpha^{(j)})^2 = (-1)^{n(n-1)/2} \prod_{i=1}^{n} g'(\alpha^{(i)}) = (-1)^{n(n-1)/2} \mathbf{N}_{K/\kappa}(\delta(\alpha))$$

for the *discriminant* of the element α.

Let K/κ be a finite separable field extension, $A \subseteq \kappa$ a Dedekind domain with field of fractions κ, and let $B \subseteq K$ be its integral closure in K. Assume that the residue class field extensions of B/A are separable. Associated to every fractional ideal $\mathfrak{B}$ of K, one can define the *dual* B-module

$$\mathfrak{B}^* = \{\lambda \in K \mid \mathbf{Tr}_{K/\kappa}(\lambda x) \in A \text{ for each } x \in \mathfrak{B}\}. \tag{1.53}$$

Theorem 1.117. *Let $\mathfrak{B}$ be a nonzero fractional ideal of B. The dual B-module $\mathfrak{B}^*$ forms a fractional ideal of B. Here $\mathfrak{B}\mathfrak{B}^* = B^*$ is a fractional ideal independent of $\mathfrak{B}$, determined only by the field K, and it is the reciprocal of an integral ideal*

$$\mathfrak{d} = \mathfrak{d}_{B/A} = \mathfrak{d}_{K/\kappa} := \frac{1}{B^*}.$$

Proof. If $w_1, \ldots, w_n \in B$ is a basis of K over κ with its discriminant

$$D = D_{K/\kappa}(w_1, \ldots, w_n) = \det(\mathbf{Tr}_{K/\kappa}(w_i w_j)),$$

then $bD\mathfrak{B}^* \subseteq B$ for every nonzero $b \in \mathfrak{B} \cap A$. Indeed, if

$$\lambda = \xi_1 w_1 + \cdots + \xi_n w_n \in \mathfrak{B}^*, \ \ \xi_i \in \kappa,$$

then the $b\xi_i$ satisfy the system of linear equations

$$\sum_{i=1}^{n} b\xi_i \mathbf{Tr}_{K/\kappa}(w_i w_j) = \mathbf{Tr}_{K/\kappa}(b\lambda w_j) \in A, \ \ j = 1, 2, \ldots, n.$$

This implies $Db\xi_i \in A$ and thus $Db\lambda \in B$.

Moreover, if $\lambda_1, \lambda_2 \in \mathfrak{B}^*$, then for all $b_1, b_2 \in B$; $x \in \mathfrak{B}$,

$$\mathbf{Tr}_{K/\kappa}((b_1\lambda_1 + b_2\lambda_2)x) = \mathbf{Tr}_{K/\kappa}(b_1\lambda_1 x) + \mathbf{Tr}_{K/\kappa}(b_2\lambda_2 x) \in A$$

since $b_1 x, b_2 x \in \mathfrak{B}$; thus $b_1\lambda_1 + b_2\lambda_2 \in \mathfrak{B}^*$, that is, $\mathfrak{B}^*$ is an ideal.

Furthermore, we have $\mathfrak{B}\mathfrak{B}^* = B^*$ which is thus independent of $\mathfrak{B}$ since if $\lambda \in \mathfrak{B}^*$, then for each $x \in B$,

$$\mathbf{Tr}_{K/\kappa}(\lambda w_i x) \in A, \ \ i = 1, 2, \ldots, n,$$

that is, $\lambda w_i \in B^*$, which means $\mathfrak{B}\mathfrak{B}^* \subseteq B^*$. Conversely, if $\mu \in B^*$ and $\rho_1, \ldots, \rho_n$ denotes a basis for $\mathfrak{B}^{-1}$, then $y\rho_i \in B$ for all $y \in \mathfrak{B}$, and hence

$$\mathbf{Tr}_{K/\kappa}(\mu y \rho_i) \in A, \ \ i = 1, 2, \ldots, n,$$

which means $\mu\rho_i \in \mathfrak{B}^*$. Thus $\mu \in \mathfrak{B}\mathfrak{B}^*$, and so $B^* \subseteq \mathfrak{B}\mathfrak{B}^*$.

Moreover B^* is the reciprocal of an integral ideal $\mathfrak{d}$ in B, as the number 1 obviously belongs to B^*, and so $B \subseteq B^*$, $\mathfrak{d} \subseteq B$. Consequently,

$$\mathfrak{B}^* = (\mathfrak{B}\mathfrak{d})^{-1},$$

where $\mathfrak{d}$ is an ideal in B independent of $\mathfrak{B}$. □

The ideal $\mathfrak{d}_{K/\kappa}$ is called the *different of K with respect to κ*.

Theorem 1.118. *For a tower of fields $\kappa \subseteq K \subseteq L$, one has*

$$\mathfrak{d}_{L/\kappa} = \mathfrak{d}_{L/K}\mathfrak{d}_{K/\kappa}. \tag{1.54}$$

Proof. Let $C \subseteq L$ be the integral closure of A in L. If y is an element in L such that $y\mathfrak{d}_{L/K}\mathfrak{d}_{K/\kappa}$ is integral, then by the definition of $\mathfrak{d}_{L/K}$, $\mathfrak{d}_{K/\kappa}\mathbf{Tr}_{L/K}(y\beta)$ is integral for each integral element β over C, since for each element α in K which is divisible by $\mathfrak{d}_{K/\kappa}$

$$\mathbf{Tr}_{L/K}(y\beta\alpha) = \alpha\mathbf{Tr}_{L/K}(y\beta)$$

is integral. From the definition of $\mathfrak{d}_{K/\kappa}$, $\mathbf{Tr}_{K/\kappa}(\mathbf{Tr}_{L/K}(y\beta))$ is integral. Hence $\mathbf{Tr}_{K/\kappa}(y\beta)$ is integral and thus $\mathfrak{d}_{K/\kappa}y$ is integral if $\mathfrak{d}_{L/K}\mathfrak{d}_{K/\kappa}y$ is integral. Conversely, if $\mathfrak{d}_{K/\kappa}y$ is integral, then for each integral element β over C and each integral element α over C, $\mathbf{Tr}_{K/\kappa}(y\beta\alpha)$ is integral; hence

$$\mathbf{Tr}_{K/\kappa}(\mathbf{Tr}_{L/K}(y\beta\alpha)) = \mathbf{Tr}_{K/\kappa}(\alpha\mathbf{Tr}_{L/K}(y\beta))$$

is integral. Thus $\mathfrak{d}_{K/\kappa}\mathbf{Tr}_{L/K}(y\beta)$ is integral, that is, $\mathbf{Tr}_{L/K}(\rho y\beta)$ is integral if ρ is any element of $\mathfrak{d}_{K/\kappa}$ in K and hence $\rho y\mathfrak{d}_{L/K}$ is integral. Thus we have shown that if $\mathfrak{d}_{K/\kappa}y$ is integral, $\mathfrak{d}_{L/K}\mathfrak{d}_{K/\kappa}y$ is also integral, from which (1.54) follows. □

Proposition 1.119. *Let $\mathfrak{P}$ be a prime ideal of B which divides a prime ideal $\mathfrak{p}$ of A. Let $\hat{B}$ and $\hat{A}$ be the associated completions. Then*

$$\mathfrak{d}_{K/\kappa}\hat{B} = \mathfrak{d}_{K_{\mathfrak{P}}/\kappa_{\mathfrak{p}}}. \tag{1.55}$$

In particular, if we consider the local different of K at $\mathfrak{P}$

$$\mathfrak{d}_{\mathfrak{P}} := B \cap \mathfrak{d}_{K_{\mathfrak{P}}/\kappa_{\mathfrak{p}}}$$

as an ideal of B, then

$$\mathfrak{d}_{K/\kappa} = \prod_{\mathfrak{P}} \mathfrak{d}_{\mathfrak{P}}. \tag{1.56}$$

Proof. We follow the proof of Neukirch [202], Chapter III, Proposition 2.2. Note that for any multiplicative subset S of A, one has

$$\mathfrak{d}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{d}_{B/A}. \tag{1.57}$$

We may assume that A is a discrete valuation ring. We show that B^* is dense in $\hat{B}^*$. By Proposition 1.116, we have

$$\mathbf{Tr}_{K/\kappa} = \sum_{\mathfrak{P}|\mathfrak{p}} \mathbf{Tr}_{K_{\mathfrak{P}}/\kappa_{\mathfrak{p}}}. \tag{1.58}$$

Take $x \in B^*$ and $y \in \hat{B}$. The approximation theorem allows us to find an $\eta \in K$ which is close to y with respect to $\mathrm{ord}_{\mathfrak{P}}$, and close to 0 with respect to $\mathrm{ord}_{\mathfrak{P}'}$, for $\mathfrak{P}'|\mathfrak{p}$, $\mathfrak{P}' \neq \mathfrak{P}$. The left-hand side of the equation (1.58) for $x\eta$

$$\mathbf{Tr}_{K/\kappa}(x\eta) = \mathbf{Tr}_{K_{\mathfrak{P}}/\kappa_{\mathfrak{p}}}(x\eta) + \sum_{\mathfrak{P}'\neq\mathfrak{P}} \mathbf{Tr}_{K_{\mathfrak{P}'}/\kappa_{\mathfrak{p}}}(x\eta)$$

belongs to $\hat{A}$ since

$$\mathbf{Tr}_{K/\kappa}(x\eta) \in A \subseteq \hat{A},$$

but same is true of the elements $\mathbf{Tr}_{K_{\mathfrak{P}'}/\kappa_{\mathfrak{p}}}(x\eta)$ because they are close to zero with respect to $\mathrm{ord}_{\mathfrak{p}}$. Therefore $\mathbf{Tr}_{K_{\mathfrak{P}}/\kappa_{\mathfrak{p}}}(x\eta) \in \hat{A}$. This shows that $B^* \subseteq \hat{B}^*$.

On the other hand, if $x \in \hat{B}^*$, and if $\xi \in K$ is sufficiently close to x with respect to $\mathrm{ord}_{\mathfrak{P}}$, and sufficiently close to 0 with respect to $\mathrm{ord}_{\mathfrak{P}'}$, for $\mathfrak{P}'|\mathfrak{p}$, $\mathfrak{P}' \neq \mathfrak{P}$, then $\xi \in B^*$. In fact, if $y \in B$, then $\mathbf{Tr}_{K_{\mathfrak{P}}/\kappa_{\mathfrak{p}}}(\xi y) \in \hat{A}$ since $\mathbf{Tr}_{K_{\mathfrak{P}}/\kappa_{\mathfrak{p}}}(xy) \in \hat{A}$. Likewise

$$\mathbf{Tr}_{K_{\mathfrak{P}'}/\kappa_{\mathfrak{p}}}(\xi y) \in \hat{A},\ \mathfrak{P}'|\mathfrak{p},$$

because these elements are close to 0. Therefore

$$\mathbf{Tr}_{K/\kappa}(\xi y) \in \hat{A} \cap \kappa = A,$$

i.e., $\xi \in B^*$. This shows that B^* is dense in $\hat{B}^*$, in other words,

$$B^*\hat{B} = \hat{B}^*,$$

and so (1.55) follows. □

Proposition 1.120. *Let $B = A[\alpha]$ for some $\alpha \in B$ and let $f(X) \in A[X]$ be the minimal polynomial of α. Then the different is the principal ideal*

$$\mathfrak{d}_{K/\kappa} = (f'(\alpha)).$$

Proof. We follow the proof of Neukirch [202], Chapter III, Proposition 2.4. Let

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

be the minimal polynomial of α and write

$$\frac{f(X)}{X-\alpha} = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}.$$

The dual basis of $1, \alpha, \ldots, \alpha^{n-1}$ with respect to $\mathbf{Tr}_{K/\kappa}$ is then given by

$$\frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)}.$$

In fact, if $\alpha_1, \ldots, \alpha_n$ are the roots of f, then one has

$$\sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i}\frac{\alpha_i^m}{f'(\alpha_i)} = X^m,\ 0 \leq m \leq n-1,$$

as the difference of the two sides is a polynomial of degree $\leq n-1$ with roots $\alpha_1, \ldots, \alpha_n$, so is identically zero. We may write these equations in the form

$$\mathbf{Tr}_{K/\kappa}\left(\frac{f(X)}{X-\alpha}\frac{\alpha^m}{f'(\alpha)}\right) = X^m,\ 0 \leq m \leq n-1.$$

Consider now the coefficient of each of the powers of X, we obtain

$$\mathbf{Tr}_{K/\kappa}\left(\alpha^i \frac{b_j}{f'(\alpha)}\right) = \delta_{ij}$$

and the claim follows.

Since

$$B = A + A\alpha + \cdots + A\alpha^{n-1},$$

we obtain

$$B^* = \frac{1}{f'(\alpha)}\{Ab_0 + Ab_1 + \cdots + Ab_{n-1}\}.$$

From the recursive formulas

$$\begin{aligned} b_{n-1} &= 1, \\ b_{n-2} - \alpha b_{n-1} &= a_{n-1}, \\ &\vdots \end{aligned}$$

it follows that

$$b_{n-i} = \alpha^{i-1} + a_{n-1}\alpha^{i-2} + \cdots + a_{n-i+1},$$

so that

$$Ab_0 + Ab_1 + \cdots + Ab_{n-1} = A[\alpha] = B;$$

then

$$B^* = \frac{1}{f'(\alpha)}B,$$

and thus $\mathfrak{d}_{K/\kappa} = (f'(\alpha))$. □

Theorem 1.121. *A prime ideal $\mathfrak{P}$ of B is ramified over A if and only if $\mathfrak{P}|\mathfrak{d}_{K/\kappa}$. Further, if $\mathfrak{P}^s$ is the maximal power of $\mathfrak{P}$ dividing $\mathfrak{d}_{K/\kappa}$, then one has $s = e-1$ if $\mathfrak{P}$ is tamely ramified, and*

$$e \leq s \leq e - 1 + \mathrm{ord}_{\mathfrak{P}}(e)$$

if $\mathfrak{P}$ is wildly ramified, where $e = e_{\mathfrak{P}/A}$.

Proof. Here we follow the proof of Neukirch [202], Chapter III, Theorem 2.6. Based on (1.55) in Proposition 1.119, we may assume that A is a complete discrete valuation ring with maximal ideal $\mathbf{m}$. By (3) of Lemma 1.99, we have $B = A[\alpha]$ for some $\alpha \in B$. If $f(X) \in A[X]$ is the minimal polynomial of α, then Proposition 1.120 implies that

$$s = \mathrm{ord}_{\mathfrak{P}}(f'(\alpha)).$$

Assume K/κ is unramified. Then

$$\bar{\alpha} = \alpha \bmod \mathfrak{P}$$

is a simple zero of

$$\bar{f}(X) = f(X) \bmod \mathbf{m},$$

so that $f'(\alpha) \in B - \{0\}$ and thus $s = 0 = e - 1$.

By Theorem 1.118 and Proposition 1.105, we may now pass to the maximal unramified extension and assume that K/κ is totally ramified. Then α may be chosen to be a prime element of B. In this case the minimal polynomial

$$f(X) = a_0 X^e + a_1 X^{e-1} + \cdots + a_e$$

with $a_0 = 1$ is an Eisenstein polynomial. Since

$$f'(\alpha) = e a_0 X^{e-1} + (e-1) a_1 X^{e-2} + \cdots + a_{e-1},$$

we obtain

$$\mathrm{ord}_{\mathfrak{P}}((e-i)a_i \alpha^{e-i-1}) = e\mathrm{ord}_{\mathfrak{P}}(e-i) + e\mathrm{ord}_{\mathfrak{P}}(a_i) + e - i - 1 \equiv -i - 1 \bmod e$$

for $i = 0, \ldots, e-1$, so that the individual terms of $f'(\alpha)$ have distinct valuations. Therefore

$$s = \mathrm{ord}_{\mathfrak{P}}(f'(\alpha)) = \min_{0 \le i < e} \mathrm{ord}_{\mathfrak{P}}((e-i)a_i \alpha^{e-i-1}).$$

If now K/κ is tamely ramified, i.e., if $\mathrm{ord}_{\mathbf{m}}(e) = 0$, then the minimum is obviously equal to $e - 1$, and for $\mathrm{ord}_{\mathbf{m}}(e) \ge 1$, we deduce that $e \le s \le \mathrm{ord}_{\mathfrak{P}}(e) + e - 1$. □

Proposition 1.122. *The different $\mathfrak{d}_{K/\kappa}$ is the annihilator of the B-module $\Omega_{B/A}$, i.e.,*

$$\mathfrak{d}_{K/\kappa} = \{x \in B \mid x dy = 0 \text{ for all } y \in B\}.$$

Proof. Based on (1.7), we may assume that A is a complete discrete valuation ring. Then by (3) of Lemma 1.99, we find that $B = A[x]$ for some $x \in B$. It is easy to show that $\Omega_{B/A}$ is generated by dx. If $f(X) \in A[X]$ is the minimal polynomial of x, the annihilator of dx is $f'(x)$. On the other hand, by Proposition 1.120 we have $\mathfrak{d}_{K/\kappa} = (f'(x))$. This proves the claim. □

We then define the *discriminant of K with respect to κ* to be the norm of the different of K, that is,

$$\mathfrak{D}_{K/\kappa} = \mathbf{N}_{K/\kappa}(\mathfrak{d}_{K/\kappa}). \tag{1.59}$$

Proposition 1.119 with (1.59) yields:

Proposition 1.123. *Let $\mathfrak{P}$ be a prime ideal of B which divides a prime ideal $\mathfrak{p}$ of A. If we consider the local discriminant of K at $\mathfrak{P}$*

$$\mathfrak{D}_{\mathfrak{P}} := A \cap \mathfrak{D}_{K_{\mathfrak{P}}/\kappa_{\mathfrak{p}}}$$

as the ideal of κ, then

$$\mathfrak{D}_{K/\kappa} = \prod_{\mathfrak{P}} \mathfrak{D}_{\mathfrak{P}}.$$

Proposition 1.124. *A prime ideal $\mathfrak{p}$ of A is ramified in B if and only if $\mathfrak{p}|\mathfrak{D}_{K/\kappa}$.*

Proof. Neukirch [202], Chapter III, Corollary 2.12. □

Chapter 2

Algebraic numbers

A complex number α will be called *algebraic* if it is algebraic over $\mathbb{Q}$, that is, it satisfies a non-zero polynomial equation with coefficients in $\mathbb{Q}$. Equivalently (clearing out denominators) we may assume the coefficients to be in $\mathbb{Z}$. We let $\bar{\mathbb{Q}}$ ($\subset \mathbb{C}$) denote the set of algebraic numbers, which, in fact, is a field. The integral elements $\bar{\mathbb{Z}} \subset \mathbb{C}$ over $\mathbb{Z}$ are called *algebraic integers*. Then we have $\mathbb{Z} = \bar{\mathbb{Z}} \cap \mathbb{Q}$.

2.1 Integral ideals

The whole field $\bar{\mathbb{Q}}$ is not as interesting, for us, as certain of its subfields. We define a *number field* to be a subfield κ of $\mathbb{C}$ such that $[\kappa : \mathbb{Q}]$ is finite. This implies that every element of κ is algebraic, and hence $\kappa \subseteq \bar{\mathbb{Q}}$. The trouble with $\bar{\mathbb{Q}}$ is that $[\bar{\mathbb{Q}} : \mathbb{Q}]$ is not finite.

2.1.1 Factorization of ideals

Let κ be a finite extension of $\mathbb{Q}$ (i.e., a number field) of degree $n = [\kappa : \mathbb{Q}]$. Let $\mathcal{O}_\kappa$ be the integral closure of $\mathbb{Z}$ in κ. Obviously, we have $\mathcal{O}_\kappa = \bar{\mathbb{Z}} \cap \kappa$.

Theorem 2.1. *The ring $\mathcal{O}_\kappa$ is a Dedekind domain.*

Proof. Since κ is a separable extension of $\mathbb{Q}$ (because the characteristic is zero), hence by Proposition 1.81 there is a basis $v_1, \ldots, v_n$ of κ over $\mathbb{Q}$ such that $\mathcal{O}_\kappa \subseteq \sum \mathbb{Z} v_j$. Hence $\mathcal{O}_\kappa$ is finitely generated as a $\mathbb{Z}$-module and therefore Noetherian. Obviously, $\mathcal{O}_\kappa$ also is integrally closed since, if $x \in \kappa$ is integral over $\mathcal{O}_\kappa$, then x is integral over $\mathbb{Z}$ by transitivity of integral dependence, and so $x \in \mathcal{O}_\kappa$. To complete the proof we must show that every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_\kappa$ is maximal. Since $\mathfrak{p} \neq 0$, it is easy to get $\mathfrak{p} \cap \mathbb{Z} \neq 0$, and so $\mathfrak{p} \cap \mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, and therefore $\mathfrak{p}$ is maximal in $\mathcal{O}_\kappa$. □

Theorem 2.2. *Every ideal $\mathfrak{a}$ of $\mathcal{O}_\kappa$ can be written in the form $(\alpha_1, \ldots, \alpha_r)$ with the α_i suitably chosen algebraic integers in κ. Moreover, we may even take $r \leq n$.*

Proof. The case $\mathfrak{a} = (0)$ is trivial. Next we assume $\mathfrak{a} \neq (0)$. The elements of $\mathfrak{a}$ obviously form an infinite Abelian group under composition by addition, which is a

subgroup of the group $\mathcal{O}_\kappa$. Consequently by Theorem 1.4, the ideal $\mathfrak{a}$ has a basis, whose size is $\leq n$. On the other hand, by Theorem 1.6, the number of elements in this basis is equal to the number of independent elements in $\mathfrak{a}$; hence it is $= n$, since, indeed, if β $(\neq 0)$ belongs to $\mathfrak{a}$, the n independent elements $\beta, \alpha\beta, \alpha^2\beta, \ldots, \alpha^{n-1}\beta$ must also belong to $\mathfrak{a}$, where $\alpha \in \mathcal{O}_\kappa$ is taken with $\kappa = \mathbb{Q}(\alpha)$. Thus in each ideal $\mathfrak{a} \neq (0)$ there are exactly n elements $\alpha_1, \ldots, \alpha_n$ such that

$$\beta = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$$

represents all elements of the ideal exactly once, if $x_1, \ldots, x_n$ run through all rational integers. Such a system $\alpha_1, \ldots, \alpha_n$ is called a *basis of the ideal* (or *ideal basis*). □

We need the following generalization of the *theorem of Gauss* about polynomials which have algebraic integers as coefficients (cf. [95], Theorem 67):

Theorem 2.3. *Take two polynomials with coefficients of algebraic integers*

$$A(x) = \sum_{i=0}^{p} \alpha_i x^i, \quad B(x) = \sum_{j=0}^{q} \beta_j x^j$$

with $\alpha_p, \beta_q \neq 0$. *Then if an algebraic integer* δ *divides all coefficients* γ_k *of*

$$A(x)B(x) = \sum_{k=0}^{p+q} \gamma_k x^k$$

it also divides all products $\alpha_i\beta_j$.

Proof. First, we show some properties of a polynomial

$$f(x) = \delta_m x^m + \delta_{m-1}x^{m-1} + \cdots + \delta_1 x + \delta_0 \ \ (\delta_m \neq 0)$$

with algebraic integral coefficients. If ρ is a root, it is easy to see that $\delta_m\rho$ is an algebraic integer. Moreover, $f(x)/(x-\rho)$ has coefficients of algebraic integers. In fact, this is true for $m = 1$, in which case

$$\frac{f(x)}{x-\rho} = \delta_1, \quad \rho = -\frac{\delta_0}{\delta_1}.$$

Suppose that this fact has already been proved for all polynomials of degree $\leq m-1$. Since

$$\varphi(x) = f(x) - \delta_m x^{m-1}(x-\rho)$$

is obviously an algebraic integral polynomial of degree $\leq m-1$ with ρ as a root,

$$\frac{\varphi(x)}{x-\rho} = \frac{f(x)}{x-\rho} - \delta_m x^{m-1}$$

is thus integral. Therefore the same holds for $f(x)/(x-\rho)$, whence the fact follows by complete induction.

Further, write

$$f(x) = \delta_m(x-\rho_1)(x-\rho_2)\cdots(x-\rho_m),$$

then $\delta_m\rho_1\rho_2\cdots\rho_i$ is an algebraic integer for each i with $1 \le i \le m$. This follows by repeated application of the fact proved above from which we obtain

$$\frac{f(x)}{(x-\rho_{i+1})(x-\rho_{i+2})\cdots(x-\rho_m)} = \delta_m(x-\rho_1)\cdots(x-\rho_i)$$

as an algebraic integral polynomial whose constant term is $\pm\delta_m\rho_1\cdots\rho_i$.

We now arrive at the proof of Theorem 2.3 as follows: let the decomposition into linear factors be

$$\begin{aligned} A(x) &= \alpha_p(x-\rho_1)(x-\rho_2)\cdots(x-\rho_p), \\ B(x) &= \beta_q(x-\sigma_1)(x-\sigma_2)\cdots(x-\sigma_q). \end{aligned}$$

By hypothesis

$$\frac{A(x)B(x)}{\delta} = \frac{\alpha_p\beta_q}{\delta}(x-\rho_1)\cdots(x-\rho_p)(x-\sigma_1)\cdots(x-\sigma_q)$$

has algebraic integral coefficients, hence each product

$$\frac{\alpha_p\beta_q}{\delta}\rho_{n_1}\cdots\rho_{n_i}\sigma_{m_1}\cdots\sigma_{m_j} \tag{2.1}$$

is an algebraic integer, where $n_1,\ldots,n_i$ and likewise $m_1,\ldots,m_j$ are any distinct indices ($i \le p$, $j \le q$). However, since α_i/α_p and β_j/β_q are elementary symmetric functions of the $\rho_1,\ldots,\rho_p$ and of the $\sigma_1,\ldots,\sigma_q$, $\alpha_i\beta_j/\delta$ is a sum of terms of the form (2.1), and consequently an algebraic integer, as was to be proved. □

Proposition 2.4. **(1)** *For each ideal* $\mathfrak{a}$ *there is an ideal* $\mathfrak{b}$ *different from* (0) *such that* $\mathfrak{ab}$ *is a principal ideal.*

(2) *If* $\mathfrak{ab} = \mathfrak{ac}$, *then if* $\mathfrak{a} \neq 0$, $\mathfrak{b} = \mathfrak{c}$.

(3) *An ideal* $\mathfrak{c}$ *is a divisor of* $\mathfrak{a}$ *if and only if every element of* $\mathfrak{a}$ *belongs to* $\mathfrak{c}$.

Proof. Assume $\mathfrak{a} = (\alpha_1,\ldots,\alpha_r)$. We obtain the algebraic integral polynomial

$$g(x) = \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_r x^r$$

and the conjugate polynomials

$$g^{(i)}(x) = \alpha_1^{(i)}x + \alpha_2^{(i)}x^2 + \cdots + \alpha_r^{(i)}x^r, \;\; i = 1,2,\ldots,n$$

among which the original polynomial $g(x)$ occurs, say for $i = 1$. The product

$$f(x) = \prod_{i=1}^{n} g^{(i)}(x) = \sum_{j=n}^{nr} c_j x^j$$

as a symmetric function of the conjugates is a polynomial with integral rational coefficients c_j. Thus $f(x)$ is divisible by $g(x)$ and the quotient

$$h(x) = \frac{f(x)}{g(x)} = \prod_{i=2}^{n} g^{(i)}(x) = \beta_1 x + \beta_2 x^2 + \cdots + \beta_m x^m$$

is a polynomial with coefficients in κ which are moreover algebraic integers. If we denote the greatest common divisor of the rational integers c_j by d, so that $f(x)/d$ is a primitive polynomial, and set $\mathfrak{b} = (\beta_1, \ldots, \beta_m)$, then we assert that the equation $\mathfrak{ab} = (d)$ is true. By Theorem 2.3, d divides all $\alpha_i \beta_k$, since it divides each coefficient of $g(x)h(x)$, and hence there are rational integers x_j such that

$$d = c_n x_n + c_{n+1} x_{n+1} + \cdots + c_{nr} x_{nr}.$$

Each c_j is a sum of products $\alpha_i \beta_k$; consequently d is representable in the form

$$d = \sum_{i,k} a_{ik} \alpha_i \beta_k$$

with rational integers a_{ik}. Thus d and all elements of (d) belong to $\mathfrak{ab}$, that is, $\mathfrak{ab} = (d)$, and so (1) follows.

To see (2), we determine an ideal $\mathfrak{m} \neq (0)$ such that $\mathfrak{am} = (\alpha)$ is a principal ideal. Then

$$\mathfrak{amb} = \mathfrak{amc}, \quad (\alpha)\mathfrak{b} = (\alpha)\mathfrak{c}.$$

The latter equation asserts that α times every element from $\mathfrak{b}$ is of the form α times an element from $\mathfrak{c}$, that is, every element of $\mathfrak{b}$ belongs to $\mathfrak{c}$, and likewise the converse is true; thus $\mathfrak{b} = \mathfrak{c}$.

Write

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r), \quad \mathfrak{c} = (\gamma_1, \ldots, \gamma_m).$$

If $\mathfrak{c}|\mathfrak{a}$, then there is a $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ for which $\mathfrak{b} \neq (0)$ and

$$(\alpha_1, \ldots, \alpha_r) = (\beta_1, \ldots, \beta_s)(\gamma_1, \ldots, \gamma_m) = (\ldots, \beta_i \gamma_j, \ldots);$$

hence every element α of $\mathfrak{a}$ can be represented in the form

$$\alpha = \sum_{i,j} \lambda_{ij} \beta_i \gamma_j = \sum_{j=1}^{m} \gamma_j \left(\sum_{i=1}^{s} \lambda_{ij} \beta_i \right)$$

with algebraic integers λ_{ij} and thus belongs to $\mathfrak{c}$.

Conversely, if every element of $\mathfrak{a}$ is also an element of $\mathfrak{c}$, then for all algebraic integers λ_{ij} there are algebraic integers μ_{lj} for which

$$\sum_i \lambda_{ij}\alpha_i = \sum_l \mu_{lj}\gamma_l;$$

then for each $\mathfrak{d} = (\delta_1, \ldots, \delta_t)$

$$\sum_j \sum_i \lambda_{ij}\alpha_i\delta_j = \sum_j \sum_l \mu_{lj}\gamma_l\delta_j,$$

that is, each element in $\mathfrak{a}\mathfrak{d}$ belongs to $\mathfrak{c}\mathfrak{d}$. Now let us choose $\mathfrak{d}$ $(\neq (0))$ so that $\mathfrak{c}\mathfrak{d} = (\delta)$ is a principal ideal $(\delta \neq 0)$. If $\mathfrak{a}\mathfrak{d} = (\rho_1, \ldots, \rho_p)$, then each ρ_i is an element from (δ); thus it is of the form $\lambda_i\delta$ with algebraic integer λ_i and hence

$$\mathfrak{a}\mathfrak{d} = (\rho_1, \ldots, \rho_p) = (\delta)(\lambda_1, \ldots, \lambda_p) = \mathfrak{c}\mathfrak{d}(\lambda_1, \ldots, \lambda_p),$$

which combining with (2) means

$$\mathfrak{a} = \mathfrak{c}(\lambda_1, \ldots, \lambda_p),$$

that is, $\mathfrak{c}|\mathfrak{a}$. □

As an immediate consequence of Proposition 2.4, (3), we emphasize: Let $\mathfrak{a}$ be an ideal which is not $= (0)$.

(4) The algebraic integer α occurs in $\mathfrak{a}$ if and only if $\mathfrak{a}|(\alpha)$.

(5) If $\mathfrak{a}|(\alpha)$ and $\mathfrak{a}|(\beta)$, then also $\mathfrak{a}|(\lambda\alpha + \mu\beta)$ for all algebraic integers λ, μ.

(6) It follows from $\mathfrak{a}\mathfrak{b} = (1)$ that $\mathfrak{a} = (1)$ and $\mathfrak{b} = (1)$.

(7) If each of two ideals is a divisor of the other, then they are equal.

Theorem 2.5. *For every two ideals $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$, $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ which are not both $= (0)$, there is a uniquely determined greatest common divisor $\mathfrak{d} = (\mathfrak{a}, \mathfrak{b})$ which has the following property: $\mathfrak{d}$ is a divisor of $\mathfrak{a}$ and $\mathfrak{b}$. Furthermore if $\mathfrak{d}_1|\mathfrak{a}$ and $\mathfrak{d}_1|\mathfrak{b}$, then $\mathfrak{d}_1$ is a divisor of $\mathfrak{d}$. Indeed $\mathfrak{d} = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$*

Proof. We show that $\mathfrak{d} = (\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$ has the stated properties of divisibility. For any

$$\alpha = \sum_{i=1}^{r} \mu_i\alpha_i \in \mathfrak{a}, \quad \beta = \sum_{j=1}^{s} \nu_j\beta_j \in \mathfrak{b}$$

with algebraic integers μ_i and ν_j, we have

$$\alpha + \beta = \sum_{i=1}^{r} \mu_i\alpha_i + \sum_{j=1}^{s} \nu_j\beta_j \in \mathfrak{d}.$$

Then all elements of $\mathfrak{a}$ and $\mathfrak{b}$ belong to $\mathfrak{d}$, and consequently by Proposition 2.4, (3), $\mathfrak{d}|\mathfrak{a}$ and $\mathfrak{d}|\mathfrak{b}$.

Moreover if $\mathfrak{d}_1|\mathfrak{a}$ and $\mathfrak{d}_1|\mathfrak{b}$, then all elements of $\mathfrak{a}$ and $\mathfrak{b}$ and consequently also each sum $\alpha+\beta$ with $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ belong to $\mathfrak{d}_1$, that is, each element of $\mathfrak{d}$ belongs to $\mathfrak{d}_1$. Again we have $\mathfrak{d}_1|\mathfrak{d}$. If an ideal $\mathfrak{d}'$ likewise has this property, then $\mathfrak{d}'|\mathfrak{d}$ and $\mathfrak{d}|\mathfrak{d}'$ thus $\mathfrak{d}' = \mathfrak{d}$. Consequently $\mathfrak{d}$ is uniquely determined by this property. □

The greatest common divisor of $\alpha_1, \alpha_2, \ldots, \alpha_r$ is accordingly the ideal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$. If this ideal $= (1)$, then we call the elements $\alpha_1, \alpha_2, \ldots, \alpha_r$ *relatively prime*. Equivalently, there are algebraic integers $\lambda_1, \ldots, \lambda_r$ satisfying

$$\lambda_1\alpha_1 + \cdots + \lambda_r\alpha_r = 1.$$

We conclude immediately from the expression for $\mathfrak{d}$ that

$$\mathfrak{c}(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{c}\mathfrak{a}, \mathfrak{c}\mathfrak{b}). \tag{2.2}$$

Thus it follows that if $\mathfrak{p}$ is a prime ideal and $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$, then $\mathfrak{p}$ divides either $\mathfrak{a}$ or $\mathfrak{b}$ or both. For if $\mathfrak{p} \nmid \mathfrak{b}$, then $(\mathfrak{p}, \mathfrak{b}) = (1)$, since, as a prime ideal, $\mathfrak{p}$ has no factors except (1) and $\mathfrak{p}$. It follows from (2.2) that

$$\mathfrak{a} = \mathfrak{a}(1) = \mathfrak{a}(\mathfrak{p}, \mathfrak{b}) = (\mathfrak{a}\mathfrak{p}, \mathfrak{a}\mathfrak{b})$$

and since $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$, $\mathfrak{p}$ must divide $\mathfrak{a}$.

Now we can show the *fundamental theorem of ideal theory*:

Theorem 2.6. *Every ideal in $\mathcal{O}_\kappa$ different from (0) and (1) can be written in one and only one way (except for order) as a product of prime ideals.*

Proof. It immediately follows from Theorem 1.36 and Theorem 2.1. Here we introduce another proof. First, we show the following two claims:

(a) Every ideal $\mathfrak{a}$ which is not (0) has only finite many divisors.

(b) Every proper divisor of $\mathfrak{a}$ $(\neq (0))$ has fewer divisors than $\mathfrak{a}$.

For the proof of (a), we recall that every ideal $\mathfrak{a}$ $(\neq (0))$ divides a certain principal ideal (α), and that each divisor of $\mathfrak{a}$ is also a divisor (α). Thus it is sufficient to verify the finiteness of the number of divisors of each principal ideal (α), and here we may take α as a rational integer, since $\alpha|\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha)$ implies $(\alpha)|\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha)$ and $\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha) = N$ is such a number.

By Proposition 2.4, (3), an ideal (N) is divisible only by those ideals $\mathfrak{a}$ in which N occurs. Now let $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ be a divisor of (N), hence let N occurs in $\mathfrak{a}$. It is sufficient to assume $r \leq n$, since, for example, we can indeed choose for the α_i a basis for $\mathfrak{a}$. Now

$$(\alpha_1, \ldots, \alpha_r) = (\alpha_1, \ldots, \alpha_r, N) = (\alpha_1 - N\beta_1, \ldots, \alpha_r - N\beta_r, N)$$

is true for arbitrary algebraic integers β_i. We show that the β_i can be chosen so that the $\alpha_i - N\beta_i$ belong to a definite finite range of values. Let $\omega_1, \ldots, \omega_n$ be a basis for the field. To each algebraic integer

$$\alpha = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n,$$

an algebraic integer

$$\beta = y_1\omega_1 + y_2\omega_2 + \cdots + y_n\omega_n$$

(x_i and y_i rational integers) can obviously be determined so that in

$$\alpha - N\beta = (x_1 - Ny_1)\omega_1 + \cdots + (x_n - Ny_n)\omega_n$$

the n rational integers $x_i - Ny_i$ belong to the interval $\mathbb{Z}[0, N-1]$. Among these numbers, which we call "reduced mod N" for the moment, there are only $|N|^n$ distinct ones. We now choose the β_i so that all elements $\alpha_i - N\beta_i$ are reduced mod N; then the, at most, n elements $\alpha_i - N\beta_i$ belong to a definite finite set of numbers determined only by N, and hence they can give rise to only finitely many distinct ideals $\mathfrak{a}$; that is, (N) has only finitely many divisors and the claim (a) is proved.

In order to prove the claim (b), let $\mathfrak{c}$ be a proper divisor of $\mathfrak{a}$. Thus $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ where $\mathfrak{b} \neq (1)$, $\mathfrak{c} \neq \mathfrak{a}$. Then $\mathfrak{c}$ surely does not have $\mathfrak{a}$ as a divisor, and consequently $\mathfrak{c}$ has at least one less divisor than $\mathfrak{a}$.

Now at least one prime ideal must occur among the finitely many, say m, divisors of $\mathfrak{a}$ which are $\neq (1)$, unless $\mathfrak{a}$ itself is (1). Namely by the claim (b), the divisor or divisors which have as few divisors as possible are obviously prime ideals. Consequently, we can split off a prime ideal $\mathfrak{p}_1$ from $\mathfrak{a}$, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, where $\mathfrak{a}_1$ has at most $m-1$ divisors which are $\neq (1)$. In case $\mathfrak{a}_1 \neq (1)$, we can again split off a prime ideal $\mathfrak{p}_2$ from $\mathfrak{a}_1$, $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$, where $\mathfrak{a}_2$ has at most $m-2$ divisors $\neq (1)$, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{a}_2$ and so on. Since $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ always have decreasing numbers of divisors, the process must come to an end after finitely many steps, which can only occur if $\mathfrak{a}_k = (1)$. Then

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$$

is represented as a product of prime ideals, and we have proved Theorem 2.6. □

This theorem gives an entirely new method for deciding whether or not an algebraic integer α is divisible by an algebraic integer β. First we decompose both ideals (α) and (β) into their distinct prime factors:

$$\begin{aligned}(\alpha) &= \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_l^{a_l} \quad (a_i \geq 0),\\ (\beta) &= \mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_l^{b_l} \quad (b_i \geq 0).\end{aligned}$$

By Theorem 2.6, β divides α if and only if $a_i - b_i \geq 0$ for $i = 1, 2, \ldots, l$.

Theorem 2.7. *There are infinitely many prime ideals in each number field.*

Proof. Each rational prime p defines an ideal (p), and moreover if p and q are distinct positive primes, then $(p, q) = 1$ in the sense of our ideal theory, since the number 1 occurs in the form $px + qy$ in (p, q). Consequently, the same primes never divide (p) and (q); hence there are at least as many prime ideals as there are positive primes p. □

Theorem 2.8. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals distinct from* (0)*, then there is always an element* ω *for which* $(\omega, \mathfrak{ab}) = \mathfrak{a}$.

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be all distinct prime ideals which divide $\mathfrak{ab}$ and let

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} \quad (a_i \geq 0).$$

We write

$$\mathfrak{d}_i = \mathfrak{p}_1^{a_1+1} \cdots \mathfrak{p}_{i-1}^{a_{i-1}+1} \mathfrak{p}_{i+1}^{a_{i+1}+1} \cdots \mathfrak{p}_r^{a_r+1}, \quad i = 1, \ldots, r.$$

Since these $\mathfrak{d}_i$ in their totality are relatively prime, there are elements $\delta_i \in \mathfrak{d}_i$ satisfying

$$\delta_1 + \delta_2 + \cdots + \delta_r = 1.$$

Since $\mathfrak{d}_i | \delta_i$, hence $\mathfrak{p}_j | \delta_i$ $(j \neq i)$. Consequently, $\mathfrak{p}_i \nmid \delta_i$ since $\mathfrak{p}_i \nmid (1)$.

We now determine r elements α_i such that

$$\mathfrak{p}_i^{a_i} | \alpha_i, \quad \mathfrak{p}_i^{a_i+1} \nmid \alpha_i, \quad i = 1, \ldots, r$$

which is obviously always possible since for this to happen α_i need only be an element from $\mathfrak{p}_i^{a_i}$ which does not occur in $\mathfrak{p}_i^{a_i+1}$. Then the element

$$\omega = \alpha_1 \delta_1 + \alpha_2 \delta_2 + \cdots + \alpha_r \delta_r$$

has the property asserted in Theorem 2.8. For each of the prime ideals $\mathfrak{p}_i$ occurs in $r - 1$ summands at least to the power $\mathfrak{p}_i^{a_i+1}$; however, it occurs precisely to the power $\mathfrak{p}_i^{a_i}$ in the i-th summand; consequently ω is divisible by precisely the a_i-th power of $\mathfrak{p}_i$, but no higher power. □

By taking $\mathfrak{ab}$ itself as a principal ideal β, which is divisible by $\mathfrak{a}$, we obtain that each ideal $\mathfrak{a}$ can be represented as the greatest common divisor of two elements of the field: $\mathfrak{a} = (\omega, \beta)$.

Let P be a polynomial of variables $x_1, \ldots, x_n$, in which the coefficients of the various products of powers are all algebraic integers in κ. We now define the *content, $J(P)$, of a polynomial P* to be the ideal generated by the coefficients of P, which is just the greatest common divisor of the coefficients of P. *Theorem of Gauss* (cf. Theorems 1.47 and 2.3) has the following form:

Theorem 2.9. *The content of a product of two polynomials is equal to the product of the contents of the two factors.*

Proof. See E. Hecke [95], Theorems 86 and 87. □

2.1.2 The norm of an ideal

Theorem 2.10. *Let κ be a finite extension of degree n over $\mathbb{Q}$. Let $\mathcal{O}_\kappa$ be the integral closure of $\mathbb{Z}$ in κ. Let $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_\kappa$. Then the number of residue classes $\mathrm{mod}(\mathfrak{a})$ is finite.*

Proof. The elements of $\mathfrak{a}$ form a subgroup of $\mathcal{O}_\kappa$. The different cosets in $\mathcal{O}_\kappa$ determined by $\mathfrak{a}$ obviously form the different residue classes $\mathrm{mod}(\mathfrak{a})$. Hence the number of distinct residue classes $\mathrm{mod}(\mathfrak{a})$ is the index of $\mathfrak{a}$ in $\mathcal{O}_\kappa$. This index is finite. For if α is any nonzero element in $\mathfrak{a}$, then the positive rational number $a = |\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha)|$ also belongs to $\mathfrak{a}$, since $\alpha|\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha)$, and consequently the product $ax \in \mathfrak{a}$ for any $x \in \mathcal{O}_\kappa$. Thus in group-theoretic terms the a-th power, in the sense of composition, of each element of $\mathcal{O}_\kappa$ belongs to $\mathfrak{a}$. Consequently, by Theorem 1.9, the index of $\mathfrak{a}$ is finite. □

The number of residue classes is denoted by $\mathcal{N}(\mathfrak{a})$, called the (*absolute*) *norm* of $\mathfrak{a}$, or is also called the *counting norm* in the sense of Theorem 2.10. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be all distinct prime ideals which divide $\mathfrak{a}$ and let

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

with $a_i > 0$ for each i. Let p_i be the positive prime integer with $(p_i) = \mathbb{Z} \cap \mathfrak{p}_i$. By the Chinese Remainder Theorem 1.13, we have

$$\mathcal{O}_\kappa/\mathfrak{a} \cong \mathcal{O}_\kappa/\mathfrak{p}_1^{a_1} \oplus \cdots \oplus \mathcal{O}_\kappa/\mathfrak{p}_r^{a_r}.$$

Observe that $\mathfrak{p}_i^b/\mathfrak{p}_i^{b+1}$ is a one-dimensional vector space over $\mathcal{O}_\kappa/\mathfrak{p}_i$. It follows that the number of elements in $\mathcal{O}_\kappa/\mathfrak{p}_i^{a_i}$ is $\mathcal{N}(\mathfrak{p}_i)^{a_i}$. The dimension of $\mathcal{O}_\kappa/\mathfrak{p}_i$ over $\mathbb{Z}/(p_i)$ is $f_{\mathfrak{p}_i/\mathbb{Z}}$ so

$$\mathcal{N}(\mathfrak{p}_i) = p_i^{f_{\mathfrak{p}_i/\mathbb{Z}}}.$$

Thus $\mathcal{O}_\kappa/\mathfrak{p}_i^{a_i}$ has $p_i^{a_i f_{\mathfrak{p}_i/\mathbb{Z}}}$ elements and

$$\mathcal{N}(\mathfrak{a}) = \prod_{i=1}^{r} p_i^{a_i f_{\mathfrak{p}_i/\mathbb{Z}}}. \tag{2.3}$$

By Proposition 1.82 and Proposition 1.83, we have

$$\mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{a}) = \prod_{i=1}^{r} \mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{p}_i)^{a_i} = \prod_{i=1}^{r} (p_i)^{a_i f_{\mathfrak{p}_i/\mathbb{Z}}},$$

which means

$$\mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{a}) = (\mathcal{N}(\mathfrak{a})). \tag{2.4}$$

Let the rational integers a, b, c $(a > 0)$ be given. A basic theorem in number theory claims that the congruence

$$bx + c \equiv 0 \ (\mathrm{mod}\ a) \tag{2.5}$$

has exactly one solution $\mathrm{mod}\ a$ if $(b, a) = 1$. In the case $(b, a) > 1$, (2.5) is solvable if and only if $(b, a)|c$. Then the number of distinct solutions $\mathrm{mod}\ a$ is equal to (b, a).

Theorem 2.11. *Let $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_\kappa$. For given α and β the congruence*

$$\alpha\xi \equiv \beta \pmod{\mathfrak{a}}$$

can be solved by an algebraic integer ξ in κ if and only if $(\alpha, \mathfrak{a})|\beta$. If $(\alpha, \mathfrak{a}) = 1$, then the solution is completely determined $\bmod \mathfrak{a}$.

Proof. First, assume $(\alpha, \mathfrak{a}) = 1$. Let ξ run through a system of $\mathcal{N}(\mathfrak{a})$ elements which are incongruent $\bmod \mathfrak{a}$. Then $\alpha\xi$ runs through all the residue classes $\bmod \mathfrak{a}$, for it follows from

$$\alpha\xi_1 \equiv \alpha\xi_2 \pmod{\mathfrak{a}}$$

that $\mathfrak{a}|\alpha(\xi_1 - \xi_2)$. However, since $(\alpha, \mathfrak{a}) = 1$ we must have $\mathfrak{a}|(\xi_1 - \xi_2)$, that is,

$$\xi_1 \equiv \xi_2 \pmod{\mathfrak{a}}$$

by the fundamental theorem. Thus, among the elements $\alpha\xi$, one from the residue class of β also occurs. For the same reason the solution is obviously determined uniquely $\bmod \mathfrak{a}$.

Moreover if we now have $(\alpha, \mathfrak{a}) = \mathfrak{d}$ and there is an algebraic integer ξ_0 with

$$\alpha\xi_0 \equiv \beta \pmod{\mathfrak{a}},$$

then $\alpha\xi_0 = \beta + \rho$, where $\mathfrak{a}|\rho$. Thus $\mathfrak{d}|\rho$ and $\mathfrak{d}|\alpha\xi_0 - \rho$, that is, $\mathfrak{d}|\beta$.

Conversely, if $\mathfrak{d}|\beta$, $\beta = \mathfrak{d}\mathfrak{b}$, then let us set

$$\alpha = \mathfrak{d}\mathfrak{a}_1, \quad \mathfrak{a} = \mathfrak{d}\mathfrak{a}_2$$

so that $(\mathfrak{a}_1, \mathfrak{a}_2) = 1$. By Theorem 2.8, there exists an element $\omega = \mathfrak{m}\mathfrak{a}_1$ such that $(\omega, \mathfrak{a}_1\mathfrak{d}\mathfrak{a}_2) = \mathfrak{a}_1$, thus $(\mathfrak{m}, \mathfrak{d}\mathfrak{a}_2) = 1$. Then $\mathfrak{d}\mathfrak{a}_1|\mathfrak{m}\mathfrak{a}_1\mathfrak{d}\mathfrak{b}$, hence $\alpha|\omega\beta$ and the congruence

$$\omega\xi \equiv \frac{\omega\beta}{\alpha} \pmod{\mathfrak{a}_2}$$

is solvable for ξ by what has just been proved, since

$$(\omega, \mathfrak{a}_2) = (\mathfrak{m}\mathfrak{a}_1, \mathfrak{a}_2) = 1$$

follows from $(\mathfrak{m}, \mathfrak{a}_2) = 1$ and $(\mathfrak{a}_1, \mathfrak{a}_2) = 1$. From $\mathfrak{a}_2|\omega\xi - \omega\beta/\alpha$ it follows that

$$\alpha\mathfrak{a}_2|(\alpha\omega\xi - \omega\beta),$$

i.e.,

$$\mathfrak{d}\mathfrak{a}_1\mathfrak{a}_2|(\omega)(\alpha\xi - \beta), \quad \mathfrak{d}\mathfrak{a}_1\mathfrak{a}_2|\mathfrak{m}\mathfrak{a}_1(\alpha\xi - \beta),$$

$$\mathfrak{d}\mathfrak{a}_2|\mathfrak{m}(\alpha\xi - \beta), \quad \mathfrak{d}\mathfrak{a}_2|(\alpha\xi - \beta)$$

(as $(\mathfrak{m}, \mathfrak{d}\mathfrak{a}_2) = 1$), that is, $\mathfrak{a}|(\alpha\xi - \beta)$. □

Theorem 2.12. *For two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_\kappa$, we always have*

$$\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}).$$

Proof. Let ω be an element divisible by $\mathfrak{a}$ such that $(\omega, \mathfrak{ab}) = \mathfrak{a}$. If we let ξ_i ($i = 1, 2, \ldots, \mathcal{N}(\mathfrak{b})$) run through a complete system of residues $\bmod \mathfrak{b}$ and let η_j ($j = 1, 2, \ldots, \mathcal{N}(\mathfrak{a})$) run through a complete system of residues $\bmod \mathfrak{a}$, then no two of the elements $\omega\xi_i + \eta_j$ are congruent $\bmod \mathfrak{ab}$. On the other hand, each algebraic integer ρ is congruent $\bmod \mathfrak{ab}$ to one of these elements $\omega\xi_i + \eta_j$. For let η_j be determined so that

$$\eta_j \equiv \rho \pmod{\mathfrak{a}}$$

and then let ξ be determined so that

$$\omega\xi \equiv \rho - \eta_j \pmod{\mathfrak{ab}}.$$

Since $(\omega, \mathfrak{ab}) = \mathfrak{a}$ and $\mathfrak{a}|\rho - \eta_j$, this congruence can be solved by Theorem 2.11 and ξ can be determined $\bmod \mathfrak{b}$ so that ξ can be chosen equal to ξ_i. Consequently, the $\mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$ elements $\omega\xi_i + \eta_j$ form a complete system of residues $\bmod \mathfrak{ab}$ and thus there must be $\mathcal{N}(\mathfrak{ab})$ of them. □

Theorem 2.12 can be deduced directly from Proposition 1.82 and the relation (2.4).

Theorem 2.13. *The norm of a prime ideal $\mathfrak{p}$ in $\mathcal{O}_\kappa$ is a power of a certain rational prime p, $\mathcal{N}(\mathfrak{p}) = p^f$, where $f = f_{\mathfrak{p}/\mathbb{Z}}$ is the relative degree of $\mathfrak{p}$ over $\mathbb{Z}$. Every ideal (p), where p is a rational prime, can be decomposed into at most n factors.*

Proof. For each prime ideal $\mathfrak{p}$ divides certain rational numbers and consequently also certain rational primes p. Suppose that $\mathfrak{p}|p$, $p = \mathfrak{pa}$. Then

$$\mathcal{N}(p) = \mathcal{N}(\mathfrak{pa}) = \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{a}),$$

and consequently the rational integer $\mathcal{N}(\mathfrak{p})$ divides $\mathcal{N}(p) = p^n$; hence $\mathcal{N}(\mathfrak{p}) = p^f$ and $f \leq n$. If we think of (p) as decomposed into its prime factors

$$p = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r,$$

then the positive rational integers $\mathcal{N}(\mathfrak{p}_1) \cdots \mathcal{N}(\mathfrak{p}_r)$ have as product $\mathcal{N}(p) = p^n$, while none of these integers is $= 1$; thus their number r must $\leq n$. □

2.2 Absolute values on number fields

We will show that the product formula (1.33) over $\mathbb{Q}$ can be extended to finite extension fields of $\mathbb{Q}$ with a proper modification.

2.2.1 Archimedean absolute values

We consider the Archimedean absolute values in an algebraic number field κ of degree n. Then we have $\kappa = \mathbb{Q}(t)$ for some algebraic number t. For every embedding $\sigma : \kappa \longrightarrow \mathbb{C}$ over $\mathbb{Q}$, we define

$$|x|_\sigma = |\sigma(x)|_\infty,$$

where $|\cdot|_\infty$ is the ordinary absolute value of $\mathbb{C}$. It is obvious that $|\cdot|_\sigma$ is an Archimedean absolute value of κ extending the ordinary absolute value on $\mathbb{Q}$. If ρ, σ are embeddings of κ over $\mathbb{Q}$ such that $|\cdot|_\rho$, $|\cdot|_\sigma$ are distinct, then $|\cdot|_\rho$, $|\cdot|_\sigma$ are not equivalent; otherwise there exists an $\alpha > 0$ such that

$$|x|_\rho = |x|_\sigma^\alpha, \ \ x \in \kappa,$$

and taking $x \in \mathbb{Q}$ we see that $\alpha = 1$.

Every Archimedean absolute value $|\cdot|$ of κ is equivalent to some $|\cdot|_\sigma$; in fact, let $(\hat{\kappa}, |\cdot|_\wedge)$ be the completion of $(\kappa, |\cdot|)$; by Theorem 1.90, there exists an isomorphism σ of $\hat{\kappa}$ onto $\mathbb{C}$ or $\mathbb{R}$ such that

$$|x|_\wedge = |\sigma(x)|_\infty^\alpha$$

for some real number $\alpha > 0$; thus $|\cdot|$ is equivalent to $|\cdot|_\sigma$.

If ρ, σ are embeddings of κ over $\mathbb{Q}$ such that $\sigma(x) = \overline{\rho(x)}$ (complex conjugate of $\rho(x)$) for all $x \in \kappa$, then for every $x \in \kappa$

$$|x|_\sigma = |\sigma(x)|_\infty = |\overline{\rho(x)}|_\infty = |\rho(x)|_\infty = |x|_\rho.$$

Conversely, we show that if $|x|_\sigma = |x|_\rho$ for every $x \in \kappa$, then $\sigma(x) = \overline{\rho(x)}$. Consider

$$\sigma\rho^{-1} : \mathbb{Q}(\rho(t)) \longrightarrow \mathbb{Q}(\sigma(t)).$$

It is continuous in the topology defined by $|\cdot|_\infty$, because given any element $\sigma(x) \in \sigma(\mathbb{Q}(t))$ and $\varepsilon > 0$ in $\mathbb{R}$, let $|\rho(y) - \rho(x)|_\infty < \varepsilon$; then $\sigma\rho^{-1}(\rho(y)) = \sigma(y)$ is such that

$$\begin{aligned} |\sigma(y) - \sigma(x)|_\infty &= |\sigma(y - x)|_\infty = |y - x|_\sigma = |y - x|_\rho \\ &= |\rho(y) - \rho(x)|_\infty < \varepsilon. \end{aligned}$$

Since $\sigma\rho^{-1}$ is continuous and acts as the identity on $\mathbb{Q}$, it may be naturally extended to an isomorphism

$$\tau : \mathbb{R}(\rho(t)) \longrightarrow \mathbb{R}(\sigma(t));$$

thus $\rho(t)$, $\sigma(t) \in \mathbb{C}$ are conjugates over $\mathbb{R}$ and so $\sigma(t) = \overline{\rho(t)}$ (complex conjugate). For every $x \in \mathbb{Q}(t) = \kappa$, there are $a_i \in \mathbb{Q}$ satisfying

$$x = \sum_{i=0}^{n-1} a_i t^i, \quad \sigma(x) = \sum_{i=0}^{n-1} a_i \sigma(t)^i = \overline{\rho(x)}.$$

Thus we arrive the following result:

Proposition 2.14. *Let r_1 be the number of embeddings of κ into $\mathbb{R}$, and let $2r_2$ be the number of embeddings of κ into $\mathbb{C}$, whose image is not contained in $\mathbb{R}$. Then*

$$r_1 + 2r_2 = [\kappa : \mathbb{Q}],$$

and κ has $r_1 + r_2$ pairwise inequivalent Archimedean absolute values $|\cdot|_\sigma$. Moreover, $|\cdot|_\sigma = |\cdot|_\rho$ if and only if $\sigma(x) = \overline{\rho(x)}$ for every $x \in \kappa$.

Here we explain Theorem 1.115 for the case $\kappa/\mathbf{F}$ with $\mathbf{F} = \mathbb{Q}$. Let

$$P_t(X) = (X - t_1)\cdots(X - t_{r_1})(X^2 + \alpha_1 X + \beta_1)\cdots(X^2 + \alpha_{r_2} X + \beta_{r_2})$$

be the decomposition of the minimal polynomial $P_t(X) \in \mathbb{Q}[X]$ of t into irreducible polynomials over $\mathbb{R}$. Let $\sigma_1, \ldots, \sigma_{r_1}, \ldots, \sigma_{r_1+r_2}$ be the embeddings in Proposition 2.14. If κ_{σ_i} denotes the completion of κ relative to the absolute value $|\cdot|_{\sigma_i}$ associated to σ_i (see Proposition 2.14), we have

$$\kappa_{\sigma_i} = \begin{cases} \mathbb{R}, & \text{if } i = 1, \ldots, r_1, \\ \mathbb{C}, & \text{if } i = r_1 + 1, \ldots, r_1 + r_2. \end{cases}$$

Then we have an $\mathbb{R}$-algebra isomorphism

$$\kappa \otimes_{\mathbf{F}} \mathbf{F}_\infty = \kappa \otimes \mathbb{R} \cong \kappa_{\sigma_1} \times \cdots \times \kappa_{\sigma_{r_1+r_2}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \tag{2.6}$$

or $\kappa \otimes \mathbb{R} \cong \mathbb{R}^n$ as a real vector space, so that

$$n = r_1 + 2r_2 = [\kappa : \mathbf{F}].$$

2.2.2 Product formula

Let κ be a field. For each $v \in M_\kappa$, let n_v be a positive real number. We shall say that M_κ satisfies the *product formula with multiplicities n_v* if for each $x \in \kappa_*$, we have

$$\prod_{v \in M_\kappa} |x|_v^{n_v} = 1.$$

We shall say that M_κ satisfies the *product formula* if all $n_v = 1$. When we deal with a fixed set of multiplicities n_v, then we write for convenience

$$\|x\|_v = |x|_v^{n_v} \tag{2.7}$$

so that the product formula reads

$$\prod_{v \in M_\kappa} \|x\|_v = 1. \tag{2.8}$$

We define a *multiplicative M_κ-constant* γ to be a real valued positive function

$$\gamma : M_\kappa \longrightarrow \mathbb{R}^+$$

such that $\gamma_v = 1$ for almost all $v \in M_\kappa$ (all but a finite number of v in M_κ). Thus if M_κ satisfies a product formula with multiplicities n_v, then for $\alpha \in \kappa_*$, $\gamma(\alpha) = \{\|\alpha\|_v\}$ is a multiplicative M_κ-constant determined by α.

Suppose now that we have a field $\mathbf{F}$ with a set $M_\mathbf{F}$ of places satisfying the product formula with multiplicities 1. Let κ be a finite separable extension of $\mathbf{F}$, and let M_κ be the set of places on κ which extend the places of $M_\mathbf{F}$. If $\mathfrak{p} \in M_\mathbf{F}$ and $v \in M_\kappa$ with $v|\mathfrak{p}$, set

$$n_v = [\kappa_v : \mathbf{F}_\mathfrak{p}].$$

Then for any $x \in \kappa_*$, we get by Proposition 1.116:

$$1 = \prod_{\mathfrak{p} \in M_\mathbf{F}} \left|\mathbf{N}_{\kappa/\mathbf{F}}(x)\right|_\mathfrak{p} = \prod_{\mathfrak{p} \in M_\mathbf{F}} \prod_{v|\mathfrak{p}} |x|_v^{n_v} = \prod_{v \in M_\kappa} |x|_v^{n_v}.$$

This shows that M_κ satisfies the product formula with multiplicities n_v. Next we concretely show this fact for the case $\mathbf{F} = \mathbb{Q}$.

Let κ be an algebraic number field of degree n. Given a prime number p and let v be a valuation of κ dividing p. Let n_v denotes the local degree of the valuation v in $\kappa/\mathbb{Q}$. Let κ_v denote the completion of κ, with respect to the valuation v, which is an algebraic extension of degree n_v over the field $\mathbb{Q}_p$ of p-adic numbers. Therefore, by the uniqueness of the extension of ord_p to κ_v, for $x \in \kappa$ we have

$$\left|\mathbf{N}_{\kappa_v/\mathbb{Q}_p}(x)\right|_p = \left|\mathbf{N}_{\kappa_v/\mathbb{Q}_p}(x)\right|_v = \prod_\sigma |\sigma(x)|_v = |x|_v^{n_v}, \tag{2.9}$$

where the product extends over all $\mathbb{Q}_p$-isomorphisms of κ_v into an algebraic closure, that is,

$$|x|_v^{n_v} = p^{-\mathrm{ord}_p(\mathbf{N}_{\kappa_v/\mathbb{Q}_p}(x))},$$

and hence

$$v(x) = \frac{1}{n_v}\mathrm{ord}_p(\mathbf{N}_{\kappa_v/\mathbb{Q}_p}(x)). \tag{2.10}$$

If we multiply the relations (2.9) for all valuations v dividing p, it follows from Proposition 1.116 that

$$\left|\mathbf{N}_{\kappa/\mathbb{Q}}(x)\right|_p = \prod_{v|p} \left|\mathbf{N}_{\kappa_v/\mathbb{Q}_p}(x)\right|_p = \prod_{v|p} |x|_v^{n_v}. \tag{2.11}$$

For the ordinary absolute value, we have an analogous result. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the isomorphisms of κ into $\mathbb{R}$ with $r_1 \geq 0$, and let $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ $(r_2 \geq 0)$ be the isomorphisms of κ into $\mathbb{C}$ having image not contained in $\mathbb{R}$, and such that every other isomorphism is the complex conjugate of some σ_i $(r_1 + 1 \leq i \leq r_1 + r_2)$. If κ_{σ_i}

denotes the completion of κ relative to the absolute value $|\cdot|_{\sigma_i}$ associated to σ_i (see Proposition 2.14), we have

$$\kappa_{\sigma_i} = \begin{cases} \mathbb{R}, & \text{if } i = 1, \dots, r_1, \\ \mathbb{C}, & \text{if } i = r_1 + 1, \dots, r_1 + r_2. \end{cases}$$

Hence the local degrees of these absolute values are

$$n_{\sigma_i} = [\kappa_{\sigma_i} : \mathbb{Q}_\infty] = \begin{cases} 1, & \text{if } \kappa_{\sigma_i} = \mathbb{R}, \\ 2, & \text{if } \kappa_{\sigma_i} = \mathbb{C}. \end{cases}$$

The same proof as that of (2.11) now gives

$$\left|\mathbf{N}_{\kappa/\mathbb{Q}}(x)\right|_\infty = \prod_{i=1}^{r_1+r_2} |x|_{\sigma_i}^{n_{\sigma_i}}. \tag{2.12}$$

For convenience, we also write $\sigma_i|\infty$ for each i, and so

$$M_\kappa^\infty = \{\sigma_1, \dots, \sigma_{r_1+r_2}\}$$

is just the set of all Archimedean places of κ, which is called the set of *places at infinity*.

Combining these facts, we arrive the *product formula*: for every element $x \in \kappa_*$,

$$\prod_{v \in M_\kappa} |x|_v^{n_v} = 1. \tag{2.13}$$

In fact, by (2.11),

$$\prod_{v \in M_\kappa^0} |x|_v^{n_v} = \prod_p \prod_{v|p} |x|_v^{n_v} = \prod_p \left|\mathbf{N}_{\kappa/\mathbb{Q}}(x)\right|_p,$$

and by (2.12)

$$\prod_{v \in M_\kappa^\infty} |x|_v^{n_v} = \prod_{i=1}^{r_1+r_2} |x|_{\sigma_i}^{n_{\sigma_i}} = \left|\mathbf{N}_{\kappa/\mathbb{Q}}(x)\right|_\infty,$$

hence by the product formula valid in $\mathbb{Q}$ (see (1.33)), we have

$$\prod_{v \in M_\kappa} |x|_v^{n_v} = \prod_{p \in M_\mathbb{Q}} \left|\mathbf{N}_{\kappa/\mathbb{Q}}(x)\right|_p = 1$$

because $\mathbf{N}_{\kappa/\mathbb{Q}}(x) \neq 0$.

By the arguments as above, the set M_κ of places extending those of $M_\mathbb{Q}$ is a set of places on κ satisfying the product formula with multiplicities n_v, where $n_v = [\kappa_v : \mathbb{Q}_p]$ is the *local degree of* v if $v|p$ for some $p \in M_\mathbb{Q}$ such that

$$\sum_{v|p} n_v = [\kappa : \mathbb{Q}].$$

The set M_κ will be called the *canonical set*. For convenience, we also write

$$|||x|||_v = \|x\|_v^{1/[\kappa:\mathbb{Q}]}, \ \ x \in \kappa. \tag{2.14}$$

From (2.10), it follows that each valuation $v \in M_\kappa^0$ is discrete with the order function

$$\mathrm{ord}_v(x) = \mathrm{ord}_p(\mathbf{N}_{\kappa_v/\mathbb{Q}_p}(x)), \ \ v|p. \tag{2.15}$$

Obviously, one also has

$$\mathcal{O}_\kappa = \bigcap_{v \in M_\kappa^0} \mathcal{O}_{\kappa,v}. \tag{2.16}$$

By Theorem 1.109, the mapping ϕ from the fractional ideals $\mathfrak{I}_\kappa$ to the divisors $\mathcal{D}_\kappa$ with $S = M_\kappa^0$ is an isomorphism. In this isomorphism, a fractional ideal corresponds to a place v in M_κ^0 if and only if the ideal, say $\mathfrak{p}$, is a nonzero prime ideal, and in this case $\mathfrak{p} = \mathcal{O}_\kappa \cap \mathbf{m}_{\kappa,v}$, while $(\mathcal{O}_\kappa)_\mathfrak{p} = \mathcal{O}_{\kappa,v}$. Usually, we denote the relation $\mathfrak{p} \mapsto v$ by $\mathfrak{p}_v$, and identity $\mathfrak{p}$ with v.

If $v \in M_\kappa^0$ is one of the places extending the p-adic absolute value on $\mathbb{Q}$, its multiplicity is

$$n_v = [\kappa_v : \mathbb{Q}_p] = e_v f_v,$$

where e_v and f_v are the ramification index and residue class degree, respectively. Note that $\mathfrak{p} = \mathfrak{p}_v$ divides $p\mathcal{O}_\kappa$, or equivalently, $\mathfrak{p} \cap \mathbb{Z} = \mathbb{Z}p$. Note that $e_v = \mathrm{ord}_v(p)$ is the power of $\mathfrak{p}$ that appears in the prime factorization of $p\mathcal{O}_\kappa$. Then

$$|x|_v = p^{-\mathrm{ord}_v(x)/e_v},$$

where e_v is needed to ensure that $|p|_v = p^{-1}$. Notice that

$$\mathcal{O}_\kappa/\mathfrak{p} \cong \mathcal{O}_{\kappa,v}/\mathfrak{p}\mathcal{O}_{\kappa,v} \cong \mathbb{F}_v(\kappa),$$

and so Theorem 2.13 or Proposition 1.112 mean

$$\mathcal{N}(\mathfrak{p}) = p^{f_v}$$

since $\mathbb{F}_v(\kappa)$ is of degree f_v over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Thus we obtain

$$\|x\|_v = \mathcal{N}(\mathfrak{p})^{-\mathrm{ord}_v(x)}. \tag{2.17}$$

Proposition 2.15. *Let $\sigma : \kappa \longrightarrow K$ be an isomorphism. If $w \in M_K$, for $x \in \kappa$ put $|x|_v = |\sigma(x)|_w$. Then $v \in M_\kappa$, and this gives a one-to-one mapping $M_K \longrightarrow M_\kappa$, and in this correspondence $n_w = n_v$.*

If we have a tower of finite extensions, $\mathbb{Q} \subset \kappa \subset K$, and if $w|v$ for $w \in M_K, v \in M_\kappa$, then K_w contains κ_v with

$$n_w = [K_w : \kappa_v] n_v,$$

and hence

$$\sum_{w|v} \frac{n_w}{n_v} = \sum_{w|v} [K_w : \kappa_v] = [K : \kappa]. \tag{2.18}$$

When $v \in M_\kappa^0$, we let $w_1, \ldots, w_g$ be all extensions of v to K. Therefore, by the uniqueness of the extension of ord_v on κ_v to K_{w_i}, for $x \in K$ we have

$$\left|\mathbf{N}_{K_{w_i}/\kappa_v}(x)\right|_v = |x|_{w_i}^{n_{w_i}} = \|x\|_{w_i}. \tag{2.19}$$

If we multiply the relations (2.19) for all valuations w_i dividing v, it follows from Proposition 1.116 that

$$\left|\mathbf{N}_{K/\kappa}(x)\right|_v = \prod_{i=1}^{g} \left|\mathbf{N}_{K_{w_i}/\kappa_v}(x)\right|_v = \prod_{i=1}^{g} \|x\|_{w_i}. \tag{2.20}$$

When $v \in M_\kappa^\infty$, we verify the formula (2.20) also holds. Suppose first that v is a complex infinite prime of κ, σ is an embedding of κ into $\mathbb{C}$ such that

$$|x|_v = |\sigma(x)|_\infty,$$

where $|\cdot|_\infty$ is the ordinary absolute value of $\mathbb{C}$. Let $\sigma_1, \ldots, \sigma_g$ be all extensions of σ to embeddings of K into $\mathbb{C}$. Then for $x \in K$,

$$\prod_{i=1}^{g} |x|_{\sigma_i} = \prod_{i=1}^{g} |\sigma_i(x)|_\infty = \left|\sigma\left(\mathbf{N}_{K/\kappa}(x)\right)\right|_\infty = \left|\mathbf{N}_{K/\kappa}(x)\right|_v.$$

Now suppose that v is a real infinite prime of κ and σ the embedding κ into $\mathbb{R}$ such that

$$|x|_v = |\sigma(x)|_\infty,$$

where $|\cdot|_\infty$ is the ordinary absolute value of $\mathbb{R}$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be all extensions of σ that map K into $\mathbb{R}$ and Let σ_{r_1+j}, $\overline{\sigma}_{r_1+j}$ $(1 \le j \le r_2)$ be the conjugate pairs of embeddings of K into $\mathbb{C}$ Then for $x \in K$,

$$\begin{aligned}
\prod_{i=1}^{r_1+r_2} \|x\|_{\sigma_i} &= \left(\prod_{i=1}^{r_1} |\sigma_i(x)|_\infty\right)\left(\prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|_\infty^2\right) \\
&= \left(\prod_{i=1}^{r_1} |\sigma_i(x)|_\infty\right)\left(\prod_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)|_\infty |\overline{\sigma}_i(x)|_\infty\right) \\
&= \left|\sigma\left(\mathbf{N}_{K/\kappa}(x)\right)\right|_\infty = \left|\mathbf{N}_{K/\kappa}(x)\right|_v.
\end{aligned}$$

2.2.3 Galois extensions of number fields

Let κ be an algebraic number field, v a place of κ which corresponds to a prime ideal $\mathfrak{p} = \mathfrak{p}_v$ of the ring of algebraic integers in κ, and K a finite dimensional Galois extension of κ. Let $w_1, \ldots, w_g$ be the places of K extending v, with corresponding prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$, respectively, that is, each $\mathfrak{P}_i$ divides $\mathfrak{p}$, and so we may write

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e, \tag{2.21}$$

where $e = e_{\mathfrak{P}_i/\mathfrak{p}}$ is the ramification index.

Take an element $\sigma \in G_{K/\kappa}$. We write the action of σ on w_i as $\sigma(w_i)$. In case v is a finite place, we may identify

$$\sigma(w_i) \cong \sigma(\mathfrak{P}_i) = \{\sigma(x) \mid x \in \mathfrak{P}_i\}.$$

If w_i is an infinite place corresponding to an embedding σ_i of K into either $\mathbb{R}$ or $\mathbb{C}$, then $\sigma(w_i)$ is the place corresponding to the embedding $\sigma_i \circ \sigma^{-1}$. The Galois group $G_{K/\kappa}$ permutes the w_i transitively. We have seen this from Theorem 1.78 for the case of finite places. For infinite places this is an immediate consequence of the description of the infinite places in one-to-one correspondence with the embeddings of K into $\mathbb{R}$ and pairs of conjugate embeddings of K into $\mathbb{C}$. We set

$$D_{w_i} = D_{\mathfrak{P}_i} = \{\sigma \in G_{K/\kappa} \mid \sigma(w_i) = w_i\},$$

and call D_{w_i} the *decomposition group* of w_i.

Theorem 2.16. *Let w be an extension in K of the place v of κ and let D_w be the decomposition group of w in the Galois group $G_{K/\kappa}$. Then K_w is a Galois extension of κ_v with Galois group D_w.*

Proof. See G. J. Janusz [119], Theorem 1.2 in Chapter III. □

Now we assume that v is a finite place of κ. Let w be a place of K extending v, with corresponding prime ideal $\mathfrak{P}$. For $\sigma \in D_w$ we have $\sigma(\mathfrak{P}) = \mathfrak{P}$ and so σ induces an automorphism $\bar{\sigma}$ of $\mathcal{O}_K/\mathfrak{P}$ by the rule

$$\bar{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}, \;\; x \in \mathcal{O}_K.$$

Then $\bar{\sigma}$ is in the Galois group of $\mathcal{O}_K/\mathfrak{P}(\cong \mathbb{F}_w(K))$ over $\mathcal{O}_\kappa/\mathfrak{p}(\cong \mathbb{F}_v(\kappa))$. The correspondence $\sigma \mapsto \bar{\sigma}$ is a homomorphism of D_w into the Galois group $G_{\mathbb{F}_w(K)/\mathbb{F}_v(\kappa)}$. The kernel of this homomorphism is called the *inertia group* of w and is denoted as I_w or $I_\mathfrak{P}$.

Theorem 2.17. *Let v be a finite place of κ corresponding a prime ideal $\mathfrak{p}$. Let w be a place of K extending v, with corresponding prime ideal $\mathfrak{P}$.*

(1) *The correspondence $\sigma \mapsto \bar{\sigma}$ maps D_w onto the Galois group $G_{\mathbb{F}_w(K)/\mathbb{F}_v(\kappa)}$.*

(2) *The order of the inertia group I_w equals ramification index $e_{\mathfrak{P}/\mathfrak{p}}$.*

(3) *The subfield $F(I_w)$ of the completion K_w left fixed elementwise by the inertia group I_w is an unramified extension of κ_v of dimension $f_{\mathfrak{P}/\mathfrak{p}}$.*

(4) *The extension $K_w/F(I_w)$ is totally ramified with dimension $e_{\mathfrak{P}/\mathfrak{p}}$.*

Proof. See G. J. Janusz [119], Theorem 1.4 in Chapter III. □

2.3 Discriminant of number fields

Let κ be a finite extension of degree n over $\mathbb{Q}$. Let $\mathcal{O}_\kappa$ be the integral closure of $\mathbb{Z}$ in κ.

Theorem 2.18. *There are n elements $w_1, \ldots, w_n$ in $\mathcal{O}_\kappa$ such that if the x_i run through all elements of $\mathbb{Z}$ in the expression*

$$\beta = x_1 w_1 + x_2 w_2 + \cdots + x_n w_n,$$

we obtain each element in $\mathcal{O}_\kappa$ exactly once, that is, $w_1, \ldots, w_n$ is a basis of $\mathcal{O}_\kappa$.

Proof. By the assumption, then there exists an element $\alpha \in \kappa$ such that $\kappa = \mathbb{Q}[\alpha]$. By Proposition 1.60, we may assume that α is integral over $\mathbb{Z}$. We first investigate those elements ρ of $\mathcal{O}_\kappa$ which have a representation in the form

$$\rho = g(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

with coefficients $c_i \in \mathbb{Q}$. The c's can be determined from the n conjugate equations

$$\rho^{(i)} = g\big(\alpha^{(i)}\big), \;\; i = 1, \ldots, n,$$

where $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are conjugates of α, since the van der Monde determinant

$$\Delta = \begin{vmatrix} 1 & \alpha^{(1)} & \cdots & \big(\alpha^{(1)}\big)^{n-1} \\ 1 & \alpha^{(2)} & \cdots & \big(\alpha^{(2)}\big)^{n-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha^{(n)} & \cdots & \big(\alpha^{(n)}\big)^{n-1} \end{vmatrix} = \prod_{i>j} \big(\alpha^{(i)} - \alpha^{(j)}\big) \neq 0.$$

The solution yields Δc_j equal to a determinant, among whose elements only the $\rho^{(i)}$ and the powers of the $\alpha^{(i)}$ occur. In any case this determinant is an integral element a_j over $\mathbb{Z}$, since α and ρ are integral over $\mathbb{Z}$. However,

$$c_j = \frac{a_j}{\Delta} = \frac{x_j}{\Delta^2}$$

implies that $x_j = a_j\Delta = \Delta^2 c_j$ is an integer in $\mathbb{Z}$, because it is integral over $\mathbb{Z}$ since a_j and Δ are integral, and rational since Δ^2 and c_j are rational. The system of all elements

$$\beta = x_1\frac{1}{\Delta^2} + x_2\frac{\alpha}{\Delta^2} + \cdots + x_n\frac{\alpha^{n-1}}{\Delta^2},$$

where $x_j \in \mathbb{Z}$, containing all elements of $\mathcal{O}_\kappa$, forms a (torsion-free) Abelian group (with composition by addition) with a basis of n elements namely $1/\Delta^2, \alpha/\Delta^2, \ldots, \alpha^{n-1}/\Delta^2$. Hence by Theorem 1.4, the subgroup $\mathcal{O}_\kappa$ contained in this group likewise has a basis. By Theorem 1.9, this subgroup $\mathcal{O}_\kappa$ is of finite index since $\Delta^2\beta$ (that is, in the sense of group theory: the Δ^2-th power of each element) is obviously integral over $\mathbb{Z}$, and belongs to the subgroup $\mathcal{O}_\kappa$. Consequently, by Theorem 1.5, the basis of $\mathcal{O}_\kappa$ also consists of n elements, say $w_1, \ldots, w_n$. By Theorem 1.7, one can obtain all system of bases $w'_1, \ldots, w'_n$ of $\mathcal{O}_\kappa$ in the form

$$w'_i = \sum_{j=1}^{n} b_{ij}w_j, \;\; i = 1, \ldots, n,$$

with rational integers $b_{ij} \in \mathbb{Z}$, whose determinant is ± 1. Consequently

$$D_{\kappa/\mathbb{Q}} = D_{\kappa/\mathbb{Q}}(w_1, \ldots, w_n)$$

is independent of the choice of basis and is determined completely by the field itself. Since in any case the w_i represent 1, $\alpha, \ldots, \alpha^{n-1}$ by linear combinations, they form a fundamental system and consequently $D_{\kappa/\mathbb{Q}} \neq 0$. □

The nonzero rational integer $D_{\kappa/\mathbb{Q}}$ is called the *discriminant of field* κ.

Theorem 2.19. *Let* $\mathfrak{a}$ *is a nonzero ideal of* $\mathcal{O}_\kappa$. *If* $\alpha_1, \ldots, \alpha_n$ *is a basis for* $\mathfrak{a}$, *then*

$$\mathcal{N}(\mathfrak{a})^2 = \frac{D_{\kappa/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)}{D_{\kappa/\mathbb{Q}}}. \tag{2.22}$$

For a principal ideal $\mathfrak{a} = (\alpha)$, $\mathcal{N}(\mathfrak{a}) = |\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha)|$.

Proof. let $w_1, \ldots, w_n$ be a basis for $\mathcal{O}_\kappa$. Then there exists a system of equations

$$\alpha_i = \sum_{j=1}^{n} c_{ij}w_j, \;\; i = 1, 2, \ldots, n,$$

with rational integers $c_{ij} \in \mathbb{Z}$, and by Theorem 1.8 the absolute value of the determinant $\det(c_{ij})$ is equal to the index $\mathcal{N}(\mathfrak{a})$. On the other hand, by passage to the conjugates

$$D_{\kappa/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \{\det(c_{ij})\}^2 D_{\kappa/\mathbb{Q}}(w_1, \ldots, w_n),$$

and since

$$D_{\kappa/\mathbb{Q}}(w_1, \dots, w_n) = D_{\kappa/\mathbb{Q}} \neq 0,$$

we thus obtain the relation (2.22). With a principal ideal (α) we obviously obtain a basis of the form $\alpha w_1, \dots, \alpha w_n$. Thus

$$D_{\kappa/\mathbb{Q}}(\alpha w_1, \dots, \alpha w_n) = \mathbf{N}_{\kappa/\mathbb{Q}}(\alpha)^2 D_{\kappa/\mathbb{Q}}(w_1, \dots, w_n),$$

that is, $\mathcal{N}(\mathfrak{a}) = |\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha)|$. □

Further, we turn to fractional ideals of $\mathcal{O}_\kappa$. The following properties are basic:

Proposition 2.20. **(i)** *Each fractional ideal $\mathfrak{g} \neq (0)$ of $\mathcal{O}_\kappa$ can be made into a principal integral ideal by multiplication by an appropriate integral ideal.*

(ii) *If three fractional ideals $\mathfrak{g}$, $\mathfrak{x}$, and $\mathfrak{y}$ satisfy $\mathfrak{g} \neq (0)$, $\mathfrak{gx} = \mathfrak{gy}$, then $\mathfrak{x} = \mathfrak{y}$.*

(iii) *If $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are two fractional ideals, $\mathfrak{g}_1 \neq (0)$, then there is exactly one fractional ideal $\mathfrak{x}$ such that $\mathfrak{g}_1\mathfrak{x} = \mathfrak{g}_2$. One writes $\mathfrak{x} = \frac{\mathfrak{g}_2}{\mathfrak{g}_1}$ or $\mathfrak{x} = \mathfrak{g}_2\mathfrak{g}_1^{-1}$, and calls $\mathfrak{x}$ the quotient of $\mathfrak{g}_2$ and $\mathfrak{g}_1$.*

(iv) *The equation $\mathfrak{a}/\mathfrak{b} = \mathfrak{c}/\mathfrak{d}$ of fractional ideals is equivalent to $\mathfrak{ad} = \mathfrak{bc}$; in particular for each fractional ideal $\mathfrak{m} \neq (0)$,*

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\mathfrak{am}}{\mathfrak{bm}}, \quad \frac{\mathfrak{a}}{(1)} = \mathfrak{a}, \quad \frac{\mathfrak{m}}{\mathfrak{m}} = (1).$$

(v) *An integral element $a \in \mathcal{O}_\kappa$ occurs in an fractional ideal $\mathfrak{g}$ if and only if there is an integral ideal $\mathfrak{m}$ such that (a) has a decomposition $(a) = \mathfrak{mg}$, in particular, 1 occurs in all ideals which are the reciprocals $1/\mathfrak{m}$ of integral ideals $\mathfrak{m}$, and only in such ideals.*

Proof. Since $\omega\mathfrak{g}$ is an integral ideal $\mathfrak{a}$, hence there is an integral ideal $\mathfrak{b}$ different from (0) such that $\mathfrak{ab}$ is a principal ideal. Thus $\omega\mathfrak{bg}$ is principal, and (i) follows.

The proof of (ii) is word for word the same as for Proposition 2.4, (2).

To show (iii), let us choose $\mathfrak{a} \neq (0)$ so that $\mathfrak{ag}_1 = (\alpha)$ is a principal ideal; thus $(\alpha) \neq 0$. If $\mathfrak{ag}_2 = (\rho_1, \dots, \rho_r)$, we set

$$\mathfrak{x} = \left(\frac{\rho_1}{\alpha}, \dots, \frac{\rho_r}{\alpha}\right).$$

Then in fact

$$\mathfrak{ag}_2 = (\alpha)\mathfrak{x} = \mathfrak{ag}_1\mathfrak{x}, \quad \mathfrak{g}_2 = \mathfrak{g}_1\mathfrak{x},$$

and by what has been said before, $\mathfrak{x}$ is uniquely determined.

The cases (iv) and (v) are trivial. □

Since each fractional ideal $\mathfrak{g}$ of $\mathcal{O}_\kappa$ can be represented as the quotient $\mathfrak{a}/\mathfrak{b}$ of two relatively prime integral ideals $\mathfrak{a}$ and $\mathfrak{b}$, then we define the *norm of* $\mathfrak{g}$:

$$\mathcal{N}(\mathfrak{g}) = \frac{\mathcal{N}(\mathfrak{a})}{\mathcal{N}(\mathfrak{b})}.$$

This equation is also correct if $\mathfrak{a}$, $\mathfrak{b}$ are not relatively prime or if they are fractional ideals. Again for two fractional ideal $\mathfrak{g}_1$ and $\mathfrak{g}_2$, we have

$$\mathcal{N}(\mathfrak{g}_1\mathfrak{g}_2) = \mathcal{N}(\mathfrak{g}_1)\mathcal{N}(\mathfrak{g}_2).$$

Between the basis and the norm there is again the relationship: If $\beta_1, \ldots, \beta_n$ is a basis for a fractional ideal $\mathfrak{g}$, then

$$D_{\kappa/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \mathcal{N}(\mathfrak{g})^2 D_{\kappa/\mathbb{Q}}. \tag{2.23}$$

To prove this choose an nonzero integral element $\omega \in \mathcal{O}_\kappa$ so that $\omega\mathfrak{g}$ is an integral ideal in $\mathcal{O}_\kappa$ with basis $\omega\beta_1, \ldots, \omega\beta_n$. Then by using (2.23), we have

$$\mathcal{N}(\mathfrak{g})^2 = \frac{\mathcal{N}(\omega\mathfrak{g})^2}{\mathcal{N}(\omega)^2} = \frac{D_{\kappa/\mathbb{Q}}(\omega\beta_1, \ldots, \omega\beta_n)}{\mathbf{N}_{\kappa/\mathbb{Q}}(\omega)^2 D_{\kappa/\mathbb{Q}}} = \frac{D_{\kappa/\mathbb{Q}}(\beta_1, \ldots, \beta_n)}{D_{\kappa/\mathbb{Q}}}.$$

2.4 Minkowski's geometry of numbers

2.4.1 Minkowski's first theorem

Let Λ be a subset of $\mathbb{R}^n$ such that Λ is a module over $\mathbb{Z}$. Further, we assume that Λ is *discrete*, that is, every point $\omega \in \Lambda$ is an isolated point in the sense that there exists a neighborhood which contains no other points of Λ.

Proposition 2.21. *If $\Lambda \subset \mathbb{R}^n$ is a discrete module over $\mathbb{Z}$, then it follows that either $\Lambda = \{0\}$, or*

$$\Lambda = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_m$$

with linearly independent vectors $\omega_1, \ldots, \omega_m$ of $\mathbb{R}^n$.

Proof. The case $\Lambda = \{0\}$ is trivially a discrete module over $\mathbb{Z}$. Next we assume that the discrete module Λ over $\mathbb{Z}$ contains non-zero elements. First of all, we claim that Λ is closed. In fact, note that if U is an arbitrary neighborhood of 0, then there exists a neighborhood $U_0 \subseteq U$ of 0 such that every difference of elements of U_0 lies in U. Thus if there were an $x \notin \Lambda$ belonging to the closure of Λ, then we could find in the neighborhood $x + U_0$ of x two distinct elements $\omega, \omega' \in \Lambda$, so that

$$0 \neq \omega - \omega' \in U_0 \subseteq U.$$

Thus 0 would not be an isolated point, a contradiction.

Next we consider the linear subspace V of $\mathbb{R}^n$ which is spanned by the set Λ. Let m be the dimension of V. Then we may choose a basis $v_1, \ldots, v_m$ of V which is contained in Λ, and so form the discrete module

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m \subseteq \Lambda$$

of V over $\mathbb{Z}$. We claim that the index j of Γ in Λ is finite. To see this, let $\lambda_i \in \Lambda$ vary over a system of representatives of the cosets in Λ/Γ. Since the translates $\gamma + \mathcal{P}_\Gamma,\ \gamma \in \Gamma$, of the *fundamental mesh*

$$\mathcal{P}_\Gamma = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R},\ 0 \leq x_i < 1\} \tag{2.24}$$

cover the space V, we may write

$$\lambda_i = \gamma_i + \xi_i,\ \ \gamma_i \in \Gamma,\ \xi_i \in \mathcal{P}_\Gamma.$$

Since $\xi_i = \lambda_i - \gamma_i \in \Lambda$ lie discretely in the bounded set $\mathcal{P}_\Gamma$, they have to be finite in number.

Therefore, we have $j\Lambda \subseteq \Gamma$ by Theorem 1.2, whence

$$\Lambda \subseteq \frac{1}{j}\Gamma = \mathbb{Z}\frac{v_1}{j} + \cdots + \mathbb{Z}\frac{v_m}{j}.$$

By the main theorem on finitely generated Abelian groups, hence Λ admits a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_m$, i.e.,

$$\Lambda = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_m.$$

The vectors $\omega_1, \ldots, \omega_m$ are also $\mathbb{R}$-linearly independent because they span the space V of dimension m. This completes the proof of Proposition 2.21. □

If $m = n$ in Proposition 2.21, then Λ is called a (*full* or *complete*) *lattice* in $\mathbb{R}^n$. This case is obviously tantamount to the fact that the set of all translates $\omega + \mathcal{P}_\Lambda,\ \omega \in \Lambda$, of the fundamental mesh $\mathcal{P}_\Lambda$ covers the space $\mathbb{R}^n$. It also is known that a discrete module $\Lambda \subset \mathbb{R}^n$ over $\mathbb{Z}$ is a lattice if and only if the quotient group $\mathbb{R}^n/\Lambda$ is compact (in the natural topology).

The Euclidean space $\mathbb{R}^n$ is equipped with a symmetric, positive definite bilinear form

$$\langle\, , \rangle : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R},$$

and so has a notion of volume – more precisely a Haar measure. By the volume of a subset $C \subset \mathbb{R}^n$ we mean the Riemann integral of the characteristic function of C. The cube spanned by an orthonormal basis $e_1, \ldots, e_n$ has volume 1, and more generally, the parallelepiped spanned by n linearly independent vectors $\omega_1, \ldots, \omega_n$,

$$\mathcal{P} = \{x_1\omega_1 + \cdots + x_n\omega_n \mid x_i \in \mathbb{R},\ \ 0 \leq x_i < 1\}$$

has volume

$$V(\mathcal{P}) = |\det(a_{ij})|,$$

where (a_{ij}) is the matrix of the base change from $e_1, \dots, e_n$ to $\omega_1, \dots, \omega_n$, so that

$$\omega_i = \sum_{j=1}^{n} a_{ij} e_j.$$

Note that

$$(\langle \omega_i, \omega_j \rangle) = \left(\sum_{k,l} a_{ik} a_{jl} \langle e_k, e_l \rangle \right) = \left(\sum_{k=1}^{n} a_{ik} a_{jk} \right) = (a_{ij}) \cdot {}^t(a_{ij}).$$

We also have the invariant notation

$$V(\mathcal{P}) = \sqrt{|\det(\langle \omega_i, \omega_j \rangle)|}.$$

Let Λ be the lattice spanned by $\omega_1, \dots, \omega_n$. Then $\mathcal{P}$ is just the fundamental mesh of Λ, and we define the *volume* of Λ as follows:

$$V(\Lambda) = V(\mathbb{R}^n/\Lambda) := V(\mathcal{P}).$$

This does not depend on the choice of a basis $\omega_1, \dots, \omega_n$ of the lattice because the transition matrix passing to a different basis, as well as its inverse, has integer coefficients, and therefore has determinant ± 1 so that the set $\mathcal{P}$ is transformed into a set of the same volume.

A *convex body* means a compact convex set C in a space $\mathbb{R}^n$ of n dimensions, *symmetric about* 0 (i.e., $\mathbf{x} \in C$ implies $-\mathbf{x} \in C$), and such that 0 lies in the interior of C, where the *convex set* means that for any two points $\mathbf{x}, \mathbf{y} \in C$, the whole line segment

$$\{t\mathbf{y} + (1-t)\mathbf{x} \mid 0 \le t \le 1\}$$

joining $\mathbf{x}$ with $\mathbf{y}$ is contained in C. Minkowski [184], [185] studied properties of a convex body C in $\mathbb{R}^n$ with respect to the lattice $\mathbb{Z}^n$. It can be proved that every convex body has a volume, and so we may suppose that this body C has the volume $V(C)$. Then *Minkowski's first theorem* states as follows:

Theorem 2.22. *If $V(C) \ge 2^n V(\Lambda)$, then C contains at least one (and so at least two) lattice points in Λ different from 0.*

Proof. See Minkowski [184], [185]; Rogers and Swinnerton-Dyer [221]; Neukirch [202], Chapter I, Theorem 4.4; and Schmidt [231], Chapter II, Theorem 2B. □

By considering the cube of $\mathbf{x}$ with $|x_i| \le 1$ $(i = 1, \dots, n)$ we see that Minkowski's first theorem is best possible.

Theorem 2.23. *Assume that there exist n homogeneous linear expressions*

$$L_i(\mathbf{x}) = \sum_{j=1}^{n} a_{ij}x_j, \;\; i = 1, 2, \ldots, n,$$

with real coefficients a_{ij}, whose determinant $\det(a_{ij})$ is different from zero, as well as n positive quantities $r_1, \ldots, r_n$, for which

$$r_1 r_2 \cdots r_n \geq |\det(a_{ij})|. \tag{2.25}$$

Then there are always n rational integer $x_1, \ldots, x_n$, not all equal to 0, such that

$$|L_i(\mathbf{x})| \leq r_i, \;\; i = 1, 2, \ldots, n. \tag{2.26}$$

Proof. We consider the lattice

$$\Lambda = \{(m_1, \ldots, m_n) \in \mathbb{R}^n \mid m_i \in \mathbb{Z}, \; 1 \leq i \leq n\}$$

with the volume $V(\Lambda) = 1$, and study the convex body

$$C = \{\mathbf{x} \in \mathbb{R}^n \mid |L_i(\mathbf{x})| \leq r_i, \; i = 1, 2, \ldots, n\}.$$

We find easily the volume

$$\begin{aligned} V(C) &= \int_C dx_1 \cdots dx_n = \frac{1}{|\det(a_{ij})|} \int_{|y_i| \leq r_i} dy_1 \cdots dy_n \\ &= \frac{2^n r_1 r_2 \cdots r_n}{|\det(a_{ij})|}. \end{aligned}$$

Thus the condition (2.25) is equivalent to $V(C) \geq 2^n V(\Lambda)$, and so Theorem 2.23 follows from Theorem 2.22. □

Theorem 2.24. *Assume that there exist n linear forms*

$$L_i(\mathbf{x}) = \sum_{j=1}^{n} a_{ij}x_j, \;\; i = 1, 2, \ldots, n,$$

with real or complex coefficients a_{ij}, whose determinant $\det(a_{ij})$ is different from zero, as well as n positive quantities $r_1, \ldots, r_n$, for which

$$r_1 r_2 \cdots r_n \geq |\det(a_{ij})|. \tag{2.27}$$

Moreover if $L_\alpha(\mathbf{x})$ is not real for some $\alpha \in \{1, \ldots, n\}$, we assume that there exist some $\beta \in \{1, \ldots, n\}$ such that $L_\beta(\mathbf{x})$ is the complex conjugate $\overline{L_\alpha(\mathbf{x})}$ of $L_\alpha(\mathbf{x})$, and such that $r_\alpha = r_\beta$. Then there are always n rational integer $x_1, \ldots, x_n$, not all equal to 0, such that

$$|L_i(\mathbf{x})| \leq r_i, \;\; i = 1, 2, \ldots, n. \tag{2.28}$$

Proof. We consider a new system $L_i'(\mathbf{x})$ induced from $L_i(\mathbf{x})$. We take $L_i'(\mathbf{x}) = L_i(\mathbf{x})$ if $L_i(\mathbf{x})$ is a real form; on the other hand if $L_\alpha(\mathbf{x})$ and $L_\beta(\mathbf{x})$ are complex conjugate and, say, $\alpha < \beta$, then we set

$$L'_\alpha(\mathbf{x}) = \frac{L_\alpha(\mathbf{x}) + L_\beta(\mathbf{x})}{2}, \quad L'_\beta(\mathbf{x}) = \frac{L_\alpha(\mathbf{x}) - L_\beta(\mathbf{x})}{2\sqrt{-1}}.$$

In the latter case we define

$$r'_\alpha = r'_\beta = \frac{r_\alpha}{\sqrt{2}},$$

and, on the other hand, set $r'_i = r_i$ in the first case.

The system of real forms L' now obviously has a determinant D' with

$$|D'| = 2^{-r_2} |\det(a_{ij})|,$$

where r_2 denote the number of pairs of complex conjugate forms among the $L_i(\mathbf{x})$. Hence since

$$r'_1 r'_2 \cdots r'_n \geq |D'|,$$

there are rational integers $x_1, \ldots, x_n$, which are not all 0, such that

$$|L'_i(\mathbf{x})| \leq r'_i, \;\; i = 1, 2, \ldots, n.$$

For a nonreal form $L_\alpha(\mathbf{x})$ we now have

$$|L_\alpha(\mathbf{x})|^2 = L'_\alpha(\mathbf{x})^2 + L'_\beta(\mathbf{x})^2 \leq (r'_\alpha)^2 + (r'_\beta)^2 = r_\alpha^2$$

from which Theorem 2.24 follows. □

2.4.2 Minkowski's bound

We consider the exact sequence (1.10):

$$1 \to \mathrm{Ker}(\vartheta) \to \kappa_* \xrightarrow{\vartheta} \mathfrak{I}_A \to I_A \to 1.$$

For Dedekind domains that arise in number theory, there are classical theorems relating to the ideal class groups I_A and $\mathrm{Ker}(\vartheta)$.

Let κ be an algebraic number field of degree n over $\mathbb{Q}$ and let A be its ring of algebraic integers $\mathcal{O}_\kappa$, which is a Dedekind domain by Theorem 2.1. Then there are n distinct embeddings $\kappa \longrightarrow \mathbb{C}$. Of these, say r_1 map κ into $\mathbb{R}$, and rest pair off (if $\sigma : \kappa \longrightarrow \mathbb{C}$ is one, then $\bar{\sigma}$ is another defined by $\bar{\sigma}(z) = \overline{\sigma(z)}$) into, say, r_2 pairs: thus $r_1 + 2r_2 = n$. We have the following *Minkowski's bound*:

Theorem 2.25. *For any nonzero fractional ideal* $\mathfrak{g}$ *of* $\mathcal{O}_\kappa$*, there is an* $\mathfrak{a} \in [\mathfrak{g}]$ *such that* $\mathfrak{a} \subseteq \mathcal{O}_\kappa$ *and*

$$\mathcal{N}(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |D_{\kappa/\mathbb{Q}}|^{1/2}.$$

Proof. See [119], Chapter I, Theorem 13.7. □

Theorem 2.25 implies easily that $I_{\mathcal{O}_\kappa}$ is a finite group. Its order $\mathbf{h}$ is called the *class number* of the field κ.

Theorem 2.26. *In each ideal class of κ, there is an integral ideal whose norm is $\leq \sqrt{|D_{\kappa/\mathbb{Q}}|}$. Thus the number $\mathbf{h}$ of ideal classes in κ is finite. The $\mathbf{h}$-th power of each ideal of $\mathcal{O}_\kappa$ is a principal ideal.*

Proof. Each ideal class of κ contains an integral ideal $\mathfrak{a}$ with

$$\mathcal{N}(\mathfrak{a}) \leq B \leq \sqrt{|D_{\kappa/\mathbb{Q}}|}$$

with B given in Theorem 2.25. It is sufficient to prove there exist only a finite number of integral ideals with norm below the fixed bound. Write

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r},$$

where $\mathfrak{p}_i$ are distinct primes, and the a_i are positive integers. Let $p_i\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}_i$, p_i a positive prime integer. By the relation (2.3), we find

$$\mathcal{N}(\mathfrak{a}) = \prod_{i=1}^{r} p_i^{a_i f_{\mathfrak{p}_i/\mathbb{Z}}} \leq B.$$

Since each $p_i \leq B$, only a finite number of p_i can appear. Thus there exist only a finite number of possible $\mathfrak{p}_i$ since each p_j is divisible by only a finite number of $\mathfrak{p}_i$. Finally only a finite number of exponents a_i are possible because $p_i^{a_i f_{\mathfrak{p}_i/\mathbb{Z}}} \leq B$. Hence only a finite number of ideals $\mathfrak{a}$ can satisfy $\mathcal{N}(\mathfrak{a}) \leq B$. Thus every ideal class is represented by one of a finite number of ideals and $I_{\mathcal{O}_\kappa}$ is finite. By Theorem 1.2, the $\mathbf{h}$-th power of each ideal of $\mathcal{O}_\kappa$ is a principal ideal.

See E. Hecke [95], Theorems 96 and 97; or [119], Chapter I, Theorem 13.8. □

Theorem 2.27. *If $\mathfrak{g}$ is an fractional ideal of $\mathcal{O}_\kappa$, then one has*

$$\mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{g}) = (\mathcal{N}(\mathfrak{g})).$$

Proof. Let $\mathbf{h}$ be the class number of κ. Then $\mathfrak{g}^{\mathbf{h}} = (\beta)$, where β is a certain element in κ, and

$$\mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{g})^{\mathbf{h}} = \mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{g}^{\mathbf{h}}) = \mathbf{N}_{\kappa/\mathbb{Q}}((\beta)) = \left(\mathbf{N}_{\kappa/\mathbb{Q}}(\beta)\right).$$

Since

$$\pm\mathbf{N}_{\kappa/\mathbb{Q}}(\beta) = \mathcal{N}\left(\mathfrak{g}^{\mathbf{h}}\right) = \mathcal{N}\left(\mathfrak{g}\right)^{\mathbf{h}} = a^{\mathbf{h}},$$

where $a = \mathcal{N}\left(\mathfrak{g}\right)$, we have

$$\mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{g})^{\mathbf{h}} = (a)^{\mathbf{h}}, \quad \mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{g}) = (a),$$

and the theorem follows. □

We can obtain information about the size of the discriminant from Theorem 2.25.

Proposition 2.28. *The discriminant of an algebraic number field κ of degree n satisfies*

$$\sqrt{|D_{\kappa/\mathbb{Q}}|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}.$$

Proof. Every ideal of $\mathcal{O}_\kappa$ has norm at least one. It follows that

$$\sqrt{|D_{\kappa/\mathbb{Q}}|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{r_2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}.$$

See Neukirch [202], Chapter III, Proposition 2.14. □

Theorem 2.29 (Minkowski, 1890). $|D_{\kappa/\mathbb{Q}}| > 1$ *for a number field* $\kappa \neq \mathbb{Q}$.

Proof. Write

$$a_n = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}.$$

We compute

$$\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{\frac{1}{2}}\left(1+\frac{1}{n}\right)^n > 1$$

for every positive n, and so $a_{n+1} > a_n$. Since $a_2 > 1$, it follows that $|D_{\kappa/\mathbb{Q}}| > 1$ if $n \geq 2$.

See Neukirch [202], Chapter III, Theorem 2.17; Weil [298]. □

Proposition 2.28 immediately implies the following important result:

Theorem 2.30 (Hermite, 1863). *There are only finitely many algebraic number fields with a given discriminant.*

Proof. Neukirch [202], Chapter III, Theorem 2.16; Weil [298]. □

The following theorem shows that for any ideal $\mathfrak{a}$ in the ring $\mathcal{O}_\kappa$ of integers of a number field κ, we can find an extension number field $K \supseteq \kappa$ such that the extended ideal $\mathcal{O}_K\mathfrak{a}$ in $\mathcal{O}_K$ is principal (see [266]).

Theorem 2.31. *Let κ be a number field, $\mathfrak{a}$ an ideal in the ring of integers $\mathcal{O}_\kappa$ of κ. Then there exists an algebraic integer w such that the field $K = \kappa(w)$ satisfies*

(i) $\mathcal{O}_K w = \mathcal{O}_K\mathfrak{a}$;

(ii) $(\mathcal{O}_K w) \cap \mathcal{O}_\kappa = \mathfrak{a}$;

(iii) $(\bar{\mathbb{Z}}w) \cap \kappa = \mathfrak{a}$;

(iv) *If $\mathcal{O}u = \mathcal{O}\mathfrak{a}$ for any $u \in \bar{\mathbb{Z}}$, and any ring $\mathcal{O}$ of integers, then $u = \eta w$ where η is a unit of $\bar{\mathbb{Z}}$.*

Proof. By Theorem 2.26, $\mathfrak{a}^{\mathbf{h}}$ is principal, say $\mathfrak{a}^{\mathbf{h}} = (\beta)$. Let $w = \beta^{1/\mathbf{h}} \in \bar{\mathbb{Z}}$, and consider $K = \kappa(w)$. It is obvious that $w \in \mathcal{O}_K$, and

$$(\mathcal{O}_K\mathfrak{a})^{\mathbf{h}} = \mathcal{O}_K\mathfrak{a}^{\mathbf{h}} = \mathcal{O}_K\beta = \mathcal{O}_K w^{\mathbf{h}} = (\mathcal{O}_K w)^{\mathbf{h}}.$$

Uniqueness of factorization of ideals in $\mathcal{O}_K$ easily yields $\mathcal{O}_K\mathfrak{a} = \mathcal{O}_K w$, proving (i).

Since (iii) implies (ii), we only consider (iii). The inclusion $\mathfrak{a} \subseteq (\bar{\mathbb{Z}}w) \cap \kappa$ is straightforward. Conversely, if $x \in (\bar{\mathbb{Z}}w) \cap \kappa$, then there exists an element $\lambda \in \bar{\mathbb{Z}}$ such that $x = \lambda w \in \kappa$. Thus, we have $\lambda = xw^{-1} \in K$, and so $\lambda \in K \cap \bar{\mathbb{Z}} = \mathcal{O}_K$. This implies

$$x^{\mathbf{h}} = \lambda^{\mathbf{h}} w^{\mathbf{h}} = \lambda^{\mathbf{h}}\beta,$$

that is, $x^{\mathbf{h}} \in \bar{\mathbb{Z}}$, and so $x \in \bar{\mathbb{Z}}$. Hence $x \in \bar{\mathbb{Z}} \cap \kappa = \mathcal{O}_\kappa$. On other hand, we find $\lambda^{\mathbf{h}} = x^{\mathbf{h}}\beta^{-1} \in \kappa$, and so $\lambda^{\mathbf{h}} \in \bar{\mathbb{Z}} \cap \kappa = \mathcal{O}_\kappa$. Taking ideals in $\mathcal{O}_\kappa$ we get

$$(x)^{\mathbf{h}} = (\lambda^{\mathbf{h}})(\beta) = (\lambda^{\mathbf{h}})\mathfrak{a}^{\mathbf{h}}.$$

Unique factorization in $\mathcal{O}_\kappa$ implies $(\lambda^{\mathbf{h}}) = \mathfrak{b}^{\mathbf{h}}$ for some ideal $\mathfrak{b}$, and hence $(x)^{\mathbf{h}} = \mathfrak{b}^{\mathbf{h}}\mathfrak{a}^{\mathbf{h}}$, and unique factorization once more implies $(x) = \mathfrak{b}\mathfrak{a}$, whence $x \in \mathfrak{a}$, as required.

The proof of (iv) is found by noting that by the remark after Theorem 2.8, $\mathfrak{a} = (\omega, \alpha)$ for $\omega, \alpha \in \mathcal{O}_\kappa$, and substituting in (iv) gives $\mathcal{O}u = \mathcal{O}(\omega, \alpha)$. Thus

$$u = a\omega + b\alpha, \ \ \{a, b\} \subset \mathcal{O} \subseteq \bar{\mathbb{Z}}.$$

From (i), $\{\omega, \alpha\} \subset \mathcal{O}_K w$, and so

$$\omega = \xi w, \ \ \alpha = \zeta w, \ \ \{\xi, \zeta\} \subset \mathcal{O}_K \subseteq \bar{\mathbb{Z}}.$$

Hence

$$u = a\xi w + b\zeta w,$$

which means $w|u$ in $\bar{\mathbb{Z}}$. Interchanging the roles of u, w proves (iv). □

Actually, we can improve Theorem 2.31 by finding a single extension ring in which the extension of every ideal is principal.

Theorem 2.32. *Let κ be a number field. Then there exists a number field $K \supseteq \kappa$ such that for each ideal $\mathfrak{a}$ in the ring of integers $\mathcal{O}_\kappa$ of κ, we have*

(I) *$\mathcal{O}_K\mathfrak{a}$ is a principal ideal;*

(II) $(\mathcal{O}_K\mathfrak{a}) \cap \mathcal{O}_\kappa = \mathfrak{a}$.

Proof. Since $\mathbf{h}$ is finite, one can select a representative set of ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_{\mathbf{h}}$ from each class and choose algebraic integers $w_1, \ldots, w_{\mathbf{h}}$ such that $\mathcal{O}_{\kappa(w_i)}\mathfrak{a}_i$ is principal. Let $K = \kappa(w_1, \ldots, w_{\mathbf{h}})$, then $\mathcal{O}_{\kappa(w_i)} \subseteq \mathcal{O}_K$, and so each ideal $\mathcal{O}_K\mathfrak{a}_i$ is principal in

$\mathcal{O}_K$. Since every ideal $\mathfrak{a}$ in $\mathcal{O}_\kappa$ is equivalent to some $\mathfrak{a}_i$, then it is easily to show that $\mathcal{O}_K\mathfrak{a}$ also is principal, say

$$\mathcal{O}_K\mathfrak{a} = \mathcal{O}_K u, \ \ u \in \bar{\mathbb{Z}}.$$

This proves (I).

Clearly $\mathfrak{a} \subseteq (\mathcal{O}_K\mathfrak{a}) \cap \mathcal{O}_\kappa$. For the converse inclusion, Theorem 2.31 (iv) implies $u = \eta w$ for a unit η in $\bar{\mathbb{Z}}$. Hence

$$(\mathcal{O}_K\mathfrak{a}) \cap \mathcal{O}_\kappa = (\mathcal{O}_K u) \cap \mathcal{O}_\kappa \subseteq (\bar{\mathbb{Z}}u) \cap \kappa = (\bar{\mathbb{Z}}w) \cap \kappa = \mathfrak{a}$$

by Theorem 2.31 (iii). □

2.4.3 Dirichlet's unit theorem

We continue to consider the exact sequence (1.10):

$$1 \to \mathrm{Ker}(\vartheta) \to \kappa_* \xrightarrow{\vartheta} \mathfrak{I}_A \to I_A \to 1$$

in which $A = \mathcal{O}_\kappa$ is the ring of algebraic integers in an algebraic number field κ of degree n. Then

$$\mathbf{U} = \mathbf{U}_\kappa = \mathrm{Ker}(\vartheta)$$

is just the group of units of $\mathcal{O}_\kappa$. The set H of all roots of unity in κ, which contains at least two elements, namely ± 1, is contained as a subgroup in $\mathbf{U}$.

Theorem 2.33. *The group H of all roots of unity in κ is finite, and indeed it is a cyclic group of order $w \geq 2$.*

Proof. See Hecke [95], Theorem 99. □

The quotient $\mathbf{U}/H$ is torsion-free. We will find the number of generators of $\mathbf{U}/H$ below. Let $\sigma_1, \ldots, \sigma_{r_1}$ be r_1 distinct embeddings of κ into $\mathbb{R}$ and let $(\sigma_{r_1+i}, \bar{\sigma}_{r_1+i})$ $(1 \leq i \leq r_2)$ be r_2 pairs of conjugate embeddings of κ into $\mathbb{C}$ that are not into $\mathbb{R}$. Now consider the mapping $\sigma : \kappa \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ defined by

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)).$$

It is clear that σ is an additive mapping,

$$\sigma(x + y) = \sigma(x) + \sigma(y).$$

If we identify $\mathbb{C}$ with $\mathbb{R}^2$ by using the correspondence

$$\imath\left(x + \sqrt{-1}y\right) = (x, y) \in \mathbb{R}^2,$$

then σ induces a mapping $\sigma^* : \kappa \longrightarrow \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} = \mathbb{R}^n$ defined by

$$\sigma^*(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \imath \circ \sigma_{r_1+1}(x), \ldots, \imath \circ \sigma_{r_1+r_2}(x)).$$

Theorem 2.34. *Let $\mathfrak{a}$ be a nonzero ideal in the ring $\mathcal{O}_\kappa$ of algebraic integers in the algebraic number field κ. Then $\sigma^*(\mathfrak{a})$ is a lattice in $\mathbb{R}^n$ satisfying the relation:*

$$\mathcal{N}(\mathfrak{a})^2 D_{\kappa/\mathbb{Q}} = (-4)^{r_2} V(\sigma^*(\mathfrak{a}))^2.$$

Proof. See [119], Chapter I, Proposition 13.2, 13.4; Theorem 13.5. □

Next consider the homomorphism

$$\ell = (\ell_1, \ldots, \ell_{r_1+r_2}) : \kappa_* \longrightarrow \mathbb{R}^{r_1+r_2}$$

defined by

$$\ell_i(x) = \begin{cases} \log|\sigma_i(x)|, & \text{if } 1 \le i \le r_1, \\ \log|\sigma_i(x)|^2, & \text{if } r_1 < i \le r_1 + r_2. \end{cases}$$

It is obvious that $\ell_i(xy) = \ell_i(x) + \ell_i(y)$ and so

$$\ell(xy) = \ell(x) + \ell(y), \ \ \{x, y\} \subset \kappa_*.$$

Proposition 2.35. *The homomorphism ℓ maps the group $\mathbf{U}$ of units in the ring $\mathcal{O}_\kappa$ onto a lattice in the $r_1 + r_2 - 1$ dimensional subspace V of $\mathbb{R}^{r_1+r_2}$ consisting of all vectors $(x_1, \ldots, x_{r_1+r_2})$ with $\sum x_i = 0$.*

Proof. See [119], Chapter I, Proposition 13.10; 13.11. □

Let $\jmath : \mathbb{R}^{r_1+r_2} \longrightarrow \mathbb{R}^{r_1+r_2-1}$ be the projection defined by

$$\jmath(x_1, \ldots, x_{r_1+r_2}) = (x_1, \ldots, x_{r_1+r_2-1}).$$

We may choose units $\eta_1, \ldots, \eta_{r_1+r_2-1} \in \mathcal{O}_\kappa$ that satisfy the following conditions:

(a) $\ell_i(\eta_j) < 0$ if $i \ne j$;

(b) $\ell_1(\eta_j) + \cdots + \ell_{r_1+r_2-1}(\eta_j) > 0$ for $1 \le j \le r_1 + r_2 - 1$;

(c) $\ell_1(\eta_j) + \cdots + \ell_{r_1+r_2}(\eta_j) = 0$ for any j;

(d) The vectors $\jmath \circ \ell(\eta_j)$, $1 \le j \le r_1 + r_2 - 1$, are linearly independent over $\mathbb{R}$.

This means *Dirichlet's unit theorem*:

Theorem 2.36. *There are $r_1 + r_2$ units $\zeta, \eta_1, \ldots, \eta_{r_1+r_2-1}$, where ζ is a w-th root of unit, such that each unit of the number field κ is obtained exactly once in the form*

$$\varepsilon = \zeta^a \eta_1^{a_1} \cdots \eta_{r_1+r_2-1}^{a_{r_1+r_2-1}},$$

where $a_1, \ldots, a_{r_1+r_2-1}$ are all rational integers and a can only take the values $0, 1, \ldots, w-1$.

Proof. By Proposition 2.35, we know that $\ell(\mathbf{U})$ is a lattice in V. Hence there exist units $\eta_1, \ldots, \eta_{r_1+r_2-1}$ in $\mathbf{U}$ such that $\ell(\mathbf{U})$ have $\mathbb{Z}$ basis $\ell(\eta_1), \ldots, \ell(\eta_{r_1+r_2-1})$. For any unit $\varepsilon \in \mathbf{U}$ there exist unique integers a_i such that

$$\ell(\varepsilon) = \sum_{i=1}^{r_1+r_2-1} a_i \ell(\eta_i).$$

It follows that

$$\ell\left(\varepsilon \prod_{i=1}^{r_1+r_2-1} \eta_i^{-a_i}\right) = 0$$

since ℓ is a homomorphism. The proof will be complete if we prove that $\ell(u) = 0$ for a unit u implies that u is a root of unity. We have $\ell(u) = 0$ if and only if $|\sigma_i(u)| = 1$ for all i. Thus

$$\sigma(u) = (\sigma_1(u), \ldots, \sigma_{r_1+r_2}(u))$$

lies in a bounded subset of the lattice $\sigma(\mathcal{O}_\kappa)$ in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. A bounded subset of the lattice contains only a finite number of points in the lattice so there are only a finite number of possible u. Thus the kernel of ℓ is a finite subgroup of the multiplicative group of a field and so it is a cyclic group. □

The $r_1 + r_2 - 1$ units $\eta_1, \ldots, \eta_{r_1+r_2-1}$ are called *fundamental units* of the field κ. Let $\mathcal{P}$ be the fundamental mesh of the unit lattice $\ell(\mathbf{U})$, spanned by the vectors $\ell(\eta_1), \ldots, \ell(\eta_{r_1+r_2-1}) \in V$. The vector

$$\epsilon = \frac{1}{\sqrt{r_1 + r_2}}(1, \ldots, 1) \in \mathbb{R}^{r_1+r_2}$$

is obviously orthogonal to V and has length 1. The $(r_1 + r_2 - 1)$-dimensional volume of $\mathcal{P}$ therefore equals the $(r_1 + r_2)$-dimensional volume of the parallelepiped spanned by $\epsilon, \ell(\eta_1), \ldots, \ell(\eta_{r_1+r_2-1})$ in $\mathbb{R}^{r_1+r_2}$. But this has volume

$$\pm \begin{vmatrix} \ell_1(\eta_1) & \cdots & \ell_{r_1+r_2}(\eta_1) \\ \vdots & \cdots & \vdots \\ \ell_1(\eta_{r_1+r_2-1}) & \cdots & \ell_{r_1+r_2}(\eta_{r_1+r_2-1}) \\ (r_1+r_2)^{-1/2} & \cdots & (r_1+r_2)^{-1/2} \end{vmatrix}.$$

Adding all columns to the last one, this column only zeros, except for the final entry, which equals $\sqrt{r_1 + r_2}$. We therefore get the

$$V(\ell(\mathbf{U})) = \sqrt{r_1 + r_2} R,$$

where R is the absolute value of the determinant

$$\begin{vmatrix} \ell_1(\eta_1) & \cdots & \ell_{r_1+r_2-1}(\eta_1) \\ \vdots & \cdots & \vdots \\ \ell_1(\eta_{r_1+r_2-1}) & \cdots & \ell_{r_1+r_2-1}(\eta_{r_1+r_2-1}) \end{vmatrix}.$$

This absolute value R is called the *regulator* of the field κ.

We refer the proofs of these results to E. Hecke [95], Theorems 99 and 100; J. Neukirch [202], Chapter I, Theorem 7.4; or G. J. Janusz [119], Chapter I, Theorem 13.12.

For a number field κ, define a number

$$\varkappa = \frac{2^{r_1+r_2}\pi^{r_2}\mathbf{h}R}{w|D_{\kappa/\mathbb{Q}}|^{1/2}}, \tag{2.29}$$

where

$$\begin{aligned} r_1 &= \text{number of real primes of } \kappa; \\ r_2 &= \text{number of complex primes of } \kappa; \\ w &= \text{number of roots of unity in } \kappa; \\ \mathbf{h} &= \text{class number of } \kappa; \\ R &= \text{the regulator of } \kappa. \end{aligned}$$

Theorem 2.37. *Let $Z(r)$ denote the number of integral ideals of the number field κ whose norm is $\leq r$. Then*

$$\lim_{r\to\infty} \frac{Z(r)}{r} = \varkappa.$$

Proof. See Hecke [95], Theorem 122. □

2.4.4 Minkowski's second theorem

Let C be a convex body in $\mathbb{R}^n$ with the volume $V(C)$. Let $\lambda_1 = \lambda_1(C)$ be the infimum of those numbers $\lambda \geq 0$ such that λC contains an integer point different from 0. In fact, this infimum is a minimum. It is easily seen that $0 < \lambda_1 < \infty$. Put $\tilde{\lambda} = 2V(C)^{-1/n}$. Then $\tilde{\lambda}C$ is a convex body with volume 2^n. By applying Minkowski's first theorem to the lattice $\mathbb{Z}^n$, $\tilde{\lambda}C$ contains an integer point $\neq 0$. Therefore, $\lambda_1 \leq 2V(C)^{-1/n}$, or

$$\lambda_1^n V(C) \leq 2^n. \tag{2.30}$$

For each integer j with $1 \leq j \leq n$, let $\lambda_j = \lambda_j(C)$ be the infimum of all $\lambda \geq 0$ such that λC contains j linearly independent integer points. Clearly each λ_j is actually a minimum, and

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n < \infty.$$

We call $\lambda_1, \lambda_2, \ldots, \lambda_n$ the *successive minima* of C. λ_1 is the *first minimum* of C, λ_2 is the *second minimum* of C, etc. Minkowski's first theorem is contained in the following deeper *Minkowski's second theorem* [184] (or cf. [231]), which is central to the study of successive minima.

Theorem 2.38. *Suppose that C is a convex body in $\mathbb{R}^n$. Then*

$$\frac{2^n}{n!} \le \lambda_1\lambda_2\cdots\lambda_n V(C) \le 2^n. \tag{2.31}$$

Note that the right hand inequality here sharpens (2.30). The cube $|x_i| \le 1$ $(i = 1,\dots,n)$ has $\lambda_1 = \cdots = \lambda_n = 1$ and $V(C) = 2^n$, so that the right inequality in (2.31) is best possible. The "octahedron" Ω consisting of points with $|x_1| + \cdots + |x_n| \le 1$ has $\lambda_1 = \cdots = \lambda_n = 1$ and $V(\Omega) = 2^n/n!$, so that the left inequality in (2.31) is best possible.

Let $f(\mathbf{x}) = f(x_1,\dots,x_n)$ be a *distance function* on $\mathbb{R}^n$. The inequality $f(\mathbf{x}) \le 1$ defines a *convex body* C in $\mathbb{R}^n$ which has its center at the origin $\mathbf{x} = 0$.

Theorem 2.39. *There are linearly independent lattice points $\mathbf{x}^{(1)},\dots,\mathbf{x}^{(n)}$ in $\mathbb{R}^n$ with the following properties:*

(1) *$f\left(\mathbf{x}^{(1)}\right) = \lambda_1$ is the minimum of $f(\mathbf{x})$ in all lattice points $\mathbf{x} \ne 0$, and for $j \ge 2$, $f\left(\mathbf{x}^{(j)}\right) = \lambda_j$ is the minimum of $f(\mathbf{x})$ in all lattice points $\mathbf{x}$ which are independent of $\mathbf{x}^{(1)},\dots,\mathbf{x}^{(j-1)}$.*

(2) *The determinant $\det\left(x_i^{(j)}\right)$ of the points $\mathbf{x}^{(1)},\dots,\mathbf{x}^{(n)}$ satisfies the inequalities*

$$1 \le \left|\det\left(x_i^{(j)}\right)\right| \le n!.$$

(3) *The numbers λ_j depend only on $f(\mathbf{x})$ and not on the special choice of the lattice points $\mathbf{x}^{(j)}$, and they satisfy the inequalities*

$$0 < \lambda_1 \le \lambda_2 \le \cdots \le \lambda_n < \infty,$$

$$\frac{2^n}{n!} \le \lambda_1\lambda_2\cdots\lambda_n V \le 2^n.$$

Proof. For a complete proof, see Cassels [25]. A simple proof for the last part of this theorem was given by H. Davenport [39]. □

2.5 Different of number fields

Let κ be a finite extension of degree n over $\mathbb{Q}$. Let $\mathcal{O}_\kappa$ be the integral closure of $\mathbb{Z}$ in κ.

Theorem 2.40. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_\kappa$ with a basis $\alpha_1,\dots,\alpha_n$. A basis for $\mathfrak{a}^*$ can be formed from the n elements $\beta_1,\dots,\beta_n$ which are determined along with their conjugates by the equations*

$$\mathbf{Tr}_{\kappa/\mathbb{Q}}(\alpha_i\beta_j) = \delta_{ij},\ \ i,j = 1,2,\dots,n.$$

Proof. The elements $\lambda \in \mathfrak{a}^*$ cannot have arbitrarily large ideal denominators. This is true since the hypothesis is equivalent to n equations

$$g_i = \mathbf{Tr}_{\kappa/\mathbb{Q}}(\lambda\alpha_i) = \sum_{j=1}^{n} \lambda^{(j)}\alpha_i^{(j)}, \;\; i = 1, 2, \ldots, n, \tag{2.32}$$

where $g_i \in \mathbb{Z}$, and from the n linear equations, these $\lambda^{(j)}$ are obtained as quotients of two determinants. The denominator is the fixed determinant of the $\alpha_i^{(j)}$ which satisfies

$$\det\left(\alpha_i^{(j)}\right)^2 = D_{\kappa/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \mathcal{N}(\mathfrak{a})^2 D_{\kappa/\mathbb{Q}}.$$

The numerator is an integral polynomial in the $\alpha_i^{(j)}$. Consequently there is an element $\omega \in \mathcal{O}_\kappa$ depending only on the α, such that $\omega\lambda \in \mathcal{O}_\kappa$.

If we define the n^2 elements $\beta_i^{(j)}$ by the uniquely solvable equations

$$\sum_{l=1}^{n} \alpha_i^{(l)}\beta_j^{(l)} = \delta_{ij}, \;\; i, j = 1, 2, \ldots, n,$$

and if we have λ satisfying (2.32) for $g_i \in \mathbb{Z}$ $(i = 1, 2, \ldots, n)$, then the n sequences of elements $\beta_i^{(1)}, \ldots, \beta_i^{(n)}$ are conjugate sequences of elements β_i in κ such that

$$\lambda = \sum_{i=1}^{n} g_i\beta_i.$$

Consequently the $\beta_1, \ldots, \beta_n$ form a basis for $\mathfrak{a}^*$, provided they are elements in κ. □

Since, moreover,

$$D_{\kappa/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \frac{1}{D_{\kappa/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)} = \frac{1}{\mathcal{N}(\mathfrak{a})^2 D_{\kappa/\mathbb{Q}}},$$

and by using (2.23),

$$D_{\kappa/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = \mathcal{N}(\mathfrak{a}^*)^2 D_{\kappa/\mathbb{Q}} = \frac{D_{\kappa/\mathbb{Q}}}{\mathcal{N}(\mathfrak{a})^2 \mathcal{N}(\mathfrak{d}_{\kappa/\mathbb{Q}})^2},$$

we have

$$|D_{\kappa/\mathbb{Q}}| = \mathcal{N}(\mathfrak{d}_{\kappa/\mathbb{Q}}). \tag{2.33}$$

Theorem 2.41. *The greatest common divisor of the differents $\delta(\alpha)$ of all $\alpha \in \mathcal{O}_\kappa$ is equal to the different $\mathfrak{d}$ of the field κ.*

Proof. See E. Hecke [95], Theorem 105. □

Let K be a finite extension of κ. Then the integral closure of $\mathcal{O}_\kappa$ in K is just $\mathcal{O}_K$ by transitivity of integral dependence. Furthermore, r arbitrary elements $\alpha_1, \ldots, \alpha_r$ of κ generate an ideal $\mathfrak{a}$ in κ and an ideal $\mathfrak{A}$ in K. It is not difficult to show that an element β belongs to $\mathfrak{A}$ if and only if β belongs to $\mathfrak{a}$. Accordingly, both ideals $\mathfrak{a}$ and $\mathfrak{A}$ are same, denoted by $(\alpha_1, \ldots, \alpha_r)$.

For each ideal $\mathfrak{B}$ of $\mathcal{O}_K$, by using the decomposition of $\mathfrak{B}$ into prime ideals of $\mathcal{O}_K$ and based on the transitivity of inertia degree and ramification index, one has

$$\mathbf{N}_{\kappa/\mathbb{Q}}\left(\mathbf{N}_{K/\kappa}(\mathfrak{B})\right) = \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{B}). \tag{2.34}$$

Theorem 2.42. *If $\mathfrak{B}$ is an fractional ideal of $\mathcal{O}_K$, then*

$$\mathcal{N}(\mathbf{N}_{K/\kappa}(\mathfrak{B})) = \mathcal{N}(\mathfrak{B}),$$

where the left-hand side is the (absolute) norm in κ, but the right-hand side is the (absolute) norm in K.

Proof. If $\mathfrak{B} = (\beta)$ for some number β in K, by (1.23) one has

$$\mathbf{N}_{\kappa/\mathbb{Q}}\left(\mathbf{N}_{K/\kappa}(\beta)\right) = \mathbf{N}_{K/\mathbb{Q}}(\beta). \tag{2.35}$$

Therefore

$$\mathcal{N}(\mathfrak{B}) = |\mathbf{N}_{K/\mathbb{Q}}(\beta)| = \mathcal{N}((\mathbf{N}_{K/\kappa}(\beta))) = \mathcal{N}(\mathbf{N}_{K/\kappa}(\mathfrak{B}))$$

follows from Theorem 2.19.

For each ideal $\mathfrak{B}$ of $\mathcal{O}_K$, then $\mathfrak{B}^{\mathbf{h}} = (\beta)$, where β is a certain element in K, and $\mathbf{h}$ is the class number of K. Thus we have

$$\mathcal{N}(\mathfrak{B})^{\mathbf{h}} = \mathcal{N}(\mathfrak{B}^{\mathbf{h}}) = \mathcal{N}(\mathbf{N}_{K/\kappa}(\mathfrak{B}^{\mathbf{h}})).$$

On the other hand,

$$\mathcal{N}(\mathbf{N}_{K/\kappa}(\mathfrak{B}))^{\mathbf{h}} = \mathcal{N}(\mathbf{N}_{K/\kappa}(\mathfrak{B})^{\mathbf{h}}) = \mathcal{N}(\mathbf{N}_{K/\kappa}(\mathfrak{B}^{\mathbf{h}})),$$

and so the theorem follows. □

By (2.33), the discriminant ideal with respect to $\kappa = \mathbb{Q}$, defined in this way, is then the same as the ideal

$$\mathfrak{D}_{K/\mathbb{Q}} = (D_{K/\mathbb{Q}}),$$

where $D_{K/\mathbb{Q}}$ is the discriminant of K. However we must distinguish the discriminant of a field, which is a well-defined number $D_{K/\mathbb{Q}}$, from the discriminant ideal of the same field with respect to $\mathbb{Q}$, which is an ideal, namely $\mathfrak{D}_{K/\mathbb{Q}}$. Then

$$\mathfrak{D}_{K/\mathbb{Q}} = \mathbf{N}_{\kappa/\mathbb{Q}}(\mathfrak{D}_{K/\kappa})\mathfrak{D}_{\kappa/\mathbb{Q}}^{[K:\kappa]} \tag{2.36}$$

follows from (1.54), (1.27) and (2.34), that is, we have a relation of principal ideals in $\mathbb{Z}$ by Theorem 2.27

$$(D_{K/\mathbb{Q}}) = (\mathcal{N}(\mathfrak{D}_{K/\kappa}))(D_{\kappa/\mathbb{Q}})^{[K:\kappa]}.$$

By comparing the minimal positive integers in these ideals, we find

$$|D_{K/\mathbb{Q}}| = \mathcal{N}(\mathfrak{D}_{K/\kappa})|D_{\kappa/\mathbb{Q}}|^{[K:\kappa]}. \tag{2.37}$$

Let α be an algebraic integer which generates the field K. Let $A(\alpha)$ be the set of all elements

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

where $n = [K : \kappa]$, and $a_0, \ldots, a_{n-1}$ run through all algebraic integers in κ. Let P_α be the irreducible polynomial over κ with leading coefficient 1 which has the root α.

Lemma 2.43. *If ω is an algebraic integer in K such that $\omega\mathfrak{d}_{K/\kappa}$ is integral, then there exists an element $\beta \in A(\alpha)$ such that ω can be represented in the form*

$$\omega = \frac{\beta}{P'_\alpha(\alpha)}.$$

Proof. We write

$$P_\alpha(x) = \prod_{i=1}^{n} \left(x - \alpha^{(i)}\right) = c_0 + c_1 x + \cdots + c_n x^n,$$

and consider the polynomial in x

$$g(x) = \sum_{i=1}^{n} \omega^{(i)} \frac{P_\alpha(x)}{x - \alpha^{(i)}}, \tag{2.38}$$

where $\omega^{(i)}$ are the conjugates of ω. Note that $g(x)$ is a polynomial with algebraic integral coefficients in κ since

$$\frac{P_\alpha(x)}{x - \alpha} = \frac{P_\alpha(x) - P_\alpha(\alpha)}{x - \alpha} = \sum_{l=1}^{n} c_l \sum_{0 \le j \le l-1} x^j \alpha^{l-j-1}$$

and hence

$$g(x) = \sum_{l=1}^{n} c_l \sum_{0 \le j \le l-1} x^j \mathbf{Tr}_{K/\kappa}\left(\omega\alpha^{l-j-1}\right).$$

However since $\omega\mathfrak{d}_{K/\kappa}$ is algebraic integral by hypothesis, the traces appearing here are integral by Theorem 1.117. If we set $x = \alpha$ in (2.38) we obtain $\omega = g(\alpha)/P'_\alpha(\alpha)$, where $g(\alpha) \in A(\alpha)$. □

Lemma 2.44. *For each element β in $A(\alpha)$, $\mathbf{Tr}_{K/\kappa}(\beta/P'_\alpha(\alpha))$ is integral.*

Proof. Obviously Lemma 2.44 needs only to be proved for $\beta = 1, \alpha, \ldots, \alpha^{n-1}$, where it follows directly from the Euler formulae

$$\sum_{i=1}^{n} \frac{\left(\alpha^{(i)}\right)^j}{P'_\alpha\left(\alpha^{(i)}\right)} = \begin{cases} 0, & \text{if } 0 \le j \le n-2, \\ 1, & \text{if } j = n-1. \end{cases}$$

These formulae follow from the Lagrange interpolation formula

$$\sum_{i=1}^{n} \frac{\left(\alpha^{(i)}\right)^{j+1}}{P'_\alpha\left(\alpha^{(i)}\right)} \frac{P_\alpha(x)}{x - \alpha^{(i)}} = \begin{cases} x^{j+1}, & \text{if } 0 \le j \le n-2, \\ x^n - P_\alpha(x), & \text{if } j = n-1, \end{cases}$$

if we set $x = 0$. □

From Lemma 2.43 it follows that $\omega P'_\alpha(\alpha)$ is integral if $\omega \mathfrak{d}_{K/\kappa}$ is integral, thus $P'_\alpha(\alpha)$ has the decomposition

$$P'_\alpha(\alpha) = \mathfrak{d}_{K/\kappa}\mathfrak{F} \tag{2.39}$$

where $\mathfrak{F}$ is an integral ideal.

Theorem 2.45. *All elements of the ideal $\mathfrak{F} = P'_\alpha(\alpha)/\mathfrak{d}_{K/\kappa}$ belong to the ring $A(\alpha)$, and if all elements of an ideal $\mathfrak{A}$ belong to the ring $A(\alpha)$, then $\mathfrak{A}$ is divisible by $\mathfrak{F}$.*

Proof. If $\beta \equiv 0 \pmod{\mathfrak{F}}$, then $\omega = \beta/P'_\alpha(\alpha)$ is an element with denominator $\mathfrak{d}_{K/\kappa}$, and by Lemma 2.43, $\omega P'_\alpha(\alpha)$ must be an element of this ring. Hence the first part of the theorem is proved.

Conversely, if all elements of $\mathfrak{A}$ belong to the ring $A(\alpha)$, then $\mathbf{Tr}_{K/\kappa}(\beta/P'_\alpha(\alpha))$ is integral for each element β of $\mathfrak{A}$ by Lemma 2.44. Consequently, by Theorem 1.117, $1/P'_\alpha(\alpha)$ is an element of the ideal $(\mathfrak{A}\mathfrak{d}_{K/\kappa})^{-1}$; thus $P'_\alpha(\alpha) = \mathfrak{d}_{K/\kappa}\mathfrak{F}$ divides $\mathfrak{A}\mathfrak{d}_{K/\kappa}$ so $\mathfrak{F}|\mathfrak{A}$, which was to be proved. □

According to this theorem, $\mathfrak{F}$ is the greatest common divisor of all ideals in K which contain only elements in $A(\alpha)$. The ideal $\mathfrak{F}$ is called the *conductor of the ring*.

Lemma 2.46. *Corresponding to each prime ideal $\mathfrak{P}$ in K there is a ring $A(\alpha)$, where $\mathfrak{P}$ does not divide $\mathfrak{F} = P'_\alpha(\alpha)/\mathfrak{d}_{K/\kappa}$.*

Proof. Let $\mathfrak{p}$ be the prime ideal in κ which is divisible by $\mathfrak{P}$, that is,

$$\mathfrak{p} = \mathfrak{P}^e\mathfrak{A}, \quad (\mathfrak{A}, \mathfrak{P}) = 1.$$

Let α be a primitive root mod $\mathfrak{P}$ such that each algebraic integer in K is congruent to an element in $A(\alpha)$ modulo each power of $\mathfrak{P}$, and such that

$$\alpha \equiv 0 \pmod{\mathfrak{A}}.$$

Finally let η be a number in κ which is divisible by $P'_\alpha(\alpha) = \mathfrak{d}_{K/\kappa}\mathfrak{F}$ and assume that $\mathfrak{p}^b$ is the highest power of $\mathfrak{p}$ dividing η. Then an appropriate power of η, say η^h, furnishes a decomposition into two numerical factors in κ,

$$\eta^h = \mathfrak{p}^{hb}\mu, \quad (\mu, \mathfrak{p}) = 1.$$

$$\eta^h \equiv 0 \pmod{\mathfrak{d}_{K/\kappa}\mathfrak{F}}.$$

Then let us determine, for an arbitrarily given algebraic integer ω in K, an element β in $A(\alpha)$, such that

$$\omega \equiv \beta \pmod{\mathfrak{P}^{ehb}}.$$

The element $(\omega - \beta)\mu\alpha^{hb}$ is then divisible by $P'_\alpha(\alpha) = \mathfrak{d}_{K/\kappa}\mathfrak{F}$, since

$$\frac{(\omega-\beta)\mu\alpha^{hb}}{P'_\alpha(\alpha)} = \frac{\mathfrak{p}^{hb}\mu}{\mathfrak{d}_{K/\kappa}\mathfrak{F}}\frac{(\omega-\beta)\alpha^{hb}}{\mathfrak{p}^{hb}} = \frac{\eta^h}{\mathfrak{d}_{K/\kappa}\mathfrak{F}}\frac{(\omega-\beta)\alpha^{hb}}{\mathfrak{P}^{ehb}\mathfrak{A}^{hb}}$$

is integral. If we apply Lemma 2.43, we thus obtain a representation $\omega\mu\alpha^{hb} \in A(\alpha)$ for each ω, from which by Theorem 2.45, $\mu\alpha^{hb}$ generates an ideal which is divisible by $\mathfrak{F}$. Thus, in any case, it follows that $\mathfrak{F}$ is prime to $\mathfrak{P}$. □

From Lemma 2.46, we immediately obtain the main theorem of this theory:

Theorem 2.47. *The different of K with respect to κ is the greatest common divisor of all differents of algebraic integers of K with respect to κ.*

Chapter 3

Algebraic geometry

We give an overview of algebraic geometry that will be used in the rest of this book. This part introduces Hermitian geometry, varieties, divisors, linear systems, algebraic curves, sheaves, vector bundles, schemes and Kobayashi hyperbolicity.

3.1 Hermitian geometry

We will introduce some technical lemmas, basic operators and their gauges on a projective space associated to a vector space. A good reference is Stoll [267] for complex case.

3.1.1 Exterior product

Let V be a vector space of finite dimension $n+1 > 0$ over a field κ. Write the *projective space* $\mathbb{P}(V) = V/\kappa_*$ and let $\mathbb{P} : V_* \longrightarrow \mathbb{P}(V)$ be the standard *projection*, where $V_* = V - \{0\}$. If $A \subset V$, abbreviate

$$\mathbb{P}(A) = \mathbb{P}(A \cap V_*).$$

The dual vector space V^* of V consists of all κ-linear functions $\alpha : V \longrightarrow \kappa$, and we shall call

$$\langle \xi, \alpha \rangle = \alpha(\xi)$$

the *inner product* of $\xi \in V$ and $\alpha \in V^*$. If $\alpha \neq 0$, the n-dimensional linear subspace

$$E[a] = E[\alpha] = \mathrm{Ker}(\alpha) = \alpha^{-1}(0)$$

depends on $a = \mathbb{P}(\alpha) \in \mathbb{P}(V^*)$ only, and $\ddot{E}[a] = \mathbb{P}(E[a])$ is a *hyperplane* in $\mathbb{P}(V)$. Thus $\mathbb{P}(V^*)$ bijectively parameterizes the hyperplanes in $\mathbb{P}(V)$.

Identify $V^{**} = V$ by $\langle \xi, \alpha \rangle = \langle \alpha, \xi \rangle$ and $\left(\bigwedge_{k+1} V \right)^* = \bigwedge_{k+1} V^*$ by

$$\langle \xi_0 \wedge \cdots \wedge \xi_k, \alpha_0 \wedge \cdots \wedge \alpha_k \rangle = \det(\langle \xi_i, \alpha_j \rangle),$$

where $\bigwedge_{k+1} V$ is the *exterior product of* V *of order* $k+1$, and where $\xi_i \in V,\ \alpha_i \in V^*$ for $i = 0, \ldots, k$. Take $k, l \in \mathbb{Z}[0, n]$ and take $\xi \in \bigwedge_{k+1} V$ and $\alpha \in \bigwedge_{l+1} V^*$, where

$$\mathbb{Z}[m, n] = \{ i \in \mathbb{Z} \mid m \leq i \leq n \}.$$

If $k \geq l$, the *interior product* $\xi \lrcorner \alpha \in \bigwedge_{k-l} V$ is uniquely defined by

$$\langle \xi \lrcorner \alpha, \beta \rangle = \langle \xi, \alpha \wedge \beta \rangle$$

for all $\beta \in \bigwedge_{k-l} V^*$. If $k = l$, then

$$\xi \lrcorner \alpha = \langle \xi, \alpha \rangle \in \kappa = \bigwedge_0 V$$

by definition. If $k < l$, we define the *interior product* $\xi \lrcorner \alpha \in \bigwedge_{l-k} V^*$ such that if $\eta \in \bigwedge_{l-k} V$,

$$\langle \eta, \xi \lrcorner \alpha \rangle = \langle \xi \wedge \eta, \alpha \rangle.$$

Take non-negative integers a and b with $a \leq b$. Let J_a^b be the set of all increasing injective mappings $\lambda : \mathbb{Z}[0, a] \longrightarrow \mathbb{Z}[0, b]$. Then $J_b^b = \{\iota\}$, where ι is the inclusion mapping. If $a < b$, there exists one and only one $\lambda^\perp \in J_{b-a-1}^b$ for each $\lambda \in J_a^b$ such that $\operatorname{Im} \lambda \cap \operatorname{Im} \lambda^\perp = \emptyset$. The mapping $\perp$: $J_a^b \longrightarrow J_{b-a-1}^b$ is bijective. A permutation $(\lambda, \lambda^\perp)$ of $\mathbb{Z}[0, b]$ is defined by

$$(\lambda, \lambda^\perp)(i) = \begin{cases} \lambda(i), & i \in \mathbb{Z}[0, a], \\ \lambda^\perp(i - a - 1), & i \in \mathbb{Z}[a + 1, b]. \end{cases}$$

The signature of the permutation is denoted by $\operatorname{sign}(\lambda, \lambda^\perp)$.

Lemma 3.1. *Let $k \geq 1$ be an integer and $\xi_0, \ldots, \xi_k \in V$; $\alpha_0, \ldots, \alpha_k \in V^*$. Set*

$$\eta_i = \xi_0 \wedge \xi_i \in W, \quad \beta_i = \alpha_0 \wedge \alpha_i \in W^*$$

for $i = 1, \ldots, k$, where $W = \bigwedge_2 V$. Then

$$\langle \eta_1 \wedge \cdots \wedge \eta_k, \beta_1 \wedge \cdots \wedge \beta_k \rangle = \langle \xi_0, \alpha_0 \rangle^{k-1} \langle \xi_0 \wedge \cdots \wedge \xi_k, \alpha_0 \wedge \cdots \wedge \alpha_k \rangle,$$

where the interior product on the left-hand side is between $\bigwedge_k W$ and $\bigwedge_k W^*$.

Proof. If $\xi_0, \ldots, \xi_k$ are linearly dependent, then both sides are zero; therefore we may assume that $\xi_0, \ldots, \xi_k$ form part of a basis for V. Let $\xi_0^*, \ldots, \xi_n^*$ be the dual basis for V^*, and let $\alpha_{i0}, \ldots, \alpha_{in}$ be the coordinates of α_i relative to this basis. Since

$$\alpha_0 \wedge \cdots \wedge \alpha_k = \sum_{\nu \in J_k^n} \det(\alpha_{i\nu(j)})_{0 \leq i,j \leq k} \xi_{\nu(0)}^* \wedge \cdots \wedge \xi_{\nu(k)}^*,$$

we have

$$\langle \xi_0 \wedge \cdots \wedge \xi_k, \alpha_0 \wedge \cdots \wedge \alpha_k \rangle = \det(\alpha_{ij})_{0 \leq i,j \leq k}.$$

Note that

$$\beta_i = \sum_{\mu \in J_1^n} (\alpha_{0\mu(0)} \alpha_{i\mu(1)} - \alpha_{0\mu(1)} \alpha_{i\mu(0)}) \xi_{\mu(0)}^* \wedge \xi_{\mu(1)}^*.$$

We can obtain

$$\langle \eta_1 \wedge \cdots \wedge \eta_k, \beta_1 \wedge \cdots \wedge \beta_k \rangle = \det(\alpha_{00}\alpha_{ij} - \alpha_{0j}\alpha_{i0})_{1 \le i,j \le k} = \alpha_{00}^{k-1} \det(\alpha_{ij})_{0 \le i,j \le k}.$$

This latter equality can be shown using properties of determinants. □

Lemma 3.2. *Take* $\xi, \xi', \xi_0, \ldots, \xi_{p-2} \in V$ *and* $\beta \in \bigwedge_{p-1} V^*$. *Write*

$$\Xi = \xi_0 \wedge \cdots \wedge \xi_{p-2}, \quad \eta = (\Xi \wedge \xi) \lrcorner \beta, \quad \eta' = (\Xi \wedge \xi') \lrcorner \beta.$$

Then

$$\eta \wedge \eta' = \langle \Xi, \beta \rangle (\Xi \wedge \xi \wedge \xi') \lrcorner \beta.$$

Proof. See also Wu [302], Lemma 3.9. This reduces to the following identity of determinants. Let M be a $(p-1) \times (p-1)$ matrix; A and A', $(p-1) \times 1$ matrices; B and B', $1 \times (p-1)$ matrices; and c, d, e, f, scalars. Then

$$\begin{vmatrix} \begin{vmatrix} M & A \\ B & c \end{vmatrix} & \begin{vmatrix} M & A' \\ B' & d \end{vmatrix} \\ \begin{vmatrix} M & A \\ B & e \end{vmatrix} & \begin{vmatrix} M & A' \\ B' & f \end{vmatrix} \end{vmatrix} = |M| \begin{vmatrix} M & A & A' \\ B & c & d \\ B' & e & f \end{vmatrix}.$$

The left-hand side is the determinant of a 2×2 matrix whose elements are determinants of $p \times p$ matrices. If this is true, then it holds as an identity of polynomials in the matrix elements, so it will suffice to prove it when M is nonsingular, which holds generically. Furthermore, if one applies the same row operators simultaneously to M, A, and A', then none of the above determinants changes. Therefore, we may assume that M is diagonal; in that case the identity is easily checked. □

3.1.2 Norms of vector spaces

We continue to consider a vector space V of dimension $n+1$ over a field κ. Take a base $e = (e_0, \ldots, e_n)$ of V, a valuation v on κ. For $\xi = \xi_0 e_0 + \cdots + \xi_n e_n \in V$, define the norm

$$|\xi|_{v,e} = \begin{cases} \left(|\xi_0|_v^2 + \cdots + |\xi_n|_v^2\right)^{\frac{1}{2}}, & \text{if } v \text{ is Archimedean,} \\ \max\limits_{0 \le i \le n} \{|\xi_i|_v\}, & \text{if } v \text{ is non-Archimedean.} \end{cases}$$

Obviously, the norm depends on the base e, and will be called a *norm over the base* e. If $|\cdot|_{v,e'}$ is another norm over a base $e' = (e'_0, \ldots, e'_n)$, it is easy to prove that there exist two multiplicative M_κ-constants $c = \{c_v\}$ and $c' = \{c'_v\}$ such that

$$c_v |\xi|_{v,e} \le |\xi|_{v,e'} \le c'_v |\xi|_{v,e}$$

hold for all $\xi \in V$, i.e., norms over bases are equivalent. We will abbreviate

$$|\xi|_v = |\xi|_{v,e}.$$

Further if κ is a number field with the set M_κ satisfying the product formula of multiplicities n_v, we will use notations

$$\|\xi\|_v = |\xi|_v^{n_v}, \ \ |||\xi|||_v = \|\xi\|_v^{1/[\kappa:\mathbb{Q}]}. \tag{3.1}$$

Let $\epsilon = (\epsilon_0, \dots, \epsilon_n)$ be the dual base of $e = (e_0, \dots, e_n)$. Then the norm on V induces a norm on V^* defined by

$$|\alpha|_v = \begin{cases} \left(|\alpha_0|_v^2 + \cdots + |\alpha_n|_v^2\right)^{\frac{1}{2}}, & \text{if } v \text{ is Archimedean,} \\ \max\limits_{0\le i\le n}\{|\alpha_i|_v\}, & \text{if } v \text{ is non-Archimedean,} \end{cases}$$

where $\alpha = \alpha_0\epsilon_0 + \cdots + \alpha_n\epsilon_n$. *Schwarz inequality*

$$|\langle \xi, \alpha\rangle|_v \le |\xi|_v \cdot |\alpha|_v$$

holds for $\xi \in V$, $\alpha \in V^*$. The *distance* from $x = \mathbb{P}(\xi)$ to $\ddot{E}[a]$ with $a = \mathbb{P}(\alpha) \in \mathbb{P}(V^*)$ is defined by

$$0 \le |x, a|_v = \frac{|\langle \xi, \alpha\rangle|_v}{|\xi|_v \cdot |\alpha|_v} \le 1. \tag{3.2}$$

Further if κ is a number field with a proper set M_κ satisfying the product formula of multiplicities n_v, we will use the normalization

$$\|\alpha\|_v = |\alpha|_v^{n_v}, \quad \|x, a\|_v = |x, a|_v^{n_v}, \tag{3.3}$$

and the notations

$$|||\alpha|||_v = \|\alpha\|_v^{1/[\kappa:\mathbb{Q}]}, \quad |||x, a|||_v = \|x, a\|_v^{1/[\kappa:\mathbb{Q}]}. \tag{3.4}$$

The norm on V also induces norms on $\bigwedge\limits_{k+1} V$ and $\bigwedge\limits_{k+1} V^*$. Take $\xi \in \bigwedge\limits_{k+1} V$, $\alpha \in \bigwedge\limits_{k+1} V^*$ and write

$$\xi = \sum_{\lambda \in J_k^n} \xi_\lambda e_\lambda, \quad \alpha = \sum_{\lambda \in J_k^n} \alpha_\lambda \epsilon_\lambda,$$

where

$$e_\lambda = e_{\lambda(0)} \wedge \cdots \wedge e_{\lambda(k)}.$$

Then we can define the norms

$$|\xi|_v = |\xi|_{v,e} = \begin{cases} \Big(\sum\limits_{\lambda \in J_k^n} |\xi_\lambda|_v^2\Big)^{\frac{1}{2}}, & \text{if } v \text{ is Archimedean,} \\ \max\limits_{\lambda \in J_k^n}\{|\xi_\lambda|_v\}, & \text{if } v \text{ is non-Archimedean,} \end{cases}$$

and

$$|\alpha|_v = |\alpha|_{v,e} = \begin{cases} \left(\sum_{\lambda \in J_k^n} |\alpha_\lambda|_v^2 \right)^{\frac{1}{2}}, & \text{if } v \text{ is Archimedean,} \\ \max_{\lambda \in J_k^n} \{|\alpha_\lambda|_v\}, & \text{if } v \text{ is non-Archimedean.} \end{cases}$$

Definition 3.3. Let $V_1, \ldots, V_m$ and W be normed vector spaces over κ. Let

$$\odot : V_1 \times \cdots \times V_m \longrightarrow W$$

be an m-linear mapping over κ. If $\xi = (\xi_1, \ldots, \xi_m) \in V_1 \times \cdots \times V_m$, we write

$$\odot(\xi) = \xi_1 \odot \cdots \odot \xi_m,$$

and say that ξ is *free for the operation* $\odot$ if $\odot(\xi) \neq 0$. Take $x_j \in \mathbb{P}(V_j)$ $(j = 1, \ldots, m)$. We will say that $x_1, \ldots, x_m$ are *free for* $\odot$ if there exist $\xi_j \in V_j$ such that $x_j = \mathbb{P}(\xi_j)$ and $\xi = (\xi_1, \ldots, \xi_m)$ is free for the operation $\odot$. For free $x_1, \ldots, x_m$, we can define

$$x_1 \odot \cdots \odot x_m = \mathbb{P}(\xi_1 \odot \cdots \odot \xi_m).$$

Also, the *gauge of* $x_1, \ldots, x_m$ *for* $\odot$ is defined to be

$$|x_1 \odot \cdots \odot x_m|_v = \frac{|\xi_1 \odot \cdots \odot \xi_m|_v}{|\xi_1|_v \cdots |\xi_m|_v}.$$

If $x_1, \ldots, x_m$ are not free for $\odot$, we define $|x_1 \odot \cdots \odot x_m|_v = 0$.

In particular, if $V = \kappa^{n+1}$, we may take the standard base $e_0, e_1, \ldots, e_n$, where

$$e_j = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}_+^{n+1}$$

in which 1 is $(j+1)$th component of e_j. Take $\xi \in \kappa^{n+1} - \{0\}$ and write

$$\xi = \xi_0 e_0 + \xi_1 e_1 + \cdots + \xi_n e_n = (\xi_0, \xi_1, \ldots, \xi_n).$$

We usually denote $\mathbb{P}(\xi)$ by $[\xi_0, \xi_1, \ldots, \xi_n]$ which are called the *homogeneous coordinates* of $\mathbb{P}\left(k^{n+1}\right)$, and abbreviate

$$\mathbb{P}^n(\kappa) = \mathbb{P}\left(\kappa^{n+1}\right).$$

We can embed κ^n into $\mathbb{P}^n(\kappa)$ by using the mapping

$$(\xi_1, \ldots, \xi_n) \mapsto [1, \xi_1, \ldots, \xi_n],$$

and obtain the disjoint union

$$\mathbb{P}^n(\kappa) = \kappa^n \cup \mathbb{P}^{n-1}(\kappa).$$

Particularly, $\mathbb{P}^0(\kappa) = \mathbb{P}(\kappa)$ consists of one point denoted by ∞, and so

$$\mathbb{P}^1(\kappa) = \kappa \cup \{\infty\}.$$

If v is non-Archimedean, set

$$\chi_v(x,a) = \begin{cases} \frac{|x-a|_v}{|x|_v^\vee |a|_v^\vee}, & x, a \in \kappa, \\ \frac{1}{|x|_v^\vee}, & a = \infty, \end{cases} \tag{3.5}$$

where, by definition,

$$r^\vee = \max\{1, r\} \ \ (r \in \mathbb{R}).$$

If v is Archimedean, set

$$\chi_v(x,a) = \begin{cases} \frac{|x-a|_v}{(1+|x|_v^2)^{1/2}(1+|a|_v^2)^{1/2}}, & x, a \in \kappa, \\ \frac{1}{\sqrt{1+|x|_v^2}}, & a = \infty. \end{cases} \tag{3.6}$$

Then we have

$$\chi_v\left(\frac{1}{x}, \frac{1}{a}\right) = \chi_v(x,a)$$

for all $x, a \in \kappa \cup \{\infty\}$, where we think

$$\frac{1}{0} = \infty, \quad \frac{1}{\infty} = 0.$$

Identify $\kappa^{n+1} = (\kappa^{n+1})^*$ such that

$$\langle \xi, \alpha \rangle = \xi_0\alpha_0 + \cdots + \xi_n\alpha_n$$

for $\xi = (\xi_0, \ldots, \xi_n), \alpha = (\alpha_0, \ldots, \alpha_n) \in \kappa^{n+1}$. It is easy to show that

$$\chi_v(x,a) = \begin{cases} |[1,x],[-a,1]|_v, & x, a \in \kappa, \\ |[1,x],[1,0]|_v, & a = \infty. \end{cases} \tag{3.7}$$

Finally, let κ be the field $\mathbb{C}$ of complex numbers. A positive definite Hermitian form

$$(,) : V \times V \longrightarrow \mathbb{C}$$

is called a *Hermitian product* or a *Hermitian metric* on V. It defines a *norm*

$$|\xi| = (\xi, \xi)^{\frac{1}{2}}, \ \ \xi \in V.$$

A complex vector space together with a Hermitian product is called a *Hermitian vector space*. For each $\xi \in V$, one and only one dual vector $\xi^* \in V^*$ is defined by $(\eta, \xi) = \langle \eta, \xi^* \rangle$ for all $\eta \in V$. The mapping $\xi \mapsto \xi^*$ is an anti-linear isomorphism of V onto V^*. Here V^* becomes a Hermitian vector space by setting

$$(\xi^*, \eta^*) = (\eta, \xi), \ \ \xi, \eta \in V.$$

Then $\xi^{**} = \xi$ and $V^{**} = V$, as Hermitian vector space. A Hermitian product is uniquely defined on $\bigwedge_{p+1} V$ by the requirement

$$(\xi_0 \wedge \cdots \wedge \xi_p, \eta_0 \wedge \cdots \wedge \eta_p) = \det((\xi_j, \eta_k)), \ \ \xi_j, \eta_j \in V.$$

3.1.3 Schwarz inequalities

We continue to study a vector space V of dimension $n+1$ over a field κ. In the following, we will prove some elementary but useful inequalities about multi-vectors and give several gauges. Take a positive number r. We will use the following symbol:

$$\varsigma_{v,r} = \begin{cases} \sqrt{r}, & \text{if } v \text{ is Archimedean,} \\ 1, & \text{if } v \text{ is non-Archimedean.} \end{cases} \tag{3.8}$$

First and easiest to prove is of course the following *generalized Schwarz's inequality*:

Lemma 3.4. *Take $k, l \in \mathbb{Z}[0,n]$ and take $\xi \in \bigwedge_{k+1} V$ and $\alpha \in \bigwedge_{l+1} V^*$. Then*

$$|\xi \angle \alpha|_v \leq \varsigma_{v,\binom{n-p}{q-p}} |\xi|_v \cdot |\alpha|_v,$$

where $p = \min\{k,l\}, q = \max\{k,l\}$, and the combinatorial symbol is defined by

$$\binom{i}{j} = \begin{cases} \frac{i!}{j!(i-j)!}, & \text{if } i \geq j, \\ 0, & \text{if } i < j. \end{cases}$$

Proof. W.l.o.g., we may assume $k \geq l$, and write

$$\xi = \sum_{\lambda \in J_k^n} \xi_\lambda e_\lambda, \quad \alpha = \sum_{\lambda \in J_l^n} \alpha_\lambda \epsilon_\lambda.$$

First of all, we consider non-Archimedean case. If $l = k$, noting that

$$\xi \angle \alpha = \langle \xi, \alpha \rangle = \sum_{\lambda \in J_k^n} \xi_\lambda \alpha_\lambda,$$

we have

$$|\xi \angle \alpha|_v \leq \max_{\lambda \in J_k^n} |\xi_\lambda \alpha_\lambda|_v \leq \left(\max_{\lambda \in J_k^n} |\xi_\lambda|_v \right) \cdot \left(\max_{\lambda \in J_k^n} |\alpha_\lambda|_v \right) = |\xi|_v \cdot |\alpha|_v$$

and so the inequality follows. If $l < k$, by the Laplace's theorem of determinant expansion

$$\begin{aligned} \langle (e_0 \wedge \cdots \wedge e_k) \angle \alpha, \beta \rangle &= \langle e_0 \wedge \cdots \wedge e_k, \alpha \wedge \beta \rangle \\ &= \sum_{\nu \in J_l^k} \operatorname{sign}(\nu, \nu^\perp) \langle e_\nu, \alpha \rangle \langle e_{\nu^\perp}, \beta \rangle \\ &= \left\langle \sum_{\nu \in J_l^k} \operatorname{sign}(\nu, \nu^\perp) \langle e_\nu, \alpha \rangle e_{\nu^\perp}, \beta \right\rangle \end{aligned}$$

holds for any $\beta \in \bigwedge_{k-l} V^*$, that is,

$$(e_0 \wedge \cdots \wedge e_k)\angle\alpha = \sum_{\nu \in J_l^k} \mathrm{sign}(\nu, \nu^\perp)\langle e_\nu, \alpha\rangle e_{\nu^\perp} = \sum_{\nu \in J_l^k} \mathrm{sign}(\nu, \nu^\perp)\alpha_\nu e_{\nu^\perp}. \quad (3.9)$$

Then

$$|(e_0 \wedge \cdots \wedge e_k)\angle\alpha|_v = \max_{\nu \in J_l^k}\{|\langle e_\nu, \alpha\rangle|_v\} \leq |\alpha|_v.$$

Thus, we have

$$|\xi\angle\alpha|_v = \left|\sum_{\lambda \in J_k^n} \xi_\lambda e_\lambda\angle\alpha\right|_v \leq \max_{\lambda \in J_k^n}\{|\xi_\lambda|_v |e_\lambda\angle\alpha|_v\} \leq |\xi|_v \cdot |\alpha|_v.$$

Finally, assume that v is Archimedean. We have

$$|\xi\angle\alpha|_v = \left|\sum_{\lambda \in J_k^n} \xi_\lambda e_\lambda\angle\alpha\right|_v \leq \sum_{\lambda \in J_k^n} |\xi_\lambda|_v |e_\lambda\angle\alpha|_v \leq |\xi|_v \left(\sum_{\lambda \in J_k^n} |e_\lambda\angle\alpha|_v^2\right)^{\frac{1}{2}}.$$

For $\lambda \in J_k^n$, set

$$J_l^\lambda = \{\nu \in J_l^n \mid \nu \subset \lambda\},$$

where $\nu \subset \lambda$ means $\{\nu(0), \ldots, \nu(l)\} \subset \{\lambda(0), \ldots, \lambda(k)\}$. By (3.9), we obtain

$$|e_\lambda\angle\alpha|_v^2 = \sum_{\nu \in J_l^\lambda} |\alpha_\nu|^2. \quad (3.10)$$

Since, by applying (3.10),

$$\begin{aligned}\sum_{\lambda \in J_k^n} |e_\lambda\angle\alpha|_v^2 &= \sum_{\lambda \in J_k^n} \sum_{\nu \in J_l^\lambda} |\alpha_\nu|^2 = \sum_{\nu \in J_l^n} \sum_{\nu \subset \lambda \in J_k^n} |\alpha_\nu|^2 \\ &= \binom{n-l}{k-l} \sum_{\nu \in J_l^n} |\alpha_\nu|^2 = \binom{n-l}{k-l} |\alpha|_v^2,\end{aligned}$$

the inequality in Lemma 3.4 follows. □

Now assume $\xi \neq 0$ and $\alpha \neq 0$ and set $x = \mathbb{P}(\xi) \in \mathbb{P}\left(\bigwedge_{k+1} V\right)$ and $a = \mathbb{P}(\alpha) \in \mathbb{P}\left(\bigwedge_{l+1} V^*\right)$. We can define the *gauge of x and a for $\angle$*

$$|x\angle a|_v = \frac{|\xi\angle\alpha|_v}{|\xi|_v \cdot |\alpha|_v}. \quad (3.11)$$

In particular, if $k = l = 0$, then $|x\angle a|_v = |x, a|_v$. The projective space $\mathbb{P}\left(\bigwedge_{n+1} V^*\right)$ consists of one and only one point denoted by ∞.

Lemma 3.5. *For all* $x \in \mathbb{P}(V)$, $|x\angle\infty|_v = 1$.

Proof. Take $\xi \in V - \{0\}$ with $x = \mathbb{P}(\xi)$. Put

$$\xi = \xi_0 e_0 + \xi_1 e_1 + \cdots + \xi_n e_n.$$

Then

$$\xi_j = \langle \xi, \epsilon_j \rangle, \ \ j = 0, 1, \ldots, n.$$

For $j \in \mathbb{Z}[0, n]$, setting

$$\hat{\epsilon}_j = (-1)^j \epsilon_0 \wedge \cdots \wedge \epsilon_{j-1} \wedge \epsilon_{j+1} \wedge \cdots \wedge \epsilon_n,$$

we have

$$\big|\xi\angle(\epsilon_0 \wedge \cdots \wedge \epsilon_n)\big|_v = \left| \sum_{j=0}^{n} \langle \xi, \epsilon_j \rangle \hat{\epsilon}_j \right|_v = \left| \sum_{j=0}^{n} \xi_j \hat{\epsilon}_j \right|_v = \big|\xi\big|_v.$$

Since $\infty = \mathbb{P}(\epsilon_0 \wedge \cdots \wedge \epsilon_n)$, then

$$|x\angle\infty|_v = \frac{|\xi\angle(\epsilon_0 \wedge \cdots \wedge \epsilon_n)|_v}{|\xi|_v \cdot |\epsilon_0 \wedge \cdots \wedge \epsilon_n|_v} = 1,$$

and so Lemma 3.5 is proved. □

Next we show a more subtle inequality (cf. Wu [302]):

Lemma 3.6. *Take* $p, q \in \mathbb{Z}[1, n]$ *with* $p + q \leq n + 1$. *If* $\xi \in \bigwedge_p V$ *and* $\eta \in \bigwedge_q V$, *then*

$$|\xi \wedge \eta|_v \leq \varsigma_{v, \binom{p+q}{p}} |\xi|_v |\eta|_v.$$

Proof. First of all, note that a norm on the p-fold tensor product $\otimes_p V$ of V can be defined as follows: Taking a base $\{e_0, \ldots, e_n\}$ of V and writing an element $\xi \in \otimes_p V$ by

$$\xi = \sum \xi_{i_1 \cdots i_p} e_{i_1} \otimes \cdots \otimes e_{i_p}, \tag{3.12}$$

then

$$|\xi|_{v,\otimes} = \begin{cases} \left(\sum |\xi_{i_1 \cdots i_n}|_v^2\right)^{\frac{1}{2}}, & \text{if } v \text{ is Archimedean,} \\ \max\{|\xi_{i_1 \cdots i_n}|_v\}, & \text{if } v \text{ is non-Archimedean.} \end{cases}$$

Let $\mathcal{J}_p$ be the permutation group on $\mathbb{Z}[1, p]$. For each $\lambda \in \mathcal{J}_p$, a linear isomorphism $\lambda : \otimes_p V \longrightarrow \otimes_p V$ is uniquely defined by

$$\lambda(\xi_1 \otimes \cdots \otimes \xi_p) = \xi_{\lambda^{-1}(1)} \otimes \cdots \otimes \xi_{\lambda^{-1}(p)}, \ \ \xi_j \in V \ \ (j = 1, \ldots, p).$$

The linear mapping

$$A_p = \frac{1}{p!}\sum_{\lambda\in\mathcal{J}_p}\operatorname{sgn}(\lambda)\lambda : \otimes_p V \longrightarrow \otimes_p V$$

is called the *anti-symmetrizer of* $\otimes_p V$ with $\operatorname{Im} A_p = \bigwedge_p V$, where $\operatorname{sgn}(\lambda)$ is the sign of the permutation λ, that is,

$$\operatorname{sgn}(\lambda) = \begin{cases} 1, & \text{if } \lambda \text{ is even permutation,} \\ -1, & \text{if } \lambda \text{ is odd permutation.} \end{cases}$$

For the tensor (3.12), we have

$$A_p(\xi) = \sum \xi_{i_1\cdots i_p} e_{i_1}\wedge\cdots\wedge e_{i_p} \in \bigwedge_p V,$$

and hence it is easy to show that $|A_p(\xi)|_v \le \varsigma_{v,p!}|\xi|_{v,\otimes}$, where the elementary inequality

$$(a_1+\cdots+a_n)^2 \le n(a_1^2+\cdots+a_n^2)\ \ (a_i\in\mathbb{R}_+)$$

is used for the proof of the Archimedean case. In particular, if $\xi \in \bigwedge_p V$, then $A_p(\xi) = \xi$. We can obtain the equality $|\xi|_v = c'_p|\xi|_{v,\otimes}$, where

$$c'_p = \begin{cases} \sqrt{p!}, & \text{if } v \text{ is Archimedean,} \\ |p!|_v, & \text{if } v \text{ is non-Archimedean.} \end{cases}$$

Further, if $\eta \in \bigwedge_q V$, noting that

$$\xi\wedge\eta = A_{p+q}(\xi\otimes\eta), \quad |\xi\otimes\eta|_{v,\otimes} = |\xi|_{v,\otimes}|\eta|_{v,\otimes},$$

then we have

$$|\xi\wedge\eta|_v \le \sqrt{(p+q)!}|\xi\otimes\eta|_{v,\otimes} = \binom{p+q}{p}^{\frac{1}{2}}|\xi|_v|\eta|_v$$

if v is Archimedean. If v is non-Archimedean, writing

$$\eta = \sum \eta_{j_1\cdots j_q} e_{j_1}\wedge\cdots\wedge e_{j_q},$$

then

$$\begin{aligned}\xi\wedge\eta &= \sum \xi_{i_1\cdots i_p}\eta_{j_1\cdots j_q} e_{i_1}\wedge\cdots\wedge e_{i_p}\wedge e_{j_1}\wedge\cdots\wedge e_{j_q} \\ &= p!q!\sum_{i_1<\cdots<i_p}\ \sum_{j_1<\cdots<j_q} \xi_{i_1\cdots i_p}\eta_{j_1\cdots j_q} e_{i_1}\wedge\cdots\wedge e_{i_p}\wedge e_{j_1}\wedge\cdots\wedge e_{j_q}\end{aligned}$$

and hence

$$|\xi\wedge\eta|_v \le |p!q!|_v \max|\xi_{i_1\cdots i_p}\eta_{j_1\cdots j_q}|_v \le |p!q!|_v|\xi|_{v,\otimes}|\eta|_{v,\otimes} = |\xi|_v|\eta|_v.$$

Therefore Lemma 3.6 is proved. □

Take $x_j \in \mathbb{P}(V)$ $(j = 0, \ldots, k \leq n)$ and take $\xi_j \in V$ such that $x_j = \mathbb{P}(\xi_j)$. The *gauge of* $x_0, \ldots, x_k$ *for* $\wedge$ is well defined to be

$$|x_0 \wedge \cdots \wedge x_k|_v = \frac{|\xi_0 \wedge \cdots \wedge \xi_k|_v}{|\xi_0|_v \cdots |\xi_k|_v} \tag{3.13}$$

which satisfies

$$0 \leq |x_0 \wedge \cdots \wedge x_k|_v \leq \varsigma_{v,2}\varsigma_{v,3} \cdots \varsigma_{v,k+1} = \varsigma_{v,(k+1)!}.$$

When $k = n$ this is a form of Hadamard's determinant inequality (see [85], [87]).

Lemma 3.7. *For* $x \in \mathbb{P}(V)$, $a_j \in \mathbb{P}(V^*)$, $j = 0, 1, \ldots, n$, *then*

$$|a_0 \wedge \cdots \wedge a_n|_v \leq \varsigma_{v,(n+1)!} \max_{0 \leq j \leq n} |x, a_j|_v.$$

Proof. If $|a_0 \wedge \cdots \wedge a_n|_v = 0$, the inequality is trivial. If $|a_0 \wedge \cdots \wedge a_n|_v > 0$, then $a_0 \wedge \cdots \wedge a_n = \infty$. Thus Lemma 3.5 implies $|x \angle (a_0 \wedge \cdots \wedge a_n)|_v = 1$. For each $j \in \mathbb{Z}[0, n]$, take $\alpha_j \in V^* - \{0\}$ with $\mathbb{P}(\alpha_j) = a_j$. Also take $\xi \in V - \{0\}$ with $\mathbb{P}(\xi) = x$. We have

$$\begin{aligned} |a_0 \wedge \cdots \wedge a_n|_v &= |a_0 \wedge \cdots \wedge a_n|_v \cdot |x \angle (a_0 \wedge \cdots \wedge a_n)|_v \\ &= \frac{|\alpha_0 \wedge \cdots \wedge \alpha_n|_v}{|\alpha_0|_v \cdots |\alpha_n|_v} \cdot \frac{|\xi \angle (\alpha_0 \wedge \cdots \wedge \alpha_n)|_v}{|\xi|_v |\alpha_0 \wedge \cdots \wedge \alpha_n|_v} \\ &= \frac{|\sum_{j=0}^n \langle \xi, \alpha_j \rangle \hat{\alpha}_j|_v}{|\xi|_v |\alpha_0|_v \cdots |\alpha_n|_v}, \end{aligned}$$

and hence

$$\begin{aligned} |a_0 \wedge \cdots \wedge a_n|_v &\leq \varsigma_{v,n+1} \max_{0 \leq j \leq n} \frac{|\langle \xi, \alpha_j \rangle|_v |\hat{\alpha}_j|_v}{|\xi|_v |\alpha_0|_v \cdots |\alpha_n|_v} \\ &= \varsigma_{v,n+1} \max_{0 \leq j \leq n} |x, a_j|_v |a_0 \wedge \cdots \wedge a_{j-1} \wedge a_{j+1} \wedge \cdots \wedge a_n|_v \\ &\leq \varsigma_{v,(n+1)!} \max_{0 \leq j \leq n} |x, a_j|_v. \end{aligned}$$

This finishes the proof. □

3.1.4 General position

Let V be a vector space of finite dimension $n + 1 > 0$ over a field κ. Let $\mathscr{A} = \{a_0, a_1, \ldots, a_q\}$ be a family of points $a_j \in \mathbb{P}(V^*)$. Take $\alpha_j \in V^* - \{0\}$ with $\mathbb{P}(\alpha_j) = a_j$. For $\lambda \in J_l^q$, set $\mathscr{A}_\lambda = \{a_{\lambda(0)}, \ldots, a_{\lambda(l)}\}$, and let $E(\mathscr{A}_\lambda)$ be the linear subspace generated by $\{\alpha_{\lambda(0)}, \ldots, \alpha_{\lambda(l)}\}$ in V^*. Define

$$J_l(\mathscr{A}) = \{\lambda \in J_l^q \mid \alpha_{\lambda(0)} \wedge \cdots \wedge \alpha_{\lambda(l)} \neq 0\}.$$

Then $\mathscr{A}$ is said to be in *general position* if $\dim E(\mathscr{A}_\lambda) = l+1$ for any $\lambda \in J_l^q$ with $l \le \min\{n, q\}$. If $\mathscr{A}$ is in general position, the hyperplanes $\ddot{E}[a_0], \ldots, \ddot{E}[a_q]$ (resp. $\alpha_0, \ldots, \alpha_q$) also are called in *general position*.

Lemma 3.8 ([287]). *Let $\alpha_0, \ldots, \alpha_q$ be $q+1$ vectors in V^* in general position. Take $\xi, \xi' \in V$. If for some index i,*

$$|(\xi \wedge \xi')\angle\alpha_i|_v > A|\xi|_v|\langle\xi, \alpha_i\rangle|_v, \tag{3.14}$$

then there exists a constant $c > 0$ depending only on the α's, an index l depending only on ξ and the α's, and an index j depending also on ξ', such that

$$|\langle\xi \wedge \xi', \alpha_j \wedge \alpha_l\rangle|_v > cA|\xi|_v|\langle\xi, \alpha_i\rangle|_v.$$

Proof. Order the vectors α_i so that,

$$|\langle\xi, \alpha_0\rangle|_v \le \cdots \le |\langle\xi, \alpha_q\rangle|_v. \tag{3.15}$$

Then $\alpha_0, \ldots, \alpha_n$ is a basis for V^*. Let $e_0, \ldots, e_n$ be the corresponding dual basis in V. Then for any vector $\eta \in V$ with coordinates $\eta_0, \ldots, \eta_n$ relative to $e_0, \ldots, e_n$,

$$|\eta|_v \ll \max\{|\eta_0|_v, \ldots, |\eta_n|_v\} \ll |\eta|_v,$$

where, and in the sequel, all constants implicit in $\ll$, etc. will depend only on the α's. Also,

$$|\xi|_v \ll |\xi_n|_v = |\langle\xi, \alpha_n\rangle|_v \ll |\eta|_v.$$

Since the lemma is unchanged if we replace ξ' by $\xi' - a\xi$ for $a \in \kappa$, we may assume $\langle\xi', \alpha_n\rangle = 0$.

We first claim that, with this choice of ξ', (3.14) implies

$$\max_{0\le j\le n} \frac{|\langle\xi', \alpha_j\rangle|_v}{|\langle\xi, \alpha_j\rangle|_v} \gg A.$$

Indeed, just for the proof of this claim, change bases on V again so that the basis is $\{e_0, \ldots, e_{n-1}, u\}$, where u is a unit vector proportional to ξ. By (3.15) both this base change and its inverse have bounded coefficients, so that the sup norm with respect to this basis is equivalent to the length of a vector in V, i.e. the sup norm with respect to the standard basis of V. Relative to this basis, the j-th coordinate of $(\xi \wedge \xi')\angle\alpha_i$ is

$$\begin{vmatrix} \langle\xi, \alpha_i\rangle & \langle\xi', \alpha_i\rangle \\ \xi_j & \xi'_j \end{vmatrix} = \begin{cases} \langle\xi, \alpha_i\rangle\xi'_j, & \text{if } 0 \le j < n, \\ \langle\xi', \alpha_i\rangle\xi_n, & \text{if } j = n. \end{cases}$$

The length of this vector is then

$$|(\xi \wedge \xi')\angle\alpha_i|_v \ll \max\{|\xi|_v|\langle\xi', \alpha_i\rangle|_v, |\xi'|_v|\langle\xi, \alpha_i\rangle|_v\} \ll |(\xi \wedge \xi')\angle\alpha_i|_v;$$

so that

$$\max\left\{\frac{|\langle\xi',\alpha_i\rangle|_v}{|\langle\xi,\alpha_i\rangle|_v},\frac{|\xi'|_v}{|\xi|_v}\right\}\gg A.$$

If the first term in the above max is the larger, than the claim is proved; otherwise, we know that

$$|\langle\xi',\alpha_j\rangle|_v\gg|\xi'|_v\gg A|\xi|_v$$

for some j; since $|\langle\xi,\alpha_j\rangle|_v\ll|\xi|_v$, the claim is again true.

Returning now to the original basis $\{e_0,\dots,e_n\}$, let $l=n$ and let j be such that $|\langle\xi',\alpha_j\rangle|_v/|\langle\xi,\alpha_j\rangle|_v\gg A$, as in the claim. Then

$$\begin{aligned}|\langle\xi\wedge\xi',\alpha_j\wedge\alpha_l\rangle|_v &= \left|\det\begin{pmatrix}\langle\xi,\alpha_j\rangle & \langle\xi',\alpha_j\rangle\\ \langle\xi,\alpha_l\rangle & \langle\xi',\alpha_l\rangle\end{pmatrix}\right|_v\\ &\gg |\langle\xi',\alpha_j\rangle|_v|\xi|_v\\ &\gg A|\langle\xi,\alpha_j\rangle|_v|\xi|_v.\end{aligned}$$

This finishes the proof of Lemma 3.8. □

Following Chen [30], we also use the concept of subgeneral position as follows:

Definition 3.9. Let $\mathscr{A}=\{a_0,a_1,\dots,a_q\}$ be a family of points $a_j\in\mathbb{P}(V^*)$. For $1\le n\le u\le q$, then $\mathscr{A}$ is said to be in *u-subgeneral position* if $E(\mathscr{A}_\lambda)=V^*$ for any $\lambda\in J_u^q$.

In particular, if $u=n$ this concept agrees with the usual concept of hyperplanes in general position. To prove Cartan's conjecture, Nochka used the following technical lemma:

Lemma 3.10. *Let $\mathscr{A}=\{a_0,a_1,\dots,a_q\}$ be a family of points $a_j\in\mathbb{P}(V^*)$ in u-subgeneral position with $1\le n\le u<q$. Then there exists a function $\omega:\mathscr{A}\longrightarrow\mathbb{R}(0,1]$ and a real number $\theta\ge1$ satisfying the properties:*

(1) $0<\omega(a_j)\theta\le1,\ \ j=0,1,\dots,q$;

(2) $q-2u+n=\theta(\sum_{j=0}^q\omega(a_j)-n-1)$;

(3) $1\le\frac{u+1}{n+1}\le\theta\le\frac{2u-n+1}{n+1}$;

(4) $\sum_{j=0}^k\omega(a_{\sigma(j)})\le\dim E(\mathscr{A}_\sigma)$ *if* $\sigma\in J_k^q$ *with* $0\le k\le u$;

(5) *Let $r_0,\dots,r_q$ be a sequence of real numbers with $r_j\ge1$ for all j. Then for any $\sigma\in J_k^q$ with $0\le k\le u$, setting $\dim E(\mathscr{A}_\sigma)=l+1$, then there exists $\lambda\in J_l(\mathscr{A})$ such that*

$$\operatorname{Im}\lambda=\{\lambda(0),\dots,\lambda(l)\}\subset\{\sigma(0),\dots,\sigma(k)\},\quad E(\mathscr{A}_\lambda)=E(\mathscr{A}_\sigma),$$

and

$$\prod_{j=0}^{k} r_{\sigma(j)}^{\omega(a_{\sigma(j)})} \leq \prod_{j=0}^{l} r_{\lambda(j)}.$$

The function ω and the real number θ are respectively called a *Nochka weight* and a *Nochka constant* of the family $\mathscr{A}$ in u-subgeneral position. If $u = n$, then $\theta = 1$ and $\omega(a_j) = 1$ for each $j = 0, 1, \ldots, q$. From Lemma 3.10, it follows that values of the function ω become small if u is large. Hence Nochka weight is a gauge of subgeneral position leaving general position. Nochka's original paper (see [203], [204], [205]) on the weights of Nochka was quite sketchy; a complete proof can be found in Chen's thesis [30] (or see Fujimoto [69], Hu and Yang [103]). Here we omit the proof since it is very long.

Let $\mathscr{A} = \{a_0, a_1, \ldots, a_q\}$ $(n \leq u \leq q)$ be in u-subgeneral position. Associated to a positive number n_v, here we write

$$\sharp x, a_j \sharp_v = |x, a_j|_v^{n_v}, \ \ x \in \mathbb{P}(V).$$

Define the *gauge* $\Gamma_v(\mathscr{A})$ of $\mathscr{A}$ on a valuation v of κ by

$$\Gamma_v(\mathscr{A}) = \frac{1}{\varsigma_{v,(n+1)!}^{n_v}} \inf_{\lambda \in J_n(\mathscr{A})} \{|a_{\lambda(0)} \wedge \cdots \wedge a_{\lambda(n)}|_v^{n_v}\}$$

with $0 < \Gamma_v(\mathscr{A}) \leq 1$.

Lemma 3.11. *For $x \in \mathbb{P}(V)$, $0 < r \in \mathbb{R}$, define*

$$\mathscr{A}(x, r, v) = \{j \in \mathbb{Z}[0, q] \mid \sharp x, a_j \sharp_v < r\}.$$

If $\Gamma_v(\mathscr{A}) \geq r$, then $\#\mathscr{A}(x, r, v) \leq u$.

Proof. Assume, to the contrary, that $\#\mathscr{A}(x, r, v) \geq u + 1$. Then $\lambda \in J_n(\mathscr{A})$ exists such that $\operatorname{Im} \lambda \subseteq \mathscr{A}(x, r, v)$. Hence

$$\sharp x, a_{\lambda(j)} \sharp_v < r, \ \ j = 0, \ldots, n.$$

Then Lemma 3.7 implies

$$\begin{aligned} 0 < \Gamma_v(\mathscr{A}) &\leq |a_{\lambda(0)} \wedge \cdots \wedge a_{\lambda(n)}|_v^{n_v} / \varsigma_{v,(n+1)!}^{n_v} \\ &\leq \max_{0 \leq j \leq n} \sharp x, a_{\lambda(j)} \sharp_v < r \leq \Gamma_v(\mathscr{A}), \end{aligned}$$

which is impossible. Hence we have $\#\mathscr{A}(x, r, v) \leq u$. □

Lemma 3.12. *Take $x \in \mathbb{P}(V)$ such that $\sharp x, a_j\sharp_v > 0$ for $j = 0, \dots, q$. Then*

$$\prod_{j=0}^{q} \left(\frac{1}{\sharp x, a_j \sharp_v} \right)^{\omega(a_j)} \leq \left(\frac{1}{\Gamma_v(\mathscr{A})} \right)^{q-u} \max_{\lambda \in J_n(\mathscr{A})} \prod_{j=0}^{n} \frac{1}{\sharp x, a_{\lambda(j)} \sharp_v}, \tag{3.16}$$

where $\omega : \mathscr{A} \longrightarrow \mathbb{R}(0,1]$ is the Nochka weight. In particular, if $u = n$ we also have

$$\prod_{j=0}^{q} \frac{1}{\sharp x, a_j \sharp_v} \leq \left(\frac{1}{\Gamma_v(\mathscr{A})} \right)^{q+1-n} \max_{\lambda \in J_{n-1}^{q}} \prod_{j=0}^{n-1} \frac{1}{\sharp x, a_{\lambda(j)} \sharp_v}. \tag{3.17}$$

Proof. Take $r = \Gamma_v(\mathscr{A})$. Lemma 3.11 implies $\#\mathscr{A}(x, r, v) \leq u$. Thus $\sigma \in J_u^q$ exists such that $\mathscr{A}(x, r, v) \subset \operatorname{Im} \sigma$. Note that $E(\mathscr{A}_\sigma) = V^*$. By Lemma 3.10, there exists $\lambda \in J_n(\mathscr{A})$ with $\operatorname{Im} \lambda \subset \operatorname{Im} \sigma$ such that $E(\mathscr{A}_\lambda) = E(\mathscr{A}_\sigma)$, and such that

$$\prod_{j=0}^{u} \left(\frac{1}{\sharp x, a_{\sigma(j)} \sharp_v} \right)^{\omega(a_{\sigma(j)})} \leq \prod_{j=0}^{n} \frac{1}{\sharp x, a_{\lambda(j)} \sharp_v}. \tag{3.18}$$

Set $C = \mathbb{Z}[0, q] - \operatorname{Im} \sigma$. Thus $\sharp x, a_j\sharp_v \geq r$ for $j \in C$. Hence

$$\prod_{j \in C} \left(\frac{1}{\sharp x, a_j \sharp_v} \right)^{\omega(a_j)} \leq \prod_{j \in C} \frac{1}{\sharp x, a_j \sharp_v} \leq \left(\frac{1}{r} \right)^{\#C} = \left(\frac{1}{\Gamma_v(\mathscr{A})} \right)^{q-u}.$$

Thus the inequality (3.16) follows.

If $u = n$, then $\sigma = \lambda$ and $\operatorname{Im} \lambda - \mathscr{A}(x, r) \neq \emptyset$, that is, there is some $j_0 \in \mathbb{Z}[0, n]$ such that $\sharp x, a_{\lambda(j_0)}\sharp_v \geq r$. Now (3.18) becomes

$$\prod_{j=0}^{n} \frac{1}{\sharp x, a_{\sigma(j)} \sharp_v} \leq \frac{1}{r} \prod_{j \neq j_0} \frac{1}{\sharp x, a_{\lambda(j)} \sharp_v},$$

and so (3.17) follows. □

3.1.5 Hypersurfaces

Let V be a normed vector space of dimension $n+1 > 0$ over a field κ. Take a positive integer d. Let $\mathcal{J}_d$ be the permutation group on $\mathbb{Z}[1, d]$ and let $\otimes_d V$ be the *d-fold tensor product of V*. For each $\lambda \in \mathcal{J}_d$, a linear isomorphism $\lambda : \otimes_d V \longrightarrow \otimes_d V$ is uniquely defined by

$$\lambda(\xi_1 \otimes \cdots \otimes \xi_d) = \xi_{\lambda^{-1}(1)} \otimes \cdots \otimes \xi_{\lambda^{-1}(d)}, \ \ \xi_j \in V \ \ (j = 1, \dots, d).$$

A vector $\xi \in \otimes_d V$ is said to be *symmetric* if $\lambda(\xi) = \xi$ for all $\lambda \in \mathcal{J}_d$. The set of all symmetric vectors in $\otimes_d V$ is a linear subspace of $\otimes_d V$, denoted by $\amalg_d V$, called the *d-fold symmetric tensor product of V*.

The linear mapping

$$S_d = \frac{1}{d!} \sum_{\lambda \in \mathcal{J}_d} \lambda : \otimes_d V \longrightarrow \otimes_d V$$

is called the *symmetrizer of* $\otimes_d V$ with $\operatorname{Im} S_d = \amalg_d V$. If $\xi \in \amalg_d V$ and $\eta \in \amalg_l V$, the *symmetric tensor product*

$$\xi \amalg \eta = S_{d+l}(\xi \otimes \eta)$$

is defined with $\xi \amalg \eta = \eta \amalg \xi$. Similarly, for $\xi_j \in V$ $(j = 1, \ldots, d)$, we can define the *symmetric tensor product*

$$\xi_1 \amalg \cdots \amalg \xi_d = S_d(\xi_1 \otimes \cdots \otimes \xi_d).$$

Let $\xi^{\amalg d}$ be the d-th *symmetric tensor power* of $\xi \in V$, and define

$$x^{\amalg d} = \mathbb{P}(\xi^{\amalg d})$$

for $x = \mathbb{P}(\xi)$. Thus a mapping $\varphi_d : \mathbb{P}(V) \longrightarrow \mathbb{P}(\amalg_d V)$ is well defined by setting $\varphi_d(x) = x^{\amalg d}$, which is called the *Veronese mapping*. We can identify $\amalg_d V^* = (\amalg_d V)^*$ by

$$\langle \xi_1 \amalg \cdots \amalg \xi_d, \alpha_1 \amalg \cdots \amalg \alpha_d \rangle = \frac{1}{d!} \sum_{\lambda \in \mathcal{J}_d} \langle \xi_1, \alpha_{\lambda(1)} \rangle \cdots \langle \xi_d, \alpha_{\lambda(d)} \rangle$$

for all $x_j \in V, \alpha_j \in V^*, j = 1, \ldots, d$.

Let $\#P$ be the *cardinality* of a set P. We have the following fact:

Lemma 3.13. *Let $J_{n,d}$ be the set of all mappings $\lambda : \mathbb{Z}[0, n] \longrightarrow \mathbb{Z}[0, d]$ such that*

$$|\lambda| = \lambda(0) + \cdots + \lambda(n) = d.$$

Then

$$\#J_{n,d} = \binom{n+d}{d}.$$

Proof. For any given $\lambda = (\lambda(0), \ldots, \lambda(n)) \in J_{n,d}$, we replace each integer $\lambda(i)$ by $\lambda(i)$ stars, making sure of leave all of the commas in place. For example, we would represent the $(n+1)$-tuple $\lambda = (2, 1, 0, 3, 0, 0, 2, 0) \in J_{7,8}$ as follows:

$$\lambda \mapsto (**, *, , * * *, , , **,).$$

The key observation is that the total number of "stars" and "commas" is $n+d = 15$. In other words, to form an $(n+1)$-tuple with $\lambda(0)+\cdots+\lambda(n) = d$, we should start with a row of $n + d$ "commas" and change d of them into stars. Each choice of d commas to change will give us a unique $(n + 1)$-tuple with the desired properties. Hence the total number of $(n + 1)$-tuples is the number of ways of choosing d elements from an ordered set of $n + d$ objects. □

For $\lambda \in J_{n,d}, e = (e_0, \dots, e_n) \in V^{n+1}$, define

$$\lambda! = \lambda(0)! \cdots \lambda(n)!, \quad e^{\amalg\lambda} = e_0^{\amalg\lambda(0)} \amalg \cdots \amalg e_n^{\amalg\lambda(n)} \in \amalg_d V.$$

If $e = (e_0, \dots, e_n)$ is a base of V, then $\{e^{\amalg\lambda}\}_{\lambda\in J_{n,d}}$ is a base of $\amalg_d V$, and $\{\frac{d!}{\lambda!}\epsilon^{\amalg\lambda}\}_{\lambda\in J_{n,d}}$ is the dual base of $\amalg_d V^*$, where $\epsilon = (\epsilon_0, \dots, \epsilon_n)$ is the dual of e, and hence

$$\dim \amalg_d V = \binom{n+d}{d}.$$

The norm $|\cdot|_v$ on V induces norms on $\amalg_d V$ and $\amalg_d V^*$ as follows: For $\eta \in \amalg_d V, \beta \in \amalg_d V^*$ with

$$\eta = \sum_{\lambda\in J_{n,d}} \frac{d!}{\lambda!}\eta_\lambda e^{\amalg\lambda}, \quad \beta = \sum_{\lambda\in J_{n,d}} \frac{d!}{\lambda!}\beta_\lambda \epsilon^{\amalg\lambda},$$

define

$$|\eta|_v = |\eta|_{v,e} = \begin{cases} \left(\sum_{\lambda\in J_{n,d}} \frac{d!}{\lambda!}|\eta_\lambda|_v^2\right)^{\frac{1}{2}}, & \text{if } v \text{ is Archimedean,} \\ \max_{\lambda\in J_{n,d}} \{|\eta_\lambda|_v\}, & \text{if } v \text{ is non-Archimedean} \end{cases}$$

and

$$|\beta|_v = |\beta|_{v,e} = \begin{cases} \left(\sum_{\lambda\in J_{n,d}} \frac{d!}{\lambda!}|\beta_\lambda|_v^2\right)^{\frac{1}{2}}, & \text{if } v \text{ is Archimedean,} \\ \max_{\lambda\in J_{n,d}} \{|\beta_\lambda|_v\}, & \text{if } v \text{ is non-Archimedean,} \end{cases}$$

where e is orthonormal if v is Archimedean. Note that

$$\xi^{\amalg d} = \sum_{\lambda\in J_{n,d}} \frac{d!}{\lambda!}\xi_0^{\lambda(0)} \cdots \xi_n^{\lambda(n)} e^{\amalg\lambda}, \quad \alpha^{\amalg d} = \sum_{\lambda\in J_{n,d}} \frac{d!}{\lambda!}\alpha_0^{\lambda(0)} \cdots \alpha_n^{\lambda(n)} \epsilon^{\amalg\lambda},$$

where

$$\xi = \xi_0 e_0 + \cdots + \xi_n e_n \in V, \quad \alpha = \alpha_0\epsilon_0 + \cdots + \alpha_n\epsilon_n.$$

Then we obtain a formula

$$|\xi^{\amalg d}|_v = |\xi|_v^d, \quad |\alpha^{\amalg d}|_v = |\alpha|_v^d. \tag{3.19}$$

Let $V_{[d]}$ be the vector space of all homogeneous polynomials of degree d on V. We obtain a linear isomorphism

$$\sim: \amalg_d V^* \longrightarrow V_{[d]}$$

defined by

$$\tilde{\alpha}(\xi) = \langle \xi^{\amalg d}, \alpha\rangle, \quad \xi \in V, \ \alpha \in \amalg_d V^*.$$

Thus if $\xi \neq 0$ and $\alpha \neq 0$, the distance $|x^{\amalg d}, a|$ is well defined for $x^{\amalg d} = \mathbb{P}(\xi^{\amalg d})$ and $a = \mathbb{P}(\alpha)$. If $\alpha \neq 0$, the n-dimensional subspace

$$E^d[a] = \mathrm{Ker}(\tilde{\alpha}) = \tilde{\alpha}^{-1}(0)$$

in V depends on a only, and $\ddot{E}^d[a] = \mathbb{P}(E^d[a])$ is a *hypersurface of degree d* in $\mathbb{P}(V)$. Thus $\mathbb{P}(\amalg_d V^*)$ bijectively parameterizes the hypersurfaces in $\mathbb{P}(V)$. Take a sequence $\{d_0, d_1, \ldots, d_q\}$ of positive integers. Let $\mathscr{A} = \{a_0, a_1, \ldots, a_q\}$ be a family of points $a_j \in \mathbb{P}\left(\amalg_{d_j} V^*\right)$. Take $\alpha_j \in \amalg_{d_j} V^* - \{0\}$ with $\mathbb{P}(\alpha_j) = a_j$, and define

$$\tilde{\alpha}_j(\xi) = \langle \xi^{\amalg d_j}, \alpha_j \rangle, \quad \xi \in V, \ \ j = 0, 1, \ldots, q.$$

According to Eremenko and Sodin [58], we will use the following notation:

Definition 3.14. The family $\mathscr{A} = \{a_0, a_1, \ldots, a_q\}$ $(q \geq n)$ is said to be *admissible* (or *in general position*) if, for every $\lambda \in J_n^q$, the system

$$\tilde{\alpha}_{\lambda(i)}(\xi) = 0, \ \ i = 0, 1, \ldots, n \tag{3.20}$$

has only the trivial solution $\xi = 0$ in V.

Next we take a positive integer q with $q \geq n$ and take an admissible family

$$\mathscr{A} = \{a_0, a_1, \ldots, a_q\}, \ \ a_j \in \mathbb{P}\left(\amalg_{d_j} V^*\right).$$

Let $|\cdot|_v$ be a norm defined over a base $e = (e_0, \ldots, e_n)$ of V. Associated to a positive number n_v, here we write

$$\sharp x^{\amalg d_j}, a_j \sharp_v = \left|x^{\amalg d_j}, a_j\right|_v^{n_v}, \ \ x \in \mathbb{P}(V).$$

Lemma 3.15. *There exists a gauge* $\Gamma_v(\mathscr{A})$ *of* $\mathscr{A}$ *with* $0 < \Gamma_v(\mathscr{A}) \leq 1$ *satisfying*

$$\max_{0 \leq i \leq n} \sharp x^{\amalg d_{\lambda(i)}}, a_{\lambda(i)} \sharp_v \geq \Gamma_v(\mathscr{A}), \quad \lambda \in J_n^q, \ \ x \in \mathbb{P}(V). \tag{3.21}$$

Proof. Take $\xi \in V$ with $x = \mathbb{P}(\xi)$ and write $\xi = \xi_0 e_0 + \cdots + \xi_n e_n$. By Theorem 1.48, for each $k \in \{0, \ldots, n\}$, $\lambda \in J_n^q$, the identity

$$\xi_k^s = \sum_{i=0}^{n} b_{ik}^{\lambda}(\xi) \tilde{\alpha}_{\lambda(i)}(\xi) \tag{3.22}$$

is satisfied for some natural number s with

$$s \geq d = \max_{0 \leq j \leq q} d_j,$$

where $b_{ik}^{\lambda} \in \kappa[\xi_0, \dots, \xi_n]$ are homogeneous polynomials of degree $s - d_{\lambda(i)}$ whose coefficients are integral-valued polynomials at the coefficients of $\tilde{\alpha}_{\lambda(i)}$ $(i = 0, \dots, n)$. Write

$$b_{ik}^{\lambda}(\xi) = \sum_{\sigma \in J_{n,s-d_{\lambda(i)}}} b_{\sigma ik}^{\lambda} \xi_0^{\sigma(0)} \cdots \xi_n^{\sigma(n)}, \ \ b_{\sigma ik}^{\lambda} \in \kappa. \tag{3.23}$$

First of all, assume that the norm $|\cdot|_v$ is non-Archimedean. From (3.22) and (3.23), we have

$$|\xi_k|_v^s \le \left(\max_{i,\sigma} \left| b_{\sigma ik}^{\lambda} \right|_v \cdot |\alpha_{\lambda(i)}|_v \right) \max_{0 \le i \le n} \left\{ \frac{|\tilde{\alpha}_{\lambda(i)}(\xi)|_v}{|\xi|_v^{d_{\lambda(i)}} |\alpha_{\lambda(i)}|_v} \right\} |\xi|_v^s. \tag{3.24}$$

Note that

$$\max_{0 \le k \le n} |\xi_k|_v^s = |\xi|_v^s, \quad |\tilde{\alpha}_j(\xi)|_v \le |\xi|_v^{d_j} |\alpha_j|_v. \tag{3.25}$$

By maximizing the inequalities (3.24) over k, $0 \le k \le n$, and using (3.25), we obtain

$$1 \le \max_{k,i,\sigma} \left| b_{\sigma ik}^{\lambda} \right|_v \cdot |\alpha_{\lambda(i)}|_v. \tag{3.26}$$

Define the *gauge*

$$\Gamma_v(\mathscr{A}) = \min_{\lambda \in J_n^q} \min_{k,i,\sigma} \left\{ \frac{1}{\left| b_{\sigma ik}^{\lambda} \right|_v^{n_v} \cdot |\alpha_{\lambda(i)}|_v^{n_v}} \right\}, \tag{3.27}$$

with $0 < \Gamma_v(\mathscr{A}) \le 1$. From (3.24), (3.25) and (3.27), we obtain

$$\Gamma_v(\mathscr{A}) \le \max_{0 \le i \le n} \left\{ \frac{|\tilde{\alpha}_{\lambda(i)}(\xi)|_v}{|\xi|_v^{d_{\lambda(i)}} |\alpha_{\lambda(i)}|_v} \right\}^{n_v},$$

that is, the inequality (3.21) holds.

If the norm $|\cdot|_v$ is Archimedean, now (3.22) and (3.23) imply

$$|\xi_k|_v^s \le \left(\sum_{i=0}^{n} \sum_{\sigma} \left| b_{\sigma ik}^{\lambda} \right|_v \cdot |\alpha_{\lambda(i)}|_v \right) \max_{0 \le i \le n} \left\{ \frac{|\tilde{\alpha}_{\lambda(i)}(\xi)|_v}{|\xi|_{*,v}^{d_{\lambda(i)}} |\alpha_{\lambda(i)}|_v} \right\} |\xi|_{*,v}^s, \tag{3.28}$$

where

$$|\xi|_{*,v} = \max_k |\xi_k|_v.$$

W.l.o.g., we may assume

$$|\xi|_v = \left(|\xi_0|_v^2 + \cdots + |\xi_n|_v^2 \right)^{\frac{1}{2}}.$$

Since $|\xi|_v \le \sqrt{n+1}|\xi|_{*,v}$, inequality (3.28) yields

$$1 \le (n+1)^{\frac{d}{2}} \max_k \sum_{i=0}^{n} \sum_{\sigma} \left| b^{\lambda}_{\sigma ik} \right|_v \cdot |\alpha_{\lambda(i)}|_v. \tag{3.29}$$

Define the *gauge*

$$\Gamma_v(\mathscr{A}) = (n+1)^{-\frac{dn_v}{2}} \min_{\lambda \in J_n^q} \min_k \left\{ \sum_{i=0}^{n} \sum_{\sigma} \left| b^{\lambda}_{\sigma ik} \right| \cdot |\alpha_{\lambda(i)}| \right\}^{-n_v}, \tag{3.30}$$

with $0 < \Gamma_v(\mathscr{A}) \le 1$. From (3.28) and (3.30), we also obtain the inequality (3.21). □

Lemma 3.16. *For $x \in \mathbb{P}(V), 0 < r \in \mathbb{R}$, define*

$$\mathscr{A}(x,r,v) = \left\{ j \;\middle|\; \sharp x^{\amalg d_j}, a_j \sharp_v < r,\ 0 \le j \le q \right\}. \tag{3.31}$$

If $0 < r \le \Gamma_v(\mathscr{A})$, then $\#\mathscr{A}(x,r,v) \le n$.

Proof. Assume that $\#\mathscr{A}(x,r,v) \ge n+1$. Then $\lambda \in J_n^q$ exists such that

$$\{\lambda(0), \ldots, \lambda(n)\} \subseteq \mathscr{A}(x,r,v).$$

Hence

$$\sharp x^{\amalg d_{\lambda(i)}}, a_{\lambda(i)} \sharp_v < r \le \Gamma_v(\mathscr{A}),\ \ i = 0, \ldots, n,$$

which is impossible according to (3.21). □

Lemma 3.17. *Take $x \in \mathbb{P}(V)$ such that $\sharp x^{\amalg d_j}, a_j \sharp_v > 0$ for $j = 0, \ldots, q$. Then*

$$\prod_{j=0}^{q} \frac{1}{\sharp x^{\amalg d_j}, a_j \sharp_v} \le \left(\frac{1}{\Gamma_v(\mathscr{A})} \right)^{q-n} \max_{\lambda \in J_n^q} \left\{ \prod_{i=0}^{n} \frac{1}{\sharp x^{\amalg d_{\lambda(i)}}, a_{\lambda(i)} \sharp_v} \right\} \tag{3.32}$$

$$\le \left(\frac{1}{\Gamma_v(\mathscr{A})} \right)^{q+1-n} \max_{\lambda \in J_{n-1}^q} \left\{ \prod_{i=0}^{n-1} \frac{1}{\sharp x^{\amalg d_{\lambda(i)}}, a_{\lambda(i)} \sharp_v} \right\}. \tag{3.33}$$

Proof. Take $r = \Gamma_v(\mathscr{A})$. Lemma 3.16 implies $\#\mathscr{A}(x,r,v) \le n$. Thus $\sigma \in J_n^q$ exists such that $\mathscr{A}(x,r,v) \subseteq \{\sigma(0), \ldots, \sigma(n)\}$. Note that $\operatorname{Im}\lambda - \mathscr{A}(x,r) \ne \emptyset$ for any $\lambda \in J_n^q$. Then we have

$$\prod_{j=0}^{q} \frac{1}{\sharp x^{\amalg d_j}, a_j \sharp_v} \le r^{n-q} \prod_{i=0}^{n} \frac{1}{\sharp x^{\amalg d_{\sigma(i)}}, a_{\sigma(i)} \sharp_v}$$

$$\le \left(\frac{1}{\Gamma_v(\mathscr{A})} \right)^{q-n} \max_{\lambda \in J_n^q} \left\{ \prod_{i=0}^{n} \frac{1}{\sharp x^{\amalg d_{\lambda(i)}}, a_{\lambda(i)} \sharp_v} \right\}$$

$$\le \left(\frac{1}{\Gamma_v(\mathscr{A})} \right)^{q+1-n} \max_{\lambda \in J_{n-1}^q} \left\{ \prod_{i=0}^{n-1} \frac{1}{\sharp x^{\amalg d_{\lambda(i)}}, a_{\lambda(i)} \sharp_v} \right\},$$

and so Lemma 3.17 is proved. □

3.2 Varieties

Let κ be a field and let $\bar{\kappa}$ be an algebraic closure of κ. The space $\bar{\kappa}^n$ is called the *affine n-space* (over κ), which is usually denoted by $\mathbb{A}^n$ or $\mathbb{A}^n(\bar{\kappa})$. The set of *$\kappa$-rational points* of $\mathbb{A}^n$ is the set

$$\mathbb{A}^n(\kappa) = \{(z_1, \ldots, z_n) \in \mathbb{A}^n \mid z_i \in \kappa\}.$$

We will introduce some geometric notations in spaces $\mathbb{A}^n$ and $\mathbb{P}^n = \mathbb{P}(\mathbb{A}^{n+1})$.

3.2.1 Affine varieties

If S is any subset in the polynomial ring in n variables $\bar{\kappa}[z_1, \ldots, z_n]$, we define the *zero set* of S to be the common zeros of all elements of S, namely

$$Z(S) := \{z \in \mathbb{A}^n \mid P(z) = 0 \text{ for all } P \in S\}.$$

Clearly if $\mathfrak{a}$ is the ideal of $\bar{\kappa}[z_1, \ldots, z_n]$ generated by S, then $Z(S) = Z(\mathfrak{a})$. Furthermore, the Hilbert basis theorem says that $\mathfrak{a}$ is generated by a finite number of polynomials $P_1, \ldots, P_r$. Thus $Z(S)$ can be expressed as the common zeros of the finite set of polynomials $P_1, \ldots, P_r$, that is,

$$Z(S) = \bigcap_{i=1}^{r} Z(P_i).$$

A subset Y of $\mathbb{A}^n$ is an *algebraic set* if there exists a subset $S \subseteq \bar{\kappa}[z_1, \ldots, z_n]$ such that $Y = Z(S)$. If the polynomials in S are of coefficients in some subfield K of $\bar{\kappa}$, we say then that Y is defined over K and denote this as Y/K. We have the following easy properties:

Proposition 3.18. *The union of two algebraic sets is an algebraic set. The intersection of any family of algebraic sets is an algebraic set. The empty set and the whose space are algebraic sets.*

Based on this proposition, we can define the *Zariski topology* on $\mathbb{A}^n$ by taking the open subsets to be the complements of the algebraic sets. An *affine algebraic variety* (or simply *affine variety*) is an irreducible closed subset of $\mathbb{A}^n$ with the induced topology. An open subset of an affine variety is a *quasi-affine variety*. Here recall that a nonempty subset Y of a topological space X is *irreducible* if it cannot be expressed as the union $Y = Y_1 \cup Y_2$ of two proper subsets, each one of which is closed in Y.

For any subset $Y \subseteq \mathbb{A}^n$, let us define the *ideal of* Y in $\bar{\kappa}[z_1, \ldots, z_n]$ by

$$I(Y) = \{P \in \bar{\kappa}[z_1, \ldots, z_n] \mid P(z) = 0 \text{ for all } z \in Y\}.$$

The properties of two mappings Z and I are summarized in the following proposition.

Proposition 3.19. **(a)** *If $S_1 \subseteq S_2$ are subsets of $\bar{\kappa}[z_1, \ldots, z_n]$, then $Z(S_1) \supseteq Z(S_2)$.*

(b) *If $Y_1 \subseteq Y_2$ are subsets of $\mathbb{A}^n$, then $I(Y_1) \supseteq I(Y_2)$.*

(c) *For any two subsets Y_1, Y_2 of $\mathbb{A}^n$, we have $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.*

(d) *For any ideal $\mathfrak{a} \subseteq \bar{\kappa}[z_1, \ldots, z_n]$, $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$, the radical of $\mathfrak{a}$.*

(e) *For any subset $Y \subseteq \mathbb{A}^n$, $Z(I(Y)) = \bar{Y}$, the closure of Y.*

(f) *An algebraic set is irreducible if and only if its ideal is a prime ideal.*

For example, $\mathbb{A}^n$ is irreducible, since it corresponds to the zero ideal in $\bar{\kappa}[z_1, \ldots, z_n]$, which is prime. Let P be an irreducible polynomial in $\bar{\kappa}[z_1, \ldots, z_n]$. Then P generates a prime ideal in $\bar{\kappa}[z_1, \ldots, z_n]$, since $\bar{\kappa}[z_1, \ldots, z_n]$ is a unique factorization domain, so the zero set $Z(P)$ is irreducible. The affine variety $Z(f)$ is called an *affine curve* if $n = 2$, a *surface* if $n = 3$, or a *hypersurface* if $n > 3$. If P has degree d, we say that $Z(P)$ is of *degree* d. A maximal ideal $\mathbf{m}$ of $\bar{\kappa}[z_1, \ldots, z_n]$ corresponds to a minimal irreducible closed subset of $\mathbb{A}^n$, which must be a point, say $a = (a_1, \ldots, a_n)$. This shows that every maximal ideal of $\bar{\kappa}[z_1, \ldots, z_n]$ is of the form

$$\mathbf{m} = (z_1 - a_1, \ldots, z_n - a_n), \ \ \{a_1, \ldots, a_n\} \subset \bar{\kappa}.$$

If $Y \subseteq \mathbb{A}^n$ is an affine algebraic set, the ring

$$\bar{\kappa}[Y] := \bar{\kappa}[z_1, \ldots, z_n]/I(Y) \tag{3.34}$$

is called the *affine coordinate ring* of Y, or simply the *affine ring* of Y. If Y is an affine variety, then $\bar{\kappa}[Y]$ is an integral domain since $I(Y)$ is a prime ideal in $\bar{\kappa}[z_1, \ldots, z_n]$. Furthermore, $\bar{\kappa}[Y]$ is a finitely generated $\bar{\kappa}$-algebra. Conversely, any finitely generated $\bar{\kappa}$-algebra A which is a domain is the affine coordinate ring of some affine variety.

For any non-empty set Y, we let $\mathcal{F}(Y, \bar{\kappa})$ be the set of all functions from Y to $\bar{\kappa}$. Then $\mathcal{F}(Y, \bar{\kappa})$ is made into a ring in the usual way: if $f, g \in \mathcal{F}(Y, \bar{\kappa})$,

$$(f + g)(z) = f(z) + g(z); \quad (fg)(z) = f(z)g(z),$$

for all $z \in Y$. It is usual to identify $\bar{\kappa}$ with the subring of $\mathcal{F}(Y, \bar{\kappa})$ consisting of all constant functions.

If $Y \subseteq \mathbb{A}^n$ is an affine variety, a function $f \in \mathcal{F}(Y, \bar{\kappa})$ is called a *polynomial function* if there is a polynomial $P \in \bar{\kappa}[z_1, \ldots, z_n]$ such that

$$f(z) = P(z), \ \ z = (z_1, \ldots, z_n) \in Y.$$

The polynomial functions form a subring of $\mathcal{F}(Y, \bar{\kappa})$ containing $\bar{\kappa}$. Two polynomials P, Q determine the same function if and only if

$$(P - Q)(z) = 0, \ \ z \in Y,$$

that is, $P - Q \in I(Y)$. Thus we may identify $\bar{\kappa}[Y]$ with the subring of $\mathcal{F}(Y, \bar{\kappa})$ consisting of all polynomial functions on Y.

The quotient field of $\bar{\kappa}[Y]$ on an affine algebraic set Y is called the *function field* of Y over κ, denoted by $\bar{\kappa}(Y)$. An element of $\bar{\kappa}(Y)$ is called a *rational function* on Y, which is the quotient of two polynomial functions on Y such that the denominator does not vanish identically on Y.

If Y is an affine variety, the set of zeros of $I(Y)$ with coordinate $(z_1, \ldots, z_n) \in \kappa^n$ is called the set of *κ-rational points* of Y, and is denoted by $Y(\kappa)$. It is equal to the set of solutions of the finite number of equations

$$P_j(z_1, \ldots, z_n) = 0, \quad j = 1, \ldots, r, \ \ (z_1, \ldots, z_n) \in \kappa^n.$$

A topological space X is called *Noetherian* if it satisfies the *descending chain condition* for closed subsets: for any sequence $Y_1 \supseteq Y_2 \supseteq \cdots$ of closed subsets, there is an integer r such that $Y_r = Y_{r+1} = \cdots$. For example, $\mathbb{A}^n$ is a Noetherian topological space. indeed, if $Y_1 \supseteq Y_2 \supseteq \cdots$ is a descending chain of closed subsets, then $I(Y_1) \subseteq I(Y_2) \subseteq \cdots$ is an ascending chain of ideals in $\bar{\kappa}[z_1, \ldots, z_n]$. Since $\bar{\kappa}[z_1, \ldots, z_n]$ is a Noetherian ring, this chain of ideals is eventually stationary. But for each i, $Y_i = Z(I(Y_i))$, so the chain Y_i is also stationary.

Proposition 3.20. *In a Noetherian topological space X, every nonempty closed subset Y can be expressed as a finite union $Y = Y_1 \cup \cdots \cup Y_r$ of irreducible closed subsets Y_i. If we require that $Y_i \not\supseteq Y_j$ for $i \neq j$, then the Y_i are uniquely determined. They are called the irreducible components of Y.*

Proof. Let $\mathcal{C}$ be the set of nonempty closed subsets of X which cannot be written as a finite union of irreducible closed subsets. If $\mathcal{C}$ is nonempty, then since X is Noetherian, it must contain a minimal element, say Y. Then Y is not irreducible, by construction of $\mathcal{C}$. Thus we can write $Y = Y' \cup Y''$, where Y' and Y'' are proper closed subsets of Y. By minimality of Y, each of Y' and Y'' can be expressed as a finite union of closed irreducible subsets, hence Y also, which is a contradiction. It follows that every closed set Y can be written as a union $Y = Y_1 \cup \cdots \cup Y_r$ of irreducible closed subsets. By throwing away a few if necessary, we may assume $Y_i \not\supseteq Y_j$ for $i \neq j$.

Now suppose $Y = Y_1' \cup \cdots \cup Y_s'$ is another such representation. Then

$$Y_1' \subseteq Y = Y_1 \cup \cdots \cup Y_r,$$

so $Y_1' = \cup (Y_1' \cap Y_i)$. But Y_1' is irreducible, so $Y_1' \subseteq Y_i$ for some i, say $i = 1$. Similarly, $Y_1 \subseteq Y_j'$ for some j. Then $Y_1' \subseteq Y_j'$, so $j = 1$, and we find that $Y_1 = Y_1'$. Now let $Z = \overline{Y - Y_1}$. Then $Z = Y_2 \cup \cdots \cup Y_r$ and so $Z = Y_2' \cup \cdots \cup Y_s'$. So proceeding by induction on r, we obtain the uniqueness of the Y_i. □

Corollary 3.21. *Every algebraic set in $\mathbb{A}^n$ can be expressed uniquely as a union of varieties, no one containing another.*

If X is a topological space, we define the *dimension* of X (denoted $\dim(X)$) to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X. We define the *dimension* of an affine or quasi-affine variety to be its dimension as a topological space.

Proposition 3.22. *If Y is an affine algebraic set, then the dimension of Y is equal to the dimension of its affine coordinate ring $\bar{\kappa}[Y]$.*

Proof. If Y is an affine algebraic set in $\mathbb{A}^n$, then the closed irreducible subsets of Y correspond to prime ideals of $\bar{\kappa}[z_1, \ldots, z_n]$ containing $I(Y)$. These in turn correspond to prime ideals of $\bar{\kappa}[Y]$. Hence $\dim(Y)$ is the length of the longest chain of prime ideals in $\bar{\kappa}[Y]$, which is its dimension. □

Theorem 3.23. *Let κ be a field, and let A be an integral domain which is a finitely generated κ-algebra. Then*

(A) *the dimension of A is equal to the transcendence degree of the quotient field of A over κ;*

(B) *For any prime ideal $\mathfrak{p}$ in A, we have*

$$\operatorname{height}(\mathfrak{p}) + \dim(A/\mathfrak{p}) = \dim(A).$$

Proof. Matsumura [173], Ch. 5, § 14 or, in the case κ is algebraically closed, Atiyah–Macdonald [2], Ch. 11. □

Proposition 3.24. *The dimension of $\mathbb{A}^n$ is n.*

Proof. According to Proposition 3.22 this means that the dimension of the polynomial ring $\bar{\kappa}[z_1, \ldots, z_n]$ is n, which follows from part (A) of Theorem 3.23. □

Proposition 3.25. *If Y is a quasi-affine variety, then $\dim(Y) = \dim(\bar{Y})$.*

Proof. Hartshorne [90], Ch. I, Proposition 1.10. □

Proposition 3.26. *A variety Y in $\mathbb{A}^n$ has dimension $n-1$ if and only if it is the zero set $Z(P)$ of a single nonconstant irreducible polynomial in $\bar{\kappa}[z_1, \ldots, z_n]$.*

Proof. If P is an irreducible polynomial, we have already seen that $Z(P)$ is a variety. Its ideal is the prime ideal $\mathfrak{p} = (P)$. By Theorem 1.16, $\mathfrak{p}$ has height 1, so by Theorem 3.23, $Z(P)$ has dimension $n-1$.

Conversely, a variety of dimension $n-1$ corresponds to a prime ideal $\mathfrak{p}$ of height 1. Now the polynomial ring $\bar{\kappa}[z_1, \ldots, z_n]$ is a unique factorization domain, so by Proposition 1.17, $\mathfrak{p}$ is principal, necessarily generated by an irreducible polynomial P. Hence $Y = Z(P)$. □

3.2.2 Projective varieties

A *graded ring* is a ring A, together with a decomposition

$$A = \sum_{r \geq 0} A_r$$

of A into a direct sum of Abelian groups A_r, such that for any $r, s \geq 0$, $A_r \cdot A_s \subseteq A_{r+s}$. An element of A_r is called a *homogeneous element of degree* r. Thus any element of A can be written uniquely as a finite sum of homogeneous elements. An ideal $\mathfrak{a} \subseteq A$ is a *homogeneous ideal* if

$$\mathfrak{a} = \sum_{r \geq 0} \mathfrak{a} \cap A_r.$$

An ideal is homogeneous if and only if it can be generated by homogeneous elements. The sum, product, intersection, and radical of homogeneous ideals are homogeneous. To test whether a homogeneous ideal is prime, it is sufficient to show for any two homogeneous elements f, g, that $fg \in \mathfrak{a}$ implies $f \in \mathfrak{a}$ or $g \in \mathfrak{a}$.

Let κ be a field and let $\bar{\kappa}$ be an algebraic closure of κ. We make the polynomial ring $A = \bar{\kappa}[\xi_0, \ldots, \xi_n]$ into a graded ring by taking A_d to be the set of all linear combinations of monomials of total weight d in $\xi_0, \ldots, \xi_n$. If f is a homogeneous polynomial of degree d, then

$$f(\lambda\xi_0, \ldots, \lambda\xi_n) = \lambda^d f(\xi_0, \ldots, \xi_n),$$

so that the property of f being zero or not depends only on the equivalence class x of $(\xi_0, \ldots, \xi_n)$. Thus f gives a function from $\mathbb{P}^n = \mathbb{P}(\mathbb{A}^{n+1})$ to $\{0, 1\}$ by $f(x) = 0$ if $f(\xi_0, \ldots, \xi_n) = 0$, and $f(x) = 1$ if $f(\xi_0, \ldots, \xi_n) \neq 1$. Thus we can talk about the *zeros* of a homogeneous polynomial $f \in A_d$, namely

$$Z(f) = \{x \in \mathbb{P}^n \mid f(x) = 0\}.$$

If S is any set of homogeneous elements of A, we define the *zero set* of S to be

$$Z(S) = \{x \in \mathbb{P}^n \mid f(x) = 0 \text{ for all } f \in S\}.$$

If $\mathfrak{a}$ is a homogeneous ideal of A, we define $Z(\mathfrak{a}) = Z(S)$, where S is the set of all homogeneous elements in $\mathfrak{a}$. Since A is a Noetherian ring, any set of homogeneous elements S has a finite subset $f_1, \ldots, f_r$ such that $Z(S) = Z(f_1, \ldots, f_r)$.

A subset X of $\mathbb{P}^n$ is an *algebraic set* if there exists a set S of homogeneous elements of A such that $X = Z(S)$. The following properties are basic:

Proposition 3.27. *The union of two algebraic sets is an algebraic set. The intersection of any family of algebraic sets is an algebraic set. The empty set and the whose space are algebraic sets.*

Thus we can define the *Zariski topology* on $\mathbb{P}^n$ by taking the (*Zariski*) *open subsets* to be the complements of algebraic sets. A *projective algebraic variety* (or simply *projective variety*) is an irreducible algebraic set X in $\mathbb{P}^n$, with the induced topology by the inclusion $X \subset \mathbb{P}^n$, that is, there exists a prime homogeneous ideal $\mathfrak{p}$ of A such that $X = Z(\mathfrak{p})$. If $\mathfrak{p} = (f)$ for some $f \in A_d$, the variety X is called a *projective hypersurface of degree* d. Further, if f is linear, X is called a *hyperplane*.

An open subset of a projective variety is a *quasi-projective variety*. The *dimension* of a projective or quasi-projective variety is its dimension as a topological space.

For any subset $X \subseteq \mathbb{P}^n$, we define the *homogeneous ideal of* X in A by

$$I(X) = \{f \in A \mid f \text{ is homogeneous and } f(x) = 0 \text{ for all } x \in X\}.$$

If X is an algebraic set, we define the *homogeneous coordinate ring* of X to be $A/I(X)$. An element $f \in A/I(X)$ will ba called a *form* of degree d if there is an element $F \in A_d$ whose equivalent class modulo $I(X)$ is f.

If K is a field containing κ, by $X(K)$ we mean the set of such zeros having some projective coordinates $[\xi_0, \ldots, \xi_n]$ with $\xi_i \in K$ for all $i = 0, \ldots, n$, called the set of *K-rational points* of X. The set of points in $X(\bar{\kappa})$ is called the set of *algebraic points* over κ. For a point $x = [\xi_0, \ldots, \xi_n] \in \mathbb{P}^n$, we denote by $\kappa(x)$ the field

$$\kappa(x) = \kappa(\xi_0, \ldots, \xi_n)$$

such that at least one of the projective coordinates is equal to 1, which is called the *field of definition* of the point x or the *residue class field of the point*. It does not matter which such coordinate is selected. If for instance $\xi_0 \neq 0$, then

$$\kappa(x) = \kappa\left(\frac{\xi_1}{\xi_0}, \ldots, \frac{\xi_n}{\xi_0}\right).$$

Let X be a projective variety in $\mathbb{P}^n$. Then $I(X)$ is a prime ideal, and so the homogeneous coordinate ring of X

$$\bar{\kappa}_{\mathrm{HCR}}[X] = \bar{\kappa}[\xi_0, \ldots, \xi_n]/I(X)$$

is a domain. Every element $f \in \bar{\kappa}_{\mathrm{HCR}}[X]$ may be written uniquely as

$$f = f_0 + \cdots + f_m,$$

where f_d is a form of degree d. In contrast with the case of affine varieties, no elements of $\bar{\kappa}_{\mathrm{HCR}}[X]$ except the constants determine functions on X.

Let $\bar{\kappa}_{\mathrm{HCR}}(X)$ be the quotient field of $\bar{\kappa}_{\mathrm{HCR}}[X]$, called the *homogeneous function field* of X. Likewise most elements of $\bar{\kappa}_{\mathrm{HCR}}(X)$ cannot be regarded as functions on X. However, if f, g are both forms in $\bar{\kappa}_{\mathrm{HCR}}[X]$ of same degree d, then f/g define a function on X, at least where g is not zero, since

$$\frac{f(\lambda\xi_0, \ldots, \lambda\xi_n)}{g(\lambda\xi_0, \ldots, \lambda\xi_n)} = \frac{\lambda^d f(\xi_0, \ldots, \xi_n)}{\lambda^d g(\xi_0, \ldots, \xi_n)} = \frac{f(x)}{g(x)},$$

so the value of f/g is independent of the choice of homogeneous coordinates. The *function field* of X, written $\bar{\kappa}(X)$, is defined to be

$$\bar{\kappa}(X) = \left\{ \frac{f}{g} \in \bar{\kappa}_{\mathrm{HCR}}(X) \;\middle|\; f, g \in \bar{\kappa}_{\mathrm{HCR}}[X] \text{ are forms of same degree} \right\}.$$

It is not difficult to verify that $\bar{\kappa}(X)$ is a subfield of $\bar{\kappa}_{\mathrm{HCR}}(X)$ satisfying

$$\bar{\kappa} \subset \bar{\kappa}(X) \subset \bar{\kappa}_{\mathrm{HCR}}(X).$$

Elements of $\bar{\kappa}(X)$ are called *rational functions* on X.

A projective variety X is covered by a finite number of affine varieties as follows. Let $\mathfrak{p}$ be a prime homogeneous ideal of A with $X = Z(\mathfrak{p})$. Then there are homogeneous polynomials $f_1, \ldots, f_r$ in A generating $\mathfrak{p}$. Set

$$z_{l,i+1} = \begin{cases} \frac{\xi_i}{\xi_l}, & 0 \le i \le l-1, \\ \frac{\xi_{i+1}}{\xi_l}, & l \le i < n, \end{cases}$$

and let

$$P_{l,j}(z_{l,1}, \ldots, z_{l,n}) = f_j(z_{l,1}, \ldots, z_{l,l}, 1, z_{l,l+1}, \ldots, z_{l,n}).$$

Then the polynomials $P_{l,1}, \ldots, P_{l,r}$ generate a prime ideal in $\bar{\kappa}[z_{l,1}, \ldots, z_{l,n}]$, and the set of solutions of the equations

$$P_{l,j}(z_{l,1}, \ldots, z_{l,n}) = 0, \;\; j = 1, \ldots, r$$

is an affine variety, which is an open subset of X, denoted by U_l. It consists of those points $[\xi_0, \ldots, \xi_n] \in X$ such that $\xi_l \neq 0$. The projective variety X is covered by the open sets $U_0, \ldots, U_n$. The function fields $\bar{\kappa}(U_0), \ldots, \bar{\kappa}(U_n)$ are all equal, and are generated by the restrictions to X of the quotients ξ_i/ξ_l (for all i, l such that ξ_l is not identically 0 on X). The *function field* $\bar{\kappa}(X)$ of X over $\bar{\kappa}$ is isomorphic to be $\bar{\kappa}(U_l)$ (for any l). In particular, the function fields of $\mathbb{A}^n$ and $\mathbb{P}^n$ are both equal to $\bar{\kappa}(z_1, \ldots, z_n)$, the field of rational functions in n variables.

A variety X is *complete* or *proper* if for any variety Y, the projection $X \times Y \longrightarrow Y$ is closed, i.e., the image of every closed subset is closed. Projective varieties are complete.

3.2.3 Local rings of varieties

Let X be an affine variety in $\mathbb{A}^n$. If $f \in \bar{\kappa}(X)$ is a rational function on X, and $x \in X$, then f is called *regular at* x if there are some $P, Q \in \bar{\kappa}[X]$ such that $Q(x) \neq 0$ and $f = P/Q$ on X. We can then define the *value* of f at x, written $f(x)$, as follows: $f(x) = P(x)/Q(x)$, which is independent of the choice of P and Q.

We define $\mathcal{O}_X(x)$, or simply by $\mathcal{O}(x)$ if no confusion is likely to arise, to be the set of rational functions on X which are regular at x. It is easy to verify that $\mathcal{O}_X(x)$ forms a subring of $\bar{\kappa}(X)$ satisfying

$$\bar{\kappa} \subset \bar{\kappa}[X] \subset \mathcal{O}_X(x) \subset \bar{\kappa}(X).$$

We call $\mathcal{O}_X(x)$ the *local ring* of X at x. The ideal of $\mathcal{O}_X(x)$

$$\mathbf{m}_X(x) = \mathbf{m}(x) = \{f \in \mathcal{O}_X(x) \mid f(x) = 0\}$$

is called the *maximal ideal* of X at x. It is the kernel of the evaluation surjective homomorphism

$$f \in \mathcal{O}_X(x) \longmapsto f(x) \in \bar{\kappa},$$

so we obtain the isomorphism:

$$\mathcal{O}_X(x)/\mathbf{m}_X(x) \cong \bar{\kappa}.$$

An element $f \in \mathcal{O}_X(x)$ is a unit in $\mathcal{O}_X(x)$ if and only if $f(x) \neq 0$, so $\mathbf{m}_X(x)$ is the set of non-units in $\mathcal{O}_X(x)$. Hence $\mathcal{O}_X(x)$ is really a local ring. Further, $\mathcal{O}_X(x)$ is a Noetherian domain (cf. [71]).

The set of points $x \in X$ where a rational function f is not regular is called the *pole set* of f.

Proposition 3.28. **(1)** *The pole set of a rational function on X is an algebraic subset of X.*

(2)

$$\bar{\kappa}[X] = \bigcap_{x \in X} \mathcal{O}_X(x).$$

Proof. See Fulton [71], Chapter 2, Proposition 2. □

Let X be a projective variety in $\mathbb{P}^n$. If $f \in \bar{\kappa}(X)$ is a rational function on X, and $x \in X$, then f is called *regular at* x if f can be written as $f = P/Q$, where P and Q are forms of the same degree, and $Q(x) \neq 0$. We define $\mathcal{O}_X(x)$ to be the set of rational functions on X which are regular at x. Similarly, $\mathcal{O}_X(x)$ is a subring of $\bar{\kappa}(X)$. It also is a *local ring* with *maximal ideal*

$$\mathbf{m}_X(x) = \mathbf{m}(x) = \{P/Q \in \mathcal{O}_X(x) \mid P(x) = 0,\ Q(x) \neq 0\}$$

The *value* $f(x)$ of a function $f \in \mathcal{O}_X(x)$ is well-defined.

Generally, let X be a (projective or affine) variety. We say that a rational function f on X is *regular on* X if it is regular at every point of X. We denote by $\mathcal{O}(X)$ the ring of all regular functions on X. A regular function on a projective variety is constant (see [90], I.3.4(a)). Note that the property of being regular is open, that is, if f is regular

at x, then it is regular at every point in some neighborhood of x. A variety is called *normal* if the local ring of every point is integrally closed. A non-singular variety is normal.

By a *subvariety* of a variety X we shall always mean a closed subvariety unless otherwise specified. Let $Y \subset X$ be a subvariety of a variety X. The *local ring of X along Y*, denoted by $\mathcal{O}_X(Y)$, is the set of pairs (U, f), where U is an open subset of X with $U \cap Y \neq \emptyset$ and $f \in \mathcal{O}(U)$ is a regular function on U, where we identify two pairs $(U, f) = (W, g)$ if $f = g$ on $U \cap W$. The ring $\mathcal{O}_X(Y)$ is a local ring, its unique maximal ideal being given by

$$\mathbf{m}_X(Y) = \{f \in \mathcal{O}_X(Y) \mid f(x) = 0 \text{ for all } x \in Y\}.$$

A mapping $\varphi : X \longrightarrow Y$ between varieties is a *morphism* if it is continuous, and if for every open set $V \subset Y$ and every regular function g on V, the function $g \circ \varphi$ is regular on $\varphi^{-1}(V)$. Note that the image of a projective variety by a morphism is a projective variety (see [98], Theorem A.1.2.3). On the other hand, morphisms have the following *rigidity*:

Proposition 3.29. *Let X be a projective variety, let Y and Z be any varieties, and let $\varphi : X \times Y \longrightarrow Z$ be a morphism. Suppose that there is a point $y_0 \in Y$ such that φ is constant on $X \times \{y_0\}$. Then φ is constant on every slice $X \times \{y\}$. If φ is also constant on some slice $\{x_0\} \times Y$, then φ is a constant mapping on all of $X \times Y$.*

Proof. See [98], Lemma A.7.1.1. □

A mapping $\varphi : X \longrightarrow Y$ between varieties is *regular* at a point $x \in X$ if it is a morphism on some open neighborhood of x. One can show that φ is regular at x if there is an affine neighborhood $U \subset \mathbb{A}^m$ of x in X and an affine neighborhood $V \subset \mathbb{A}^n$ of $\varphi(x)$ in Y such that φ sends U into V and such that φ can be defined on U by n polynomials in m variables. That these definitions are equivalent comes from the fact that a morphism of affine varieties is defined globally by polynomials, as can be deduced readily from Theorem 3.30 below. If $\varphi : X \longrightarrow Y$ is regular at each point of X, then φ is said to be a *regular mapping*.

A regular mapping $\varphi : X \longrightarrow Y$ is an *isomorphism* if it has an inverse, that is, if there exists a regular mapping $\psi : Y \longrightarrow X$ such that both $\varphi \circ \psi : Y \longrightarrow Y$ and $\psi \circ \varphi : X \longrightarrow X$ are the identity mappings. In this case we say that X and Y are *isomorphic*. An isomorphism from X to itself is also called an *automorphism* on X. The group $\mathrm{Aut}(X)$ of automorphisms of X is an extremely interesting object. For example, some examples of $\mathrm{Aut}(\mathbb{A}^2)$ are simple to construct: the affine linear mappings, and *elementary mappings* of the form

$$y_1 = \alpha x_1 + f(x_2), \quad y_2 = \beta x_2 + \gamma, \tag{3.35}$$

where α, β, γ are constants with $\alpha\beta \neq 0$, and f a polynomial. It is known that the whole group $\mathrm{Aut}(\mathbb{A}^2)$ is generated by these automorphisms in the sense that every

element of $\mathrm{Aut}(\mathbb{A}^2)$ is a finite composition of the affine linear mappings and the elementary mappings (cf. [120]). A famous unsolved problem related to automorphisms of $\mathbb{A}^n$ is the *Jacobian conjecture*. This asserts that, if the ground field κ has characteristic 0, a mapping given by

$$y_i = f_i(x_1, \ldots, x_n), \;\; i = 1, \ldots, n$$

with $f_i \in \bar{\kappa}[x_1, \ldots, x_n]$ is an automorphism of $\mathbb{A}^n$ if and only if the Jacobian determinant $\det\left(\frac{\partial f_i}{\partial y_j}\right)$ is a nonzero constant (cf. [7]). The necessity is easy. For the case $n = 2$, this conjecture is proved when the degrees of f_1 and f_2 are not too large (the order of 100).

A *rational mapping* from a variety X to a variety Y is a mapping that is a morphism on some nonempty open subset of X. Let $\varphi : X \longrightarrow Y$ be a rational mapping. Then there is a largest open subset Ω on which φ is a morphism. This open subset is called the *domain of definition* of φ, denoted $\mathrm{dom}(\varphi)$. The rational mapping φ is said to be *dominant* if $\varphi(U)$ is dense in Y for some (and consequently every) nonempty open set $U \subset X$ on which it is a morphism. A *birational mapping* is a rational mapping that has a rational inverse. Two varieties are said to be *birationally equivalent* if there is a birational mapping between them.

Theorem 3.30. *Let Z and Z' be affine varieties. Then*

(i) $\mathcal{O}(Z) \cong \bar{\kappa}[Z]$*;*

(ii) *a morphism $\varphi : Z \longrightarrow Z'$ induces a ring homomorphism $\varphi^* : \bar{\kappa}[Z'] \longrightarrow \bar{\kappa}[Z]$ defined by $g \mapsto g \circ \varphi$. The natural mapping*

$$\mathrm{Mor}(Z, Z') \longrightarrow \mathrm{Hom}_{\bar{\kappa}}(\bar{\kappa}[Z'], \bar{\kappa}[Z])$$

defined by $\varphi \mapsto \varphi^*$ is a bijection;

(iii) *for each $P \in Z$, let $\mathfrak{m}_P \subseteq \bar{\kappa}[Z]$ be the ideal of functions vanishing at P. Then $P \longmapsto \mathfrak{m}_P$ gives a $1-1$ correspondence between the points of Z and the maximal ideals of $\bar{\kappa}[Z]$;*

(iv) *for each P, $\mathcal{O}(P) \cong \bar{\kappa}[Z]_{\mathfrak{m}_P}$, and $\dim \mathcal{O}(P) = \dim Z$;*

(v) *$\bar{\kappa}(Z)$ is isomorphic to the quotient field of $\bar{\kappa}[Z]$, and hence $\bar{\kappa}(Z)$ is a finitely generated extension field of κ, of transcendence degree $= \dim Z$.*

Proof. Hartshorne [90], I.3.2. □

If $\varphi : Z \longrightarrow Z'$ is a morphism between affine varieties, we may view $\bar{\kappa}[Z]$ as a $\bar{\kappa}[Z']$-module by means of φ^*. The morphism φ is called *finite* if $\bar{\kappa}[Z]$ is a finitely generated $\bar{\kappa}[Z']$-module. A morphism $\varphi : X \longrightarrow Y$ between varieties is *finite* if for every affine open subset $V \subset Y$, the set $\varphi^{-1}(V)$ is affine and the mapping $\varphi : \varphi^{-1}(V) \longrightarrow V$ is finite.

A mapping φ between affine varieties is dominant if and only if φ^* is injective, so we say that φ is *finite surjective* if it is finite and φ^* is injective. If $\varphi : X \longrightarrow Y$ is a finite mapping, then it is a closed mapping and all fibers $\varphi^{-1}(y)$ consist of a finite number of points. Further, there is an integer d and a nonempty open $V \subset \varphi(X)$ such that

$$\#\varphi^{-1}(y) = d, \;\; y \in V.$$

The degree d can be described algebraically as the degree of the associated field extension, and we define this quantity to be the *degree of the finite mapping* φ,

$$\deg(\varphi) = [\bar{\kappa}(X) : \varphi^*\bar{\kappa}(Y)].$$

Example 3.31. Let $m, n \geq 1$ be integers and let $N = (m+1)(n+1) - 1$. We define the *Segre mapping*

$$S_{m,n} : \mathbb{P}^m \times \mathbb{P}^n \longrightarrow \mathbb{P}^N$$

by the formula

$$(x, y) \longmapsto [x_i y_j \mid 0 \leq i \leq m, 0 \leq j \leq n]$$

where we have written

$$x = [x_0, \ldots, x_m] \in \mathbb{P}^m, \quad y = [y_0, \ldots, y_n] \in \mathbb{P}^n.$$

The Segre mappings are morphisms and give embeddings of the product $\mathbb{P}^m \times \mathbb{P}^n$ into $\mathbb{P}^N$.

3.2.4 Dimensions

The *dimension* of a variety X is defined to be the transcendence degree of its function field $\bar{\kappa}(X)$ over $\bar{\kappa}$ (cf. [71], [98]), denoted by $\dim X$. There is another definition of dimension. Consider a maximal chain of subvarieties

$$Y_0 \subset Y_1 \subset \cdots \subset Y_m = X,$$

where Y_0 is a point and $Y_i \neq Y_{i+1}$ for all i. Then all such chains have the same number of elements m, and m is the *dimension* of X (cf. [98], [150]). In particular, we have the following useful corollary.

Proposition 3.32. *Let X be a variety, and let Y be a subvariety of X. If $Y \neq X$, then* $\dim Y < \dim X$.

Proof. Hindry–Silverman [98], Corollary A.1.3.3 or Shafarevich [239], I.6, Theorem 1. □

If $Y \subset X$ is a closed subvariety of X, then the number $\dim X - \dim Y$ is called the *codimension* of Y in X, and written $\operatorname{codim}(Y)$ or $\operatorname{codim}_X(Y)$. Not surprisingly, both $\mathbb{A}^n$ and $\mathbb{P}^n$ have dimension n. Similarly, the dimension of a hypersurface in $\mathbb{A}^n$ or $\mathbb{P}^n$ is $n - 1$. In fact, a kind of converse is true.

Theorem 3.33. *A variety of dimension $n-1$ is birational equivalent to a hypersurface in $\mathbb{A}^n$ or $\mathbb{P}^n$.*

Proof. See Hindry and Silverman [98], or Hartshorne [90], Ch. I, Proposition 4.9. Main idea is that the function field $\bar{\kappa}(X)$ of the variety X of dimension $n-1$ over $\bar{\kappa}$ is a finitely generated extension of $\bar{\kappa}$ so that $\bar{\kappa}(X)$ is separably generated (see Zariski and Samuel [307], Ch. II, Theorem 31, p. 105, or Matsumura [173], Ch. 10, Corollary, p. 194). Hence we can find a transcendence base $\{x_1, \ldots, x_{n-1}\} \subset \bar{\kappa}(X)$ such that $\bar{\kappa}(X)$ is a finite separable extension of $\bar{\kappa}(x_1, \ldots, x_{n-1})$. Then by Theorem 1.70, we can find one further element $x_n \in \bar{\kappa}(X)$ such that $\bar{\kappa}(X) = \bar{\kappa}(x_1, \ldots, x_{n-1}, x_n)$. Now x_n is algebraic over $\bar{\kappa}(x_1, \ldots, x_{n-1})$, so it satisfies a polynomial equation with coefficients which are rational functions in $x_1, \ldots, x_{n-1}$. Clearing denominators, we obtain an irreducible polynomial $f(x_1, \ldots, x_n) = 0$. This defines a hypersurface in $\mathbb{A}^n$ with function field $\bar{\kappa}(X)$, which is birational to X. Its projective closure is a hypersurface in $\mathbb{P}^n$. □

The *dimension* of an algebraic subset V is the maximum of the dimensions of its irreducible components. If all the irreducible components of V have the same (finite) dimension d, then V is said to be of *pure dimension* d. If V is an algebraic subset of $\mathbb{A}^n$ (or $\mathbb{P}^n$) of dimension $n-r$, defined by r equations

$$f_j = 0, \;\; j = 1, \ldots, r,$$

then we say that V is a *complete intersection*.

Theorem 3.34. *Any affine variety of dimension d can be realized as an irreducible component of some affine complete intersection of pure dimension d.*

Proof. C. Musili [198], Theorem 25.7. □

To conform with the usual terminology, a variety of dimension one is called a *curve*, and a variety of dimension two is called a *surface*. If κ is a subfield of $\mathbb{C}$, then $X(\mathbb{C})$ is a complex analytic space of complex analytic dimension 1. Now a curve is also sometimes called a *Riemann surface*.

In order to compute the dimension of a variety, we need to know how the dimension behaves for intersections of algebraic sets, which is answered by the *affine* (or *projective*) *dimension theorem*:

Theorem 3.35. *Let X and Y be varieties in $\mathbb{A}^n$ (or $\mathbb{P}^n$) of dimensions l and m, respectively. Then every component of $X \cap Y$ has dimension at least $l + m - n$.*

Proof. Hindry–Silverman [98] or Shafarevich [239] or Hartshorne [90], Ch. I, Proposition 7.1 and Theorem 7.2. □

Theorem 3.36. *Let $\varphi : X \longrightarrow Y$ be a surjective morphism of varieties. Then*
(I) $\dim \varphi^{-1}(y) \geq \dim X - \dim Y$ *for all* $y \in Y$.
(II) *There is a nonempty open subset* $V \subset Y$ *such that for all* $y \in V$,

$$\dim \varphi^{-1}(y) = \dim X - \dim Y.$$

Proof. Shafarevich [239], I.6, Theorem 7. □

Let Z be an affine variety in affine space $\mathbb{A}^n$, with coordinates $(z_1, \ldots, z_n)$, and defined over a field κ. Let $a = (a_1, \ldots, a_n)$ be a point of Z. Suppose κ algebraically closed and $a_i \in \kappa$ for all i. Let

$$P_j(z_1, \ldots, z_n) = 0, \;\; j = 1, \ldots, r$$

be a set of defining equations for Z. We say that the point a is *regular* (or *non-singular* or *smooth*) if

$$\operatorname{rank} \left(\frac{\partial P_j}{\partial z_i}(a) \right) = n - m,$$

where m is the dimension of Z, otherwise, is *singular*. We say that Z is *non-singular* or *smooth* if every point on Z is regular. A projective variety is called *non-singular* if all the affine open sets $U_0, \ldots, U_n$ above are non-singular.

Theorem 3.37. *Let φ be a rational mapping from a smooth variety X to a projective variety. Then*

$$\operatorname{codim}(X - \operatorname{dom}(\varphi)) \geq 2.$$

Proof. See Shafarevich [239], II.3, Theorem 3. □

Theorem 3.37 yields immediately the following result:

Theorem 3.38. *A rational mapping from a smooth curve to a projective variety extends to a morphism defined on the whole curve.*

3.2.5 Differential forms

Let x be a point on a variety X. The *tangent space to X at x* is the $\bar{\kappa}$-vector space

$$T_x(X) = \operatorname{Hom}_{\bar{\kappa}}(\mathbf{m}(x)/\mathbf{m}(x)^2, \bar{\kappa}).$$

In other words, the tangent space is defined to be the dual of the vector space $\mathbf{m}(x)/\mathbf{m}(x)^2$. We naturally call $\mathbf{m}(x)/\mathbf{m}(x)^2$ the *cotangent space to X at x*, denoted by $T_x^*(X)$. It is not difficult to check that $T_x(X)$ and $T_x^*(X)$ are vector spaces over $\bar{\kappa}$ since

$$\mathcal{O}(x)/\mathbf{m}(x) \cong \bar{\kappa}.$$

Theorem 3.39. *Let X be a variety. Then $\dim T_x(X) \geq \dim X$ for all $x \in X$. Furthermore, there is a nonempty open set $U \subset X$ such that $\dim T_x(X) = \dim X$ for $x \in U$.*

Proof. See Hartshorne [90], I.5, Proposition 2A and Theorem 3 or Shafarevich [239], II.1, Theorem 3. □

According to Jacobian criterion (see [90], I.5), a point x in an affine variety Z is regular if and only if $\dim T_x(Z) = \dim Z$. An *ordinary singularity* in a curve is a singularity whose tangent cone is composed of distinct lines. The *multiplicity* of an ordinary singularity is the number of lines in its tangent cone.

Consider a rational mapping $\varphi : X \longrightarrow Y$ between two varieties that is regular at x, and let $y = \varphi(x)$. According to Hartshorne [90], I.4, Theorem 4, the mapping

$$\varphi^* : \mathcal{O}_Y(y) \longrightarrow \mathcal{O}_X(x), \;\; g \mapsto g \circ \varphi$$

is a homomorphism of local rings, in particular,

$$\varphi^*(\mathbf{m}(y)) \subset \mathbf{m}(x), \quad \varphi^*(\mathbf{m}(y)^2) \subset \mathbf{m}(x)^2,$$

and hence it induces a $\bar{\kappa}$-linear mapping

$$\varphi^* : T_y^*(Y) \longrightarrow T_x^*(X).$$

The *tangent mapping* or *differential* of φ at x

$$d\varphi(x) : T_x(X) \longrightarrow T_y(Y)$$

is defined to be the transpose of the mapping φ^*.

Let X be a variety. Take a function $f \in \bar{\kappa}(X)_*$ and fix a point x in the domain of f. We obtain a tangent mapping

$$df(x) : T_x(X) \longrightarrow T_{f(x)}(\mathbb{A}^1) = \bar{\kappa},$$

so $df(x)$ is a linear form on $T_x(X)$, that is, $df(x) \in T_x^*(X)$. Obviously, the classical rules

$$d(f+g) = df + dg, \quad d(fg) = f dg + g df \tag{3.36}$$

are valid. Thus we may view df as a mapping that associates to each point $x \in \mathrm{dom}(f)$ a cotangent vector in $T_x^*(X)$. According to Hindry and Silverman [98], such a mapping is called an *abstract differential 1-form*. From the formulas (3.36) one deduces easily an identity that holds for any polynomial $P \in \bar{\kappa}[x_1, \ldots, x_m]$ and any functions $f_1, \ldots, f_m \in \bar{\kappa}(X)$:

$$dP(f_1, \ldots, f_m) = \sum_{i=1}^{m} \frac{\partial P}{\partial x_i}(f_1, \ldots, f_m) df_i. \tag{3.37}$$

It generalizes immediately to rational functions P.

A *regular differential 1-form* on X is an abstract differential 1-form ω such that for all $x \in X$ there is a neighborhood U of x and regular functions $f_i, g_i \in \mathcal{O}(U)$ such that

$$\omega(x) = \sum g_i(x) df_i(x), \;\; x \in U.$$

We denote the set of regular differential 1-forms on X by $\Omega^1[X]$. It is clearly a $\bar{\kappa}$-vector space, and in fact, it is an $\mathcal{O}(X)$-module.

Let x be a nonsingular point on a variety X of dimension n. Functions $t_1, \ldots, t_n \in \mathcal{O}(x)$ are called *local parameters* at x if each $t_i \in \mathbf{m}(x)$, and if the images of $t_1, \ldots, t_n$ form a basis of $T_x^*(X)$. The functions $t_1, \ldots, t_n$ give *local coordinates* on X if $u_i := t_i - t_i(x)$ give local parameters at all x in X. It is easy to see that $t_1, \ldots, t_n$ are local parameters if and only if n linear forms $dt_1(x), \ldots, dt_n(x)$ on $T_x(X)$ are linearly independent. Since $\dim T_x(X) = n$, this in turn is equivalent to saying that in $T_x(X)$,

$$\bigcap_i \ker(dt_i(x)) = \{0\}.$$

According to Shafarevich [239], III.5, Theorem 1, any nonsingular point x of a variety X has local parameters $t_1, \ldots, t_n$ defined on a neighborhood U of x such that

$$\Omega^1[U] = \bigoplus_{i=1}^{n} \mathcal{O}(U) dt_i, \tag{3.38}$$

which means that $\Omega^1[U]$ is a free $\mathcal{O}(U)$-module of rank n.

The abstract differential 1-forms considered were mappings sending each point $x \in X$ to an element of $T_x^*(X)$. We now consider more general *abstract differential r-forms* that send $x \in X$ to a skewsymmetric r-linear form on $T_x(X)$, that is, to an element of the r-th exterior product $\bigwedge_r T_x^*(X)$ of $T_x^*(X)$, or equivalently, to a linear mapping $\bigwedge_r T_x(X) \longrightarrow \bar{\kappa}$. A *regular differential r-form* ω on X is an abstract differential r-form such that for all $x \in X$ there is a neighborhood U containing x and functions $f_i, g_{i_1,\ldots,i_r} \in \mathcal{O}(U)$ such that

$$\omega = \sum g_{i_1,\ldots,i_r} df_{i_1} \wedge \cdots \wedge df_{i_r}.$$

We denote the set of regular differential r-forms on X by $\Omega^r[X]$. It is clearly an $\mathcal{O}(X)$-module. The analogue of (3.38) is true. If $t_1, \ldots, t_n$ are local coordinates on U, then

$$\Omega^r[U] = \bigoplus_{i_1 < \cdots < i_r} \mathcal{O}(U) dt_{i_1} \wedge \cdots \wedge dt_{i_r}. \tag{3.39}$$

Hence $\Omega^r[U]$ is a free $\mathcal{O}(U)$-module of rank $\binom{n}{r}$.

We now introduce a new object, consisting of an open set $U \subset X$ and a differential r-form $\omega \in \Omega^r[U]$. On pairs (U, ω) we introduce the equivalence relation $(\omega, U) \sim (\omega', U')$ if $\omega = \omega'$ on $U \cap U'$. Note that the set of points at which a regular differential

form is 0 is closed (see Shafarevich [239], III.5.4, Lemma). It is enough to require that $\omega = \omega'$ on some open subset of $U \cap U'$. The transitivity of the equivalence relation follows from this. An equivalence class under this relation is called a *rational differential r-form* on X. We denote the set of rational differential r-forms on X by $\Omega^r(X)$, which is a vector space of dimension $\binom{n}{r}$ over $\bar{\kappa}(X)$ (see Shafarevich [239], III.5.4, Theorem 3). Obviously,

$$\Omega^0(X) = \bar{\kappa}(X).$$

If $t_1, \ldots, t_n$ is a separable transcendence basis of $\bar{\kappa}(X)$, then the forms

$$\{dt_{i_1} \wedge \cdots \wedge dt_{i_r} \mid 1 \leq i_1 < \cdots < i_r \leq n\}$$

form a basis of $\Omega^r(X)$ over $\bar{\kappa}(X)$ (see Shafarevich [239], III.5.4, Theorem 4). Each element $\omega \in \Omega^r(X)$ has a largest open $U \subset X$ such that ω defines a regular r-form on U, called the *domain of regularity* of ω.

Let $\varphi : X \longrightarrow Y$ be a morphism of smooth varieties. Then there is a mapping

$$\varphi^* : \Omega^r[Y] \longrightarrow \Omega^r[X]$$

defined by the formula

$$\varphi^*\left(\sum g_{i_1,\ldots,i_r} df_{i_1} \wedge \cdots \wedge df_{i_r}\right) = \sum (g_{i_1,\ldots,i_r} \circ \varphi) d(f_{i_1} \circ \varphi) \wedge \cdots \wedge d(f_{i_r} \circ \varphi).$$

3.2.6 Abelian varieties

An *algebraic group* defined over κ is a variety G defined over κ, an *identity element* $e \in G(\kappa)$, and morphisms $m : G \times G \longrightarrow G$ and $i : G \longrightarrow G$ satisfying the axioms of a group law:

(α) $m(e, x) = m(x, e) = x$.

(β) $m(i(x), x) = m(x, i(x)) = e$.

(γ) $m(m(x, y), z) = m(x, m(y, z))$.

We temporarily write the group laws multiplicatively, that is,

$$m(x, y) = xy, \quad i(x) = x^{-1}.$$

If G is an algebraic group, then for any $a \in G$, the *right translation*

$$R_a : G \longrightarrow G, \ \ x \mapsto ax$$

and the *left translation*

$$L_a : G \longrightarrow G, \ \ x \mapsto xa$$

are isomorphisms.

Algebraic groups are smooth varieties. Indeed, if an algebraic group G has a singular point a, we would deduce that all points of G are singular by using the translation mappings and their tangent mappings, which contradicts Theorem 3.39.

Let G_1 and G_2 be two algebraic groups. A homomorphism $\varphi : G_1 \longrightarrow G_2$ is called an *isogeny* if it is surjective, has finite kernel, and $\dim G_1 = \dim G_2$. The cardinality of the kernel of φ is called the *degree* of φ.

Proposition 3.40 (Weil). *A rational mapping from a smooth variety into an algebraic group either extends to a morphism or is undefined on a set of pure codimension one.*

Proof. See Hindry and Silverman [98], Lemma A.7.1.4. □

An *Abelian variety* is a projective variety that is also an algebraic group. By using Theorem 3.37 and above Weil's result, it follows that a rational mapping from a smooth variety into an Abelian variety must extend to a morphism.

Proposition 3.41. *If $\varphi : A \longrightarrow B$ is a morphism between two Abelian varieties, then φ is the composition of a translation and a homomorphism.*

Proof. By composing φ with a translation, we may assume that $\varphi(e_A) = e_B$, where e_A and e_B are the identity elements of A and B, respectively. Consider the mapping

$$\psi : A \times A \longrightarrow B, \;\; \psi(x, y) = \varphi(xy)\varphi(x)^{-1}\varphi(y)^{-1}.$$

It is clear that

$$\psi(e_A, A) = \{e_B\}, \quad \psi(A, e_A) = \{e_B\},$$

and hence Proposition 3.29 implies that ψ is a constant. Hence

$$\psi(x, y) = \psi(e_A, e_A) = e_B,$$

which means precisely that φ is a homomorphism. □

Proposition 3.42. *An Abelian variety is a commutative algebraic group.*

Proof. Proposition 3.41 means that the inversion morphism $i : A \longrightarrow A$ must be a homomorphism. Hence

$$i(xy) = i(x)i(y),$$

so A is commutative. □

We now know that the group law on an Abelian variety A is commutative, so we will henceforth write the group law additively. In particular, an integer n gives an endomorphism of A by

$$[n]x = x + x + \cdots + x \;\; (n \text{ terms})$$

if $n > 0$, $[n]x = [-n](-x)$ if $n < 0$, and $[0]x = e_A$. The *n-torsion subgroup* of A, denoted $A[n]$, is the set of points of order n in A,

$$A[n] = \{x \in A \mid [n]x = e_A\}.$$

The *torsion subgroup* of A, denoted A_{tors}, is the set of points of finite order,

$$A_{\mathrm{tors}} = \bigcup_{n=1}^{\infty} A[n].$$

Then $A_{\mathrm{tors}}(\kappa)$ will denote the points of finite order in $A(\kappa)$.

Proposition 3.43. *Let A be an Abelian variety of dimension g over an algebraically closed field $\bar{\kappa}$ of characteristic $p \geq 0$.*

(δ1) *The multiplication mapping $[n] : A(\bar{\kappa}) \longrightarrow A(\bar{\kappa})$ is a degree n^{2g} isogeny,*

(δ2) *If $p = 0$ or if n is prime to p, then*

$$A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

(δ3) *If $p > 0$, then for some integer $0 \leq r \leq g$,*

$$A[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^r, \ \ e = 1, 2, 3, \ldots .$$

Proof. See [98], Theorem A.7.2.7; or [256]. □

3.3 Divisors

In this part, we describe divisors on an algebraic variety X. There are two kinds. The *group of Weil divisors on X* is the free Abelian group generated by the subvarieties of codimension one on X. It is denoted by $\mathrm{Div}(X)$. In other words, a Weil divisor can be written as a linear combination

$$D = \sum_i n_i Y_i,$$

where Y_i is a subvariety of codimension 1, and $n_i \in \mathbb{Z}$. For example, if X is a curve, then the Y_i's are points; if X is a surface, then the Y_i's are irreducible curves; and so on. If all $n_i \geq 0$ then D is called *effective* or *positive*. We write $D \geq 0$ for D effective.

The *support of the divisor D* is the union of all those Y_i's for which the *multiplicity* n_i is nonzero. It is denoted by $\mathrm{supp}(D)$. Let us denote by D_{red} the *reduced divisor* of D. In other words, D_{red} is the sum of all the irreducible components of D, with multiplicity 1.

Let Y be a subvariety of codimension 1 of X. For any regular point $x \in X$, Y can be given in a neighborhood $U \subset X$ of x as the zeros of a regular function $g \in \mathcal{O}(U)$.

Moreover, any function $f \in \mathcal{O}(x)$ vanishing on $U \cap Y$ is divisible by g. The function g is called a *local defining function*, $g = 0$ is called the *local equation* of Y at x, and is unique, up to multiplication by a function nonzero at x (see Shafarevich [239], II.3, Theorem 1).

A divisor D on the variety X is called *normal crossings* if each irreducible component of D is nonsingular, and whenever r irreducible components $Y_1, \ldots, Y_r$ of D meet at a point x, then the local defining functions $g_1, \ldots, g_r$ of the Y_i form a part of a regular sequence for $\mathcal{O}(x)$, i.e., $g_1, \ldots, g_r$ are linearly independent $(\mathrm{mod}\ \mathbf{m}(x))$, where $g_1 \cdots g_r = 0$ is just the local equation of D at x. Therefore, a normal crossings divisor must be effective, and all irreducible components of its support must occur with multiplicity 1.

Let Y be a subvariety of codimension 1 of X. We recall that $\mathcal{O}_X(Y)$ is the local ring of functions regular in a neighborhood of some point of Y. In particular, if X is nonsingular along Y, then $\mathcal{O}_X(Y)$ is a discrete valuation ring. Take $f \in \mathcal{O}_X(Y) - \{0\}$. Let $x \in X$ be a regular point, and g a local defining function for Y near x. Since $f \in \mathcal{O}_X(x)$ and $\mathcal{O}_X(x)$ is a discrete valuation ring, there exist a unit u in $\mathcal{O}_X(x)$ and an non-negative integer d such that

$$f = ug^d.$$

Note that the integer d is independent of the choice of regular points in $X \cap Y$ and will be called the *order of f along Y*, denoted by $\mathrm{ord}_Y(f)$. We can extend ord_Y to $\bar{\kappa}(X)_*$ in the usual way. Its main properties are summarized as follows:

Proposition 3.44. *Fix $f \in \bar{\kappa}(X)_*$. The order function $\mathrm{ord}_Y : \bar{\kappa}(X)_* \longrightarrow \mathbb{Z}$ has the following properties:*

(a) $\mathrm{ord}_Y(fg) = \mathrm{ord}_Y(f) + \mathrm{ord}_Y(g)$ *for all $g \in \bar{\kappa}(X)_*$.*

(b) $\mathrm{ord}_Y(f+g) \geq \min\{\mathrm{ord}_Y(f), \mathrm{ord}_Y(g)\}$ *for all $g \in \bar{\kappa}(X)_*$ with $f + g \neq 0$.*

(c) *There are only finitely many Y's with $\mathrm{ord}_Y(f) \neq 0$.*

(d) $\mathrm{ord}_Y(f) \geq 0$ *if and only if $f \in \mathcal{O}_X(Y)$. Similarly, $\mathrm{ord}_Y(f) = 0$ if and only if f is a unit in $\mathcal{O}_X(Y)$.*

(e) *Assume further that X is projective. Then the following are equivalent:*

(e1) $\mathrm{ord}_Y(f) \geq 0$ *for all Y.*
(e2) $\mathrm{ord}_Y(f) = 0$ *for all Y.*
(e3) $f \in \bar{\kappa}_*$.

Proof. Hindry–Silverman [98], Lemma A.2.1.2 or Shafarevich [239], III.1.1, (2). □

Let $f \in \bar{\kappa}(X)_*$ be a rational function on X. The *divisor* of f is the divisor

$$(f) = \sum_Y \mathrm{ord}_Y(f) Y.$$

Usually we say that f has a *zero of order d along Y* if $\mathrm{ord}_Y(f) = d > 0$, and that f has a *pole of order d along Y* if $\mathrm{ord}_Y(f) = -d < 0$. A divisor is said to be *principal* if it is the divisor of a function. Two divisors D and D' are said to be *linearly equivalent*, denoted by $D \sim D'$, if their difference is a principal divisor. The *divisor class group of X* is the group of divisor classes modulo linear equivalence. It is denoted by $\mathrm{Cl}(X)$. The linear equivalence class of a divisor D will be denoted by $\mathrm{Cl}(D)$. A divisor class is called *effective* if it contains an effective divisor.

Proposition 3.45. *Let $\deg(Y)$ denote the degree of an irreducible hypersurface $Y \subset \mathbb{P}^n$, and extend the function $\deg$ by linearity to the group of divisors $\mathrm{Div}(\mathbb{P}^n)$. Then a divisor $D \in \mathrm{Div}(\mathbb{P}^n)$ is principal if and only if it has degree 0, and the induced mapping $\deg : \mathrm{Cl}(\mathbb{P}^n) \longrightarrow \mathbb{Z}$ is an isomorphism.*

Proof. See Hindry and Silverman [98], Proposition A.2.1.3. □

A *Cartier divisor* on a variety X is an (equivalence class of) collections of pairs $\{(U_i, f_i)\}_{i\in I}$ satisfying the following conditions:

(A) The U_i's are Zariski open sets that cover X.

(B) The f_i's are nonzero rational functions $f_i \in \bar{\kappa}(U_i)_* = \bar{\kappa}(X)_*$.

(C) $f_i f_j^{-1} \in \mathcal{O}^*(U_i \cap U_j)$ (i.e., $f_i f_j^{-1}$ has no poles or zeros on $U_i \cap U_j$).

Two collections $\{(U_i, f_i)\}_{i\in I}$ and $\{(V_j, g_j)\}_{j\in J}$ are considered to be equivalent (define the same divisor) if $f_i g_j^{-1} \in \mathcal{O}^*(U_i \cap V_j)$ for all $i \in I$ and $j \in J$. The *support* of a Cartier divisor $\{(U_i, f_i)\}_{i\in I}$ is the set of zeros and poles of the f_i's. A pair (U_i, f_i) is said to *represent the divisor locally*, or on the open set U_i. The Cartier divisor is said to be *effective* if for all representing pairs (U_i, f_i) the rational function f_i is regular at all points of U_i, that is, f_i has no poles on U_i. We then view the Cartier divisor as a hypersurface on X, defined locally on U_i by the equation $f_i = 0$. The Cartier divisors form a group, denoted by $\mathrm{CaDiv}(X)$. Indeed, if Cartier divisors are respectively $\{(U_i, f_i)\}_{i\in I}$ and $\{(V_j, g_j)\}_{j\in J}$, then their sum is

$$\{(U_i, f_i)\}_{i\in I} + \{(V_j, g_j)\}_{j\in J} = \{(U_i \cap V_j, f_i g_j)\}_{(i,j)\in I\times J}.$$

Associated to a function $f \in \bar{\kappa}(X)_*$ is its *principal Cartier divisor*, denoted by

$$\mathrm{div}(f) = \{(X, f)\}.$$

Two divisors are said to be *linearly equivalent* if their difference is a principal Cartier divisor. The group of Cartier divisor classes of X is the group of divisor classes modulo linear equivalence. It is called the *Picard group* of X and is denoted by $\mathrm{Pic}(X)$.

We now compare the two types of divisors. Let Y be an irreducible subvariety of codimension 1 in X, and let D be a Cartier divisor defined by $\{(U_i, f_i)\}_{i\in I}$. We define

the order of D along Y, denoted by $\mathrm{ord}_Y(D)$, as follows. Choose one of the open sets U_i such that $U_i \cap Y \neq \emptyset$ and set

$$\mathrm{ord}_Y(D) = \mathrm{ord}_Y(f_i).$$

It is easily seen that $\mathrm{ord}_Y(D)$ is independent of the choice of (U_i, f_i), so that we obtain a map from Cartier divisors to Weil divisors by sending D to $\sum \mathrm{ord}_Y(D)Y$. In general, this mapping is neither surjective nor injective. For example, see Fulton [72], Examples 2.1.2 and 2.1.3 or Hartshorne [90], II.6.11.3.

Theorem 3.46. *If X is a smooth variety, then the natural mappings*

$$\mathrm{CaDiv}(X) \longrightarrow \mathrm{Div}(X), \quad \mathrm{Pic}(X) \longrightarrow \mathrm{Cl}(X)$$

are isomorphisms.

Proof. Hartshorne [90], II.6.11. □

In the sequel we will consider only Cartier divisors when the variety in question might be singular, and we will freely identify Weil and Cartier divisors when we work with smooth varieties.

Let X be a smooth variety of dimension n, and let ω be a nonzero rational differential n-form on X. We cover X by affine open subsets U_i of X with local coordinates $t_1^{(i)}, \ldots, t_n^{(i)}$. In U_i, we can write

$$\omega = g^{(i)} dt_1^{(i)} \wedge \cdots \wedge dt_n^{(i)}.$$

In particular, we have the expression

$$dt_\alpha^{(i)} = \sum_{\beta=1}^{n} h_{\alpha\beta} dt_\beta^{(j)}, \ \ \alpha = 1, \ldots, n. \tag{3.40}$$

Since $dt_1^{(i)}(x), \ldots, dt_n^{(i)}(x)$ form a basis of $T_x^*(X)$ for each $x \in U_i$, it follows from (3.40) that the *Jacobian determinant* of the functions $t_1^{(i)}, \ldots, t_n^{(i)}$ with respect to $t_1^{(j)}, \ldots, t_n^{(j)}$ satisfies

$$\frac{D\big(t_1^{(i)}, \ldots, t_n^{(i)}\big)}{D\big(t_1^{(j)}, \ldots, t_n^{(j)}\big)} := \det(h_{\alpha\beta}) \neq 0.$$

Substituting (3.40) in the expression for ω and simple calculations in the exterior algebra shows that on the intersection $U_i \cap U_j$, we get

$$g^{(j)} = g^{(i)} \frac{D\big(t_1^{(i)}, \ldots, t_n^{(i)}\big)}{D\big(t_1^{(j)}, \ldots, t_n^{(j)}\big)}.$$

Since the Jacobian determinant is regular and nowhere zero in $U_i \cap U_j$, the collection of pairs $(U_i, g^{(i)})$ defines a divisor on X. This divisor is called the *divisor* of ω, and is denoted by $\mathrm{div}(\omega)$.

Any other nonzero rational differential n-form ω' on X has the form $\omega' = f\omega$ for some rational function $f \in \bar{\kappa}(X)_*$. It follows that

$$\mathrm{div}(\omega') = \mathrm{div}(\omega) + \mathrm{div}(f),$$

so that the divisor class associated to an n-form is independent of the chosen form. This divisor class is called the *canonical class* of X. By abuse of language, any divisor in the canonical class is called a *canonical divisor* and is denoted by K, as well as its class, or by K_X if we wish to emphasize the dependence on X.

Let $\varphi : X \longrightarrow Y$ be a morphism of varieties, let $D \in \mathrm{CaDiv}(Y)$ be a Cartier divisor defined by $\{(V_j, g_j)\}_{j\in J}$, and assume that $\varphi(X)$ is not contained in the support of D. Then the Cartier divisor $\varphi^* D \in \mathrm{CaDiv}(X)$ is the divisor defined by

$$\varphi^* D = \{(\varphi^{-1}(V_j), g_j \circ \varphi)\}_{j\in J}.$$

Proposition 3.47. *Let A be an Abelian variety, let X be an arbitrary variety, and let $\varphi, \psi, \chi : X \longrightarrow A$ be three morphisms. Then for any divisor $D \in \mathrm{CaDiv}(A)$,*

$$(\varphi+\psi+\chi)^* D - (\varphi+\psi)^* D - (\varphi+\chi)^* D - (\psi+\chi)^* D + \varphi^* D + \psi^* D + \chi^* D \sim 0.$$

Proof. See Hindry and Silverman [98], Corollary A.7.2.4. □

Let $\varphi : X \longrightarrow Y$ be a finite mapping of smooth projective varieties, let Z be an irreducible divisor on X, and let $Z' = \varphi(Z)$ be the image of Z under φ. Note that the dimension theorem (Theorem 3.36) tells us that Z' is an irreducible divisor on Y. Let s_Z be a generator of the maximal ideal of $\mathcal{O}_X(Z)$, and similarly set $s_{Z'}$ be a generator of the maximal ideal of $\mathcal{O}_Y(Z')$, that is, s_Z and $s_{Z'}$ are local equations for Z and Z'. The *ramification index of f along Z* is defined to be the integer

$$e_Z = e_Z(\varphi) = \mathrm{ord}_Z(s_{Z'} \circ \varphi),$$

where we recall that $\mathrm{ord}_Z : \mathcal{O}_X(Z) \longrightarrow \mathbb{Z}$ is the valuation on $\mathcal{O}_X(Z)$. Equivalently,

$$s_{Z'} \circ \varphi = u s_Z^{e_Z}, \;\; u \in \mathcal{O}_X(Z)^*.$$

The mapping φ is said to be *ramified along Z* if $e_Z(\varphi) \geq 2$. If $e_Z(\varphi) = 1$, we say that φ is *unramified along Z*. If $\mathrm{char}\,\kappa = 0$, or $\mathrm{char}\,\kappa = p$, and p does not divide $e_Z(\varphi)$, we say that the ramification is *tame*. If p does divide $e_Z(\varphi)$, it is *wild*. We then have the following *Hurwitz formula*:

Theorem 3.48. *Let $\varphi : X \longrightarrow Y$ be a finite mapping between smooth projective varieties.*

(1) *The mapping φ is ramified only along a finite number of irreducible divisors.*

(2) *If we assume further either that the characteristic of κ is 0 or that the characteristic of κ does not divide any of the ramification indices, then we have the formula*

$$K_X \sim \varphi^*(K_Y) + R,$$

where R is the ramification divisor of φ given by

$$R = \sum_Z (e_Z(\varphi) - 1)Z.$$

Proof. Hindry–Silverman [98], Proposition A.2.2.8. □

Two divisors D_1, D_2 on X are *algebraically equivalent* if there exists a connected algebraic set T, two points $t_1, t_2 \in T$, and a divisor $\mathcal{D}$ on $X \times T$ such that

$$D_i = \mathcal{D}|_{X \times \{t_i\}}, \quad i = 1, 2.$$

Linear equivalence of divisors implies algebraic equivalence.

Lemma 3.49. *Let X be a complete non-singular variety. Let D be a divisor on X such that some positive multiple of D is very ample. Then there exists an integer $m > 0$ such that for any divisor E on X algebraically equivalent to 0, the divisor $E + mD$ is very ample.*

Proof. See S. Lang [144], Chapter 4, Lemma 3.2. □

One sees easily that algebraic equivalence is compatible with addition in $\mathrm{Div}(X)$: divisors D algebraically equivalent to 0 form a subgroup. We denote this by $\mathrm{Div}^0(X)$. An important result is the following theorem proved by Severi (for fields of characteristic 0) and Néron (in the general case).

Theorem 3.50. *For X a nonsingular projective variety, the group $\mathrm{Div}(X)/\mathrm{Div}^0(X)$ is finitely generated.*

When X is a nonsingular projective variety, one can define $\mathrm{Pic}^0(X)$ to be the subgroup of $\mathrm{Pic}(X) = \mathrm{Cl}(X)$ composed of divisor classes algebraically equivalent to 0. The group $\mathrm{Pic}^0(X)$ can always be given the structure of an Abelian variety, which is called the *Picard variety* of X. The quotient

$$\mathrm{NS}(X) = \mathrm{Pic}(X)/\mathrm{Pic}^0(X)$$

is called the *Néron–Severi group* of X and is a finitely generated group.

3.4 Linear systems

Let D be a divisor on a variety X. The *associated vector space* or *Riemann–Roch space* of D is defined to be the subset of rational functions

$$\mathcal{L}(D) = \mathcal{L}(X, D) = \{f \in \bar{\kappa}(X)_* \mid D + (f) \geq 0\} \cup \{0\}. \tag{3.41}$$

This set is a vector space over $\bar{\kappa}$ under the usual algebraic operations on functions. Indeed, if $D = \sum n_i Y_i$ then $f \in \bar{\kappa}(X)_*$ belongs to $\mathcal{L}(D)$ if and only if

$$\operatorname{ord}_Y(f) \geq \begin{cases} -n_i, & Y = Y_i, \\ 0, & Y \neq Y_i \text{ for all } i, \end{cases}$$

and because of this, our assertion follows at once from (b) in Proposition 3.44. The dimension of $\mathcal{L}(D)$ is denoted by $\ell(D)$ (which is called the *dimension* of D by some authors).

Theorem 3.51. *Let D be a divisor on a projective variety. Then $\ell(D)$ is finite.*

Proof. See, for example, Hartshorne [90], Theorem III.2, Hindry and Silverman [98], Corollary A.3.2.7, or Shafarevich [239], III.2.3, Theorem 5. □

We know $\ell(D) = \ell(D')$ if $D \sim D'$ (see [239], III.1.5, Theorem 3). Thus we see that it makes sense to speak of the dimension $\ell(c)$ of a divisor class c, that is, the common dimension of all the divisors of this class. This number has the following meaning. If $D \in c$ and $f \in \mathcal{L}(D)$, then the divisor

$$D_f = D + (f) \in c$$

is effective. Conversely, any effective divisor $D' \in c$ is of the form D_f for some $f \in \mathcal{L}(D)$. Obviously, if X is projective, f is uniquely determined by D_f up to a constant factor. Thus we can set up a one-to-one correspondence between effective divisors in the class c and points of $\mathbb{P}(\mathcal{L}(D)) \cong \mathbb{P}^{\ell(D)-1}$.

The following definition slightly generalizes this construction. A *linear system* L on a variety X is a subset of effective divisors all linearly equivalent to a fixed divisor D and parametrized by a linear subvariety of $\mathbb{P}(\mathcal{L}(D))$. The *dimension* of the linear system L is the dimension of the linear subvariety. The set of *base points* of L is the intersection of the supports of all divisors in L. We will say that L is *base point free* if this intersection is empty. The set of effective divisors linearly equivalent to D is a linear system, called the *complete linear system* of D. It is denoted by $|D|$. If $|D|$ is base point free, the divisor D is also said to be *base point free*.

Let L be a linear system of dimension n parametrized by a projective space $\mathbb{P}(V) \subset \mathbb{P}(\mathcal{L}(D))$, where V is a subspace of $\mathcal{L}(D)$ of dimension $n+1$ over $\bar{\kappa}$. Let B_L be the set of base points of L. When $x \in X - B_L$, the subspace of V

$$V_x = \{f \in V \mid f(x) = 0\}$$

has dimension n. Thus there exists unique element $\varphi_L(x) \in \mathbb{P}(V^*)$ such that

$$E[\varphi_L(x)] = V_x.$$

It is easy to show that if $L \neq \emptyset$, then

$$\varphi_L : X - B_L \longrightarrow \mathbb{P}(V^*)$$

is regular, which further extends a rational mapping

$$\varphi_L : X \longrightarrow \mathbb{P}(V^*) \tag{3.42}$$

called the *dual classification mapping*.

Next we explain it clearly. Select a basis $f_0, \ldots, f_n$ of V and let $e_0, \ldots, e_n$ be the dual basis in V^*. Choose $\tilde{\varphi}_L(x) \in V^* - \{0\}$ such that $\mathbb{P}(\tilde{\varphi}_L(x)) = \varphi_L(x)$. Thus we can write

$$\tilde{\varphi}_L(x) = \sum_{i=0}^{n} \tilde{\varphi}_i(x) e_i.$$

By the definition,

$$E[\varphi_L(x)] = \left\{ \xi = \sum_{i=0}^{n} \xi_i f_i \in V \;\middle|\; \langle \xi, \tilde{\varphi}_L(x) \rangle = \sum_{i=0}^{n} \xi_i \tilde{\varphi}_i(x) = 0 \right\}.$$

Since $E[\varphi_L(x)] = V_x$, then $\xi \in E[\varphi_L(x)]$ means that

$$\xi(x) = \sum_{i=0}^{n} \xi_i f_i(x) = 0,$$

that is, $[f_0(x), \ldots, f_n(x)]$ can serve as the homogeneous coordinates of $\varphi_L(x)$. Therefore we can identify

$$\varphi_L = [f_0, \ldots, f_n] : X \longrightarrow \mathbb{P}^n. \tag{3.43}$$

We will abbreviate

$$\varphi_D = \varphi_{|D|}.$$

The *fixed component of a linear system* L is the largest divisor D_0 such that for all $D \in L$, we have $D \geq D_0$. If $D_0 = 0$, we say that the linear system has no fixed component. We can now formulate the correspondence between rational mappings and linear systems.

Theorem 3.52. *There is a natural bijection between:*

⟨1⟩ *Linear systems L of dimension n without fixed components.*

⟨2⟩ *Morphisms $\varphi : X \longrightarrow \mathbb{P}^n$ with image not contained in a hyperplane, up to projective automorphism. (That is, we identify two rational mappings $\varphi, \varphi' : X \longrightarrow \mathbb{P}^n$ if there is an automorphism $\sigma : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ such that $\varphi' = \sigma \circ \varphi$.)*

Proof. See Mumford [196], Theorem 6.8 or Hartshorne [90], II.7.1 and II.7.8.1. □

A linear system L on a projective variety X is *very ample* if the associated mapping φ_L is an embedding, that is, φ_L is a morphism that maps X isomorphically onto its image $\varphi_L(X)$. A divisor D is said to be *very ample* if the complete linear system $|D|$ is very ample, and to be *ample* if some positive multiple of D is very ample.

Proposition 3.53. *Let X be a projective variety. Every divisor on X can be written as the difference of two very ample divisors. More precisely, let D be an arbitrary divisor on D and let E be a very ample divisor.*

$\{1\}$ *There exists an $m \geq 0$ such that $D + mE$ is base point free.*

$\{2\}$ *If D is base point free, then $D + E$ is very ample.*

Proof. Lang [150], Proposition 1.1; Hindry–Silverman [98], Theorem A.3.2.3. □

Proposition 3.54. *Let $f : X \longrightarrow Y$ be a morphism between two projective varieties and let D be a divisor on Y.*

$\lfloor 1 \rfloor$ *If D is base point free, then f^*D is a base point free divisor on X.*

$\lfloor 2 \rfloor$ *If f is finite, and if D is ample, then f^*D is an ample divisor on X.*

Proof. See Hartshorne [90], III, Exercise 5.7. □

The *dimension* of a divisor D on a projective variety X is the quantity

$$\dim D = \max_{m \geq 1} \dim \varphi_{mD}(X);$$

that is, it is the maximal dimension of the image of X under the dual classification mapping φ_{mD}, which is also called *D-dimension* of X. If $\mathcal{L}(mD)$ is always empty, then let $\dim D = -1$ by convention (some authors instead prefer to set $\dim D = -\infty$ in this situation). If $\dim D = \dim X$, then we say that D is *pseudo ample*, which means that there exists some positive integer m such that φ_{mD} is an imbedding of some non-empty Zariski open subset of X into a locally closed subset of $\mathbb{P}(\mathcal{L}(mD))$. Usually, $\dim K_X$ is called the *Kodaira dimension* of X. It is a result of Kodaira that:

Theorem 3.55. *On a non-singular projective variety, a divisor D is pseudo ample if and only if there exists some positive integer m such that $mD \sim E + Z$, where E is ample and Z is effective.*

Proof. See [131], Appendix; [287], Proposition 1.2.7; [130], Lemma 7.3.6 and Lemma 7.3.7; or Lemma 3.141. □

A non-singular projective variety X is defined to be *canonical* if the canonical class K_X is ample, *very canonical* if K_X is very ample, and *pseudo canonical* if K_X is pseudo ample. Instead of pseudo canonical, a variety has been called of *general type*. This new notion comes from Lang and Griffiths (cf. [150]). Generally, a projective variety (possibly singular) is called *pseudo canonical* if X is birationally equivalent to a projective non-singular pseudo canonical variety.

If κ has characteristic 0, *resolution of singularities* is known, and due to Hironaka. This means that given X a projective variety, there exists a birational morphism

$$\varphi : \tilde{X} \longrightarrow X$$

such that $\tilde{X}$ is projective and non-singular and φ is an isomorphism over the Zariski open subset of X consisting of the regular points. The non-singular projective variety $\tilde{X}$ is called a *normalization* of X.

An important characterization of a subvariety of an Abelian variety being pseudo canonical was given by Ueno [278] (or see Iitaka [115], [116]):

Theorem 3.56. *Let X be a subvariety of an Abelian variety over an algebraically closed field. Then X is pseudo canonical if and only if the group of translations which preserve X is finite.*

We have quite generally *Ueno's theorem* (see [278], Theorem 3.10):

Theorem 3.57. *Let X be a subvariety of an Abelian variety A, and let B be the connected component of the group of translations preserving X. Then the quotient $\varphi : X \longrightarrow X/B$ is a morphism, whose image is a pseudo canonical subvariety of the Abelian quotient A/B, and whose fibers are translations of B. In particular, if X does not contain any translations of Abelian subvarieties of dimension ≥ 1, then X is pseudo canonical.*

Proof. See Iitaka [117], Theorem 10.13, and Mori [192], Theorem 3.7. □

The mapping φ is called the *Ueno fibration of X*. Lang [150] formulated the Kawamata's theorem [125] into the following *Kawamata's structure theorem*:

Theorem 3.58. *Let X be a pseudo canonical subvariety of an Abelian variety A in characteristic 0. Then there exists a finite number of proper subvarieties Z_i with Ueno fibrations $\varphi_i : Z_i \longrightarrow Y_i$ whose fibers have dimension ≥ 1, such that every translate of an Abelian subvariety of A of dimension ≥ 1 contained in X is actually contained in the union of the subvarieties Z_i.*

The union of the subvarieties Z_i is called the *Ueno-Kawamata fibrations in X* when X is pseudo canonical. Note that the set of Z_i is empty if and only if X does not contain any translations of an Abelian subvariety of dimension ≥ 1.

3.5 Algebraic curves

3.5.1 Bézout's theorem

A curve C is a variety of dimension one, so its function field $\bar{\kappa}(C)$ is of transcendence degree one. It follows that $\bar{\kappa}(C)$ is algebraic over any subfield $\bar{\kappa}(x)$ generalized by a nonconstant function $x \in \bar{\kappa}(C)$. Hence we may write $\bar{\kappa}(C) = \bar{\kappa}(x, y)$, where x and y are nonconstant functions on C satisfying an algebraic relation

$$f(x, y) = 0. \tag{3.44}$$

Let $C_0 \subset \mathbb{A}^2$ denote the affine plane curve defined by f, and let $C_1 \subset \mathbb{P}^2$ be the projective plane curve defined by the homogenized equation

$$F(X, Y, Z) := Z^m f\left(\frac{X}{Z}, \frac{Y}{Z}\right) = 0, \tag{3.45}$$

where $m = \deg(f)$. Clearly, C is birational to both C_0 and C_1. Any curve birational to C is called a *model of* C, so we can say that C has a plane affine model and a plane projective model. The following main result shows that C has a smooth plane projective model, which is called a *normalization* of C.

Theorem 3.59. *Any algebraic curve is birational to a unique* (*up to isomorphism*) *smooth projective curve.*

Proof. See Fulton [71], VII.5, Theorem 3, Hartshorne [90], I, Corollary 6.11, or Hindry and Silverman [98], Theorem A.4.1.4. □

We explain Theorem 3.59 on normalization of algebraic curves clearly. Let $f(x, y)$ be an irreducible polynomial of two variables x and y over an algebraically closure $\bar{\kappa}$ of a field κ and consider the equations (3.44) and (3.45). If the point (x_0, y_0) lies on the affine curve (3.44), then $[x_0, y_0, 1]$ lies on C_1. Conversely, if $[X_0, Y_0, Z_0]$ lies on C_1 with $Z_0 \neq 0$, then $(X_0/Z_0, Y_0/Z_0)$ lies on the affine curve (3.44). Points on C_1 with $Z = 0$ are called the *points at infinity* of the affine curve.

In affine space, recall that we say the *simple* (or *regular*) *point* $p = (a, b) \in C_0$ of C_0 if either derivative $\frac{\partial f}{\partial x}(p) \neq 0$ or $\frac{\partial f}{\partial y}(p) \neq 0$. In this case the line

$$\frac{\partial f}{\partial x}(p)(x - a) + \frac{\partial f}{\partial y}(p)(y - b) = 0$$

is called the *tangent line* to C_0 at p. A point which is not simple is called *multiple* (or *singular*) correspond to a solution of the equations

$$f(x, y) = \frac{\partial f}{\partial x}(x, y) = \frac{\partial f}{\partial y}(x, y) = 0.$$

Theorem 3.60. *Let C_0 be an irreducible plane curve. Then $p \in C_0$ is a simple point of C_0 if and only if $\mathcal{O}_{C_0}(p)$ is a discrete valuation ring. In this case, if $L(x, y)$ is any line through p which is not tangent to C_0 at p, then the image (residue) ℓ of L in $\mathcal{O}_{C_0}(p) \subset \bar{\kappa}[C_0]$ is a uniformizing parameter for $\mathcal{O}_{C_0}(p)$.*

Proof. See Fulton [71], Chapter 3, Theorem 1. □

W.l.o.g., we may assume that $p = (0, 0)$ is a point on the affine curve (3.44), otherwise, it is sufficient to consider the function $f(x + a, y + b)$ at the point $(0, 0)$. Write

$$f(x, y) = f_\mu(x, y) + f_{\mu+1}(x, y) + \cdots + f_m(x, y),$$

where $f_j(x, y)$ $(j = \mu, \ldots, m)$ is a homogeneous polynomial of degree j with $f_\mu(x, y) \not\equiv 0$, and $\mu \geq 1$ since $f(0, 0) = 0$. We define μ to be the *multiplicity* of f (or C_0) at $p = (0, 0)$, and write $\mu_f^0(p)$ or $\mu_{C_0}(p)$. Note that $p \in C_0$ if and only if $\mu_f^0(p) > 0$. Using the rules for derivatives, it is easy to check that p is a simple point on C_0 if and only if $\mu_f^0(p) = 1$, otherwise, p is a singular point if and only if $\mu_f^0(p) \geq 2$. Recall that when $\mu \geq 2$, the singular point p is called a *μ-fold point*, say, *double point* for the case $\mu = 2$, *triple point* when $\mu = 3$, and so on.

Theorem 3.61. *Let C_0 be an irreducible plane curve defined. Then*

$$\mu_{C_0}(p) = \dim_{\bar{\kappa}} \mathbf{m}_{C_0}(p)^n / \mathbf{m}_{C_0}(p)^{n+1}$$

for all sufficiently large n.

Proof. See Fulton [71], Chapter 3, Theorem 2. □

Since a homogeneous polynomial of two variables defined over an algebraically closed field can be factored into a product of linear factors (see [71], Chapter 2, Corollary after Proposition 5), we can write

$$f_\mu(x, y) = \prod_i L_i(x, y)^{r_i},$$

where the $L_i(x, y)$ are distinct lines, and r_i are positive integers. The L_i are called the *tangent lines* to C_0 at $p = (0, 0)$; r_i is the *multiplicity* of the tangent line. The L_i is a *simple* (resp. *double*, etc.) *tangent line* if $r_i = 1$ (resp. 2, etc.). Further, if μ tangent lines at p are distinct, then p is called an *ordinary* μ-fold point of the affine curve (3.44).

Suppose p is a simple point on irreducible curve C_0. We let ord_p be the order function on $\bar{\kappa}(C_0)$ with the discrete valuation ring $\mathcal{O}_{C_0}(p)$. If $g \in \bar{\kappa}[x, y]$, and $[g]$ is the image of g in $\bar{\kappa}[C_0]$, we write $\mathrm{ord}_p(g)$ instead of $\mathrm{ord}_p([g])$. If p is a simple point on a reducible curve $Z(f)$, let $f = \prod f_i^{e_i}$ be the factorization of f into irreducible components. Then

$$\mu_f^0(p) = \sum_i e_i \mu_{f_i}^0(p);$$

and if L is a tangent line to $Z(f_i)$ with multiplicity r_i, then L is a tangent line to $Z(f)$ with multiplicity $\sum e_i r_i$. In particular, a point p is a simple point of $Z(f)$ if and only if p belongs to just one component $Z(f_i)$ of $Z(f)$, and p is a simple point of $Z(f_i)$.

Take $f, g \in \bar{\kappa}[x, y]$ and $p \in \mathbb{A}^2$. We say that $Z(f)$ and $Z(g)$ *intersect properly* at p if $Z(f)$ and $Z(g)$ have no common component which passes through p. There is a unique number

$$i_{f,g}(p) = \dim_{\bar{\kappa}} \mathcal{O}_{\mathbb{A}^2}(p)/(f, g),$$

called the intersect number of $Z(f)$ and $Z(g)$ at p, satisfying the following properties (See Fulton [71], Chapter 3, Theorem 3):

(1) $i_{f,g}(p)$ is a non-negative integer for any f, g, and p such that $Z(f)$ and $Z(g)$ intersect properly at p. However, $i_{f,g}(p) = \infty$ if $Z(f)$ and $Z(g)$ do not intersect properly at p.

(2) $i_{f,g}(p) = 0$ if and only if $p \notin Z(f) \cap Z(g)$. Also $i_{f,g}(p)$ depends only on the components of $Z(f)$ and $Z(g)$ which pass through p.

(3) If L is an affine linear change of coordinates on $\mathbb{A}^2$, and $L(q) = p$, then $i_{f,g}(p) = i_{f\circ L, g\circ L}(q)$.

(4) $i_{f,g}(p) = i_{g,f}(p)$.

(5) $i_{f,g}(p) \geq \mu_f^0(p)\mu_g^0(p)$, with equality occurring if and only if $Z(f)$ and $Z(g)$ have no tangent lines in common at p.

(6) If $f = \prod f_i^{r_i}$ and $g = \prod g_j^{s_j}$, then $i_{f,g}(p) = \sum_{i,j} r_i s_j i_{f_i,g_j}(p)$.

(7) $i_{f,g}(p) = i_{f,g+hf}(p)$ for any $h \in \bar{\kappa}[x, y]$.

(8) If p is a simple point on $Z(f)$, then $i_{f,g}(p) = \mathrm{ord}_p(g)$.

(9) If $Z(f)$ and $Z(g)$ have no common components, then

$$\sum_p i_{f,g}(p) = \dim_{\bar{\kappa}} \bar{\kappa}[x, y]/(f, g).$$

A point $p \in C_1$ is *singular* if

$$F(p) = \frac{\partial F}{\partial X}(p) = \frac{\partial F}{\partial Y}(p) = \frac{\partial F}{\partial Z}(p) = 0.$$

By the Euler's formula of homogeneous functions, we know

$$\deg(F)F(X, Y, Z) = X\frac{\partial F}{\partial X}(X, Y, Z) + Y\frac{\partial F}{\partial Y}(X, Y, Z) + Z\frac{\partial F}{\partial Z}(X, Y, Z).$$

Hence a point $p \in C_1$ is singular if and only if

$$\frac{\partial F}{\partial X}(p) = \frac{\partial F}{\partial Y}(p) = \frac{\partial F}{\partial Z}(p) = 0.$$

It is a simple lemma to prove that if an affine point is non-singular, then the corresponding projective point is also non-singular, and conversely. If the algebraic curve C_1 defined by (3.45) is irreducible, then C_1 has at most finitely many singular points (cf. [80]).

The projective plane curve C_1 can be covered by 3 affine plane curves U_0, U_1 and U_2. If $p \in U_i$, we can dehomogenize F with respect to X_i, say $X_2 = Z$, and define the *multiplicity* of F or C_1 at p, $\mu_F^0(p)$ or $\mu_{C_1}(p)$, to be $\mu_f^0(p)$. The multiplicity is independent of the choice of U_i.

If we are considering a finite set of points $p_1, \ldots, p_r \in \mathbb{P}^2$, we can always find a line L which does not pass through any of the points, and set

$$F_* = \frac{F}{L^m} \in \bar{\kappa}(\mathbb{P}^2).$$

Note that we may always find a projective change of coordinates so that the line L becomes the line Z at infinity. Then, under the natural identification of $\bar{\kappa}(\mathbb{A}^2)$ with $\bar{\kappa}(\mathbb{P}^2)$, this F_* is the same as the function $f(x, y) = F(x, y, 1)$.

If p is a simple point on C_1, and F is irreducible, then $\mathcal{O}_{C_1}(p)$ is a discrete valuation ring. We let ord_p denote the corresponding order function on $\bar{\kappa}(C_1)$. If $g \in \bar{\kappa}[x, y]$ with

$$G(X, Y, Z) := Z^n g\left(\frac{X}{Z}, \frac{Y}{Z}\right), \tag{3.46}$$

where $n = \deg(g)$, then $G_* \in \bar{\kappa}(\mathbb{P}^2)$ is determined as in the preceding paragraph. If $[G_*]$ is the residue class of G_* in $\bar{\kappa}(C_1)$, we define

$$\mathrm{ord}_p(G) = \mathrm{ord}_p([G_*]).$$

Take $F, G \in \bar{\kappa}[X, Y, Z]$ and $p \in \mathbb{P}^2$. We define

$$i_{F,G}(p) = \dim_{\bar{\kappa}} \mathcal{O}_{\mathbb{P}^2}(p)/(F_*, G_*).$$

This is independent of the way F_* and G_* are formed, and it satisfies properties (1)–(8) above: in (3), however, L should be a projective change of coordinates, and in (7), h, f, g should be homogeneous polynomials with $\deg(h) = \deg(g) - \deg(f)$.

We can define a line L to be *tangent* to a curve $Z(F)$ at p if $i_{F,L}(p) > \mu_F^0(p)$. Thus p is an *ordinary multiple point* of $Z(F)$ if $Z(F)$ has $\mu_F^0(p)$ distinct tangent lines at p.

Theorem 3.62. *Let $Z(F)$ and $Z(G)$ be projective plane curves of degree m and n respectively. Assume $Z(F)$ and $Z(G)$ have no common component. Then*

$$\sum_p i_{F,G}(p) = mn.$$

Proof. See Fulton [71], Chapter 5, Bézout's theorem. □

3.5.2 Riemann–Roch theorem

In view of Theorem 3.59, we will concentrate on smooth projective curves. Let C be a smooth projective curve. A divisor on C is simply a finite formal sum

$$D = \sum n_P P,$$

and we can define the *degree* of D to be

$$\deg(D) = \sum n_P.$$

The following *Riemann–Roch theorem* which allows us to compute the dimension $\ell(D)$ in most cases, is of inestimable value in the study of algebraic curves.

Theorem 3.63. *Let C be a smooth projective curve. There exists an integer $g \geq 0$ such that for all divisors $D \in \mathrm{Div}(C)$,*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1.$$

Proof. See Serre [236], II.9, Théorème 3, Hartshorne [90], IV, Theorem 1.3 or Fulton [71], VIII.6. □

The integer g is called the *genus* of smooth projective curve C. When C is not necessarily smooth or projective, its *genus* is defined to be the genus of a normalization of C. It is tautological from this definition that the genus is a birational invariant.

Corollary 3.64. *Let C be a smooth projective curve of genus g. Then*

$$\ell(K_C) = g, \quad \deg(K_C) = 2g - 2.$$

Proof. We first apply the Riemann–Roch theorem to the divisor $D = 0$ to get $1 - \ell(K_C) = -g + 1$. Note that $\ell(0) = 1$, since the only regular functions on a projective variety are the constant functions. Next we apply the theorem to $D = K_C$ to get $\ell(K_C) - 1 = \deg(K_C) - g + 1$. □

Corollary 3.65. *Let C be a smooth projective curve of genus g and take $D \in \mathrm{Div}(C)$.*

⌈1⌉ *If $\deg(D) < 0$, then $\ell(D) = 0$.*

⌈2⌉ *If $\deg(D) \geq 2g - 1$, then $\ell(D) = \deg(D) - g + 1$.*

⌈3⌉ *If $\ell(D) \neq 0$ and $\ell(K_C - D) \neq 0$, then we have $\ell(D) \leq \frac{1}{2}\deg(D) + 1$.*

Proof. If $f \in \mathcal{L}(D)$ is a nonzero function, then $D + (f)$ is effective, so

$$0 \leq \deg(D + (f)) = \deg(D)$$

since the divisors of functions have degree 0. Hence if $\deg(D) < 0$, then $\mathcal{L}(D) = \{0\}$, so $\ell(D) = 0$. This proves $\lceil 1 \rceil$, and then $\lceil 2 \rceil$ follows from $\lceil 1 \rceil$, Corollary 3.64, and the Riemann–Roch theorem.

To prove $\lceil 3 \rceil$, we observe that the linear systems $|D|$ and $|K_C - D|$ are nonempty and that the addition mapping $|K_C - D| \times |D| \longmapsto |K_C|$ is finite-to-one. Therefore,

$$\ell(K_C - D) - 1 + \ell(D) - 1 \leq \ell(K_C) - 1.$$

Combining this inequality with the Riemann–Roch theorem applied to D yields the desired result. □

Corollary 3.66. *Let C be a smooth projective curve of genus g and take $D \in \mathrm{Div}(C)$.*

(a) *If $\deg(D) \geq 2g$, then D is base point free.*

(b) *If $\deg(D) \geq 2g + 1$, then D is very ample.*

(c) *D is ample if and only if $\deg(D) > 0$.*

Proof. From Proposition 3.53, we deduce that D is base point free if and only if

$$\ell(D - P) = \ell(D) - 1$$

for all $P \in C$. Similarly, it follows that D is very ample if and only if

$$\ell(D - P - Q) = \ell(D) - 2$$

for all $P, Q \in C$. Since $\ell(K_C - E) = 0$ when $\deg(E) > 2g - 2$ (Corollary 3.65, $\lceil 1 \rceil$), statements (a) and (b) follows from the Riemann–Roch theorem applied to D, $D - P$, $D - P - Q$. Then (c) is a simple consequence of (b) and Corollary 3.65, $\lceil 1 \rceil$. □

Theorem 3.67. *Let C be a smooth projective plane curve of degree n. Then the genus g of C is given by the formula*

$$g = \frac{(n-1)(n-2)}{2}.$$

Proof. A regular differential form whose divisor has degree $n(n-3)$ can be constructed on C. Then Corollary 3.64 implies that

$$n(n-3) = \deg(K_C) = 2g - 2,$$

which gives the desired result (cf. [98]). □

When a plane curve has singularities, the formula for the genus must be modified as follows:

Theorem 3.68. *Let C be a projective plane curve of degree n with only ordinary singularities. Then its genus is given by the formula*

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P \in S} \frac{\delta_P(\delta_P - 1)}{2},$$

where S is the set of singular points and δ_P the multiplicity of C at P.

Proof. See Fulton [71], VIII.3, Proposition 5. □

We now describe a useful formula, called *Riemann–Hurwitz formula*, that can frequently be used to compute the genus of a curve.

Theorem 3.69. *Let C be a curve of genus g, let C' be a curve of genus g', and let $\varphi : C \longrightarrow C'$ be a finite separable mapping of degree $d \geq 1$. For each point $P \in C$, write e_P for the ramification index of φ at P, and assume either that $\mathrm{char}(\bar{\kappa}) = 0$ or else that $\mathrm{char}(\bar{\kappa})$ does not divide any of the e_P's. Then*

$$2g - 2 = d(2g' - 2) + \sum_{P \in C} (e_P - 1). \tag{3.47}$$

Proof. See Hindry and Silverman [98], Theorem A.4.2.5. □

Since the number $2 - 2g$ is just the *Euler characteristic* $\chi(C)$ of C, then (3.47) also assumes the following form:

$$\chi(C) = d\chi(C') + \sum_{P \in C} (1 - e_P). \tag{3.48}$$

The formula (3.48) for functions may be regarded as a logarithmic analogue of the formula (2.37) for numbers.

Let $C = Z(F)$ be an irreducible projective curve of degree m and let $\varphi : \tilde{C} \longrightarrow C$ be the birational morphism from the non-singular model $\tilde{C}$ onto C. Take $G \in \bar{\kappa}[X, Y, Z]$ with degree n such that $Z(G)$ do not contain C as a component. Define the *divisor* of G to be

$$\mathrm{div}(G) = \sum_{q \in \tilde{C}} \mathrm{ord}_q(G) q.$$

Then for $p \in C$,

$$i_{F,G}(p) = \sum_{q \in \varphi^{-1}(p)} \mathrm{ord}_q(G).$$

See [71], Chapter 7, Proposition 2. By the property (8),

$$\sum_{p \in C} i_{F,G}(p) = \sum_{p \in C} \sum_{q \in \varphi^{-1}(p)} \mathrm{ord}_q(G) = \sum_{q \in \tilde{C}} \mathrm{ord}_q(G).$$

By Bézout's theorem, $\operatorname{div}(G)$ is a divisor of degree mn.

If C has only ordinary multiple points, define the effective divisor

$$E = \sum_{q \in \tilde{C}} \{\mu_C(\varphi(q)) - 1\}\, q$$

with the degree

$$\deg(E) = \sum_{p \in C} \mu_C(p)\{\mu_C(p) - 1\}.$$

Further, if $m \geq 3$, $n = m - 3$, then $\operatorname{div}(G) - E$ is a canonical divisor (if $m = 3$, $\operatorname{div}(G) = 0$). See [71], Chapter 8, Proposition 8.

Let K be a function field of dimension 1 over an algebraically closed field κ (i.e., a finitely generated extension field of transcendence degree 1). We wish to establish a connection between nonsingular curves with function field K and the set of discrete valuation rings of K/κ. If x is a point on nonsingular curve C, then the local ring $\mathcal{O}(x)$ is a regular local ring of dimension one, and so it is a discrete valuation ring. Its quotient field is the function field K of C, and since $\kappa \subseteq \mathcal{O}(x)$, it is a valuation ring of K/κ. Thus the local rings of C define a subset of the set C_K of all discrete valuation rings of K/κ. We will sometimes call the elements of C_K *points*, and write $v \in C_K$, where v stands for the valuation ring $\mathcal{O}_{K,v}$. Note that the set C_K is infinite, because it contains all the local rings of any nonsingular curve with function field K; those local rings are all distinct, and there are infinitely many of them (see [90], Chapter I, Section 6).

We make C_K into a topological space by taking the closed sets to be the finite subsets and the whole space. If $U \subseteq C_K$ is an open subset of C_K, we define the ring of *regular functions* on U to be

$$\mathcal{O}(U) = \bigcap_{v \in U} \mathcal{O}_{K,v}.$$

An element $f \in \mathcal{O}(U)$ defines a function from U to κ by taking $f(v)$ to be the residue of f modulo the maximal ideal of $\mathcal{O}_{K,v}$. Note that any $f \in K$ is a regular function on some open set U (see [90], Chapter I, Lemma 6.5). Thus the function field of C_K is just K.

Theorem 3.70. *Let K be a function field of dimension 1 over an algebraically closed field κ. Then C_K defined above is isomorphic to a nonsingular projective curve.*

Proof. See [90], Chapter I, Theorem 6.9. □

3.5.3 Rational curves

Proposition 3.71. *Let C be a smooth projective curve. Then the following are equivalent:*

(i) *C has genus 0.*

(ii) *There exists a point $P \in C$ such that $\ell(P) = 2$.*

(iii) *For every point $P \in C$ we have $\ell(P) = 2$.*

Proof. Clearly, (iii) implies (ii), and applying Corollary 3.65 (ii) with $g = 0$ shows that (i) implies (iii). Finally, if (ii) holds, then the linear system associated to the divisor P gives a morphism $\varphi_P : C \longrightarrow \mathbb{P}(\mathcal{L}(P)) = \mathbb{P}^1$ of degree one, which must be an isomorphism since C and $\mathbb{P}^1$ are smooth curves. This proves that (ii) implies (i). □

Let C be a smooth projective curve of genus 0 defined over a field κ. Let K_C be a canonical divisor defined over κ. Then $-K_C$ is a divisor of degree 2 (Corollary 3.64), and is very ample (Corollary 3.66, (b)). The Riemann–Roch theorem tells us that the dimension of the associated embedding is $\ell(-K_C) = 3$. Hence C can be embedded into $\mathbb{P}^2$ as a smooth curve X of degree 2 (i.e., as a conic).

Theorem 3.72. *Let C be a smooth projective curve of genus 0 defined over a field κ.*

(1) *The curve C is isomorphic over κ to a conic in $\mathbb{P}^2$.*

(2) *The curve C is isomorphic over κ to $\mathbb{P}^1$ if and only if it possesses a κ-rational point.*

The conclusion (2) in Theorem 3.72 was proved simultaneously in a joint paper of Hilbert and Hurwitz and a paper of Poincaré. In particular, notice that over an algebraically closed field, all curves of genus 0 are isomorphic to $\mathbb{P}^1$. A curve is said to be *rational* if it is birational to the projective line.

A natural question is how one obtains all the irreducible algebraic curves which have a rational parametric representation in an independent variable z. In other words, if

$$f(x, y) = 0 \tag{3.49}$$

is an irreducible equation of the curve, then we require two rational functions

$$x = \varphi(z), \quad y = \psi(z)$$

of a variable z, not both constant, which satisfy the equation (3.49) identically in z.

Theorem 3.73 (cf. [253]). *An algebraic curve has a rational parametric representation if and only if it is of genus 0.*

3.5.4 Elliptic curves

An algebraic curve defined over a field κ is called an *elliptic curve* if a normalization of the curve has genus 1.

Proposition 3.74. *Let C be a curve of genus 1 defined over a field κ, and let $O \in C(\kappa)$. Then there exists $a_1, a_2, a_3, a_4, a_6 \in \kappa$ such that C is isomorphic over κ to the plane cubic E given by the generalized Weierstrass equation*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{3.50}$$

Under this isomorphism, the point O is mapped to the inflection point $[X, Y, Z] = [0, 1, 0] \in E$.

Proof. From Corollary 3.64, we know that any canonical divisor K_C has

$$\deg(K_C) = 0, \quad \ell(K_C) = 1.$$

Thus we can find an effective canonical divisor K_C with degree 0, which means that $K_C = 0$. In other words, the zero divisor is a canonical divisor. This means that there exists a regular differential form without zeros.

Let D be a nonzero effective divisor on C. The Riemann–Roch theorem with $g = 1$ and $K_C = 0$ implies that $\ell(D) = \deg(D)$. Fix a point $O \in C(\kappa)$, and for each integer $n \geq 1$, consider the vector space $\mathcal{L}(D_n)$ of the divisor $D_n = nO$ whose dimension is

$$\ell(D_n) = \deg(D_n) = n.$$

Notice that

$$\mathcal{L}(D_1) \subset \mathcal{L}(D_2) \subset \mathcal{L}(D_3) \subset \cdots.$$

Since $\dim \mathcal{L}(D_n) = n$, we can find two functions $x, y \in \bar{\kappa}(C)$ such that

$$\mathcal{L}(D_1) = \kappa, \quad \mathcal{L}(D_2) = \kappa \oplus \kappa x, \quad \mathcal{L}(D_3) = \kappa \oplus \kappa x \oplus \kappa y.$$

We know by Corollary 3.66 that the linear system associated to the vector space $\mathcal{L}(D_3)$ is very ample. This means that the rational mapping

$$\varphi_{D_3} = [x, y, 1] : C \longrightarrow \mathbb{P}^2$$

extends to an isomorphism between C and its image $\varphi_{D_3}(C)$. In particular, $\varphi_{D_3}(C)$ is a smooth plane curve.

Notice that x has a pole of order 2 at O, that y has a pole of order 3 at O, and that x and y have no other poles. Thus we have

$$\mathcal{L}(D_4) = \kappa \oplus \kappa x \oplus \kappa y \oplus \kappa x^2, \quad \mathcal{L}(D_5) = \kappa \oplus \kappa x \oplus \kappa y \oplus \kappa x^2 \oplus \kappa xy.$$

The functions $1, x, y, x^2, xy$ are linearly independent over κ since their poles have different orders at O. But when we look at $\mathcal{L}(D_6)$, we find that there are 7 functions that can be naturally constructed using x and y, namely

$$\{1, x, x^2, x^3, y, xy, y^2\} \subset \mathcal{L}(D_6).$$

The vector space $\mathcal{L}(D_6)$ has dimension 6, so these functions satisfy a nontrivial κ-linear relation:

$$ay^2 + bxy + cy = dx^3 + ex^2 + fx + g.$$

Since only the y^2 and x^3 terms have poles of order 6, either the coefficients a and d are both nonzero, or they both vanish. But if $a = d = 0$, then every term has a different-order pole at O, so all of the other coefficients would have to vanish. Hence $ad \neq 0$. This allows us to replace (x, y) by (adx, ad^2y) and cancel a^3d^4, which gives an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.51}$$

with $a_i \in \kappa$, that is, we obtain a plane affine model of C given by (3.51). As usual, the plane affine model of C is as the locus of the homogeneous coordinate equation (3.50) in $\mathbb{P}^2$ with only one point $[0, 1, 0]$ on the line at ∞. □

Conversely, every smooth cubic curve E given by a generalized Weierstrass equation is an elliptic curve defined over κ. The functions $x, y \in \bar{\kappa}(C)$ in the proof of proposition are called *Weierstrass coordinate functions* on C, which have the following property

$$\bar{\kappa}(C) = \bar{\kappa}(x, y), \quad [\bar{\kappa}(C) : \bar{\kappa}(x)] = 2.$$

The point O in C corresponding to $[0, 1, 0]$ under the mapping φ is called a *basepoint of* C, or the *origin of* C.

Any two generalized Weierstrass equations for C are related by a linear change of variables of the form

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + su^2x' + t, \end{aligned} \tag{3.52}$$

with $u, r, s, t \in \kappa,\ u \neq 0$. The coefficients a_i' for the new equation are computed as follows:

$$\begin{aligned} ua_1' &= a_1 + 2s, \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\ u^3a_3' &= a_3 + ra_1 + 2t, \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6a_6' &= a_6 + ra_4 - ta_3 + r^2a_2 - rta_1 + r^3 - t^2. \end{aligned}$$

Next we introduce the smoothness condition of the plane cubic E given by the generalized Weierstrass equation (3.50). The following quantities are usually used:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_2a_3^2 - a_1a_3a_4 - a_4^2 + a_1^2a_6 + 4a_2a_6, \\ \Delta &= 9b_2b_4b_6 - b_2^2b_8 - 8b_4^3 - 27b_6^2. \end{aligned}$$

One easily verifies that they satisfy the relations

$$4b_8 = b_2b_6 - b_4^2, \quad 1728\Delta = c_4^3 - c_6^2,$$

where

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= 36b_2b_4 - b_2^3 - 216b_6. \end{aligned}$$

The quantity Δ is called the *discriminant* of the generalized Weierstrass equation. The following quantities

$$\begin{aligned} j &= \frac{c_4^3}{\Delta}, \\ \omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} \end{aligned}$$

are called the *j-invariant* and the *invariant differential* associated with the generalized Weierstrass equation, respectively. Under the linear change of variables (3.52), the associated quantities for new equation can be given by

$$\begin{aligned} u^2b_2' &= b_2 + 12r, \\ u^4b_4' &= b_4 + rb_2 + 6r^2, \\ u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3, \\ u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4, \end{aligned}$$

$u^4c_4' = c_4$, $u^6c_6' = c_6$, $u^{12}\Delta' = \Delta$, $j' = j$ and $u^{-1}\omega' = \omega$.

Proposition 3.75. *The curve given by a generalized Weierstrass equation is non-singular if and only if $\Delta \neq 0$. Otherwise the curve is singular with exactly one singular point. The curve has an ordinary 2-fold point (node) if and only if $\Delta = 0$ and $c_4 \neq 0$. The curve has a non-ordinary 2-fold point (cusp) if and only if $\Delta = 0$ and $c_4 = 0$.*

Proof. Let E be given by the generalized Weierstrass equation

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - \left(X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\right) = 0.$$

Obviously, the point at infinity $O = [0,1,0]$ is never singular since

$$\frac{\partial F}{\partial Z}(O) = 1 \neq 0.$$

Thus to study the singularity of E, it is sufficient to consider the affine equation

$$f(x,y) = F(x,y,1) = y^2 + a_1xy + a_3y - \left(x^3 + a_2x^2 + a_4x + a_6\right).$$

First of all, suppose that E is singular, say at $p_0 = (x_0, y_0)$. The substitution

$$x = x' + x_0, \quad y = y' + y_0$$

leaves Δ and c_4 invariant, so without loss of generality we may assume $p_0 = (0,0)$. Then

$$a_6 = f(p_0) = 0, \quad a_4 = \frac{\partial f}{\partial x}(p_0) = 0, \quad a_3 = \frac{\partial f}{\partial y}(p_0) = 0,$$

so the equation for E takes the form

$$f(x,y) = y^2 + a_1xy - a_2x^2 - x^3 = 0.$$

This equation has associated quantities

$$\Delta = 0, \quad c_4 = \left(a_1^2 + 4a_2\right)^2.$$

Note that

$$y^2 + a_1xy - a_2x^2 = (y - \alpha x)(y - \beta x)$$

for some $\alpha, \beta \in \bar{\kappa}$. Now by definition, E has a node (respectively cusp) if $\alpha \neq \beta$ (respectively $\alpha = \beta$), which occurs if and only if its discriminant

$$a_1^2 + 4a_2 \neq 0 \ \text{(respectively} = 0).$$

To complete the proof, it remains to show that if E is non-singular, then $\Delta \neq 0$. Here we omit the proof, which can be found by late discussion. □

If $\mathrm{char}(\bar{\kappa}) = 2$, one easily computes

$$j = \frac{a_1^{12}}{\Delta}.$$

Hence we have that the condition $j = 0$ is equivalent to $a_1 = 0$, and the equation (3.51) transforms as follows: if $a_1 \neq 0$ (i.e. $j \neq 0$), then choosing suitably r, s, t we can achieve $a_1 = 1$, $a_3 = 0$, $a_4 = 0$, and the equation (3.51) takes the form

$$y^2 + xy = x^3 + a_2x^2 + a_6, \tag{3.53}$$

with the condition of smoothness given by $\Delta = a_6 \neq 0$. For this case, one has $j = 1/a_6$. Suppose next that $a_1 = 0$ (i.e. $j = 0$), then the equation (3.51) transforms to

$$y^2 + a_3 y = x^3 + a_4 x + a_6, \tag{3.54}$$

and the condition of smoothness in this case is $\Delta = a_3^4 \neq 0$.

If $\mathrm{char}(\bar{\kappa}) = 3$, the equation (3.51) transforms to

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6, \tag{3.55}$$

where multiple roots are again disallowed. Moreover, we have $a_4 = 0$ in the case $j \neq 0$. Now it follows

$$\Delta = -a_2^3 a_6, \quad j = -\frac{a_2^3}{a_6}.$$

When $j = 0$, we have $a_2 = 0$, $\Delta = -a_4^3$.

If $\mathrm{char}(\bar{\kappa}) \neq 2$, then we can simplify the generalized Weierstrass equation by completing the square. Thus replacing y by $\frac{1}{2}(y - a_1 x - a_3)$ gives an equation of the form

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6. \tag{3.56}$$

Now E is singular if and only if there is a point $(x_0, y_0) \in E$ satisfying

$$2y_0 = 12x_0^2 + 2b_2 x_0 + 2b_4 = 0.$$

In other words, the singular points are exactly points of the form $(x_0, 0)$ with x_0 a double root of the equation

$$4x^3 + b_2 x^2 + 2b_4 x + b_6 = 0.$$

This cubic polynomial has a double root if and only if its discriminant (which equals 16Δ) vanishes.

If further $\mathrm{char}(\bar{\kappa}) \neq 2, 3$, then replacing (x, y) by $((x - 3b_2)/36, y/108)$ eliminates the x^2 term of (3.56), yielding the simple *Weierstrass equation*

$$y^2 = x^3 + ax + b,$$

where

$$a = -27c_4, \quad b = -54c_6.$$

The only change of variables preserving this form of the equation is

$$x = u^2 x', \quad y = u^3 y' \tag{3.57}$$

for some $u \in \bar{\kappa}_*$, and then

$$u^4 a' = a, \quad u^6 b' = b, \quad u^{12}\Delta' = \Delta.$$

We summary the above discussion as follows:

Theorem 3.76 (cf. [80], [256]). *For each smooth elliptic curve E defined over a field κ of characteristic $\neq 2, 3$, there exists a coordinate system such that the affine equation of E may be expressed by a Weierstrass equation*

$$y^2 = x^3 + ax + b \tag{3.58}$$

with $a, b \in \kappa$, and

$$\Delta = -16(4a^3 + 27b^2) \neq 0, \quad j = \frac{1728(-4a)^3}{\Delta}. \tag{3.59}$$

The only change of variables preserving this form of the equation is (3.57).

The condition that the discriminant Δ is nonzero is equivalent to the curve being smooth. It is also equivalent to the cubic $x^3 + ax + b$ having 3 different roots since

$$16(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = \Delta,$$

where x_1, x_2, x_3 are the three zeros of the polynomial $x^3 + ax + b$.

Proposition 3.77. *The invariant differential ω on an elliptic curve associated to a generalized Weierstrass equation is regular and non-vanishing, i.e.* $\operatorname{div}(\omega) = 0$.

Proof. Silverman [256], Chapter III, Proposition 1.5. □

Proposition 3.78. *Two elliptic curves associated to generalized Weierstrass equations are isomorphic over $\bar{\kappa}$ if and only if they have the same j-invariant.*

Proof. Schmitt–Zimmer [233], Proposition 1.8. □

Conjecture 3.79 (Lang, Stark [145]). *If $(x, y) \in \mathbb{Z}^2$ is a point on the elliptic curve E defined by* (3.58) *with $a, b \in \mathbb{Z}$, then for $\varepsilon > 0$, there exists a number $C(\varepsilon)$ such that*

$$|x| \leq C(\varepsilon) \max\{|a|^3, |b|^2\}^{\frac{5}{3}+\varepsilon}. \tag{3.60}$$

Lang originally posed the conjecture with an unknown exponent; then Stark suggested that the exponent should be $5/3$.

Question 3.80. *Given polynomials a, b satisfying* (3.59). *If polynomials x, y satisfy* (3.58)*, does the following relation hold*

$$\frac{3}{5} \deg(x) \leq \max\{3 \deg(a), 2 \deg(b)\}? \tag{3.61}$$

Let E be an elliptic curve given by a generalized Weierstrass equation (3.51). Remember that $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the equation together with the point $O = [0, 1, 0]$ at infinity. Let $L \subset \mathbb{P}^2$ be a line. Then since the equation has degree three, L intersects E at exactly three points, say P, Q, R. Note that if L is tangent to E, then P, Q, R may not be distinct. The fact that $L \cap E$ (counting multiplicity) consists of three points is a special case of Bézout's theorem. One can use this fact to define an addition law on E. Namely, given $P, Q \in E$, draw the line L through P and Q (tangent line to E if $P = Q$). Let R be the third point of intersection of L with E. Let L' be the line connecting R and O. Define $P + Q$ to be the third point of intersection of E with L'. The composition law makes E into an Abelian group with identity element O.

The resulting group is called the Mordell–Weil group of E. It is rather easy to determine explicit formulae for the above group law. We now give such formulae in terms of an elliptic curve given by generalized Weierstrass equation (3.51). Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ denote points on the curve. Then

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3).$$

Set

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

when $x_1 \neq x_2$ and

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

when $x_1 = x_2$. If $P_3 = (x_3, y_3) = P_1 + P_2$, then x_3 and y_3 are given by the formulae

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \mu - a_3. \end{aligned}$$

Further,

$$E(\kappa) = \{\text{solutions } (x, y) \in \kappa^2 \text{ of (3.51)}\} \cup \{O\}$$

is a subgroup of E (see [256], Proposition 2.2).

Example 3.81 (cf. [300]). Let $E/\mathbb{Q}$ be an elliptic curve defined by the equation (3.58). If $a = -1$, $b = 0$, then

$$E(\mathbb{Q}) = \{(0, 0), (1, 0), (-1, 0), O\}.$$

Let E/κ be an elliptic curve and $\ell \in \mathbb{Z}$ a prime. The (ℓ-*adic*) *Tate module of* E is the group

$$T_\ell(E) = \lim_{\leftarrow n} E[\ell^n],$$

the inverse limit being taken with respect to the natural mappings

$$[\ell] : E[\ell^{n+1}] \longrightarrow E[\ell^n].$$

Since each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a $\mathbb{Z}_\ell$-module. Note that since the multiplication mappings $[\ell]$ are surjective, the inverse limit topology on $T_\ell(E)$ is equivalent to the ℓ-adic topology it gains as a $\mathbb{Z}_\ell$-module. Proposition 3.43 implies immediately

Proposition 3.82 ([256]). *The Tate module has the following structure:*

(d1) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *if* $\ell \neq \mathrm{char}(\kappa)$.

(d2) $T_p(E) \cong \{0\}$ *or* $\mathbb{Z}_p$ *if* $p = \mathrm{char}(\kappa) > 0$.

Let $m \geq 2$ be an integer (prime to $\mathrm{char}(\kappa)$ if $\mathrm{char}(\kappa) > 0$). Note that each element σ of the Galois group $G_{\bar{\kappa}/\kappa}$ acts on $E[m]$ since, if $[m]P = O$, then

$$[m]\sigma(P) = \sigma([m]P) = O.$$

We thus obtain a representation

$$G_{\bar{\kappa}/\kappa} \longrightarrow \mathrm{Aut}(E[m]) \cong GL(2, \mathbb{Z}/m\mathbb{Z}),$$

where the latter isomorphism involves choosing a basis for $E[m]$. The action of $G_{\bar{\kappa}/\kappa}$ on each $E[\ell^n]$ commutes with the multiplication mappings $[\ell]$ used to form the inverse limit, so $G_{\bar{\kappa}/\kappa}$ also acts on $T_\ell(E)$. The *ℓ-adic representation* (*of* $G_{\bar{\kappa}/\kappa}$ *on* E), denoted $\rho_{E,\ell}$, is the mapping

$$\rho_{E,\ell} : G_{\bar{\kappa}/\kappa} \longrightarrow \mathrm{Aut}(T_\ell(E))$$

giving the action of $G_{\bar{\kappa}/\kappa}$ on $T_\ell(E)$ as described above. If $\ell \neq \mathrm{char}(\kappa)$, by choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$ we obtain a representation

$$G_{\bar{\kappa}/\kappa} \longrightarrow GL(2, \mathbb{Z}_\ell);$$

and then the natural inclusion $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$ gives

$$G_{\bar{\kappa}/\kappa} \longrightarrow GL(2, \mathbb{Q}_\ell).$$

If κ is a local field, complete with respect to a discrete valuation $v = \mathrm{ord}$, we can find a generalized Weierstrass equation (3.51) for E/κ with all coefficients $a_i \in \mathcal{O}_{\kappa,v}$ since replacing (x, y) by $(u^{-2}x, u^{-3}y)$ causes each a_i to become $a_i u^i$, if we choose u divisible by a large power of a uniformizing parameter t for the valuation ring $\mathcal{O}_{\kappa,v}$. Since v is discrete, we can look for an equation of v-integral coefficients (and so the discriminant Δ is v-integral) with $v(\Delta)$ as small as possible among all curves in the same isomorphism class, called a *minimal* (*Weierstrass*) *equation* for E at v. Let E/κ

be an elliptic curve associated to a generalized Weierstrass equation (3.51) with v-integral coefficients. If $v(\Delta) < 12$ (or $v(c_4) < 4$ or $v(c_6) < 6$), then the equation is minimal. If $\mathrm{char}(\mathbb{F}_v(\kappa)) \neq 2, 3$, the converse is also true (cf. [233], Theorem 4.2).

The natural reduction mapping $\mathcal{O}_{\kappa,v} \longrightarrow \mathbb{F}_v(\kappa)$ is denoted $z \mapsto \tilde{z}$. Now having chosen a minimal Weierstrass equation (3.51) for E/κ, we can reduce its coefficients modulo t to obtain a (possibly singular) curve over $\mathbb{F}_v(\kappa)$, namely

$$\tilde{E}: \quad y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6.$$

The curve $\tilde{E}/\mathbb{F}_v(\kappa)$ is called the *reduction of E modulo t*. Further, E is said to has *good* (or *stable*) *reduction* over κ if $\tilde{E}$ is non-singular, otherwise, has *bad reduction*. In the case of having bad reduction, E is also said to have *multiplicative* (or *semi-stable*) *reduction* over κ if $\tilde{E}$ has an ordinary double point, otherwise, have *additive* (or *unstable*) *reduction* over κ. If E has multiplicative reduction, then the reduction is said to be *split* (respectively *non-split*) if the slopes of the tangent lines at the double point are in $\mathbb{F}_v(\kappa)$ (respectively not in $\mathbb{F}_v(\kappa)$).

Proposition 3.83. *Let E be an elliptic curve over a local field κ with minimal Weierstrass equation* (3.51).

(A) *E has good reduction if and only if $v(\Delta) = 0$.*

(B) *E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$. The multiplicative reduction is split if $-c_4c_6$ is a square in $\mathbb{F}_v(\kappa)$ at $\mathrm{char}(\mathbb{F}_v(\kappa)) \neq 2, 3$; b_2 is a square in $\mathbb{F}_v(\kappa)$ at $\mathrm{char}(\mathbb{F}_v(\kappa)) = 3$; the polynomial $x^2 + a_1x + (a_3a_1^{-1} + a_2)$ has a root in $\mathbb{F}_v(\kappa)$ at $\mathrm{char}(\mathbb{F}_v(\kappa)) = 2$.*

(C) *E has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$.*

Proof. See [233], Proposition 4.4; or [256]. □

3.5.5 Hyperelliptic curves

A curve C of genus $g \geq 2$ is called a *hyperelliptic* if there exists a double covering $\varphi : C \longrightarrow \mathbb{P}^1$. Let C be a hyperelliptic curve defined over a field κ with $\mathrm{char}(\bar{\kappa}) \neq 2$. The function field of C is a quadratic extension of $\bar{\kappa}(\mathbb{P}^1)$, hence has the shape $\bar{\kappa}(x, y)$, where

$$y^2 = F(x) \tag{3.62}$$

for some polynomial $F(x) \in \bar{\kappa}[x]$. This equation gives an affine model C' for C. If the polynomial F has a double root, say α, then we can replace y by $(x - \alpha)y$ and cancel $(x - \alpha)^2$. So we may assume that C' is given by an affine equation (3.62) for some $F(x) \in \bar{\kappa}[x]$ with distinct roots. Then the affine curve C' is smooth. We can use the functions x and y to embed C' into $\mathbb{P}^{g+1}$ via the mapping

$$(x, y) \longmapsto [1, x, x^2, \ldots, x^g, y].$$

Define

$$d = \begin{cases} \deg(F), & \text{if } \deg(F) \text{ is even,} \\ \deg(F) + 1, & \text{if } \deg(F) \text{ is odd,} \end{cases}$$

and consider the affine curve C'' defined by the equation

$$v^2 = G(u) = u^d F\left(\frac{1}{u}\right). \tag{3.63}$$

Since the mapping

$$\big(u, v\big) = \big(x^{-1}, yx^{-d/2}\big)$$

defines an isomorphism

$$\{(x, y) \in C' \mid x \neq 0\} \longrightarrow \{(u, v) \in C'' \mid u \neq 0\},$$

then C'' also is a smooth affine model of C. Note that the mapping $\varphi : C \longrightarrow \mathbb{P}^1$ has degree 2 and is ramified at the points where $F(x) = 0$, and if $\deg(F)$ is odd, it is also ramified at the point at infinity. Thus φ is ramified at exactly d points. The ramification index at each ramified point must be 2, so the Riemann–Hurwitz formula (3.47) yields

$$2g - 2 = \deg(\varphi)\big(2g(\mathbb{P}') - 2\big) + \sum_{P \in C}(e_P - 1) = -4 + d,$$

and we thus find that

$$g = \frac{d}{2} - 1 = \left[\frac{\deg(F) - 1}{2}\right],$$

where $[x]$ denotes the maximal integer $\leq x$.

Proposition 3.84 (cf. [80], [98]). *Every curve of genus* 2 *is hyperelliptic.*

Proof. If C is a curve of genus 2, then Riemann–Roch theorem says that

$$\ell(K_C) = \deg(K_C) = 2,$$

so the linear $|K_C|$ gives a mapping $\varphi_{K_C} : C \longrightarrow \mathbb{P}^1$ of degree 2. Hence the curve C is hyperelliptic. □

Theorem 3.85. *Let C be a smooth projective curve of genus g.*

(1) *The canonical divisor K_C is base point free if and only if $g \geq 1$.*

(2) *The canonical divisor K_C is ample if and only if $g \geq 2$.*

(3) *The canonical divisor K_C is very ample if and only if $g \geq 3$ and the curve is not hyperelliptic.*

Proof. If K_C is not base point free, then there is a point $P \in C$ with

$$\ell(K_C - P) = \ell(K_C) = g.$$

Hence Riemann–Roch theorem implies

$$\ell(P) = \ell(K_C - P) + 2 - g = 2,$$

and by Proposition 3.71, this implies that C is rational. This gives (1).

We have already seen that if C has genus 1, then $K_C = 0$. Corollary 3.64 and Corollary 3.66 tell us that $\deg(K_C) = 2g - 2$ and that K_C is ample if and only if $\deg(K_C) > 0$, which proves (2).

For the remaining parts, we may assume that $g \geq 2$. From the proof of Corollary 3.66, it follows that K_C is very ample if and only if

$$\ell(K_C - P - Q) = \ell(K_C) - 2 = g - 2$$

for all $P, Q \in C$. On the other hand, Riemann–Roch theorem yields

$$\ell(P + Q) - \ell(K_C - P - Q) = \deg(P + Q) - g + 1 = 3 - g.$$

Combining these two equations, we find that K_C is very ample if and only if $\ell(P + Q) = 1$ for all $P, Q \in C$. If C is hyperelliptic, say $\varphi : C \longrightarrow \mathbb{P}^1$, then the inverse image of any point in $\mathbb{P}^1$ consists of two points P, Q that satisfy $\ell(P + Q) = 2$. Thus K_C is not very ample on a hyperelliptic curve. Conversely, if K_C is not ample, then there are two points $P, Q \in C$ with $\ell(P+Q) = 2$, and hence the linear system $|P+Q|$ defines a mapping of degree 2 from C to $\mathbb{P}^1$. This completes the proof of (3). □

3.5.6 Jacobian of curves

Theorem 3.86. *Let C be a smooth projective curve of genus $g \geq 1$. There exists an Abelian variety $\mathrm{Jac}(C)$, called the Jacobian of C, and an injection $j : C \longrightarrow \mathrm{Jac}(C)$, called the Jacobian embedding of C, with the following properties:*

⟨1⟩ *Extend j linearly to divisors on C. Then j induces a group isomorphism between $\mathrm{Pic}^0(C)$ and $\mathrm{Jac}(C)$.*

⟨2⟩ *For each $r \geq 0$, define a subvariety $W_r \subset \mathrm{Jac}(C)$ by*

$$W_r = \begin{cases} \{0\}, & \text{if } r = 0, \\ \underbrace{j(C) + \cdots + j(C)}_{r \text{ copies}}, & \text{if } r > 0. \end{cases}$$

Then

$$\dim W_r = \min\{r, g\}, \;\; W_g = \mathrm{Jac}(C).$$

⟨3⟩ *Let* $\Theta = W_{g-1}$. *Then* Θ *is an irreducible ample divisor on* $\mathrm{Jac}(C)$.

Proof. See [98], Theorem A.8.1.1. □

It is clear that the curve C determines the pair $(\mathrm{Jac}(C), \Theta)$ up to a natural isomorphism. The converse is called *Torelli's theorem*: Over an algebraically closed field, the isomorphism class of the pair $(\mathrm{Jac}(C), \Theta)$ determines the isomorphism class of the curve C. See Theorem 12.1 in Milne [182] for a further discussion.

Suppose that the curve C is defined over a field κ. Then its Jacobian variety $\mathrm{Jac}(C)$ is also defined over κ. But, it may not be possible to define the injection $j : C \longrightarrow \mathrm{Jac}(C)$ over κ. More precisely, the mapping j is defined by choosing a divisor D of degree 1 and then setting

$$j : C \longrightarrow \mathrm{Pic}^0(C) \cong \mathrm{Jac}(C), \;\; j(x) = \mathrm{Cl}(x - D).$$

In particular, if there is a point $x_0 \in C(\kappa)$, then we can take $D = x_0$ to get a mapping j that is defined over κ. This will suffice for the proof of Faltings' Theorem 8.3 (Mordell conjecture), since if C has no κ-rational points, then it is trivial to prove that $C(\kappa)$ is finite. We also note that once we have identified $\mathrm{Jac}(C)$ and $\mathrm{Pic}^0(C)$, then the embedding j is unique up to translation.

3.6 Sheaves and vector bundles

3.6.1 Sheaves

Definition 3.87. Let X be a topological space. A *presheaf* $\mathcal{F}$ of Abelian groups on X associates to each open set $U \subset X$ a Abelian group $\mathcal{F}(U)$, called the *sections* of $\mathcal{F}$ over U, and to each pair $V \subset U$ of open sets a mapping $r_{U,V} : \mathcal{F}(U) \longrightarrow \mathcal{F}(V)$, called the *restriction mapping*, satisfying

(i) $\mathcal{F}(\emptyset) = 0$, where $\emptyset$ is the empty set,

(ii) $r_{U,U} : \mathcal{F}(U) \longrightarrow \mathcal{F}(U)$ is the identity,

(iii) $r_{W,V} = r_{U,V} \circ r_{W,U}$ for any triple $V \subset U \subset W$ of open sets. By virtue of this relation, we may write $\eta|_V$ for $r_{U,V}(\eta)$ without loss of information.

We define a *presheaf of rings*, a *presheaf of sets*, or a *presheaf* with values in any fixed category $\mathfrak{C}$, by replacing the words "Abelian group" in the definition by "ring", "set", or "object of $\mathfrak{C}$" respectively. We will stick to the case of Abelian groups in this section, and let the reader make the necessary modifications for the case of rings, sets, etc.

Definition 3.88. A presheaf $\mathcal{F}$ on a topological space X is a *sheaf* $\mathcal{F}$ if it satisfies the following supplementary conditions:

(iv) if $\zeta \in \mathcal{F}(U \cup V)$ and $\zeta|_U = \zeta|_V = 0$, then $\zeta = 0$;

(v) for any pair of open sets $U,\ V$ in X and sections $\xi \in \mathcal{F}(U),\ \eta \in \mathcal{F}(V)$ such that

$$\xi|_{U\cap V} = \eta|_{U\cap V},$$

there exists a section $\zeta \in \mathcal{F}(U \cup V)$ with

$$\zeta|_U = \xi, \quad \zeta|_V = \eta.$$

(Note condition (iv) implies that ζ is unique.)

Example 3.89. Let X be a variety over a field κ. For each open set $U \subseteq X$, let $\mathcal{O}(U)$ be the ring of all regular functions on U, and for each pair $U \subseteq V$ of open sets, let $r_{V,U} : \mathcal{O}(V) \longrightarrow \mathcal{O}(U)$ be the restriction mapping in the usual sense. Then $\mathcal{O}$ is a sheaf of rings on X, called the *sheaf of regular functions* on X.

Example 3.90. The sheaf of invertible functions $\mathcal{O}^*$ associated to an open set U of a variety X the set of regular functions without zeros on U. It is a sheaf of groups. Notice that $\mathcal{O}^*(U)$ is exactly the group of units in the ring $\mathcal{O}(U)$.

Example 3.91. On a variety X, the sheaf of rational functions $\mathcal{K}_X$ attaches to each open set U the set of rational functions on U.

Example 3.92. The sheaf of differential r-forms Ω^r on a variety X associates to an open set U the set $\Omega^r[U]$ of regular r-differentials on U.

Example 3.93. In the same way, one can define the sheaf C^0 of continuous real-valued functions on any topological space, or the sheaf C^∞ of C^∞-functions on a C^∞-manifold, or the sheaf $\mathcal{A}$ of holomorphic functions on a complex manifold.

Example 3.94. Let X be a topological space, and A an Abelian group, say, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. We define the *constant sheaf*, also denoted by A, on X determined by A as follows. Give A the discrete topology, and for any open set $U \subseteq X$, let $A(U)$ be the group of all continuous mappings of U into A. Then with the usual restriction mappings, we obtain a sheaf A. Note that for every connected open set U, $A(U) \cong A$.

There is an obvious way to form the direct sum and tensor product of two sheaves of modules:

$$(\mathcal{F} \oplus \mathcal{G})(U) = \mathcal{F}(U) \oplus \mathcal{G}(U), \quad (\mathcal{F} \otimes \mathcal{G})(U) = \mathcal{F}(U) \otimes \mathcal{G}(U).$$

Definition 3.95. If $\mathcal{F}$ is a presheaf on a topological space X, and if x is a point of X, we define the *stalk* $\mathcal{F}(x)$ of $\mathcal{F}$ at x to be the direct limit of the groups $\mathcal{F}(U)$ for all open sets U containing x, via the restriction mappings r.

Thus an element of $\mathcal{F}(x)$ is represented by a pair (U, f) where U is an open subset of X containing x, and f is an element of $\mathcal{F}(U)$. Two such pairs (U, f) and (W, g) define the same element of $\mathcal{F}(x)$ if and only if there is a neighborhood $V \subset U \cap W$ of x such that $f|_V = g|_V$. Thus we may speak of elements of the stalk $\mathcal{F}(x)$ as *germs* of sections of $\mathcal{F}$ at the point x. In the case of a variety X and its sheaf of regular functions $\mathcal{O}$, the stalk $\mathcal{O}(x)$ at a point x is just the local ring of x on X, which was defined in Section 3.2.3.

Let $\mathcal{F}$ be a sheaf on X. The set of *global sections* of $\mathcal{F}$ is the set $\mathcal{F}(X)$. This set is also frequently denoted by $\Gamma(X, \mathcal{F})$.

Definition 3.96. If $\mathcal{F}$ and $\mathcal{G}$ are presheaves (or sheaves) on a topological space X, a *mapping* (or *morphism*, or *homomorphism*) $\varphi : \mathcal{F} \longrightarrow \mathcal{G}$ consists of a homomorphism of Abelian groups $\varphi_U : \mathcal{F}(U) \longrightarrow \mathcal{G}(U)$ for each open set $U \subset X$ such that for $V \subset U \subset X$, φ_U and φ_V commute with the restriction mappings, that is, the diagram

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{\varphi_U} & \mathcal{G}(U) \\ \Big\downarrow{\scriptstyle r_{U,V}} & & \Big\downarrow{\scriptstyle r'_{U,V}} \\ \mathcal{F}(V) & \xrightarrow{\varphi_V} & \mathcal{G}(V) \end{array}$$

is commutative, where r and r' are the restriction mappings in $\mathcal{F}$ and $\mathcal{G}$. An *isomorphism* is a mapping which has a two-sided inverse.

Proposition 3.97. *Let $\varphi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaves on a topological space X. Then φ is an isomorphism if and only if the induced mapping on the stalk $\varphi_x : \mathcal{F}(x) \longrightarrow \mathcal{G}(x)$ is an isomorphism for every $x \in X$.*

Proof. See Hartshorne [90], Chap. II, Proposition 1.1. □

Definition 3.98. Let $\varphi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of presheaves on a topological space X. We define the *presheaf kernel* of φ, *presheaf image* of φ, and *presheaf cokernel* of φ to be the presheaves given respectively by

$$U \mapsto \mathrm{Ker}(\varphi_U), \;\; U \mapsto \mathrm{Im}(\varphi_U), \;\; U \mapsto \mathrm{Coker}(\varphi_U) = \mathcal{G}(U)/\mathrm{Im}(\varphi_U).$$

Note that if $\varphi : \mathcal{F} \longrightarrow \mathcal{G}$ is a morphism of sheaves, then the presheaf kernel of φ is a sheaf, but the presheaf cokernel and presheaf image of φ are in general not sheaves. This leads us to the notion of a sheaf associated to a presheaf.

Proposition 3.99. *Given a presheaf $\mathcal{F}$, there is a sheaf $\mathcal{F}^+$ and a morphism $\theta : \mathcal{F} \longrightarrow \mathcal{F}^+$ with the property that for any sheaf $\mathcal{G}$ and any morphism $\varphi : \mathcal{F} \longrightarrow \mathcal{G}$, there is a unique morphism $\phi : \mathcal{F}^+ \longrightarrow \mathcal{G}$ such that $\varphi = \psi \circ \theta$. Furthermore the pair $(\mathcal{F}^+, \theta)$ is unique up to unique isomorphism, called the sheaf associated to the presheaf $\mathcal{F}$.*

Proof. We construct the sheaf $\mathcal{F}^+$ as follows. For any open set U, let $\mathcal{F}(U)$ be the set of functions s from U to the union $\cup_{x\in U}\mathcal{F}(x)$ of the stalks of $\mathcal{F}$ over points of U such that

(I) $s(x) \in \mathcal{F}(x)$ for each $x \in U$,

(II) for each $x \in U$, there is a neighborhood V of x, contained in U, and an element $t \in \mathcal{F}(V)$, such that for all $y \in V$, the germ $[t]_y$ of t at y is equal to $s(y)$.

Now one can verify immediately that $\mathcal{F}^+$ with the natural restriction mappings is a sheaf, that there is a natural morphism $\theta : \mathcal{F} \longrightarrow \mathcal{F}^+$, and that it has the universal property described. □

Note that for any point x, $\mathcal{F}^+(x) = \mathcal{F}(x)$. Note also that if $\mathcal{F}$ itself was a sheaf, then $\mathcal{F}^+$ is isomorphic to $\mathcal{F}$ via θ.

Definition 3.100. A *subsheaf* of a sheaf $\mathcal{F}$ is a sheaf $\mathcal{F}'$ such that for every open set $U \subset X$, $\mathcal{F}'(U)$ is a subgroup of $\mathcal{F}(U)$, and the restriction mappings of the sheaf $\mathcal{F}'$ are induced by those of $\mathcal{F}$. It follows that for any point x, the stalk $\mathcal{F}'(x)$ is a subgroup of $\mathcal{F}(x)$.

If $\varphi : \mathcal{F} \longrightarrow \mathcal{G}$ is a morphism of sheaves, we define the *kernel* of φ, denoted $\mathrm{Ker}(\varphi)$, to be the presheaf kernel of φ (which is a sheaf). Thus $\mathrm{Ker}(\varphi)$ is a subsheaf of $\mathcal{F}$. If $\mathrm{Ker}(\varphi) = 0$, the morphism φ is called *injective*. Thus φ is injective if and only if the induced mapping $\varphi_U : \mathcal{F}(U) \longrightarrow \mathcal{G}(U)$ is injective for every open set U of X.

If $\varphi : \mathcal{F} \longrightarrow \mathcal{G}$ is a morphism of sheaves, we define the *image* of φ, denoted $\mathrm{Im}(\varphi)$, to be the sheaf associated to the presheaf image of φ. By the universal property of the sheaf associated to a presheaf, there is a natural injective mapping $\mathrm{Im}(\varphi) \mapsto \mathcal{G}$. Thus $\mathrm{Im}(\varphi)$ can be identified with a subsheaf of $\mathcal{G}$. If $\mathrm{Im}(\varphi) = \mathcal{G}$, the morphism φ is said to be *surjective*. We say that a sequence

$$\cdots \to \mathcal{F}^{i-1} \xrightarrow{\varphi^{i-1}} \mathcal{F}^i \xrightarrow{\varphi^i} \mathcal{F}^{i+1} \to \cdots$$

of sheaves and morphisms is *exact* if at each stage $\mathrm{Ker}(\varphi^i) = \mathrm{Im}(\varphi^{i-1})$. Thus a sequence

$$0 \to \mathcal{F} \xrightarrow{\varphi} \mathcal{G}$$

is exact if and only if φ is injective, and

$$\mathcal{F} \xrightarrow{\varphi} \mathcal{G} \to 0$$

is exact if and only if φ is surjective.

Now let $\mathcal{F}'$ be a subsheaf of a sheaf $\mathcal{F}$. We define the *quotient sheaf* $\mathcal{F}/\mathcal{F}'$ to be the sheaf associated to the presheaf $U \mapsto \mathcal{F}(U)/\mathcal{F}'(U)$. It follows that for any point x, the stalk of $\mathcal{F}/\mathcal{F}'$ at x is the quotient $\mathcal{F}(x)/\mathcal{F}'(x)$.

If $\varphi : \mathcal{F} \longrightarrow \mathcal{G}$ is a morphism of sheaves, we define the *cokernel* of φ, denoted $\mathrm{Coker}(\varphi)$, to be the sheaf associated to the presheaf cokernel of φ.

Definition 3.101. Let $f : X \longrightarrow Y$ be a continuous mapping of topological spaces. For any $\mathcal{F}$ on X, we define the *direct image* sheaf $f_*\mathcal{F}$ on Y by

$$(f_*\mathcal{F})(V) = \mathcal{F}(f^{-1}(V))$$

for any open set $V \subset Y$. For any sheaf $\mathcal{G}$ on Y, we define the *inverse image* sheaf $f^{-1}\mathcal{G}$ on X to be the sheaf associated to the presheaf

$$U \mapsto \lim_{f(U)\subseteq V} \mathcal{G}(V),$$

where U is any open set in X, and the limit is taken over all open sets V of Y containing $f(U)$.

If Z is a topological subspace of X with the induced topology, if $i : Z \longrightarrow X$ is the inclusion mapping, and if $\mathcal{F}$ is a sheaf on X, then we call $i^{-1}\mathcal{F}$ the restriction of $\mathcal{F}$ to Z, and we often denote it by $\mathcal{F}|_Z$. Note that the stalk of $\mathcal{F}|_Z$ at any point $x \in Z$ is just $\mathcal{F}(x)$.

Definition 3.102. Let X be a variety. A *sheaf of $\mathcal{O}_X$-modules* (or simply an *$\mathcal{O}_X$-module*) is a sheaf $\mathcal{F}$ on X such that for every $U \subset X$, $\mathcal{F}(U)$ is a module over the ring $\mathcal{O}(U)$, and such that for every $V \subset U \subset X$, the mapping $r_{U,V} : \mathcal{F}(U) \longrightarrow \mathcal{F}(V)$ is a homomorphism of modules. In other words, if $s_1, s_2 \in \mathcal{F}(U)$ and $f_1, f_2 \in \mathcal{O}(U)$, then

$$r_{U,V}(f_1 s_1 + f_2 s_2) = r_{U,V}(f_1) r_{U,V}(s_1) + r_{U,V}(f_2) r_{U,V}(s_2).$$

Note that there are two different restriction mappings $r_{U,V}$ here, one for $\mathcal{F}$ and one for $\mathcal{O}$.

For example, the sheaves $\mathcal{K}_X$ and Ω^r are clearly $\mathcal{O}_X$-modules. Similarly, the direct sum

$$\mathcal{O}^r = \mathcal{O} \oplus \cdots \oplus \mathcal{O} \ (r \text{ times})$$

is an $\mathcal{O}_X$-module called a *free $\mathcal{O}_X$-module of rank r*.

Definition 3.103. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module on X. We say that $\mathcal{F}$ is *locally free* if each point in X has a neighborhood over which $\mathcal{F}$ is free. The *rank* of a locally free sheaf $\mathcal{F}$ is the integer r such that $\mathcal{F}(U) \cong \mathcal{O}(U)^r$ for all sufficiently small open sets U. A locally free sheaf of rank 1 is called an *invertible sheaf* (or sometimes a *line sheaf*).

For example, when X is smooth, the sheaf of r-forms Ω^r is a locally free sheaf. The reason that locally free sheaves of rank 1 are called "invertible" is because they are the sheaves $\mathcal{F}$ for which there exists another sheaf $\mathcal{G}$ such that $\mathcal{F} \otimes \mathcal{G} \cong \mathcal{O}$. Thus the set of invertible sheaves naturally form a group, using tensor product as the group law and $\mathcal{O}$ as the identity element.

Let D be a Cartier divisor on a variety X defined by $\{(U_i, f_i)\}_{i\in I}$. We define the sheaf $\mathcal{L}_D$ to be the subsheaf of $\mathcal{K}_X$ determined by the conditions

$$\mathcal{L}_D(U_i) = \frac{1}{f_i}\mathcal{O}(U_i),\ \ i \in I.$$

This determines $\mathcal{L}_D$, since the U_i's cover X. It is not hard to check that $\mathcal{L}_D$ is well-defined and is locally free of rank 1. It is also easy to see that up to isomorphism, $\mathcal{L}_D$ depends only on the linear equivalence class of D, and that

$$\mathcal{L}_{D+D'} = \mathcal{L}_D \otimes \mathcal{L}_{D'}.$$

Proposition 3.104. *The association* $\mathrm{CaDiv}(X) \longmapsto \mathcal{L}_D$ *defines an isomorphism from* $\mathrm{Pic}(X)$ *to the group of invertible sheaves* (*modulo isomorphism*).

Proof. See Hartshorne [90], Proposition II.6.13 or Shafarevich [239], Theorem 3, Chapter VI.1.4. □

3.6.2 Vector bundles

A *vector bundle of rank* r over a variety X is a variety E and a morphism $p : E \longrightarrow X$ with the following two properties:

(1) Each fiber $E_x = p^{-1}(x)$ is a vector space of dimension r;

(2) The fibration p is locally trivial.

A vector bundle of rank 1 is called a *line bundle*. The *trivial bundle* of rank r over X is $X \times \mathbb{A}^r \longmapsto X$.

The condition (2) means that for each point $x_0 \in X$, there is a neighborhood U of x_0 over which the fibration is trivial. In other words, if we write $E_U = p^{-1}(U)$, then there is an isomorphism $\varphi_U : U \times \mathbb{A}^r \longrightarrow E_U$ such that

$$p \circ \varphi_U(x, \xi) = x, \quad x \in U,\ \xi \in \mathbb{A}^r.$$

The mappings φ_U are called *local trivializations* of E. For each $x \in U$, setting

$$\varphi_{U,x}(\xi) = \varphi_U(x, \xi),\ \ \xi \in \mathbb{A}^r,$$

then $\varphi_{U,x} : \mathbb{A}^r \longrightarrow E_x$ is a linear isomorphism.

Let $\mathcal{B} = \{U, W, Z, \dots\}$ be an open covering of X such that for each element in $\mathcal{B}$, say U, there is a local trivialization φ_U of $U \times \mathbb{A}^r$ onto E_U. We thus obtain a mapping

$$g_{UW} : U \cap W \longrightarrow GL(r, \bar{\kappa}) \tag{3.64}$$

given by

$$g_{UW}(x) = \varphi_{U,x}^{-1} \circ \varphi_{W,x}$$

with entries in $\mathcal{O}(U \cap W)$; the mappings g_{UW} are consist of $r \times r$ matrices, called *transition matrices* for E relative to the local trivializations φ_U, φ_W. The transition matrices of E necessarily satisfy the identities:

(3) $g_{UW}g_{WU}$ is the identity in $U \cap W$,

(4) $g_{UW}g_{WZ}g_{ZU}$ is the identity in $U \cap W \cap Z$.

Conversely, if there exist an open covering $\mathcal{B} = \{U, W, Z, \dots\}$ of X and matrices g_{UW} with entries in $\mathcal{O}(U \cap W)$ satisfying the conditions (3) and (4), then there is a vector bundle (E, p, X) such that $\{g_{UW}\}$ is the system of transition matrices: it is not hard to check that E as a point set must be the union

$$\bigcup_{U \in \mathcal{B}} U \times \mathbb{A}^r$$

with points $(x, \xi) \in U \times \mathbb{A}^r$ and $(x, g_{UW}(x)\xi) \in U \times \mathbb{A}^r$ identified and with the variety structure induced by the inclusions $U \times \mathbb{A}^r \hookrightarrow E$.

As a general rule, operations on vector spaces induce operations on vector bundles. For example, if $E \longmapsto X$ is a vector bundle, we can define the *dual* of E to be the bundle E^* whose fibers are the dual vector spaces of the fibers of E; trivializations $\varphi_U : U \times \mathbb{A}^r \longrightarrow E_U$ then induce mappings

$$\varphi_U^* : U \times V^* \longrightarrow E_U^*,$$

where V^* is the dual of $V = \mathbb{A}^r$, which give $E^* = \cup E_x^*$ the structure of a variety. The construction is most easily expressed in terms of transition matrices: if $E \longmapsto X$ has transition matrices $\{g_{UW}\}$, then $E^* \longmapsto X$ is just the vector bundle given by transition matrices

$$g_{UW}^* = {}^t g_{UW}^{-1}.$$

Similarly, if $E \longmapsto X$, $E' \longmapsto X$ are vector bundles of rank r and r' with transition matrices $\{g_{UW}\}$ and $\{g'_{UW}\}$, respectively, then one can define *direct sum*, *tensor product*, and *exterior power* of bundles, respectively,

$\langle 1 \rangle$ $E \oplus E'$, given by transition matrices

$$h_{UW} = \begin{pmatrix} g_{UW} & 0 \\ 0 & g'_{UW} \end{pmatrix} : U \cap W \longrightarrow GL(r + r', \bar{\kappa}),$$

$\langle 2 \rangle$ $E \otimes E'$, given by transition matrices

$$h_{UW} = g_{UW} \otimes g'_{UW} : U \cap W \longrightarrow GL(rr', \bar{\kappa}),$$

$\langle 3 \rangle$ $\bigwedge_l E$, given by transition matrices

$$h_{UW} = \bigwedge_l g_{UW} : U \cap W \longrightarrow GL\left(\frac{r!}{l!(r-l)!}, \bar{\kappa}\right).$$

In particular, $\det(E) := \bigwedge_r E$ is a line bundle given by

$$h_{UW} = \det g_{UW} : U \cap W \longrightarrow \bar{\kappa}_*,$$

called the *determinant bundle* of E.

A morphism of vector bundles $f : E' \longrightarrow E$ which is a closed embedding of varieties is an *embedding of vector bundles*. In this case the image $f(E')$ is called a *subbundle* of E. If $F \subset E$ is a subbundle of a vector bundle E, then F is a collection $\{F_x \subset E_x\}_{x \in X}$ of subspaces of the fibers E_x of E such that $F = \cup F_x$ is a subvariety of E. The condition that $F \subset E$ is a subvariety is equivalent to saying that for every $x \in X$, there exists a neighborhood U of x in X and a trivialization

$$\varphi_U : U \times \mathbb{A}^r \longrightarrow E_U$$

such that

$$\varphi_U^{-1}|_{F_U} : F_U \longrightarrow U \times \mathbb{A}^l \subset U \times \mathbb{A}^r.$$

The transition matrices g_{UW} of E relative to these trivializations will then look like

$$g_{UW} = \begin{pmatrix} h_{UW} & k_{UW} \\ 0 & j_{UW} \end{pmatrix}.$$

The bundle F will have transition matrices h_{UW}, and the mappings j_{UW} are transition matrices for the *quotient bundle* E/F given by

$$E/F = \bigcup_{x \in X} E_x/F_x.$$

For a structure of variety, see [239].

We also define the *pullback* of a bundle $p : E \longrightarrow X$ by a morphism $f : Y \longrightarrow X$ to be the fibered product

$$f^*E = E \times_X Y = \{(y, v) \in Y \times E \mid f(y) = p(v)\}.$$

Let $p : E \longrightarrow X$ be a vector bundle of rank r. A *section* of E is a morphism $s : X \longrightarrow E$ such that $p \circ s = \mathrm{id}_X$. Similarly, a *rational section* of E is a rational mapping $s : X \longrightarrow E$ such that $p \circ s = \mathrm{id}_X$. It is easy to check from the definition of vector bundle that if s_1 and s_2 are sections of E then there exists a section $s_1 + s_2$ such that

$$(s_1 + s_2)(x) = s_1(x) + s_2(x)$$

for any point $x \in X$. The sum on the right-hand side is meaningful, since $s_1(x), s_2(x) \in E_x$, and E_x is a vector space. In a similar way the equality

$$(fs)(x) = f(x)s(x)$$

determines a multiplication of a section s by an element $f \in \mathcal{O}(X)$. The set of sections to a vector bundle clearly form a module over the ring $\mathcal{O}(X)$, which we will denote by $\Gamma(X, E)$.

A *frame* for E over $U \subset X$ is a collection $\xi_1, \ldots, \xi_r$ of sections over U such that $\{\xi_1(x), \ldots, \xi_r(x)\}$ is a basis of E_x for all $x \in U$. A frame for E over U is essentially the same thing as a trivialization of E over U: given a trivialization

$$\varphi_U : U \times \mathbb{A}^r \longrightarrow E_U,$$

the sections

$$\xi_i(x) = \varphi_U(x, e_i)$$

form a frame, where $\{e_1, \ldots, e_r\}$ is the standard basis of $\mathbb{A}^r$, and conversely given $\xi_1, \ldots, \xi_r$ a frame, we can define a trivialization φ_U by

$$\varphi_U\left(x, \sum_{i=1}^r \lambda_i e_i\right) = \sum_{i=1}^r \lambda_i \xi_i(x).$$

Given a trivialization φ_U of E over U, we can represent every section s of E over U uniquely as a $\mathcal{O}(U)$ vector-valued function $s_U = (s_{U1}, \ldots, s_{Ur})$ by writing

$$s(x) = \sum_{i=1}^r s_{Ui}(x)\varphi_U(x, e_i);$$

if φ_W is a trivialization of E over W and $s_W = (s_{W1}, \ldots, s_{Wr})$ the corresponding representation of $s|_{U\cap W}$, then

$$\sum_{i=1}^r s_{Ui}(x)\varphi_U(x, e_i) = \sum_{i=1}^r s_{Wi}(x)\varphi_W(x, e_i)$$

so

$$\varphi_{U,x}(s_U(x)) = \varphi_{W,x}(s_W(x)),$$

i.e.

$$s_U = g_{UW} s_W. \tag{3.65}$$

Thus, in terms of trivializations $\{\varphi_U\}_{U\in\mathcal{B}}$, sections of E over X correspond exactly to collections $\{s_U\}_{U\in\mathcal{B}}$ of vector-valued $\mathcal{O}(U)$ functions such that (3.65) hold for all U, W, where g_{UW} are transition matrices of E relative to $\{\varphi_U\}$.

Let $p : E \longrightarrow X$ be a vector bundle. We associate to each open set U the vector space of sections $\Gamma(U, E_U)$. Notice that $\Gamma(U, E_U)$ is an $\mathcal{O}(U)$-module. It is easy to check that the association $U \longmapsto \Gamma(U, E_U)$ defines a locally free sheaf $\mathcal{L}_E$ whose rank is equal to the rank of the vector bundle E.

Proposition 3.105. *The association $E \longmapsto \mathcal{L}_E$ is a bijection between (isomorphism classes of) vector bundles of rank r and (isomorphism classes of) locally free sheaves of rank r.*

Proof. See Hartshorne [90], Exercise II.5.18 or Shafarevich [239], Theorem 2, Chapter VI.1.3. □

Let X be a nonsingular variety. The sheaf of differential r-forms Ω^r on X is locally free. Hence by Proposition 3.105 it defines a vector bundle, denoted by Λ^r. In particular, $T^*(X) := \Lambda^1$ is called the *cotangent bundle*. Obviously,

$$\Lambda^r = \bigwedge_r T^*(X).$$

The vector bundle dual to the cotangent bundle is called the *tangent bundle*, and is denoted by $T(X)$.

Example 3.106. Consider $\mathbb{P}^n$ to be the set of lines of $\mathbb{A}^{n+1}$ through 0. Define a variety

$$E = \{(x, v) \in \mathbb{P}^n \times \mathbb{A}^{n+1} \mid v \text{ lies on the line } x\}.$$

The projection onto the first factor, $p : E \longrightarrow \mathbb{P}^n$, gives E the structure of a line bundle. Indeed, the first condition is clear, and it is easy to check that the fibration p trivializes above each standard affine open subset. Thus if we let $U_j = \mathbb{P}^n - \{X_j = 0\}$, then the trivialization $\varphi_{U_j} : U_j \times \mathbb{A}^1 \longrightarrow E_{U_j}$ is given explicitly by

$$\varphi_{U_j}(x, \lambda) = \left(x, \left(\frac{\lambda x_0}{x_j}, \frac{\lambda x_1}{x_j}, \ldots, \frac{\lambda x_n}{x_j}\right)\right).$$

3.6.3 Line bundles

Recall that for any line bundle $p : L \longrightarrow X$ on the variety X, we can find an open cover $\mathcal{B} = \{U, W, Z, \ldots\}$ of X and trivializations

$$\varphi_U : U \times \mathbb{A}^1 \longrightarrow L_U$$

of $L_U = p^{-1}(U)$. We define the *transition functions*

$$g_{UW} : U \cap W \longrightarrow \bar{\kappa}_*$$

for L relative to the trivializations $\{\varphi_U\}$ by

$$g_{UW}(x) = \varphi_{U,x}^{-1} \circ \varphi_{W,x} \in \bar{\kappa}_*.$$

The functions g_{UW} are clearly regular, nonvanishing, and satisfy

$$\begin{aligned} g_{UW} g_{WU} &= 1, \\ g_{UW} g_{WZ} g_{ZU} &= 1; \end{aligned} \tag{3.66}$$

conversely, given a collection of nonvanishing functions $\{g_{UW} \in \mathcal{O}(U \cap W)\}$ satisfying these identities, we can construct a line bundle L with transition functions $\{g_{UW}\}$

by taking the union of $U \times \mathbb{A}^1$ over all $U \in \mathcal{B}$ and identifying $\{x\} \times \mathbb{A}^1$ in $U \times \mathbb{A}^1$ and $W \times \mathbb{A}^1$ via multiplication by $g_{UW}(x)$.

Now, given L as above, for any collection of nonvanishing regular functions $f_U \in \mathcal{O}(U)$ we can define alternate trivilizations of L over $\mathcal{B}$ by

$$\varphi'_U = f_U \varphi_U;$$

transition functions g'_{UW} for L relative to $\{\varphi'_U\}$ will then given by

$$g'_{UW} = \frac{f_W}{f_U} g_{UW}. \tag{3.67}$$

On the other hand, any other trivialization of L over $\mathcal{B}$ can be obtained in this way, and so we see that collections $\{g_{UW}\}$ and $\{g'_{UW}\}$ of transition functions define the same line bundle if and only if there exist nonvanishing functions $f_U \in \mathcal{O}(U)$ satisfying (3.67).

We can give the set of line bundles on X the structure of a group, multiplication being given by tensor product and inverses by dual bundles. If L is given by data $\{g_{UW}\}$, L' by $\{g'_{UW}\}$, we have seen that

$$L \otimes L' \sim \{g_{UW} g'_{UW}\}, \quad L^* \sim \{g_{UW}^{-1}\}.$$

Based on the form of transition functions for L^*, we often use the symbol L^{-1} to express the line bundle L^*.

We now describe the basic correspondence between divisors and line bundles. Let D be a Cartier divisor on X which is represented by a set of pairs $\{(U, f_U)\}_{U \in \mathcal{B}}$, where the $\mathcal{B}$ form a open covering of X and

$$g_{UW} := \frac{f_U}{f_W} \in \mathcal{O}^*(U \cap W),$$

and in $U \cap W \cap Z$ we have

$$g_{UW} g_{WZ} g_{ZU} = \frac{f_U}{f_W} \cdot \frac{f_W}{f_Z} \cdot \frac{f_Z}{f_U} = 1.$$

The line bundle given by the transition functions $\{g_{UW} = f_U / f_W\}$ is called the *associated line bundle* of D, and written $[D]$. Obviously, a rational section of $[D]$ is given by the collection $\{f_U\}$. We check that $[D]$ is well defined: if $\{f'_U\}$ are alternate local data for D, then

$$h_U = \frac{f_U}{f'_U} \in \mathcal{O}^*(U),$$

and

$$g'_{UW} = \frac{f'_U}{f'_W} = \frac{h_W}{h_U} g_{UW}$$

for each $U, W \in \mathcal{B}$. We further observe that replacing the f_U's by ff_U does not affect the construction, where $f \in \bar{\kappa}(X)_*$, so the isomorphism class of the resulting line bundle depends only on the linear equivalence class of D. Also it is easy to show that the line bundle $[D]$ associated to a divisor D on X is trivial if and only if D is principal.

Conversely, suppose that L is a line bundle defined in an open cover $\mathcal{B} = \{U, W, Z, \dots\}$ of X by transition functions $\{g_{UW}\}$ for L relative to the trivializations $\{\varphi_U\}$, with $g_{UW} \in \mathcal{O}(U \cap W)$. It follows from the gluing conditions (3.66) that $g_{WU} = g_{UW}^{-1}$ and

$$g_{UW} = g_{UZ} g_{WZ}^{-1} \tag{3.68}$$

over $U \cap W \cap Z$. The inclusion $\mathcal{O}(U \cap W) \hookrightarrow \bar{\kappa}(X)$ allows us to consider the g_{UW} as elements of $\bar{\kappa}(X)$, and (3.68) holds for these in the same way. Fix some subscript Z, set $s_U = g_{UZ}$. Since

$$s_U s_W^{-1} = g_{UW}, \tag{3.69}$$

the system $\{(U, s_U)\}_{U \in \mathcal{B}}$ define a certain divisor D with $[D] = L$. Let ξ_U be the frame of L over U defined by

$$\xi_U(x) = \varphi_U(x, 1), \ \ x \in U.$$

Then we can prove easily the relation

$$\xi_W = g_{UW} \xi_U$$

over $U \cap W$. Since

$$s_U \xi_U = s_W g_{UW} g_{UW}^{-1} \xi_W = s_W \xi_W,$$

the collection $\{s_U\}$ just defines a rational section s. Thus we also denote this divisor by $(s) = D$.

Proposition 3.107. *The association $D \longmapsto [D]$ induces a functorial isomorphism between the group of Cartier divisor classes and the group of isomorphism classes of line bundles on X. More precisely,*

$$[D + D'] = [D] \otimes [D'], \quad [-D] = [D]^*.$$

Further, $[f^* D] = f^*[D]$ for any morphism f of varieties.

Let L be a line bundle defined in an open cover $\mathcal{B} = \{U, W, Z, \dots\}$ of X by transition functions $\{g_{UW}\}$. An absolute value $|\cdot|_v$ on $\bar{\kappa}$ induces a *metric* v on L, which amounts to the giving of a norm on each fiber, varying as smoothly as the conditions prescribe (continuously, C^∞, real analytic, and so on). Suppose given for each $U \in \mathcal{B}$ a function

$$\rho_U : U \longrightarrow \mathbb{R}^+$$

such that on $U \cap W$ we have

$$\rho_U = |g_{UW}|_v^2 \rho_W.$$

Then we say that the family of triples $\{(U, g_{UW}, \rho_U)\}$ represents the metric. We could also write a representative family as $\{(U, \varphi_U, \rho_U)\}$ using the trivializations φ_U instead of the transition functions g_{UW}. A line bundle with a metric v will be denoted by a pair (L, v), and will be called a *metrized line bundle*.

Here we introduce a construction of metrics on L. By Proposition 3.53, there are very ample line bundles E, H on X such that $L \cong E \otimes H^{-1}$. Now choose generating global sections $s_0, \ldots, s_p$ of E and $t_0, \ldots, t_q$ of H. Then there is a unique metric on L given by

$$\rho_U(x) = \max_i \min_j \left| \frac{s_{iU}(x)}{t_{jU}(x)} \right|_v^2, \quad x \in U.$$

If $s = \{s_U\}_{U \in \mathcal{B}}$ is a section of L, then we define

$$|s(x)|_v^2 = \frac{|s_U(x)|_v^2}{\rho_U(x)}, \quad x \in U.$$

The value on the right-hand side is independent of the choice of U, as one sees at once from the transformation law. The metric is said to be *locally bounded* if $\log |s|_v$ is locally bounded for every open subset U of X and every nowhere vanishing section $s \in \Gamma(U, L)$.

For the case $X = \mathbb{P}^n$, let H be the line bundle associated to a hyperplane. It is easy to see that H is the dual of the line bundle defined in Example 3.106. The global sections of H can be identified with linear forms

$$\Gamma\left(\mathbb{P}^n, H\right) = \bar{\kappa} X_0 \oplus \cdots \oplus \bar{\kappa} X_n.$$

We let H^d denote the line bundle obtained by tensoring H with itself d times. The global sections of H^d are the homogeneous polynomials of degree d,

$$\Gamma\left(\mathbb{P}^n, H^d\right) = \bigoplus_{i_0 + \cdots + i_n = d} \bar{\kappa} X_0^{i_0} \cdots X_n^{i_n}.$$

3.6.4 Intersection multiplicity

Let A be a graded ring. If M is a module over A, then a sequence of submodules

$$0 = M^0 \subset M^1 \subset \cdots \subset M^r = M$$

is also called a finite *filtration*, and we call r the *length* of the filtration. A module M is said to be *simple* if it does not contain any submodule other than 0 and M itself, and if $M \neq 0$. A filtration is said to be *simple* if each M_i / M_{i-1} is simple. A module M is said to be of *finite length* if it is 0, or if it admits a simple finite filtration. The length of such a simple finite filtration is uniquely determined, called the *length of the module*, and denoted by $\operatorname{length}(M)$, or $\operatorname{length}_A(M)$ to stress the role of the ring A.

A *graded A-module* is an A-module M, together with a decomposition

$$M = \sum_{r \in \mathbb{Z}} M_r,$$

such that $A_r \cdot M_s \subseteq M_{r+s}$. For any graded A-module M, and for $l \in \mathbb{Z}$, we define the *twisted module* $M(l)$ by shifting l places to the left, i.e., $M(l)_r = M_{r+l}$. If M is a graded A-module, we define the *annihilator* of M,

$$\mathrm{Ann}(M) = \{a \in A \mid a \cdot M = 0\}.$$

This is a homogeneous ideal in A.

Proposition 3.108. *Let M be a finitely generated graded module over a Noetherian graded ring A. Then there exists a filtration*

$$0 = M^0 \subset M^1 \subset \cdots \subset M^r = M$$

by graded submodules, such that for each i,

$$M^i/M^{i-1} \cong (A/\mathfrak{p}_i)(l_i),$$

where $\mathfrak{p}_i$ is a homogeneous prime ideal of A, and $l_i \in \mathbb{Z}$. The filtration is not unique, but for any such filtration we do have:

($\boldsymbol{\mu}$) *if $\mathfrak{p}$ is a homogeneous prime ideal of A, then for some i,*

$$\mathrm{Ann}(M) \subseteq \mathfrak{p} \Longleftrightarrow \mathfrak{p}_i \subseteq \mathfrak{p}.$$

In particular, the minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ are just the minimal primes of M, i.e., the primes which are minimal containing $\mathrm{Ann}(M)$;

($\boldsymbol{\nu}$) *for each minimal prime of M, the number of times which $\mathfrak{p}$ occurs in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ is equal to the length of $M_\mathfrak{p}$ over the local ring $A_\mathfrak{p}$ (and hence is independent of the filtration).*

Proof. For the existence of the filtration, we consider the set of graded submodules of M which admit such a filtration. Clearly, the zero module does, so the set is nonempty. Since M is a Noetherian module, so there is a maximal submodule $M' \subseteq M$. Now consider $M'' = M/M'$. If $M'' = 0$, we are done. If not, we consider the set of ideals

$$\mathcal{I} = \{I_m = \mathrm{Ann}(m) \mid m \in M'' - \{0\} \text{ is a homogeneous element }\}.$$

Each I_m is a homogeneous ideal, and $I_m \neq A$. Since A is a Noetherian ring, we can find an element $m \in M'' - \{0\}$ such that I_m is a maximal element of the set $\mathcal{I}$. We claim that I_m is a prime ideal. Let $a, b \in A$. Suppose that $ab \in I_m$, but $b \notin I_m$. We will show $a \in I_m$. By splitting into homogeneous components, we may assume that

a, b are homogeneous elements. Now consider the element $bm \in M''$. Since $b \notin I_m$, then $bm \neq 0$. We have $I_m \subseteq I_{bm}$, so by maximality of I_m, one has $I_m = I_{bm}$. But $ab \in I_m$, so $abm = 0$, so $a \in I_{bm} = I_m$ as required. Thus I_m is a homogeneous prime ideal of A, denoted $\mathfrak{p}$. Let m have degree l. Then the module $N \subseteq M''$ generated by m is isomorphic to $(A/\mathfrak{p})(-l)$. Let $N' \subseteq M$ be the inverse image of N in M. Then $M' \subseteq N'$, and $N'/M' \cong (A/\mathfrak{p})(-l)$. So N' also has a filtration of the type required. This contradicts the maximality of M'. We conclude that M' was equal to M, which proves the existence of the filtration.

Now suppose given such a filtration of M. Then it is clear that for some i,

$$\operatorname{Ann}(M) \subseteq \mathfrak{p} \Longleftrightarrow \operatorname{Ann}(M^i/M^{i-1}) \subseteq \mathfrak{p}.$$

But $\operatorname{Ann}((A/\mathfrak{p}_i)(l)) = \mathfrak{p}_i$ so this proves (μ).

To prove (ν) we localize at a minimal prime $\mathfrak{p}$. Since $\mathfrak{p}$ is minimal in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, after localization, we will have $M^i_{\mathfrak{p}} = M^{i-1}_{\mathfrak{p}}$ except in the cases where $\mathfrak{p}_i = \mathfrak{p}$, and in those cases

$$M^i_{\mathfrak{p}}/M^{i-1}_{\mathfrak{p}} \cong (A/\mathfrak{p})_{\mathfrak{p}},$$

the quotient field of $A/\mathfrak{p}$. This shows that $M_{\mathfrak{p}}$ is an $A_{\mathfrak{p}}$-module of finite length equal to the number of times $\mathfrak{p}$ occurs in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. □

Definition 3.109. If $\mathfrak{p}$ is a minimal prime of a graded A-module M, we define the *multiplicity* of M at $\mathfrak{p}$ to be the length of $M_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$, denoted $\operatorname{length}(M_{\mathfrak{p}})$.

Theorem 3.110 (Hilbert–Serre). *Let M be a finitely generated graded $\kappa[x_0, \ldots, x_n]$-module. Then there is a unique polynomial $P_M(z) \in \mathbb{Q}[z]$ such that $P_M(l) = \dim_\kappa M_l$ for all $l \gg 0$. Furthermore, $\deg P_M = \dim Z(\operatorname{Ann}(M))$, where Z denotes the zero set in $\mathbb{P}^n$ of a homogeneous ideal.*

The polynomial P_M of the theorem is the *Hilbert polynomial* of M. If $Y \subseteq \mathbb{P}^n$ is an algebraic set of dimension r, we define the *homogeneous ideal* of Y in $\kappa[x_0, \ldots, x_n]$, denoted $I(Y)$, to be the ideal generated by

$$\{f \in \kappa[x_0, \ldots, x_n] \mid f \text{ is homogeneous and } f(x) = 0 \text{ for all } x \in Y\},$$

and define the *homogeneous coordinate ring* of Y to be $\kappa[x_0, \ldots, x_n]/I(Y)$. Further, we define the *Hilbert polynomial* of Y to be the Hilbert polynomial P_Y of its homogeneous coordinate ring. By the theorem, P_Y is a polynomial of degree r. We define the *degree* of Y to be $r!$ times the leading coefficient of P_Y.

Proposition 3.111. **(ξ1)** *If $Y \subseteq \mathbb{P}^n$, $Y \neq \emptyset$, then the degree of Y is a positive integer.*

(ξ2) *Let $Y = Y_1 \cup Y_2$, where Y_1 and Y_2 have the same dimension r, and where $\dim(Y_1 \cap Y_2) < r$. Then $\deg(Y) = \deg(Y_1) + \deg(Y_2)$.*

(ξ3) $\deg(\mathbb{P}^n) = 1$.

(ξ4) *If $H \subseteq \mathbb{P}^n$ is a hypersurface whose ideal is generated by a homogeneous polynomial of degree d, then* $\deg(H) = d$.

Let $Y \subseteq \mathbb{P}^n$ be a projective variety of dimension r. Let H be a hypersurface not containing Y. Then

$$Y \cap H = Z_1 \cup \cdots \cup Z_s,$$

where Z_j are varieties of dimension $r-1$. Let $\mathfrak{p}_j$ be the homogeneous prime ideal of Z_j. We define the *intersection multiplicity* of Y and H along Z_j to be

$$i_{Y,H}(Z_j) = \operatorname{length}(\kappa[x_0, \ldots, x_n]/(I(Y) + I(H)))_{\mathfrak{p}_j}.$$

Here $I(Y), I(H)$ are the homogeneous ideals of Y and H. The module

$$M = \kappa[x_0, \ldots, x_n]/(I(Y) + I(H))$$

has annihilator $I(Y) + I(H)$, and $Z(I(Y) + I(H)) = Y \cap H$, so $\mathfrak{p}_j$ is a minimal prime of M.

Theorem 3.112. *Let Y be a variety of dimension ≥ 1 in $\mathbb{P}^n$, and let H be a hypersurface not containing Y. Let $Z_1, \ldots, Z_s$ be the irreducible components of $Y \cap H$. Then*

$$\sum_{j=1}^{s} i_{Y,H}(Z_j) \deg(Z_j) = \deg(Y) \deg(H).$$

3.7 Schemes

3.7.1 Schemes

We will construct the space $\operatorname{Spec} A$ associated to a (commutative) ring A. As a set, we define $\operatorname{Spec} A$ to be the set of all prime ideals of A. If $\mathfrak{a}$ is any ideal of A, we define the subset $V(\mathfrak{a}) \subseteq \operatorname{Spec} A$ to be the set of all prime ideals which contain $\mathfrak{a}$. The following properties are basic:

(a) If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of A, then $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

(b) If $\{\mathfrak{a}_i\}$ is any set of ideals of A, then $V(\sum \mathfrak{a}_i) = \cap V(\mathfrak{a}_i)$.

(c) If $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals, $V(\mathfrak{a}) \subseteq V(\mathfrak{b})$ if and only if $\sqrt{\mathfrak{a}} \supseteq \sqrt{\mathfrak{b}}$, where the *radical* of $\mathfrak{a}$ is defined as

$$\sqrt{\mathfrak{a}} = \{f \in A \mid f^r \in \mathfrak{a} \text{ for some } r > 0\}.$$

Now we define a topology on $\operatorname{Spec} A$ by taking the subsets of the form $V(\mathfrak{a})$ to be the closed subsets. Note that

$$V(A) = \emptyset; \quad V((0)) = \operatorname{Spec} A;$$

and the properties (a), (b), (c) shows that finite unions and arbitrary intersections of sets of the form $V(\mathfrak{a})$ are again of that form. Hence they do form the set of closed sets for a topology on $\operatorname{Spec} A$. For any element $f \in A$, we denote by $D(f)$ the open complement of $V((f))$. Note that open sets of the form $D(f)$ form a base for the topology of $\operatorname{Spec} A$. Indeed, if $V(\mathfrak{a})$ is a closed set, and $\mathfrak{p} \notin V(\mathfrak{a})$, then $\mathfrak{a} \nsubseteq \mathfrak{p}$, so there is an $f \in \mathfrak{a}$, $f \notin \mathfrak{p}$. Then $\mathfrak{p} \in D(f)$ and $D(f) \cap V(\mathfrak{a}) = \emptyset$. By using this fact, it is easy to show that $\operatorname{Spec} A$ is compact.

Note that if $\mathfrak{p}$ is a prime ideal of A, which determines a point in $\operatorname{Spec} A$, then its closure in $\operatorname{Spec} A$ is $V(\mathfrak{p})$, that is, it consists of all prime ideals $\mathfrak{p}'$ with $\mathfrak{p} \subset \mathfrak{p}'$. In particular, a prime ideal $\mathfrak{p} \subset A$ is a *closed point* of $\operatorname{Spec} A$ if and only if $\mathfrak{p}$ is a maximal ideal. If A does not have zero divisors, then (0) is prime, and is contained in every prime ideal. Thus its closure is the whole space; (0) is an everywhere dense point.

If a topological space has non-closed points, then there is a certain hierarchy among its points, that we formulate in the following definition: x is a *specialization* of y if x is contained in the closure of y. An everywhere dense point is called a *generic point* of a space.

When does $\operatorname{Spec} A$ have an everywhere dense point? Note that the intersection of all prime ideals $\mathfrak{p} \subset A$ consists of all nilpotent elements of A, that is, it is the nilradical. If this is a prime ideal, then it defines a point of $\operatorname{Spec} A$; but any prime ideal must contain all nilpotent elements, that is, must contain the nilradical. Hence $\operatorname{Spec} A$ has a generic point if and only if its nilradical is prime. The generic point is unique, and is the point defined by the nilradical.

Next we will define a sheaf of rings $\mathcal{O}$ on $\operatorname{Spec} A$. For each prime ideal $\mathfrak{p} \subset A$, let $A_{\mathfrak{p}}$ be the localization of A at $\mathfrak{p}$. For an open set $U \subset \operatorname{Spec} A$, we define $\mathcal{O}(U)$ to be the set of functions

$$s : U \longrightarrow \bigcup_{\mathfrak{p} \in U} A_{\mathfrak{p}}$$

such that $s(\mathfrak{p}) \in A_{\mathfrak{p}}$ for each $\mathfrak{p}$, and such that s is locally a quotient of elements of A: to be precise, we require that for each $\mathfrak{p} \in U$, there are a neighborhood V of $\mathfrak{p}$, contained in U, and elements $a, f \in A$, such that for each $\mathfrak{q} \in V$, $f \notin \mathfrak{q}$, and $s(\mathfrak{q}) = a/f$ in $A_{\mathfrak{q}}$.

Now it is clear that sums and products of such functions are again such, and that the element 1 which gives 1 in each $A_{\mathfrak{p}}$ is an identity. Thus $\mathcal{O}(U)$ is a commutative ring with identity. If $U \subset V$ are two open sets, the natural restriction mapping $\mathcal{O}(V) \longrightarrow \mathcal{O}(U)$ is a homomorphism of rings. It is then clear that $\mathcal{O}$ is a presheaf. Finally, it is clear from the local nature of the definition that $\mathcal{O}$ is a sheaf.

Definition 3.113. Let A be a ring. The *spectrum* of A is the pair consisting of the topological space $\operatorname{Spec} A$ together with the sheaf of rings $\mathcal{O}$ defined above.

Proposition 3.114. *Let A be a ring, and $(\operatorname{Spec} A, \mathcal{O})$ its spectrum.*

(A) *For any $\mathfrak{p} \in \operatorname{Spec} A$, the stalk $\mathcal{O}_{\mathfrak{p}}$ of the sheaf $\mathcal{O}$ is isomorphic to the local ring $A_{\mathfrak{p}}$.*

(B) *For any element $f \in A$, the ring $\mathcal{O}(D(f))$ is isomorphic to the localized ring A_f.*

(C) *In particular, $\mathcal{O}(\operatorname{Spec} A) \cong A$.*

Proof. See Hartshorne [90], Chap. II, Proposition 2.2. □

A *ringed space* is a pair $(X, \mathcal{O}_X)$ consisting of a topological space X and a sheaf of rings $\mathcal{O}_X$ on X. The ringed space $(X, \mathcal{O}_X)$ is a *locally ringed space* if for each point $x \in X$, the stalk $\mathcal{O}_X(x)$ is a local ring. The sheaf $\mathcal{O}_X$ is called the *structure sheaf* of the ringed space.

A *morphism* of ringed spaces from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is a pair $(f, f^\#)$ of a continuous mapping $f : X \longrightarrow Y$ and a mapping $f^\# : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ of sheaves of rings on Y, in which the latter $f^\#$ induces a homomorphism of rings

$$f^\#_V : \mathcal{O}_Y(V) \longrightarrow (f_*\mathcal{O}_X)(V) = \mathcal{O}_X(f^{-1}(V))$$

for every open set V in Y. Given a point $x \in X$, as V ranges over all open neighborhoods of $f(x)$, $f^{-1}(V)$ ranges over a subset of the neighborhoods of x. Taking direct limits

$$\varinjlim_{V \to f(x)} \mathcal{O}_Y(V) = \mathcal{O}_Y(f(x)), \quad \varinjlim_{V \to f(x)} \mathcal{O}_X(f^{-1}(V)) = \mathcal{O}_X(x),$$

thus we obtain an induced homomorphism

$$f^\#_x : \mathcal{O}_Y(f(x)) \longrightarrow \mathcal{O}_X(x).$$

A *morphism* of locally ringed spaces is a morphism $(f, f^\#)$ such that for each point $x \in X$, the induced mapping of local rings $f^\#_x : \mathcal{O}_Y(f(x)) \longrightarrow \mathcal{O}_X(x)$ is a local homomorphism of local rings. Recall that if A and B are local rings with maximal ideals $\mathbf{m}_A$ and $\mathbf{m}_B$ respectively, a homomorphism $\varphi : A \longrightarrow B$ is called a *local homomorphism* if $\varphi^{-1}(\mathbf{m}_B) = \mathbf{m}_A$.

Examples of locally ringed spaces include algebraic varieties with their sheaves of regular functions and differential (respectively analytic) varieties with their sheaves of differential (respectively analytic) functions.

Proposition 3.115. (D) *If A is a ring, then $(\operatorname{Spec} A, \mathcal{O})$ is a locally ringed space.*

(E) *If $\varphi : A \longrightarrow B$ is a homomorphism of rings, then φ induces a natural morphism of locally ringed spaces*

$$(f, f^\#) : (\operatorname{Spec} B, \mathcal{O}_{\operatorname{Spec} B}) \longrightarrow (\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A}).$$

(F) *If A and B are rings, then any morphism of locally ringed spaces from $\operatorname{Spec} B$ to $\operatorname{Spec} A$ is induced by a homomorphism of rings $\varphi : A \longrightarrow B$ as in* (E).

Proof. (D) This follows from Proposition 3.114, (A).

(E) Given a homomorphism $\varphi : A \longrightarrow B$, we define a mapping $f : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ by $f(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$ for any $\mathfrak{p} \in \operatorname{Spec} B$. If $\mathfrak{a}$ is an ideal of A, then it is immediate that $f^{-1}(V(\mathfrak{a})) = V(\varphi(\mathfrak{a}))$, so f is continuous. For each $\mathfrak{p} \in \operatorname{Spec} B$, we can localize φ to obtain a local homomorphism of local rings $\varphi_{\mathfrak{p}} : A_{\varphi^{-1}(\mathfrak{p})} \longrightarrow B_{\mathfrak{p}}$. Now for any open set $V \subseteq \operatorname{Spec} A$, we obtain a homomorphism of rings

$$f_V^{\#} : \mathcal{O}_{\operatorname{Spec} A}(V) \longrightarrow \mathcal{O}_{\operatorname{Spec} B}(f^{-1}(V))$$

by the definition of $\mathcal{O}$, composing with the mappings f and $\varphi_{\mathfrak{p}}$. This gives the morphism of sheaves

$$f^{\#} : \mathcal{O}_{\operatorname{Spec} A} \longrightarrow f_* \mathcal{O}_{\operatorname{Spec} B}.$$

The induced mappings $f^{\#}$ on the stalks are just the local homomorphisms $\varphi_{\mathfrak{p}}$, so $(f, f^{\#})$ is a morphism of locally ringed spaces.

(F) Conversely, suppose given a morphism of locally ringed spaces $(f, f^{\#})$ from $\operatorname{Spec} B$ to $\operatorname{Spec} A$. Taking global sections, $f^{\#}$ induces a homomorphism of rings

$$\varphi : \mathcal{O}(\operatorname{Spec} A) \longrightarrow \mathcal{O}(\operatorname{Spec} B).$$

By Proposition 3.114, (C), these rings are A and B, respectively, so we have a homomorphism $\varphi : A \longrightarrow B$. For any $\mathfrak{p} \in \operatorname{Spec} B$, we have an induced local homomorphism on the stalks,

$$f_{\mathfrak{p}}^{\#} : \mathcal{O}_{\operatorname{Spec} A}(f(\mathfrak{p})) \longrightarrow \mathcal{O}_{\operatorname{Spec} B}(\mathfrak{p}),$$

or $f_{\mathfrak{p}}^{\#} : A_{f(\mathfrak{p})} \longrightarrow B_{\mathfrak{p}}$, which must be compatible with the mapping φ on global sections and the localization homomorphisms. In other words, we have a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow & & \downarrow \\ A_{f(\mathfrak{p})} & \xrightarrow{f_{\mathfrak{p}}^{\#}} & B_{\mathfrak{p}}. \end{array}$$

Since $f^{\#}$ is a local homomorphism, it follows that $\varphi^{-1}(\mathfrak{p}) = f(\mathfrak{p})$, which shows that f coincides with the mapping $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ induced by φ. Now it is immediate that $f^{\#}$ also is induced by φ, so that the morphism $(f, f^{\#})$ of locally ringed spaces does indeed come from the homomorphism of rings φ. □

Definition 3.116. An *affine scheme* is a locally ringed space $(X, \mathcal{O}_X)$ which is isomorphic to the spectrum $(\operatorname{Spec} A, \mathcal{O})$ of some ring A. A *scheme* is a locally ringed spaces $(X, \mathcal{O}_X)$ in which every point has an open neighborhood U such that the topological space U, together with the restricted sheaf $\mathcal{O}_X|_U$, is an affine scheme. We call X the *underlying topological space* of the scheme $(X, \mathcal{O}_X)$, and $\mathcal{O}_X$ its structure

sheaf. By abuse of notation we will often write simply X for the scheme $(X, \mathcal{O}_X)$. A *morphism* of schemes is a morphism as locally ringed spaces. An *isomorphism* is a morphism with a two-sided inverse.

If X is a topological space, and Z an irreducible closed subset of X, a *generic point* for Z is a point η such that $Z = \overline{\{\eta\}}$. Every (nonempty) irreducible closed subset in a scheme has a unique generic point. A scheme of fundamental importance is the affine scheme $\operatorname{Spec}\mathbb{Z}$. It has one generic point, corresponding to the ideal (0), and all of its other points are closed and correspond to prime numbers,

$$\operatorname{Spec}\mathbb{Z} = \{(0), 2\mathbb{Z}, 3\mathbb{Z}, \dots, p\mathbb{Z}, \dots\}.$$

The structure sheaf of $\operatorname{Spec}\mathbb{Z}$ is easy to describe

$$\mathcal{O}(D(p_1, \dots, p_k)) = \mathbb{Z}\left(\frac{1}{p_1}, \dots, \frac{1}{p_k}\right).$$

The function field of $\operatorname{Spec}\mathbb{Z}$ (i.e., the stalk at (0)) is $\mathbb{Q}$.

Associated to a ring A, we have a scheme

$$\mathbb{A}^n_A = \operatorname{Spec} A[x_1, \dots, x_n].$$

In particular, if κ is a field, $\mathbb{A}^1_\kappa$ has a generic point η, corresponding to the zero ideal, whose closure is the whole space. The other points, which correspond to the maximal ideals in $\kappa[x]$, are all closed points. There are in one-to-one correspondence with the nonconstant monic irreducible polynomials in x. Therefore, if κ is algebraically closed, the closed points of $\mathbb{A}^1_\kappa$ are in one-to-one correspondence with elements of κ.

A *graded ring* is a ring S, together with a decomposition

$$S = \bigoplus_{r \geq 0} S_r$$

of S into a direct sum of Abelian groups S_r, such that for any $r, s \geq 0$, $S_r \cdot S_s \subseteq S_{r+s}$. An element of S_r is called a *homogeneous element of degree* r. Thus any element of S can be written uniquely as a (finite) sum of homogeneous elements. An ideal $\mathfrak{a} \subseteq S$ is a *homogeneous ideal* if

$$\mathfrak{a} = \bigoplus_{r \geq 0} \mathfrak{a} \cap S_r.$$

An ideal is homogeneous if and only if it can be generated by homogeneous elements. The sum, product, intersection, and radical of homogeneous ideals are homogeneous. To test whether a homogeneous ideal $\mathfrak{a}$ is prime, it is sufficient to show for any two homogeneous elements f, g, that $fg \in \mathfrak{a}$ implies $f \in \mathfrak{a}$ or $g \in \mathfrak{a}$ (see Matsumura [173], § 10 or Zariski-Samuel [307], Vol. 2, Ch. VII, § 2).

Let S be a graded ring. We denote by S_+ the ideal

$$S_+ = \bigoplus_{r > 0} S_r.$$

We define the set $\operatorname{Proj} S$ to be the set of all homogeneous prime ideals $\mathfrak{p}$, who do not contain all of S_+. If $\mathfrak{a}$ is a homogeneous ideal of S, we define the subset

$$V(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Proj} S \mid \mathfrak{a} \subseteq \mathfrak{p}\}.$$

Lemma 3.117. **(α)** *If $\mathfrak{a}$ and $\mathfrak{b}$ are homogeneous ideals in S, then $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.*

(β) *If $\{\mathfrak{a}_i\}$ is any set of homogeneous ideals of A, then $V(\sum \mathfrak{a}_i) = \cap V(\mathfrak{a}_i)$.*

Proof. The proofs are the same as (a) and (b), taking into account the fact that a homogeneous ideal $\mathfrak{p}$ is prime if and only if for any two homogeneous elements $a, b \in S$, $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. □

Because of the lemma we can define a topology on $\operatorname{Proj} S$ by taking the closed subsets to be the subsets of the form $V(\mathfrak{a})$. Next we define a sheaf of ring $\mathcal{O}$ on $\operatorname{Proj} S$. For each $\mathfrak{p} \in \operatorname{Proj} S$, we consider the ring $S_{(\mathfrak{p})}$ of elements of degree zero in the localized ring $T^{-1}S$, where T is the multiplicative system consisting of all homogeneous elements of S which are not in $\mathfrak{p}$. For any open subset $U \subseteq \operatorname{Proj} S$, we define $\mathcal{O}(U)$ to be the set of functions $s : U \longrightarrow \coprod S_{(\mathfrak{p})}$ such that for each $\mathfrak{p} \in U$, $s(\mathfrak{p}) \in S_{(\mathfrak{p})}$, and such that s is locally a quotient of elements of S: for each $\mathfrak{p} \in U$, there exists a neighborhood V of $\mathfrak{p}$ in U, and homogeneous elements a, f in S, of the same degree, such that for all $\mathfrak{q} \in V$, $f \notin \mathfrak{q}$, and $s(\mathfrak{q}) = a/f$ in $S_{(\mathfrak{q})}$. Now it is clear that $\mathcal{O}$ is a presheaf of rings, with the natural restrictions, and it is also clear from the local nature of the definition that $\mathcal{O}$ is a sheaf. Thus a ringed space $(\operatorname{Proj} S, \mathcal{O})$ follows.

Proposition 3.118. *Let S be a graded ring.*

(γ) *For any $\mathfrak{p} \in \operatorname{Proj} S$, the stalk $\mathcal{O}(\mathfrak{p})$ is isomorphic to the local ring $S_{(\mathfrak{p})}$.*

(δ) *For any homogeneous $f \in S_+$, let*

$$D_+(f) = \{\mathfrak{p} \in \operatorname{Proj} S \mid f \notin \mathfrak{p}\}.$$

Then $D_+(f)$ is open in $\operatorname{Proj} S$. Furthermore, these open sets cover $\operatorname{Proj} S$, and for each such open set, we have an isomorphism of locally ringed spaces

$$\left(D_+(f), \mathcal{O}|_{D_+(f)}\right) \cong \operatorname{Spec} S_{(f)},$$

where $S_{(f)}$ is the subring of elements of degree 0 in the localized ring S_f.

(ϵ) *$\operatorname{Proj} S$ is a scheme.*

Proof. Note that (γ) says that $\operatorname{Proj} S$ is a locally ringed space, and (δ) tells us it is covered by open affine schemes, so (ϵ) is a consequence of (γ) and (δ). See Hartshorne [90], Chap. II, Proposition 2.5. □

If A is a ring, we make the polynomial ring $A[x_0, \ldots, x_n]$ into a graded ring S by taking S_d to be the set of all linear combinations of monomials of total weight d in $x_0, \ldots, x_n$. We define *projective n-space* over A to be the scheme

$$\mathbb{P}^n_A = \operatorname{Proj} A[x_0, \ldots, x_n]. \tag{3.70}$$

In particular, if A is an algebraically closed field κ, then $\mathbb{P}^n_\kappa$ is a scheme whose subspace of closed points is naturally homeomorphic to the variety called projective n-space.

A scheme X is called a *scheme over* a scheme S, or *S-scheme* if it is equipped with a morphism $X \longmapsto S$. In this context, if $f : X \longrightarrow S$ and $g : Y \longrightarrow S$ are two S-schemes, then an *S-morphism* is a morphism $\phi : X \longrightarrow Y$ satisfying $f = g \circ \phi$. This generalizes the notion of varieties and morphisms defined over κ, which corresponds to the case $S = \operatorname{Spec} \kappa$. We also note that since every ring A has a (unique) canonical homomorphism $\mathbb{Z} \longrightarrow A$, all schemes have a canonical morphism to $\operatorname{Spec} \mathbb{Z}$, so every scheme is a scheme over $\operatorname{Spec} \mathbb{Z}$. We denote by $\mathfrak{Sch}(S)$ the category of schemes over S. If A is a ring, then by abuse of notation we write $\mathfrak{Sch}(A)$ for the category of schemes over $\operatorname{Spec} A$.

Proposition 3.119. *Let κ be an algebraically closed field. There is a natural fully faithful functor $t : \mathfrak{Var}(\kappa) \longrightarrow \mathfrak{Sch}(\kappa)$ from the category of varieties over κ to schemes over κ. For any variety X, its topological space is homeomorphic to the set of closed points of $t(X)$, and its sheaf of regular functions is obtained by restricting the structure sheaf of $t(X)$ via this homeomorphism.*

Proof. To begin with, let X be any topological space, and let $t(X)$ be the set of (nonempty) irreducible closed subsets of X. If Y is a closed subset of X, then $t(Y) \subseteq t(X)$. Furthermore,

$$t(Y_1 \cup Y_2) = t(Y_1) \cup t(Y_2), \quad t(\cap Y_i) = \cap t(Y_i).$$

So we can define a topology on $t(X)$ by taking as closed sets the subsets of the form $t(Y)$, where Y is a closed subset of X. If $f : X_1 \longrightarrow X_2$ is a continuous mapping, then we obtain a mapping $t(f) : t(X_1) \longrightarrow t(X_2)$ by sending an irreducible closed subset to the closure of its image. Thus t is a functor on topological spaces. Furthermore, one can define a continuous mapping $\alpha : X \longrightarrow t(X)$ by $\alpha(P) = \overline{\{P\}}$. Note that α induces a bijection between the set of open subsets of X and the set of open subsets of $t(X)$.

Now let κ be an algebraically closed field. Let X be a variety over κ, and let $\mathcal{O}_X$ be its sheaf of regular functions (Example 3.89). We will show that $(t(X), \alpha_* \mathcal{O}_X)$ is a scheme over κ. Since any variety can be covered by open affine subvarieties, it will be sufficient to show that if X is affine, then $(t(X), \alpha_* \mathcal{O}_X)$ is a scheme. So let X be an affine variety with affine coordinate ring $A = \kappa[X]$. We define a morphism of locally ringed spaces

$$\beta : (X, \mathcal{O}_X) \longrightarrow \mathcal{X} = \operatorname{Spec} A$$

as follows. For each point $P \in X$, let $\beta(P) = \mathfrak{m}_P$, the ideal of A consisting of all regular functions which vanish at P. Then by Theorem 3.30, β is a bijection of X onto the set of closed points of $\mathcal{X}$. It is easy to see that β is a homeomorphism onto its image. Now for any open set $U \subseteq \mathcal{X}$, we will define a homomorphism of rings

$$\mathcal{O}_{\mathcal{X}}(U) \longmapsto \beta_* \mathcal{O}_X(U) = \mathcal{O}_X(\beta^{-1}(U)).$$

Given a section $s \in \mathcal{O}_{\mathcal{X}}(U)$, and given a point $P \in \beta^{-1}(U)$, we define $s(P)$ by taking the image of s in the stalk $\mathcal{O}_{\mathcal{X}}(\beta(P))$, which is isomorphic to the local ring $A_{\mathfrak{m}_P}$, and then passing to the quotient ring $A_{\mathfrak{m}_P}/\mathfrak{m}_P$ which is isomorphic to the field κ. Thus s gives a function from $\beta^{-1}(U)$ to κ. It is easy to see that this is a regular function, and that this mapping gives an isomorphism $\mathcal{O}_{\mathcal{X}}(U) \cong \mathcal{O}_X(\beta^{-1}(U))$. Finally, since the prime ideals of A are in $1-1$ correspondence with the irreducible closed subsets of X, these remarks show that $(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$ is isomorphic to $(t(X), \alpha_* \mathcal{O}_X)$, so the latter is indeed an affine scheme.

To give a morphism of $(t(X), \alpha_* \mathcal{O}_X)$ to $\operatorname{Spec} \kappa$, we have only to give a homomorphism of rings

$$\kappa \longmapsto \Gamma(t(X), \alpha_* \mathcal{O}_X) = \Gamma(X, \mathcal{O}_X).$$

We send $\lambda \in \kappa$ to the constant function λ on X. Thus $t(X)$ becomes a scheme over κ. Finally, if X and Y are two varieties, then one can check that the natural mapping

$$\operatorname{Hom}_{\mathfrak{Var}(\kappa)}(X, Y) \longmapsto \operatorname{Hom}_{\mathfrak{Sch}(\kappa)}(t(X), t(Y))$$

is bijective. This shows that the functor $t : \mathfrak{Var}(\kappa) \longrightarrow \mathfrak{Sch}(\kappa)$ is fully faithful. In particular, it implies that $t(X)$ is isomorphic to $t(Y)$ if and only if X is isomorphic to Y.

It is clear from the construction that $\alpha : X \longrightarrow t(X)$ induces a homeomorphism from X onto the set of closed points of $t(X)$, with the induced topology. □

To any affine variety X over an algebraically closed field κ we can associate a κ-scheme, denoted by X^{sch}, which is simply $\operatorname{Spec} \kappa[X]$. The *closed points* of X^{sch} (i.e., the maximal ideals of $\kappa[X]$) correspond to the points of the variety X and are called *geometric points*. However, X^{sch} has many other (nonclosed) points, in fact, one for each irreducible closed subvariety of X. Of particular interest is the ideal (0), which is dense in X^{sch} and is called the *generic point* of X. Having turned affine varieties into schemes, it is easy to extend the construction to any quasi-projective variety X. We simply cover X by affine open sets U_i, form the affine schemes U_i^{sch}, and then glue the U_i^{sch}'s together to form the scheme X^{sch}.

3.7.2 Basic properties of schemes

A scheme is *connected* if its topological space is connected. A scheme is *irreducible* if its topological space is irreducible. A scheme is *reduced* if for every open set U,

the ring $\mathcal{O}_X(U)$ has no non-zero nilpotent elements. Equivalently, X is reduced if and only if the local ring $\mathcal{O}(x)$, for all $x \in X$, have no non-zero nilpotent elements.

Let $(X, \mathcal{O}_X)$ be a scheme. Let $(\mathcal{O}_X)_{\mathrm{red}}$ be the sheaf associated to the presheaf $U \mapsto \mathcal{O}_X(U)_{\mathrm{red}}$. Then $(X, (\mathcal{O}_X)_{\mathrm{red}})$ is a scheme, called the *reduced scheme* associated to X, and denote it by X_{red}. There is a morphism of schemes $X_{\mathrm{red}} \longrightarrow X$, which is a homeomorphism on the underlying topological spaces. If $f : X \longrightarrow Y$ is a morphism of schemes, where X is reduced, then there is a unique morphism $g : X \longrightarrow Y_{\mathrm{red}}$ such that f is obtained by composing g with the natural mapping $Y_{\mathrm{red}} \longrightarrow Y$.

A scheme is *integral* if for every open set U, the ring $\mathcal{O}_X(U)$ is an integral domain. A scheme is *normal* if all of its local rings are integrally closed domains. A scheme is *locally Noetherian* if it can be covered by open affine subsets $\operatorname{Spec} A_\alpha$, where each A_α is a Noetherian ring. A scheme X is *Noetherian* if it is locally Noetherian and quasi-compact. Equivalently, X is Noetherian if it can be covered by a finite number of open affine subsets $\operatorname{Spec} A_i$, where each A_i is a Noetherian ring.

Example 3.120. If $X = \operatorname{Spec} A$ is an affine scheme, then X is irreducible if and only if the nilradical $\operatorname{Nil}(A)$ of A is prime; X is reduced if and only if $\operatorname{Nil}(A) = 0$; X is integral if A is an integral domain; and X is Noetherian if and only if A is a Noetherian ring.

Proposition 3.121. *A scheme is integral if and only if it is both reduced and irreducible.*

Proof. See Hartshorne [90], Chap. II, Proposition 3.1. □

A morphism $f : X \longrightarrow Y$ of schemes is *locally of finite type* if there exists a covering of Y by open affine subsets $V_i = \operatorname{Spec} B_i$, such that for each i, $f^{-1}(V_i)$ can be covered by open affine subsets $U_{ij} = \operatorname{Spec} A_{ij}$, where each A_{ij} is a finitely generated B_i-algebra. The morphism f is *of finite type* if in addition each $f^{-1}(V_i)$ can be covered by a finite number of the U_{ij}.

A morphism $f : X \longrightarrow Y$ of schemes is *finite* if there exists a covering of Y by open affine subsets $V_i = \operatorname{Spec} B_i$, such that for each i, $f^{-1}(V_i)$ is affine, equal to $\operatorname{Spec} A_i$, where A_i is a B_i-algebra which is a finitely generated B_i-module.

An *open subscheme* of a scheme X is a scheme U, whose topological space is an open subset of X, and whose structure sheaf $\mathcal{O}_U$ is isomorphic to the restriction $\mathcal{O}_X|_U$ of the structure sheaf of X. An *open immersion* is a morphism $f : X \longrightarrow Y$ which induces an isomorphism of X with an open subscheme of Y.

A *closed immersion* is a morphism $f : X \longrightarrow Y$ of schemes such that f induces a homeomorphism of the space X onto a closed subset of the space Y, and furthermore the induced mapping $f^{\#} : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ of sheaves on Y is surjective. A *closed subscheme* of a scheme Y is an equivalence class of closed immersions, where we say $f : X \longrightarrow Y$ and $f' : X' \longrightarrow Y$ are equivalent if there is an isomorphism $i : X' \longrightarrow X$ such that $f' = f \circ i$.

The *dimension* of an irreducible scheme X is the maximal length n of a chain of distinct irreducible closed subsets

$$X_0 \subset X_1 \subset \cdots \subset X_n = X.$$

The *dimension* of a scheme is the maximal dimension of its irreducible components. Clearly, the dimension of $\operatorname{Spec} A$ is just the Krull dimension of A, so the dimension of a variety X is the same as the dimension of the scheme X^{sch}. The scheme of integers satisfies $\dim \operatorname{Spec} A = 1$, and more generally,

$$\dim \operatorname{Spec}(\mathbb{Z}[X_1, \ldots, X_n]) = n + 1.$$

If A is a Dedekind domain, then $\operatorname{Spec} A$ is irreducible, reduced, and has dimension 1.

Let S be a scheme, and let X, Y be schemes over S, i.e., schemes with morphisms to S. We define the *fibred product* of X and Y over S, denoted $X \times_S Y$, to be a scheme, together with morphisms $p_1 : X \times_S Y \longrightarrow X$ and $p_2 : X \times_S Y \longrightarrow Y$, which make a commutative diagram with the given morphisms $X \longmapsto S$ and $Y \longmapsto S$

$$\begin{array}{ccc} X \times_S Y & \xrightarrow{p_2} & Y \\ {\scriptstyle p_1}\downarrow & & \downarrow \\ X & \longrightarrow & S, \end{array}$$

such that given any scheme Z over S, and given morphisms $f : Z \longrightarrow X$ and $g : Z \longrightarrow Y$ which make a commutative diagram with the given morphisms $X \longmapsto S$ and $Y \longmapsto S$

$$\begin{array}{ccc} Z & \xrightarrow{g} & Y \\ {\scriptstyle f}\downarrow & & \downarrow \\ X & \longrightarrow & S, \end{array}$$

then there exists a unique morphism $\theta : Z \longrightarrow X \times_S Y$ such that $f = p_1 \circ \theta$, and $g = p_2 \circ \theta$. The morphisms p_1 and p_2 are called the *projection morphisms* of the fibred product onto its factors.

If X and Y are schemes given without reference to any base scheme S, we take $S = \operatorname{Spec} \mathbb{Z}$ and define the *product* of X and Y, denoted $X \times Y$, to be $X \times_{\operatorname{Spec} \mathbb{Z}} Y$. Here notice that by Proposition 3.115, each scheme X admits a unique morphism to $\operatorname{Spec} \mathbb{Z}$, since every ring A has a canonical homomorphism $\mathbb{Z} \longmapsto A$, so every scheme is a scheme over $\operatorname{Spec} \mathbb{Z}$.

Theorem 3.122. *For any two schemes X and Y over a scheme S, the fibred product $X \times_S Y$ exists, and is unique up to unique isomorphism. Further, if $S = \operatorname{Spec} R$, $X = \operatorname{Spec} A$, and $Y = \operatorname{Spec} B$ are affine, then the fibred product is affine and can be described as $X \times_S Y = \operatorname{Spec} A \otimes_R B$.*

Proof. See Hartshorne [90], Chap. II, Theorem 3.3. □

Let $f : X \longrightarrow Y$ be a morphism of schemes, and let $y \in Y$ be a point. Let $\mathcal{O}(y)$ be the local ring at y, namely the stalk of the structure sheaf at y, and $\mathbf{m}_y$ its maximal ideal. We define the *residue field* of y on Y to be the field

$$\kappa(y) := \mathcal{O}(y)/\mathbf{m}_y.$$

If K is any field, to give a morphism of $\operatorname{Spec} K$ to Y it is equivalent to give a point $y \in Y$ and an inclusion mapping $\kappa(y) \longmapsto K$. In particular, one obtains the natural morphism $\operatorname{Spec} \kappa(y) \longmapsto Y$. Then we define the *fibre* of the morphism f over the point y to be the scheme

$$X_y = X \times_Y \operatorname{Spec} \kappa(y).$$

The fibre X_y is a scheme over $\kappa(y)$, and one can show that its underlying topological space is homeomorphic to the subset $f^{-1}(y)$ of X.

The notion of the fibre of a morphism $f : X \longrightarrow Y$ of schemes allows us to regard a morphism as a *family of schemes* (namely its fibres) parametrized by the points of the image scheme. If Y is irreducible and η is its *generic point*, we call $X_\eta = X \times_Y \operatorname{Spec} \kappa(Y)$ the *generic fibre* of the family. The fibre X_y over a closed point $y \in Y$ is called the *special fibre* at y. A morphism $f : X \longrightarrow Y$, with Y irreducible, is *generically finite* if $f^{-1}(\eta)$ is a finite set, where η is the generic point of Y. Here we state *Zariski's connectedness principle*:

Proposition 3.123. *Let $f : X \longrightarrow S$ be an irreducible family of projective schemes over an irreducible curve S (i.e., a irreducible scheme of dimension 1). Then the generic fiber of f is irreducible. Further, every special fiber of f is connected, and all but finitely many of them are irreducible.*

Proof. See Hartshorne [90], Chap. III, Exercise 11.4. □

Another important application of fibred products is to the notion of base extension. Let S be a fixed scheme which we think of as a *base scheme*, meaning that we are interested in the category of schemes over S. If S' is another base scheme, and if $S' \longmapsto S$ is a morphism, then for any scheme X over S, we let $X' = X \times_S S'$, which will be a scheme over S'. We say that X' is obtained from X by making a *base extension* $S' \longmapsto S$. Note, by the way, that base extension is a transitive operation: if $S'' \longmapsto S' \longmapsto S$ are two morphisms, then

$$(X \times_S S') \times_{S'} S'' \cong X \times_S S''.$$

Let $f : X \longrightarrow Y$ be a morphism of schemes. The *diagonal morphism* is the unique morphism $\Delta : X \longrightarrow X \times_Y X$ whose composition with both projections $p_1, p_2 : X \times_Y X \longrightarrow X$ is the identity mapping of $X \longmapsto X$. We say that the morphism f is *separated* if the diagonal morphism Δ is a closed immersion. In that

case we also say X is *separated* over Y. A scheme X is *separated* if it is separated over $\operatorname{Spec}\mathbb{Z}$.

Proposition 3.124. *An arbitrary morphism $f : X \longrightarrow Y$ is separated if and only if the image of the diagonal morphism is a closed subset of $X \times_Y X$.*

A morphism $f : X \longrightarrow Y$ is *proper* if it is separated, of finite type, and universally closed. Here we say that a morphism is *closed* if the image of any closed subset is closed. A morphism $f : X \longrightarrow Y$ is *universally closed* if it is closed, and for any morphism $Y' \longmapsto Y$, the corresponding morphism $f' : X' \longrightarrow Y'$ obtained by base extension is also closed.

If Y is any scheme, we define *projective n-space* over Y, denoted $\mathbb{P}^n_Y$, to be $\mathbb{P}^n_{\mathbb{Z}} \times_{\operatorname{Spec}\mathbb{Z}} Y$. A morphism $f : X \longrightarrow Y$ of schemes is *projective* if it factors into a closed immersion $i : X \longrightarrow \mathbb{P}^n_Y$ for some n, followed by the projection $\mathbb{P}^n_Y \longmapsto Y$. A morphism $f : X \longrightarrow Y$ is *quasi-projective* if it factors into an open immersion $j : X \longrightarrow X'$ followed by a projective morphism $g : X' \longrightarrow Y$.

Proposition 3.125. *Let κ be an algebraically closed field. The image of the functor $t : \mathfrak{Var}(\kappa) \longrightarrow \mathfrak{Sch}(\kappa)$ of Proposition 3.119 is exactly the set of quasi-projective integral schemes over κ. The image of the set of projective varieties is the set of projective integral schemes. In particular, for any variety X, $t(X)$ is an integral, separated scheme of finite type over κ.*

Proof. See Hartshorne [90], Chap. II, Proposition 4.10. □

An *abstract variety* is an integral separated scheme of finite type over an algebraically closed field κ. If it is proper over κ, we will also say it is *complete*. The following *Chow's lemma* says that proper morphisms are fairly close to projective morphisms:

Lemma 3.126. *Let X be proper over a Noetherian scheme S. Then there is a scheme X' and a morphism $g : X' \longrightarrow X$ such that X' is projective over S, and there is an open dense subset $U \subseteq X$ such that g induces an isomorphism of $g^{-1}(U)$ to U.*

Recall the algebraic notion of a flat module. Let A be a ring, and let M be an A-module. We say that M is *flat* over A if the functor $N \longmapsto M \otimes_A N$ is an exact functor for any module N over A. Let $f : X \longrightarrow Y$ be a morphism of schemes, and let $\mathcal{F}$ be an $\mathcal{O}(X)$-module. We say $\mathcal{F}$ is *flat over Y at a point $x \in X$*, if the stalk $\mathcal{F}(x)$ is a flat $\mathcal{O}_Y(y)$-module, where $y = f(x)$ and we consider $\mathcal{F}(x)$ as an $\mathcal{O}_Y(y)$-module via the natural mapping $f^{\#} : \mathcal{O}_Y(y) \longrightarrow \mathcal{O}_X(x)$. We say simply $\mathcal{F}$ is *flat over Y* if it is flat at every point of X. We say X is *flat* over Y if $\mathcal{O}(X)$ is.

3.7.3 Sheaves of modules

Let A be a ring and let M be an A-module. We define the *sheaf associated* to M on $\operatorname{Spec} A$, denoted by $\tilde{M}$, as follows. For each prime ideal $\mathfrak{p} \subseteq A$, let $M_{\mathfrak{p}}$ be the localization of M at $\mathfrak{p}$. For any open set $U \subseteq \operatorname{Spec} A$ we define the group $M(U)$ to be the set of functions $s : U \longrightarrow \coprod_{\mathfrak{p} \in U} M_{\mathfrak{p}}$ such that for each $\mathfrak{p} \in U$, $s(\mathfrak{p}) \in M_{\mathfrak{p}}$, and such that s is locally a fraction m/f with $m \in M$ and $f \in A$. To be precise, we require that for each $\mathfrak{p} \in U$, there is a neighborhood V of $\mathfrak{p}$ in U, and there are elements $m \in M$ and $f \in A$, such that for each $\mathfrak{q} \in V$, $f \notin \mathfrak{q}$, and $s(\mathfrak{q}) = m/f$ in $M_{\mathfrak{q}}$. We make $\tilde{M}$ into a sheaf by using the obvious restriction mappings.

Let $(X, \mathcal{O}_X)$ be a scheme. A sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ is *quasi-coherent* if X can be covered by open affine subsets $U_i = \operatorname{Spec} A_i$, such that for each i there is an A_i-module M_i with $\mathcal{F}|_{U_i} \cong \tilde{M}_i$. We say that $\mathcal{F}$ is *coherent* if furthermore each M_i can be taken to be a finitely generated A_i-module.

A *sheaf of ideals* on X is a sheaf of modules $\mathcal{J}$ which is a subsheaf of $\mathcal{O}_X$. In other words, for every open set U, $\mathcal{J}(U)$ is an ideal in $\mathcal{O}_X(U)$. Let Y be a closed subscheme of a scheme X, and let $i : Y \longrightarrow X$ be the inclusion morphism. We define the *ideal sheaf* of Y, denoted $\mathcal{J}_Y$, to be the kernel of the morphism $i^{\#} : \mathcal{O}_X \longrightarrow i_* \mathcal{O}_Y$.

Proposition 3.127. *Let X be a scheme. For any closed subscheme Y of X, the corresponding ideal sheaf $\mathcal{J}_Y$ is a quasi-coherent sheaf of ideals on X. If X is Noetherian, it is coherent. Conversely, any quasi-coherent sheaf of ideals on X is the ideal sheaf of a uniquely determined closed subscheme of X.*

Proof. See Hartshorne [90], Chapter II, Proposition 5.9. □

3.7.4 Differentials over schemes

We now carry the definition of the module of relative differential forms to schemes. Let $f : X \longrightarrow Y$ be a morphism of schemes. We consider the diagonal morphism $\Delta : X \longrightarrow X \times_Y X$. It follows from the proof of Proposition 3.124 that Δ gives an isomorphism of X onto its image $\Delta(X)$, which is a locally closed subscheme of $X \times_Y X$, i.e., a closed subscheme of an open subset W of $X \times_Y X$. Let $\mathcal{J}$ be the sheaf of ideals of $\Delta(X)$ in W. Then we define the *sheaf of relative differentials* of X over Y to be the sheaf

$$\Omega_{X/Y} = \Delta^*(\mathcal{J}/\mathcal{J}^2) \tag{3.71}$$

on X. First note that $\mathcal{J}/\mathcal{J}^2$ has a natural structure of $\mathcal{O}_{\Delta(X)}$-module. Then since Δ induces an isomorphism of X to $\Delta(X)$, $\Omega_{X/Y}$ has a natural structure of $\mathcal{O}_X$-module. Furthermore, it follows from Proposition 3.127 that $\Omega_{X/Y}$ is quasi-coherent; if Y is Noetherian and f is a morphism of finite type, then $X \times_Y X$ is also Noetherian, and so $\Omega_{X/Y}$ is coherent.

If $U = \operatorname{Spec} A$ is an open affine subset of Y and $V = \operatorname{Spec} B$ is an open affine subset of X such that $f(V) \subseteq U$, then $V \times_U V$ is an open affine subset of $X \times_Y X$

isomorphic to $\mathrm{Spec}(B \otimes_A B)$, and $\Delta(X) \cap (V \times_U V)$ is the closed subscheme defined by the kernel of the diagonal homomorphism $B \otimes_A B \longrightarrow B$. Thus $\mathcal{J}/\mathcal{J}^2$ is the sheaf associated to the module I/I^2 of (1.6). It follows that

$$\Omega_{V/U} = \Omega_{\mathrm{Spec}\, B/\mathrm{Spec}\, A} \cong \widetilde{\Omega_{B/A}}.$$

Thus our definition of the sheaf of differentials of X/Y is compatible, in the affine case, with the module of differentials defined Section 1.2.4, via the functor $\sim$.

Proposition 3.128. *Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be morphisms of schemes. Then there is an exact sequence of sheaves on X:*

$$f^*\Omega_{Y/Z} \longrightarrow \Omega_{X/Z} \longrightarrow \Omega_{X/Y} \longrightarrow 0.$$

Proof. See Hartshorne [90], Chapter II, Proposition 8.11. □

A morphism $f : X \longrightarrow Y$ of schemes of finite type over a field κ is *smooth of relative dimension n* if:

(i) f is flat;

(ii) if $X' \subseteq X$ and $Y' \subseteq Y$ are irreducible components such that $f(X') \subseteq Y'$, then $\dim X' = \dim Y' + n$;

(iii) for each point $x \in X$ (closed or not),

$$\dim_{\kappa(x)} \Omega_{X/Y} \otimes \kappa(x) = n.$$

If X is integral, then condition (iii) is equivalent to saying $\Omega_{X/Y}$ is locally free on X of rank n.

Theorem 3.129. *Let $f : X \longrightarrow Y$ be a morphism of schemes of finite type over a field κ. Then f is smooth of relative dimension n if and only if f is flat; and the fibres of f are geometrically regular of dimension n.*

Proof. See Hartshorne [90], Chapter III, Theorem 10.2. □

By definition, the fibres of f are *geometrically regular of dimension n* if, for each point $y \in Y$, letting

$$X_{\bar{y}} = X_y \otimes_{\kappa(y)} \overline{\kappa(y)},$$

where $\overline{\kappa(y)}$ is the algebraic closure of $\kappa(y)$, then $X_{\bar{y}}$ is equidimensional of dimension n and regular.

Let $f : X \longrightarrow Y$ be a morphism of schemes of finite type over a field κ. For each $x \in X$, let $y = f(x)$. Let $\hat{\mathcal{O}}(x)$ and $\hat{\mathcal{O}}(y)$ be the completions of the local rings at x and y. Choose fields of representatives $\kappa(x) \subseteq \hat{\mathcal{O}}(x)$ and $\kappa(y) \subseteq \hat{\mathcal{O}}(y)$ so that $\kappa(y) \subseteq \kappa(x)$ via the natural mapping $\hat{\mathcal{O}}(y) \longrightarrow \hat{\mathcal{O}}(x)$. A morphism $f : X \longrightarrow Y$ of

schemes of finite type over a field κ is *étale* if it is smooth of relative dimension 0. It is *unramified* if for every $x \in X$, letting $y = f(x)$, we have

$$\mathbf{m}(y) \cdot \mathcal{O}(x) = \mathbf{m}(x),$$

and $\kappa(x)$ is a separable algebraic extension of $\kappa(y)$.

Proposition 3.130. *Let $f : X \longrightarrow Y$ be a morphism of schemes of finite type over a field κ. The following conditions are equivalent:*

(1) *f is étale;*

(2) *f is flat, and $\Omega_{X/Y} = 0$;*

(3) *f is flat and unramified;*

(4) *for every $x \in X$, $\kappa(x)$ is a separable algebraic extension of $\kappa(y)$, and the nature mapping*

$$\hat{\mathcal{O}}(y) \otimes_{\kappa(y)} \kappa(x) \longrightarrow \hat{\mathcal{O}}(x)$$

is an isomorphism.

Proof. See Hartshorne [90], Chapter III, Exercise 10.3, 10.4. □

3.7.5 Ramification divisors

A scheme X is said to be *regular* (or sometimes *nonsingular*) *in codimension one* if every local ring $\mathcal{O}_X(x)$ of X of dimension one is regular. The most important examples of such schemes are nonsingular varieties over a field and Noetherian normal schemes.

Let X be a Noetherian integral separated scheme over κ which is regular in codimension one. A *prime divisor* on X is a closed integral subscheme Y of codimension one. A *Weil divisor* is an element of the free Abelian group $\mathrm{Div}(X)$ generated by the prime divisors. We write a divisor as

$$D = \sum n_i Y_i,$$

where the Y_i are prime divisors, the n_i are integers, and only finitely many n_i are different from 0. If all the $n_i \geq 0$, we say that D is *effective*.

Let κ be an algebraically closed field. Let X be a Noetherian integral separated scheme over κ which is regular in codimension one. If Y is a prime divisor on X, let $\eta \in Y$ be its generic point. Then the local ring $\mathcal{O}_X(\eta)$ is a discrete valuation ring with quotient field $K := \kappa(X)$, the *function field* of X. We call the corresponding discrete valuation v_Y the *valuation* of Y. Let $f \in K_*$ be any nonzero rational function on X. Then $v_Y(f)$ is an integer. If it is positive, we say f has a *zero* along Y, of that order; if it is negative, we say f has a *pole* along Y, of order $-v_Y(f)$. Note that $v_Y(f) = 0$

for all except finitely many prime divisor (see [90], Chapter II, Lemma 6.1). Thus we can define the *divisor* of f, denoted (f), by

$$(f) = \sum v_Y(f)Y,$$

where the sum is taken over all prime divisors of X. Any divisor which is equal to the divisor of a function is called a *principal divisor*.

Two (Weil) divisors D and D' on X are said to be *linearly equivalent*, written $D \sim D'$, if $D - D'$ is a principal divisor. The group $\mathrm{Div}(X)$ of all divisors dived by the subgroup of principal divisors is called the *divisor class group* of X, and is denoted by $\mathrm{Cl}(X)$.

Let $f : X \longrightarrow Y$ be a generically finite morphism of Noetherian integral separated schemes which are regular in codimension one. The *ramification divisor* of f is defined by

$$R = R_{X/Y} = \sum_Z \mathrm{length}\{(\Omega_{X/Y})_Z\}Z, \tag{3.72}$$

where the sum extends over all prime divisors Z of X, and $\mathrm{length}\{(\Omega_{X/Y})_Z\}$ means the length of the localized module $(\Omega_{X/Y})_Z$ at Z.

Let κ be an algebraically closed field. An abstract variety X of dimension one over κ is called an *abstract curve* over κ. If all local rings of X are regular local rings, we say that X is *nonsingular*.

Proposition 3.131. *Let X be a nonsingular abstract curve over κ with function field K. Then the following condition are equivalent:*

(a) *X is projective;*

(b) *X is complete;*

(c) *$X \cong t(C_K)$, where C_K is the set of all discrete valuation rings of K/κ, and t is the functor from varieties to schemes of Proposition 3.119.*

Proof. See [90], Chapter II, Proposition 6.7. □

Proposition 3.132. *Let X be a complete nonsingular abstract curve over κ, let Y be any abstract curve over κ, and let $f : X \longrightarrow Y$ be a morphism. Then either (1) $f(X) =$ a point, or (2) $f(X) = Y$. In case (2), $\kappa(X)$ is a finite extension field of $\kappa(Y)$, f is a finite morphism, and Y is also complete.*

Proof. See [90], Chapter II, Proposition 6.8. □

If $f : X \longrightarrow Y$ is a finite morphism of abstract curves, we define the *degree* of f to be the degree of the field extension $[\kappa(X) : \kappa(Y)]$. We say the morphism $f : X \longrightarrow Y$ is *separable* if $\kappa(X)$ is a separable field extension of $\kappa(Y)$.

If X is a nonsingular abstract curve, a prime divisor on X is just a closed point, so an arbitrary divisor can be written

$$D = \sum n_i P_i,$$

where the P_i are closed points, and $n_i \in \mathbb{Z}$. We define the *degree* of D to be

$$\deg(D) = \sum n_i.$$

If $f : X \longrightarrow Y$ is a finite morphism of nonsingular abstract curves, we define a homomorphism $f^* : \mathrm{Div}(Y) \longrightarrow \mathrm{Div}(X)$ as follows. For any point $Q \in Y$, let $t \in \mathcal{O}_Y(Q)$ be a *local parameter* at Q, i.e., t is an element of $\kappa(Y)$ with $v_Q(t) = 1$, where v_Q is the valuation corresponding to the discrete valuation ring $\mathcal{O}_Y(Q)$. Consider t as an element of $\mathcal{O}_X(P)$ for $P \in f^{-1}(Q)$ via the natural mapping $f^{\#} : \mathcal{O}_Y(Q) \longrightarrow \mathcal{O}_X(P)$. We define

$$f^*Q = \sum_{f(P)=Q} v_P(t)P.$$

Since f is a finite morphism, this is a finite sum, so we obtain a divisor on X. Note that f^*Q is independent of the choice of the local parameter t. Indeed, if t' is another local parameter at Q, then $t' = ut$ where u is a unit in $\mathcal{O}_Y(Q)$. For any point $P \in f^{-1}(Q)$, $f^{\#}(u)$ will be a unit in $\mathcal{O}_X(P)$, so $v_P(t') = v_P(t)$. We extend the definition by linearity to all divisors on Y. One sees easily that f^* preserves linear equivalence, so it induces a homomorphism $f^* : \mathrm{Cl}(Y) \longrightarrow \mathrm{Cl}(X)$.

The integer $v_P(t)$ is called the *ramification index* of f at $P \in X$, denoted by e_P. If $e_P > 1$, we say f is *ramified* at P, and that Q is a *branch point* of f. If $e_P = 1$, we say f is *unramified* at P. This definition is consistent with the earlier definition of unramified (Section 3.7.4) since our ground field κ is algebraically closed, and so $\kappa(P) = \kappa(Q)$ for any point P of X with $Q = f(P)$. If $\mathrm{char}(\kappa) = 0$, or if $\mathrm{char}(\kappa) = p$, and p does not divide e_P, we say that the ramification is *tame*. If p does divide e_P, it is *wild*.

For any point $P \in X$, let $Q = f(P)$, let t be a local parameter at Q, and let s be a local parameter at P. Then dt is a generator of the free $\mathcal{O}_Y(Q)$-module $\Omega^1[Y]_Q$, and ds is a generator of the free $\mathcal{O}_X(P)$-module $\Omega^1[X]_P$. There is a unique element $g \in \mathcal{O}_X(P)$ such that $f^*(dt) = g\,ds$. We denote this element by dt/ds.

Proposition 3.133. *Let $f : X \longrightarrow Y$ be a finite, separable morphism of abstract curves. Then*

(α) *$\Omega_{X/Y}$ is a torsion sheaf (meaning a sheaf whose stalk at the generic point is zero) on X, with support equal to the set of ramification points of f. In particular, f is ramified at only finitely many points;*

(β) *for each $P \in X$, the stalk $(\Omega_{X/Y})_P$ is a principal $\mathcal{O}_X(P)$-module of finite length equal to $v_P(dt/ds)$;*

(γ) *if f is tamely ramified at P, then*

$$\text{length}\{(\Omega_{X/Y})_P\} = e_P - 1.$$

If f is wildly ramified, then the length is $> e_P - 1$.

(δ) *if K_X and K_Y are the canonical divisors of X and Y, respectively, then*

$$K_X \sim f^* K_Y + R.$$

Proof. See [90], Chapter IV, Proposition 2.2; Proposition 2.3. □

3.8 Kobayashi hyperbolicity

There are rich theory and a lot of researches on Kobayashi hyperbolicity. Here we only introduce simple notations and some open problems related to topics in this book. For more details, see Kobayashi [129], [130], and Lang [148].

3.8.1 Hyperbolicity

Let $\mathbb{D}$ be the open unit disc $\{z \in \mathbb{C} \mid |z| < 1\}$. Let $\text{Hol}(M, N)$ denote the set of holomorphic mappings from a complex space M into another complex space N. We have the classic *Schwarz–Pick lemma* (cf. Kobayashi [129]):

Theorem 3.134. *Assume $f \in \text{Hol}(\mathbb{D}, \mathbb{D})$. Then*

$$\frac{|f'(z)|}{1 - |f(z)|^2} \leq \frac{1}{1 - |z|^2}, \quad z \in \mathbb{D},$$

and equality at a single point z implies that $f \in \text{Aut}(\mathbb{D})$.

We consider the *Hermitian metric* h on $\mathbb{D}$ given by

$$h = \frac{2}{(1 - |z|^2)^2} dz \otimes d\overline{z},$$

which induces the *Riemann metric*

$$ds^2_{\mathbb{D}} = \frac{4}{(1 - |z|^2)^2} dz d\overline{z}.$$

Then the inequality in Theorem 3.134 may be written as follows:

$$f^* ds^2_{\mathbb{D}} \leq ds^2_{\mathbb{D}},$$

or

$$d_h(f(z), f(z')) \leq d_h(z, z')$$

for the associated distance function d_h. The metric h (or $ds^2_{\mathbb{D}}$) is called the *Poincaré metric* or the *Poincaré–Bergman metric* of $\mathbb{D}$. We note that the Gaussian curvature of the metric h is equal to -1 everywhere. By a simple calculation we have

$$d_h(z,w) = \log \frac{1+|\alpha|}{1-|\alpha|} \ (z,w \in \mathbb{D}),$$

where

$$\alpha = \frac{w-z}{1-\overline{z}w}.$$

Definition 3.135. Let M be a complex space. Let $x, y \in M$ be arbitrary points. A *holomorphic chain* α from x to y is the collection of holomorphic mappings $f_i \in \mathrm{Hol}(\mathbb{D}, M)$ and $p_i, q_i \in \mathbb{D}$ for $i = 0, \ldots, l$ such that

$$f_0(p_0) = x, \quad f_i(q_i) = f_{i+1}(p_{i+1}) \ (0 \le i \le l-1), \quad f_l(q_l) = y.$$

Then the *Kobayashi pseudo distance* d_M is given by

$$d_M(x,y) = \inf_{\alpha} \left\{ \sum_{i=0}^{l} d_h(p_i, q_i) \right\}, \tag{3.73}$$

where the infimum is taken for all holomorphic chains α from x to y.

For the existence of a holomorphic chain from x to y, the reader is referred to S. Lang [148]. It is easy to see that for $x, y, z \in M$,

$$d_M(x,x) = 0, \ \ d_M(x,y) = d_M(y,x), \ \ d_M(x,z) \le d_M(x,y) + d_M(y,z). \tag{3.74}$$

In general, a mapping $d_M : M \times M \longrightarrow \mathbb{R}_+$ satisfying the relation above is called a *pseudo distance* which may identically vanish. If f is a holomorphic mapping between two complex spaces M and N, then the Kobayashi pseudo distances satisfy

$$d_N(f(x), f(y)) \le d_M(x,y), \ \ \{x,y\} \subset M. \tag{3.75}$$

Example 3.136. Let $M = \mathbb{C}$ with the Euclidean metric. Then $d_{\mathbb{C}}(x,y) = 0$ for all $x, y \in \mathbb{C}$. In fact, given two points $x, y \in \mathbb{C}$ and an arbitrarily small positive number ε, there is a mapping $f \in \mathrm{Hol}(\mathbb{D}, \mathbb{C})$ such that $f(0) = x$ and $f(\varepsilon) = y$. Hence $d_{\mathbb{C}}(x,y) \le \log \frac{1+\varepsilon}{1-\varepsilon}$.

It will be useful to consider the following generalization. Let M be a subset of a complex Hermitian manifold $\bar{M}$. We can define d_M on M by taking the mappings f_i to lie in M, and to be holomorphic as mappings into $\bar{M}$. Then we obtain a pseudo distance on M. We say that M is *Kobayashi hyperbolic* in $\bar{M}$ if this pseudo distance is a distance, that is if $x \neq y$ implies $d_M(x,y) \neq 0$. For simplicity, we shall say *hyperbolic* instead of Kobayashi hyperbolic. If M is a complex space imbedded in

a complex manifold $\bar{M}$, then a mapping into M is analytic if and only if it is analytic viewed as a mapping into $\bar{M}$. Therefore the definition of the Kobayashi pseudo distance on M is intrinsic, independent of the imbedding of M into a manifold.

If M is hyperbolic, then it follows directly from (3.75) and Example 3.136 that there cannot be a non-constant holomorphic mapping $f : \mathbb{C} \longrightarrow M$. The converse is due to Brody [18]:

Theorem 3.137 ([18]). *Let M be a relatively compact complex subspace of a complex Hermitian manifold $\bar{M}$, and suppose M is not hyperbolic. Then there exists a non-constant holomorphic mapping $f : \mathbb{C} \longrightarrow \bar{M}$ such that*

$$\|f'(0)\| = 1; \quad \|f'(z)\| \leq 1, \ \ z \in \mathbb{C}.$$

Recall that the induced linear mapping

$$f'(z) : \mathbf{T}_z(\mathbb{C}) = \mathbb{C} \longrightarrow \mathbf{T}_{f(z)}(\bar{M}),$$

is the *holomorphic differential* at each $z \in \mathbb{C}$. Each complex tangent space has its norm: $\mathbf{T}_{f(z)}(\bar{M})$ has the Hermitian norm, and $\mathbf{T}_z(\mathbb{C}) = \mathbb{C}$ has the Euclidean norm. The *norm* of the linear mapping $f'(z)$ is defined as usual:

$$\|f'(z)\| = \sup_v \frac{\|f'(z)v\|}{\|v\|}, \quad v \in \mathbf{T}_z(\mathbb{C}), \ \ v \neq 0.$$

Based on this theorem, it is useful to define a complex space M to be *Brody hyperbolic* if every holomorphic mapping of $\mathbb{C}$ into M is constant.

Let M be any variety. Lang [147], [150] introduces the *holomorphic special set* $\mathrm{Sp}_{\mathrm{hol}}(M)$ of M to be the Zariski closure of the union of all images of non-constant holomorphic mappings $f : \mathbb{C} \longrightarrow M$. Thus M is hyperbolic if and only if this special set is empty. In general the special set may be the whole variety. Here we consider a smooth toroidal compactification M of $\mathcal{D}/\Gamma$, where $\mathcal{D}$ is a bounded symmetric domain of $\mathbb{C}^m$ and $\Gamma \subset \mathrm{Aut}(\mathcal{D})$ is an arithmetic subgroup. In general, Γ may not act freely on $\mathcal{D}$, but a subgroup of finite index will act without fixed points, and we lose no essential generality in assuming that this is true for $\mathcal{D}$. It is well known that $\mathcal{D}/\Gamma$ is negatively curved since in fact the *Bergman metric* on $\mathcal{D}$ has negative holomorphic sectional curvatures $\leq -c < 0$ and is Γ-invariant. Further, $\mathcal{D}/\Gamma$ is hyperbolic (see [129], [200]), and so $\mathrm{Sp}_{\mathrm{hol}}(M) \not\subset \mathcal{D}/\Gamma$. It is a basic theorem of Baily–Borel [4] that $\mathcal{D}/\Gamma$ is quasi-projective. It is natural to ask whether $\mathrm{Sp}_{\mathrm{hol}}(M) \subset M - \mathcal{D}/\Gamma$?

Kiernan and Kobayashi [127] discuss the notion of M being *hyperbolic modulo a subset S*, meaning that the Kobayashi pseudo distance in M satisfies $d_M(x, y) \neq 0$ unless $x = y$ or $x, y \in S$. According to S. Lang [147], the variety M is said to be *pseudo Brody hyperbolic* if the special set $\mathrm{Sp}_{\mathrm{hol}}(M)$ is a proper subset; and M is *pseudo Kobayashi hyperbolic* if there exists a proper algebraic subset S such that M is hyperbolic modulo S. S. Lang [147] conjectures that the two definitions are equivalent with $S = \mathrm{Sp}_{\mathrm{hol}}(M)$.

3.8.2 Measure hyperbolicity

Let M be a complex manifold with volume or pseudo volume form Ψ. Let $C_0(M)$ be the set of continuous functions with compact support. Then Ψ defines a positive functional on $C_0(M)$ by

$$\varphi \mapsto \int_M \varphi\Psi.$$

Hence there is a unique regular positive measure μ_Ψ such that

$$\int_M \varphi d\mu_\Psi = \int_M \varphi\Psi, \ \ \varphi \in C_0(M).$$

For example, on the ball of radius r in $\mathbb{C}^m$ with center at 0:

$$\mathbb{C}^m(0;r) = \{(z_1,\ldots,z_m) \in \mathbb{C}^m \mid |z|^2 = |z_1|^2 + \cdots + |z_m|^2 < r^2\},$$

there is the standard positive $(1,1)$-form

$$\omega = 2i\left\{\sum_k \frac{1}{r^2-|z|^2} dz_k \wedge d\bar{z}_k + \frac{4|z|^2}{(r^2-|z|^2)^2}\partial|z| \wedge \overline{\partial}|z|\right\} \tag{3.76}$$

with

$$\Theta_r = \frac{1}{m!}\omega^m = \frac{2^m r^2}{(r^2-|z|^2)^{m+1}} \prod_{k=1}^m i dz_k \wedge d\bar{z}_k, \tag{3.77}$$

$$\mathrm{Ric}(\Theta_r) = -(m+1)dd^c \log(r^2-|z|^2) = \frac{m+1}{4\pi}\omega. \tag{3.78}$$

Thus the Einstein–Kähler metric on $\mathbb{C}^m(0;r)$ is given by

$$h_r = \sum_{k=1}^m \frac{2}{r^2-|z|^2} dz_k \otimes d\bar{z}_k + \frac{2}{(r^2-|z|^2)^2}\left(\sum_{k=1}^m \bar{z}_k dz_k\right) \otimes \left(\sum_{k=1}^m z_k d\bar{z}_k\right) \tag{3.79}$$

such that holomorphic sectional curvatures are -1 everywhere.

Lemma 3.138. *Let M be a complex manifold of dimension m and let Ψ be a pseudo volume form on M such that $\mathrm{Ric}(\Psi)$ is positive, and such that there exists a constant $c > 0$ such that the Griffiths function $G(\Psi)$ of Ψ satisfies $cG(\Psi) \geq 1$. Then for all holomorphic mappings $f : \mathbb{C}^m(0;r) \longrightarrow M$, we have*

$$f^*\Psi \leq c\left(\frac{m+1}{4\pi}\right)^m \Theta_r.$$

Proof. See [129], Theorem 4.4; [130], Corollary 2.4.15; or [102]. □

For $r = 1$, we write Θ for Θ_1. The unit ball $\mathbb{C}^m(0;1)$ will be denoted $\mathbb{B}^m$.

Definition 3.139. Let M be a complex manifold of dimension m. Let A be a Borel measurable subset of M. A *holomorphic chain* α for A is the collection of holomorphic mappings $f_i \in \mathrm{Hol}(\mathbb{B}^m, M)$ and open sets U_i in $\mathbb{B}^m$ for $i = 1, 2, \ldots$ such that

$$A \subset \bigcup_i f_i(U_i).$$

The space M is said to be *covered by holomorphic chains* if there exists a holomorphic chain for M. Then the Kobayashi measure μ_M is defined by

$$\mu_M(A) = \inf_\alpha \sum_{i=1}^{\infty} \mu_\Theta(U_i), \tag{3.80}$$

where the infimum is taken for all holomorphic chains α for A, where μ_Θ is the regular measure on $\mathbb{B}^m$ induced by Θ. If $\mu_M(W) > 0$ for all non-empty open sets W in M, then M is called *measure hyperbolic*.

Since the open sets generate the σ-algebra of Borel measurable sets, it follows that if B is measurable in $\mathbb{B}^m$ and f is holomorphic, then $f(B)$ is measurable. Furthermore, a regular measure satisfies the property that the measure of a set is the infimum of the measures of the open sets containing it. Hence in the definition of the Kobayashi measure, instead of taking open sets U_i we could take measurable sets B_i in $\mathbb{B}^m$. A basic fact is that if μ is a measure on a complex manifold M of dimension m such that every holomorphic mapping $f : \mathbb{B}^m \longrightarrow M$ satisfies

$$\mu(f(B)) \leq \mu_\Theta(B)$$

for every Borel measurable set B in $\mathbb{B}^m$, then $\mu \leq \mu_M$ (cf. [129], Proposition 1.5; [130], Theorem 7.2.6). Thus the complex manifold M satisfying the conditions in Lemma 3.138 is measure hyperbolic (cf. [130], Theorem 7.4.1).

We let

$$n \to_{\mathrm{div}} \infty$$

denote the property that n tends to infinity, ordered by divisibility. In speaking of estimates, we use the standard notation of number theorists

$$A(n) \ll B(n), \;\; n \to \infty$$

to mean that there is a constant c such that $A(n) \leq cB(n)$ for all sufficiently large n. Here, sufficiently large may mean with respect to the divisibility ordering. We recall two lemmas from basic algebraic geometry (cf. [130], [147]).

Lemma 3.140. *Let X be a variety of dimension n. Let L be a holomorphic line bundle on X. Then*

$$\dim H^0(X, \mathcal{O}(L^m)) \ll m^n, \;\; m \to \infty.$$

Proof. Let H be an ample line bundle such that $E = L \otimes H$ is ample. If m is large enough so that H^m is very ample, then the exact sequence of sheaves (cf. [81], p. 139)

$$0 \longrightarrow \mathcal{O}(L^m) \longrightarrow \mathcal{O}(E^m) \longrightarrow \mathcal{O}(E^m|_D) \longrightarrow 0$$

where D is a smooth effective divisor of X obtained as the zero set of a general holomorphic section of H^m, and $E^m|_D$ denotes the restriction of E^m to D, induces an exact sequence

$$0 \longrightarrow H^0(X, \mathcal{O}(L^m)) \longrightarrow H^0(X, \mathcal{O}(E^m)) \longrightarrow H^0(D, \mathcal{O}(E^m|_D))$$

which further implies

$$\dim H^0(X, \mathcal{O}(L^m)) \leq \dim H^0(X, \mathcal{O}(E^m)).$$

Furthermore, since E^m is ample, then Kodaira's vanishing theorem implies

$$\dim H^0(X, \mathcal{O}(E^m)) = \chi(X, E^m).$$

On the other hand (Hirzebruch [100], p. 150), we have

$$\chi(X, E^m) = a_0 + a_1 m + \cdots + a_n m^n,$$

where $a_0, a_1, \ldots, a_n$ are rational numbers determined by characteristic classes of X and E, thus proving the lemma. □

Lemma 3.141. *Let X be a non-singular variety of dimension n. Let L be a holomorphic line bundle on X such that*

$$\dim H^0(X, \mathcal{O}(L^m)) \gg m^n, \;\; m \to_{\text{div}} \infty.$$

Then for a very ample line bundle E on X,

$$\dim H^0(X, \mathcal{O}(L^m \otimes E^*)) \gg m^n, \;\; m \to_{\text{div}} \infty,$$

in particular, $H^0(X, \mathcal{O}(L^m \otimes E^*)) \neq \{0\}$.

Proof. Let D be a non-singular effective divisor of X obtained as the zero set of a general holomorphic section of E. We have the exact sequence of sheaves

$$0 \to \mathcal{O}(L^m \otimes E^*) \to \mathcal{O}(L^m) \to \mathcal{O}(L^m|_D) \to 0,$$

whence the exact cohomology sequence

$$0 \to H^0(X, \mathcal{O}(L^m \otimes E^*)) \to H^0(X, \mathcal{O}(L^m)) \to H^0\left(D, \mathcal{O}(L^m|_D)\right).$$

Applying Lemma 3.140 to this invertible sheaf on D we conclude that the dimension of the term on the right is $\ll m^{n-1}$, so for m large

$$\dim H^0(X, \mathcal{O}(L^m \otimes E^*)) \gg m^n,$$

and in particular is positive for m large, whence the lemma follows. □

Conversely, if L is a holomorphic line bundle on X, and if E is a very ample line bundle on X such that

$$H^0(X, \mathcal{O}(L^m \otimes E^*)) \neq \{0\}$$

for some positive integer m, then L is pseudo ample (see [130], Lemma 7.3.7). In fact, let α be a non-trivial holomorphic section of $L^m \otimes E^*$ and set

$$\Gamma_X = \{\alpha s \mid s \in \Gamma(X, E)\} \subset \Gamma(X, L^m).$$

A holomorphic projective imbedding of X is well defined by using only the subspace Γ_X, i.e., the sections of L^m that are divisible by α. The imbedding thus obtained is none other than the imbedding φ_E obtained by using $\Gamma(X, E)$. If we use $\Gamma(X, L^m)$, then we obtain only a meromorphic imbedding φ_{L^m} of X into a projective space.

Theorem 3.142 (Kodaira [134], Kobayashi–Ochiai [131]). *Let X be a non-singular pseudo canonical variety. Then X admits a pseudo volume form Ψ with* $\mathrm{Ric}(\Psi)$ *positive, and X is measure hyperbolic.*

Proof. Set $n = \dim X$. Since X is pseudo canonical, then

$$\dim H^0(X, \mathcal{O}(K_X^m)) \gg m^n$$

for m large, so we can apply Lemma 3.141. Let L be a very ample line bundle on X. We shall obtain a projective imbedding of X by means of some of the sections in $H^0(X, \mathcal{O}(K_X^m))$. By Lemma 3.141, for m large there exists a non-trivial holomorphic section α of $K_X^m \otimes L^*$. Let $\{s_0, \ldots, s_N\}$ be a basis of $H^0(X, \mathcal{O}(L))$. Then

$$\alpha \otimes s_0, \ldots, \alpha \otimes s_N$$

are linearly independent sections of $H^0(X, \mathcal{O}(K_X^m))$. Since $[s_0, \ldots, s_N]$ gives a projective imbedding of X into $\mathbb{P}^N$ because L is assumed very ample, it follows that $\alpha \otimes s_0, \ldots, \alpha \otimes s_N$ vanish simultaneously only at the zeros of α, but nevertheless give the same projective imbedding, which is determined only by their ratios. Then

$$\alpha\overline{\alpha} \otimes \sum_{j=0}^{N} s_j \otimes \overline{s}_j$$

may be considered as a section of

$$(K_X^m L^*)L \otimes (\overline{K}_X^m \overline{L}^*)\overline{L} = K_X^m \otimes \overline{K}_X^m,$$

and can be locally expressed in terms of complex coordinates in the form

$$|g(z)|^2 \sum_{j=0}^{N} |g_j(z)|^2 \Phi(z)^{\otimes m},$$

where as usual $\Phi(z)$ is the standard Euclidean volume form on $\mathbb{C}^n$, while $g(z), g_0(z), \ldots, g_N(z)$ are local holomorphic functions representing $\alpha, s_0, \ldots, s_N$ respectively. Set

$$h(z) = \left(\sum_{j=0}^{N} |g_j(z)|^2 \right)^{\frac{1}{m}}.$$

Then there is a unique pseudo volume form Ψ on X which has the local expression

$$\Psi(z) = |g(z)|^{\frac{2}{m}} h(z) \Phi(z).$$

Furthermore $\mathrm{Ric}(\Psi)$ is positive, because $\mathrm{Ric}(\Psi)$ is the pull-back of the Fubini–Study form on $\mathbb{P}^N$ by the projective imbedding. □

Its converse is due to Burt Totaro [277] (or see Kobayashi [130]), that is, if a non-singular projective variety X admits a pseudo volume form Ψ with $\mathrm{Ric}(\Psi)$ positive, then X is pseudo canonical. In fact, take an open cover $\{U_j\}$ of X with holomorphic coordinates $z_1^j, \ldots, z_n^j$ on U_j, where $n = \dim X$. We obtain a non-vanishing holomorphic section of K_X on each U_j:

$$\xi_j = dz_1^j \wedge \cdots \wedge dz_n^j.$$

We know that Ψ induces a "pseudo" metric $\kappa = \kappa_\Psi$ on K_X such that

$$i_n \xi_j \wedge \overline{\xi_j} = |\xi_j|_\kappa^2 \Psi.$$

Then our assumption on Ψ means

$$\Psi = h_j |g_j|^{2q} i_n \xi_j \wedge \overline{\xi_j},$$

where h_j is a positive C^∞ function on U_j, $q > 0$ is some fixed rational number, and g_j is holomorphic not identically zero. Hence we have

$$|\xi_j|_\kappa^{-2} = h_j |g_j|^{2q}.$$

Write $q = p/m$ for coprime positive integers p and m. If $\xi_k = \lambda_{jk} \xi_j$ on $U_j \cap U_k$, then

$$h_j^m |g_j|^{2p} = |\lambda_{jk}|^{2m} h_k^m |g_k|^{2p}.$$

Define

$$\chi_{jk} = \lambda_{jk}^m \big(g_k g_j^{-1}\big)^p$$

so that

$$h_j^{-m} = |\chi_{jk}|^{-2} h_k^{-m}.$$

Since $g_k g_j^{-1}$ is a holomorphic function on $U_j \cap U_k$ without zeroes, we can define a line bundle H by the system of transition functions $\{\chi_{jk}\}$. Then $\{h_j^{-m}\}$ define a metric ρ on H such that

$$c_1(H, \rho)|_{U_j} = -dd^c \log h_j^{-m} = m \mathrm{Ric}(\Psi)|_{U_j} > 0,$$

that is, H is positive, and so H is ample. Hence $E = H^l$ is very ample for some positive integer l. Since the transition functions for $K_X^{ml} \otimes E^*$ are given by $\{\lambda_{jk}^{ml}\chi_{jk}^{-l}\}$ and since

$$g_j^{pl} = \lambda_{jk}^{ml}\chi_{jk}^{-l}g_k^{pl},$$

$\{g_j^{pl}\}$ represents a holomorphic section of $K_X^{ml} \otimes E^*$.

This shows that $\Gamma(X, K_X^{ml} \otimes E^*) \neq \{0\}$. Therefore K_X is pseudo ample according to the remark after Lemma 3.141.

3.8.3 Open problems

Problem 3.143. Let M be a projective algebraic variety. Determine which of the following conditions are equivalent:

(1) M is Kobayashi hyperbolic;

(2) All subvarieties of M (including M itself) are pseudo canonical;

(3) Every subvariety of M is measure hyperbolic;

(4) M is negatively curved;

(5) M is Brody hyperbolic.

Now we know that (1) $\Longleftrightarrow$ (5). Kobayashi has shown that (4) implies (1); otherwise all equivalence above remain unproved. He stated $(1) \Longrightarrow (4)$ as a problem; other implications in the above list are conjectures of Lang.

Problem 3.144. Let M be a projective algebraic variety. Determine which of the following conditions are equivalent:

(i) M is pseudo Kobayashi hyperbolic;

(ii) M is pseudo canonical;

(iii) M is measure hyperbolic;

(iv) There exists a pseudo volume form Ψ for which $\mathrm{Ric}(\Psi) > 0$;

(v) M is pseudo Brody hyperbolic.

Currently what is known is that (ii) $\Longleftrightarrow$ (iv) (see Kodaira [134], Totaro [277]), (ii) $\Longrightarrow$ (iii) (see Kobayashi–Ochiai [131]), (i) $\Longrightarrow$ (iii) (see Kobayashi [129]), and (iii) $\Longrightarrow$ (ii) for surfaces (see Mori–Mukai [193]). Kobayashi [129] prosed (iii) $\Longrightarrow$ (ii) as a problem; other implications are conjectures of Lang.

If M is a non-singular projective variety over $\mathbb{C}$, Kobayashi and Ochiai [132] conjectured that if M is hyperbolic then the canonical class K_M is pseudo ample, but Lang [150] made the stronger conjecture:

Conjecture 3.145. *If M is non-singular and hyperbolic then K_M is ample.*

Here we consider a non-singular hypersurface M of degree d in $\mathbb{P}^n(\mathbb{C})$. When $d \leq n-1$, then M contains a line through every point (cf. [147]). The adjunction formula immediately implies

$$K_M = \left(K_{\mathbb{P}^n(\mathbb{C})} \otimes [M]\right)|_M = (H|_M)^{d-n-1},$$

where H is the hyperplane line bundle on $\mathbb{P}^n(\mathbb{C})$. Then $d \geq n+2$ is precisely the condition that makes the canonical bundle K_M ample. When $n \geq 3$, since the Fermat hypersurface

$$x_0^d + \cdots + x_n^d = 0$$

contains a line

$$z \in \mathbb{C} \longmapsto [z, c_1 z, \ldots, c_r z, c_{r+1}, \ldots, c_{n-1}, 1] \in \mathbb{P}^n(\mathbb{C}),$$

where $1 \leq r \leq n-2$, and $c_1, \ldots, c_{n-1}$ are numbers such that

$$1 + c_1^d + \cdots + c_r^d = 0, \;\; c_{r+1}^d + \cdots + c_{n-1}^d + 1 = 0,$$

we see that in general the condition that M has ample canonical bundle does not imply M hyperbolic. However, in 1970, S. Kobayashi ([129], p. 132) made the following conjecture:

Conjecture 3.146. *A generic hypersurface of degree* $\geq 2n+1$ *of* $\mathbb{P}^n(\mathbb{C})$ *is hyperbolic, and that its complement is complete hyperbolic.*

This conjecture is still open, but there has been some progress on the existence of hyperbolic hypersurfaces of $\mathbb{P}^n(\mathbb{C})$. Examples of hyperbolic hypersurfaces were constructed by R. Brody and M. Green [19], M. Zaidenberg [305], A. M. Nadel [199], H.-K. Hà [84], M. McQuillan [178], J.-P. Demailly and J. El Goul [47], B. Shiffman and M. Zaidenberg [242] in dimension 2, M. Shirosaki [247], C. Ciliberto and M. Zaidenberg [31] in dimension 3, and finally by K. Masuda and J. Noguchi [170], Y. T. Siu and S. K. Yeung [257], B. Shiffman and M. Zaidenberg [243], and H. Fujimoto [70] in any dimension. J. El Goul [55] gave a construction of a hyperbolic surface of degree 14 and J.-P. Demailly [46] later reduced the degree in El Goul's construction to 11. Y. T. Siu and S. K. Yeung [257] also obtained an elegant hyperbolic surface of degree 11 by using their generalized Borel lemma. M. Shirosaki [248] constructed a hyperbolic surface of degree 10. H. Fujimoto [70] improved Shirosaki's construction to give examples of degree 8. J. Duval [53] gave hyperbolic surfaces of degree 6 in $\mathbb{P}^3(\mathbb{C})$. Hu and Yang [113] also constructed hyperbolic hypersurfaces of lower degrees.

Chapter 4

Height functions

A height function is a means of measuring the "size" of a rational or integral point on an algebraic variety. Based on the product formula in Section 2.2, one defines heights on projective spaces defined over number fields, and further defines heights on varieties associated to divisors, which will be compared with the heights defined by using Weil functions of the divisors. The corresponding first main theorems also be exhibited.

4.1 Heights on projective spaces

4.1.1 Basic properties

Let $V = V_{\bar{\mathbb{Q}}}$ be a vector space of finite dimension $n+1 > 0$ over $\bar{\mathbb{Q}}$. Take $\xi \in V - \{0\}$ and write $\xi = \xi_0 e_0 + \cdots + \xi_n e_n$ for a fixed basis $\{e_0, \ldots, e_n\}$ of V. Then $(\xi_0, \ldots, \xi_n) \in \kappa^{n+1}$ for some number field κ. We will denote the case by $\xi \in V_\kappa$ and say that ξ is defined over κ. Let M_κ be the set of absolute values on κ satisfying product formula with multiplicities n_v. Then $|\xi|_v = 1$ for all but finitely many $v \in M_\kappa$, that is, $\gamma = \{|\xi|_v\}$ is a multiplicative M_κ-constant. We can define the *relative* (*multiplicative*) *height* of ξ (relate to κ) by

$$H_\kappa(\xi) = \prod_{v \in M_\kappa} |\xi|_v^{n_v}.$$

If, e.g., $\xi_0 \neq 0$, then $|\xi|_v \geq |\xi_0|_v$ for each v, which implies

$$H_\kappa(\xi) \geq 1. \tag{4.1}$$

Also $|\lambda\xi|_v = |\lambda|_v |\xi|_v$ for $\lambda \in \kappa_*$, so

$$H_\kappa(\lambda\xi) = H_\kappa(\xi) \tag{4.2}$$

by the product formula.

If we have a tower of finite extensions $\mathbb{Q} \subset \kappa \subset K$ and if $\xi \in V - \{0\}$ is defined over κ, then

$$H_K(\xi) = \prod_{w \in M_K} |\xi|_w^{n_w} = \prod_{v \in M_\kappa} \prod_{w \in M_K, w|v} |\xi|_v^{n_w}.$$

By using (2.18), we have

$$H_K(\xi) = \prod_{v \in M_\kappa} |\xi|_v^{n_v[K:\kappa]} = H_\kappa(\xi)^{[K:\kappa]},$$

and so

$$H_K(\xi)^{\frac{1}{[K:\mathbb{Q}]}} = H_\kappa(\xi)^{\frac{[K:\kappa]}{[K:\mathbb{Q}]}} = H_\kappa(\xi)^{\frac{1}{[\kappa:\mathbb{Q}]}}. \tag{4.3}$$

The transformation formula (4.3) allows us to define a height function that is independent of the field. The *absolute* (*multiplicative*) *height* is defined by

$$H(\xi) = H_\kappa(\xi)^{\frac{1}{[\kappa:\mathbb{Q}]}},$$

which does not depend on finite field extensions of $\mathbb{Q}$, that is, we obtain the function

$$H : V \longrightarrow \mathbb{R}[1, +\infty).$$

We often use the *absolute* (*logarithmic*) *height* $h(\xi)$ which is defined by

$$h(\xi) = \log H(\xi) = \frac{1}{[\kappa : \mathbb{Q}]} \log H_\kappa(\xi).$$

In many references, the *relative* (*multiplicative*)*height* (relate to κ) is defined by

$$H_{*,\kappa}(\xi) = \prod_{v \in M_\kappa} |\xi|_{*,v}^{n_v}$$

for $\xi = \xi_0 e_0 + \cdots + \xi_n e_n \in V_\kappa - \{0\}$, where

$$|\xi|_{*,v} = \max\{|\xi_0|_v, |\xi_1|_v, \ldots, |\xi_n|_v\}.$$

Obviously, $H_{*,\kappa}$ also satisfies (4.1), (4.2) and (4.3). Thus the *absolute* (*multiplicative*) *height*

$$H_*(\xi) = H_{*,\kappa}(\xi)^{\frac{1}{[\kappa:\mathbb{Q}]}}$$

and the *absolute* (*logarithmic*) *height*

$$h_*(\xi) = \log H_*(\xi) = \frac{1}{[\kappa : \mathbb{Q}]} \log H_{*,\kappa}(\xi)$$

are well defined. Note that

$$|\xi|_{*,v} \le |\xi|_v \le \varsigma_{v,n+1} |\xi|_{*,v},$$

and so

$$H_{*,\kappa}(\xi) \le H_\kappa(\xi) \le (n+1)^{\frac{[\kappa:\mathbb{Q}]}{2}} H_{*,\kappa}(\xi).$$

We have

$$h_* \le h \le h_* + \frac{1}{2} \log(n+1).$$

Definition 4.1. Two heights H_1 and H_2 (resp. logarithmic heights h_1 and h_2) are called *equivalent* if

$$cH_1 < H_2 < c'H_1 \ \ (\text{resp. } h_2 = h_1 + O(1))$$

holds for some positive constants c and c'.

Hence if the base of V is changed, we obtain an equivalent height. In particular, H and H_* are equivalent.

Take $x \in \mathbb{P}(V) \cong \mathbb{P}^n$. Then there exists a coordinate $\xi \in V_\kappa$ for some number field κ such that $x = \mathbb{P}(\xi)$. The *relative* (*multiplicative*) *heights* of x are defined by

$$H_\kappa(x) = H_\kappa(\xi), \quad H_{*,\kappa}(x) = H_{*,\kappa}(\xi).$$

Similarly, the *absolute* (*multiplicative*) *heights*

$$H(x) = H(\xi), \quad H_*(x) = H_*(\xi)$$

and the *absolute* (*logarithmic*) *heights* of x

$$h(x) = h(\xi), \quad h_*(x) = h_*(\xi)$$

are defined respectively. By the product formula, these do not depend on the choice of ξ.

Example 4.2. Any point $x \in \mathbb{P}(\mathbb{Q}^{n+1})$ has a set of coordinates $(\xi_0, \ldots, \xi_n)$ which are relatively prime integers, and we then see that

$$H_{\mathbb{Q}}(x) = \sqrt{\xi_0^2 + \cdots + \xi_n^2}, \quad H_{*,\mathbb{Q}}(x) = \max\{|\xi_0|, |\xi_1|, \ldots, |\xi_n|\}.$$

In particular, the set of points x in $\mathbb{P}(\mathbb{Q}^{n+1})$ of height $H_{\mathbb{Q}}(x) \leq$ a fixed number is finite. Such a fact is also true in a number field (see Theorem 4.29).

Lemma 4.3. *Any element x of $\mathbb{P}(V)$ has a coordinate $\xi \in V_\kappa$ for some number field κ with $x = \mathbb{P}(\xi)$ such that*

(i) $|\xi|_v \leq 1$ *for non-Archimedean v;*

(ii) $\displaystyle\prod_{v \in M_\kappa^0} \|\xi\|_v \geq |D_{\kappa/\mathbb{Q}}|^{-1/2}$;

(iii) $|\xi|_v \leq c(\kappa)|\xi|_w$ *for any Archimedean v, w.*

Proof. For a fixed basis $\{e_0, \ldots, e_n\}$ of V, take $\xi' = \xi_0' e_0 + \cdots + \xi_n' e_n \in V_\kappa$ with $x = \mathbb{P}(\xi')$. Consider the ideal $\mathfrak{g}(\xi')$ generated by $\xi_0', \ldots, \xi_n'$. By Theorem 2.26, there is an integral ideal $\mathfrak{a}$ in the same ideal class as $\mathfrak{g}(\xi')$ such that the norm satisfies $\mathcal{N}(\mathfrak{a}) \leq \sqrt{|D_{\kappa/\mathbb{Q}}|}$. After multiplying ξ' by some $\lambda \in \kappa$, we get a new ξ with $\mathfrak{g}(\xi) = \mathfrak{a}$. Then $\xi_0, \ldots, \xi_n$ are integers in κ, and so (i) holds.

If we write

$$(\xi_i) = \prod_j \mathfrak{p}_j^{\nu_{ij}},$$

then

$$\|\xi\|_{\mathfrak{p}_j} = \mathcal{N}(\mathfrak{p}_j)^{-\min(\nu_{0j},\ldots,\nu_{nj})}.$$

On the other hand,

$$\mathfrak{a} = \mathfrak{g}(\xi) = \prod_j \mathfrak{p}_j^{\min(\nu_{0j},\ldots,\nu_{nj})},$$

so we obtain

$$\prod_{v\in M_\kappa^0} \|\xi\|_v = \prod_j \|\xi\|_{\mathfrak{p}_j} = \mathcal{N}(\mathfrak{a})^{-1},$$

and (ii) holds.

By Dirichlet's unit theorem, if $\sigma_1,\ldots,\sigma_{r_1}$ correspond to real embeddings of κ into $\mathbb{R}$ and $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}},\ldots,\sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$ correspond to the complex embeddings of κ into $\mathbb{C}$, then given any $c_1,\ldots,c_{r_1+r_2}$, there exists a unit η such that

$$c_i|\sigma_i(\eta)| \le c_j c(\kappa)|\sigma_j(\eta)|$$

for $1 \le i,j \le r_1+r_2$ and some constant $c(\kappa)$. To prove (iii), it suffice to show

$$|\sigma_i(\xi)| \le c(\kappa)|\sigma_j(\xi)|,$$

and this can be deduced by multiplying ξ by a suitable unit η. □

4.1.2 Heights on number fields

We define the *height* of an element x of the number field κ to be the height of the point $[1,x]$ in $\mathbb{P}^1(\kappa) = \mathbb{P}(\kappa^2)$, so that we have

$$H_\kappa(x) = \Big(\prod_{v\in M_\kappa^\infty} \Big(\sqrt{1+|x|_v^2}\Big)^{n_v}\Big)\Big(\prod_{v\in M_\kappa - M_\kappa^\infty} \max\big\{1,|x|_v^{n_v}\big\}\Big),$$

$$H_{*,\kappa}(x) = \prod_{v\in M_\kappa} \max\big\{1,|x|_v^{n_v}\big\},$$

and similarly for $H(x)$, $H_*(x)$, $h(x)$ and $h_*(x)$. We see that if $x \ne 0$, then

$$H_\kappa(x) = H_\kappa(x^{-1}), \quad H_{*,\kappa}(x) = H_{*,\kappa}(x^{-1}).$$

Furthermore, we have trivially

$$H_{*,\kappa}(x_1\cdots x_n) \le H_{*,\kappa}(x_1)\cdots H_{*,\kappa}(x_n)$$

and for $x \in \kappa$,

$$H_{*,\kappa}(x^n) = H_{*,\kappa}(x)^n.$$

For $x \ne 0$, $h_*(x) = 0$ if and only if x is a root of unity (see [144]).

For the proof of Roth's theorem, we will need the *Liouville's inequality*:

Lemma 4.4. *Let κ be a number field, let x be a nonzero element of κ, and let $S \subset M_\kappa$ be any set of absolute values on κ. Then*

$$\prod_{v\in S} \min\{1, \|x\|_v\} \geq \frac{1}{H_{*,\kappa}(x)}.$$

Proof. Using the product formula, we compute

$$\begin{aligned} H_{*,\kappa}(x) &= \prod_{v\in M_\kappa} \max\{1, \|x\|_v\} = \prod_{v\in M_\kappa} \|x\|_v \max\left\{1, \frac{1}{\|x\|_v}\right\} \\ &= \prod_{v\in M_\kappa} \max\left\{1, \frac{1}{\|x\|_v}\right\} = \prod_{v\in M_\kappa} \frac{1}{\min\{1, \|x\|_v\}} \\ &\geq \prod_{v\in S} \frac{1}{\min\{1, \|x\|_v\}}. \end{aligned}$$

Taking reciprocals gives the desired result. □

Proposition 4.5. *Take $x \in \kappa_*$ and let $(x) = \mathfrak{b}/\mathfrak{d}$ be an ideal factorization for x where $\mathfrak{b}$, $\mathfrak{d}$ are relatively prime ideals in $\mathcal{O}_\kappa$. Then*

$$H_{*,\kappa}(x) = \mathcal{N}(\mathfrak{d}) \prod_{v\in M_\kappa^\infty} \max\{1, \|x\|_v\}. \tag{4.4}$$

Proof. Indeed, we have

$$\max\{1, \|x\|_v\} > 1$$

for a $\mathfrak{p}$-adic valuation v if and only if $\mathfrak{p}$ divides the denominator $\mathfrak{d}$. Write

$$\mathfrak{d} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

with $a_i > 0$ for each i. We obtain

$$\prod_{v\in M_\kappa^0} \max\{1, \|x\|_v\} = \prod_{i=1}^{r} \mathcal{N}(\mathfrak{p}_i)^{a_i} = \mathcal{N}(\mathfrak{d}),$$

and hence (4.4) follows from definition. □

Proposition 4.6. *Suppose that α is algebraic of degree d over the rational numbers, and let*

$$f(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0 = 0, \;\; a_d > 0,$$

be its irreducible equation, with coefficients $a_i \in \mathbb{Z}$, and $\gcd(a_0, \ldots, a_d) = 1$. If $\kappa = \mathbb{Q}(\alpha)$, then one has the formula

$$H_{*,\kappa}(\alpha) = a_d \prod_{i=1}^{d} \max\{1, \|\alpha_i\|_\infty\}, \tag{4.5}$$

where $\alpha_1, \ldots, \alpha_d$ are the distinct conjugates of α in $\mathbb{C}$.

Proof. Indeed,

$$\prod_{v\in M_\kappa^\infty} \max\{1, \|\alpha\|_v\} = \prod_{i=1}^{d} \max\{1, \|\alpha_i\|_\infty\}.$$

By using the standard Gauss lemma, which will be recalled in the next section, we see

$$|f|_v = |a_d|_v \prod_{j=1}^{d} \max\{1, |\alpha_j|_v\}$$

for $v \in M_\kappa^0$. However, by definition,

$$|f|_v = \max_{0\le j\le d} |a_j|_v = 1,$$

and hence

$$\begin{aligned} 1 &= \prod_{v\in M_\kappa^0} |f|_v^{n_v} = \prod_{v\in M_\kappa^0} \left(\|a_d\|_v \prod_{j=1}^{d} \max\{1, \|\alpha_j\|_v\} \right) \\ &= \prod_{p\in M_\mathbb{Q}^0} \left(|\mathbf{N}_{\kappa/\mathbb{Q}}(a_d)|_p \prod_{j=1}^{d} \max\{1, |\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha_j)|_p\} \right) \\ &= a_d^{-d} \prod_{p\in M_\mathbb{Q}^0} \max\{1, |\mathbf{N}_{\kappa/\mathbb{Q}}(\alpha)|_p^d\} = a_d^{-d} \prod_{v\in M_\kappa^0} \max\{1, \|\alpha\|_v^d\}, \end{aligned}$$

that is,

$$\prod_{v\in M_\kappa^0} \max\{1, \|\alpha\|_v\} = a_d.$$

Therefore (4.5) follows from definition of the height. □

Theorem 4.7 (cf. [144]). *Let κ be a number field. Let $a = r_1 + r_2 - 1$ where r_1 is the number of real absolute values and r_2 the number of complex ones.*

(1) *The number of algebraic integers $x \in \mathcal{O}_\kappa$ with height $H_{*,\kappa}(x) \le r$ is*

$$c_0 r(\log r)^a + O\left(r(\log r)^{a-1}\right)$$

for some constant c_0.

(2) *The number of units $\eta \in \mathcal{O}_\kappa$ with $H_{*,\kappa}(\eta) \le r$ is*

$$c_1(\log r)^a + O\left((\log r)^{a-1}\right)$$

for some constant c_1.

Recall that we will use $O(1)$ to denote a *bounded function*. Generally, if $h(r)$ is a non-negative function, we will denote

$$O(h(r)) := O(1)h(r).$$

We also use the symbol $o(h(r))$ to denote a function such that $o(h(r))/h(r) \to 0$ as $r \to \infty$.

Lemma 4.8 (cf. [233]). *Let κ be a number field of degree $n = [\kappa : \mathbb{Q}]$. Fix a positive number $r \in \mathbb{R}$ with $r \geq 1$ and take $x \in \kappa$ such that $H_*(x) \leq r$. Then there exist an $\alpha \in \mathcal{O}_\kappa$ and an $m \in \mathbb{Z}$ such that $x = \frac{\alpha}{m}$ and $0 < m \leq r^n$.*

Proof. By the theorem on the unique prime ideal decomposition, we can write the fractional ideal (x) in the form $(x) = \mathfrak{b}/\mathfrak{d}$, where $\mathfrak{b}$, $\mathfrak{d}$ are relatively prime ideals in $\mathcal{O}_\kappa$. Denote by m the norm of $\mathfrak{d}$: $\mathcal{N}(\mathfrak{d}) = m$. Then m is a positive integer and the principal ideal (m) is divisible by $\mathfrak{d}$. There exists an integral ideal $\mathfrak{m}$ such that $(m) = \mathfrak{d}\mathfrak{m}$, and hence

$$(x) = \mathfrak{b}\mathfrak{m}(m)^{-1},$$

which means that $\mathfrak{b}\mathfrak{m}$ is a principal ideal. Denoting its generator by β we have

$$(x) = (\beta)(m)^{-1}.$$

Hence the first assertion of the lemma follows by taking $\alpha = \eta\beta$ for a suitable unit η.

By Proposition 4.5, we have

$$m = \mathcal{N}(\mathfrak{d}) \leq H_{*,\kappa}(x) = H_*(x)^n,$$

and hence the lemma is proved. □

For $x \in \kappa$, we denote by $x^{(i)}$ the conjugates of x, $1 \leq i \leq n$, and set

$$T_2(x) = \sum_{i=1}^{n} \left|x^{(i)}\right|^2.$$

Theorem 4.9 (cf. [233]). *Let κ be a number field of degree $n = [\kappa : \mathbb{Q}]$. Let $\{w_1, \ldots, w_n\}$ be a basis of $\mathcal{O}_\kappa$ over $\mathbb{Z}$. Fix a positive number $r \in \mathbb{R}$ with $r \geq 1$. Then any $x \in \kappa$ with $H_*(x) \leq r$ can be represented in the form*

$$x = \frac{x_1 w_1 + \cdots + x_n w_n}{m}$$

with $x_1, \ldots, x_n, m \in \mathbb{Z}$, satisfying $0 < m \leq r^n$ and

$$|x_i| \leq \frac{r^n m\sqrt{n}}{\sqrt{|D_{\kappa/\mathbb{Q}}|}} \prod_{j \neq i} \sqrt{T_2(w_j)}, \quad i = 1, \ldots, n.$$

Proof. By Lemma 4.8, there exist an algebraic integer $\alpha \in \mathcal{O}_\kappa$ and a rational integer $m \in \mathbb{Z}$ such that $x = \alpha/m$ and $0 < m \leq r^n$. The assumption $H_*(x) \leq r$ implies that

$$|x|_v \leq r^{n/n_v} \leq r^n, \ \ v \in M_\kappa,$$

and hence

$$|\alpha|_v \leq r^n |m|_v.$$

If we consider Archimedean absolute values and interpret the $\alpha^{(k)}$ as complex numbers, we see that all conjugates of α satisfy the inequality

$$|\alpha|_v = \left|\alpha^{(k)}\right| \leq r^n m,$$

and hence

$$\left(\sum_{k=1}^{n} \left|\alpha^{(k)}\right|^2\right)^{1/2} \leq \left(\sum_{k=1}^{n} r^{2n} m^2\right)^{1/2} = r^n m\sqrt{n}.$$

We choose an integral basis $\{w_1, \ldots, w_n\}$ of $\mathcal{O}_\kappa$. Then α can be written in the form

$$\alpha = x_1 w_1 + \cdots + x_n w_n$$

with $x_i \in \mathbb{Z}$. Taking conjugates and using Cramer's rule we see that

$$x_i = \frac{a_i}{\sqrt{|D_{\kappa/\mathbb{Q}}|}}, \ \ i = 1, \ldots, n,$$

where

$$a_i = \begin{vmatrix} w_1^{(1)} & \cdots & \alpha^{(1)} & \cdots & w_n^{(1)} \\ \vdots & & \vdots & & \vdots \\ w_1^{(n)} & \cdots & \alpha^{(n)} & \cdots & w_n^{(n)} \end{vmatrix}$$

is the determinant of the matrix $(w_j^{(k)})$, where the i-th column is replaced by the vector $(\alpha^{(k)})$. By using Hadamard inequality for a_i, we obtain the estimate:

$$\begin{aligned} |a_i| &\leq \left(\sum_{k=1}^{n} \left|\alpha^{(k)}\right|^2\right)^{1/2} \prod_{j \neq i} \left(\sum_{k=1}^{n} \left|w_j^{(k)}\right|^2\right)^{1/2} \\ &= \left(\sum_{k=1}^{n} \left|\alpha^{(k)}\right|^2\right)^{1/2} \prod_{j \neq i} \sqrt{T_2(w_j)}, \end{aligned}$$

and this proves the theorem. □

It is an old conjecture of Lehmer [156] that when α is of degree d over $\mathbb{Q}$, and is not 0 or a root of unity, then

$$h_*(\alpha) \geq \frac{\log \alpha_0}{d} \tag{4.6}$$

where $\alpha_0 = 1.1762808\cdots$ is the larger real root of the 10th-degree *Lehmer polynomial*

$$L(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1. \tag{4.7}$$

Of special interest to Lehmer were *palindromic polynomials* (also sometimes called *reciprocal* or *symmetric* polynomials): these are polynomials $P(x) \in \mathbb{Z}[x]$ that satisfy

$$P(x) = x^m P\left(\frac{1}{x}\right),$$

where m is the degree of $P(x)$. A nonlinear irreducible palindromic polynomial must have even degree since palindromic polynomials of odd degree always have -1 as a root. Obviously, $L(x)$ is a palindromic polynomial.

Note that

$$h_*\left(2^{1/d}\right) = \frac{\log 2}{d}.$$

The example shows that (4.6) would be best possible on the order of d. The best result in this direction is due to Dobrowolski [51] and says that if $d \geq 3$, then

$$h_*(\alpha) > \frac{c}{d}\left(\frac{\log\log d}{\log d}\right)^3 \tag{4.8}$$

with an absolute constant $c > 0$.

In contrast, there is the following result of Zhang [308]: Suppose α is algebraic but not 0, 1, $(1 \pm \sqrt{-3})/2$. Then

$$h_*(\alpha) + h_*(1-\alpha) \geq c > 0 \tag{4.9}$$

with an absolute constant $c > 0$. Zagier [304] gave a more natural proof and determined the best value of the constant

$$c = \frac{1}{2}\log\frac{1+\sqrt{5}}{2}.$$

4.1.3 Functional properties of heights

Proposition 4.10. *The action of the Galois group on $\mathbb{P}^n(\bar{\mathbb{Q}})$ leaves the height invariant. In other words, let $x \in \mathbb{P}^n(\bar{\mathbb{Q}})$ and let $\sigma \in G_{\bar{\mathbb{Q}}/\mathbb{Q}}$. Then $H(\sigma(x)) = H(x)$.*

Proof. Let $\kappa/\mathbb{Q}$ be a number field with $x \in \mathbb{P}^n(\kappa)$. The automorphism σ of $\bar{\mathbb{Q}}$ defines an isomorphism $\sigma : \kappa \longrightarrow \sigma(\kappa)$, and it likewise identifies the sets of absolute values on κ and $\sigma(\kappa)$. More precisely, σ induces an isomorphism

$$\sigma : M_\kappa \longrightarrow M_{\sigma(\kappa)},$$

where for $\mathfrak{p} \in M_\kappa$, the absolute value $\sigma(\mathfrak{p}) \in M_{\sigma(\kappa)}$ is defined by

$$|\sigma(a)|_{\sigma(\mathfrak{p})} = |a|_{\mathfrak{p}}, \;\; a \in \kappa.$$

It is also clear that σ induces an isomorphism on the completions, $\kappa_{\mathfrak{p}} \cong \sigma(\kappa)_{\sigma(\mathfrak{p})}$, so $n_{\mathfrak{p}} = n_{\sigma(\mathfrak{p})}$. Take $\xi \in \kappa^{n+1} - \{0\}$ with $x = [\xi]$. This allows us to compute

$$\begin{aligned} H_{\sigma(\kappa)}(\sigma(x)) &= \prod_{\mathfrak{P} \in M_{\sigma(\kappa)}} |\sigma(\xi)|_{\mathfrak{P}}^{n_{\mathfrak{P}}} = \prod_{\mathfrak{p} \in M_\kappa} |\sigma(\xi)|_{\sigma(\mathfrak{p})}^{n_{\sigma(\mathfrak{p})}} \\ &= \prod_{\mathfrak{p} \in M_\kappa} |\xi|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = H_\kappa(x). \end{aligned}$$

We also have

$$[\kappa : \mathbb{Q}] = [\sigma(\kappa) : \mathbb{Q}],$$

so taking $[\kappa : \mathbb{Q}]$th roots gives the desired result. □

Example 4.11. Let $S_{m,n}$ be the Segre embedding described in Example 3.31. Then

$$h_*(S_{m,n}(x, y)) = h_*(x) + h_*(y), \quad x \in \mathbb{P}^m, \;\; y \in \mathbb{P}^n.$$

By using heights, one can describe completely growth of morphisms between projective spaces (cf. [144], [98], [256]).

Lemma 4.12. *Let $f : \mathbb{P}^m \longrightarrow \mathbb{P}^n$ be a rational mapping of degree d defined over $\bar{\mathbb{Q}}$. Let I_f denote the indeterminacy lotus of f. Then there exists a constant c satisfying*

$$h(f(x)) \leq dh(x) + c$$

for all $x \in \mathbb{P}^m - I_f$.

Proof. Note that $f = \mathbb{P}(\tilde{f})$ can be given by an $(n+1)$-tuple $\tilde{f} = (f_0, \ldots, f_n)$ of homogeneous polynomials of degree d with coefficients in some number field κ, and in $m+1$ variables $X_0, \ldots, X_m$. Let $A = \mathbb{P}^m - I_f$ be the set of points $x = [x_0, \ldots, x_m]$ in projective space $\mathbb{P}^m$ such that not all polynomials $f_i(x)$ vanish, $i = 0, \ldots, n$. Then $f : A \longrightarrow \mathbb{P}^n$ is a morphism. Trivial estimates using the triangle inequality show that for any point $x \in \mathbb{P}^m(\kappa) - I_f$, we have

$$H_\kappa(f(x)) \leq C^{[\kappa:\mathbb{Q}]} H_\kappa(x)^d.$$

Taking the $[\kappa : \mathbb{Q}]$ root and the logarithm yield the lemma. □

Theorem 4.13. *Let $f : \mathbb{P}^m \longrightarrow \mathbb{P}^n$ be a rational mapping of degree d defined over $\bar{\mathbb{Q}}$. Let I_f denote the indeterminacy lotus of f and let X be a closed subvariety of $\mathbb{P}^m$ with the property that $X \cap I_f = \emptyset$. Then*

$$h(f(x)) = dh(x) + O(1), \;\; x \in X.$$

Proof. One inequality was proved in Lemma 4.12. Next we prove the inequality in the other direction. Note that f defines a morphism $X \longrightarrow \mathbb{P}^n$. Fix a field of definition κ for f, so f is given in homogeneous coordinates by $[f_0, \ldots, f_n]$, where the homogeneous polynomials $f_0, \ldots, f_n$ of degree d in the variables $X_0, \ldots, X_m$ have coefficients in the number field κ.

Let $g_1, \ldots, g_r$ be homogeneous polynomials generating the ideal of X. Then we know that $g_1, \ldots, g_r, f_0, \ldots, f_n$ have no common zeros in $\mathbb{P}^m$. By Theorem 1.48, there exist polynomials $a_{ij}, b_{ij} \in \bar{\mathbb{Q}}[X_0, \ldots, X_m]$ and a non-negative integer l such that

$$X_i^{d+l} = \sum_{j=1}^{r} a_{ij} g_j + \sum_{j=0}^{n} b_{ij} f_j, \;\; 0 \leq i \leq m.$$

Disregarding the monomials in b_{ij} of degree $\neq l$, we can assume without loss of generality that b_{ij} is homogeneous of degree l. Extending κ if necessary, we may also assume that the a_{ij}'s, b_{ij}'s and g_j's have coefficients in κ.

It is also convenient to clear denominators, so we pick an element a in κ, integral at all valuations of M_κ such that a is a denominator for all coefficients of the polynomials b_{ij}. Multiplying by a, we may assume without loss of generality that we have the equation

$$aX_i^{d+l} = \sum_{j=1}^{r} a_{ij} g_j + \sum_{j=0}^{n} b_{ij} f_j,$$

where the coefficients of b_{ij} are integral in κ. Take

$$x = [x_0, \ldots, x_m] \in X(\kappa)$$

with x_i integral in κ. The assumption that $x \in X$ implies that $g_j(x) = 0$ for all j, so when we evaluate the above formula at x we obtain

$$ax_i^{d+l} = \sum_{j=0}^{n} b_{ij}(x) f_j(x), \;\; 0 \leq i \leq m.$$

Take $\alpha \in \{0, \ldots, m\}$ such that

$$|x_\alpha|_v = \max_i |x_i|_v.$$

If $v \in M_\kappa$ is non-Archimedean, then

$$|a|_v |x_\alpha|_v^{d+l} \leq |x_\alpha|_v^l \max_j |f_j(x)|_v,$$

whence

$$|a|_v^{n_v} \max_i |x_i|_v^{(d+l)n_v} \le \max_i |x_i|_v^{ln_v} \max_j |f_j(x)|_v^{n_v}.$$

If $v \in M_\kappa$ is Archimedean, then

$$|a|_v |x_\alpha|_v^{d+l} \le (n+1)\binom{m+l}{l} C_v |x_\alpha|_v^l \max_j |f_j(x)|_v,$$

where C_v is a constant giving the bound for the coefficients of the polynomials $b_{\alpha j}$ $(j = 0, \dots, n)$. Taking the product yields

$$H_\kappa(x)^{d+l} \le C H_\kappa(x)^l H_\kappa(f(x)),$$

where

$$C = \prod_{v \in M_\kappa^\infty} \left\{ (n+1)\binom{m+l}{l} C_v \right\}^{n_v},$$

so taking logarithms gives the desired inequality. □

Corollary 4.14. *Let P and Q be two coprime polynomials in $\bar{\mathbb{Q}}[X]$. Then we have*

$$h\left(\frac{P(x)}{Q(x)}\right) = \max\{\deg(P), \deg(Q)\} h(x) + O(1). \tag{4.10}$$

4.2 Heights of polynomials

4.2.1 Coefficients for polynomials

We assume that κ is a number field. Let M_κ be a proper set of absolute values on κ with multiplicities n_v. An element f in the ring $\kappa[X_1, \dots, X_n]$ can be written as a sum

$$f(\mathbf{X}) = \sum_{\mathbf{i} \in I} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}},$$

where I is a finite set of distinct elements in $\mathbb{Z}_+^n$, $a_{\mathbf{i}} \in \kappa$, $\mathbf{X} = (X_1, \dots, X_n)$, and

$$\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_n^{i_n}, \ \ \mathbf{i} = (i_1, \dots, i_n) \in \mathbb{Z}_+^n.$$

We will use the symbols

$$\partial_{\mathbf{i}} f = \frac{1}{i_1! \cdots i_n!} \cdot \frac{\partial^{|\mathbf{i}|} f}{\partial X_1^{i_1} \cdots \partial X_n^{i_n}},$$

where $|\mathbf{i}| = i_1 + \cdots + i_n$ is the *length of index* $\mathbf{i}$. We also write $\deg_{X_h}(f)$ for the degree of f on the variable X_h.

If we define the *Gauss norm*

$$|f|_v = \begin{cases} \left(\sum_{\mathbf{i}\in I} |a_{\mathbf{i}}|_v^2\right)^{\frac{1}{2}}, & \text{if } v \text{ is Archimedean,} \\ \max\limits_{\mathbf{i}\in I}\{|a_{\mathbf{i}}|_v\}, & \text{if } v \text{ is non-Archimedean} \end{cases}$$

or

$$|f|_{*,v} = \max_{\mathbf{i}\in I}\{|a_{\mathbf{i}}|_v\},$$

the (*projective*) *relative* (*multiplicative*)*height* of f (relate to κ) is defined to be the height of its coefficients taken as homogeneous coordinates:

$$H_\kappa(f) = \prod_{v\in M_\kappa} |f|_v^{n_v},$$

or

$$H_{*,\kappa}(f) = \prod_{v\in M_\kappa} |f|_{*,v}^{n_v}.$$

The (*projective*) *absolute* (*multiplicative*) *height* are defined by

$$H(f) = H_\kappa(f)^{\frac{1}{[\kappa:\mathbb{Q}]}}, \quad H_*(f) = H_{*,\kappa}(f)^{\frac{1}{[\kappa:\mathbb{Q}]}}.$$

Thus the (*projective*) *absolute* (*logarithmic*) *heights* can be defined by

$$h(f) = \log H(f), \quad h_*(f) = \log H_*(f).$$

It is easy to show

$$|f|_{*,v} \le |f|_v \le \varsigma_{v,\binom{n+d}{d}} |f|_{*,v},$$

where $d = \deg(f)$, and so

$$H_*(f) \le H(f) \le \binom{n+d}{d}^{\frac{1}{2}} H_*(f).$$

If σ is an isomorphism of κ over $\mathbb{Q}$ then we get the polynomial

$$\sigma(f) = \sum_{\mathbf{i}\in I} \sigma(a_{\mathbf{i}}) X^{\mathbf{i}},$$

and thus, as for points, we have

$$H(\sigma(f)) = H(f), \quad H_*(\sigma(f)) = H_*(f).$$

For some applications, it is more convenient to use the (*affine*) *relative* (*multiplicative*) *height* of f (relate to κ)

$$H_{\vee,\kappa}(f) = \prod_{v\in M_\kappa} \max\{1, |f|_{*,v}^{n_v}\},$$

the (*affine*) *absolute* (*multiplicative*) *height*)

$$H_\vee(f) = H_{\vee,\kappa}(f)^{\frac{1}{[\kappa:\mathbb{Q}]}},$$

and the (*affine*) *absolute* (*logarithmic*) *height*

$$h_\vee(f) = \log H_\vee(f).$$

Lemma 4.15. *Let $f(X_1,\dots,X_n) \in \mathbb{Z}[X_1,\dots,X_n]$ be a polynomial with integer coefficients, and let $\mathbf{i} = (i_1,\dots,i_n)$ be an n-tuple of nonnegative integers. Then $\partial_{\mathbf{i}} f \in \mathbb{Z}[X_1,\dots,X_n]$. Further, if $\deg_{X_h}(f) \le r_h$ for each $h = 1,\dots,n$, then*

$$|\partial_{\mathbf{i}} f|_* \le 2^{r_1+\cdots+r_n}|f|_*.$$

Proof. Differentiating f, we obtain

$$\begin{aligned}\partial_{\mathbf{i}} f &= \sum_{\mathbf{j}\in\mathbb{Z}_+^n} a_{\mathbf{j}}\partial_{\mathbf{i}}\mathbf{X}^{\mathbf{j}} = \sum_{\mathbf{j}\in\mathbb{Z}_+^n} a_{\mathbf{j}}\frac{1}{i_1!}\frac{\partial^{i_1}X_1^{j_1}}{\partial X_1^{i_1}}\cdots\frac{1}{i_n!}\frac{\partial^{i_n}X_n^{j_n}}{\partial X_n^{i_n}}\\ &= \sum_{\mathbf{j}\in\mathbb{Z}_+^n} a_{\mathbf{j}}\binom{j_1}{i_1}\cdots\binom{j_n}{i_n}X_1^{j_1-i_1}\cdots X_n^{j_n-i_n}.\end{aligned}$$

The combinatorial symbols are integers, so this proves the first part of Lemma 4.15.

To prove the second part, we use the binomial formula for $(1+1)^j$ to estimate

$$\binom{j}{i} \le \sum_{l=0}^{j}\binom{j}{l} = (1+1)^j = 2^j.$$

Hence taking the maximum over all n-tuples $\mathbf{j} = (j_1,\dots,j_n)$ of integers satisfying

$$0 \le j_1 \le r_1,\ \dots,\ 0 \le j_n \le r_n,$$

we obtain

$$\begin{aligned}|\partial_{\mathbf{i}} f|_* &= \max\left|a_{\mathbf{j}}\binom{j_1}{i_1}\cdots\binom{j_n}{i_n}\right|\\ &\le \max|a_{\mathbf{j}}|\cdot\max 2^{j_1+\cdots+j_n} = 2^{r_1+\cdots+r_n}|f|_*.\end{aligned}$$

This completes the proof of second part in Lemma 4.15. □

Lemma 4.16. *Let $f \in \mathbb{Z}[X_1,\dots,X_n]$ with $\deg_{X_h}(f) \le r_h$, and let $\mathbf{x} = (x_1,\dots,x_n)$ be an n-tuple of algebraic numbers in a number field κ. Then for all n-tuples of nonnegative integers $\mathbf{i} = (i_1,\dots,i_n)$ we have*

$$H_{*,\kappa}(\partial_{\mathbf{i}} f(\mathbf{x})) \le 4^{(r_1+\cdots+r_n)[\kappa:\mathbb{Q}]}H_{*,\kappa}(f)\prod_{h=1}^{n}H_{*,\kappa}(x_h)^{r_h}.$$

Proof. Let $\mathbf{j} = (j_1, \ldots, j_n)$ be any n-tuple of nonnegative integers. Lemma 4.15 tells us that $\partial_{\mathbf{j}}\partial_{\mathbf{i}} f$ has integer coefficients that are bounded by

$$|\partial_{\mathbf{j}}\partial_{\mathbf{i}} f|_* \leq 2^{r_1+\cdots+r_n}|\partial_{\mathbf{i}} f|_* \leq 4^{r_1+\cdots+r_n}|f|_*.$$

If $v \in M_\kappa^\infty$, we have

$$\begin{aligned} |\partial_{\mathbf{i}} f(\mathbf{x})|_v &\leq (r_1+1)\cdots(r_n+1)|\partial_{\mathbf{i}} f|_* \max\{1,|x_1|_v\}^{r_1}\cdots\max\{1,|x_n|_v\}^{r_n} \\ &\leq 4^{r_1+\cdots+r_n}|f|_* \max\{1,|x_1|_v\}^{r_1}\cdots\max\{1,|x_n|_v\}^{r_n}. \end{aligned}$$

If v is non-Archimedean, we can obtain the stronger bound

$$|\partial_{\mathbf{i}} f(\mathbf{x})|_v \leq \max\{1,|x_1|_v\}^{r_1}\cdots\max\{1,|x_n|_v\}^{r_n}$$

since $\partial_{\mathbf{i}} f$ has integer coefficients. Thus

$$\begin{aligned} H_{*,\kappa}(\partial_{\mathbf{i}} f(\mathbf{x})) &= \prod_{v\in M_\kappa} \max\{1,|\partial_{\mathbf{i}} f(\mathbf{x})|_v\}^{n_v} \\ &\leq 4^{(r_1+\cdots+r_n)[\kappa:\mathbb{Q}]} H_{*,\kappa}(f)\prod_{h=1}^{n} H_{*,\kappa}(x_h)^{r_h}, \end{aligned}$$

and so the lemma is proved. □

If v is non-Archimedean, Gauss' lemma (cf. [144]) for valuations then asserts that $|\cdot|_v$ is a valuation.

Lemma 4.17. *Take $f, g \in \kappa[X_1, \ldots, X_n]$. If v is a non-trivial non-Archimedean valuation, then $|fg|_v = |f|_v|g|_v$.*

For a polynomial $f \in \kappa[X_1, \ldots, X_n]$, we write

$$f(\mathbf{X}) = \sum_{\mathbf{i}\in I} a_{\mathbf{i}}\mathbf{X}^{\mathbf{i}} = \sum_{i_1=0}^{d_1}\cdots\sum_{i_n=0}^{d_n} a_{\mathbf{i}} X_1^{i_1}\cdots X_n^{i_n},$$

where $\mathbf{i} = (i_1, \ldots, i_n)$, $d_h = \deg_{X_h}(f)$. We observe that the number N of nonzero monomials appearing in f satisfies

$$\begin{aligned} N &\leq \prod_{h=1}^{n}(d_h+1) \leq \min\left\{\prod_{h=1}^{n} 2^{d_h}, \prod_{h=1}^{n}(2\deg(f)\right\} \\ &\leq \min\left\{2^{\deg(f)}, (2\deg(f))^n\right\}. \end{aligned} \tag{4.11}$$

Lemma 4.18. *Let $\mathcal{F} = \{f_1, \dots, f_p\}$ be a collection of polynomials in $\kappa[X_1, \dots, X_n]$. Then*

$$h_*(f_1 \cdots f_p) \le \sum_{j=1}^{p} h_*(f_j) + \sum_{j=2}^{p} \log \min \left\{ 2^{\deg(f_j)}, (2\deg(f_j))^n \right\}; \tag{4.12}$$

$$h_\vee(f_1 + \cdots + f_p) \le \sum_{j=1}^{p} h_\vee(f_j) + \log p. \tag{4.13}$$

Proof. Write

$$f_j(\mathbf{X}) = \sum_{\mathbf{i}} a_{j\mathbf{i}} \mathbf{X}^{\mathbf{i}}.$$

Then we have

$$f_1(\mathbf{X}) \cdots f_p(\mathbf{X}) = \sum_{\mathbf{i}} \left(\sum_{\mathbf{i}_1 + \cdots + \mathbf{i}_p = \mathbf{i}} a_{1\mathbf{i}_1} \cdots a_{p\mathbf{i}_p} \right) \mathbf{X}^{\mathbf{i}},$$

and hence for any $v \in M_\kappa^\infty$,

$$|f_1 \cdots f_p|_{*,v} = \max_{\mathbf{i}} \left| \sum_{\mathbf{i}_1 + \cdots + \mathbf{i}_p = \mathbf{i}} a_{1\mathbf{i}_1} \cdots a_{p\mathbf{i}_p} \right|_v.$$

We fix a multi-index $\mathbf{i} = (i_1, \dots, i_n)$ and look at the coefficient of $\mathbf{X}^{\mathbf{i}}$:

$$\sum_{\mathbf{i}_1 + \cdots + \mathbf{i}_p = \mathbf{i}} a_{1\mathbf{i}_1} \cdots a_{p\mathbf{i}_p} = \sum_{i_{11} + \cdots + i_{p1} = i_1} \cdots \sum_{i_{1n} + \cdots + i_{pn} = i_n} a_{1\mathbf{i}_1} \cdots a_{p\mathbf{i}_p}. \tag{4.14}$$

If we choose values for $\mathbf{i}_2, \dots, \mathbf{i}_p$, then there is at most one value of $\mathbf{i}_1$ for which $a_{1\mathbf{i}_1} \cdots a_{p\mathbf{i}_p}$ is a term in (4.14). Hence the number $N_{\mathbf{i}}$ of nonzero terms in (4.14) is at most the number of ways to choose $\mathbf{i}_2, \dots, \mathbf{i}_p$ such that $a_{2\mathbf{i}_2}, \dots, a_{p\mathbf{i}_p}$ are all nonzero. Applying (4.11) to each of $f_2, \dots, f_p$, we obtain an estimate

$$N := \max_{\mathbf{i}} N_{\mathbf{i}} \le \prod_{j=2}^{p} \min \left\{ 2^{\deg(f_j)}, (2\deg(f_j))^n \right\}. \tag{4.15}$$

Then we have

$$\begin{aligned} |f_1 \cdots f_p|_{*,v} &\le N \max_{\mathbf{i}} \max_{\mathbf{i}_1 + \cdots + \mathbf{i}_p = \mathbf{i}} \left| a_{1\mathbf{i}_1} \cdots a_{p\mathbf{i}_p} \right|_v \\ &\le N \prod_{j=1}^{p} \max_{\mathbf{i}} \{ |a_{j\mathbf{i}}|_v \} = N \prod_{j=1}^{p} |f_j|_{*,v}. \end{aligned} \tag{4.16}$$

Combining with Lemma 4.17, it follows that

$$h_*(f_1 \cdots f_p) \le \sum_{j=1}^{p} h_*(f_j) + \log N,$$

and so (4.12) follows.

To prove (4.13), now we have

$$f_1(\mathbf{X}) + \cdots + f_p(\mathbf{X}) = \sum_{\mathbf{i}} (a_{1\mathbf{i}} + \cdots + a_{p\mathbf{i}}) \mathbf{X}^{\mathbf{i}},$$

and hence for any $v \in M_\kappa$,

$$\begin{aligned} |f_1 + \cdots + f_p|_{*,v} &= \max_{\mathbf{i}} |a_{1\mathbf{i}} + \cdots + a_{p\mathbf{i}}|_v \\ &\le \varsigma_{v,p}^2 \max_{j,\mathbf{i}} |a_{j\mathbf{i}}|_v = \varsigma_{v,p}^2 \max_j |f_j|_{*,v}. \end{aligned} \tag{4.17}$$

Therefore

$$|f_1 + \cdots + f_p|_{*,v} \le \varsigma_{v,p}^2 \prod_{j=1}^{p} \max\{1, |f_j|_{*,v}\},$$

which easily yield (4.13). □

4.2.2 Gelfand's inequality

To prove a converse inequality of (4.12), we first introduce a multiplicative norm and an L^2-norm on the space of polynomials. For any complex polynomial

$$f(\mathbf{X}) = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}} \in \mathbb{C}[X_1, \ldots, X_n], \tag{4.18}$$

we define the *Mahler measure of* f by

$$\mathrm{Mah}(f) = \exp\left(\int_{I^n} \log \left| f\big(e^{2\pi i t_1}, \ldots, e^{2\pi i t_n}\big) \right| dt_1 \cdots dt_n \right), \tag{4.19}$$

where $I = \mathbb{R}[0, 1]$, $i = \sqrt{-1}$. The *L^2-norm of* f is just the quantity

$$\left(\int_{I^n} \left| f\big(e^{2\pi i t_1}, \ldots, e^{2\pi i t_n}\big) \right|^2 dt_1 \cdots dt_n \right)^{\frac{1}{2}} = \left(\sum_{\mathbf{i}} |a_{\mathbf{i}}|^2 \right)^{\frac{1}{2}} = |f|.$$

Then we have the following simple properties:

Proposition 4.19. *Take* $f, g \in \mathbb{C}[X_1, \ldots, X_n]$ *and suppose that* $\deg_{X_h}(f) \leq d_h$. *Then*

(i) $|f| \leq \{(d_1+1)\cdots(d_n+1)\}^{1/2}|f|_*$;

(ii) $\mathrm{Mah}(fg) = \mathrm{Mah}(f)\mathrm{Mah}(g)$;

(iii) $\mathrm{Mah}(f) \leq |f|$.

Lemma 4.20. *Let* $f \in \mathbb{C}[X_1, \ldots, X_n]$ *be defined by* (4.18) *with* $\deg_{X_h}(f) \leq d_h$. *Then*

$$|a_{\mathbf{i}}| \leq \binom{d_1}{i_1} \cdots \binom{d_n}{i_n} \mathrm{Mah}(f).$$

Proof. The proof is by induction on the number n of variables. For the case $n = 1$, we factor

$$f(X) = a_0 + a_1 X + \cdots + a_d X^d = a_d(X - \alpha_1)\cdots(X - \alpha_d),$$

and note that

$$\int_0^1 \log \left| e^{2\pi i t} - \alpha \right| dt = \log \max\{1, |\alpha|\}. \tag{4.20}$$

Then

$$\begin{aligned} |a_j| &= |a_d| \left| \sum_{h_1 < \cdots < h_{d-j}} \alpha_{h_1} \cdots \alpha_{h_{d-j}} \right| \\ &\leq \binom{d}{j} |a_d| \prod_{h=1}^{d} \max\{1, |\alpha_h|\} = \binom{d}{j} \mathrm{Mah}(f). \end{aligned}$$

To complete the induction, now we give a decomposition of f. Since f has the following form

$$f(X_1, \ldots, X_n) = \sum_{i_1=0}^{d_1} \cdots \sum_{i_n=0}^{d_n} a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n},$$

and if we define

$$f_{i_1 \cdots i_p}(X_{p+1}, \ldots, X_n) = \sum_{i_{p+1}=0}^{d_{p+1}} \cdots \sum_{i_n=0}^{d_n} a_{i_1 \cdots i_p i_{p+1} \cdots i_n} X_{p+1}^{i_{p+1}} \cdots X_n^{i_n}, \ \ 1 \leq p \leq n,$$

where $f_{i_1 \cdots i_n} = a_{\mathbf{i}}$ for the case $p = n$, we obtain

$$f(X_1, \ldots, X_n) = \sum_{i_1=0}^{d_1} f_{i_1}(X_2, \ldots, X_n) X_1^{i_1}, \tag{4.21}$$

and more generally

$$f_{i_1\cdots i_{p-1}}(X_p,\dots,X_n)=\sum_{i_p=0}^{d_p} f_{i_1\cdots i_p}(X_{p+1},\dots,X_n)X_p^{i_p}. \tag{4.22}$$

From (4.21) and the previous lemma in one variable, we deduce that for all $x_2,\dots,x_n\in\mathbb{C}$,

$$|f_{i_1}(x_2,\dots,x_n)|\le\binom{d_1}{i_1}\exp\left(\int_0^1\log\left|f\left(e^{2\pi it_1},x_2,\dots,x_n\right)\right|dt_1\right),$$

and hence

$$\begin{aligned}\log\mathrm{Mah}(f_{i_1}) &= \int_{I^{n-1}}\log\left|f_{i_1}\left(e^{2\pi it_2},\cdots,e^{2\pi it_n}\right)\right|dt_2\cdots dt_n\\ &\le \log\binom{d_1}{i_1}+\int_{I^n}\log\left|f\left(e^{2\pi it_1},\cdots,e^{2\pi it_n}\right)\right|dt_1\cdots dt_n\\ &\le \log\binom{d_1}{i_1}+\log\mathrm{Mah}(f).\end{aligned}$$

This gives the inequality

$$\mathrm{Mah}(f_{i_1})\le\binom{d_1}{i_1}\mathrm{Mah}(f),$$

and more generally, starting from (4.22) and using the same argument, we obtain

$$\mathrm{Mah}(f_{i_1\cdots i_p})\le\binom{d_p}{i_p}\mathrm{Mah}(f_{i_1\cdots i_{p-1}}),$$

which gives the bound

$$|a_{\mathbf{i}}|\le\binom{d_n}{i_n}\mathrm{Mah}(f_{i_1\cdots i_{n-1}})$$

for the coefficients, and now the claim follows by putting together these inequalities.□

Let $\mu(f)$ denote the number of variables $X_1,\dots,X_n$ that genuinely appear in f. Then using the trivial estimate

$$\binom{d}{p}\le 2^{d-1},\ \ d\ge 1,$$

we find

$$|f|_*\le 2^{d_1+\cdots+d_n-\mu(f)}\mathrm{Mah}(f). \tag{4.23}$$

Lemma 4.21. *Let $f_1, \dots, f_p \in \mathbb{C}[X_1, \dots, X_n]$ be polynomials and set*

$$d_h = \deg_{X_h}(f_1 \cdots f_p), \ \ h = 1, \dots, n.$$

Then we have

$$\prod_{j=1}^{p} |f_j|_* \le e^{d_1+\cdots+d_n} |f_1 \cdots f_p|_*. \tag{4.24}$$

Proof. Let $f = f_1 \cdots f_p$ and set $d_{hj} = \deg_{X_h}(f_j)$. Then

$$d_h = \sum_{j=1}^{p} d_{hj}, \quad \mu(f) \le \sum_{j=1}^{p} \mu(f_j),$$

and so

$$\begin{aligned} |f_1|_* \cdots |f_p|_* &\le \prod_{j=1}^{p} 2^{d_{1j}+\cdots+d_{nj}-\mu(f_j)} \mathrm{Mah}(f_j) = 2^{d_1+\cdots+d_n-\sum_j \mu(f_j)} \mathrm{Mah}(f) \\ &\le 2^{d_1+\cdots+d_n-\mu(f)} \{(d_1+1)\cdots(d_n+1)\}^{1/2} |f|_*. \end{aligned}$$

Now we observe that for $d \ge 2$ and for $d = 0$,

$$2^d \sqrt{d+1} \le e^d,$$

while if $d_h = 1$, then the X_h variable contributes to $\mu(f)$. This lets us to obtain the inequality (4.24). □

Lemma 4.17 and Lemma 4.21 yield immediately the *Gelfand's inequality* (cf. [98], Proposition B.7.3):

Lemma 4.22. *Let $d_1, \dots, d_n$ be integers and let $f_1, \dots, f_p \in \bar{\mathbb{Q}}[X_1, \dots, X_n]$ be polynomials whose product satisfies*

$$\deg_{X_h}(f_1 \cdots f_p) \le d_h, \ \ h = 1, \dots, n.$$

Then we have

$$\sum_{j=1}^{p} h_*(f_j) \le h_*(f_1 \cdots f_p) + d_1 + \cdots + d_n.$$

Finally, we make some remarks on the following *Lehmer's question*:

Problem 4.23. Is there a $\delta > 0$ such that the Mahler measure of every irreducible monic polynomial $P(x)$ with integer coefficients is either 1 or larger than $1 + \delta$?

It may be checked that if $P(x)$ is monic and irreducible, then $\mathrm{Mah}(P) = 1$ if and only if $P(x)$ is a cyclotomic polynomial or the monomial x. In [156], Lehmer found the monic palindromic polynomials of degree 2, 4, 6, and 8 with smallest Mahler measure. For degree 10 and higher, the best polynomial Lehmer could find was $L(x)$ defined by (4.7). This polynomial still stands today as the palindromic polynomial with smallest known Mahler measure:

$$\mathrm{Mal}(L) = 1.17628\cdots .$$

If $P(x) \in \mathbb{Z}[x]$ is a monic, irreducible polynomial with

$$1 < \mathrm{Mal}(P) < \mathrm{Mal}(L),$$

then $P(x)$ must be palindromic, since Smyth [259] has shown that $1.32471\cdots$, the unique real root of $S(x) = x^3 - x - 1$, is a lower bound for the set of Mahler measures of non-palindromic polynomials with Mahler measure strictly large than 1.

A *Salem number* is a real algebraic integer α, greater than 1, with the property that all its conjugates lie on or within the unit circle, and at least one conjugate lies on the unit circle. The minimal polynomial of a Salem number α is also called a *Salem polynomial*. Its Mahler measure is clearly just α. It is not difficult to prove that Salem polynomials are always palindromic.

The Lehmer polynomial $L(x)$ defined by (4.7) is a Salem polynomial: it is the minimal polynomial of the Salem number

$$\alpha_0 = 1.17628\cdots = \mathrm{Mah}(L).$$

Thus α_0 is both the smallest known Salem number and the smallest known Mahler measure. In 1996, Voutier [296] obtained a lower bound for the Mahler measures of irreducible monic polynomials $P(x) \in \mathbb{Z}[x]$ in one variable:

Theorem 4.24. *If $P(x)$ is not a cyclotomic polynomial and has degree $d > 1$, then*

$$\log \mathrm{Mah}(P) > \frac{1}{4}\left\{\frac{\log\log d}{\log d}\right\}^3 .$$

4.2.3 Finiteness theorems

Lemma 4.25. *Let $|\cdot|$ be an absolute value on κ which coincides with the ordinary one on $\mathbb{Q}$. Let $f \in \kappa[X]$ be a polynomial of degree d, and let*

$$f(X) = \prod_{i=1}^{d}(X - \alpha_i)$$

be a factorization in $\bar{\kappa}$. We assume that our absolute value is extended to $\bar{\kappa}$. Then

$$5^{-\frac{d}{2}} \prod_{i=1}^{d} \sqrt{1 + |\alpha_i|^2} \le |f| \le 2^{\frac{d-1}{2}} \prod_{i=1}^{d} \sqrt{1 + |\alpha_i|^2}.$$

Proof. The right inequality is trivially proved by induction, estimating the coefficients in a product of a polynomial $g(X)$ by $(X-\alpha)$. We prove the other by induction on the number of indices i such that $|\alpha_i| > 2$. If $|\alpha_i| \leq 2$ for all i, our assertion is obvious. Suppose that

$$f(X) = g(X)(X-\alpha)$$

with $|\alpha| > 2$ and suppose that our assertion is true for

$$g(X) = X^d + b_{d-1}X^{d-1} + \cdots + b_0.$$

We have

$$f(X) = X^{d+1} + \sum_{i=0}^{d}(b_{i-1} - \alpha b_i)X^i,$$

where $b_d = 1,\ b_{-1} = 0$. Then

$$\begin{aligned}
|f| &= \left(1 + \sum_{i=0}^{d}|b_{i-1} - \alpha b_i|^2\right)^{\frac{1}{2}} \geq \left(1 + \sum_{i=0}^{d}(|\alpha b_i| - |b_{i-1}|)^2\right)^{\frac{1}{2}} \\
&\geq \left(1 + \sum_{i=0}^{d}(|\alpha| - 1)(|\alpha||b_i|^2 - |b_{i-1}|^2)\right)^{\frac{1}{2}} \geq (|\alpha| - 1)|g| \\
&\geq \frac{\sqrt{1+|\alpha|^2}}{\sqrt{5}}|g|
\end{aligned}$$

and our lemma is now obvious. □

Lemma 4.26. *Let $|\cdot|$ be an absolute value which coincides with the ordinary one on $\mathbb{Q}$. Take $d \in \mathbb{Z}_+$. If f and g are two polynomials in $\kappa[X_1, \ldots, X_n]$ such that $\deg(f) + \deg(g) \leq d$, then*

$$10^{-d^n/2}|fg| \leq |f||g| \leq 10^{d^n/2}|fg|.$$

Proof. Let us first assume that $f,\ g$ are polynomials in one variable, so we can write

$$f(X) = a\prod_{i=1}^{p}(X - \alpha_i),$$

$$g(X) = b\prod_{j=1}^{q}(X - \beta_j).$$

Without loss of generality, we may assume $a = b = 1$, and that we have extended our absolute value to $\bar{\kappa}$. By Lemma 4.25, we get

$$|f||g| \leq 2^{\frac{d}{2}-1}\left(\prod_{i=1}^{p}\sqrt{1+|\alpha_i|^2}\right)\prod_{j=1}^{q}\sqrt{1+|\beta_j|^2} \leq 2^{\frac{d}{2}-1}5^{\frac{d}{2}}|fg| \leq 10^{\frac{d}{2}}|fg|.$$

Similarly, we can obtain

$$|f||g| \geq 10^{-\frac{d}{2}}|fg|.$$

Now let f be a polynomial in n variables $X_1, \ldots, X_n$ of degree $\leq d$. Then the polynomial in one variable

$$S_d(f)(Y) = f\big(Y, Y^d, \ldots, Y^{d^{n-1}}\big)$$

has the same set of non-zero coefficients as f. Thus, if f and g are two polynomials in n variables $X_1, \ldots, X_n$ such that the sum of their degrees is $\leq d$, then

$$S_d(fg) = S_d(f)S_d(g)$$

has the same non-zero coefficients as fg. From this our reduction of the n-variable case to the 1-variable case is clear. □

From Lemma 4.26 we can deduce analogous results for heights.

Lemma 4.27. *Take $d \in \mathbb{Z}_+$. If f and g are two polynomials in $\kappa[X_1, \ldots, X_n]$ such that $\deg(f) + \deg(g) \leq d$, then*

$$10^{-\frac{d^n}{2}} H(fg) \leq H(f)H(g) \leq 10^{\frac{d^n}{2}} H(fg).$$

Proof. Set

$$\|f\|_v = |f|_v^{n_v}, \ \ v \in M_\kappa.$$

We have

$$H_\kappa(fg) = \prod_{v \in M_\kappa} \|fg\|_v \geq \prod_{v \in M_\kappa} \varsigma_{v,r}^{n_v} \|f\|_v \|g\|_v,$$

where $r = 10^{-d^n}$. Since

$$\sum_{v \in M_\kappa^\infty} n_v = [\kappa : \mathbb{Q}],$$

whence

$$\prod_{v \in M_\kappa} c_{v,r}^{n_v} = 10^{-\frac{d^n}{2}[\kappa:\mathbb{Q}]}$$

and the inequality on the left follows immediately. The one on the right follows in a similar way. □

Let α be algebraic over $\mathbb{Q}$, and let $f(X)$ be its irreducible polynomial over $\mathbb{Q}$. Then

$$f(X) = \prod_{j=1}^{d} (X - \alpha_j),$$

where d is the degree of α over $\mathbb{Q}$ and α_j are the conjugates of α. In view of the above results we get:

Proposition 4.28. *Take $d \in \mathbb{Z}^+$. There exist two numbers $c_1, c_2 > 0$ depending on d, such that if α is algebraic over $\mathbb{Q}$ of degree d, and $f(X)$ is its irreducible polynomial over $\mathbb{Q}$, then*

$$c_1 H(\alpha)^d \leq H(f) \leq c_2 H(\alpha)^d.$$

Recall that the field of definition of a point $x = [\xi_0, \ldots, \xi_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$ is the field

$$\mathbb{Q}(x) = \mathbb{Q}(\xi_0/\xi_i, \xi_1/\xi_i, \ldots, \xi_n/\xi_i)$$

for any i with $x_i \neq 0$. The following finiteness theorem is of fundamental importance for the application of height functions in Diophantine geometry.

Theorem 4.29 ([206], [207]). *Let $d_0,\ r_0$ be two fixed positive numbers. Then the set of points x in $\mathbb{P}^n(\bar{\mathbb{Q}})$ algebraic over $\mathbb{Q}$, and such that*

$$[\mathbb{Q}(x) : \mathbb{Q}] < d_0, \quad H(x) < r_0$$

is finite. In particular, for any fixed number field κ, the set

$$\{x \in \mathbb{P}^n(\kappa) \mid H_\kappa(x) < r_0\}$$

is finite.

Proof. Take a point $x = [\xi_0, \ldots, \xi_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$ of degree d and consider the polynomial

$$f(X_0, \ldots, X_n) = \xi_0 X_0 + \cdots + \xi_n X_n.$$

Then $H(f)$ is the height of the point x. Let

$$g = \prod_\sigma \sigma(f)$$

be the product being taken over all distinct isomorphisms σ of $\bar{\mathbb{Q}}$ over $\mathbb{Q}$. Then g has coefficients in $\mathbb{Q}$, and $H(g),\ H(f)^d$ have the same order of magnitude. We have already seen in Section 4.1 that the number of points with height less than a fixed number, in a projective space, and rational over $\mathbb{Q}$ is bounded. Consequently Theorem 4.29 follows. □

An immediate corollary of the finiteness property in Theorem 4.29 is the following important result due to Kronecker:

Theorem 4.30. *Let κ be a number field, and let $x = [\xi_0, \ldots, \xi_n] \in \mathbb{P}^n(\kappa)$ with $\xi_i \neq 0$ for some i. Then $H_*(x) = 1$ if and only if the ratio ξ_j/ξ_i is a root of unity or zero for every $j \neq i$.*

Proof. Here we follow Hindry and Silverman [98], Corollary B.2.3.1. Without loss of generality, we may divide the coordinates of x by ξ_i and then reorder them, so we may assume that $x = [1, \xi_1, \ldots, \xi_n]$. If every ξ_j is a root of unity, then $|\xi_j|_v = 1$ for every absolute value on κ, and hence $H_*(x) = 1$.

Suppose that $H_*(x) = 1$. Write

$$x^r = [1, \xi_1^r, \ldots, \xi_n^r], \;\; r = 1, 2, \ldots.$$

It is clear from the definition of the height that $H_*(x^r) = H_*(x)^r$, so $H_*(x^r) = 1$ for every $r \geq 1$. But $x^r \in \mathbb{P}^n(\kappa)$, so Theorem 4.29 tells us that the sequence $\{x^r\}$ contains only finitely many distinct points. Choose integers $s > r \geq 1$ such that $x^s = x^r$. This implies that $\xi_j^s = \xi_j^r$ for each $1 \leq j \leq n$. Therefore, each ξ_j is a root of unity or is zero. □

Finally, we introduce a quantitative result related to Theorem 4.29. Let κ be a number field. A real function ν on $\mathbb{P}^n$ will be said to be a *weight function* for κ if $\nu(x) = 0$ for each $x \notin \mathbb{P}^n(\kappa)$. Denote the *center* of absolute height h on $\mathbb{P}^n$ by

$$O = \{x \in \mathbb{P}^n \mid h(x) = 0\}.$$

Take a subset $A \subseteq \mathbb{P}^n$. For $r \geq 0$, set

$$A[O; r] = \{x \in A \mid h(x) \leq r\}.$$

Note that $h(x) = 0$ for $x = [\xi_0, \ldots, \xi_n] \in \mathbb{P}^n(\kappa)$ with $\xi_i \neq 0$ if and only if $\xi_j = 0$ $(j \neq i)$.

Let ν be a weight function on $\mathbb{P}^n$ for κ. Based on Theorem 4.29, we can define the *spherical image* of κ for ν by

$$n_\nu(r) = \sum_{x \in \mathbb{P}^n[O;r]} \nu(x). \tag{4.25}$$

Fix $r_0 > 0$. For $r > r_0$, we define the *characteristic function* of κ for ν by

$$N_\nu(r) = N_\nu(r, r_0) = \int_{r_0}^{r} n_\nu(t) \frac{dt}{t}. \tag{4.26}$$

A basic weight function of κ is the characteristic function

$$\chi_\kappa(x) = \begin{cases} 1, & \text{if } x \in \mathbb{P}^n(\kappa), \\ 0, & \text{if } x \notin \mathbb{P}^n(\kappa). \end{cases} \tag{4.27}$$

We will write

$$n(r, \mathbb{P}^n(\kappa)) = n_{\chi_\kappa}(r). \tag{4.28}$$

Theorem 4.31 ([226]). *Let κ be a number field and set $[\kappa : \mathbb{Q}] = d$. Then there exists a constant $c > 0$ such that*

$$n(r, \mathbb{P}^n(\kappa)) = ce^{d(n+1)r} + \begin{cases} O\left(re^{dr}\right), & \text{if } d = 1,\ n = 1, \\ O\left(e^{(dn+d-1)r}\right), & \text{otherwise.} \end{cases}$$

4.3 Heights on varieties

Let X be a variety defined over $\bar{\mathbb{Q}}$. Let $f : X \longrightarrow \mathbb{P}^n$ be a morphism of X into a projective space, defined over $\bar{\mathbb{Q}}$. Then for each point x of X, if $f(x)$ is a point of $\mathbb{P}^n(\kappa)$, rational over a number field κ, we can thus define its *relative height*

$$H_{f,\kappa}(x) = H_\kappa(f(x)).$$

Generally, we can define the *absolute height*

$$H_f(x) = H(f(x))$$

and the *absolute* (*logarithmic*) *height*

$$h_f(x) = h(f(x)).$$

Theorem 4.32. *Let X be a projective variety defined over $\bar{\mathbb{Q}}$, let $f : X \longrightarrow \mathbb{P}^n$ and $g : X \longrightarrow \mathbb{P}^m$ be morphisms, and let H and L be hyperplanes in $\mathbb{P}^n$ and $\mathbb{P}^m$, respectively. Suppose that f^*H and g^*L are linearly equivalent. Then*

$$h_f(x) = h_g(x) + O(1).$$

Proof. Let $D \in \mathrm{Div}(X)$ be any effective divisor in the linear equivalence class of f^*H and g^*L. The morphisms f and g are determined respectively by certain subspaces V and W in the vector space $\mathcal{L}(D)$ and choices of bases for V and W (see Section 3.4). In other words, if we choose a basis $s_0, \ldots, s_N$ for $\mathcal{L}(D)$, then there are linear combinations

$$f_i = \sum_{j=0}^{N} a_{ij} s_j, \;\; 0 \le i \le n,$$

and

$$g_i = \sum_{j=0}^{N} b_{ij} s_j, \;\; 0 \le i \le m,$$

such that f and g are given by

$$f = [f_0, \ldots, f_n], \quad g = [g_0, \ldots, g_m],$$

where the a_{ij}'s and b_{ij}'s are constants.

Let $\varphi = [s_0, \ldots, s_N] : X \longrightarrow \mathbb{P}^N$ be the morphism corresponding to the complete linear system determined by D. Let $A : \mathbb{P}^N \longrightarrow \mathbb{P}^n$ be the linear mapping defined by the matrix (a_{ij}), and similarly let $B : \mathbb{P}^N \longrightarrow \mathbb{P}^m$ be the linear mapping defined by (b_{ij}). Then we have $f = A \circ \varphi$ and $g = B \circ \varphi$. The mappings A and B are not morphisms on all of $\mathbb{P}^N$, but the fact that f and g are morphisms associated to the

linear system $\mathcal{L}(D)$ implies that A is defined at every point of the image $\varphi(X)$, and similarly for B. Hence we can apply Theorem 4.13 to conclude that

$$h(A(y)) = h(y) + O(1), \quad h(B(y)) = h(y) + O(1)$$

for all $y \in \varphi(X)$. Writing $y = \varphi(x)$ with $x \in X$, we obtain

$$\begin{aligned} h(f(x)) &= h(A(\varphi(x))) = h(\varphi(x)) + O(1) \\ &= h(B(\varphi(x))) + O(1) = h(g(x)) + O(1), \end{aligned}$$

which is the desired result. □

We are now ready to give Weil's construction that associates a height function to every divisor. Let X be a projective variety defined over κ. Take $D \in \mathrm{Div}(X)$. First, suppose that D is very ample. Then we have the associated dual classification mapping $\varphi_D : X \longrightarrow \mathbb{P}(V^*)$, where $V = \mathcal{L}(D)$. The *absolute* (*multiplicative*) *height* of $x \in X$ for D is defined by

$$H_D(x) = H(\varphi_D(x)),$$

and the *absolute* (*logarithmic*) *height* of x for D is defined as

$$h_D(x) = h(\varphi_D(x)) \geq 0.$$

If $\psi : X \longrightarrow \mathbb{P}^m$ is another dual classification mapping associated to D, this means that

$$\varphi_D^* H \sim D \sim \psi^* L,$$

where H is a hyperplane in $\mathbb{P}(V^*)$ and L is a hyperplane in $\mathbb{P}^m$. Now Theorem 4.32 tells us that

$$h(\varphi_D(x)) = h(\psi(x)), \ \ x \in X.$$

Hence for very ample divisors, we can use any associated dual classification mapping to compute the height, up to $O(1)$.

Lemma 4.33 ([144]). *If D and D' are two very ample divisors on X, then*

$$h_{D+D'} = h_D + h_{D'} + O(1).$$

Proof. Let

$$\varphi_D : X \longrightarrow \mathbb{P}^m, \quad \varphi_{D'} : X \longrightarrow \mathbb{P}^n$$

be the associated dual classification mappings. Composing the product

$$\varphi_D \times \varphi_{D'} : X \longrightarrow \mathbb{P}^m \times \mathbb{P}^n$$

with the *Segre mapping* (cf. Example 3.31)

$$S_{m,n} : \mathbb{P}^m \times \mathbb{P}^n \longrightarrow \mathbb{P}^N$$

gives a morphism

$$\varphi_D \otimes \varphi_{D'} : X \longrightarrow \mathbb{P}^N, \ \ \varphi_D \otimes \varphi_{D'}(x) = S_{m,n}(\varphi_D(x), \varphi_{D'}(x)).$$

Since

$$S_{m,n}^* H \sim L \times \mathbb{P}^n + \mathbb{P}^m \times J \in \mathrm{Div}(\mathbb{P}^m \times \mathbb{P}^n),$$

where H, L and J are hyperplanes in $\mathbb{P}^N$, $\mathbb{P}^m$, and $\mathbb{P}^n$, respectively, the morphism $\varphi_D \otimes \varphi_{D'}$ is associated to the divisor $D + D'$, that is,

$$(\varphi_D \otimes \varphi_{D'})^* H \sim D + D'.$$

Since the height for a very ample divisor can be computed using any associated morphism, therefore

$$h_{D+D'}(x) = h(\varphi_D \otimes \varphi_{D'}(x)) + O(1), \ \ x \in X,$$

and hence, by Example 4.11,

$$\begin{aligned} h_{D+D'}(x) &= h(S_{m,n}(\varphi_D(x), \varphi_{D'}(x))) + O(1) \\ &= h(\varphi_D(x)) + h(\varphi_{D'}(x)) + O(1) \\ &= h_D(x) + h_{D'}(x) + O(1). \end{aligned}$$

This gives Lemma 4.33. □

Next, for any divisor $D \in \mathrm{Div}(X)$, we can write $D = E - E'$ where E and E' are very ample, and define

$$h_D = h_E - h_{E'}.$$

This definition depends on the choices of E and E', but by Lemma 4.33, h_D is well defined up to equivalence. In fact, suppose now that we have two decompositions

$$D = E - E' = E_1 - E_1'$$

of a divisor D as the difference of very ample divisors. Then

$$E + E_1' = E' + E_1,$$

and hence Lemma 4.33 yields

$$h_E + h_{E_1'} = h_{E+E_1'} + O(1) = h_{E'+E_1} + O(1) = h_{E'} + h_{E_1} + O(1),$$

which implies

$$h_E - h_{E'} = h_{E_1} - h_{E_1'} + O(1).$$

Basic properties of height functions associated to divisors are summarized in the following Theorem 4.34. This theorem may be viewed as a machine, called *Weil's height machine*, that converts geometric statements described in terms of divisor class relations into arithmetic statements described by relations between height functions.

Theorem 4.34. *For every smooth projective variety X defined over a number field κ, the mapping*

$$h : \mathrm{Div}(X) \longrightarrow \{\textit{functions } X \longrightarrow \mathbb{R}\}$$

has the following properties:

(1) (*Normalization*) *If H is a hyperplane in $\mathbb{P}^n$, then*

$$h_H(x) = h(x) + O(1), \;\; x \in \mathbb{P}^n.$$

(2) (*Functoriality*) *If $f : X \longrightarrow Y$ is a morphism and if $D \in \mathrm{Div}(Y)$, then*

$$h_{f^*D}(x) = h_D(f(x)) + O(1), \;\; x \in X.$$

(3) (*Additivity*) *If $D, D' \in \mathrm{Div}(X)$, then*

$$h_{D+D'}(x) = h_D(x) + h_{D'}(x) + O(1), \;\; x \in X.$$

(4) (*Linear Equivalence*) *If $D, D' \in \mathrm{Div}(X)$ with D linearly equivalent to D', then*

$$h_D(x) = h_{D'}(x) + O(1), \;\; x \in X.$$

(5) (*Positivity*) *If $D \in \mathrm{Div}(X)$ is an effective divisor and if B_D is the base locus of the linear system $|D|$, then*

$$h_D(x) \geq O(1), \;\; x \in X - B_D.$$

(6) (*Algebraic Equivalence*) *If $D, E \in \mathrm{Div}(X)$ with D ample and E algebraically equivalent to 0, then*

$$\lim_{h_D(x) \to \infty} \frac{h_E(x)}{h_D(x)} = 0.$$

(7) (*Finiteness*) *If $D \in \mathrm{Div}(X)$ is ample, then for every finite extension K/κ and every constant r_0, the set*

$$\{x \in X(K) \mid h_D(x) \leq r_0\}$$

is finite.

(8) (*Uniqueness*) *The height functions h_D are determined, up to $O(1)$, by normalization* (1)*, functoriality* (2) *just for embeddings $f : X \longrightarrow \mathbb{P}^n$, and additivity* (3)*.*

Proof. We first check additivity property (3), which we already know for very ample divisors. Now let D and D' be arbitrary divisors, and write them as differences $D = E - E'$ and $D' = E_1 - E'_1$ of very ample divisors. Then $E + E_1$ and $E' + E'_1$ are very ample, so we can compute

$$\begin{aligned} h_{D+D'} &= h_{E+E_1} - h_{E'+E'_1} + O(1) \\ &= h_E + h_{E_1} - h_{E'} - h_{E'_1} + O(1) \\ &= h_D + h_{D'} + O(1). \end{aligned}$$

This completes the proof of additivity (3).

It is now easy to check the property (1). Since the identity $\mathrm{id} : \mathbb{P}^n \longrightarrow \mathbb{P}^n$, $\mathrm{id}(x) = x$, is the associated dual classification mapping φ_H. This gives (1).

To verify (2), we denote $D \in \mathrm{div}(Y)$ as a difference of very ample divisors, $D = E - E'$. Then it follows from Proposition 3.54 that f^*E and f^*E' are base point free, with associated morphisms $\varphi_E \circ f$ and $\varphi_{E'} \circ f$, respectively. Therefore,

$$\begin{aligned} h_{f^*D} &= h_{f^*E} - h_{f^*E'} + O(1) \\ &= h \circ \varphi_E \circ f - h \circ \varphi_{E'} \circ f + O(1) \\ &= h_E \circ f - h_{E'} \circ f + O(1) \\ &= h_D \circ f + O(1). \end{aligned}$$

Let h'_D be other functions associated to divisors D on X which satisfy the normalization (1), functoriality (2) just for embeddings $f : X \longrightarrow \mathbb{P}^n$, and additivity (3). If D is very ample with the associated embedding $\varphi_D : X \longrightarrow \mathbb{P}^n$, then (1) and (2) imply that

$$h'_D = h'_{\varphi_D^* H} + O(1) = h'_H \circ \varphi_D + O(1) = h \circ \varphi_D + O(1),$$

where H is a hyperplane in $\mathbb{P}^n$. Hence

$$h'_D = h_D + O(1).$$

Since any divisor D can be written as the difference $E - E'$ of very ample divisors, so the additivity (3) forces

$$h'_D = h'_E - h'_{E'} + O(1) = h_E - h_{E'} + O(1) = h_D + O(1).$$

This proves the uniqueness property (8) of the height.

Next suppose that $D, D' \in \mathrm{Div}(X)$ are linearly equivalent. Writing $D = E - E'$ and $D' = E_1 - E'_1$ as the difference of very ample divisors as usual, we have $E + E'_1 \sim E' + E_1$. This means that the morphisms $\varphi_{E+E'_1}$ and $\varphi_{E'+E_1}$ are associated to the same linear system, so Theorem 4.32 implies

$$h(\varphi_{E+E'_1}(x)) = h(\varphi_{E'+E_1}(x)), \;\; x \in X.$$

Using this equality and additivity gives

$$h_E + h_{E_1'} = h_{E+E_1'} + O(1) = h_{E'+E_1} + O(1) = h_{E'} + h_{E_1} + O(1).$$

Hence

$$h_D = h_E - h_{E'} + O(1) = h_{E_1} - h_{E_1'} + O(1) = h_{D'} + O(1),$$

which proves (4).

To prove positivity (5), for an effective divisor D, write $D = E - E'$ as a difference of very ample divisors as usual. Choose a basis $f_0, \ldots, f_n$ for $\mathcal{L}(E')$. Then the fact that D is effective implies that

$$E + (f_i) = D + E' + (f_i) \geq 0,$$

so $f_0, \ldots, f_n$ are also in $\mathcal{L}(E)$. We extend this set to form a basis

$$\{f_0, \ldots, f_n, f_{n+1}, \ldots, f_m\} \subset \mathcal{L}(E).$$

These bases give morphisms

$$\varphi_E = [f_0, \ldots, f_m] : X \longrightarrow \mathbb{P}^m, \quad \varphi_{E'} = [f_0, \ldots, f_n] : X \longrightarrow \mathbb{P}^n$$

associated to E and E'. The functions $f_0, \ldots, f_m$ are regular at all points not in the support of E, so for any $x \in X$ with $x \notin \operatorname{supp}(E)$ we can compute

$$\begin{aligned} h_D(x) &= h_E(x) - h_{E'}(x) + O(1) \\ &= h(\varphi_E(x)) - h(\varphi_{E'}(x)) + O(1) \\ &\geq O(1). \end{aligned}$$

The last inequality follows directly from the definition of the height, since the fact that $m \geq n$ clearly yields

$$\prod_{v \in M_\kappa} \|\varphi_E(x)\|_v \geq \prod_{v \in M_\kappa} \|\varphi_{E'}(x)\|_v.$$

This gives the desired estimate for points not in the support of E. Now choose very ample divisors $E_0, E_1, \ldots, E_r$ on X with the property that $E_i + D$ is very ample, and

$$E_0 \cap \cdots \cap E_r = \emptyset.$$

For example, use Proposition 3.53 to find a very ample divisor E' such that $D + E'$ is also very ample, take an embedding $\varphi_{E'} : X \longrightarrow \mathbb{P}^r$ corresponding to E', and take the E_i's to be the pullbacks of the coordinate hyperplanes in $\mathbb{P}^r$. Now we apply our above result to each of the decompositions $D = (D + E_i) - E_i$ to deduce the inequality $h_D \geq O(1)$ for all points not in the support of D. Finally, varying D in its

linear system $|D|$, we obtain the positivity (5) for all points not lying in the base locus of $|D|$.

We will give a proof of the algebraic equivalence (6) using the fact that if D is ample and E is algebraically equivalent to 0, then there is an integer $m > 0$ such that $mD + nE$ is very ample for all integers n (see Lemma 3.49). The height associated to a very ample divisor is nonnegative by construction, so

$$h_{mD+nE}(x) \geq O(1), \;\; x \in X.$$

Using additivity (3), we obtain

$$mh_D(x) + nh_E(x) \geq -c, \;\; x \in X,$$

where the constant c will depend on D, E, m, and n, but is independent of x. This holds for all integers n, so we can rewrite using positive and negative values for n. Thus for any $n \geq 1$ we obtain

$$\frac{m}{n} + \frac{c}{nh_D(x)} \geq \frac{h_E(x)}{h_D(x)} \geq -\frac{m}{n} - \frac{c}{nh_D(x)}, \;\; x \in X.$$

Therefore,

$$\frac{m}{n} \geq \limsup_{h_D(x)\to\infty} \frac{h_E(x)}{h_D(x)} \geq \liminf_{h_D(x)\to\infty} \frac{h_E(x)}{h_D(x)} \geq -\frac{m}{n}.$$

These inequalities hold for all $n \geq 1$, so letting $n \to \infty$, we obtain the desired result.

It remains to prove the finiteness property (7). Note that if we replace the ample divisor D by a very ample multiple mD, then additivity (3) implies that

$$h_{mD} = mh_d + O(1);$$

hence it suffices to prove (7) under the assumption that D is very ample. Let $\varphi_D : X \longrightarrow \mathbb{P}^n$ be an embedding associated to D, so $\varphi_D^* H = D$. Then (1) and (2) imply that

$$h_D = h_{\varphi_D^* H} = h_H \circ \varphi_D + O(1) = h \circ \varphi_D + O(1),$$

so we are reduced to showing that $\mathbb{P}^n(K)$ has finitely many points of bounded height. This follows from Theorem 4.29, which completes the proof of (7), and with it the proof of Theorem 4.34. □

If the variety X is not smooth, Theorem 4.34 is still valid, provided that one works entirely with Cartier divisors, rather than with Weil divisors.

We illustrate the use of the height machine by quickly proving that if D is ample, then h_D is the largest possible height function, up to a constant; i.e. for any other divisor E,

$$h_E \ll h_D + O(1).$$

In fact, by Proposition 3.53, there exists $m > 0$ such that $mD - E$ is very ample, so the properties (3) and (5) in Theorem 4.34 imply

$$O(1) \le h_{mD-E} = mh_D - h_E + O(1),$$

which means

$$h_E \le mh_D + O(1).$$

This is the desired result.

Up to a bounded function, the height h_D associated to a divisor D depends only the divisor class of D. It is sometimes convenient to reformulate Theorem 4.34 purely in terms of divisor classes or line bundles.

Theorem 4.35. *Let X be a projective variety defined over a number field κ. There is a unique homomorphism*

$$h : \mathrm{Pic}(X) \longrightarrow \frac{\{\textit{functions } X \longrightarrow \mathbb{R}\}}{\{\textit{bounded functions } X \longrightarrow \mathbb{R}\}}$$

with the property that if $L \in \mathrm{Pic}(X)$ is very ample and $\varphi_L : X \longrightarrow \mathbb{P}^n$ is an associated embedding, then

$$h_L = h \circ \varphi_L + O(1). \tag{4.29}$$

The height functions h_L have the following additional properties:

(a) (*Functoriality*) *Let $f : X \longrightarrow Y$ be a morphism of smooth varieties, and let $L \in \mathrm{Pic}(Y)$. Then*

$$h_{f^*L} = h_L \circ f + O(1).$$

(b) (*Positivity*) *Let B_L be the base locus of $L \in \mathrm{Pic}(X)$, and assume that $B_L \ne X$. Then*

$$h_L(x) \ge O(1), \ \ x \in X - B_L.$$

(c) (*Algebraic equivalence*) *Let $L, E \in \mathrm{Pic}(X)$ with L ample and E algebraically equivalent to 0. Then*

$$\lim_{h_L(x)\to\infty} \frac{h_E(x)}{h_L(x)} = 0.$$

Proof. All of this is a restatement of Theorem 4.34 in terms of line bundles. Note that the linear equivalence and additivity properties of Theorem 4.34 are included in the statement that the height mapping h is defined and is a homomorphism on $\mathrm{Pic}(X)$ and that we do not need a smoothness hypotheses because $\mathrm{Pic}(X)$ is defined in terms of Cartier divisors. □

Proposition 4.36. *Let C/κ be a smooth projective curve.*

(i) *Let D, $E \in \mathrm{Div}(C)$ be divisors with $\deg(D) \geq 1$. Then*

$$\lim_{h_D(x)\to\infty} \frac{h_E(x)}{h_D(x)} = \frac{\deg(E)}{\deg(D)}.$$

(ii) *Let f, $g \in \bar{\kappa}(C)$ be rational functions on C with f nonconstant. Then*

$$\lim_{h(f(x))\to\infty} \frac{h(g(x))}{h(f(x))} = \frac{\deg(g)}{\deg(f)}.$$

Proof. Set $d = \deg(D)$ and $e = \deg(E)$. For every integer n, we consider the divisor

$$D_n = n(eD - dE) + D.$$

Since $\deg(D_n) = \deg(D) \geq 1$, then Corollary 3.66 implies that D_n is ample. The positivity property of the height machine (Theorem 4.34) implies that $h_{D_n}(x)$ is bounded below for all $x \in C(\bar{\kappa})$. By using the additivity of the height, we find that

$$-c \leq h_{D_n} = n(eh_D - dh_E) + h_D,$$

where $c = c(D, E, n)$ is constant depending only on D, E, and n, and so

$$-\frac{c}{dh_D} \leq n\left(\frac{e}{d} - \frac{h_E}{h_D}\right) + \frac{1}{d}.$$

This holds for positive and negative values of n, so taking both n and $-n$ with $n \geq 1$, we obtain the estimate

$$-\frac{c}{ndh_D} - \frac{1}{nd} \leq \frac{e}{d} - \frac{h_E}{h_D} \leq \frac{c}{ndh_D} + \frac{1}{nd}.$$

Therefore

$$-\frac{1}{nd} \leq \liminf_{h_D(x)\to\infty}\left(\frac{e}{d} - \frac{h_E(x)}{h_D(x)}\right) \leq \limsup_{h_D(x)\to\infty}\left(\frac{e}{d} - \frac{h_E(x)}{h_D(x)}\right) \leq \frac{1}{nd}.$$

These inequalities hold for all $n \geq 1$, so we can let $n \to \infty$ to obtain

$$\lim_{h_D(x)\to\infty}\left(\frac{e}{d} - \frac{h_E(x)}{h_D(x)}\right) = 0.$$

This completes the proof of (i).

To prove (ii), write $\mathrm{div}(f) = D' - D$ and $\mathrm{div}(g) = E' - E$. Note that

$$\deg(f) = \deg(D), \quad \deg(g) = \deg(E).$$

Further, if we consider f to be a mapping $f : C \longrightarrow \mathbb{P}^1$, then $D = f^*(\infty)$, so

$$h_D = h \circ f + O(1).$$

Similarly,

$$h_E = h \circ g + O(1).$$

Now we can use (i) to compute

$$\lim_{h(f(x))\to\infty} \frac{h(g(x))}{h(f(x))} = \lim_{h_D(x)\to\infty} \frac{h_E(x) + O(1)}{h_D(x) + O(1)} = \frac{\deg(E)}{\deg(D)} = \frac{\deg(g)}{\deg(f)}.$$

□

Let X be a projective variety defined over a number field κ. Denote the *center* of absolute height h_D on X relative to some ample divisor D by

$$O = \{x \in X \mid h_D(x) = 0\}.$$

Take a subset $A \subseteq X$. For $r \geq 0$, set

$$A[O; r] = \{x \in A \mid h_D(x) \leq r\}.$$

A real function ν on A will be said to be a *weight function* for κ if $\nu(x) = 0$ for each $x \notin A(\kappa)$.

Assume that $A[O; r]$ is finite for each $r > 0$. Let ν be a weight function on A for κ. We can define the *spherical image* of κ for ν by

$$n_\nu(r) = \sum_{x\in A[O;r]} \nu(x). \tag{4.30}$$

Fix $r_0 > 0$. For $r > r_0$, we define the *characteristic function* of κ for ν by

$$N_\nu(r) = N_\nu(r, r_0) = \int_{r_0}^{r} n_\nu(t)\frac{dt}{t}. \tag{4.31}$$

A basic weight function of κ is the characteristic function

$$\chi_\kappa(x) = \begin{cases} 1, & \text{if } x \in A(\kappa), \\ 0, & \text{if } x \notin A(\kappa). \end{cases} \tag{4.32}$$

The spherical image $n_{\chi_\kappa}(r)$ of κ for χ_κ also is called the *counting function* of $A(\kappa)$, which is also denoted by $n(r, A(\kappa))$. Now we give Néron's description of the counting function of an Abelian variety.

Theorem 4.37. *Let κ be a number field, let A be an Abelian variety over κ, and let $\Gamma \subseteq A(\kappa)$ be a finitely generated group of rank d. Then there exists constant $a > 0$, which depend on A/κ, Γ, and on the height, such that*

$$n(r, \Gamma) = ar^{d/2} + O(r^{(d-1)/2}).$$

Theorem 4.38 (Mumford [195]). *Let κ be a number field, and let C be a curve of genus $g \geq 2$ over κ. Then there exists constant a, which depend on C/κ and on the height, such that for all $r \geq e$,*

$$n(r, C(\kappa)) \leq a \log r.$$

4.4 Heights and Weil functions

In this section, we discuss a class of functions on varieties, called Weil functions, which have logarithmic singularities on a given divisor, and are parameterized by a proper set of absolute values over a number field. Associated to Weil functions of divisors, proximity functions, valence functions and heights are well defined by the divisors, up to $O(1)$.

4.4.1 Weil functions

Let κ be a number field and let M_κ be a set of absolute values satisfying product formula with multiplicities n_v. Take $v \in M_\kappa$. Let κ_v be the completion of κ for v and extend $|\cdot|_v$ to an absolute value on the algebraic closure $\overline{\kappa}_v$. Let D be a Cartier divisor on a variety X, given by a collection $\{(U_i, f_i)\}_{i\in I}$. A *local Weil function* for D relative to v is a function

$$\lambda_{D,v} : X(\overline{\kappa}_v) - \operatorname{supp} D \longrightarrow \mathbb{R}$$

with the following form:

$$\lambda_{D,v}(x) = -\log |||f_i(x)|||_v + u_i(x),$$

where u_i is a continuous function on $U_i(\overline{\kappa}_v)$. We sometimes think of $\lambda_{D,v}$ as a function of $X(\kappa) - \operatorname{supp} D$ or $X(\overline{\kappa}) - \operatorname{supp} D$ by implicitly choosing an embedding $\overline{\kappa} \mapsto \overline{\kappa}_v$.

We define an (*additive*) M_κ*-constant* γ to be a real valued function

$$\gamma : M_\kappa \longrightarrow \mathbb{R}$$

such that $\gamma_v = 0$ for almost all $v \in M_\kappa$ (all but a finite number of v in M_κ). If w is an extension of an element v in M_κ to the algebraic closure $\overline{\kappa}$, then we define

$$\gamma_w = \gamma_v.$$

Thus γ is extended to a function of $M_{\overline{\kappa}}$ into $\mathbb{R}$.

Let X be a variety defined over κ. A subset E of $X(\overline{\kappa}) \times M_{\overline{\kappa}}$ is said to be *affine bounded* if there exists a coordinated affine open subset U of $X(\overline{\kappa})$ with coordinates $(x_1, \ldots, x_m)$ and an $M_{\overline{\kappa}}$-constant γ such that for all $(x, v) \in E$ we have

$$\max_i |x_i|_v \leq e^{\gamma_v}.$$

If there is only one absolute value and κ is algebraically closed, this notion coincides with the notion of a bounded set of points on an affine variety. The subset E is called *bounded* if it is contained in the finite union of affine bounded subsets. In particular, if X is a projective variety, then $X(\overline{\kappa}) \times M_{\overline{\kappa}}$ is bounded (see [144]).

A function

$$u : X(\overline{\kappa}) \times M_{\overline{\kappa}} \longrightarrow \mathbb{R}$$

is called *bounded from above* if there exists an M_κ-constant γ such that

$$u_v(x) \leq \gamma_v, \quad (x, v) \in X(\overline{\kappa}) \times M_{\overline{\kappa}}.$$

We define similarly *bounded from below* and *bounded*. We say that u is *locally bounded* if it is bounded on every bounded subset of $X(\overline{\kappa}) \times M_{\overline{\kappa}}$; and define *locally bounded from above* or *below* similarly. The function u is called *continuous* if for each $v \in M_{\overline{\kappa}}$ the function u_v is continuous on $X(\overline{\kappa})$.

Let D be a divisor on X. By a (*global*) *Weil function* associated with D we mean a function

$$\lambda_D : (X(\overline{\kappa}) - \operatorname{supp} D) \times M_{\overline{\kappa}} \longrightarrow \mathbb{R}$$

having the following property. Let (U, f) be a pair representing D. Then there exists a locally bounded continuous function

$$u : U(\overline{\kappa}) \times M_{\overline{\kappa}} \longrightarrow \mathbb{R}$$

such that for any point in $U(\overline{\kappa}) - \operatorname{supp} D$ we have

$$\lambda_{D,v}(x) = -\log |||f(x)|||_v + u_v(x).$$

The function u is then uniquely determined by λ_D and the pair (U, f). Let $[D]$ be the line bundle associated to D with a meromorphic section s. For $x \notin \operatorname{supp} D$, the Weil function λ_D associated with D can be given by

$$\lambda_{D,v} = -\log |||s(x)|||_v .$$

If (U_1, f_1) is another local representative of the divisor D with $U \cap U_1 \neq \emptyset$, by the definition there exists a locally bounded continuous function

$$u_1 : U_1(\overline{\kappa}) \times M_{\overline{\kappa}} \longrightarrow \mathbb{R}$$

such that for any point in $U_1(\overline{\kappa}) - \operatorname{supp} D$ we have

$$\lambda_{D,v}(x) = -\log |||f_1(x)|||_v + u_{1,v}(x).$$

Hence on $U \cap U_1$, we have

$$u_{1,v} - u_v = -\log |||f f_1^{-1}|||_v. \tag{4.33}$$

If (4.33) holds, the triples (U, f, u) and (U_1, f_1, u_1) are called *compatible*.

We sometimes think of λ_D as a function over κ, that is, λ_D is defined on $(X(\kappa) - \operatorname{supp} D) \times M_\kappa$. If K is a finite extension of the number field κ and λ_D is a Weil function for D over κ, then

$$\lambda_{D,w}(x) = \frac{[K_w : \kappa_v]}{[K : \kappa]} \lambda_{D,v}(x)$$

is a Weil function for D over K. Thus, if $x \in X(\kappa)$, then

$$\lambda_{D,v}(x) = \sum_{w|v} \lambda_{D,w}(x) + O(1),$$

where $O(1)$ means a *bounded function* of x.

In particular, if f is a rational function on X, a Weil function λ_f associated with the principal divisor (f) is given by

$$\lambda_{f,v}(x) = -\log |||f(x)|||_v.$$

Proposition 4.39. *Weil functions satisfy the following properties:*

(a) *If λ_D and $\lambda_{D'}$ are Weil functions for D and D', then $\lambda_D + \lambda_{D'}$ is a Weil function for $D + D'$ and $-\lambda_D$ is a Weil function for $-D$.*

(b) *Assume that X is projective. If D is an effective divisor, then its Weil functions are bounded from below.*

(c) *Assume that X is projective. If λ, λ' are Weil functions with the same divisor, then $\lambda - \lambda'$ is bounded.*

(d) *Let $f : X \longrightarrow Y$ be a morphism of varieties and let D be a divisor on Y not containing the image of f. If λ_D is a Weil function for D on Y then $\lambda_D \circ f$ is a Weil function for f^*D on X.*

Proof. See Lang [144], Chapter 10, Proposition 2.1 for (a), Proposition 3.1 for (b), Proposition 2.2 for (c), and Proposition 2.6 for (d). □

Proposition 4.40. *Let $D_1, \ldots, D_m$ and D be divisors on X such that $E_i = D_i - D$ are effective divisors for all i, and such that the supports of $E_1, \ldots, E_m$ have no points in common. Then*

$$\lambda_D = \inf_i \lambda_{D_i}$$

is a Weil function for D.

Proof. Given a point x, for each i let (U_i, f_i) be a local representative of the divisor D_i on an open set U_i containing x. Then there exists a locally bounded continuous function

$$u_i : U_i(\overline{\kappa}) \times M_{\overline{\kappa}} \longrightarrow \mathbb{R}$$

such that in $U_i(\overline{\kappa}) - \operatorname{supp} D_i$ we have

$$\lambda_{D_i,v} = -\log |||f_i|||_v + u_{i,v}.$$

Let $i(x)$ be an index such that $x \notin \operatorname{supp} E_{i(x)}$, and let

$$U_x = (X - \operatorname{supp} E_{i(x)}) \cap U_1 \cap \cdots \cap U_m.$$

Then U_x is an open set containing x. Let

$$u_x : U_x(\overline{\kappa}) \times M_{\overline{\kappa}} \longrightarrow \mathbb{R}$$

be defined by

$$u_{x,v}(y) = \inf_i \left\{ -\log |||f_i(y) f_{i(x)}^{-1}(y)|||_v + u_{i,v}(y) \right\}.$$

Since the rational function $f_{i(x)}$ has Cartier divisor $D + E_{i(x)}$ on $U_{i(x)}$, it has the Cartier divisor $D|_{U_x}$ on U_x. Hence the family $\{(U_x, f_{i(x)})\}$ defines the Cartier divisor D on X.

Next, by definition we know that $f_i f_{i(x)}^{-1}$ represents the Cartier divisor E_i on U_x and hence is morphic on U_x. Therefore the function

$$(y, v) \longmapsto -\log |||f_i(y) f_{i(x)}^{-1}(y)|||_v$$

is locally bounded from below on $U_x(\overline{\kappa}) \times M_{\overline{\kappa}}$. Since u_i is locally bounded, it follows that u_x is locally bounded from below on $U_x(\overline{\kappa}) \times M_{\overline{\kappa}}$. Since

$$f_{i(x)} f_{i(x)}^{-1} = 1,$$

it follows that u_x is also locally bounded from above. Hence u_x is locally bounded, and its definition shows directly that it is continuous.

Further we check the compatibility condition. Let x' be a point of X and let $i(x')$ be an index such that $x' \notin \operatorname{supp} E_{i(x')}$. Define $(U_{x'}, f_{i(x')}, u_{x'})$ as we did $(U_x, f_{i(x)}, u_x)$. Thus on $U_x \cap U_{x'}$, we obtain

$$u_{x',v} - u_{x,v} = -\log |||f_{i(x)} f_{i(x')}^{-1}|||_v,$$

thus proving the compatibility, and defining a Weil function λ_D associated with D such that in $U_x(\overline{\kappa}) - \operatorname{supp} D$ we have

$$\lambda_{D,v} = -\log |||f_{i(x)}|||_v + u_{x,v}.$$

Substituting $y = x$ in the definition of $u_{x,v}(y)$ we find that

$$\lambda_{D,v}(x) = \inf_i \lambda_{D_i,v}(x),$$

thus proving the proposition. □

The existence of a Weil function associated with a given divisors on a projective variety is referred to S. Lang [144]:

Theorem 4.41. *Let X be a projective variety. Let D be a divisor on X. Then there exists a Weil function having this divisor.*

Proof. Applying Proposition 3.53, then there exist effective Cartier divisors D_i $(i = 1, \ldots, m)$ and E_j $(j = 1, \ldots, n)$ such that the $\operatorname{supp} D_i$ have no common point, the $\operatorname{supp} E_j$ have no common point, and $D + D_i \sim E_j$. Thus there are rational functions f_{ij} such that

$$D - E_j + D_i = (f_{ij}).$$

By Proposition 4.40, there exists a Weil function λ_{H_j} for $H_j = D - E_j$ such that

$$\lambda_{H_j} = \inf_i \lambda_{f_{ij}}.$$

Since the Cartier divisors of $\lambda_{-H_j} = -\lambda_{H_j}$ have the forms

$$-H_j = E_j - D,$$

we apply Proposition 4.40 once more to get the desired function λ_D, which is defined by the formula

$$\lambda_D = \sup_j \inf_i \lambda_{f_{ij}}.$$

This proves the theorem. □

4.4.2 Heights expand Weil functions

Theorem 4.42. *Let X be a projective variety over κ and let λ_D be a Weil function of a divisor D on X. Then*

$$h_D(x) = \sum_{v \in M_\kappa} \lambda_{D,v}(x) + O(1), \;\; x \in X(\kappa) - \operatorname{supp} D. \tag{4.34}$$

Proof. We will compare h_D with the function

$$\hbar_D(x) = \sum_{v \in M_\kappa} \lambda_{D,v}(x), \;\; x \in X(\kappa) - \operatorname{supp} D. \tag{4.35}$$

A Weil functions $\lambda_{D'}$ for another divisor D' on X is said to be *linearly equivalent* to λ_D if there exists a rational function f such that

$$\lambda_{D'} - \lambda_D = \lambda_f + \gamma,$$

where γ is a M_κ-constant. Thus if $\lambda_{D'}$ is linearly equivalent to λ_D, by the product formula we have

$$\hbar_{D'}(x) = \hbar_D(x) + O(1), \;\; x \notin \operatorname{supp} D \cup \operatorname{supp} D'.$$

Now we can extend the definition of $\hbar_D$ to $\operatorname{supp} D$ as follows. For each point $x \in \operatorname{supp} D$, there exists a rational function f such that x does not lie in the support of $D' = D - (f)$. Put $\lambda_{D'} = \lambda_D - \lambda_f$. We then define

$$\hbar_D(x) = \hbar_{D'}(x).$$

This value is independent of the choice of f.

Next we prove that $\hbar$ satisfies the normalization property in Theorem 4.34, that is, if H is a hyperplane in $\mathbb{P}^n$, then

$$\hbar_H(x) = h(x) + O(1), \quad x \in \mathbb{P}^n.$$

Let $H_0, \ldots, H_n$ be the hyperplane corresponding to the coordinate functions. There exist rational functions f_i such that

$$(f_i) = H_i - H.$$

For any point $x \notin H$, it is easy to obtain

$$h(x) = \sum_{v \in M_\kappa} \sup_i \log |||f_i(x)|||_v + O(1),$$

or equivalently,

$$h(x) = -\sum_{v \in M_\kappa} \inf_i \lambda_{f_i,v}(x) + O(1),$$

where λ_{f_i} is a Weil function associated with the principal divisor (f_i). We conclude the proof by applying Proposition 4.39, (a), (c) and Proposition 4.40.

Obviously, $\hbar$ also satisfies the functoriality and additivity properties of Theorem 4.34 from Proposition 4.39, (a) and (d). Hence the uniqueness property in Theorem 4.34 implies

$$h_D = \hbar_D + O(1).$$

This proves the desired result. □

Let D be a divisor on a nonsingular projective variety X over κ. If D is effective, by Theorem 4.34, (5), we have $h_D \geq O(1)$, in other words we can choose h_D in its equivalence class such that $h_D \geq 0$. If D is ample, by the definition there exists $m \in \mathbb{Z}^+$ such that mD is very ample, and so

$$0 \leq h_{mD} = mh_D + O(1).$$

W.l.o.g. we may assume $h_D \geq 0$. If D is pseudo ample, by Theorem 3.55 there exists some positive integer m such that $mD \sim E + Z$, where E is ample and Z is effective. Hence

$$h_{mD} = h_E + h_Z + O(1).$$

Thus we can choose h_D in its equivalence class such that $h_D \geq 0$.

Let D be an effective divisor on X and let $\mathcal{R}$ be a subset of $X(\bar{\kappa}) - \operatorname{supp} D$. Then $\mathcal{R}$ is a set of (S, D)-*integralizable points* if there exists a global Weil function λ_D and a M_κ-constant γ such that for all $x \in \mathcal{R}$, all $v \in M_\kappa - S$, and all embeddings of $\bar{\kappa}$ in $\bar{\kappa}_v$,

$$\lambda_D(x, v) \leq \gamma(v).$$

As easy consequences of the properties of Weil functions, one finds (cf. [287], p. 11): If K is a finite extension field of κ, and if T is the set of places of K lying over places in S, then $\mathcal{R} \subset X(\bar{\kappa})$ is a set of (S, D)-integralizable points if and only if it is a set of (T, D)-integralizable points.

4.4.3 Proximity functions

Let κ be a number field and let M_κ be a set of absolute values satisfying product formula with multiplicities n_v. Let S be a finite set of places containing M_κ^∞. Let λ_D be a Weil function for a divisor D on a variety X. For any point $x \in X(\kappa)$ not in the support of D, the *proximity function* for D is defined by

$$m(x, D) = m_S(x, D) = \sum_{v \in S} \lambda_{D,v}(x).$$

Then

$$N(x, D) = N_S(x, D) = \sum_{v \in M_\kappa - S} \lambda_{D,v}(x)$$

serves as the *valence function* for D.

Lemma 4.43. *The proximity and valence functions satisfy the following properties:*

(A) *If D and D' are divisors, then*

$$\begin{aligned} m(x, D + D') &= m(x, D) + m(x, D') + O(1), \\ N(x, D + D') &= N(x, D) + N(x, D') + O(1). \end{aligned}$$

(B) *Assume that X is projective. If D is an effective divisor, then $m(x, D)$ and $N(x, D)$ are bounded from below.*

(C) *Let $f : X \longrightarrow Y$ be a morphism of varieties and let D be a divisor on Y not containing the image of f. Then*

$$m(x, f^*D) = m(f(x), D) + O(1), \quad N(x, f^*D) = N(f(x), D) + O(1).$$

(D) *$m(x, D)$ and $N(x, D)$ do not depend on the number field used in the definition. In other words, if K is a number field containing κ and T is the set of places of K lying over places $v \in S$, then for all $x \in X(\kappa)$*

$$m_S(x, D) = m_T(x, D) + O(1), \quad N_S(x, D) = N_T(x, D) + O(1).$$

Proof. This follows directly from Proposition 4.39 and the definitions, or see Lemma 3.4.1 of Vojta [287]. □

If X is projective, by Theorem 4.42, one obtains the *first main theorem*:

$$m(x,D)+N(x,D)=h_D(x)+O(1). \tag{4.36}$$

Proposition 4.39, (c) implies that the functions $m(x,D),\ N(x,D)$ are well determined by the divisor D, up to $O(1)$, respectively. Further, if D is an effective divisor, by Proposition 4.39 (b), we may assume

$$m(x,D)\geq 0,\quad N(x,D)\geq 0$$

by using a proper Weil function of D. We will construct concrete Weil functions such that these inequalities hold.

Let $V=V_\kappa$ be a vector space of finite dimension $n+1>0$ over κ. Take $a\in\mathbb{P}(V^*)$. Obviously,

$$\lambda_{a,v}(x)=\log\frac{1}{|||x,a|||_v}$$

determine a Weil function λ_a for the hyperplane $\ddot{E}[a]$. Thus we obtain the *proximity function* for a

$$m(x,a):=m\big(x,\ddot{E}[a]\big)=\sum_{v\in S}\log\frac{1}{|||x,a|||_v}, \tag{4.37}$$

and the *valence function* for a

$$N(x,a):=N\big(x,\ddot{E}[a]\big)=\sum_{v\in M_\kappa-S}\log\frac{1}{|||x,a|||_v}. \tag{4.38}$$

Note that

$$\sum_{v\in M_\kappa}\log\frac{1}{|||x,a|||_v}=h(x)+h(a),\quad x\notin\ddot{E}[a]. \tag{4.39}$$

We obtain the *first main theorem*:

$$m(x,a)+N(x,a)=h(x)+h(a),\quad x\notin\ddot{E}[a], \tag{4.40}$$

and therefore,

$$N(x,a)\leq h(x)+h(a),\quad x\notin\ddot{E}[a].$$

In particular, if $V=\kappa^2$, then

$$\mathbb{P}(V)=\mathbb{P}^1(\kappa)=\kappa\cup\{\infty\}.$$

For $x\in\kappa$, we abbreviate

$$m(x,a)=\begin{cases}m([1,x],[-a,1]), & \text{if } a\in\kappa,\\ m([1,x],[1,0]), & \text{if } a=\infty\end{cases}$$

and similarly

$$N(x,a) = \begin{cases} N([1,x],[-a,1]), & \text{if } a \in \kappa, \\ N([1,x],[1,0]), & \text{if } a = \infty. \end{cases}$$

By the formula (3.7), we find

$$m(x,a) = \frac{1}{[\kappa:\mathbb{Q}]} \sum_{v \in S} \log \frac{1}{\chi_v(x,a)^{n_v}}$$

and similarly

$$N(x,a) = \frac{1}{[\kappa:\mathbb{Q}]} \sum_{v \in M_\kappa - S} \log \frac{1}{\chi_v(x,a)^{n_v}}.$$

Fix $a, x \in \kappa$. Obviously, there exists a constant C depending only on $|a|_v$ such that

$$\max\left\{1, \frac{1}{|x-a|_v}\right\} \leq \frac{1}{\chi_v(x,a)} \leq C \max\left\{1, \frac{1}{|x-a|_v}\right\}.$$

Thus we obtain

$$m(x,a) = \sum_{v \in S} \log^+ \frac{1}{|||x-a|||_v} + O(1)$$

and similarly

$$N(x,a) = \sum_{v \in M_\kappa - S} \log^+ \frac{1}{|||x-a|||_v} + O(1),$$

where by definition,

$$\log^+ r = \log r^\vee = \max\{0, \log r\} \ \ (r \in \mathbb{R}_+).$$

Let D be a very ample divisor over a nonsingular projective variety X. Take $s \in V^* = \Gamma(X,[D])$ with $(s) = D$ and set $a = \mathbb{P}(s)$. For $x \notin D$, the *proximity function* $m(x,D)$ and the *valence function* $N(x,D)$ are given respectively by

$$m(x,D) = m(\varphi_D(x),a) = \sum_{v \in S} \log \frac{1}{|||\varphi_D(x),a|||_v},$$

and

$$N(x,D) = N(\varphi_D(x),a) = \sum_{v \in M_\kappa - S} \log \frac{1}{|||\varphi_D(x),a|||_v}.$$

4.5 Arakelov theory

Let κ be a *global field of dimension* 1, in other words, κ is either a number field or the function field $\mathbf{F}(C)$ of a smooth projective curve C over a field $\mathbf{F}$, and let X be a smooth projective variety defined over κ. Let $\mathcal{C} = \operatorname{Spec} \mathcal{O}_\kappa$ if κ is a number field, and let $\mathcal{C} = C^{\mathrm{sch}}$ if κ is a function field. A *model* for X over $\mathcal{C}$ is a scheme $\mathcal{X} \longmapsto \mathcal{C}$ whose generic fiber is isomorphic to X. It is easy to see that there exists a model $\mathcal{X} \longmapsto \mathcal{C}$ that is projective (by which we mean that all fibers are projective varieties) and whose generic fiber $\mathcal{X}_\eta = \mathcal{X} \times_{\mathcal{C}} \operatorname{Spec} \kappa$ is isomorphic to X. Indeed, fix an embedding $i : X \longrightarrow \mathbb{P}^n_\kappa$. We know that $\mathbb{P}^n_\kappa$ is the generic fiber of the scheme $\mathbb{P}^n_{\mathcal{C}} \longmapsto \mathcal{C}$, so we may take $\mathcal{X}$ to be the Zariski closure of $i(X)$ inside $\mathbb{P}^n_\kappa$.

A smooth projective variety X over κ has *good reduction* at x if there exists a projective model of X over $\mathcal{O}(x)$ whose special fiber is smooth. If such a model does not exist, we say that X has *bad reduction* at x. We know that the variety X has good reduction at all but finitely many points (cf. [98], Proposition A.9.1.6). For example, $\mathbb{P}^n/\mathbb{Q}$ has good reduction everywhere.

4.5.1 Function fields

We start with a smooth projective variety X defined over a function field $\kappa = \mathbf{F}(C)$, where C is a smooth projective curve over $\mathbf{F}$. We will assume that $\mathbf{F}$ is algebraically closed. We can construct a projective variety $\mathcal{X}$ over $\mathbf{F}$ with a morphism $\pi : \mathcal{X} \longrightarrow C$ such that the generic fiber of π is isomorphic to X/κ. We further assume that $\mathcal{X}$ is smooth so that Weil divisors and Cartier divisors are the same. A point $x \in X(\kappa)$ induces a rational mapping $C \longrightarrow \mathcal{X}$, and since C is smooth and $\mathcal{X}$ is projective, x will extend to a section (i.e., to a morphism) $\bar{x} : C \longrightarrow \mathcal{X}$. Any divisor $D = \sum n_Y Y$ on X extends to a divisor $\bar{D}$ on $\mathcal{X}$ by taking the Zariski closure of each component and keeping the same multiplicities, say $\bar{D} := \sum n_Y \bar{Y}$. The divisor $\bar{D}$ is a Weil divisor, and hence is a Cartier divisor by hypothesis. Now observe that $\bar{x}^* \bar{D}$ is well-defined as a divisor class on the curve C, and even as a divisor if we add the hypothesis that $x \notin \operatorname{supp}(D)$. We now define a function $\hbar_{D,\mathcal{X}}$ on $X(\kappa)$ by the formula

$$\hbar_{D,\mathcal{X}}(x) := \deg \bar{x}^* \bar{D}, \;\; x \in X(\kappa). \tag{4.41}$$

If x is a point defined over the algebraic closure of $\kappa = \mathbf{F}(C)$, say $x \in X(K)$ with K a finite extension of κ, we can still define its *height* as follows. Fix a smooth projective curve C' and a covering $f : C' \longrightarrow C$ such that $K = \mathbf{F}(C')$ and such that the mapping f induces the inclusion $\kappa \subset K$. The point x corresponds to a morphism $\bar{x} : C' \longrightarrow \mathcal{X}$ as above, and we can define

$$\hbar_{D,\mathcal{X}}(x) := \frac{1}{[K : \kappa]} \deg \bar{x}^* \bar{D}. \tag{4.42}$$

One readily checks that this quantity is independent of the field K as long as $x \in X(K)$. Generally, the extension of height functions from $X(\kappa)$ to $X(\bar{\kappa})$ will be

straightforward, so we will be content in this section to restrict attention to points in $X(\kappa)$.

Lemma 4.44. *Let $x = [f_0, \dots, f_n] \in \mathbb{P}^n(\kappa)$, let $\bar{x}$ be the associated $\mathbf{F}$-morphism $\bar{x} : C \longrightarrow \mathbb{P}^n$, and let D be a hyperplane (divisor class) in $\mathbb{P}^n$. Then*

$$\deg \bar{x}^* D = \sum_{p \in C} \max_{0 \le i \le n} \{-\mathrm{ord}_p(f_i)\}.$$

Proof. Changing coordinates if necessary, we may assume that $\bar{x}(C) \not\subset H_i$, where H_i is the hyperplane defined by $\xi_i = 0$. Let $D_i := \bar{x}^* H_i$. Then

$$D_i - D_j = \bar{x}^* H_i - \bar{x}^* H_j = (f_i / f_j)$$

and

$$\mathrm{ord}_p(D_i) - \mathrm{ord}_p(D_j) = \mathrm{ord}_p(f_i) - \mathrm{ord}_p(f_j),$$

and hence

$$\inf_i \{\mathrm{ord}_p(D_i)\} - \mathrm{ord}_p(D_j) = \inf_i \{\mathrm{ord}_p(f_i)\} - \mathrm{ord}_p(f_j).$$

But since the D_i's are effective and the intersection of their supports is empty, we see that $\inf_i \{\mathrm{ord}_p(D_i)\} = 0$. Hence

$$-\inf_i \{\mathrm{ord}_p(f_i)\} = \mathrm{ord}_p(D_j) - \mathrm{ord}_p(f_j).$$

Now summing over $p \in C$ and using the fact that $\sum_p \mathrm{ord}_p(f_j) = 0$ gives the desired result. □

Notice that the sum in Lemma 4.44 is nothing more than the height

$$h(x) = \sum_{p \in C} \max_{0 \le i \le n} \{-\mathrm{ord}_p(f_i)\} \tag{4.43}$$

of the κ-rational point in $\mathbb{P}^n$ for the usual collection of valuations on the function field κ.

Next we observe that if Y is an irreducible hypersurface on $\mathcal{X}$, then its image $\pi(Y)$ is either equal to all of C, or else it is equal to a single point. We say that D is a *vertical divisor* if π maps all of the components of D to points, and similarly we say that D is a *horizontal divisor* if π maps all of its components surjectively onto C. Clearly, any divisor can be written as the sum of a horizontal and a vertical divisor in a unique way. We also note that vertical divisors are characterized by the property that their restriction to the generic fiber of π is trivial.

Lemma 4.45. *Let D be a vertical divisor on $\mathcal{X}$ with respect to $\pi : \mathcal{X} \longrightarrow C$. Then the mapping*

$$\hbar_{D,\mathcal{X}} : X(\kappa) \longrightarrow \mathbb{Z},\ x \longmapsto \deg \bar{x}^* D,$$

takes finitely many values. In particular, $\hbar_{D,\mathcal{X}}$ is a bounded function.

Proof. The proof is immediate once we note that if D is an irreducible component of a fiber of π, then $\deg \bar{x}^* D = 1$ if the section $\bar{x}$ meets D, and $\deg \bar{x}^* D = 0$ otherwise. □

Lemma 4.46. *Let D be a divisor on X. Let $\pi : \mathcal{X} \longrightarrow C$ and $\pi' : \mathcal{X}' \longrightarrow C$ be two models for X/κ. Then the difference $\hbar_{D,\mathcal{X}} - \hbar_{D,\mathcal{X}'}$ is bounded on $X(\kappa)$.*

Proof. We can find a third model $\mathcal{X}''$ that will dominate the other two, and hence we can reduce to the case where there is a birational morphism $f : \mathcal{X} \longrightarrow \mathcal{X}'$ such that $\pi = \pi' \circ f$. If $x \in X(\kappa)$ and $\bar{x}$ is the associated section from C to $\mathcal{X}$, then $\bar{x}' = f \circ \bar{x}$ is the section from C to $\mathcal{X}'$ corresponding to x'. In fact, they coincide on a dense subset of C, hence are identical. Now let $\bar{D}$ be the Zariski closure of D in $\mathcal{X}$, and let $\bar{D}'$ be the Zariski closure of D in $\mathcal{X}'$. Then the divisor $E := f^* \bar{D}' - \bar{D}$ is trivial when restricted to the generic fiber, so E is a vertical divisor. Hence

$$\hbar_{D,\mathcal{X}} - \hbar_{D,\mathcal{X}'} = \deg \bar{x}^* E$$

is a bounded function by Lemma 4.45. □

Proposition 4.47. **(a)** *Take $X = \mathbb{P}^n$, let D be a hyperplane of $\mathbb{P}^n$ defined over κ, and let h be the usual height on $\mathbb{P}^n(\kappa)$. Then*

$$\hbar_{D,\mathcal{X}} = h + O(1).$$

(b) *Let $\varphi : X' \longrightarrow X$ be a κ-morphism of varieties defined over κ and let D be a divisor on X not containing the image of φ. Then*

$$\hbar_{\varphi^* D,\mathcal{X}'} = \hbar_{D,\mathcal{X}} \circ \varphi + O(1).$$

(c) *For all divisors D, D' on X defined over κ,*

$$\hbar_{D+D',\mathcal{X}} = \hbar_{D,\mathcal{X}} + \hbar_{D',\mathcal{X}} + O(1).$$

(d) *Let $f \in \kappa(X)_*$ and $D = (f)$. Then*

$$\hbar_{D,\mathcal{X}} = O(1).$$

(e) *If D is an effective divisor and $x \notin \operatorname{supp}(D)$, then $\hbar_{D,\mathcal{X}}(x) \geq 0$.*

Proof. Property (a) is just Lemma 4.44. Property (c) is immediate by additivity of π^* and $\deg$.

To prove (b), we use that fact that we can choose models $\pi : \mathcal{X} \longrightarrow C$ and $\pi' : \mathcal{X}' \longrightarrow C$ such that φ extends to a morphism $\bar{\varphi}$ from $\mathcal{X}'$ to $\mathcal{X}$. Having done this, we see that $\bar{\varphi}^*\bar{D} - \overline{\varphi^* D}$ is trivial when restricted to the generic fiber of π; hence it is a vertical divisor E. Again by Lemma 4.45 and additivity, we conclude that $\hbar_{D,\mathcal{X}} \circ \varphi - \hbar_{\varphi^* D,\mathcal{X}'}$ is bounded.

To prove (d), we observe that $f \in \kappa(X)$ will be extend to a rational function $\bar{f}$ on $\mathcal{X}$ and that the restriction to the generic fiber of π of the two divisors $\left(\bar{f}\right)$ and $\overline{D}$ are the same; hence their difference is a vertical divisor, say

$$E = \left(\bar{f}\right) - \overline{D}.$$

It follows from Lemma 4.45 that the function

$$\hbar_{D,\mathcal{X}}(x) = \deg \bar{x}^* \overline{D} = \deg \bar{x}^*(\bar{f}) - \deg \bar{x}^* E = -\deg \bar{x}^* E$$

is bounded.

Finally, notice that the effectiveness of D implies that $\bar{D}$, and hence $\bar{x}^*\bar{D}$, is also effective. Therefore $\bar{x}^*\bar{D}$ has positive degree, which gives (e). □

4.5.2 Number fields

We now want to built an analogue of the above construction when the function field is replaced by a number field κ. This is accomplished by formally adding analytic information to $\mathcal{X}$ for each Archimedean place; hence the role of $\mathcal{C}$ is played by an *arithmetic scheme* $\mathbb{M}_\kappa$ consisting of $\operatorname{Spec} \mathcal{O}_\kappa$, with finitely many points added, corresponding to the Archimedean places. Therefore, one can think of the arithmetic scheme $\mathbb{M}_\kappa$ as an object whose closed points are in canonical bijection with M_κ. Recall that the set of non-Archimedean places on κ is naturally identified with the set of prime ideals in $\mathcal{O}_\kappa$, hence our identification of M_κ^0 with $\operatorname{Spec} \mathcal{O}_\kappa$. We will also write $\mathfrak{p}_v \in \operatorname{Spec} \mathcal{O}_\kappa$ for the prime ideal corresponded to the place $v \in M_\kappa^0$; $\mathfrak{p}_v \in \mathbb{M}_\kappa - \operatorname{Spec} \mathcal{O}_\kappa$ for the place $v \in M_\kappa^\infty$; and so give the canonical bijection

$$M_\kappa \longrightarrow \mathbb{M}_\kappa, \;\; v \mapsto \mathfrak{p}_v. \tag{4.44}$$

A *compactified divisor* on $\operatorname{Spec} \mathcal{O}_\kappa$ (or *Arakelov divisor* on $\mathbb{M}_\kappa$) is a formal sum

$$\mathbf{D} := \sum_{v \in M_\kappa} m_v \mathfrak{p}_v, \tag{4.45}$$

where

$$m_v \in \begin{cases} \mathbb{Z}, & \text{if } v \in M_\kappa^0, \\ \mathbb{R}, & \text{if } v \in M_\kappa^\infty; \end{cases}$$

and almost all $m_v = 0$. A *principal compactified divisor* on $\operatorname{Spec} \mathcal{O}_\kappa$ is a divisor of the form

$$\operatorname{div}(a) := \sum_{v \in M_\kappa^0} \operatorname{ord}_v(a)\mathfrak{p}_v + \sum_{v \in M_\kappa^\infty} \log \frac{1}{\|a\|_v}\mathfrak{p}_v \tag{4.46}$$

for some $a \in \kappa_*$. The *degree* of the compactified divisor $\mathbf{D}$ is defined to be

$$\deg(\mathbf{D}) := \sum_{v \in M_\kappa} \deg_v(\mathbf{D}), \tag{4.47}$$

where

$$\deg_v(\mathbf{D}) = \begin{cases} m_v \log \mathcal{N}(\mathfrak{p}_v), & \text{if } v \in M_\kappa^0, \\ m_v, & \text{if } v \in M_\kappa^\infty. \end{cases} \tag{4.48}$$

Observe that the product formula (2.13) says exactly that the degree of a principal compactified divisor is zero.

Let κ be a number field and let X/κ be a smooth projective variety. We can construct a projective scheme $\pi : \mathcal{X} \longrightarrow \operatorname{Spec} \mathcal{O}_\kappa$ with generic fiber X/κ, and the fact that $\mathcal{X}$ is proper over $\operatorname{Spec} \mathcal{O}_\kappa$ implies that any rational point $x \in X(\kappa)$ gives a section

$$\bar{x} : \operatorname{Spec} \mathcal{O}_\kappa \longrightarrow \mathcal{X}.$$

Similarly, we can still define the closure of a divisor D on X to be its Zariski closure $\bar{D}$ in $\mathcal{X}$. If $\mathcal{X}$ is sufficiently smooth (e.g., if it is regular as an abstract scheme), then $\bar{x}^*\bar{D}$ will give a well-defined divisor class on $\operatorname{Spec} \mathcal{O}_\kappa$, and indeed if the image of x does not lie in the support of D, then we get a well-defined divisor on $\operatorname{Spec} \mathcal{O}_\kappa$

$$\bar{x}^*\bar{D} = \sum_{v \in M_\kappa^0} m_v \mathfrak{p}_v.$$

To define the degree of $\bar{x}^*\bar{D}$ which should depend only on the divisor class of D, we need to complete the divisor $\bar{x}^*\bar{D}$ by adding to it a finite sum that takes account of the places "at infinity". In other words, we need to extend $\bar{x}$ into a section

$$\tilde{x} : \mathbb{M}_\kappa \longrightarrow \mathcal{X}.$$

Our approach is to use *Green functions* (also called *Néron functions* in this context). For our purposes a Green function attached to a divisor D and a place $v \in M_\kappa^\infty$ is simply a continuous function

$$G_{D,v} : X_D(\mathbb{C}) \longrightarrow \mathbb{R}$$

with a logarithmic pole along D, where $X_D := X - \operatorname{supp}(D)$. This last condition means that if U is an open subset of X and if $f = 0$ is a local equation for D on U, then the function

$$G_{D,v}(x) + \log \|f(x)\|_v,$$

defined a priori only on $U_D(\mathbb{C})$, extends to a continuous function on $U(\mathbb{C})$. Thus we obtain a compactified divisor on $\operatorname{Spec}\mathcal{O}_\kappa$

$$\tilde{x}^*\bar{D} = \sum_{v\in M_\kappa^0} m_v\mathfrak{p}_v + \sum_{v\in M_\kappa^\infty} G_{D,v}(x)\mathfrak{p}_v. \tag{4.49}$$

The *height* of x ($\notin \operatorname{supp}(D)$) relative to these choices is

$$\hbar_{D,\mathcal{X}}(x) := \frac{1}{[\kappa:\mathbb{Q}]}\deg \tilde{x}^*\bar{D}. \tag{4.50}$$

A variant of this point of view is furnished by the notion of a line bundle equipped with a norm or a metric. A line sheaf $\mathscr{L}$ on $\operatorname{Spec}\mathcal{O}_\kappa$ being coherent, there exists a module $\mathbf{L} = \Gamma(\operatorname{Spec}\mathcal{O}_\kappa, \mathscr{L})$ over $\mathcal{O}_\kappa$ such that $\mathscr{L} = \widetilde{\mathbf{L}}$. The module $\mathbf{L}$ is locally free of rank 1. Take $v \in M_\kappa^\infty$. We identify

$$\mathscr{L}_v = \mathbf{L}_v = \mathbf{L}\otimes_{\mathcal{O}_\kappa}\kappa_v.$$

By a *metric* on $\mathbf{L}$ (or $\mathscr{L}$) induced by v, we mean a norm $|\cdot|_v$ on $\mathbf{L}_v$, so this norm satisfies the triangle inequality and satisfies

$$|a\ell|_v = |a|_v|\ell|_v, \quad a\in\kappa_v,\ \ \ell\in\mathbf{L}_v.$$

A *metrized line bundle* on $\operatorname{Spec}\mathcal{O}_\kappa$ is a projective module $\mathbf{L}$ of rank 1 over $\mathcal{O}_\kappa$ together with a collection of nontrivial norms

$$T = \{|\cdot|_v \mid v\in M_\kappa^\infty\} \tag{4.51}$$

such that $|\cdot|_v$ is a norm on the κ_v vector space $\mathbf{L}_v = \mathbf{L}\otimes\kappa_v$ that is compatible with the norm on κ_v. As usual, we then use the normalized form

$$\|\ell\|_v = |\ell|_v^{n_v},$$

where

$$n_v = \begin{cases} 1, & \text{if } v \text{ is real,}\\ 2, & \text{if } v \text{ is complex.}\end{cases}$$

As $\mathcal{O}_\kappa$-module, such $\mathbf{L}$ is isomorphic to some fractional ideal $\mathfrak{g}$. Alternatively, we may let $\mathbf{L}$ be a finitely generated torsion free module over $\mathcal{O}_\kappa$.

Given $\ell\in\mathbf{L}$, $\ell\neq 0$, we can associate a divisor to $\mathbf{L}$ as follows. There is a unique injection of $\mathcal{O}_\kappa$ into $\mathbf{L}$ as $\mathcal{O}_\kappa$-module, sending 1 to ℓ. Then $\mathbf{L}$ can be identified with a fractional ideal in κ, and so an ideal $\mathfrak{a}_\ell = \mathbf{L}^{-1}$ is defined well. We define the *associated divisor*

$$\mathbf{D}_\ell = \sum_{v\in M_\kappa^0}\operatorname{ord}_v(\mathfrak{a}_\ell)\mathfrak{p}_v + \sum_{v\in M_\kappa^\infty}\log\frac{1}{\|\ell\|_v}\mathfrak{p}_v.$$

The *Arakelov degree* of a metrized line bundle $\mathbf{L}$ is defined to be the degree of its associated divisor

$$\deg(\mathbf{L}) := \log \mathcal{N}(\mathfrak{a}_\ell) + \sum_{v \in M_\kappa^\infty} \log \frac{1}{\|\ell\|_v}. \tag{4.52}$$

As usual, the product formula (2.13) tells us that the degree is independent of the choice of ℓ. We also have the relation

$$\mathcal{N}(\mathfrak{a}_\ell) = \#(\mathbf{L}/\ell\mathcal{O}_\kappa).$$

Let κ be a number field, let X/κ be a smooth projective variety, and let L be a line bundle on X defined over κ. We can construct a projective scheme $\pi : \mathcal{X} \longrightarrow \operatorname{Spec} \mathcal{O}_\kappa$ with generic fiber X/κ, and the fact that $\mathcal{X}$ is proper over $\operatorname{Spec} \mathcal{O}_\kappa$ implies that any rational point $x \in X(\kappa)$ gives a section $\bar{x} : \operatorname{Spec} \mathcal{O}_\kappa \longrightarrow \mathcal{X}$ by the valuative criterion of properness (see [90], Theorem 4.7) with an extension

$$\tilde{x} : \mathbb{M}_\kappa \longrightarrow \mathcal{X}.$$

Choose an extension $\mathcal{L}$ of L to $\mathcal{X}$ and metrics (4.51) on L (extending scalars to $\bar{\kappa}_v \cong \mathbb{C}$). Then the pullback

$$\tilde{x}^*\mathcal{L} = \tilde{x}^*(\mathcal{L})_T$$

is a metrized line bundle on $\operatorname{Spec} \mathcal{O}_\kappa$, and the *metrized height* (or *degree*) of x relative to these choices is

$$\hbar_{\mathcal{L},\mathcal{X},T}(x) := \frac{1}{[\kappa : \mathbb{Q}]} \deg \tilde{x}^*\mathcal{L}. \tag{4.53}$$

Proposition 4.48. *Let $\mathcal{L}, \mathcal{X}, T$ and $\mathcal{L}', \mathcal{X}', T'$ be two extensions with metrics of a variety X and a line bundle L on X as above. Then*

$$\hbar_{\mathcal{L},\mathcal{X},T}(x) = \hbar_{\mathcal{L}',\mathcal{X}',T'}(x) + O(1), \;\; x \in X(\kappa).$$

Proof. We consider first the case that $\mathcal{X} = \mathcal{X}'$. Let $\ell \neq 0$ be a section to L. Since $X(\mathbb{C})$ is compact, there exist constants $C_1, C_2 > 0$ such that

$$C_1 \leq \frac{|\ell(z)|_v}{|\ell(z)|'_v} \leq C_2, \;\; z \in X(\mathbb{C}).$$

This shows that the Archimedean pieces of $\hbar_{\mathcal{L},\mathcal{X},T}$ and $\hbar_{\mathcal{L}',\mathcal{X},T'}$ differ by a bounded amount.

Next, since $\mathcal{L}' \otimes \mathcal{L}^{-1}$ is trivial on the generic fiber of $\mathcal{X}$, there exists a vertical divisor E such that $\mathcal{L}' = \mathcal{L} \otimes [E]$. The line bundle $[E]$ is trivial when restricted to the generic fiber; hence it may be equipped with the trivial metric, and then the function

$$x \longmapsto \deg \tilde{x}^*[E]$$

is bounded for $x \in X(\kappa)$. This takes care of the non-Archimedean pieces, which proves that $\hbar_{\mathcal{L},\mathcal{X},T}$ and $\hbar_{\mathcal{L}',\mathcal{X},T'}$ differ by a bounded amount.

Finally, we consider the effect of choosing different models $\mathcal{X}$ and $\mathcal{X}'$. We may suppose that there is a birational morphism $f : \mathcal{X}' \longrightarrow \mathcal{X}$ that is the identity on the generic fiber. We then choose $\mathcal{L}' := f^*\mathcal{L}$, and we take as a metric on $\mathcal{L}'$ the pullback of the metric on $\mathcal{L}$. If $x \in X(\kappa)$, then the corresponding sections

$$\bar{x}' : \operatorname{Spec} \mathcal{O}_\kappa \longrightarrow \mathcal{X}', \quad \bar{x} : \operatorname{Spec} \mathcal{O}_\kappa \longrightarrow \mathcal{X}$$

are linked by $\bar{x} = f \circ \bar{x}'$. Therefore,

$$\bar{x}^*\mathcal{L} = (f \circ \bar{x}')^*\mathcal{L} = \bar{x}'^*\mathcal{L}',$$

so in this case we get an equality $\hbar_{\mathcal{L},\mathcal{X},T}(x) = \hbar_{\mathcal{L}',\mathcal{X}',T'}(x)$. □

A *metrized height function* (*associated to* L) is any function $\hbar_L$ of the form $\hbar_{\mathcal{L},\mathcal{X},T}$ for any model $\mathcal{X} \longrightarrow \operatorname{Spec} \mathcal{O}_\kappa$ for X, any extension $\mathcal{L}$ of L to $\mathcal{X}$, and any choice of metrics (4.51) on L.

Theorem 4.49. *Let κ be a number field and let X/κ be a smooth projective variety.*

(A) *The usual Weil height h on $\mathbb{P}^n(\kappa)$ is a metrized height on $\mathbb{P}^n$ associated to the hyperplane line bundle H.*

(B) *Let $\varphi : X' \longrightarrow X$ be a morphism of projective varieties, let L be a line bundle on X, and let $\hbar_L$ be a metrized height function for L. Then $\hbar_L \circ \varphi$ is a metrized height function for the line bundle φ^*L on X'.*

(C) *Let L and L' be line bundles on X, and choose metrized heights $\hbar_L$ and $\hbar_{L'}$ for L and L', respectively. Then $\hbar_L + \hbar_{L'}$ is a metrized height function associated to $L \otimes L'$.*

(D) *If L is the trivial bundle on X, then $\hbar_L = 0$ is a metrized height function for L.*

(E) *There is a metrized height $\hbar_L$ for L such that $\hbar_L(x) \ge 0$ for all x not in the base locus of L.*

Proof. (A) Take $X = \mathbb{P}^n$ and let $L = H$ be the hyperplane line bundle on $\mathbb{P}^n$. We choose $\mathcal{X} = \mathbb{P}^n_{\mathcal{O}_\kappa}$ with an extension $\mathcal{H}$ of H to $\mathbb{P}^n_{\mathcal{O}_\kappa}$. Fix

$$\alpha = (\alpha_0, \dots, \alpha_n) \in \bar{\kappa}^{n+1} - \{0\}.$$

For $x \in \mathbb{P}^n(\kappa)$, there exists

$$\xi = (\xi_0, \dots, \xi_n) \in \kappa^{n+1} - \{0\}$$

such that $x = \mathbb{P}(\xi)$. Then α determines uniquely a global section s to H given by

$$\langle \xi, \alpha \rangle = \alpha_0\xi_0 + \cdots + \alpha_n\xi_n,$$

up to a non-zero multiple. The *Fubini–Study metric* on H is defined by the formula

$$|s(x)|_v = \frac{|\langle \xi, \alpha \rangle|_v}{|\xi|_v}.$$

Then the associated metrized height function is

$$\hbar_{\mathcal{H},\mathcal{X},T}(x) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in M_\kappa} \log \frac{1}{|s(x)|_v^{n_v}} = h(x).$$

(B) Fix a model $\mathcal{X}$ for X, an extension $\mathcal{L}$ for L to $\mathcal{X}$, and metrics (4.51) on L corresponding to the selected metrized height $\hbar_L$. Choose a model $\mathcal{X}'$ for X' such that φ extends to a morphism $\bar{\varphi} : \mathcal{X}' \longrightarrow \mathcal{X}$. To do this, first choose any $\mathcal{X}'$. Then φ extends to a rational mapping, and we can blow up to resolve the indeterminacy (see Hartshorne [90], II. 7.17.3). We take $\bar{\varphi}^*\mathcal{L}$ as a model for φ^*L and the pullback metrics

$$|\varphi^*(s)|_v = |s|_v$$

as metrics on φ^*L, and then the equality

$$\hbar_{\varphi^*L} = \hbar_L \circ \varphi$$

is clear.

(C) Fix a model $\mathcal{X}$ for X, extensions $\mathcal{L}$ and $\mathcal{L}'$ for L and L' to $\mathcal{X}$, and metrics $T = \{|\cdot|_v\}_{v \in M_\kappa^\infty}$ and $T' = \{|\cdot|'_v\}_{v \in M_\kappa^\infty}$ on L and L', corresponding to the choice of metrized heights $\hbar_L$ and $\hbar_{L'}$. We take $\mathcal{L} \otimes \mathcal{L}'$ as an extension of $L \otimes L'$, and we take

$$|s \otimes s'|_v = |s|_v |s'|'_v$$

as the family of metrics on $L \otimes L'$. Letting $\hbar_{L \otimes L'}$ be the associated metrized height, the equality

$$\hbar_{L \otimes L'} = \hbar_L + \hbar_{L'}$$

is then clear from the definition of metrized height.

(D) The trivial metric on the trivial line bundle gives the zero function.

(E) Take any model $\mathcal{X}$ for X, any extension $\mathcal{L}$ of L to $\mathcal{X}$, and any set of metrics $T = \{|\cdot|_v\}_{v \in M_\kappa^\infty}$ on L. Let s be any nonzero section to L, and let $\bar{s}$ be its unique extension to $\mathcal{L}$. We can use the section $\bar{x}^*\bar{s}$ to $\bar{x}^*\mathcal{L}$ to compute

$$\hbar_{\mathcal{L},\mathcal{X},T}(x) = \frac{1}{[\kappa : \mathbb{Q}]} \log \#(\bar{x}^*\mathcal{L}/\bar{s}(x)\mathcal{O}_\kappa) + \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in M_\kappa^\infty} \log \frac{1}{|s(x)|_v^{n_v}}.$$

The first term on the right-hand side is clearly nonnegative. To deal with the sum of Green functions for L over Archimedean places, we write

$$|s|_\infty = \sup_{v \in M_\kappa^\infty,\ x \in X(\kappa_v)} |s(x)|_v.$$

Note that $|s|_\infty$ is finite, because $X(\mathbb{C})$ is compact and the various norms are continuous. Further, we need only a finite number of sections to define the base locus of L, so we have proven that there is a constant c (depending on all of our choices) such that

$$\hbar_{\mathcal{L},\mathcal{X},T}(x) \geq -c$$

for all x not in the base locus of L. Hence if we replace the original metrics by the equivalent metrics

$$|s|'_v := e^{-c}|s|_v,$$

we obtain a metrized height that is nonnegative off of the base locus of L. □

Here we follow the proof of Theorem B.10.7 in Hindry and Silverman [98]. Theorem 4.49 shows that metrized height functions are Weil heights, since the normalization property (A), the functoriality property (B) just for embeddings $X \longmapsto \mathbb{P}^N$, and the additivity property (C) determine the height functions up to $O(1)$. The point is that if L is very ample with associated embedding $\varphi_L : X \longrightarrow \mathbb{P}^N$, then (A) and (B) imply that

$$\hbar_L = h \circ \varphi_L + O(1) = h_L + O(1). \tag{4.54}$$

This determines the height function for very ample line bundles. But any line bundle L can be written as the product $L_1 \otimes L_2^{-1}$ of very ample line bundles L_1 and L_2, so the additivity (C) forces us to define

$$\hbar_L = \hbar_{L_1} - \hbar_{L_2} + O(1) = h_L + O(1). \tag{4.55}$$

Let S be a finite set of places of M_κ containing the Archimedean places. According to the expression (4.49), the valence function for D is of the form:

$$N(x, D) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in M_\kappa - S} m_v \log \mathcal{N}(\mathfrak{p}_v) + O(1).$$

Fix an positive integer m. Then we may define the *truncated valence function*

$$N_m(x, D) = N_{S,m}(x, D) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in M_\kappa - S} \min\{m, m_v\} \log \mathcal{N}(\mathfrak{p}_v) \tag{4.56}$$

of x to multiplicity m for each effective divisor D on X. Usually, we also write

$$\overline{N}(x, D) = \overline{N}_S(x, D) := N_1(x, D). \tag{4.57}$$

If $\mathbb{Q} \subset \kappa \subset K$ are finite separable algebraic extensions, then we have a finite morphism $\mathbb{M}_K \longrightarrow \mathbb{M}_\kappa$. In this case, let $R_{K/\kappa}$ denote the Arakelov divisor on $\mathbb{M}_K$ such that its restriction on $\operatorname{Spec} \mathcal{O}_K$ is the ramification divisor of the corresponding

mapping $\operatorname{Spec}\mathcal{O}_K \longrightarrow \operatorname{Spec}\mathcal{O}_\kappa$, and such that the corresponding Green functions are all zero. Thus $R_{K/\kappa}$ is of the form

$$R_{K/\kappa} = \sum_{w\in M_K^0} \operatorname{length}\{(\Omega_{\mathcal{O}_K/\mathcal{O}_\kappa})_{\mathfrak{p}_w}\}\mathfrak{p}_w. \tag{4.58}$$

We then define

$$\begin{aligned} d_{K/\kappa,S} &= \frac{1}{[K:\mathbb{Q}]}\deg_{M_K-S} R_{K/\kappa} \\ &= \frac{1}{[K:\mathbb{Q}]}\sum_{w\in M_K-S} \operatorname{length}\{(\Omega_{\mathcal{O}_K/\mathcal{O}_\kappa})_{\mathfrak{p}_w}\}\log\mathcal{N}(\mathfrak{p}_w), \end{aligned} \tag{4.59}$$

where $M_K - S$ is the set in which each valuation is an extension of some element in $M_\kappa - S$. In particular, we define the *logarithmic discriminant of K with respect to κ* as follows

$$d_{K/\kappa} = \frac{1}{[K:\mathbb{Q}]}\sum_{w\in M_K^0} \operatorname{length}\{(\Omega_{\mathcal{O}_K/\mathcal{O}_\kappa})_{\mathfrak{p}_w}\}\log\mathcal{N}(\mathfrak{p}_w). \tag{4.60}$$

Obviously, one has

$$0 \le d_{K/\kappa} - d_{K/\kappa,S} \le O(1). \tag{4.61}$$

If we have a tower $\kappa \subseteq K \subseteq L$, then

$$d_{L/\kappa,S} - d_{K/\kappa,S} = \frac{1}{[L:\mathbb{Q}]}\deg_{M_L-S} R_{L/K}. \tag{4.62}$$

By Theorem 1.121, we have

$$d_{K/\kappa} = \frac{1}{[K:\mathbb{Q}]}\log\mathcal{N}(\mathfrak{d}_{K/\kappa}), \tag{4.63}$$

and hence (1.59) and Theorem 2.42 yield

$$d_{K/\kappa} = \frac{1}{[K:\mathbb{Q}]}\log\mathcal{N}(\mathfrak{D}_{K/\kappa}). \tag{4.64}$$

Thus (2.37) implies

$$d_{K/\kappa} = \frac{1}{[K:\mathbb{Q}]}\log|D_{K/\mathbb{Q}}| - \frac{1}{[\kappa:\mathbb{Q}]}\log|D_{\kappa/\mathbb{Q}}|, \tag{4.65}$$

where

$$d_{\kappa/\mathbb{Q}} = \frac{1}{[\kappa:\mathbb{Q}]}\log|D_{\kappa/\mathbb{Q}}| \tag{4.66}$$

is just the *absolute* (*logarithmic*) *discriminant* of κ (cf. P. Vojta [287]).

Arakelov theory may be extended to a complete variety (cf. [293]).

4.6 Canonical heights on Abelian varieties

4.6.1 Periodic points

Let X be a smooth variety defined over a number field κ and let $f : X \longrightarrow X$ be a morphism. For each $n \geq 1$, let

$$f^n = f \circ f \circ \cdots \circ f : X \longrightarrow X$$

denote the n-th iterate of f. An element $x \in X$ is called *periodic* for f if $f^n(x) = x$ for some $n \geq 1$, and it is called *preperiodic* for f if $f^n(x)$ is periodic for some $n \geq 1$. Equivalent, x is preperiodic if its *forward orbit*

$$O^+(x) = \{x, f(x), f^2(x), \ldots\}$$

is finite.

Take $D \in \mathrm{Div}(X)$ such that $f^*D \sim \alpha D$ for some number $\alpha > 1$. Applying Theorem 4.34 to the relation $f^*D \sim \alpha D$, there exists a constant c such that

$$|h_D(f(x)) - \alpha h_D(x)| \leq c$$

hold for all $x \in X$. Take two integers n and m with $n > m \geq 0$. We have

$$\begin{aligned}
\left| \frac{h_D\left(f^n(x)\right)}{\alpha^n} - \frac{h_D\left(f^m(x)\right)}{\alpha^m} \right| &= \left| \sum_{i=m+1}^{n} \left\{ \frac{h_D(f^i(x))}{\alpha^i} - \frac{h_D(f^{i-1}(x))}{\alpha^{i-1}} \right\} \right| \\
&\leq \sum_{i=m+1}^{n} \frac{c}{\alpha^i} \\
&= \frac{c}{\alpha - 1} \left(\frac{1}{\alpha^m} - \frac{1}{\alpha^n} \right). \qquad (4.67)
\end{aligned}$$

The last quantity goes to 0 as $n, m \to \infty$, which shows that $\{\alpha^{-n} h_D(f^n(x))\}$ is a Cauchy's sequence, hence converges. Néron and Tate studied the *canonical height* on X relative to f and D

$$\hbar_{D,f}(x) = \lim_{n \to \infty} \frac{1}{\alpha^n} h_D\left(f^n(x)\right), \qquad (4.68)$$

with the following two properties:

(i) $\hbar_{D,f}(x) = h_D(x) + O(1)$ for all $x \in X$.

(ii) $\hbar_{D,f}(f(x)) = \alpha \hbar_{D,f}(x)$ for all $x \in X$.

In fact, the property (ii) follows directly from (4.68), and the property (i) follows from the inequality (4.67) by taking $m = 0$ and letting $n \to \infty$, which is of the explicit form

$$|\hbar_{D,f}(x) - h_D(x)| \leq \frac{c}{\alpha - 1}.$$

The canonical height $\hat{h}_{D,f}$ is unique. In fact, suppose that h and h' are two functions with properties (i) and (ii). Then (i) implies that $h - h'$ is bounded, say

$$|h(x) - h'(x)| \le c_1, \ \ x \in X.$$

On the other hand, the property (ii) means that

$$h(f(x)) - h'(f(x)) = \alpha\{h(x) - h'(x)\},$$

and iterating this relation yields

$$h(f^n(x)) - h'(f^n(x)) = \alpha^n\{h(x) - h'(x)\}, \ \ n \ge 1.$$

Thus we obtain

$$|h(x) - h'(x)| \le \frac{c_1}{\alpha^n} \to 0$$

as $n \to \infty$. This shows that $h = h'$.

Theorem 4.50. *Let $f : X \longrightarrow X$ be a morphism of a smooth variety defined over a number field κ. Let $D \in \mathrm{Div}(X)$ be an ample divisor such that $f^*D \sim \alpha D$ for some $\alpha > 1$. Then $\hat{h}_{D,f}(x) \ge 0$ for all $x \in X$, and $\hat{h}_{D,f}(x) = 0$ if and only if x is preperiodic for f. In particular, the set*

$$\{x \in X(\kappa) \mid x \text{ is preperiodic for } f\}$$

is finite.

Proof. Since D is ample, we can choose a height function h_D with nonnegative values. It is then immediate from (4.68) that $\hat{h}_{D,f}$ is nonnegative. Now take $x \in X(\bar{\kappa})$. Replacing κ by a finite extension, we may assume that $x \in X(\kappa)$ and that D and f are defined over κ. If x is preperiodic for f, then the forward orbit $O^+(x)$ repeats, so the sequence $\{h_D(f^n(x)\}$ is bounded. It follows that

$$\hat{h}_{D,f}(x) = \lim_{n\to\infty} \frac{1}{\alpha^n} h_D\left(f^n(x)\right) = 0.$$

Conversely, if $\hat{h}_{D,f}(x) = 0$, then for any integer $n \ge 1$ we have

$$h_D(f^n(x)) = \hat{h}_{D,f}(f^n(x)) + O(1) = \alpha^n \hat{h}_{D,f}(x) + O(1) = O(1).$$

Since all of points $f^n(x)$ are in $X(\kappa)$, there exists a constant r_0 such that

$$O^+(x) \subset \{y \in X(\kappa) \mid h_D(y) \le r_0\}.$$

By Theorem 4.34 (7), the set $O^+(x)$ is finite, and so x is preperiodic for f. □

Theorem 4.50 shows a relation between height functions and dynamics (see [98], Theorem B.4.2). The finiteness of preperiodic points is due to Northcott [208].

Corollary 4.51. *If $f : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ is a morphism of degree $d \geq 2$, then the set*

$$\{x \in \mathbb{P}^n(\kappa) \mid x \text{ is preperiodic for } f\}$$

is finite.

Proof. Since $f^*H \sim dH$ for any hyperplane $H \in \mathrm{Div}(\mathbb{P}^n)$, the corollary follows immediately from Theorem 4.50. □

Corollary 4.52. *Let A be an Abelian variety and let $D \in \mathrm{Div}(A)$ be an ample symmetric divisor (i.e. $[-1]^*D \sim D$). Then for each integer $n \geq 2$, $A(\kappa)$ has only finitely many points that are preperiodic for $[n]$.*

Proof. Take any $D \in \mathrm{Div}(A)$. Applying Proposition 3.47 with $\varphi = [n]$, $\psi = [1]$ and $\chi = [-1]$ to obtain

$$[n+1]^*D + [n-1]^*D - 2[n]^*D \sim D + [-1]^*D. \tag{4.69}$$

Now an easy induction, both upwards and downwards from $n = 0$, gives the *Mumford's formula* (or cf. [98], Corollary A.7.2.5):

$$[n]^*D \sim \left(\frac{n^2+n}{2}\right) D + \left(\frac{n^2-n}{2}\right) [-1]^*D. \tag{4.70}$$

In particular,

$$[n]^*D \sim \begin{cases} n^2 D, & \text{if } D \text{ is symmetric,} \\ nD, & \text{if } D \text{ is antisymmetric } ([-1]^*D \sim -D). \end{cases} \tag{4.71}$$

Therefore, if $D \in \mathrm{Div}(A)$ is an ample symmetric divisor, we can apply Theorem 4.50 to conclude Corollary 4.52. □

Note that $x \in A$ is preperiodic for $[n]$ if and only if there are integers $i > j$ such that

$$[n^i]x = [n^j]x,$$

so it follows that the preperiodic points for $[n]$ are precisely the torsion points. Hence

$$A_{\mathrm{tors}}(\kappa) = \{x \in A(\kappa) \mid [m]x = e_A,\ m \geq 1\}$$

is finite.

4.6.2 Canonical heights

Theorem 4.53. *Let A be an Abelian variety defined over a number field κ, and let $D \in \mathrm{Div}(A)$ be a divisor whose divisor class is symmetric. The canonical height $\hat{h}_{D,[2]}$ on A relative to D satisfies the following properties:*

(a) *For all $x \in A(\bar{\kappa})$,*

$$\hat{h}_{D,[2]}(x) = h_D(x) + O(1).$$

(b) *For all integers m, and for all $x \in A(\bar{\kappa})$,*

$$\hat{h}_{D,[2]}([m]x) = m^2 \hat{h}_{D,[2]}(x).$$

(c) (*Uniqueness*) *The canonical height $\hat{h}_{D,[2]}$ depends only on the divisor class of the divisor D. It is uniquely determined by* (a) *and* (b) *for any integer $m \geq 2$.*

(d) (*Parallelogram law*) *For all $x, y \in A(\bar{\kappa})$,*

$$\hat{h}_{D,[2]}(x+y) + \hat{h}_{D,[2]}(x-y) = 2\hat{h}_{D,[2]}(x) + 2\hat{h}_{D,[2]}(y).$$

(e) *The canonical height $\hat{h}_{D,[2]} : A(\bar{\kappa}) \longrightarrow \mathbb{R}$ is a quadratic form. The associated pairing $\langle , \rangle : A(\bar{\kappa}) \times A(\bar{\kappa}) \longrightarrow \mathbb{R}$ defined by*

$$\langle x, y \rangle_D = \frac{1}{2}\left\{\hat{h}_{D,[2]}(x+y) - \hat{h}_{D,[2]}(x) - \hat{h}_{D,[2]}(y)\right\}$$

is bilinear and satisfies $\langle x, x \rangle_D = \hat{h}_{D,[2]}(x)$.

Proof. Note that $[2]^*D \sim 4D$ from (4.71), so we can apply (4.68) to obtain

$$\hat{h}_{D,[2]}(x) = \lim_{n\to\infty} \frac{1}{4^n} h_D\left([2^n]x\right).$$

Then (a) and (b) with $m = 2$ follow respectively from the properties (i) and (ii) with $f = [2]$. The relation (4.71) tells us that

$$h_D([m]y) = m^2 h_D(y) + O(1)$$

holds for all $y \in A(\bar{\kappa})$, where $O(1)$ is bounded independently of y. We replace y by $[2]^n x$, divide by 4^n, and let $n \to \infty$. The result is

$$\begin{aligned} \hat{h}_{D,[2]}([m]x) &= \lim_{n\to\infty} \frac{1}{4^n} h_D\left([2^n][m]x\right) \\ &= \lim_{n\to\infty} \frac{1}{4^n}\left(m^2 h_D\left([2^n]x\right) + O(1)\right) = m^2 \hat{h}_{D,[2]}(x), \end{aligned}$$

where one uses the fact the mappings $[m]$ and $[2^n]$ commute with one another. This completes the proof of (b).

The uniqueness statement (c) follows from the uniqueness assertion of the canonical height $\hbar_{D,f}$ applied to $f = [2]$.

To prove (d), use the relation

$$h_D(x+y) + h_D(x-y) = 2h_D(x) + 2h_D(y) + O(1) \tag{4.72}$$

which is satisfied by arbitrary symmetric divisors on A (see [98], Corollary B.3.4). Thus the parallelogram law (d) follows if we replace x and y by $[2^n]x$ and $[2^n]y$, divide by 4^n, and let $n \to \infty$.

Finally, putting $x = y = e_A$ into the parallelogram law (d) gives $\hbar_{D,[2]}(e_A) = 0$, and then putting $x = e_A$ gives

$$\hbar_{D,[2]}(-y) = \hbar_{D,[2]}(y),$$

so $\hbar_{D,[2]}$ is an even function. We apply the parallelogram law four times to obtain

$$\begin{aligned}
0 &= \hbar_{D,[2]}(x+z+y) + \hbar_{D,[2]}(x+z-y) - 2\hbar_{D,[2]}(x+z) - 2\hbar_{D,[2]}(y),\\
0 &= \hbar_{D,[2]}(x+z-y) + \hbar_{D,[2]}(x-z+y) - 2\hbar_{D,[2]}(x) - 2\hbar_{D,[2]}(z-y),\\
0 &= \hbar_{D,[2]}(x-z+y) + \hbar_{D,[2]}(x+z+y) - 2\hbar_{D,[2]}(x+y) - 2\hbar_{D,[2]}(z),\\
0 &= 2\hbar_{D,[2]}(z+y) + 2\hbar_{D,[2]}(z-y) - 4\hbar_{D,[2]}(z) - 4\hbar_{D,[2]}(y).
\end{aligned}$$

The alternating sum of these four equations gives

$$\langle x+z, y\rangle_D = \langle x, y\rangle_D + \langle z, y\rangle_D,$$

which yields the desired result (e). □

Proposition 4.54. *Let A be an Abelian variety defined over a number field κ, and let $D \in \mathrm{Div}(A)$ be an ample divisor with symmetric divisor class.*

(f) *For all $x \in A(\bar{\kappa})$, we have $\hbar_{D,[2]}(x) \ge 0$, with equality if and only if x is a point of finite order.*

(g) *The associated canonical height function extends $\mathbb{R}$-linearly to a positive definite quadratic form*

$$\hbar_{D,[2]} : A(\bar{\kappa}) \otimes \mathbb{R} \longrightarrow \mathbb{R}.$$

In particular, if $x_1, \ldots, x_r \in A(\bar{\kappa}) \otimes \mathbb{R}$ are linearly independent, then the height regulator

$$\det(\langle x_i, x_j\rangle_D)_{1\le i,j\le r}$$

is strictly greater than 0.

Proof. See [98], Proposition B.5.3. □

Theorem 4.55. *Let A be an Abelian variety defined over a number field κ, and let $D \in \mathrm{Div}(A)$ be a divisor whose divisor class is antisymmetric. The canonical height $\hbar_{D,[2]}$ on A relative to D satisfies the following properties:*

(A) *For all $x \in A(\bar{\kappa})$,*

$$\hbar_{D,[2]}(x) = h_D(x) + O(1).$$

(B) *For all integers m, and for all $x \in A(\bar{\kappa})$,*

$$\hbar_{D,[2]}([m]x) = m\hbar_{D,[2]}(x).$$

(C) (*Uniqueness*) *The canonical height $\hbar_{D,[2]}$ depends only on the divisor class of the divisor D. It is uniquely determined by* (a) *and* (b) *for any one integer $m \geq 2$.*

(D) *For all $x, y \in A(\bar{\kappa})$,*

$$\hbar_{D,[2]}(x+y) = \hbar_{D,[2]}(x) + \hbar_{D,[2]}(y).$$

Proof. The proof is almost the same as the proof of Theorem 4.53, here we merely give a sketch of (D). To do it, use the relation

$$h_D(x+y) = h_D(x) + h_D(y) + O(1) \tag{4.73}$$

which is satisfied by arbitrary antisymmetric divisors on A (see [98], Corollary B.3.4). Now replace x and y by $[2^n]x$ and $[2^n]y$, divide by 2^n, and let $n \to \infty$ to obtain (D).□

Generally, if $D \in \mathrm{Div}(A)$ is an arbitrary divisor on the Abelian variety A, define divisors

$$D^+ = D + [-1]^*D, \quad D^- = D - [-1]^*D.$$

It is clear that D^+ is symmetric and D^- is antisymmetric. Then a unique quadratic function $\hat{h}_D : A(\bar{\kappa}) \longrightarrow \mathbb{R}$ is defined by

$$\hat{h}_D = \frac{1}{2}\left(\hbar_{D^+,[2]} + \hbar_{D^-,[2]}\right), \tag{4.74}$$

called the *canonical height* on A relative D.

4.6.3 Tate–Shafarevich groups

Let κ be a number field and let A be an Abelian variety over κ. Recall that the multiplication mapping $[m] : A(\bar{\kappa}) \longrightarrow A(\bar{\kappa})$ is surjective with finite kernel, denoted by $A[m]$, and that $A[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$.

For each $x \in A(\kappa)$, we select a point $y \in A(\bar{\kappa})$ satisfying $[m]y = x$, and then we define a mapping $t_y : G_{\bar{\kappa}/\kappa} \longrightarrow A[m]$ by $t_y(\sigma) = \sigma(y) - y$ for each $\sigma \in G_{\bar{\kappa}/\kappa}$. Note that $\sigma(y) - y \in A[m]$, since

$$[m](\sigma(y) - y) = \sigma([m]y) - [m]y = \sigma(x) - x = 0.$$

We also have

$$\begin{aligned} t_y(\sigma'\sigma) &= \sigma'\sigma(y) - y = \sigma'(\sigma(y) - y) + \sigma'(y) - y \\ &= \sigma'(t_y(\sigma)) + t_y(\sigma'). \end{aligned}$$

In other words, the mappings t_y is a 1-cocycle from G to $A[m]$.

Take other $y' \in A(\bar{\kappa})$ such that $[m]y' = x$. Then the point $a = y' - y \in A[m]$ satisfies

$$t_{y'}(\sigma) - t_y(\sigma) = (\sigma(y') - y') - (\sigma(y) - y) = \sigma(a) - a.$$

Thus the difference $t_{y'} - t_y$ is a coboundary, so the cohomology class of t_y in $H^1(G_{\bar{\kappa}/\kappa}, A[m])$ depends only on x, independent of the choice of y. In other words, we get a well-defined mapping

$$\delta : A(\kappa) \longrightarrow H^1(G_{\bar{\kappa}/\kappa}, A[m]). \tag{4.75}$$

Let $\alpha : A \longrightarrow B$ be an isogeny of two Abelian varieties defined over κ. Then the short exact sequence

$$0 \to \mathrm{Ker}(\alpha) \xrightarrow{\iota} A(\bar{\kappa}) \xrightarrow{\alpha} B(\bar{\kappa}) \to 0 \tag{4.76}$$

induces a long exact sequence of cohomology groups

$$\begin{aligned} 0 \;&\to\; \mathrm{Ker}(\alpha)(\kappa) \xrightarrow{\iota} A(\kappa) \xrightarrow{\alpha} B(\kappa) \\ &\xrightarrow{\delta}\; H^1(G_{\bar{\kappa}/\kappa}, \mathrm{Ker}(\alpha)) \xrightarrow{\iota} H^1(G_{\bar{\kappa}/\kappa}, A(\bar{\kappa})) \xrightarrow{\alpha} H^1(G_{\bar{\kappa}/\kappa}, B(\bar{\kappa})). \end{aligned} \tag{4.77}$$

The homomorphism δ is defined as follows: Take $x \in B(\kappa)$, and choose $y \in A(\bar{\kappa})$ such that $\alpha(y) = x$. Then define $\delta(x)$ to be the cohomology class associated to the cocycle

$$\delta(x) : G_{\bar{\kappa}/\kappa} \longrightarrow \mathrm{Ker}(\alpha), \;\; \delta(x)(\sigma) = \sigma(y) - y.$$

The above long exact sequence gives rise to the following fundamental short exact sequence:

$$0 \to B(\kappa)/\alpha(A(\kappa)) \xrightarrow{\delta} H^1(G_{\bar{\kappa}/\kappa}, \mathrm{Ker}(\alpha)) \to H^1(G_{\bar{\kappa}/\kappa}, A(\bar{\kappa}))[\alpha] \to 0, \tag{4.78}$$

where $H^1(G_{\bar{\kappa}/\kappa}, A(\bar{\kappa}))[\alpha]$ denotes the kernel of the mapping

$$\alpha : H^1(G_{\bar{\kappa}/\kappa}, A(\bar{\kappa})) \longrightarrow H^1(G_{\bar{\kappa}/\kappa}, B(\bar{\kappa})).$$

For each place v of κ, let κ_v be the completion of κ at v. We may consider $G_{\bar{\kappa_v}/\kappa_v}$ to be a subgroup of $G_{\bar{\kappa}/\kappa}$. Then for an arbitrary Abelian group $\mathscr{A}$ on which $G_{\bar{\kappa}/\kappa}$ acts we obtain restriction homomorphisms

$$H^1(G_{\bar{\kappa}/\kappa}, \mathscr{A}) \longrightarrow H^1(G_{\bar{\kappa_v}/\kappa_v}, \mathscr{A}).$$

There is a local exact sequence analogous to the exact sequences (4.77) and (4.78), and the global exact sequence maps to the local exact sequence via restriction, yielding the following commutative diagram:

$$\begin{array}{ccccccccc} 0 \to & B(\kappa)/\alpha(A(\kappa)) & \xrightarrow{\delta} & H^1(G_{\bar\kappa/\kappa}, \mathrm{Ker}(\alpha)) & \to & H^1(G_{\bar\kappa/\kappa}, A(\bar\kappa))[\alpha] & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & B(\kappa_v)/\alpha(A(\kappa_v)) & \xrightarrow{\delta_v} & H^1(G_{\bar\kappa_v/\kappa_v}, \mathrm{Ker}(\alpha)) & \to & H^1(G_{\bar\kappa_v/\kappa_v}, A(\bar\kappa_v))[\alpha] & \to 0. \end{array}$$

The *Selmer group of A with respect to α* is the group

$$\mathrm{Sel}^{(\alpha)}(A/\kappa) = \bigcap_v \mathrm{Ker}\left\{H^1(G_{\bar\kappa/\kappa}, \mathrm{Ker}(\alpha)) \to H^1(G_{\bar\kappa_v/\kappa_v}, A(\bar\kappa_v))[\alpha]\right\}.$$

The *Tate-Shafarevich group of A* is the group

$$Ш(A/\kappa) = \bigcap_v \mathrm{Ker}\left\{H^1(G_{\bar\kappa/\kappa}, A(\bar\kappa)) \to H^1(G_{\bar\kappa_v/\kappa_v}, A(\bar\kappa_v))\right\}.$$

In both formulae, v is taken over all places of κ. From the exact sequences (4.77) and (4.78), one deduces the following important exact sequence

$$0 \to B(\kappa)/\alpha(A(\kappa)) \to \mathrm{Sel}^{(\alpha)}(A/\kappa) \to Ш(A/\kappa)[\alpha] \to 0.$$

Conjecture 4.56. *Let A be an Abelian variety defined over a number field κ. Then $Ш(A/\kappa)$ is finite.*

4.6.4 Mordell–Weil theorem

Let κ be a number field and let A be an Abelian variety of dimension g over κ. We continue to study $A[m]$. Without loss of generality, we may assume that $A[m] \subset A(\kappa)$.

For each $x \in A(\kappa)$, we select a point $y \in A(\bar\kappa)$ satisfying $[m]y = x$, and then for each $\sigma \in G_{\bar\kappa/\kappa}$ we define

$$\langle \sigma, x\rangle = \sigma(y) - y \in A[m].$$

We verify below that the value of $\langle \sigma, x\rangle$ depends only on x, and not on the choice of y. So suppose that

$$[m]y' = [m]y = x.$$

Then $y' - y \in A[m] \subset A(\kappa)$, hence

$$\{\sigma(y) - y\} - \{\sigma(y') - y'\} = \sigma(y - y') - (y - y') = 0.$$

The resulting mapping

$$\langle\, ,\rangle : G_{\bar\kappa/\kappa} \times A(\kappa) \longrightarrow A[m] \tag{4.79}$$

is called the *Kummer pairing on* A, which is bilinear. We start with the first variable:

$$\begin{aligned}\langle \sigma'\sigma, x\rangle &= \sigma'\sigma(y) - y = \sigma'(\sigma(y) - y) + \sigma'(y) - y \\ &= \sigma'(\langle \sigma, x\rangle) + \langle \sigma', x\rangle = \langle \sigma, x\rangle + \langle \sigma', x\rangle.\end{aligned}$$

Next we compute

$$\begin{aligned}\langle \sigma, x + x'\rangle &= \sigma(y + y') - (y + y') = \sigma(y) - y + \sigma(y') - y' \\ &= \langle \sigma, x\rangle + \langle \sigma, x'\rangle.\end{aligned}$$

This completes the proof of the bilinearity of t.

Proposition 4.57. *Let K be the extension of κ obtained by adjoining to κ the coordinates of all points $y \in A(\bar{\kappa})$ satisfying $[m]y \in A(\kappa)$.*

(1) *The Kummer pairing induces a nondegenerate pairing*

$$\langle\, ,\rangle : G_{K/\kappa} \times A(\kappa)/mA(\kappa) \longrightarrow A[m].$$

In particular, $A(\kappa)/mA(\kappa)$ is finite if and only if K is a finite extension of κ.

(2) *The field K is a finite Galois extension of κ with Galois group*

$$G_{K/\kappa} \cong (\mathbb{Z}/m\mathbb{Z})^{s+1}$$

for some integer s.

Proof. The kernel of the Kummer pairing on the right consists of those x such that $\langle \sigma, x\rangle = 0$ for all $\sigma \in G_{\bar{\kappa}/\kappa}$. This means that $\sigma(y) = y$ for all $\sigma \in G_{\bar{\kappa}/\kappa}$, and hence that $y \in A(\kappa)$ and $x = [m]y \in mA(\kappa)$. Note that the kernel contains $mA(\kappa)$. Therefore, the kernel is exactly $mA(\kappa)$.

Next we observe that the kernel of the Kummer pairing on the left consists of those σ such that $\sigma(y) = y$ for all $y \in A(\bar{\kappa})$ satisfying $[m]y \in A(\kappa)$. From the definition of K, this is equivalent to saying that $\sigma \in G_{\bar{\kappa}/K}$, which means that the kernel is $G_{\bar{\kappa}/K}$. Taking the quotient by the right and left kernels give a nondegenerate pairing as stated in (1).

For the proof of (2), see [98], Corollary C.1.8. □

Take $m \geq 2$. Based on Proposition 4.57, we get an injection (see [98]):

$$A(\kappa)/mA(\kappa) \longmapsto \mathrm{Hom}(G_{K/\kappa}, A[m]) \cong \mathrm{Hom}\left((\mathbb{Z}/m\mathbb{Z})^{s+1}, (\mathbb{Z}/m\mathbb{Z})^{2g}\right).$$

Clearly,

$$\#\mathrm{Hom}\left((\mathbb{Z}/m\mathbb{Z})^{s+1}, (\mathbb{Z}/m\mathbb{Z})^{2g}\right) = m^{2g(s+1)}.$$

On the other hand, since $A[m] \subset A(\kappa)$ by assumption, and since $\#A[m] = m^{2g}$, then the dimension r of group $A(\kappa)$ over $\mathbb{Z}$ satisfies

$$\#A(\kappa)/mA(\kappa) = m^{2g+r},$$

and hence $r \leq 2gs$. This shows the *Mordell–Weil theorem*:

Theorem 4.58. *Let A be an Abelian variety defined over a number field κ. Then the group $A(\kappa)$ of κ-rational points of A is finitely generated.*

In the special case that the Abelian variety is a cubic curve in the projective plane, the theorem is due to Mordell [190] whose original statement is for rational points. Weil, in his thesis, extended Mordell's theorem to arbitrary number fields and to Abelian varieties of higher dimension. Using elementary group theory and the structure of the kernel of multiplication by m, we may rephrase Theorem 4.58 by saying that there are points $P_1, \dots, P_r$ such that

$$A(\kappa) = A_{\mathrm{tors}}(\kappa) \oplus \mathbb{Z}P_1 \oplus \cdots \oplus \mathbb{Z}P_r.$$

The integer r is called the *rank* of the Abelian variety A/κ, and $A(\kappa)$ is the *Mordell–Weil group* of A/κ. Note that the torsion subgroup $A_{\mathrm{tors}}(\kappa)$ is a finite Abelian group, so it can be written as

$$A_{\mathrm{tors}}(\kappa) \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z},$$

where $m_1, \dots, m_s$ are integers satisfying $m_i | m_{i+1}$ and $s \le 2 \dim A$.

Chapter 5

The abc-conjecture

The abc-conjecture has been an important problem in number theory. This conjecture and its generalized forms for integers are counterparts of Nevanlinna's third main theorem and its variations in complex analysis.

5.1 The abc-theorem for function fields

For a non-zero polynomial f in $\mathbb{C}$, let $\deg^{(1)}(f)$ denote the number of distinct roots of f. Then one has *Stothers–Mason's theorem* (cf. [165], [166], [167], [268], or [79], [149], [287]):

Theorem 5.1. *Let $a(z),\ b(z),\ c(z)$ be relatively prime polynomials in $\mathbb{C}$ and not all constants such that $a+b=c$. Then*

$$\max\{\deg(a),\deg(b),\deg(c)\} \le \deg^{(1)}(abc)-1. \tag{5.1}$$

Proof. We consider the Wronskian determinant of a and b

$$\mathbf{W}=\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}.$$

We differentiate $a+b=c$ to get $a'+b'=c'$. It is easy to show that

$$\mathbf{W}=\begin{vmatrix} a & c \\ a' & c' \end{vmatrix}=\begin{vmatrix} c & b \\ c' & b' \end{vmatrix}.$$

Note that $\mathbf{W}\neq 0$, else $ab'-a'b=0$, that is, $(b/a)'=0$, so b is a scalar multiple of a, contradicting our statement that a and b have no common factor.

Suppose that α is a root of a and that $(z-\alpha)^l$ is the highest power of $z-\alpha$ which divides $a(z)$. Evidently $(z-\alpha)^{l-1}$ is the highest power of $z-\alpha$ which divides $a'(z)$, and thus it is the highest power of $z-\alpha$ which divides $\mathbf{W}(z)=a(z)b'(z)-a'(z)b(z)$ since α is not a root of b. Therefore $(z-\alpha)^l$ divides $\mathbf{W}(z)(z-\alpha)$. Multiplying all such $(z-\alpha)^l$ together, we obtain

$$a(z)\mid \mathbf{W}(z)\prod_{a(\alpha)=0}(z-\alpha).$$

Analogous statements for b and c are also true. Since a, b, c have no common roots, we can combine those statements to read

$$a(z)b(z)c(z) \mid \mathbf{W}(z) \prod_{(abc)(\alpha)=0} (z-\alpha). \tag{5.2}$$

Using the three different representations of $\mathbf{W}$ above, we have

$$\deg(\mathbf{W}) \leq \begin{cases} \deg(a)+\deg(b)-1, \\ \deg(a)+\deg(c)-1, \\ \deg(c)+\deg(b)-1. \end{cases}$$

The degree of $\prod_{(abc)(\alpha)=0}(z-\alpha)$ is precisely the total number $\deg^{(1)}(abc)$ of distinct roots of abc. Inserting all this into (5.2), we find the inequality (5.1). □

In particular, if

$$a(z) = (1+z)^2, \quad b(z) = -(1-z)^2, \quad c(z) = 4z,$$

then the inequality in Theorem 5.1 becomes the equality $2 = 2$ (cf. [83]). For applications of Theorem 5.1, see [166]; [201], pp. 183–185.

Let κ be a number field with algebraic closure $\bar{\kappa} = \bar{\mathbb{Q}}$. Belyĭ [9] constructs a function with the following property:

Theorem 5.2. *Let X be an algebraic curve defined over κ and let $D \subset X(\bar{\mathbb{Q}})$ be a finite set of algebraic points of X. Then there exists a morphism $f : X \longrightarrow \mathbb{P}^1$ defined over κ such that $f(D) \subseteq \{0, 1, \infty\}$ and f is only ramified over $\{0, 1, \infty\}$.*

Proof. For the proof, we refer the reader to Belyĭ [9], Serre [238], van Frankenhuysen [284]. □

Belyĭ [9] also proves the converse, that is, if $f : X \longrightarrow \mathbb{P}^1$ is ramified over three points alone, then X is defined over $\bar{\mathbb{Q}}$.

Let $f : X \longrightarrow \mathbb{P}^1$ be a morphism of a complete nonsingular curve X to the projective line. Let e_x denote the ramification index of f at $x \in X$. Thus, for any point $a \in \mathbb{P}^1$, the total index of the fiber over a is constant,

$$\sum_{x \in f^{-1}(a)} e_x = \deg(f).$$

By Riemann–Hurwitz formula (3.47), writing g for the genus of X,

$$2g-2 = -2\deg(f) + \sum_{x \in X}(e_x - 1) = -2\deg(f) + \sum_{a \in \mathbb{P}^1} \sum_{x \in f^{-1}(a)} (e_x - 1).$$

Counting only the ramification above $0, 1$ and ∞, we obtain

$$\deg(f) \leq 2g - 2 + \#f^{-1}\{0, 1, \infty\}. \tag{5.3}$$

This is the *abc-theorem for function fields*. The function f corresponds to the abc-sum $f + (1 - f) = 1$ of height $\deg(f)$ and radical $\#f^{-1}\{0, 1, \infty\}$. Equality holds if and only if f is a Belyĭ function. In that case, a canonical divisor of X is given by

$$K = (df/f) = f^*(1) - f^{-1}\{0, 1, \infty\}. \tag{5.4}$$

5.2 The abc-conjecture for integers

Many results for Diophantine equations in integers are analogous to results for Diophantine equations in polynomials. Lang ([152], p. 196) said: "One of the most fruitful analogies in mathematics is that between the integers $\mathbb{Z}$ and the ring of polynomials $F[t]$ over a field F." Given Mason's wonderfully simple inequality for polynomial solutions to $a + b = c$ (namely Theorem 5.1), one wonders whether there is a similar result for integers.

The *radical* of a non-zero integer A is defined to be

$$r(A) = \prod_{p|A} p$$

i.e. the product of distinct primes dividing A. On the other hand, we note that in Theorem 5.1 (cf. [201], p. 182 or [83])

$$\deg^{(1)}(f) = \deg(\mathrm{rad}(f)),$$

where $\mathrm{rad}(f)$ is the *radical* of a polynomial f on $\mathbb{C}$, which is the product of distinct irreducible factors of f.

There is a classical analogy between polynomials and integers, that is, prime factors of an integer are often considered to be an appropriate analogy to irreducible factors of a polynomial. Under that analogy, $\deg^{(1)}(f)$ of a polynomial f corresponds to $\log r(A)$ of an integer A, and in addition, the value $\log|A|$ of an integer A is a measure of how "large" the integer is, while the degree of a polynomial is a measure of how "large" the polynomial is (cf. [149] or [79]). Thus for polynomials we had an inequality formulated additively, whereas for integers we formulate the corresponding inequality multiplicatively.

After being influenced by Stothers–Mason's theorem (see Theorem 5.1), and based on considerations of Szpiro and Frey, Oesterlé [209] and Masser [169] formulated the *abc-conjecture* for integers as follows:

Conjecture 5.3. *Given $\varepsilon > 0$, there exists a number $C(\varepsilon)$ having the following property. For any nonzero relatively prime integers $a,\ b,\ c$ such that $a + b = c$, we have*

$$\max\{|a|, |b|, |c|\} \leq C(\varepsilon) r\,(abc)^{1+\varepsilon}\,. \tag{5.5}$$

An interesting discussion in [79] illustrates how one is naturally led from Theorem 5.1 to the formulation of the abc-conjecture. In this setting Stewart and Tijdeman [263] proved that the conjecture would be false without the ε. In other words, it is not true that

$$\max\{|a|, |b|, |c|\} \leq Cr\,(abc)\,.$$

However, we note that the statement

$$\max\{|a|, |b|, |c|\} \leq r\,(abc)^2$$

has in fact been conjectured by several authors.

To prove or disprove the abc-conjecture would be an important contribution to number theory. For instance, some results that would follow from the abc-conjecture are in [201], pp. 185–188, [57], [286] (or see [79], [149], [152], [287]).

Although the abc-conjecture seems completely out of reach, there are some results towards the truth of this conjecture. In 1986, C. L. Stewart and R. Tijdeman [263] proved

$$\max\{|a|, |b|, |c|\} < \exp\left\{Cr(abc)^{15}\right\},$$

where C is an absolute constant. In 1991, C. L. Stewart and Kunrui Yu [264] obtained

$$\max\{|a|, |b|, |c|\} < \exp\left\{C(\varepsilon)r(abc)^{2/3+\varepsilon}\right\}.$$

In 1996, C. L. Stewart and Kunrui Yu [265] further proved

$$\max\{|a|, |b|, |c|\} < \exp\left\{C(\varepsilon)r(abc)^{1/3+\varepsilon}\right\}.$$

The abc-conjecture is unsatisfactory because it does not make precise the constant $C(\varepsilon)$. A. Baker [5] proposed the following more explicit statement:

Conjecture 5.4. *There exists an absolute constant $\mathcal{K}$ having the following property. For any nonzero relatively prime integers $a,\ b,\ c$ such that $a + b = c$, the inequality*

$$\max\{|a|, |b|, |c|\} \leq \frac{\mathcal{K}}{\varepsilon^{d(1+\varepsilon)}} r(abc)^{1+\varepsilon} \tag{5.6}$$

holds for every ε with $0 < \varepsilon \leq 1$, where d denotes the number of distinct prime factors of abc.

Conjecture 5.5 (Erdös and Woods). *There exists an absolute constant $k > 2$ such that for every positive integers x and y, the conditions*

$$r(x + i) = r(y + i),\ \ i = 0, 1, 2, \ldots, k - 1$$

imply $x = y$.

This conjecture cannot hold with $k = 2$ since

$$75 = 3 \times 5^2, \quad 1215 = 3^5 \times 5; \quad 76 = 2^2 \times 19, \quad 1216 = 2^6 \times 19.$$

However, it is believed that $k = 3$ is an admissible value. Langevin ([153], [154]) proved that the abc-conjecture implies the Erdös–Woods conjecture with $k = 3$ except perhaps a finite number of counter examples. Applying the abc-conjecture with $a = x(x+2)$, $b = 1$, and $c = (x+1)^2$ leads to

$$(x+1)^2 \leq C(\varepsilon) r(x(x+1)(x+2))^{1+\varepsilon}. \tag{5.7}$$

We suppose that $x > y$ and show that in this case there are only finitely many x for which the statement of the Erdös–Woods conjecture with $k = 3$ holds, i.e.,

$$r(x+i) = r(y+i), \ \ i = 0, 1, 2.$$

As an immediate consequence of the latter condition one finds

$$x - y = (x+i) - (y+i) \equiv 0 \bmod r(x+i), \ \ i = 0, 1, 2.$$

Since the greatest common divisor of any two of the three numbers $r(x)$, $r(x+1)$, $r(x+2)$ is one or two, it follows that $r(x(x+1)(x+2))$ divides $2(x-y)$. This yields in (5.7)

$$x^2 \leq C(\varepsilon) r(x(x+1)(x+2))^{1+\varepsilon} \leq C(\varepsilon)(2x)^{1+\varepsilon},$$

and so

$$x \leq \left(2^{1+\varepsilon} C(\varepsilon)\right)^{\frac{1}{1-\varepsilon}}.$$

Thus x is bounded by some constant.

5.3 Equivalent abc-conjecture

Next we show that the abc-conjecture is equivalent to the following:

Conjecture 5.6. *Let A, B be fixed nonzero integers. Take positive integers m, n with*

$$\alpha = 1 - \frac{1}{m} - \frac{1}{n} > 0. \tag{5.8}$$

Let $x, y, z \in \mathbb{Z}$ be variables such that x, y are relatively prime and

$$Ax + By = z \neq 0.$$

Assume that for a prime p (resp. q), $p \mid x$ (resp. $q \mid y$) implies $p^m \mid x$ (resp. $q^n \mid y$). Then for any $\varepsilon > 0$ there exists a number $C = C(\varepsilon, m, n, A, B)$ such that

$$\max\{|x|^\alpha, |y|^\alpha, |z|^\alpha\} \leq C r(z)^{1+\varepsilon}. \tag{5.9}$$

Remark. We introduce a notation related to Conjecture 5.6. A positive integer A is *powerful* if for every prime p dividing A, p^2 also divides A. Every powerful number can be written as a^2b^3, where a and b are positive integers. The Erdös–Mollin–Walsh conjecture asserts that there do not exist three consecutive powerful integers. The abc-conjecture implies the weaker assertion that the set of triples of consecutive powerful integers is finite.

Here we first show that Conjecture 5.3 implies Conjecture 5.6. To simplify notation in dealing with the possible presence of constants C, if a, b are positive functions, we write

$$a \ll b$$

to mean that there exists a constant $C > 0$ such that $a \leq Cb$. Thus $a \ll b$ means $a = O(b)$ in the big oh notation. By the abc-conjecture, we get

$$\max\{|x|, |y|, |z|\} \ll \left\{|x|^{\frac{1}{m}}|y|^{\frac{1}{n}}r(z)\right\}^{1+\varepsilon}.$$

If, say, $|Ax| \leq |By|$ then $|x| \ll |y|$. We substitute this estimate for x to get an inequality entirely in terms of y, namely

$$|y| \ll \left\{|y|^{\frac{1}{m}+\frac{1}{n}}r(z)\right\}^{1+\varepsilon}.$$

We first bring all powers of y to the left-hand side, and take care of the extra ε, so we obtain

$$|y|^{\alpha} \ll r(z)^{1+\varepsilon},$$

and then also

$$|x|^{\alpha} \ll r(z)^{1+\varepsilon}$$

because the situation is symmetric in x and y. Again by the abc-conjecture, we have

$$|z| \ll \left\{|x|^{\frac{1}{m}}|y|^{\frac{1}{n}}r(z)\right\}^{1+\varepsilon}.$$

By using the estimate for $|xy|$ coming from the product of the inequalities above we find

$$|z|^{\alpha} \ll r(z)^{1+\varepsilon}.$$

Conversely, Conjecture 5.3 can be derived from Conjecture 5.6. To do this, we see that Conjecture 5.6 contains obviously the following *generalized Szpiro conjecture* (cf. [149], [287]):

Conjecture 5.7. *Take integers x and y with $D = 4x^3 - 27y^2 \neq 0$ such that the common factor of x, y is bounded by M. Then for any $\varepsilon > 0$, there exists a constant $C = C(\varepsilon, M)$ satisfying*

$$\max\{|x|^3, y^2, |D|\} \leq Cr(D)^{6+\varepsilon}. \tag{5.10}$$

This is trivial if x, y are relatively prime. Suppose that x, y have some common factor, say d, bounded by M. Write

$$x = ud, \quad y = vd$$

with u, v relatively prime. Then

$$D = 4d^3u^3 - 27d^2v^2.$$

Now we can apply the inequality (5.9) with $A = 4d^3, m = 3$; $B = -27d^2, n = 2$, and we find the same inequality (5.10), with the constant depending also on M.

Further, it is well known that the generalized Szpiro conjecture implies the abc-conjecture (cf. [150], [287]). Here we introduce the proof roughly. Let $a + b = c$, and consider the Frey elliptic curve ([67], [68]),

$$y^2 = x(x - a)(x + b).$$

The discriminant of the right-hand side is the product of the differences of the roots squared, and so

$$D = (abc)^2.$$

We make a translation

$$\xi = x + \frac{b - a}{3}$$

to get rid of the x^2-term, so that the equation can be rewritten

$$y^2 = \xi^3 - \gamma_2\xi - \gamma_3,$$

where

$$\gamma_2 = \frac{1}{3}(a^2 + ab + b^2), \quad \gamma_3 = \frac{1}{27}(a - b)(2a + b)(a + 2b).$$

The discriminant does not change because the roots of the polynomial in ξ are translations of the roots of the polynomial in x. Then

$$D = 4\gamma_2^3 - 27\gamma_3^2.$$

One may avoid the denominator 27 by using the curve

$$y^2 = x(x - 3a)(x + 3b),$$

so that γ_2, γ_3 then come out to be integers, and one can apply the generalized Szpiro conjecture to the discriminant

$$D = 3^6(abc)^2 = 4\gamma_2^3 - 27\gamma_3^2,$$

and obtain

$$\max\left\{\sqrt[3]{|abc|}, \sqrt{|\gamma_2|}, \sqrt[3]{|\gamma_3|}\right\} \ll r(abc)^{1+\varepsilon}.$$

A simple algebraic manipulation shows that the estimates on γ_2, γ_3 imply the desired estimates on $|a|, |b|$.

The following conjecture by Hall, Szpiro, and Lang–Waldschmidt (cf. [287], [149]) becomes a special case of Conjecture 5.6:

Conjecture 5.8. *Let A, B be fixed nonzero integers and take positive integers m and n satisfying* (5.8). *Let $x, y, z \in \mathbb{Z}$ be variables such that x, y are relatively prime and*

$$Ax^m + By^n = z \neq 0.$$

Then for any $\varepsilon > 0$ there exists a number $C = C(\varepsilon, m, n, A, B)$ such that

$$\max\{|x|^{m\alpha}, |y|^{n\alpha}, |z|^{\alpha}\} \leq Cr(z)^{1+\varepsilon}. \tag{5.11}$$

In particular, take non-zero integers x, y with $z = x^3 - y^2 \neq 0$. If x, y are relatively prime, then Conjecture 5.8 implies that there exists a constant $C = C(\varepsilon)$ such that

$$\max\left\{|x|^{\frac{1}{2}}, |y|^{\frac{1}{3}}\right\} \leq C(\varepsilon)r(x^3 - y^2)^{1+\varepsilon}, \tag{5.12}$$

which further yields

$$|x|^{\frac{1}{2}} \ll \left|x^3 - y^2\right|^{1+\varepsilon}. \tag{5.13}$$

This is just the content of *Hall's conjecture*:

Conjecture 5.9 ([88]). *There exists a constant $C = C(\varepsilon)$ such that*

$$|x^3 - y^2| > C(\varepsilon)|x|^{\frac{1}{2}-\varepsilon} \tag{5.14}$$

holds for integers x, y with $x^3 \neq y^2$.

The inequality (5.14) is equivalent to the form (5.13). Danilov [37] has proved that $1/2$ is the best possible exponent, who proved that $0 < |x^3 - y^2| < 0.97|x|^{1/2}$ has infinitely many solutions in integers x, y. Actually, the original conjecture made by M. Hall Jr. [88] states the following: There exists a constant C such that

$$|x^3 - y^2| > C|x|^{\frac{1}{2}} \tag{5.15}$$

holds for integers x, y with $x^3 \neq y^2$. The final setting of the proofs in the simple abc context which we gave above had to await Mason and the abc-conjecture a decade later.

Another special case of Conjecture 5.8 is the following *Hall–Lang–Waldschmidt's conjecture* (cf. [287]):

Conjecture 5.10. *For all integers m, n, x, y with $x^m \neq y^n$,*

$$\max\{|x|^{m\alpha}, |y|^{n\alpha}\} < C(\varepsilon)\left|x^m - y^n\right|^{1+\varepsilon}, \tag{5.16}$$

where $C(\varepsilon)$ is a constant depending on ε.

5.4 Generalized abc-conjecture

For a non-zero polynomial f in $\mathbb{C}$, we can write

$$f(z) = a(z - z_1)^{n_1} \cdots (z - z_p)^{n_p},$$

where $a \in \mathbb{C}_*$; $z_1, \ldots, z_p$ are the distinct roots of f, and

$$\deg(f) = n_1 + \cdots + n_p.$$

Related to a positive integer k, we define

$$\deg^{(k)}(f) = \sum_{j=1}^{p} \min\{n_j, k\}.$$

Theorem 5.11 (cf. [111]). *Let $f_0, f_1, \ldots, f_n$ $(n \geq 2)$ be polynomials in $\mathbb{C}$ satisfying*

$$f_0 = f_1 + \cdots + f_n. \tag{5.17}$$

Assume that no proper subsum of (5.17) is equal to 0, the f_j are not all constant, and that $f_0, f_1, \ldots, f_n$ have no non-constant common divisors. Then for any positive integer k, there exist two constants $\mathfrak{x}_n(k)$ and $\mathfrak{y}_n(k)$ satisfying

$$0 < \mathfrak{x}_n(k) \leq \max\left\{1, \frac{n-1}{k}\right\},$$

$$0 < \mathfrak{y}_n(k) \leq \max\left\{1, \frac{n(n-1)}{2k}\right\},$$

such that the following inequalities hold:

$$\max_{0\leq j\leq n}\{\deg(f_j)\} \leq \mathfrak{x}_n(k) \sum_{j=0}^{n} \deg^{(k)}(f_j) - \frac{n(n-1)}{2}, \tag{5.18}$$

$$\max_{0\leq j\leq n}\{\deg(f_j)\} \leq \mathfrak{y}_n(k) \deg^{(k)}(f_0 \cdots f_n) - \frac{n(n-1)}{2}. \tag{5.19}$$

In this section, we will make the following general assumptions for integers:

(N1) Let $a_0, a_1, \ldots, a_n$ $(n \geq 2)$ be non-zero integers satisfying

$$a_0 = a_1 + a_2 + \cdots + a_n. \tag{5.20}$$

Assume that no proper subsum of (5.20) is equal to 0.

(N2) Let $a_0, a_1, \ldots, a_n$ be non-zero integers satisfying $\gcd(a_0, \ldots, a_n) = 1$, where the symbol $\gcd(a_0, \ldots, a_n)$ denotes the *greatest common divisor* of $a_0, \ldots, a_n$.

For a non-zero integer a, write

$$a = \pm p_1^{i_1} \cdots p_s^{i_s} \tag{5.21}$$

for distinct primes $p_1, \ldots, p_s$ and $(i_1, \ldots, i_s) \in (\mathbb{Z}^+)^s$, and define

$$r_k(a) = \prod_{\nu=1}^{s} p_\nu^{\min\{i_\nu, k\}}. \tag{5.22}$$

Based on the classical analogy between polynomials and integers, we think that the number $\deg^{(k)}(f)$ of a polynomial f corresponds to $\log r_k(a)$ of an integer a. Based on Theorem 5.11, we propose the following *n-term abc-conjecture* for integers (see Hu and Yang [110]).

Conjecture 5.12. *If* (N1) *and* (N2) *are true, then for* $\varepsilon > 0,\ k \in \mathbb{Z}^+$, *there exists a number* $C = C(n, k, \varepsilon)$ *satisfying*

$$\max_{0\le j\le n}\{|a_j|\} \le C\left(\prod_{i=0}^{n} r_k(a_i)\right)^{\mathfrak{r}_n(k)+\varepsilon}, \tag{5.23}$$

$$\max_{0\le j\le n}\{|a_j|\} \le C r_k(a_0 a_1 \cdots a_n)^{\mathfrak{y}_n(k)+\varepsilon}. \tag{5.24}$$

In [103], [107] (or see [108]), we proposed the conjecture for the case

$$\mathfrak{r}_n(n-1) = 1, \quad \mathfrak{y}_n\left(\frac{n(n-1)}{2}\right) = 1. \tag{5.25}$$

If $n = 2$, Conjecture 5.12 corresponds to the well-known abc-conjecture.

We discuss the example studied by J. Browkin and J. Brzeziński [20]. If we choose $a = 2^i$, where $i > n-2$, and $b = -1$, then we have

$$a_1 + \cdots + a_n = a_0,$$

where

$$a_{j+1} = s_j(2^i - 1)^{2j+1} 2^{i(n-2-j)}\ \ (0 \le j \le n-2), \quad a_n = 1, \quad a_0 = 2^{i(2n-3)}.$$

Obviously, it has no proper subsum equal to zero. Since $a_n = 1$, hence the greatest common divisor of all a_j is 1. Therefore the conditions in Conjecture 5.12 are satisfied. Now we have

$$M_n = \max_{0\le j\le n}\{|a_j|\} = a_0 = 2^{i(2n-3)}.$$

A positive integer $\chi_n \geq 2n-3$ exists such that

$$L_n := \prod_{i=0}^{n} r_{n-1}(a_i) = 2^{n-2} \prod_{j=0}^{n-2} r_{n-1}\left(s_j (2^i-1)^{2j+1} 2^{i(n-2-j)}\right)$$
$$\geq 2^{(n-2)(n-2)} \prod_{j=0}^{n-2} r_{n-1}\left((2^i-1)^{2j+1}\right) = 2^{(n-2)(n-2)} (2^i-1)^{\chi_n}.$$

Since there are infinitely many $i > n-2$ such that the numbers 2^i-1 are relatively prime (e.g., all prime $i > n-2$), there exists a positive constant $C(n)$ which is independent of i such that

$$\frac{2^{i(2n-3)}}{2^{(n-2)(n-2)}(2^i-1)^{\chi_n}} \leq C(n),$$

that is, $M_n \leq C(n) L_n$. We can also show that for some constant $C(n)$,

$$M_n \leq C(n) r_{\frac{n(n-1)}{2}}(a_0 a_1 \cdots a_n)$$

Thus for the case (5.25), Conjecture 5.12 holds for such a_j.

Next we exhibit a few of conjectures related to Conjecture 5.12. If a_j $(j = 0, \ldots, n)$ are nonzero integers such that $a_i,\ a_j$ are coprime for $i \neq j$, then

$$\prod_{i=0}^{n} r_k(a_i) = r_k(a_0 a_1 \cdots a_n) \leq r(a_0 a_1 \cdots a_n)^k.$$

Hence Conjecture 5.12 implies immediately the following conjecture due to W. M. Schmidt [232]:

Conjecture 5.13. *If* (N1) *holds such that a_i and a_j are coprime for $i \neq j$, then for $\varepsilon > 0$, there exists a number $C = C(n, \varepsilon)$ such that*

$$\max_{0 \leq j \leq n} \{|a_j|\} \leq C r(a_0 a_1 \cdots a_n)^{n-1+\varepsilon}. \tag{5.26}$$

It was indicated by Vojta in [293] that Conjecture 8.24 could derive the following conjecture:

Conjecture 5.14. *If* (N2) *and* (5.20) *with $n \geq 2$ hold, then for $\varepsilon > 0$, there exists a number $C = C(n, \varepsilon)$ such that*

$$\max_{0 \leq j \leq n} \{|a_j|\} \leq C r(a_0 a_1 \cdots a_n)^{1+\epsilon} \tag{5.27}$$

hold for all $a_0, \ldots, a_n$ as above outside a proper Zariski-closed subset of the hyperplane $x_1 + \cdots + x_n = x_0$ in $\mathbb{P}^n$.

J. Browkin and J. Brzeziński [20] conjectured as follows:

Conjecture 5.15. *If* (N1) *and* (N2) *are true, then for* $\varepsilon > 0$*, there exists a number* $C = C(n, \varepsilon)$ *such that*

$$\max_{0\le j\le n}\{|a_j|\} \le C r \left(a_0 a_1 \cdots a_n\right)^{2n-3+\varepsilon}. \tag{5.28}$$

J. Browkin and J. Brzeziński use the above example to show that the number $2n-3$ is a sharp lower bound. Thus the number $\mathfrak{y}_n(1)$ should satisfy

$$2n-3 \le \mathfrak{y}_n(1) \le \frac{n(n-1)}{2}. \tag{5.29}$$

Generally, we suggested the following problem (cf. [111]):

Conjecture 5.16. *Assume that* (N2) *holds and further assume that there exist integers* M *and* N *with* $M < N$ *such that*

$$B_0 a_0 + \cdots + B_n a_n \neq 0, \quad (B_0, \ldots, B_n) \in \mathbb{Z}[M, N]^{n+1} - \{0\}.$$

Take an integer q *with* $q > n \ge 1$ *and let a family* $\{[A_{j0}, \ldots, A_{jn}] \mid j = 0, \ldots, q\}$ *of* $\mathbb{P}(\mathbb{C}^{n+1})$ *be in general position with* $A_{ji} \in \mathbb{Z}[M, N]$*. Then for* $\varepsilon > 0,\ k \in \mathbb{Z}^+$*, there exists a number* $C = C(n, k, q, M, N, \varepsilon)$ *satisfying*

$$\max_{0\le j\le n}\{|a_j|^{q-n}\} \le C\left(\prod_{j=0}^{q} r_k\left(A_{j0}a_0 + \cdots + A_{jn}a_n\right)\right)^{\mathfrak{x}_n(k)+\varepsilon}, \tag{5.30}$$

$$\max_{0\le j\le n}\{|a_j|^{q-n}\} \le C r_k\left(\prod_{j=0}^{q} \left(A_{j0}a_0 + \cdots + A_{jn}a_n\right)\right)^{\mathfrak{y}_n(k)+\varepsilon}. \tag{5.31}$$

Conjecture 5.12 corresponds to a special case of Conjecture 5.16 by taking $M = 0,\ N = 1$ and $q = n+1$.

5.5 Generalized Hall's conjecture

We make the following assumptions:

(P1) Let $f_0, f_1, \ldots, f_n$ $(n \ge 2)$ be non-zero polynomials in $\mathbb{C}$ satisfying

$$f_0 = f_1 + f_2 + \cdots + f_n. \tag{5.32}$$

Assume that no proper subsum of (5.32) is equal to 0, and that the f_j are not all constant.

(P2) Let $f_1, f_2, \ldots, f_n$ $(n \geq 2)$ be polynomials in $\mathbb{C}$ such that they have no common zeroes, and that the f_j are not all constant.

(P3) Let $f_1, f_2, \ldots, f_n$ $(n \geq 2)$ be polynomials in $\mathbb{C}$. Assume that there exist positive integers d_j such that the multiplicity of each root of f_j is not less than d_j for $j = 1, \ldots, n$.

Theorem 5.11 implies directly the following fact:

Theorem 5.17. *Let $f_0, f_1, \ldots, f_n$ be polynomials in $\mathbb{C}$ satisfying the conditions* (P1)*,* (P2) *and* (P3)*. Then for any positive integer k, we have the following inequality*

$$\left\{1 - \sum_{j=1}^{n} \frac{k\mathfrak{x}_n(k)}{d_j}\right\} \max_{0\leq j\leq n} \deg(f_j) \leq \mathfrak{x}_n(k) \deg^{(k)}(f_0) - \frac{n(n-1)}{2}. \tag{5.33}$$

Proof. Note that for $j = 1, \ldots, n$,

$$\deg^{(k)}(f_j) \leq k \deg^{(1)}(f_j) \leq \frac{k}{d_j} \deg(f_j) \leq \frac{k}{d_j} \max_{0\leq j\leq n} \deg(f_j).$$

Hence Theorem 5.17 follows from Theorem 5.11. □

As a consequence, we obtain the following fact (see [109]):

Theorem 5.18. *Let $f_0, f_1, \ldots, f_n$ be polynomials in $\mathbb{C}$ satisfying* (P1) *and* (P2)*. Assume that there exist positive integers d_j and polynomials P_j in $\mathbb{C}$ such that*

$$f_j = P_j^{d_j}, \ \ j = 1, \ldots, n.$$

Then for any positive integer k, we have the following inequality

$$\left\{1 - \sum_{j=1}^{n} \frac{k\mathfrak{x}_n(k)}{d_j}\right\} \max_{0\leq j\leq n} d_j \deg(P_j) \leq \mathfrak{x}_n(k) \deg^{(k)}(f_0) - \frac{n(n-1)}{2}. \tag{5.34}$$

Since $\mathfrak{x}_n(k) = 1$ for the case $k = n-1$, the inequality (5.34) implies

$$\left\{1 - \sum_{j=1}^{n} \frac{n-1}{d_j}\right\} \max_{0\leq j\leq n} d_j \deg(P_j) \leq (n-1) \left\{\deg^{(1)}\left(\sum_{j=1}^{n} P_j^{d_j}\right) - \frac{n}{2}\right\}. \tag{5.35}$$

In particular, if f and g are non-zero polynomials in $\mathbb{C}$ with $f^2 - g^3 \neq 0$, and are not all constant, then (5.35) yields

$$\frac{1}{6} \max\{2\deg(f), 3\deg(g)\} \leq \deg^{(1)}\left(f^2 - g^3\right) - 1 \tag{5.36}$$

when f and g have no common zeros, which means the inequality in the following *Davenport's theorem* (or see [11], [268]):

Theorem 5.19 ([40]). *If f and g are non-constant polynomials in $\mathbb{C}$ with $f^2 - g^3 \neq 0$, then*

$$\frac{1}{2}\deg(g) \leq \deg\left(f^2 - g^3\right) - 1. \tag{5.37}$$

The analogue of Theorem 5.19 in number theory is just Hall's conjecture. The inequality (5.36) is an analogue of (5.12). For the case

$$n = 2, \quad d_1 = k, \quad d_2 = n, \tag{5.38}$$

and

$$f_1 = f, \quad f_2 = \lambda g, \tag{5.39}$$

where λ is a constant such that $\lambda^n = -1$, the inequality (5.35) yields

$$\left\{1 - \frac{1}{k} - \frac{1}{n}\right\} \max\{k\deg(f), n\deg(g)\} \leq \deg^{(1)}\left(f^k - g^n\right) - 1 \tag{5.40}$$

when f and g have no common zeros, which implies

$$\left\{1 - \frac{1}{k} - \frac{1}{n}\right\} \max\left\{k\deg(f), n\deg(g)\right\} \leq \deg\left(f^k - g^n\right) - 1. \tag{5.41}$$

This inequality is just an analogue of the Hall–Lang–Waldschmidt's conjecture (5.16) for polynomials.

For integers, the conditions (P1), (P2) and (P3) are respectively replaced by:

(N1) Let $A_1, \ldots, A_n$ $(n \geq 2)$ be fixed nonzero integers and let x_j $(j = 0, 1, \ldots, n)$ be nonzero integers satisfying

$$A_1 x_1 + \cdots + A_n x_n = x_0. \tag{5.42}$$

Assume that no proper subsum of (5.42) is equal to 0.

(N2) Let $x_1, x_2, \ldots, x_n$ $(n \geq 2)$ be integers satisfying $\gcd(x_1, \ldots, x_n) = 1$.

(N3) Suppose that there are positive integers d_j such that for each $j = 1, \ldots, n$, $p \mid x_j$ for some prime p implies $p^{d_j} \mid x_j$.

We conjectured that the analogue of Theorem 5.17 in number theory would be the following problem:

Conjecture 5.20. *If* (N1), (N2) *and* (N3) *hold such that for some $k \in \mathbb{Z}^+$*

$$\alpha = 1 - \sum_{j=1}^{n} \frac{k\mathfrak{r}_n(k)}{d_j} > 0, \tag{5.43}$$

then for $\varepsilon > 0$, there exists a number $C = C(n, k, \varepsilon, A_1, \ldots, A_n)$ such that

$$\max_{0 \leq j \leq n}\{|x_j|^\alpha\} \leq C r_k(x_0)^{\mathfrak{r}_n(k)+\varepsilon}. \tag{5.44}$$

Conjecture 5.20 is a generalization of Conjecture 5.6. Note that when x_0 is fixed, the equation (5.42) has integer solutions $x_1, \dots, x_n$ if and only if the fixed nonzero integers $A_1, \dots, A_n$ satisfy

$$\gcd(A_1, \dots, A_n) \mid x_0.$$

According to the discussion in Section 5.2, it is easy to show that Conjecture 5.20 follows from Conjecture 5.12.

Conjecture 5.21. *Assume that* (N1) *and* (N2) *hold and suppose that there are positive integers d_j and integers a_j such that*

$$x_j = a_j^{d_j}, \ \ j = 1, \dots, n.$$

If (5.43) *holds, then for $\varepsilon > 0$, there is a number $C = C(n, k, \varepsilon, A_1, \dots, A_n)$ such that*

$$\max_{0 \le j \le n} \{|a_j|^{\alpha d_j}\} \le C r_k(x_0)^{\mathfrak{r}_n(k)+\varepsilon}, \tag{5.45}$$

where $a_0 = x_0, \ d_0 = 1$.

Conjecture 5.21 is a generalization of Conjecture 5.8, and follows easily from Conjecture 5.20. Some special cases of Conjecture 5.21 were suggested in [109] and [108].

5.6 The abc-conjecture for number fields

5.6.1 Generalizations of the abc-conjecture

Let κ be a number field and take a positive integer n. Let X be the hyperplane of $\mathbb{P}^{n+1}$ defined by

$$\xi_0 + \xi_1 + \cdots + \xi_{n+1} = 0.$$

To simplify statements, an element $[a_0, a_1, \dots, a_{n+1}] \in \mathbb{P}^{n+1}$ will be called an *abc-point* if $a_0 a_1 \cdots a_{n+1} \neq 0$, and if

$$a_0 + a_1 + \cdots + a_{n+1} = 0 \tag{5.46}$$

such that no proper subsum of (5.46) is equal to 0.

The complementary set of abc-points in X is called *abc-exceptional set*, denoted by E^n_{abc}, which is just the subset of X defined by

$$\sum_{i \in I} \xi_i = 0,$$

where I is a subset of $\{0, 1, \dots, n+1\}$ with at least one, but not more than $n+1$, elements. Thus E^n_{abc} is an algebraic subset of X. For example,

$$E^1_{abc} = \{[0, 1, -1], [1, 0, -1], [1, -1, 0]\}.$$

Take a point

$$x = [a_0, a_1, \ldots, a_{n+1}] \in \mathbb{P}^{n+1}(\kappa).$$

By Proposition 1.60, we may assume that each a_i is integral over $\mathbb{Z}$. Further, we may suppose that the elements $a_0, a_1, \ldots, a_{n+1}$ are relatively prime. Such $(a_0, \ldots, a_{n+1}) \in \mathcal{O}_\kappa^{n+2}$ is called a *reduced representation* of x, which is unique up to integral units. In fact, if $(b_0, \ldots, b_{n+1}) \in \mathcal{O}_\kappa^{n+2}$ is another reduced representation of x, then there exists $\lambda \in \kappa_*$ such that

$$(b_0, \ldots, b_{n+1}) = \lambda(a_0, \ldots, a_{n+1}).$$

Since $a_0, a_1, \ldots, a_{n+1}$ are relatively prime, there are algebraic integers $\lambda_0, \ldots, \lambda_{n+1}$ satisfying

$$\lambda_0 a_0 + \cdots + \lambda_{n+1} a_{n+1} = 1,$$

and hence

$$\lambda_0 b_0 + \cdots + \lambda_{n+1} b_{n+1} = \lambda,$$

which shows that λ is an algebraic integer. Symmetrically, we may prove that λ^{-1} also is an algebraic integer. Thus λ is a unit.

Let $x \in \mathbb{P}^{n+1}(\kappa)$ be an abc-point with a reduced representation $(a_0, \ldots, a_{n+1}) \in \mathcal{O}_\kappa^{n+2}$ and fix an positive integer m. Let $\mathcal{X}$ be a model X over $\operatorname{Spec} \mathcal{O}_\kappa$. Denote by H_i the hyperplane of $\mathbb{P}^{n+1}$

$$H_i = \{\xi_i = 0\}, \ \ 0 \leq i \leq n+1.$$

Let $E_i = H_i|_X$ and let $\bar{E}_i$ be the Zariski closure of E_i in $\mathcal{X}$. Then $x \in X(\kappa)$ gives a section $\bar{x} : \operatorname{Spec} \mathcal{O}_\kappa \longrightarrow \mathcal{X}$ with an extension $\tilde{x} : \mathbb{M}_\kappa \longrightarrow \mathcal{X}$. By using the canonical bijection (4.44), we have

$$\tilde{x}^* \bar{E}_i = \sum_{v \in M_\kappa^0} \operatorname{ord}_v(a_i) \mathfrak{p}_v + \sum_{v \in M_\kappa^\infty} \log \frac{1}{\|a_i\|_v} \mathfrak{p}_v.$$

Thus the *truncated valence function*

$$N_m(x, E_i) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in M_\kappa^0} \min\{m, \operatorname{ord}_v(a_i)\} \log \mathcal{N}(\mathfrak{p}_v) \tag{5.47}$$

of x to multiplicity m is well defined.

Let H be the divisor

$$H = H_0 + H_1 + \cdots + H_{n+1}$$

on $\mathbb{P}^{n+1}$. Let $E = H|_X$ and let $\bar{E}$ be the Zariski closure of E in $\mathcal{X}$. Then we have

$$\tilde{x}^* \bar{E} = \sum_{v \in M_\kappa^0} \operatorname{ord}_v(a_0 \cdots a_{n+1}) \mathfrak{p}_v + \sum_{v \in M_\kappa^\infty} \log \frac{1}{\|a_0 \cdots a_{n+1}\|_v} \mathfrak{p}_v.$$

Hence the *truncated valence function*

$$N_m(x,E) = \frac{1}{[\kappa:\mathbb{Q}]} \sum_{v\in M_\kappa^0} \min\{m, \mathrm{ord}_v(a_0\cdots a_{n+1})\} \log \mathcal{N}(\mathfrak{p}_v) \tag{5.48}$$

of x to multiplicity m is obtained.

Now we can formulate the $(n+1)$-term abc-conjecture for integers into the *uniform* $(n+1)$*-term* abc*-conjecture for* κ as follows:

Conjecture 5.22. *There exists a positive increasing function* ψ *with* $\psi(h) = o(h)$ *such that*

$$h(x) \le d_{\kappa/\mathbb{Q}} + \mathfrak{x}_{n+1}(m) \sum_{i=0}^{n+1} N_m(x,E_i) + \psi(h(x)), \tag{5.49}$$

$$h(x) \le d_{\kappa/\mathbb{Q}} + \mathfrak{y}_{n+1}(m) N_m(x,E) + \psi(h(x)) \tag{5.50}$$

hold for every abc*-point* $x \in \mathbb{P}^{n+1}(\kappa)$.

Originally, we formulated the n-term abc-conjecture for $\kappa = \mathbb{Q}$ with $\varepsilon h(x) + C$ instead of $\psi(h(x))$. These formulations are equivalent, proved $C = C(\varepsilon)$ is explicitly known as a function of ε. Indeed, in that case we determine for every value of h,

$$\psi(h) = \min_{\varepsilon>0}\{\varepsilon h + C(\varepsilon)\}.$$

On the other hand, if $\psi(h) = o(h)$ is known, then for $\varepsilon > 0$ we determine

$$C(\varepsilon) = \max_{h>0}\{\psi(h) - \varepsilon h\}.$$

In particular, Conjecture 5.22 contains the following *uniform* abc*-conjecture for* κ (cf. [17], [78], [284], [285], [286], [287]):

Conjecture 5.23. *There exists a positive increasing function* ψ *with* $\psi(h) = o(h)$ *such that*

$$h(x) \le d_{\kappa/\mathbb{Q}} + \overline{N}(x,E) + \psi(h(x)) \tag{5.51}$$

holds for every abc*-point* $x \in \mathbb{P}^2(\kappa)$.

The function ψ may depend on the number field, however, conjectured that ψ does not depend on κ (cf. van Frankenhuysen [286]). Computationally, formulation (5.51) is not the most useful, but one can easily derive a more useful inequality:

$$h(x) \le \overline{N}(x,E) + \psi(h(x)). \tag{5.52}$$

Note that $\psi(h) = o(h)$ implies $h \le 2\overline{N}$ for $h \gg 0$, and this in turn implies

$$h(x) \le \overline{N}(x,E) + \psi(2\overline{N}(x,E)). \tag{5.53}$$

This formulation, which is equivalent to Conjecture 5.23, is most useful in applications.

The truncated valence function depends on the number field. For a field extension K of κ, if $w \in M_K$ is one of the valuations extending the valuation v on κ one has

$$\log \#\mathbb{F}_w(K) = [\mathbb{F}_w(K) : \mathbb{F}_v(\kappa)] \log \#\mathbb{F}_v(\kappa).$$

Thus, the contribution $\sum_{w|v} \log \#\mathbb{F}_w(K)$ of the valuations above v to $\overline{N}(x, D)$ satisfies

$$\log \#\mathbb{F}_v(\kappa) \leq \sum_{w|v} \log \#\mathbb{F}_w(K) \leq [K : \kappa] \log \#\mathbb{F}_v(\kappa), \tag{5.54}$$

with equality on the right if v is unramified in K. In general, we have the bounds

$$\overline{N}(x, E)_{x\in K} \leq \overline{N}(x, E)_{x\in\kappa} \leq d_{K/\kappa} + \overline{N}(x, E)_{x\in K}. \tag{5.55}$$

5.6.2 Further formulations of the abc-conjecture

Take two integers M and N with $0 \leq M < N$. An element $[a_0, \ldots, a_n] \in \mathbb{P}^n$ $(n \geq 1)$ will be called *linearly independent* over $\mathbb{Z}[M, N]$ if $a_0 \cdots a_n \neq 0$, and if

$$B_0a_0 + \cdots + B_na_n \neq 0, \quad (B_0, \ldots, B_n) \in \mathbb{Z}[M, N]^{n+1} - \{0\}.$$

Let $E^n[M, N]$ denote the points $[a_0, \ldots, a_n] \in \mathbb{P}^n$ satisfying

$$B_0a_0 + \cdots + B_na_n = 0, \quad (B_0, \ldots, B_n) \in \mathbb{Z}[M, N]^{n+1} - \{0\}.$$

Take an integer q with $q > n$ and take a family

$$\tilde{\mathscr{A}} = \big\{(A_{j0}, \ldots, A_{jn}) \in \mathbb{Z}[M, N]^{n+1} \mid 0 \leq j \leq q\big\}$$

such that

$$\mathscr{A} = \{[A_{j0}, \ldots, A_{jn}] \in \mathbb{P}^n(\mathbb{Z}) \mid 0 \leq j \leq q\}$$

is in general position. Let D_j be the divisor defined by the equation

$$A_{j0}\xi_0 + \cdots + A_{jn}\xi_n = 0$$

on $\mathbb{P}^n$. Then Conjecture 5.16 can be formulated into the following form over the number field κ:

Conjecture 5.24. *Assume that $x \in \mathbb{P}^n(\kappa)$ is linearly independent over $\mathbb{Z}[M, N]$. There exists a positive increasing function ψ with $\psi(h) = o(h)$ satisfying*

$$(q - n)h(x) \leq d_{\kappa/\mathbb{Q}} + \mathfrak{x}_{n+1}(m) \sum_{j=0}^{q} N_m(x, D_j) + \psi(h(x)), \tag{5.56}$$

$$(q - n)h(x) \leq d_{\kappa/\mathbb{Q}} + \mathfrak{y}_{n+1}(m) N_m\bigg(x, \sum_{j=0}^{q} D_j\bigg) + \psi(h(x)). \tag{5.57}$$

The general abc-conjecture due to P. Vojta [293] can be formulated into the following form:

Conjecture 5.25. *There exists a proper Zariski-closed subset Z of $\mathbb{P}^n(\kappa)$ such that*

$$(q-n)h(x) \leq d_{\kappa/\mathbb{Q}} + \overline{N}\left(x, \sum_{j=0}^{q} D_j\right) + \varepsilon h(x) + O(1) \tag{5.58}$$

holds for $x \in \mathbb{P}^n(\kappa) - Z$.

It seems to us that in general, the exceptional set Z in Conjecture 5.25 is larger than the exceptional set $E^n[M,N]$ in Conjecture 5.24.

Take $M=0$, $N=1$, $q=n+1$,

$$D_j = \{\xi_j = 0\},\ \ j = 0, \ldots, n;$$

and

$$D_{n+1} = \{\xi_0 + \cdots + \xi_n = 0\}.$$

Consider the inclusion $\iota : \mathbb{P}^n \longrightarrow \mathbb{P}^{n+1}$ defined by

$$[\xi_0, \ldots, \xi_n] \mapsto [\xi_0, \ldots, \xi_n, -\xi_0 - \cdots - \xi_n].$$

Then

$$\iota(\mathbb{P}^n) = X = \{\xi_0 + \xi_1 + \cdots + \xi_{n+1} = 0\},$$

and

$$D_j = \iota^* H_j = H_j|_X = E_j,\ \ j = 0, 1, \ldots, n+1.$$

Note that

$$h([\xi_0, \ldots, \xi_{n+1}]) = h([\xi_0, \ldots, \xi_n]) + O(1),\ \ [\xi_0, \ldots, \xi_{n+1}] \in X$$

and $\iota(E^n[0,1]) = E^n_{abc}$. The inequality (5.56) and (5.57) become

$$h(x) \leq d_{\kappa/\mathbb{Q}} + \mathfrak{x}_{n+1}(m) \sum_{j=0}^{n+1} N_m(x, E_j) + \psi(h(x)), \tag{5.59}$$

$$h(x) \leq d_{\kappa/\mathbb{Q}} + \mathfrak{y}_{n+1}(m) N_m\left(x, \sum_{j=0}^{n+1} E_j\right) + \psi(h(x)) \tag{5.60}$$

for all abc-points $x \in \mathbb{P}^{n+1}$. Hence Conjecture 5.22 is a special case of Conjecture 5.24.

For above special case, the formula (5.58) becomes

$$h(x) \leq d_{\kappa/\mathbb{Q}} + \overline{N}\,(x, E) + \psi(h(x)) \tag{5.61}$$

with $x \in X(\kappa) - \iota(Z) \subseteq \mathbb{P}^{n+1}(\kappa)$. If $\kappa = \mathbb{Q}$, this is just the logarithmic form of the general abc-conjecture due to P. Vojta [293].

When $n = 1$, the set $\iota(Z)$ is a finite set in the line X. Taking the constant in $O(1)$ sufficiently large, then (5.61) with $n = 1$ holds for all abc-points $x \in \mathbb{P}^2(\kappa)$. Thus Conjecture 5.23 follows from (5.61) with $n = 1$.

5.7 Fermat equations

Fermat's conjecture, now a theorem proved by Wiles [301], Taylor and Wiles [271], states that there cannot be non-zero integers x, y, z and an integer d, where $d \geq 3$, such that

$$x^d + y^d = z^d. \tag{5.62}$$

Related to the *Fermat's equation* (5.62) is *Catalan's equation*

$$x^k - y^l = 1. \tag{5.63}$$

In 1844, Eugène Catalan [27] conjectured that this equation had only the trivial solution

$$(x, y, k, l) = (3, 2, 2, 3).$$

About 100 years before Catalan (1814–1894) sent his letter to Crelle, Euler had proven that 8 and 9 are the only consecutive integers among squares and cubes, that is, the only solution of the Diophantine equations

$$x^2 - y^3 = \pm 1, \quad x > 0, \ y > 0.$$

To prove the *Catalan's conjecture*, it obviously suffices to consider the equation

$$x^p - y^q = 1, \quad x > 0, \ y > 0, \tag{5.64}$$

where p and q are different primes. The case $q = 2$ was solved in 1850 by V. A. Lebesgue [155]. Chao Ko [128] proved the case $p = 2$. In 1976, E. Z. Chein [29] published a new, very elegant proof.

Next we may assume that p and q are different odd primes. One of the early observations was that the number of solutions (x, y) to (5.64), for fixed exponents p and q, is at most finite. This is a consequence of a general theorem about integer points on a curve, published by C. L. Siegel in 1929. For other results about the number of solutions, see the introductory section in Tijdeman [274].

By way of multiplication of the equation, rewrite (5.64) as

$$(x - 1)\frac{x^p - 1}{x - 1} = y^q.$$

By considering the identity $x^p = ((x-1)+1)^p$ one easily finds that there are two possibilities: the greatest common divisor of the two factors on the left hand side is either 1 or p. When the greatest common divisor equals 1, we obtain the equations

$$x - 1 = a^q, \quad \frac{x^p - 1}{x - 1} = b^q, \quad y = ab,$$

where a and b are coprime and not divisible by p. In 1960, J. W. S. Cassels [26] showed that these equations yield a contradiction.

When the greatest common divisor equals p, we obtain the equations

$$x - 1 = p^{q-1}a^q, \quad \frac{x^p - 1}{x - 1} = pb^q, \quad y = pab,$$

where again a and b are coprime and p does not divide b. Preda Mihăilescu [180], [181] showed that these equations also yield a contradiction. A deep theorem about cyclotomic fields plays a crucial role in his proof. For a survey about the proof of Catalan's conjecture, see [179], or see [10] for an exposition of Mihăilescu's proof.

Generally, the following conjecture was made by Pillai [212].

Conjecture 5.26. *Given integers $A > 0$, $B > 0$, $C > 0$, the equation*

$$Ax^k - By^l = C$$

in integers $x > 1$, $y > 1$, $k > 1$, $l > 1$ and with $(k, l) \neq (2, 2)$ has only a finite number of solutions.

If k, l were fixed, this would be a special case of an algebraic Diophantine equation, the superelliptic equation. *Pillai's conjecture* can be derived from the abc-conjecture (see [232]).

It might be natural to combine Fermat's last theorem with the Catalan problem. The *Fermat–Catalan conjecture* claims that there are only finitely many powers x^k, y^l, z^n satisfying

$$x^k + y^l = z^n, \tag{5.65}$$

where x, y, z are coprime integers, and k, l, n are positive integers with

$$\frac{1}{k} + \frac{1}{l} + \frac{1}{n} < 1; \tag{5.66}$$

the restriction on the exponents excludes certain infinite families of solutions relating to curves with small genus. A more general application is as follows. Tijdeman [275] proved that for given non-zero integers A, B, C the *generalized Fermat–Catalan equation*

$$Ax^k + By^l = Cz^n \tag{5.67}$$

has only finitely many solutions in positive integers $x > 1$, $y > 1$, $z > 1$, $k,\ l,\ n$ subject to $\gcd(Ax, By, Cz) = 1$ and (5.66). On the other hand, Hindry has shown that for each triple $k,\ l,\ n$ with

$$\frac{1}{k} + \frac{1}{l} + \frac{1}{n} \geq 1,$$

there exist A, B, C such that the above equation has infinitely many solutions $x,\ y,\ z$ with $\gcd(Ax, By, Cz) = 1$. H. Darmon and A. Granville [38] (or cf. [14]) proved the following result:

Theorem 5.27. *Take positive integers k, l, n satisfying* (5.66) *and let $A, B, C \in \mathbb{Z} - \{0\}$. There are only finitely many solutions $(x, y, z) \in \mathbb{Z}^3$ of the generalized Fermat–Catalan equation* (5.67) *with* $\gcd(x, y, z) = 1$.

We make the following assumptions on integers.

(N1) Let $x_0, x_1, \ldots, x_n$ $(n \geq 2)$ be non-zero integers satisfying the equation

$$x_0 + x_1 + \cdots + x_n = 0. \tag{5.68}$$

(N2) Take positive integers n and d_j $(j = 0, 1, \ldots, n)$ with $n \geq 2$. Let $x_0, x_1, \ldots, x_n$ be non-zero integers such that for each $i \in \{0, 1, \ldots, n\}$, there is no prime p satisfying

$$0 < v_p(x_i) < d_i. \tag{5.69}$$

(N3)

$$\beta = 1 - \sum_{j=0}^{n} \frac{n-1}{d_j} \geq 0. \tag{5.70}$$

According to the classic analogy between polynomials and integers, we think that the analogue of the Borel type theorem in number theory should be the following problem:

Conjecture 5.28. *If* (N1), (N2) *and* (5.70) *hold, then either there are a finite number of coprime integers $x_0, \ldots, x_n$ satisfying these properties, or there exists a partition of indices*

$$\{0, 1, \ldots, n\} = I_0 \cup I_1 \cup \cdots \cup I_k$$

such that $I_\alpha \neq \emptyset$ $(\alpha = 0, 1, \ldots, k)$, $I_\alpha \cap I_\beta = \emptyset$ $(\alpha \neq \beta)$,

$$\sum_{i \in I_\alpha} x_i = 0, \ \ \alpha = 0, 1, \ldots, k,$$

$x_i/x_j \in \{-1, 1\}$ for any $i, j \in I_\alpha$, and each I_α contains at least two indices.

If $d_i = d$ for $i = 0, \ldots, n$, we think that this conjecture can be strengthened as follows:

Conjecture 5.29. *If* (N1) *and* (N2) *hold for* $d_i = d \geq n^2 - 1$ $(i = 0, \ldots, n)$, *then there exists a partition of indices*

$$\{0, 1, \ldots, n\} = I_0 \cup I_1 \cup \cdots \cup I_k$$

such that $I_\alpha \neq \emptyset$ $(\alpha = 0, 1, \ldots, k)$, $I_\alpha \cap I_\beta = \emptyset$ $(\alpha \neq \beta)$,

$$\sum_{i \in I_\alpha} x_i = 0, \ \ \alpha = 0, 1, \ldots, k,$$

and $x_i/x_j \in \{-1, 1\}$ *for any* $i, j \in I_\alpha$.

This conjecture yields the following special case:

Conjecture 5.30. *Assume that* (N1) *holds. If there are integers* $d \geq n^2 - 1$, $a_i = \pm 1$ *and* y_i *such that*

$$x_i = a_i y_i^d, \ \ i = 0, 1, \ldots, n,$$

then there exists a partition of indices

$$\{0, 1, \ldots, n\} = I_0 \cup I_1 \cup \cdots \cup I_k$$

such that $I_\alpha \neq \emptyset$ $(\alpha = 0, 1, \ldots, k)$, $I_\alpha \cap I_\beta = \emptyset$ $(\alpha \neq \beta)$,

$$\sum_{i \in I_\alpha} a_i y_i^d = 0, \ \ \alpha = 0, 1, \ldots, k,$$

and $y_i/y_j \in \{-1, 1\}$ *for any* $i, j \in I_\alpha$.

Obviously, the Fermat–Wiles theorem is a special case of Conjecture 5.30. Assume that $y_0, y_1, \ldots, y_n$ $(n \geq 2)$ are non-zero integers satisfying

$$a_0 y_0^d + a_1 y_1^d + \cdots + a_n y_n^d = 0, \tag{5.71}$$

where $d \geq n^2 - 1$ and $a_i = \pm 1$ for each i. Further we may assume $\gcd(y_0, y_1, \ldots, y_n) = 1$. If $(y_0, y_1, \ldots, y_n)$ is a non-trivial solution of (5.71), that is, no proper subsums of (5.71) is equal to 0, then Conjecture 5.12 implies that for $\varepsilon > 0$, there exists a number $C = C(n, \varepsilon)$ satisfying

$$\max_{0 \leq j \leq n} \{|y_j|^d\} \leq C \left(\prod_{i=0}^{n} r_{n-1}\big(y_i^d\big) \right)^{1+\varepsilon} \leq C |y_0 y_1 \cdots y_n|^{(n-1)(1+\varepsilon)}$$

which implies

$$\max_{0 \leq j \leq n} \{|y_j|\}^{d - n^2 + 1 - (n^2 - 1)\varepsilon} \leq C(n, \varepsilon).$$

In particular, taking $\varepsilon = \frac{1}{2(n^2-1)}$ and $d \geq n^2$, so

$$d - n^2 + 1 - (n^2 - 1)\varepsilon \geq \frac{d}{2n^2},$$

we deduce from Conjecture 5.12 that

$$\max_{0 \leq j \leq n} \{|y_j|^d\} \leq C\left(n, \frac{1}{2(n^2-1)}\right)^{2n^2}.$$

We have thus proved that in any non-trivial solution of (5.71) with $d \geq n^2$, the numbers $|y_j|^d$ are all less than some absolute bound depending only n, and so there are no more than finitely many such solutions. If we had an explicit version of Conjecture 5.12 (that is, with the values of $C(n, \varepsilon)$ given), then we could give an explicit bound on all non-trivial solutions to the equation (5.71) and compute up to that bound to finally determine whether there are any non-trivial solutions.

Euler had a false intuition when he guessed that the Fermat hypersurface

$$y_1^d + \cdots + y_n^d = y_0^d$$

would have no non-trivial rational solutions for $d = n + 1$. Lander and Parkin [138] found the solution in degree 5:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Then Elkies [56] found infinitely many solutions in degree 4, including

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Chapter 6

Roth's theorem

In this chapter, we introduce simply Roth's theorem, and show that abc-conjecture implies Roth's theorem. Further, following Vojta [287], we compare the analogy between Roth's theorem and Nevanlinna's second main theorem in complex analysis.

6.1 Statement of the theorem

In a relatively early version of determining the best approximations of algebraic numbers by rational numbers, Liouville's theorem [159] implies that if α is a real algebraic number of degree $n \geq 2$, the inequality

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{\mu}} \tag{6.1}$$

has only finitely many rational solutions $\frac{x}{y}$ if $\mu > n$. The great Norwegian mathematician Thue ([272], [273]) showed that (6.1) has only finitely many rational solutions if $\mu > \frac{1}{2}n + 1$. Then Siegel [249] in his thesis showed that this is already true if $\mu > 2\sqrt{n}$. A slight improvement to $\mu > \sqrt{2n}$ was made by Dyson [54]. See also Gelfond [74], [75]. In 1958, K. F. Roth received a Fields prize for his result:

Theorem 6.1 ([223]). *If α is algebraic and $\varepsilon > 0$, there are only finitely many rational numbers $\frac{x}{y}$ with*

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\varepsilon}}.$$

In 1842, Dirichlet [50] proved that given $\alpha \in \mathbb{R}$ and $N > 1$, there exist integers x, y with $1 \leq y \leq N$ and $|\alpha y - x| < 1/N$, which means that when α is irrational, there are infinitely many reduced fractions x/y with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2}.$$

Hence Dirichlet's theorem shows that Roth's result is best possible. An unknown conjecture (cf. Bryuno [21]; Lang [141]; Richtmyer, Devaney and Metropolis [218])

is the following: If α is algebraic and $\varepsilon > 0$, there are only finitely many rational numbers $\frac{x}{y}$ with

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^2(\log y)^{1+\varepsilon}}.$$

In other words, given ε and α algebraic, the inequality

$$-\log\left|\alpha - \frac{x}{y}\right| \leq 2\log y + (1+\varepsilon)\log\log y$$

holds for all but a finite number of fractions x/y in lowest form. A theorem due to A. Khintchine [126] shows that this is true for almost all α.

In 1955, Ridout extended Roth's theorem to p-adic numbers and LeVeque did so for approximations by elements from some fixed number field. In 1960, Lang formulated the following common generalization (cf. [144], [287]). The set of algebraic numbers, that is, the algebraic closure of κ, is denoted by $\bar{\kappa}$.

Theorem 6.2. *Let κ be a number field, let $S \subset M_\kappa$ be a finite subset of absolute values on κ, and assume that each absolute value in S has been extended in some way to $\bar{\kappa}$. Let ε be a positive constant. For each $v \in S$, fix a number $a_v \in \bar{\kappa}$. Then there are only finitely many $x \in \kappa$ such that*

$$\prod_{v\in S} \min\{1, |||x - a_v|||_v\} < \frac{1}{H_*(x)^{2+\varepsilon}}. \tag{6.2}$$

Rather than deal with the approximation condition (6.2), it is easier to deal with a simultaneous set of approximations for all $v \in S$. This idea of reduction to simultaneous approximation is due to Mahler [161], who was also the first one to study Diophantine approximation for p-adic absolute values.

Theorem 6.3. *Let κ be a number field and let $S \subset M_\kappa$ be a finite subset of absolute values on κ with each absolute value extended in some way to $\bar{\kappa}$. Let ε be a positive constant. For each $v \in S$, fix a number $a_v \in \bar{\kappa}$. For each $v \in S$, suppose a real number $\lambda_v \geq 0$ is given such that*

$$\sum_{v\in S} \lambda_v = 1. \tag{6.3}$$

Then there are only finitely many $x \in \kappa$ satisfying the simultaneous system of inequalities

$$\min\{1, |||x - a_v|||_v\} < \frac{1}{H_*(x)^{(2+\varepsilon)\lambda_v}} \tag{6.4}$$

for all $v \in S$.

Proposition 6.4. *Theorem 6.2 is true if and only if Theorem 6.3 is true.*

Proof. Suppose first that Theorem 6.2 is true. Let $\lambda : S \longrightarrow \mathbb{R}[0,1]$ be a function as described in Theorem 6.3, and suppose that $x \in \kappa$ satisfies (6.4). Multiplying the estimate (6.4) over $v \in S$ and using the condition (6.3) shows that x satisfies the inequality (6.2), so Theorem 6.2 tells us that there are only finitely many x's.

We shall now show that Theorem 6.3 implies Theorem 6.2. Suppose we have a sequence of solutions x to (6.2), whose height tends to infinity. For such x, write

$$\min\{1, |||x - a_v|||_v\} = \frac{1}{H_*(x)^{(2+\varepsilon)\xi_v(x)}}$$

with a real number $\xi_v(x) \geq 0$. Then by hypothesis,

$$\sum_{v \in S} \xi_v(x) \geq 1.$$

Now select ε' such that $\varepsilon > \varepsilon' > 0$ and choose a positive integer N such that

$$\left(\frac{2+\varepsilon}{2+\varepsilon'} - 1\right) N > s = \#S.$$

Using induction, and the obvious fact that

$$[\alpha + \beta] \leq [\alpha] + [\beta] + 1, \ \ \{\alpha, \beta\} \subset \mathbb{R},$$

we obtain

$$N + s < \frac{2+\varepsilon}{2+\varepsilon'} N \leq \left[\sum_{v \in S} \frac{2+\varepsilon}{2+\varepsilon'} N\xi_v(x)\right] + 1 \leq \sum_{v \in S} \left[\frac{2+\varepsilon}{2+\varepsilon'} N\xi_v(x)\right] + s,$$

whence

$$N \leq \sum_{v \in S} \left[\frac{2+\varepsilon}{2+\varepsilon'} N\xi_v(x)\right].$$

Consequently there exist integers $i_v(x) \geq 0$ such that

$$i_v(x) \leq \left[\frac{2+\varepsilon}{2+\varepsilon'} N\xi_v(x)\right] \leq \frac{2+\varepsilon}{2+\varepsilon'} N\xi_v(x)$$

and $\sum\limits_v i_v(x) = N$. From this we see that there is only a finite number of possible distributions of such integers $i_v(x)$, and hence, restricting our attention to a subsequence of our elements x if necessary, we can assume that the $i_v(x)$ are the same for all x. We write them i_v. We then put $\lambda_v = i_v/N$ so that $0 \leq \lambda_v \leq 1$ and $\sum \lambda_v = 1$. For each x in our subsequence we have

$$(2+\varepsilon')\lambda_v \leq (2+\varepsilon)\xi_v(x),$$

and hence these x satisfy the simultaneous system of inequalities

$$\min\{1, |||x - a_v|||_v\} \leq \frac{1}{H_*(x)^{(2+\varepsilon')\lambda_v}}.$$

We can therefore apply Theorem 6.3, and have therefore shown what we wanted. □

Proposition 6.5. *If Theorem 6.2 is true for all algebraic integers, then it is true for all algebraic numbers.*

Proof. Let a_v be an algebraic number for each $v \in S$, and suppose that Theorem 6.2 is false for them. This means that there are infinitely many $x \in \kappa$ satisfying the inequality (6.2). We may assume without loss of generality that the a_v satisfy an equation

$$d_n X^n + \cdots + d_0 = 0$$

with $d_i \in \kappa$ (For example, take the product of their irreducible equations over κ). We can clear denominators, and thus assume that all d_i lie in $\mathcal{O}_\kappa$. Multiplying this equation by d_n^{n-1}, we see that $d_n a_v$ is integral over $\mathcal{O}_\kappa$ for each v.

Let $x \in \kappa$ be a solution to (6.2) with

$$H_{*,\kappa}(x) > H_{*,\kappa}(d_n)^{1+6/\varepsilon}.$$

It is clear from the definition of the height that

$$H_{*,\kappa}(d_n x) \le H_{*,\kappa}(d_n) H_{*,\kappa}(x).$$

Further,

$$\prod_{v\in S} \|d_n\|_v \le \prod_{v\in S} \max\{1, \|d_n\|_v\} \le H_{*,\kappa}(d_n).$$

Hence, we have

$$\begin{aligned}
\prod_{v\in S} \min\{1, \|d_n x - d_n a_v\|_v\} &< \frac{H_{*,\kappa}(d_n)}{H_{*,\kappa}(x)^{2+\varepsilon}} = \frac{H_{*,\kappa}(d_n)}{H_{*,\kappa}(x)^{2+\varepsilon/2}} \cdot \frac{1}{H_{*,\kappa}(x)^{\varepsilon/2}} \\
&\le \frac{H_{*,\kappa}(d_n)}{(H_{*,\kappa}(d_n x)/H_{*,\kappa}(d_n))^{2+\varepsilon/2}} \cdot \frac{1}{(H_{*,\kappa}(d_n)^{1+6/\varepsilon})^{\varepsilon/2}} \\
&= \frac{1}{H_{*,\kappa}(d_n x)^{2+\varepsilon/2}}.
\end{aligned}$$

Thus $d_n x$ is a close approximation to $d_n a_v$ in the sense that the inequality (6.2) is true when x, a_v, ε are replaced by $d_n x$, $d_n a_v$, $\varepsilon/2$. Hence the falsity of Theorem 6.2 for a_v implies its falsity for the algebraic integers $d_n a_v$. This proves the proposition. □

6.2 Siegel's lemma

Consider a system of homogeneous linear equations

$$a_{i1}x_1 + \cdots + a_{in}x_n = 0, \quad i = 1, \ldots, m. \tag{6.5}$$

If $m < n$ and the coefficients lie in $\mathbb{Z}$, then there is a nontrivial solution with components in $\mathbb{Z}$. It is reasonable to believe that if the coefficients are small integers, then there will also be a solution in small integers. This idea was used by A. Thue [272] and formalized by Siegel [251], called the *first version of Siegel's lemma*:

Lemma 6.6. *Let $m < n$ be positive integers, and let (6.5) be a system of linear equations with integer coefficients not all zero. Then there is a solution $\mathbf{x} = (x_1, \dots, x_n)$ to this system of equations with $x_1, \dots, x_n$ integers, not all zero, and satisfying*

$$|\mathbf{x}|_* = \max_{1 \le j \le n} |x_j| \le \Big(n \max_{i,j} |a_{ij}| \Big)^{\frac{m}{n-m}}.$$

Proof. For any real number r we set

$$r^+ = \max\{0, r\}, \quad r^- = \max\{0, -r\},$$

so that $r = r^+ - r^-$ and $|r| = r^+ + r^-$. We also define linear forms

$$L_i(\mathbf{x}) = \sum_{j=1}^{n} a_{ij} x_j,$$

and set

$$L_i^+ = \sum_{j=1}^{n} a_{ij}^+, \quad L_i^- = \sum_{j=1}^{n} a_{ij}^-, \quad L_i = L_i^+ + L_i^-.$$

Taking B to be an integer and assuming $0 \le x_i \le B$, we deduce that $L_i(\mathbf{x})$ lies in the interval $\mathbb{R}[-BL_i^-, BL_i^+]$. The number of integer vectors in the box consisting of these intervals is equal to

$$\#\Big(\mathbb{Z}^m \cap \prod_{i=1}^{m} \mathbb{R}[-BL_i^-, BL_i^+] \Big) = \prod_{i=1}^{m} (1 + BL_i^- + BL_i^+) = \prod_{i=1}^{m} (1 + BL_i),$$

while the number of integer vectors $\mathbf{x}$ with $0 \le x_i \le B$ is $(B+1)^n$. Hence if we choose B to satisfy

$$(B+1)^n > \prod_{i=1}^{m} (1 + BL_i), \tag{6.6}$$

then the pigeonhole principle provides us with distinct integer vectors $\mathbf{y}$ and $\mathbf{y}'$ such that

$$L_i(\mathbf{y}) = L_i(\mathbf{y}'), \ \ i = 1, \dots, m.$$

Then the vector $\mathbf{x} = \mathbf{y} - \mathbf{y}'$ is an integer solution of our linear system satisfying $|\mathbf{x}|_* \le B$.

To complete the proof of Siegel's lemma, it remains only to verify that the values

$$B = \Big[(nA)^{\frac{m}{n-m}} \Big], \quad A = \max_{i,j} |a_{ij}|$$

satisfy the condition (6.6). Since

$$B + 1 > (nA)^{\frac{m}{n-m}},$$

and hence

$$(B+1)^n = (B+1)^m(B+1)^{n-m} > (B+1)^m(nA)^m,$$

we observe that

$$L_i \le n \max_j |a_{ij}|, \quad 1 \le nA,$$

and hence

$$\prod_{i=1}^{m}(1+BL_i) \le \{(B+1)nA\}^m < (B+1)^n.$$

Thus Siegel's lemma is proved. □

Now we show the *second version of Siegel's lemma* (cf. [98]):

Lemma 6.7. *Let κ be a number field with $d = [\kappa : \mathbb{Q}]$, let m, n be positive integers with $dm < n$, let (6.5) be a system of linear equations with coefficients in κ not all zero, and let*

$$A = H_*(a_{11}, \dots, a_{ij}, \dots, a_{mn})$$

be the height of the vector formed by the a_{ij}'s. Then there is a solution $\mathbf{x} = (x_1, \dots, x_n)$ to this system of equations with $x_1, \dots, x_n$ integers, not all zero, and satisfying

$$|\mathbf{x}|_* \le (nA)^{\frac{dm}{n-dm}}.$$

Proof. Take a family $a = \{a_v\}_{v \in M_\kappa}$ of elements in κ. Let $c = \{c_v\}$ be a multiplicative M_κ-constant with $c_v \ge 1$ for all $v \in M_\kappa$, write

$$C = \prod_{v \in M_\kappa} c_v^{n_v},$$

and set

$$\kappa[a;c] = \{x \in \kappa \mid |x - a_v|_v \le c_v,\ v \in M_\kappa\}.$$

One claims that

$$\#\kappa[a;c] \le \left(1 + 2\sqrt[d]{C}\right)^d. \tag{6.7}$$

Using the notations in Proposition 2.14 and its remarks, set

$$\kappa_{\mathbb{R}} = \prod_{v \in M_\kappa^\infty} \kappa_v = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},$$

and for $\alpha \in \kappa$ and $\varepsilon > 0$, consider the box

$$B(\alpha, \varepsilon) = \{\mathbf{x} \in \kappa_{\mathbb{R}} \mid |x_v - \sigma_v(\alpha)| < \varepsilon c_v,\ v \in M_\kappa^\infty\}.$$

We first observe that if $\alpha, \beta \in \kappa[a;c]$ and if we take $\varepsilon = \frac{1}{2}C^{-1/d}$, then the intersection $B(\alpha,\varepsilon) \cap B(\beta,\varepsilon)$ is empty. To verify this, suppose that $\mathbf{x}$ sits in both boxes. If v is Archimedean, then

$$|\alpha - \beta|_v = |\sigma_v(\alpha) - \sigma_v(\beta)| \le |x_v - \sigma_v(\alpha)| + |x_v - \sigma_v(\beta)| < 2\varepsilon c_v;$$

and if v is non-Archimedean, then

$$|\alpha - \beta|_v \le \max\{|\alpha - a_v|_v, |\beta - a_v|_v\} \le c_v.$$

It follows that

$$\prod_{v \in M_\kappa} |\alpha - \beta|_v^{n_v} < (2\varepsilon)^d C = 1,$$

and then the product formula tells us that $\alpha = \beta$.

Now the disjointedness of the $B(\alpha,\varepsilon)$'s for $\alpha \in \kappa[a;c]$ implies that

$$\mathrm{Vol}\Big(\bigcup_{\alpha \in \kappa[a;c]} B(\alpha,\varepsilon)\Big) = \#\kappa[a;c]\mathrm{Vol}(B(0,\varepsilon)) = \#\kappa[a;c]\varepsilon^d \mathrm{Vol}(B(0,1)).$$

Next, if $\mathbf{x} \in B(\alpha,\varepsilon)$ with $\alpha \in \kappa[a;c]$, then

$$|x_v - \sigma_v(a_v)| \le |x_v - \sigma_v(\alpha)| + |\alpha - a_v|_v < (1+\varepsilon)c_v.$$

These inequalities define a box with volume equal to $(1+\varepsilon)^d \mathrm{Vol}(B(0,1))$; hence

$$\#\kappa[a;c] \le \left(\frac{1+\varepsilon}{\varepsilon}\right)^d = \left(1 + 2\sqrt[d]{C}\right)^d.$$

This proves the claim.

We now proceed with the proof of Lemma 6.7. Set

$$\delta = \frac{dm}{n - dm}, \quad N = [(nA)^\delta].$$

Applying the claim with

$$a_v = \begin{cases} L_i\left(\frac{N}{2}, \dots, \frac{N}{2}\right), & \text{if } v \in M_\kappa^\infty, \\ 0, & \text{otherwise,} \end{cases}$$

$$c_v = \begin{cases} \frac{nN}{2} \max |a_{ij}|_v, & \text{if } v \in M_\kappa^\infty, \\ \max |a_{ij}|_v, & \text{otherwise,} \end{cases}$$

and noting that for integers $\mathbf{y} = (y_1, \dots, y_n)$ with $0 \le y_i \le N$

$$|L_i(\mathbf{y}) - a_v|_v \le c_v,$$

we then compute the associated constant

$$C = \prod_{v\in M_\kappa} c_v^{n_v} = \left(\frac{nN}{2}\right)^d \prod_{v\in M_\kappa} \max|a_{ij}|_v^{n_v} \le \left(\frac{nNA}{2}\right)^d,$$

and conclude that the linear form $L_i(\mathbf{y})$ takes at most $(1+nNA)^d$ values, and hence that $L = (L_1,\dots,L_m)$ takes at most $(1+nNA)^{dm}$ values. But $N+1 > (nA)^\delta$, which implies that

$$(N+1)^n = (N+1)^{n-dm}(N+1)^{dm} > (nA)^{dm}(N+1)^{dm} \ge (1+nNA)^{dm}.$$

The pigeonhole principle says that there are distinct n-tuples of integers $\mathbf{y}$ and $\mathbf{y}'$ satisfying $L(\mathbf{y}) = L(\mathbf{y}')$. Hence

$$L(\mathbf{y}-\mathbf{y}') = 0, \quad |\mathbf{y}-\mathbf{y}'|_* \le N \le (nA)^\delta$$

as required. □

6.3 Indices of polynomials

Let κ be any field, let $P(X_1,\dots,X_n) \in \kappa[X_1,\dots,X_n]$ be a polynomial, and take

$$\alpha = (\alpha_1,\dots,\alpha_n) \in \kappa^n; \quad \mathbf{r} = (r_1,\dots,r_n) \in (\mathbb{Z}^+)^n.$$

The *index of P with respect to* $(\alpha;\mathbf{r})$, denoted by $\mathrm{Ind}(P)$, is the smallest value

$$\mathrm{Ind}(P) = \min_{\partial_{\mathbf{i}}P(\alpha)\ne 0} \left\{ \frac{i_1}{r_1} + \cdots + \frac{i_n}{r_n} \right\}.$$

If P is the zero polynomial, we set the index equal to ∞.

Lemma 6.8. *Let $P, P' \in \kappa[X_1,\dots,X_n]$ be polynomials. The index with respect to $(\alpha;\mathbf{r})$ has the following properties:*

(i) $\mathrm{Ind}(\partial_{\mathbf{i}}P) \ge \mathrm{Ind}(P) - \left(\frac{i_1}{r_1} + \cdots + \frac{i_n}{r_n}\right)$.

(ii) $\mathrm{Ind}(P+P') \ge \min\{\mathrm{Ind}(P), \mathrm{Ind}(P')\}$.

(iii) $\mathrm{Ind}(PP') = \mathrm{Ind}(P) + \mathrm{Ind}(P')$.

Proof. Using the definition of the index, we can choose

$$\mathbf{j} = (j_1,\dots,j_n) \in \mathbb{Z}_+^n$$

such that $\partial_{\mathbf{j}}\partial_{\mathbf{i}}P(\alpha) \ne 0$ and such that

$$\mathrm{Ind}(\partial_{\mathbf{i}}P) = \frac{j_1}{r_1} + \cdots + \frac{j_n}{r_n}.$$

Since $\partial_{\mathbf{i}+\mathbf{j}}P(\alpha) \neq 0$, we have

$$\mathrm{Ind}(P) \leq \frac{i_1+j_1}{r_1} + \cdots + \frac{i_n+j_n}{r_n} = \left(\frac{i_1}{r_1} + \cdots + \frac{i_n}{r_n}\right) + \mathrm{Ind}(\partial_{\mathbf{i}}P),$$

and so (i) follows.

To prove (ii), we choose

$$\mathbf{j} = (j_1, \ldots, j_n) \in \mathbb{Z}_+^n$$

such that $\partial_{\mathbf{j}}(P+P')(\alpha) \neq 0$ and such that

$$\mathrm{Ind}(P+P') = \frac{j_1}{r_1} + \cdots + \frac{j_n}{r_n}.$$

Then either $\partial_{\mathbf{j}}P(\alpha) \neq 0$ or $\partial_{\mathbf{j}}P'(\alpha) \neq 0$ (or both), which implies that

$$\min\{\mathrm{Ind}(P), \mathrm{Ind}(P')\} \leq \frac{j_1}{r_1} + \cdots + \frac{j_n}{r_n} = \mathrm{Ind}(P+P').$$

Finally, using Leibniz's formula for the derivative of a product, we can write

$$\partial_{\mathbf{j}}(PP') = \sum_{\mathbf{i}+\mathbf{i}'=\mathbf{j}} \partial_{\mathbf{i}}P\partial_{\mathbf{i}'}P'.$$

Choose

$$\mathbf{j} = (j_1, \ldots, j_n) \in \mathbb{Z}_+^n$$

such that $\partial_{\mathbf{j}}(PP')(\alpha) \neq 0$ and such that

$$\mathrm{Ind}(PP') = \frac{j_1}{r_1} + \cdots + \frac{j_n}{r_n}.$$

Then there exist

$$\mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{Z}_+^n, \quad \mathbf{i}' = (i_1', \ldots, i_n') \in \mathbb{Z}_+^n$$

with $\mathbf{i}+\mathbf{i}' = \mathbf{j}$ such that $\partial_{\mathbf{i}}P(\alpha) \neq 0$ and $\partial_{\mathbf{i}'}P'(\alpha) \neq 0$. Hence

$$\mathrm{Ind}(P) \leq \frac{i_1}{r_1} + \cdots + \frac{i_n}{r_n}, \quad \mathrm{Ind}(P') \leq \frac{i_1'}{r_1} + \cdots + \frac{i_n'}{r_n},$$

and adding these inequalities gives

$$\mathrm{Ind}(P) + \mathrm{Ind}(P') \leq \mathrm{Ind}(PP').$$

To get the inequality in the other direction, we look at the set

$$I_P = \left\{ \mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{Z}_+^n \;\middle|\; \partial_{\mathbf{i}}P(\alpha) \neq 0,\ \mathrm{Ind}(P) = \sum_{h=1}^{n} \frac{i_h}{r_h} \right\}.$$

We order I_P lexicographically and choose the smallest one, call it $\imath = (\imath_1, \ldots, \imath_n)$. This means that if $\mathbf{i} \in I_P - \{\imath\}$, then there exists an $l \geq 1$ such that

$$\imath_h = i_h \ (1 \leq h < l), \quad \imath_l < i_l.$$

Similarly, we choose $\imath'$ for $I_{P'}$, and we set $\jmath = \imath + \imath'$. Then

$$\partial_\jmath(PP')(\alpha) = \partial_\imath P(\alpha)\partial_{\imath'}P'(\alpha) \neq 0,$$

since all of the other terms will be zero. Therefore

$$\mathrm{Ind}(PP') \leq \sum_{h=1}^{n} \frac{\jmath_h}{r_h} = \sum_{h=1}^{n} \frac{\imath_h + \imath'_h}{r_h} = \mathrm{Ind}(P) + \mathrm{Ind}(P').$$

This is the other inequality, which completes the proof of (iii). □

The average value $\frac{1}{2}$ in the next *combinatorial lemma* will explain the 2 in Roth's theorem.

Lemma 6.9. *Let $r_1, \ldots, r_n$ be positive integers and fix an $0 < \delta < 1$. Then there are at most*

$$(r_1 + 1) \cdots (r_n + 1)e^{-\delta^2 n/4}$$

n-tuples of integers $(i_1, \ldots, i_n)$ in the range

$$0 \leq i_1 \leq r_1,\ 0 \leq i_2 \leq r_2, \ldots, 0 \leq i_n \leq r_n$$

that satisfy the condition

$$\sum_{h=1}^{n} \frac{i_h}{r_h} < n\left(\frac{1}{2} - \delta\right).$$

Proof. Let $I(n, \delta)$ be the set of n-tuples that we are trying to count,

$$I(n,\delta) = \left\{ \mathbf{i} \in \mathbb{Z}[0, r_1] \times \cdots \times \mathbb{Z}[0, r_n] \;\middle|\; \sum_{h=1}^{n} \frac{i_h}{r_h} < n\left(\frac{1}{2} - \delta\right) \right\}.$$

Since $e^t \geq 1$ for all $t \geq 0$, then we have

$$\begin{aligned} \#I(n,\delta) &= \sum_{\mathbf{i} \in I(n,\delta)} 1 \leq \sum_{\mathbf{i} \in I(n,\delta)} \exp\left(\frac{\delta}{2}\left\{\frac{n}{2} - \delta n - \frac{i_1}{r_1} - \cdots - \frac{i_n}{r_n}\right\}\right) \\ &\leq \sum_{i_1=0}^{r_1} \cdots \sum_{i_n=0}^{r_n} \exp\left(\frac{\delta}{2}\left\{\frac{n}{2} - \delta n - \frac{i_1}{r_1} - \cdots - \frac{i_n}{r_n}\right\}\right), \end{aligned}$$

which further yields

$$\#I(n,\delta) \le \exp\left(-\frac{\delta^2 n}{2}\right) \prod_{h=1}^{n} \left\{ \sum_{i=0}^{r_h} \exp\left(\frac{\delta}{2}\left(\frac{1}{2} - \frac{i}{r_h}\right)\right)\right\}.$$

When $|t| \le 1$, we use the inequality

$$e^t \le 1 + t + t^2$$

to estimate one of the inner sums as

$$\begin{aligned} \sum_{i=0}^{r} \exp\left(\frac{\delta}{2}\left(\frac{1}{2} - \frac{i}{r}\right)\right) &\le \sum_{i=0}^{r} \left\{ 1 + \frac{\delta}{2}\left(\frac{1}{2} - \frac{i}{r}\right) + \frac{\delta^2}{4}\left(\frac{1}{2} - \frac{i}{r}\right)^2 \right\} \\ &= (r+1)\left(1 + \frac{\delta^2}{48} + \frac{\delta^2}{24r}\right) \\ &\le (r+1)\left(1 + \frac{\delta^2}{16}\right) \end{aligned}$$

since $r \ge 1$. Substituting this estimate in above, we find that

$$\#I(n,\delta) \le \exp\left(-\frac{\delta^2 n}{2}\right) \prod_{h=1}^{n} \left\{ (r_h+1)\left(1 + \frac{\delta^2}{16}\right)\right\}.$$

Note that $1 + t \le e^t$ for $t \ge 0$. Then

$$\begin{aligned} \#I(n,\delta) &\le \exp\left(-\frac{\delta^2 n}{2}\right) \prod_{h=1}^{n} \left\{ (r_h+1)\exp\left(\frac{\delta^2}{16}\right)\right\} \\ &= (r_1+1)\cdots(r_n+1)\exp\left(-\frac{7\delta^2 n}{16}\right), \end{aligned}$$

and so the lemma is proved. □

Proposition 6.10. *Let κ be a number field with $d = [\kappa : \mathbb{Q}]$, fix a number $a_v \in \kappa$ for each $v \in S$, let $1 > \delta > 0$ be a fixed constant, set $m = \#S$, and let n be an integer satisfying*

$$e^{\delta^2 n/4} > 2md. \tag{6.8}$$

Take $\mathbf{r} = (r_1, \ldots, r_n) \in (\mathbb{Z}^+)^n$. Then there exists a polynomial $P(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ satisfying the following three conditions:

(1) *P has degree at most r_h in the variable X_h.*

(2) *For each $v \in S$, the index of P with respect to $((a_v, \ldots, a_v); \mathbf{r})$ satisfies*

$$\theta_v = \mathrm{Ind}(P) \ge n\left(\frac{1}{2} - \delta\right). \tag{6.9}$$

(3) *If setting* $\mathbf{a} = (a_v)_{v\in S} \in \kappa^m$*, the largest coefficient of* P *satisfies*

$$|P|_* \le \{4H_*(1,\mathbf{a})\}^{r_1+\cdots+r_n}. \tag{6.10}$$

Proof. We write the polynomial P as

$$P(X_1,\dots,X_n) = \sum_{j_1=0}^{r_1}\cdots\sum_{j_n=0}^{r_n} b_{j_1\cdots j_n} X_1^{j_1}\cdots X_n^{j_n},$$

where the integers $b_{j_1\cdots j_n}$ are unknowns to be determined. Clearly, the number of coefficients $b_{j_1\cdots j_n}$ is

$$N = (r_1+1)\cdots(r_n+1).$$

For any n-tuple

$$\mathbf{i} = (i_1,\dots,i_n) \in \mathbb{Z}[0,r_1]\times\cdots\times\mathbb{Z}[0,r_n],$$

we have

$$\partial_{\mathbf{i}}P(X_1,\dots,X_n) = \sum_{j_1=0}^{r_1}\cdots\sum_{j_n=0}^{r_n} b_{j_1\cdots j_n}\binom{j_1}{i_1}\cdots\binom{j_n}{i_n} X_1^{j_1-i_1}\cdots X_n^{j_n-i_n},$$

Evaluating this identity at $(a_v,\dots,a_v)$, we find that

$$\partial_{\mathbf{i}}P(a_v,\dots,a_v) = \sum_{\mathbf{j}} b_{\mathbf{j}}\binom{j_1}{i_1}\cdots\binom{j_n}{i_n} a_v^{j_1-i_1+\cdots+j_n-i_n}.$$

Hence $\partial_{\mathbf{i}}P(a_v,\dots,a_v) = 0$ if we choose the $b_{\mathbf{j}}$ to satisfy linear equations

$$\sum_{\mathbf{j}}\binom{j_1}{i_1}\cdots\binom{j_n}{i_n} a_v^{j_1-i_1+\cdots+j_n-i_n} b_{\mathbf{j}} = 0,\ \ l = 1,\dots,m. \tag{6.11}$$

In order to satisfy condition (2), we need $\partial_{\mathbf{i}}P(a_v,\dots,a_v) = 0$ for all n-tuple

$$\mathbf{i} = (i_1,\dots,i_n) \in \mathbb{Z}[0,r_1]\times\cdots\times\mathbb{Z}[0,r_n],$$

satisfying

$$\frac{i_1}{r_1}+\cdots+\frac{i_n}{r_n} < n\left(\frac{1}{2}-\delta\right).$$

According to Lemma 6.9, there are at most $Ne^{-\delta^2 n/4}$ such n-tuples. Hence we can find a P that satisfies (2) by choosing the $b_{\mathbf{j}}$ to satisfy the system (6.11) of M linear equations, where

$$M \le mNe^{-\delta^2 n/4} < \frac{N}{2d}.$$

Now applying Siegel's Lemma 6.7, we find that there is a polynomial P satisfying (1) and (2) whose coefficients $b_{\mathbf{j}}$ are bounded by

$$|P|_* \le (NA)^{\frac{dM}{N-dM}} \le NA,$$

where

$$A = H_*\left(\ldots, \binom{j_1}{i_1}\cdots\binom{j_n}{i_n} a_v^{j_1-i_1+\cdots+j_n-i_n}, \ldots\right) \le \{2H_*(1,\mathbf{a})\}^{r_1+\cdots+r_n},$$

and hence

$$|P|_* \le (r_1+1)\cdots(r_n+1)\{2H_*(1,\mathbf{a})\}^{r_1+\cdots+r_n} \le \{4H_*(1,\mathbf{a})\}^{r_1+\cdots+r_n},$$

which yields the estimate (6.10) in (3). □

6.4 Roth's lemma

Let $P \in \bar{\mathbb{Q}}[X_1,\ldots,X_n]$ be a polynomial with algebraic coefficients and $\deg_{X_h}(P) \le r_h$. We can choose a decomposition of P in the form

$$P(X_1,\ldots,X_n) = \sum_{j=1}^{l} \varphi_j(X_1,\ldots,X_{n-1})\psi_j(X_n), \tag{6.12}$$

where φ_j, ψ_j are polynomials with coefficients in $\bar{\mathbb{Q}}$, with the smallest number of summands, that is, the number l is smallest. It follows that $l \le r_n + 1$.

Lemma 6.11. *The polynomials $\varphi_1,\ldots,\varphi_l$ appearing in the minimal decomposition* (6.12) *of P are linearly independent over $\bar{\mathbb{Q}}$. Similarly, the polynomials $\psi_1,\ldots,\psi_l$ are linearly independent over $\bar{\mathbb{Q}}$.*

Proof. Assume, to the contrary, that $\varphi_1,\ldots,\varphi_l$ are linearly dependent over $\bar{\mathbb{Q}}$, that is, there is a nontrivial linear relation

$$c_1\varphi_1 + \cdots + c_l\varphi_l = 0.$$

Without loss of generality, we may assume that $c_l \ne 0$. Thus

$$P = \sum_{j=1}^{l} \varphi_j\psi_j = \sum_{j=1}^{l-1} \varphi_j\psi_j - \sum_{j=1}^{l-1} \frac{c_j}{c_l}\varphi_j\psi_l = \sum_{j=1}^{l-1} \varphi_j\left(\psi_j - \frac{c_j}{c_l}\psi_l\right),$$

contradicting the minimality of l. This proves that $\varphi_1,\ldots,\varphi_l$ are linearly independent over $\bar{\mathbb{Q}}$. Similarly, it can be proved that $\psi_1,\ldots,\psi_l$ are linearly independent over $\bar{\mathbb{Q}}$. □

For nonzero multi-indices

$$\mathbf{i}_\nu \in (\mathbb{Z}_+)^{n-1},\ \ \nu = 1, \dots, l-1,$$

we define the *generalized Wronskian determinant* of $\varphi_1, \dots, \varphi_l$ by

$$\mathbf{W}(\varphi_1, \dots, \varphi_l) = \mathbf{W}_{\mathbf{i}_1 \cdots \mathbf{i}_{l-1}}(\varphi_1, \dots, \varphi_l) = \begin{vmatrix} \varphi_1 & \varphi_2 & \cdots & \varphi_l \\ \partial_{\mathbf{i}_1}\varphi_1 & \partial_{\mathbf{i}_1}\varphi_2 & \cdots & \partial_{\mathbf{i}_1}\varphi_l \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{\mathbf{i}_{l-1}}\varphi_1 & \partial_{\mathbf{i}_{l-1}}\varphi_2 & \cdots & \partial_{\mathbf{i}_{l-1}}\varphi_l \end{vmatrix}.$$

It is a standard theorem that the functions $\varphi_1, \dots, \varphi_l$ are linearly independent over $\bar{\mathbb{Q}}$ if and only if there exist multi-indices $\mathbf{i}_\nu$ with $0 < |\mathbf{i}_\nu| \le \nu$ such that $\mathbf{W}(\varphi_1, \dots, \varphi_l) \not\equiv 0$. Next we will use the multi-indices satisfying above properties.

In particular, if taking

$$e_n = (0, \dots, 0, 1) \in \mathbb{Z}^n,$$

and noting that

$$\partial_{je_n} = \frac{1}{j!}\frac{\partial^j}{\partial X_n^j},\ \ j \in \mathbb{Z}_+,$$

we obtain the classical *Wronskian determinant* of $\psi_1, \dots, \psi_l$

$$\mathbf{W}(\psi_1, \dots, \psi_l) = \begin{vmatrix} \psi_1 & \psi_2 & \cdots & \psi_l \\ \partial_{e_n}\psi_1 & \partial_{e_n}\psi_2 & \cdots & \partial_{e_n}\psi_l \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{(l-1)e_n}\psi_1 & \partial_{(l-1)e_n}\psi_2 & \cdots & \partial_{(l-1)e_n}\psi_l \end{vmatrix},$$

up to a multiple $\{1!2!\cdots(l-1)!\}^{-1}$. Lemma 6.11 implies that $\mathbf{W}(\psi_1, \dots, \psi_l) \not\equiv 0$.

We consider the polynomial

$$\mathcal{P} = \mathbf{W}_{\mathbf{i}_1 \cdots \mathbf{i}_{l-1}}\left(P, \partial_{e_n}P, \dots, \partial_{(l-1)e_n}P\right).$$

Note that the differential operators $\partial_{\mathbf{i}_\nu}$ involve only $X_1, \dots, X_{n-1}$. We obtain

$$\mathcal{P} = \mathbf{W}_{\mathbf{i}_1 \cdots \mathbf{i}_{l-1}}\left(\sum_{j=1}^{l}\varphi_j\psi_j, \sum_{j=1}^{l}\varphi_j\partial_{e_n}\psi_j, \dots, \sum_{j=1}^{l}\varphi_j\partial_{(l-1)e_n}\psi_j\right) = \Phi\Psi,$$

where

$$\Phi = \mathbf{W}(\varphi_1, \dots, \varphi_l), \quad \Psi = \mathbf{W}(\psi_1, \dots, \psi_l).$$

It is obvious that

$$\deg_{X_h}(\Phi) \le lr_h\ (1 \le h \le n-1); \quad \deg_{X_n}(\Psi) \le lr_n. \tag{6.13}$$

We also note that since Φ and Ψ use distinct sets of variables, it is clear from the definition of height of a polynomial that

$$h_*(\mathcal{P}) = h_*(\Phi) + h_*(\Psi). \tag{6.14}$$

Finally, we state the *Roth's lemma* (See [98], Proposition D.6.2):

Lemma 6.12. *Let n be a positive integer and let $P \in \bar{\mathbb{Q}}[X_1, \ldots, X_n]$ be a polynomial with algebraic coefficients and $\deg_{X_h}(P) \le r_h$. Let $\mathbf{x} = (x_1, \ldots, x_n)$ be an n-tuple of algebraic numbers. Fix a real number $\eta > 0$ such that*

$$\frac{r_{h+1}}{r_h} \le \eta^{2^{n-1}}, \quad h = 1, \ldots, n-1, \tag{6.15}$$

and

$$\eta^{2^{n-1}} \min_{1 \le h \le n} \{r_h \log H_*(x_h)\} \ge \log H_*(P) + 2nr_1. \tag{6.16}$$

Then the index of P with respect to $(\mathbf{x}; \mathbf{r})$ satisfies

$$\mathrm{Ind}(P) \le 2n\eta.$$

Proof. If $\eta \ge \frac{1}{2}$, the conclusion of Lemma 6.12 is trivial since we always have $\mathrm{Ind}(P) \le n$. Next we assume that $\eta < \frac{1}{2}$. Let κ be a number field containing all the x_h's and the coefficients of P, and set $d = [\kappa : \mathbb{Q}]$.

The proof is by induction on n, the number of variables. We begin with the case $n = 1$. Let s be the order of vanishing of $P(X_1)$ at $X_1 = x_1$, so

$$P(X_1) = (X_1 - x_1)^s Q(X_1), \quad Q(x_1) \ne 0.$$

Since the index of P at $(x_1; r_1)$ is $\mathrm{Ind}(P) = s/r_1$, then Gelfand's inequality (Lemma 4.22) yields

$$\begin{aligned} H_*(x_1)^{r_1 \mathrm{Ind}(P)} &= H_*(x_1)^s = H_*(X_1 - x_1)^s \\ &\le H_*(X_1 - x_1)^s H_*(Q) \le e^{r_1} H_*(P), \end{aligned}$$

which implies

$$\mathrm{Ind}(P) \le \frac{\log H_*(P) + r_1}{r_1 \log H_*(x_1)} \le \eta$$

by using (6.16). This completes the proof of Roth's lemma for polynomials of one variable.

We mow assume that Roth's lemma is true for polynomials with strictly fewer than n variables, and we prove it for a polynomial $P(X_1, \ldots, X_n)$ of n variables with $n \ge 2$. First of all, we claim that

$$h_*(\mathcal{P}) \le l \left\{ h_*(P) + 2r_1 \right\}. \tag{6.17}$$

When $l = 1$, this is trivial since $\mathcal{P} = P$. Next we assume that $l \geq 2$. The determinant $\mathcal{P}$ is the sum of $l!$ terms, each of which is a product of l polynomials of degree at most r_h with respect to X_h and satisfying (see (4.17), (4.16))

$$\begin{aligned} |\mathcal{P}|_{*,v} &\leq \varsigma_{v,l!}^2 \max_{(j_1,\dots,j_l)} |(\partial_{j_1 e_n} P)(\partial_{\mathbf{i}_1}\partial_{j_2 e_n} P)\cdots(\partial_{\mathbf{i}_{l-1}}\partial_{j_l e_n} P)|_{*,v} \\ &\leq \varsigma_{v,l!}^2 \varsigma_{v,N}^{2(l-1)} \max_{(j_1,\dots,j_l)} |\partial_{j_1 e_n} P|_{*,v} |\partial_{\mathbf{i}_1}\partial_{j_2 e_n} P|_{*,v} \cdots |\partial_{\mathbf{i}_{l-1}}\partial_{j_l e_n} P|_{*,v}, \end{aligned}$$

where $(j_1, \dots, j_l)$ runs over all permutations of $\{0, 1, \dots, l-1\}$, $v \in M_\kappa$ and

$$N = 2^{r_1 + \cdots + r_n}.$$

According to the proof of Lemma 4.15, we get

$$|\mathcal{P}|_{*,v} \leq \varsigma_{v,l!}^2 \varsigma_{v,N}^{2(2l-1)} |P|_{*,v}^l, \tag{6.18}$$

which yields a bound

$$h_*(\mathcal{P}) \leq l h_*(P) + (2l-1)(r_1 + \cdots + r_n)\log 2 + \log l!. \tag{6.19}$$

The condition (6.15) implies

$$r_1 + \cdots + r_n \leq (1 + \omega + \cdots + \omega^{n-1}) r_1 = \frac{1-\omega^n}{1-\omega} r_1,$$

where $\omega = \eta^{2^{n-1}}$. Since $n \geq 2$ and $\eta < \frac{1}{2}$, we have $\omega < \frac{1}{4}$, and hence

$$\frac{1-\omega^n}{1-\omega} \leq \begin{cases} \frac{5}{4}, & \text{if } n = 2, \\ \frac{4}{3}, & \text{if } n \geq 3. \end{cases}$$

On the other hand,

$$\frac{\log l!}{l} \leq \log l \leq l - 1 \leq r_n \leq \omega^{n-1} r_1.$$

Thus (6.19) implies

$$h_*(\mathcal{P}) \leq l \left\{ h_*(P) + c_n r_1 \right\}, \tag{6.20}$$

where

$$c_n = \begin{cases} \frac{10}{4}\log 2 + \frac{1}{4} \approx 1.983, & \text{if } n = 2, \\ \frac{8}{3}\log 2 + \frac{1}{16} \approx 1.911, & \text{if } n \geq 3, \end{cases}$$

and so (6.17) follows from (6.20).

Secondly, we claim that if Roth's lemma is true for polynomials in $n-1$ or fewer variables, then the index of Φ with respect to $(x_1, \dots, x_{n-1}; r_1, \dots, r_{n-1})$ and the index of Ψ with respect to $(x_n; r_n)$ satisfy

$$\mathrm{Ind}(\Phi) \leq 2l(n-1)\eta^2, \quad \mathrm{Ind}(\Psi) \leq l\eta^{2^{n-1}}, \tag{6.21}$$

and hence the index of $\mathcal{P}$ with respect to $(\mathbf{x};\mathbf{r})$ satisfies

$$\mathrm{Ind}(\mathcal{P}) = \mathrm{Ind}(\Phi) + \mathrm{Ind}(\Psi) \leq 2l(n-1)\eta^2 + l\eta^{2^{n-1}}. \tag{6.22}$$

In fact, by applying Roth's lemma to Φ and Ψ, we can prove the claim. Set

$$m = n-1, \quad d_h = lr_h, \quad \theta = \eta^2.$$

We obtain $\deg_{X_h}(\Phi) \leq d_h$ from (6.13). The condition (6.15) follows from

$$\frac{d_{h+1}}{d_h} = \frac{r_{h+1}}{r_h} \leq \eta^{2^{n-1}} = \theta^{2^{m-1}}, \ \ h = 1, \ldots, m-1.$$

Next we check condition (6.16):

$$\begin{aligned} \theta^{2^{m-1}} d_h h_*(x_h) &= l\eta^{2^{n-1}} r_h h_*(x_h) \geq l(h_*(P) + 2nr_1) \\ &\geq h_*(\mathcal{P}) + 2mlr_1 \geq h_*(\Phi) + 2mr_1. \end{aligned}$$

By induction we conclude that

$$\mathrm{Ind}(\Phi) = \mathrm{Ind}_{(r_1,\ldots,r_m)}(\Phi) = l\mathrm{Ind}_{(d_1,\ldots,d_m)}(\Phi) \leq 2lm\theta = 2l(n-1)\eta^2.$$

Similarly, we may apply Roth's lemma in one variable to Ψ with

$$m = 1, \quad d_n = lr_n, \quad \omega = \eta^{2^{n-1}}.$$

We have $\deg_{X_n}(\Psi) \leq d_n$ from (6.13). Note that the condition (6.15) is empty when $n = 1$, so we only need to check the condition (6.16):

$$\begin{aligned} h_*(\Psi) + 2d_n &\leq l(h_*(P) + 2r_1) + 2lr_n \leq l\left\{h_*(P) + \left(2 + 2\omega^{n-1}\right) r_1\right\} \\ &\leq l\{h_*(P) + 2nr_1\} \leq \eta^{2^{n-1}} lr_n h_*(x_n) = \omega d_n h_*(x_n). \end{aligned}$$

We apply Roth's lemma for a polynomial in one variable and conclude that

$$\mathrm{Ind}(\Psi) = \mathrm{Ind}_{r_n}(\Psi) = l\mathrm{Ind}_{d_n}(\Psi) \leq l\omega = l\eta^{2^{n-1}}.$$

This completes the proof of the claim.

Thirdly, we claim that the following estimate is valid:

$$\mathrm{Ind}(\mathcal{P}) \geq \frac{l}{2} \min\{\mathrm{Ind}(P), \mathrm{Ind}(P)^2\} - \frac{lr_n}{r_{n-1}}. \tag{6.23}$$

In fact, for $\mathbf{i} \in (\mathbb{Z}_+)^{n-1}$, $j \in \mathbb{Z}_+$ with $|\mathbf{i}| \leq l-1$, we observe

$$\mathrm{Ind}(\partial_{(\mathbf{i},j)} P) \geq \mathrm{Ind}(P) - \frac{i_1}{r_1} - \cdots - \frac{i_{n-1}}{r_{n-1}} - \frac{j}{r_n}$$

from Lemma 6.8 (i). Since $r_1 \geq r_2 \geq \cdots$ from (6.15), it follows that

$$\mathrm{Ind}(\partial_{(\mathbf{i},j)}P) \geq \mathrm{Ind}(P) - \frac{i_1 + \cdots + i_{n-1}}{r_{n-1}} - \frac{j}{r_n} \geq \mathrm{Ind}(P) - \frac{r_n}{r_{n-1}} - \frac{j}{r_n}$$

since $i_1 + \cdots + i_{n-1} \leq l - 1 \leq r_n$. By (ii) and (iii) of Lemma 6.8, we obtain

$$\begin{aligned} \mathrm{Ind}(\mathcal{P}) &\geq \min_{(j_1,\ldots,j_l)} \mathrm{Ind}\left(\partial_{j_1 e_n} P \cdot \partial_{\mathbf{i}_1}\partial_{j_2 e_n} P \cdots \partial_{\mathbf{i}_{l-1}}\partial_{j_l e_n} P\right) \\ &= \min_{(j_1,\ldots,j_l)} \left\{\mathrm{Ind}\left(\partial_{j_1 e_n} P\right) + \mathrm{Ind}\left(\partial_{\mathbf{i}_1}\partial_{j_2 e_n} P\right) + \cdots + \mathrm{Ind}\left(\partial_{\mathbf{i}_{l-1}}\partial_{j_l e_n} P\right)\right\}. \end{aligned}$$

Substituting in the lower bound obtained above, we have

$$\begin{aligned} \mathrm{Ind}(\mathcal{P}) &\geq \sum_{j=0}^{l-1} \max\left\{\mathrm{Ind}(P) - \frac{r_n}{r_{n-1}} - \frac{j}{r_n}, 0\right\} \\ &\geq \sum_{j=0}^{l-1} \max\left\{\mathrm{Ind}(P) - \frac{j}{r_n}, 0\right\} - \frac{l r_n}{r_{n-1}}, \end{aligned}$$

which gives the fundamental inequality

$$\sum_{j=0}^{l-1} \max\left\{\mathrm{Ind}(P) - \frac{j}{r_n}, 0\right\} \leq \mathrm{Ind}(\mathcal{P}) + \frac{l r_n}{r_{n-1}}. \tag{6.24}$$

If $\mathrm{Ind}(P) \geq \frac{l-1}{r_n}$, then (6.23) follows immediately from

$$\sum_{j=0}^{l-1} \max\left\{\mathrm{Ind}(P) - \frac{j}{r_n}, 0\right\} = l\mathrm{Ind}(P) - \frac{(l-1)l}{2r_n} \geq \frac{l}{2}\mathrm{Ind}(P).$$

Next we study the case $\mathrm{Ind}(P) < \frac{l-1}{r_n}$, which means

$$N = [r_n \mathrm{Ind}(P)] \leq l - 1.$$

Then

$$\begin{aligned} \sum_{j=0}^{l-1} \max\left\{\mathrm{Ind}(P) - \frac{j}{r_n}, 0\right\} &= \sum_{j=0}^{N} \left\{\mathrm{Ind}(P) - \frac{j}{r_n}\right\} \\ &= (N+1)\mathrm{Ind}(P) - \frac{N(N+1)}{2r_n}. \end{aligned} \tag{6.25}$$

From the definition of N, we obtain

$$\sum_{j=0}^{l-1} \max\left\{\mathrm{Ind}(P) - \frac{j}{r_n}, 0\right\} \geq \frac{N+1}{2}\mathrm{Ind}(P) \geq \frac{r_n}{2}\mathrm{Ind}(P)^2,$$

and so (6.23) follows from (6.24) when $l \le r_n$. When $l > r_n$, it must be $l = r_n + 1$ since $l \le r_n + 1$. Note that

$$(l-1)\mathrm{Ind}(P) - 1 < N \le (l-1)\mathrm{Ind}(P)$$

and that the quadratic function (6.25) of N arrives the same value at above lower bound and upper bound for N. We find that

$$\begin{aligned}(N+1)\mathrm{Ind}(P) - \frac{N(N+1)}{2(l-1)} &\ge \frac{1}{2}\left\{(l-1)\mathrm{Ind}(P)^2 + \mathrm{Ind}(P)\right\} \\ &\ge \frac{l}{2}\mathrm{Ind}(P)^2\end{aligned}$$

since $\mathrm{Ind}(P) < 1$. Thus we complete the proof of claim (6.23).

Finally, we finish the proof of Roth's lemma. Since $\mathrm{Ind}(P) \le n$, we may use (6.23) to deduce

$$\mathrm{Ind}(\mathcal{P}) + \frac{lr_n}{r_{n-1}} \ge \frac{l}{2n}\mathrm{Ind}(P)^2,$$

while (6.22) implies that

$$\begin{aligned}\mathrm{Ind}(\mathcal{P}) + \frac{lr_n}{r_{n-1}} &\le 2l(n-1)\eta^2 + l\eta^{2^{n-1}} + \frac{lr_n}{r_{n-1}} \\ &\le l\{2(n-1)\eta^2 + 2\eta^{2^{n-1}}\} \le 2nl\eta^2.\end{aligned}$$

We deduce that $\mathrm{Ind}(P)^2 \le 4n^2\eta^2$, and hence $\mathrm{Ind}(P) \le 2n\eta$. □

6.5 Proof of Roth's theorem

It is sufficient to show Theorem 6.3. To do this, we assume that there are infinitely many solutions to (6.4) and derive a contradiction. Decreasing ε only serves to make the theorem stronger, so we may assume that $0 < \varepsilon < 1$. Without loss of generality, we may assume that all $a_v \in \kappa$. Otherwise, let K be some finite extension field of κ containing all a_v, let T be the set of places w of K lying over $v \in S$, and for each $w|v$ let a_w be a certain conjugate of a_v. With proper choices of a_w, the left-hand side of (6.4) will decrease when κ is replaced by K, but the right-hand side will remain unchanged. Based on Proposition 6.5, we may assume that all $a_v \in \kappa$ are algebraic integers. Write $\mathbf{a} = (\dots, a_v, \dots)$ and set $m = \#S$.

Choose an δ with $0 < \delta < \frac{\varepsilon}{22}$, set $d = [\kappa : \mathbb{Q}]$, and take an integer n with

$$e^{\delta^2 n/4} > 2md. \tag{6.26}$$

We define

$$\omega = \omega(n, \delta) = (\delta/4)^{2^{n-1}},$$

which implies

$$2\omega^{2^{-n+1}} = \frac{\delta}{2} < \delta.$$

Since by assumption (6.4) has infinitely many solutions in κ, and since κ has only finitely many elements of bounded height, we can find a solution x_1 whose height satisfies

$$H_*(x_1) \geq \{2^9 H_*(1,\mathbf{a})\}^{12d/\varepsilon}, \quad \log H_*(x_1) \geq \frac{n}{\omega}\{\log(4H_*(1,\mathbf{a})) + 2\}. \tag{6.27}$$

We then choose successively $x_2, \ldots, x_n$ to be solutions to (6.4), that is,

$$\min\{1, \|x_h - a_v\|_v\} < \frac{1}{H_{*,\kappa}(x_h)^{(2+\varepsilon)\lambda_v}}, \ \ v \in S, \tag{6.28}$$

such that

$$H_{*,\kappa}(x_{h+1})^{\omega} \geq H_{*,\kappa}(x_h)^2, \ \ h = 1, \ldots, m-1. \tag{6.29}$$

The sequence of $H_{*,\kappa}(x_h)$'s will be increasing since $\omega < 1$.

Choose an integer r_1 satisfying

$$H_{*,\kappa}(x_1)^{\omega r_1} \geq H_{*,\kappa}(x_n)^2, \tag{6.30}$$

and then define $r_2, \ldots, r_n$ to be the integers

$$r_h = \left\lceil \frac{r_1 \log H_{*,\kappa}(x_1)}{\log H_{*,\kappa}(x_h)} \right\rceil = \left\lceil \frac{r_1 \log H_*(x_1)}{\log H_*(x_h)} \right\rceil, \ \ h = 2, \ldots, n,$$

where $\lceil r \rceil$ denotes the *ceiling* of r, that is, the smallest integer that is greater than or equal to r. By using $r \leq \lceil r \rceil \leq r+1$, we obtain

$$r_1 \log H_{*,\kappa}(x_1) \leq r_h \log H_{*,\kappa}(x_h) \leq r_1 \log H_{*,\kappa}(x_1) + \log H_{*,\kappa}(x_h),$$

which means

$$r_h \log H_{*,\kappa}(x_h) \leq r_1 \log H_{*,\kappa}(x_1) + \log H_{*,\kappa}(x_n) \leq (1+\delta) r_1 \log H_{*,\kappa}(x_1).$$

Exponentiating gives

$$D := \min_{1\leq h\leq n} H_*(x_h)^{r_h} \leq \max_{1\leq h\leq n} H_*(x_h)^{r_h} \leq D^{1+\delta}. \tag{6.31}$$

From the choice of the r_h's, we compute

$$\begin{aligned} \frac{r_{h+1}}{r_h} &\leq \left(\frac{r_1 \log H_*(x_1)}{\log H_*(x_{h+1})} + 1\right) \Big/ \left(\frac{r_1 \log H_*(x_1)}{\log H_*(x_h)}\right) \\ &= \frac{\log H_*(x_h)}{\log H_*(x_{h+1})} + \frac{\log H_*(x_h)}{r_1 \log H_*(x_1)} \leq \frac{\omega}{2} + \frac{\omega}{2} = \omega. \end{aligned}$$

Thus by using (6.29) and (6.30), we find

$$\frac{r_{h+1}}{r_h} \le \omega, \;\; h = 1, \dots, n-1. \tag{6.32}$$

Since n was chosen to verify (6.26), we can use Proposition 6.10 to produce a polynomial $P(X_1, \dots, X_n)$ with $\deg_{X_h}(P) \le r_h$ satisfying (6.9) and (6.10). Take θ_0 satisfying

$$0 < \theta_0 < \theta = \min_{v \in S} \theta_v.$$

Now we claim that if $\mathbf{i} = (i_1, \dots, i_n)$ is any n-tuple satisfying

$$\frac{i_1}{r_1} + \cdots + \frac{i_n}{r_n} \le \theta_0,$$

then

$$\prod_{v \in S} \|\partial_{\mathbf{i}} P(x_1, \dots, x_n)\|_v \le \{8H_*(1, \mathbf{a})\}^{d(r_1 + \cdots + r_n)} H_*(P) D^{-(2+\varepsilon)(\theta - \theta_0)}. \tag{6.33}$$

In fact, we use Lemma 6.8 to compute

$$\mathrm{Ind}(\partial_{\mathbf{i}} P) \ge \mathrm{Ind}(P) - \left(\frac{i_1}{r_1} + \cdots + \frac{i_n}{r_n} \right) \ge \theta - \theta_0.$$

So if we write the Taylor expansion of $\partial_{\mathbf{i}} P$ about $(a_v, \dots, a_v)$, then many of the initial terms will be zero. Thus

$$\partial_{\mathbf{i}} P(X_1, \dots, X_n) = \sum_{\mathbf{j} \in I} \partial_{\mathbf{j}} \partial_{\mathbf{i}} P(a_v, \dots, a_v)(X_1 - a_v)^{j_1} \cdots (X_n - a_v)^{j_n},$$

where

$$I = \left\{ \mathbf{j} \in \mathbb{Z}[0, r_1] \times \cdots \times \mathbb{Z}[0, r_n] \;\middle|\; \frac{j_1}{r_1} + \cdots + \frac{j_n}{r_n} \ge \theta - \theta_0 \right\}.$$

Hence we obtain

$$\begin{aligned} |\partial_{\mathbf{i}} P(x_1, \dots, x_n)|_v &\le \sum_{\mathbf{j} \in I} |\partial_{\mathbf{j}} \partial_{\mathbf{i}} P(a_v, \dots, a_v)|_v |x_1 - a_v|_v^{j_1} \cdots |x_n - a_v|_v^{j_n} \\ &\le (r_1 + 1) \cdots (r_n + 1) \max_{\mathbf{j}} |\partial_{\mathbf{j}} \partial_{\mathbf{i}} P(a_v, \dots, a_v)|_v \\ &\quad \times \max_{\mathbf{j} \in I} |x_1 - a_v|_v^{j_1} \cdots |x_n - a_v|_v^{j_n}. \end{aligned}$$

Note that

$$\begin{aligned} |\partial_{\mathbf{j}} \partial_{\mathbf{i}} P(a_v, \dots, a_v)|_v &\le (r_1 + 1) \cdots (r_n + 1) |\partial_{\mathbf{i}} P|_{*,v} \max\{1, |a_v|_v\}^{r_1 + \cdots + r_n} \\ &\le |P|_{*,v} (4 \max\{1, |\mathbf{a}|_{*,v}\})^{r_1 + \cdots + r_n}. \end{aligned}$$

We have

$$\begin{aligned}|\partial_{\mathbf{i}}P(x_1,\dots,x_n)|_v &\le |P|_{*,v}(8\max\{1,|\mathbf{a}|_{*,v}\})^{r_1+\cdots+r_n}\\ &\quad\times\max_{\mathbf{j}\in I}\{H_{*,\kappa}(x_1)^{j_1}\cdots H_{*,\kappa}(x_n)^{j_n}\}^{-(2+\varepsilon)\lambda_v/n_v}.\end{aligned}$$

We can estimate this last quantity as follows:

$$H_{*,\kappa}(x_1)^{j_1}\cdots H_{*,\kappa}(x_n)^{j_n}=\{H_{*,\kappa}(x_1)^{r_1}\}^{\frac{j_1}{r_1}}\cdots\{H_{*,\kappa}(x_n)^{r_n}\}^{\frac{j_n}{r_n}}\ge D^{\theta-\theta_0}.$$

It follows from above that

$$|\partial_{\mathbf{i}}P(x_1,\dots,x_n)|_v\le\frac{|P|_{*,v}}{D^{(\theta-\theta_0)(2+\varepsilon)\lambda_v/n_v}}(8\max\{1,|\mathbf{a}|_{*,v}\})^{r_1+\cdots+r_n}.$$

Now raising to the n_v power, multiplying over all $v\in S$, and using the fact that $\sum_{v\in S}\lambda_v=1$, we arrive at the desired estimate (6.33).

Further, if setting

$$\mathbf{x}=(x_1,\dots,x_n),\quad \mathbf{r}=(r_1,\dots,r_n),$$

we claim that the index of P with respect to $(\mathbf{x};\mathbf{r})$ satisfies

$$\operatorname{Ind}(P)\ge n\delta. \tag{6.34}$$

Let $\mathbf{i}=(i_1,\dots,i_n)$ be an n-tuple satisfying

$$\frac{i_1}{r_1}+\cdots+\frac{i_n}{r_n}<n\delta.$$

We want to show that $\partial_{\mathbf{i}}P(\mathbf{x})=0$. From (6.33), (6.9) and (6.10), we get

$$\prod_{v\in S}\|\partial_{\mathbf{i}}P(\mathbf{x})\|_v\le\frac{\{32H_*(1,\mathbf{a})\}^{d(r_1+\cdots+r_n)}}{D^{(2+\varepsilon)(n(\frac{1}{2}-\delta)-n\delta)}}.$$

On the other hand, from Lemma 4.16 we obtain

$$H_{*,\kappa}(\partial_{\mathbf{i}}P(\mathbf{x}))\le 4^{d(r_1+\cdots+r_n)}H_{*,\kappa}(P)\prod_{h=1}^{n}H_{*,\kappa}(x_h)^{r_h}.$$

Thus by using (6.10) and (6.31), it follows that

$$H_{*,\kappa}(\partial_{\mathbf{i}}P(\mathbf{x}))\le\{16H_*(1,\mathbf{a})\}^{d(r_1+\cdots+r_n)}D^{n(1+\delta)}.$$

Now Liouville's inequality implies that either the derivative $\partial_{\mathbf{i}}P(\mathbf{x})$ is zero, or else

$$\prod_{v\in S}\min\{1,\|\partial_{\mathbf{i}}P(\mathbf{x})\|_v\}\ge\frac{1}{H_{*,\kappa}(\partial_{\mathbf{i}}P(\mathbf{x}))}.$$

So it suffices to show that our hypotheses contradict that latter. Assuming $\partial_{\mathbf{i}} P(\mathbf{x}) \neq 0$. Liouville's inequality thus yields

$$D^{n\{(1+\varepsilon/2)(1-4\delta)-(1+\delta)\}} \leq \{2^9 H_*(1,\mathbf{a})\}^{d(r_1+\cdots+r_n)}.$$

Since we assumed $\varepsilon < 1$ and $\delta < \frac{\varepsilon}{22}$, we get

$$(1+\varepsilon/2)(1-4\delta) - (1+\delta) = \frac{\varepsilon}{2} - 5\delta - 2\delta\varepsilon > \frac{\varepsilon}{6},$$

and hence

$$\max_{1\leq h\leq n} H_*(x_h)^{r_h} \leq D^{1+\delta} \leq \{2^9 H_*(1,\mathbf{a})\}^{6d(r_1+\cdots+r_n)(1+\delta)/(n\varepsilon)}.$$

Noting that

$$r_1 = \max_{1\leq h\leq n} r_h,$$

we deduce that

$$H_*(x_1) \leq \{2^9 H_*(1,\mathbf{a})\}^{6d(1+\delta)/\varepsilon} < \{2^9 H_*(1,\mathbf{a})\}^{12d/\varepsilon},$$

and obtain the desired contradiction to (6.27), which concludes the proof of claim (6.34).

Finally, we would like to apply Roth's Lemma 6.12. We have verified condition (6.15) with $\eta^{2^{n-1}} = \omega$, so it remains to check condition (6.16). By using the fact

$$\log D = \min_{1\leq h\leq n} \{r_h \log H_*(x_h)\} = r_1 \log H_*(x_1),$$

and applying (6.10), we compute

$$\begin{aligned} \frac{\log |P|_* + 2nr_1}{\log D} &\leq \frac{(r_1+\cdots+r_n)\log(4H_*(1,\mathbf{a})) + 2nr_1}{\log D} \\ &\leq \frac{n\{\log(4H_*(1,\mathbf{a})) + 2\}}{\log H_*(x_1)} \leq \omega, \end{aligned}$$

where the last inequality follows from the choice of x_1 in (6.27). This completes the verification of all of the conditions necessary to apply Lemma 6.12 with

$$\eta = \omega^{2^{-n+1}} = \frac{\delta}{4},$$

so we conclude that the index of P with respect to $(\mathbf{x};\mathbf{r})$ satisfies

$$\mathrm{Ind}(P) \leq 2n\eta = \frac{n\delta}{2}. \tag{6.35}$$

We now observe that the lower and upper bounds for the index of P given in (6.34) and (6.35) contradict each other. This completes the proof of Theorem 6.3 that (6.4) has only finitely many solutions. Then using the reduction Proposition 6.4, we conclude that Roth's Theorem 6.2 is also true.

6.6 Formulation of Roth's theorem

6.6.1 A generalization

S. Lang [144] noted that if a_v, a'_v are two distinct elements of $\bar{\mathbb{Q}}$ for some v, and if x approximates a_v, then x stays away from a'_v. As x approaches a_v, its distance from a'_v approaches the distance between a_v and a'_v. Hence it would add no greater generality to the statement if we took a product over several a_v for each v. Based on this observation, we have the following fact:

Theorem 6.13. *Let S be a finite subset of M_κ. For each $v \in S$, let $P_v(X)$ be a polynomial in $\kappa[X]$ (one variable) and assume that the multiplicity of their roots is at most r for some integer $r > 0$. Take $\varepsilon > 0$. Then there are only finitely many $x \in \kappa$ such that*

$$\prod_{v\in S} \min\{1, \|P_v(x)\|_v\} < \frac{1}{H_{*,\kappa}(x)^{r(2+\varepsilon)}}. \tag{6.36}$$

Proof. We may assume that P_v has leading coefficient 1 for each $v \in S$, and say

$$P_v(X) = \prod_{j=1}^{q_v} (X - a_{vj})^{r_{vj}}$$

is a factorization in $\bar{\mathbb{Q}}$. The expression on the left-hand side of our inequality is greater or equal to

$$\prod_{v\in S} \prod_{j=1}^{q_v} \min\{1, \|x - a_{vj}\|_v\}^{r_{vj}},$$

which is itself greater or equal to the expression obtained by replacing r_{vj} by r for all v and j. Now we are in the situation of Theorem 6.2, taking into account the above remark following it, the solutions x of the inequality

$$\prod_{v\in S} \prod_{j=1}^{q_v} \min\{1, \|x - a_{vj}\|_v\}^{r} < \frac{1}{H_{*,\kappa}(x)^{r(2+\varepsilon)}} \tag{6.37}$$

are only finite in number, hence the same is true for the solutions of original inequality. □

Particularly, take $r = 1$; $q_v = q$, $a_{vj} = a_j$ for each $v \in S$; and hence

$$P_v(X) = P(X) = \prod_{j=1}^{q} (X - a_j).$$

The inequality (6.37) implies that all but finitely many $x \in \kappa$ satisfy

$$\sum_{v\in S} \sum_{j=1}^{q} \log^+ \frac{1}{\|\|x - a_j\|\|_v} \le (2 + \varepsilon)h_*(x) + O(1). \tag{6.38}$$

If we assume $M_\kappa^\infty \subseteq S$, the inequality (6.38) can be rewritten into the following form:

$$\sum_{j=1}^{q} m(x, a_j) \leq (2+\varepsilon)h_*(x) + O(1), \tag{6.39}$$

or equivalently

$$(q-2)h(x) \leq \sum_{j=1}^{q} N(x, a_j) + \varepsilon h(x) + O(1). \tag{6.40}$$

6.6.2 Approach infinity

S. Lang [144] observed that there is no reason not to let x approach infinity. For example, we can change Theorem 6.13 into the following form:

Theorem 6.14. *Let κ be a number field, let $S \subset M_\kappa$ be a finite subset of absolute values on κ, and assume that each absolute value in S has been extended in some way to $\bar{\kappa}$. Let $a_1, \ldots, a_q$ be distinct elements in $\bar{\kappa}$. Let ε be a positive constant. Then there are only finitely many $x \in \kappa$ such that*

$$\prod_{v\in S}\left(\min\left\{1, \frac{1}{\|x\|_v}\right\}\prod_{j=1}^{q}\min\{1, \|x-a_j\|_v\}\right) < \frac{1}{H_{*,\kappa}(x)^{2+\varepsilon}}. \tag{6.41}$$

Proof. We show that this version of the theorem can be reduced to the other by making a linear transformation

$$\sigma(x) = \frac{ax+b}{cx+d}$$

such that the transform of x approaches elements at a finite distance for all $v \in S$. It is trivially checked that if σ is a non-singular transformation with coefficients in κ, then $H_{*,\kappa}(\sigma(x))$ is equivalent to $H_{*,\kappa}(x)$, i.e., each is less than a constant multiple of the other.

Now we choose the linear transformation as follows

$$\sigma(x) = \frac{ax+1}{x+d} = \begin{cases} \frac{1}{x}, & \text{if } 0 \notin \{a_1, \ldots, a_q\}, \\ \frac{x+1}{x-1}, & \text{if } 0 \in \{a_1, \ldots, a_q\}. \end{cases}$$

Then (6.41) is equivalent to

$$\prod_{v\in S}\left(\min\left\{1, \left\|\frac{x+d}{ax+1}\right\|_v\right\}\prod_{j=1}^{q}\min\left\{1, \left\|\frac{ax+1}{x+d} - a_j\right\|_v\right\}\right) < \frac{1}{H_{*,\kappa}(\sigma(x))^{2+\varepsilon}}. \tag{6.42}$$

Without loss of generality, we only consider the case $\sigma(x) = x^{-1}$. Now the inequality (6.42) becomes

$$\prod_{v\in S}\left(\min\{1,\|x\|_v\}\prod_{j=1}^{q}\min\left\{1,\frac{\|x-b_j\|_v}{\|b_jx\|_v}\right\}\right) < \frac{1}{H_{*,\kappa}(x)^{2+\varepsilon}} \tag{6.43}$$

since $H_{*,\kappa}(x^{-1}) = H_{*,\kappa}(x)$, where $b_j = a_j^{-1}$. We claim that for each pair (v,j) with $v \in S$ and $j \in \{1,\dots,q\}$, there exists a constant $c_{vj} \geq 1$ satisfying

$$\min\left\{1,\frac{\|x-b_j\|_v}{\|b_jx\|_v}\right\} \leq c_{vj}\min\{1,\|x-b_j\|_v\}. \tag{6.44}$$

In fact, for the case $v \in S - M_\kappa^\infty$, we have

$$\frac{\|x-b_j\|_v}{\|b_jx\|_v} \leq c_{vj}\|x-b_j\|_v$$

when $\|x\|_v \geq \min\{1,\|b_j\|_v\} = c_{vj}^{-1/2}$, and so (6.44) holds. If $\|x\|_v < c_{vj}^{-1/2}$, then

$$\frac{\|x-b_j\|_v}{\|b_jx\|_v} = \frac{1}{\|x\|_v} \geq 1,$$

and hence (6.44) is trivial since

$$c_{vj}\min\{1,\|x-b_j\|_v\} = c_{vj}\min\{1,\|b_j\|_v\} \geq 1.$$

If $v \in S \cap M_\kappa^\infty$, we have

$$\frac{\|x-b_j\|_v}{\|b_jx\|_v} \leq c_{vj}\|x-b_j\|_v$$

when $\|x\|_v \geq 2^{-n_v}\min\{1,\|b_j\|_v\} = c_{vj}^{-1/2}$, and so (6.44) holds. If $\|x\|_v < c_{vj}^{-1/2}$, then

$$\frac{\|x-b_j\|_v}{\|b_jx\|_v} \geq \frac{||b_j|_v - |x|_v|^{n_v}}{\|b_jx\|_v} \geq \frac{1}{2^{n_v}\|x\|_v} \geq 1,$$

and hence (6.44) follows from

$$c_{vj}\min\{1,\|x-b_j\|_v\} \geq c_{vj}\min\left\{1,2^{-n_v}\|b_j\|_v\right\} \geq 1.$$

Therefore, for each $v \in S$ we obtain an inequality

$$\min\{1,\|x\|_v\}\prod_{j=1}^{q}\min\left\{1,\frac{\|x-b_j\|_v}{\|b_jx\|_v}\right\} \leq c_v\prod_{j=0}^{q}\min\{1,\|x-b_j\|_v\}, \tag{6.45}$$

where $c_v = c_{v1}\cdots c_{vq}$, $b_0 = 0$. Hence (6.43) follows from (6.45) and Theorem 6.13.□

Next we assume $M_\kappa^\infty \subseteq S$. Similar to the arguments of (6.40), we can prove that all but finitely many $x \in \kappa$ satisfy

$$(q-1)h(x) \le \sum_{j=0}^{q} N(x, a_j) + \varepsilon h(x) + O(1), \tag{6.46}$$

where $a_0 = \infty$. Without loss of generality, we may assume $a_j \in \kappa$ for $j \ge 1$. By using the formula (2.17), we find

$$N(x, a_j) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S^c(x-a_j)} \operatorname{ord}_v(x - a_j) \log \mathcal{N}(\mathfrak{p}_v) + O(1) \tag{6.47}$$

for each $j = 1, \ldots, q$, and

$$N(x, \infty) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S^c(x^{-1})} \operatorname{ord}_v(x^{-1}) \log \mathcal{N}(\mathfrak{p}_v) + O(1), \tag{6.48}$$

where

$$S^c(y) = \{v \in M_\kappa - S \mid \operatorname{ord}_v(y) > 0\}.$$

Define

$$\overline{N}(x, a_j) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S^c(x-a_j)} \log \mathcal{N}(\mathfrak{p}_v) \tag{6.49}$$

and

$$\overline{N}(x, \infty) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S^c(x^{-1})} \log \mathcal{N}(\mathfrak{p}_v). \tag{6.50}$$

It was conjectured that the inequality (6.46) could be strengthened as follows:

Conjecture 6.15. *Let $a_0, a_1, \ldots, a_q$ be distinct elements in $\bar{\kappa} \cup \{\infty\}$. Let ε be a positive constant. All but finitely many $x \in \kappa$ satisfy the inequality*

$$(q-1)h(x) \le \sum_{j=0}^{q} \overline{N}(x, a_j) + \varepsilon h(x) + O(1). \tag{6.51}$$

6.6.3 Ramification term

We consider the following rational function

$$Q(X) = \sum_{j=1}^{q} \frac{1}{X - a_j}.$$

Set

$$\delta_v = \min_{1 \le i < j \le q} |a_i - a_j|_v,$$

$$E_{vj} = \left\{ x \in \kappa \;\middle|\; |x - a_j|_v < \frac{\delta_v}{2q} \right\}.$$

When $i \neq j$, $x \in E_{vj}$, we have

$$|x - a_i|_v \geq |a_i - a_j|_v - |x - a_j|_v \geq \delta_v \left(1 - \frac{1}{2q}\right) \geq \frac{\delta_v}{2q}.$$

Since

$$Q(x) = \frac{1}{x - a_j} \left\{ 1 + \sum_{i \neq j} \frac{x - a_j}{x - a_i} \right\},$$

we find

$$|Q(x)|_v > \frac{1}{|x - a_j|_v} \left\{ 1 - (q-1) \frac{\frac{\delta_v}{2q}}{\delta_v \left(1 - \frac{1}{2q}\right)} \right\} > \frac{1}{2|x - a_j|_v},$$

and so

$$\begin{aligned} \log^+ \|Q(x\|_v &> \log^+ \frac{1}{\|x - a_j\|_v} - n_v \log 2 \\ &\geq \sum_{i=1}^{q} \log^+ \frac{1}{\|x - a_i\|_v} - q n_v \log^+ \frac{2q}{\delta_v} - n_v \log 2. \end{aligned}$$

Obviously, this inequality also is true if $x \notin \cup_i E_{vi}$. Thus we obtain

$$m(Q(x), \infty) \geq \sum_{j=1}^{q} m(x, a_j) - C_S,$$

where

$$C_S = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S} \left(q n_v \log^+ \frac{2q}{\delta_v} + n_v \log 2 \right).$$

On the other hand, for some $x' \in \kappa_*$, we have

$$\begin{aligned} m(Q(x), \infty) &\leq m\left(x' Q(x), \infty\right) + m\left(x', 0\right) \\ &\leq m\left(x' Q(x), \infty\right) + h(x') - N\left(x', 0\right) + O(1). \end{aligned}$$

Note that

$$\begin{aligned} h(x') &= m(x', \infty) + N(x', \infty) \\ &\leq m(x - a_1, \infty) + N(x', \infty) + m\left(\frac{x'}{x - a_1}, \infty\right) + O(1) \\ &= h(x) + N(x', \infty) - N(x, \infty) + m\left(\frac{x'}{x - a_1}, \infty\right) + O(1). \end{aligned}$$

Therefore

$$m(x,\infty)+\sum_{j=1}^{q}m(x,a_j)\le 2h(x)-N_{x'}(x)+S_{x'}(x)+O(1), \tag{6.52}$$

where

$$N_{x'}(x)=2N(x,\infty)-N(x',\infty)+N(x',0),$$
$$S_{x'}(x)=m\left(\frac{x'}{x-a_1},\infty\right)+m\left(x'Q(x),\infty\right).$$

According to the proof of Theorem 6.5, it is easy to show that if (6.52) is true for all algebraic integers a_j, then it is true for all algebraic numbers a_j.

Now we choose the element $x'\in\kappa$. Without loss of generality, we will assume that all a_j are algebraic integers. Write

$$(x)=\mathfrak{P}_1^{t_1}\cdots\mathfrak{P}_l^{t_l}\mathfrak{h}^{-1},\quad \mathfrak{h}=\mathfrak{Q}_1^{u_1}\cdots\mathfrak{Q}_h^{u_h}\mathfrak{Q}_{h+1}^{u_{h+1}}\cdots\mathfrak{Q}_{h+g}^{u_{h+g}},$$

where $t_i,\ u_j$ are positive integers, and

$$\mathfrak{Q}_i\in M_\kappa-S\ (i=1,\dots,h);\quad \mathfrak{Q}_{h+j}\in S\ \ (j=1,\dots,g).$$

Similarly, we can write

$$(x-a_j)=\mathfrak{h}^{-1}\mathfrak{p}_{m_{j-1}+1}^{r_{m_{j-1}+1}}\cdots\mathfrak{p}_{m_j}^{r_{m_j}}\mathfrak{q}_{n_{j-1}+1}^{s_{n_{j-1}+1}}\cdots\mathfrak{q}_{n_j}^{s_{n_j}},$$

where r_i, s_j are positive integers, $m_0=n_0=0$, and

$$\mathfrak{p}_i\in M_\kappa-S\ (i=1,\dots,m_q);\quad \mathfrak{q}_j\in S\ (j=1,\dots,n_q).$$

First of all, we assume that $\mathfrak{p}_1,\dots,\mathfrak{p}_{m_q}$ are distinct. We write

$$\mathfrak{a}_0=\prod_{i=1}^{m_q}\mathfrak{p}_i^{r_i-1},$$

and further define ideals $\mathfrak{d}_i$ by

$$\mathfrak{p}_i^{r_i}\mathfrak{d}_i=\mathfrak{a}_0\mathfrak{p}_1\cdots\mathfrak{p}_{m_q},\ \ i=1,2,\dots,m_q,$$

so that $\mathfrak{d}_i$ is relatively prime to $\mathfrak{p}_i$. Since these $\mathfrak{d}_i$ in their totality are relatively prime, there are elements $\delta_i\in\mathfrak{d}_i$ satisfying

$$\delta_1+\delta_2+\cdots+\delta_{m_q}=1.$$

Since $\mathfrak{d}_i|\delta_i$, hence $\mathfrak{p}_j|\delta_i$ $(j\ne i)$. Consequently, $\mathfrak{p}_i\nmid\delta_i$ since $\mathfrak{p}_i\nmid(1)$.

We now determine elements α_i such that

$$\mathfrak{p}_i^{r_i-1}|\alpha_i,\quad \mathfrak{p}_i^{r_i}\nmid\alpha_i,\ \ i=1,\dots,m_q$$

which is obviously always possible since for this to happen α_i need only be an element from $\mathfrak{p}_i^{r_i-1}$ which does not occur in $\mathfrak{p}_i^{r_i}$. Then the element

$$x_0 = \alpha_1\delta_1 + \alpha_2\delta_2 + \cdots + \alpha_{m_q}\delta_{m_q}$$

has the property $\mathfrak{a}_0 \mid x_0$. For each of the prime ideals $\mathfrak{p}_i$ occurs in $m_q - 1$ summands at least to the power $\mathfrak{p}_i^{r_i}$; however, it occurs precisely to the power $\mathfrak{p}_i^{r_i-1}$ in the i-th summand; consequently x_0 is divisible by precisely the $(r_i - 1)$-th power of $\mathfrak{p}_i$, but no higher power.

If $\mathfrak{p}_1, \ldots, \mathfrak{p}_{m_q}$ are not distinct, say $\mathfrak{p}_1 = \mathfrak{p}_2$, but $\mathfrak{p}_2, \ldots, \mathfrak{p}_{m_q}$ are distinct, now $\mathfrak{d}_2$ is replaced by

$$\mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\mathfrak{d}_2 = \mathfrak{a}_0\mathfrak{p}_1 \cdots \mathfrak{p}_{m_q}$$

and determine the element α_2 such that

$$\mathfrak{p}_1^{r_1+r_2-2} | \alpha_2, \quad \mathfrak{p}_1^{r_1+r_2-1} \nmid \alpha_2.$$

Then the element x_0 is replaced by

$$x_0 = \alpha_2\delta_2 + \alpha_3\delta_3 + \cdots + \alpha_{m_q}\delta_{m_q}.$$

Similarly, if we define

$$\mathfrak{a}_\infty = \mathfrak{Q}_1^{u_1+1} \cdots \mathfrak{Q}_h^{u_h+1},$$

then we can find an element x_∞ such that when $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_h$ are distinct, each of the prime ideals $\mathfrak{Q}_i$ occurs in $h - 1$ summands at least to the power $\mathfrak{Q}_i^{u_i+2}$; however, it occurs precisely to the power $\mathfrak{Q}_i^{u_i+1}$ in the i-th summand; consequently x_∞ is divisible by precisely the $(u_i + 1)$-th power of $\mathfrak{Q}_i$, but no higher power.

Finally, we take $x' \in \kappa_*$ satisfying

$$x' = \frac{x_0}{x_\infty}.$$

Thus we have

$$(q-1)h(x) \leq \sum_{j=0}^{q} \overline{N}(x, a_j) + S_{x'}(x) + O(1), \tag{6.53}$$

where $a_0 = \infty$.

Problem 6.16. Let $a_0, a_1, \ldots, a_q$ be distinct elements in $\bar{\kappa} \cup \{\infty\}$, which define $Q(X)$. Let ε be a positive constant. Are there $x' \in \kappa$ associated to all but finitely many $x \in \kappa$ satisfying the inequality

$$S_{x'}(x) \leq \varepsilon h(x) + O(1)? \tag{6.54}$$

We can simply construct x' on some extension field of κ by using Theorem 2.32, which means that there exists a number field $K \supseteq \kappa$ such that for each ideal $\mathfrak{a}$ in the ring of integers $\mathcal{O}_\kappa$ of κ, we have

(I) $\mathcal{O}_K\mathfrak{a}$ is a principal ideal;

(II) $(\mathcal{O}_K\mathfrak{a}) \cap \mathcal{O}_\kappa = \mathfrak{a}$.

Thus there exist x_0, $x_\infty \in \mathcal{O}_K$ such that

$$(x_0) = \mathcal{O}_K\mathfrak{a}_0,\ (x_\infty) = \mathcal{O}_K\mathfrak{a}_\infty,$$

and

$$(\mathcal{O}_K\mathfrak{a}_0) \cap \mathcal{O}_\kappa = \mathfrak{a}_0, \quad (\mathcal{O}_K\mathfrak{a}_\infty) \cap \mathcal{O}_\kappa = \mathfrak{a}_\infty.$$

Therefore we get $x' = x_0/x_\infty \in K$.

6.6.4 Roth's theorem and abc-conjecture

Conjecture 6.15 implies the abc-conjecture. In fact, taking an abc-point $y \in \mathbb{P}^2(\kappa)$ with a reduced representation $(a, b, c) \in \mathcal{O}_\kappa^3$ and applying (6.51) to $x = a/c$, we obtain

$$h\left(\frac{a}{c}\right) \le \overline{N}\left(\frac{a}{c}, 0\right) + \overline{N}\left(\frac{a}{c}, -1\right) + \overline{N}\left(\frac{a}{c}, \infty\right) + \varepsilon h\left(\frac{a}{c}\right) + O(1). \tag{6.55}$$

Since $a + b + c = 0$, and the elements a, b, c are relatively prime, we obtain

$$\begin{aligned}
\overline{N}\left(\frac{a}{c}, 0\right) &= \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S^c(a)} \log \mathcal{N}(\mathfrak{p}_v), \\
\overline{N}\left(\frac{a}{c}, -1\right) &= \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S^c(b)} \log \mathcal{N}(\mathfrak{p}_v), \\
\overline{N}\left(\frac{a}{c}, \infty\right) &= \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S^c(c)} \log \mathcal{N}(\mathfrak{p}_v).
\end{aligned}$$

Thus (6.55) becomes

$$h\left(\frac{a}{c}\right) \le \overline{N}(y, E) + \varepsilon h\left(\frac{a}{c}\right) + O(1). \tag{6.56}$$

Similarly, we can obtain

$$h\left(\frac{b}{c}\right) \le \overline{N}(y, E) + \varepsilon h\left(\frac{b}{c}\right) + O(1). \tag{6.57}$$

It is easy to show that

$$h(y) = \max\left\{h\left(\frac{a}{c}\right), h\left(\frac{b}{c}\right)\right\} + O(1).$$

Combining (6.56) and (6.57), we finally obtain

$$h(y) \le \overline{N}(y, E) + \varepsilon h(y) + O(1), \tag{6.58}$$

and so the abc-conjecture follows.

Conversely, for $x \in \kappa_*$, applying the abc-conjecture to $y = [x, -1-x, 1]$ and noting that

$$h(y) = h(x) + O(1),$$

it is easy to find

$$h\,(x) \leq \overline{N}(x, 0) + \overline{N}(x, -1) + \overline{N}(x, \infty) + \varepsilon h\,(x) + O(1). \tag{6.59}$$

Hence the inequality in the abc-conjecture is equivalent to (6.59).

Suppose that $F(x, y) \in \mathbb{Z}[x, y]$ is a homogenous polynomial of degree d with distinct linear factors over $\mathbb{C}$. Then $F(t, 1)$ is a polynomial of degree $\geq d - 1$, without repeated roots, and

$$F(x, y) = y^d F\left(\frac{x}{y}, 1\right).$$

For any coprime integers x and y, Roth's theorem yields

$$|F(x, y)| \gg |y|^d \prod_{F(\alpha,1)=0} \left|\alpha - \frac{x}{y}\right| \gg |y|^{d-2-\varepsilon}, \tag{6.60}$$

except at most finitely many rational numbers $\frac{x}{y}$. This statement is actually equivalent to Roth's theorem.

The abc-conjecture implies something that is somewhat stronger than Roth's theorem: For any coprime integers x and y,

$$r(F(x, y)) \gg \max\{|x|, |y|\}^{d-2-\varepsilon}. \tag{6.61}$$

Note that by taking

$$F(x, y) = xy(x + y),$$

the original abc-conjecture is recovered. Thus the conjecture (6.61) is equivalent to the abc-conjecture, although it appears far stronger. One sketchy proof of (6.61) following from the abc-conjecture is referred to [79] (See also [284]).

Chapter 7

Subspace theorems

Schmidt's subspace theorem is just an analogue of the second main theorem due to H. Cartan for holomorphic curves into projective spaces. The Shiffman's conjecture on hypersurface targets in value distribution theory corresponds to a subspace theorem for homogeneous polynomial forms in Diophantine approximation.

7.1 *p*-adic Minkowski's second theorem

Let κ be a field with a non-Archimedean absolute value $|\cdot|$. Let K be the perfect extension of κ with respect to this absolute value. According to Mahler [162], a function $f(\mathbf{x})$ of the variable point $\mathbf{x}$ in K^n is called a *general distance function* if it has the properties:

(N1) $f(\mathbf{x}) \geq 0$;

(N2) $f(a\mathbf{x}) = |a|f(\mathbf{x})$ for all $a \in K$, hence $f(0) = 0$;

(N3) $f(\mathbf{x} \pm \mathbf{y}) \leq \max\{f(\mathbf{x}), f(\mathbf{y})\}$;

it is called a *special distance function* or simply a *distance function* if instead of (N1) it satisfies the stronger condition

(N1′) $f(\mathbf{x}) > 0$ for $\mathbf{x} \neq 0$.

If r is a positive number, then the set $C(r)$ of all points $\mathbf{x}$ with $f(\mathbf{x}) \leq r$ is called a *convex set*; if $f(\mathbf{x})$ is a special distance function, then it is called a *convex body*. It is clear from the definition of $f(\mathbf{x})$ that a convex set $C(r)$ contains the original 0, and that with $\mathbf{x}$ and $\mathbf{y}$ also $a\mathbf{x} + b\mathbf{y}$ belong to it, if $a, b \in K$ with $|a| \leq 1, |b| \leq 1$. Further, if

$$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$$

are the n unit vectors of the coordinate system, then

$$\mathbf{x} = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n,$$

and therefore

$$f(\mathbf{x}) \leq \Gamma \max_{1 \leq i \leq n} |x_i| = \Gamma |\mathbf{x}|, \tag{7.1}$$

where Γ is the positive constant

$$\Gamma = \max_{1 \leq i \leq n} \{f(e_i)\}.$$

Proposition 7.1. *For a special distance function $f(\mathbf{x})$, there is a positive constant γ, such that $f(\mathbf{x}) \geq \gamma|\mathbf{x}|$ holds for all points $\mathbf{x}$ in K^n.*

Next we assume that κ is the field $\mathbf{F}(z)$ of all rational functions in an indeterminant z with coefficients in an arbitrary field $\mathbf{F}$. The special absolute value $|\cdot|$ of κ is defined by

$$|x| = \begin{cases} 0, & \text{if } x = 0, \\ e^f, & \text{if } x \neq 0 \text{ is of order } f, \end{cases}$$

where the order f of a rational function x in κ is the degree of its numerator minus the degree of its denominator. Let K be the perfect extension of κ with respect to this absolute value, i.e., the field of all formal Laurent series

$$x = a_f z^f + a_{f-1} z^{f-1} + a_{f-2} z^{f-2} + \cdots$$

with coefficients in $\mathbf{F}$; if a_f is the non-vanishing coefficient with highest index ($\gtreqless 0$), then $|x| = e^f$. Let Λ be the set of all *lattice points* in K^n, i.e. that of all points with coordinates in $\mathbf{F}[z]$.

Let $f(\mathbf{x})$ be a special distance function, $C(e^t)$ the convex body $f(\mathbf{x}) \leq e^t$, where t is an arbitrary integer. It is obvious that the set $\Lambda \cap C(e^t)$ forms a $\mathbf{F}$-module. In the special case $f(\mathbf{x}) = |\mathbf{x}|$, this set has exactly

$$n_0(t) = n(t+1)$$

$\mathbf{F}$-independent elements. Hence, by (7.1) and Proposition 7.1, $\Lambda \cap C(e^t)$ has always a finite dimension $n(t)$, and this dimension is certainly positive for large t. Obviously,

$$n_0(t+1) = n_0(t) + n. \tag{7.2}$$

Suppose that t is already so large that $e^{t+1} \geq \Gamma$. Then a lattice point in $C(e^{t+1})$ can be written as

$$\mathbf{x} = \mathbf{x}^{(0)} + z\mathbf{x}^{(1)},$$

where $\mathbf{x}^{(0)}$ and $\mathbf{x}^{(1)}$ are again lattice points, and the coordinates of $\mathbf{x}^{(0)}$ lie in $\mathbf{F}$, i.e.,

$$\left|\mathbf{x}^{(0)}\right| \leq 1, \quad f\left(\mathbf{x}^{(0)}\right) \leq \Gamma \leq e^{t+1}.$$

Hence

$$f\left(z\mathbf{x}^{(1)}\right) \leq \max\left\{f(\mathbf{x}), f\left(\mathbf{x}^{(0)}\right)\right\} \leq e^{t+1}, \quad f\left(\mathbf{x}^{(1)}\right) \leq e^t,$$

so that $\mathbf{x}^{(1)} \in \Lambda \cap C(e^t)$. Conversely, if $\mathbf{x}^{(1)} \in \Lambda \cap C(e^t)$, then

$$f\left(\mathbf{x}\right) \leq \max\left\{f\left(z\mathbf{x}^{(1)}\right), f\left(\mathbf{x}^{(0)}\right)\right\} \leq e^{t+1}.$$

Now the two vectors $\mathbf{x}^{(0)}$ and $z\mathbf{x}^{(1)}$, where $\mathbf{x}^{(0)}$ and $\mathbf{x}^{(1)}$ are lattice points and $|\mathbf{x}^{(0)}| \leq 1$, are $\mathbf{F}$-independent, and the $\mathbf{x}^{(0)}$ form a $\mathbf{F}$-module of dimension n. Hence

$$n(t+1) = n(t) + n. \tag{7.3}$$

The two equation (7.2) and (7.3) show that for large t, the function $n(t) - n_0(t)$ of t is independent of t. Hence the limit

$$V = \lim_{t\to\infty} e^{n(t)-n_0(t)} \tag{7.4}$$

exists; it is called the *volume of the convex body* $C(1)$. In particular, if $f(\mathbf{x}) = |\mathbf{x}|$, then $V = 1$.

Proposition 7.2 ([162]). *Let* $\Omega = (a_{hk})_{1\le h,k\le n}$ *be a matrix with elements in* K *such that* $\det(\Omega) \neq 0$. *The linear transformation* $\mathbf{y} = \Omega\mathbf{x}$ *changes* $f(\mathbf{x})$ *into the new distance function*

$$g(\mathbf{y}) = f(\mathbf{x}) = f\left(\Omega^{-1}\mathbf{y}\right);$$

let $C_g(e^t)$ *be the corresponding convex body* $g(\mathbf{y}) \le e^t$, *and* V_g *the volume of* $C_g(1)$. *Then*

$$V_g = |\det(\Omega)|V.$$

Proof. We denote by $n_g(t)$ the dimension of the $\mathbf{F}$-module $\Lambda \cap C_g(e^t)$ of all lattice points in $C_g(e^t)$, and prove the statement in a number of steps.

1. The elements of Ω lie in $\mathbf{F}[z]$, and $\det(\Omega)$ belongs to $\mathbf{F}$.

The formulae $\mathbf{y} = \Omega\mathbf{x}$, $\mathbf{x} = \Omega^{-1}\mathbf{y}$ establish a $(1,1)$-correspondence between the elements $\mathbf{x}$ of $\Lambda \cap C(e^t)$ and $\mathbf{y}$ of $\Lambda \cap C_g(e^t)$. Obviously, this correspondence changes every linear relation

$$\alpha_1\mathbf{x}^{(1)} + \cdots + \alpha_r\mathbf{x}^{(r)} = 0$$

with coefficients in $\mathbf{F}$ into the identical relation in the $\mathbf{y}'$s, and vice versa; therefore $\mathbf{F}$-independent elements of $\Lambda \cap C(e^t)$ or $\Lambda \cap C_g(e^t)$ are transformed into $\mathbf{F}$-independent members of the other module. Hence both modules have the same dimension: $n(t) = n_g(t)$.

2. Ω is a triangle matrix

$$\Omega = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

with elements in $\mathbf{F}[z]$ and determinant $\det(\Omega) = a_{11}a_{22}\cdots a_{nn} \neq 0$.

The equation $\mathbf{y} = \Omega\mathbf{x}$ denotes that for $i = 1, \ldots, n$,

$$y_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{ii}x_i;$$

hence every lattice point $\mathbf{y}$ can be written as

$$\mathbf{y} = \Omega\mathbf{x}^* + \mathbf{y}^*,$$

where $\mathbf{x}^*$ and $\mathbf{y}^*$ are again lattice points and $\mathbf{y}^* = (y_1^*, \ldots, y_n^*)$ satisfies the inequalities

$$|y_i^*| < |a_{ii}|, \ \ i = 1, 2, \ldots, n.$$

Therefore $|\mathbf{y}^*| \leq c_1$, i.e. $g(\mathbf{y}^*) \leq c_1\Gamma_g$, where c_1 is a positive constant depending only on Ω, and Γ_g is the constant in (7.1) belonging to $g(\mathbf{y})$. The set of all vectors $\mathbf{y}^*$ forms a $\mathbf{F}$-module $\mathfrak{m}^*$ of dimension d, where

$$e^d = |a_{11}||a_{22}| \cdots |a_{nn}| = |\det(\Omega)|.$$

Let t be so large that $e^t \geq c_1\Gamma_g$. Then for $\mathbf{x}^* \in \Lambda \cap C(e^t)$,

$$g(\mathbf{y}) = f\left(\Omega^{-1}\mathbf{y}\right) = f\left(\mathbf{x}^* + \Omega^{-1}\mathbf{y}^*\right) \leq \max\{f(\mathbf{x}^*), g(\mathbf{y}^*)\} \leq e^t,$$

and conversely for $\mathbf{y} \in \Lambda \cap C_g(e^t)$,

$$f\left(\mathbf{x}^* + \Omega^{-1}\mathbf{y}^*\right) = g(\mathbf{y}) \leq e^t,$$

that is,

$$f(\mathbf{x}^*) \leq \max\{f\left(\mathbf{x}^* + \Omega^{-1}\mathbf{y}^*\right), g(\mathbf{y}^*)\} \leq e^t.$$

There is therefore a $(1, 1)$-correspondence between the elements $\mathbf{y}$ of $\Lambda \cap C_g(e^t)$ and the pairs $(\mathbf{x}^*, \mathbf{y}^*)$ of one element $\mathbf{x}^*$ of $\Lambda \cap C(e^t)$ and one element $\mathbf{y}^*$ in $\mathfrak{m}^*$. Hence $n_g(t) = n(t) + d$.

3. The elements of Ω belong to $\mathbf{F}[z]$.

The result follows immediately from the two previous steps, since Ω can be written as $\Omega = \Omega_1\Omega_2$, where the two factors are of the classes 1 and 2.

4. The elements of Ω lie in $\mathbf{F}(z)$.

Now $\Omega = \Omega_a\Omega_b^{-1}$, where Ω_a and Ω_b are of the class 3, so that the statement follows at once.

5. Ω has elements in K such that

$$|\det(\Omega)| = 1, \ \ |a_{hk}| \leq 1 \ \ (h, k = 1, 2, \ldots, n).$$

Then the same inequalities hold for the inverse matrix Ω^{-1}, so that for every point $\mathbf{x}$

$$|\Omega\mathbf{x}| \leq |\mathbf{x}| = |\Omega^{-1}\Omega\mathbf{x}| \leq |\Omega\mathbf{x}|,$$

and therefore

$$|\mathbf{x}| = |\Omega\mathbf{x}| = |\Omega^{-1}\mathbf{x}|.$$

Now to every lattice point $\mathbf{x}$ there is a second lattice point $\mathbf{y}$ such that with a suitable point $\mathbf{y}^*$

$$\Omega\mathbf{x} = \mathbf{y} + \mathbf{y}^*, \quad |\mathbf{y}^*| < 1;$$

then conversely,

$$\Omega^{-1}\mathbf{y} = \mathbf{x} + \mathbf{x}^*, \quad |\mathbf{x}^*| < 1,$$

and

$$\mathbf{x}^* = -\Omega^{-1}\mathbf{y}^*, \quad \Omega\mathbf{x}^* = -\mathbf{y}^*.$$

The relation between $\mathbf{x}$ and $\mathbf{y}$ is therefore a $(1,1)$-correspondence which obviously leaves invariant the property of $\mathbf{F}$-independence. Suppose that $e^t \geq \Gamma$. Then for $\mathbf{x} \in \Lambda \cap C(e^t)$,

$$f(\mathbf{x}^*) < \Gamma \leq e^t,$$

and therefore

$$g(\mathbf{y}) = f\left(\Omega^{-1}\mathbf{y}\right) = f(\mathbf{x} + \mathbf{x}^*) \leq \max\{f(\mathbf{x}), f(\mathbf{x}^*)\} \leq e^t,$$

so that $\mathbf{y} \in \Lambda \cap C_g(e^t)$; conversely, if $\mathbf{y} \in \Lambda \cap C_g(e^t)$, then $\mathbf{x} \in \Lambda \cap C(e^t)$. Hence $n_g(t) = n(t)$.

6. Finally, let Ω have elements in K.

Then it can be split into $\Omega = \Omega_4 + \Omega^*$, where Ω_4 is of the class 4, while the elements of Ω^* lie in K and have so small values that $\Omega_5 = \Omega_4^{-1}\Omega$ is of the class 5. Then the result follows at once, since $\Omega = \Omega_4\Omega_5$. □

Theorem 7.3 ([162]). *To the distance function $f(\mathbf{x})$, there exist n K-independent lattice points*

$$\mathbf{x}^{(j)} = \left(x_1^{(j)}, \ldots, x_n^{(j)}\right), \quad j = 1, 2, \ldots, n,$$

such that $f\left(\mathbf{x}^{(1)}\right) = \lambda_1$ is the minimum of $f(\mathbf{x})$ in all lattice points $\mathbf{x} \neq 0$, $f\left(\mathbf{x}^{(2)}\right) = \lambda_2$ is the minimum of $f(\mathbf{x})$ in all lattice points $\mathbf{x}$ which are K-independent of $\mathbf{x}^{(1)}$, etc., and finally, $f\left(\mathbf{x}^{(n)}\right) = \lambda_n$ is the minimum of $f(\mathbf{x})$ in all lattice points $\mathbf{x}$ which are K-independent of $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(n-1)}$. The numbers $\lambda_1, \ldots, \lambda_n$ are called the n successive minima of $f(\mathbf{x})$. By this construction, the determinant $\det\left(x_i^{(j)}\right)$ lies in $\mathbf{F}[z]$ and does not vanish; further

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n, \tag{7.5}$$

$$\left|\det\left(x_i^{(j)}\right)\right| = 1, \tag{7.6}$$

$$\lambda_1\lambda_2\cdots\lambda_n = \frac{1}{V}; \tag{7.7}$$

where V is the volume of $C(1)$. Thus, in particular, $\det\left(x_i^{(j)}\right)$ is an element of $\mathbf{F}$, and may obviously be taken as equal to 1.

Proof. Every point $\mathbf{x}$ in K^n can be written as

$$\mathbf{x} = y_1\mathbf{x}^{(1)} + \cdots + y_n\mathbf{x}^{(n)},$$

where $y_i \in K$ for each $i = 1, \ldots, n$. Then the coordinates x_h of $\mathbf{x}$ are linear functions with determinant $\det\left(x_i^{(j)}\right)$ of the coordinates y_h of $\mathbf{y} = (y_1, \ldots, y_n)$. We define

a new distance function $g(\mathbf{x})$ by $g(\mathbf{x}) = |\mathbf{y}|$. By Proposition 7.2, the convex body $g(\mathbf{x}) \leq 1$ has the volume $\det\left(x_i^{(j)}\right)$; we determine it in the following way:

If $\mathbf{x}$ is a lattice point, then $\mathbf{y}$ also has its coordinates y_h in $\mathbf{F}[z]$. For since with $\mathbf{x}$ also $\mathbf{y}$ is obviously a lattice point, we may assume without loss of generality that

$$g(\mathbf{x}) = |\mathbf{y}| < 1, \tag{7.8}$$

and have to show that no lattice point $\mathbf{x} \neq 0$ satisfies this inequality. Let m, where $1 \leq m \leq n$, be the greatest index for which $y_m \neq 0$. Then $\mathbf{x}, \mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(m-1)}$ are $\mathbf{F}(z)$-independent lattice points, and by (7.8)

$$f(\mathbf{x}) \leq \max\left\{|y_1| f\left(\mathbf{x}^{(1)}\right), \ldots, |y_m| f\left(\mathbf{x}^{(m)}\right)\right\} < \lambda_m,$$

in contradiction to the minimum property of λ_m. Hence there are exactly $n_1(t) = n(t+1)$ $\mathbf{F}$-independent lattice points such that $g(\mathbf{x}) \leq e^t$, viz. all points corresponding to a basis of $\mathbf{F}$-independent points $\mathbf{y}$ with $\mathbf{y} \leq e^t$. Therefore

$$\left|\det\left(x_i^{(j)}\right)\right| = \lim_{t\to\infty} e^{n_1(t)-n_0(t)} = 1.$$

Set $\lambda_j = e^{t_j}$ for $j = 1, \ldots, n$. Now we use the fact that every point $\mathbf{x} \in K^n$ can be written as

$$\mathbf{x} = y_1 z^{-t_1}\mathbf{x}^{(1)} + \cdots + y_n z^{-t_n}\mathbf{x}^{(n)},$$

where $y_j \in K$. Let $G(\mathbf{x})$ be the distance function defined by $G(\mathbf{x}) = |\mathbf{y}|$. Since

$$f\left(z^{-t_j}\mathbf{x}^{(j)}\right) = 1, \;\; j = 1, 2, \ldots, n,$$

obviously $f(\mathbf{x}) \leq 1$ if $G(\mathbf{x}) \leq 1$. But the converse is also true: If $f(\mathbf{x}) \leq 1$, then $G(\mathbf{x}) \leq 1$, and therefore evidently

$$f(\mathbf{x}) = G(\mathbf{x}) = |\mathbf{y}| \tag{7.9}$$

identically in $\mathbf{x}$.

For suppose that on the contrary for a certain point $\mathbf{x} \in K^n$,

$$f(\mathbf{x}) \leq 1, \quad G(\mathbf{x}) > 1.$$

Then let m with $1 \leq m \leq n$ be the greatest index for which $|y_m| > 1$; hence if $m < n$

$$|y_{m+1}| \leq 1, \ldots, |y_n| \leq 1.$$

Write

$$y_h = z y_h^* + y_h^{**}, \;\; h = 1, 2, \ldots, n,$$

where the y_h^* are elements of $\mathbf{F}[z]$, the y_h^{**} elements of K, and

$$y_m^* \neq 0, \; y_{m+1}^* = \cdots = y_n^* = 0, \; |y_i^{**}| \leq 1 \;\; (i = 1, \ldots, n),$$

and put

$$\mathbf{y}^* = (y_1^*, \dots, y_n^*), \quad \mathbf{y}^{**} = (y_1^{**}, \dots, y_n^{**}),$$

so that

$$\mathbf{y} = z\mathbf{y}^* + \mathbf{y}^{**}.$$

Obviously, $\mathbf{y}^*$ is a lattice point, $\mathbf{y}^{**}$ a point such that $|\mathbf{y}^{**}| \leq 1$. Also write

$$\mathbf{x}^* = \sum_{i=1}^{m} y_i^* z^{-t_i} \mathbf{x}^{(i)}, \quad \mathbf{x}^{**} = \sum_{i=1}^{n} y_i^{**} z^{-t_i} \mathbf{x}^{(i)},$$

so that

$$\mathbf{x} = z\mathbf{x}^* + \mathbf{x}^{**}.$$

Then from $G(\mathbf{x}^{**}) = |\mathbf{y}^{**}| \leq 1$, one has $f(\mathbf{x}^{**}) \leq 1$. Hence

$$f(z\mathbf{x}^*) \leq \max\{f(\mathbf{x}), f(\mathbf{x}^{**})\} \leq 1, \quad f(\mathbf{x}^*) < 1,$$

and $f(\mathbf{x}^0) < \lambda_m$, where $\mathbf{x}^0 = z^{t_m}\mathbf{x}^*$. This inequality, however, is impossible, since the m lattice points

$$\mathbf{x}^0 = \sum_{i=1}^{m} y_i^* z^{t_m - t_i} \mathbf{x}^{(i)}, \ \mathbf{x}^{(1)}, \ \dots, \ \mathbf{x}^{(m-1)}$$

are K-independent, so that by the minimum property of λ_m, $f(\mathbf{x}^0) \geq \lambda_m$.

Therefore (7.9) is true, so that by Proposition 7.2

$$V = \frac{\left|\det\left(x_i^{(j)}\right)\right|}{\lambda_1\lambda_2\cdots\lambda_n} = \frac{1}{\lambda_1\lambda_2\cdots\lambda_n},$$

since the transformation of $\mathbf{x}$ into $\mathbf{y}$ has the determinant $\det\left(x_i^{(j)}\right) z^{-t_1-\cdots-t_n}$. The equation (7.7) is therefore proved. □

7.2 Adelic Minkowski's second theorem

7.2.1 Haar measures

Generally, there exists a *Haar measure* $\mu = \mu_G$ on a locally compact group G, i.e. a measure invariant under group shifts $x \mapsto gx$ $(x, g \in G)$:

$$\int_G f(gx)\, d\mu(x) = \int_G f(x) d\mu(x)$$

for all integrable functions $f : G \longrightarrow \mathbb{C}$. This measure is defined uniquely up to a multiplicative constant.

Let H be a normal closed subgroup and $\pi : G \longrightarrow G/H$ be the quotient morphism. By definition, a subset U of G/H is open if and only if $\pi^{-1}(U)$ is open in G. Note that π is an open mapping and hence G/H is a locally compact group. Given Haar measures μ_G, μ_H on G and H, there is a unique Haar measure $\mu_{G/H}$ on G/H such that

$$\int_G f(x)d\mu_G(x) = \int_{G/H} \left(\int_H f(xy)d\mu_H(y) \right) d\mu_{G/H}(\pi(x)) \tag{7.10}$$

for all continuous complex functions f with compact support. Moreover, this formula continues to hold for all $f \in L^1(G, \mu_G)$ (see [14]).

Example 7.4. **(1)** If $G = \mathbb{R}$ (the additive group), then $d\mu(x) = dx$ is the Lebesgue measure, and $d(x + a) = dx,\ a \in \mathbb{R}$. If $G = \mathbb{R}_*$ (the multiplicative group), then $d\mu(x) = \frac{dx}{x}$.

(2) If $G = \mathbb{C}$, then $d\mu(z) = dxdy$ for $z = x + \sqrt{-1}y$.

(3) If $\kappa/\mathbb{Q}_p$ is a finite dimensional extension, then the measure $d\mu$ on the additive group κ is uniquely determined by the number

$$\int_{\mathcal{O}_{\kappa,p}} d\mu = \mu(\mathcal{O}_{\kappa,p}) = c > 0.$$

Example 7.5 (cf. [14]). Let κ be a number field of degree d and take $v \in M_\kappa^0$ with valuation ring R_v in the completion κ_v, residue field $\mathbb{F}_v(\kappa)$, and local parameter t (i.e., t is a generator of the maximal ideal in R_v). We denote by e_v, f_v the ramification index and the residue class degree of v over $p := \mathrm{char}(\mathbb{F}_v(\kappa))$. We consider the closed balls

$$\kappa_v[x; \varepsilon] := \{y \in \kappa_v \mid \|y - x\|_v \leq \varepsilon,\ x \in \kappa_v\}.$$

Note that we need only consider balls of radius r^n $(n \in \mathbb{Z})$, where

$$r = \|t\|_v = p^{-f_v}.$$

By the ultrametric triangle inequality, two balls are either disjoint or one is contained in the other. Every open subset of κ_v is a countable disjoint union of such closed balls. In particular, $\kappa_v[0; 1] = R_v$ is the disjoint union of p^{f_v} balls $\kappa_v[x; r]$. Thus

$$\mu_v(\kappa_v[x; r^n]) := p^{-nf_v} = r^n$$

is a σ-additive and translation invariant set function on these balls, and extends uniquely to a function on the compact open subsets of κ_v with the same properties. By standard arguments of measure theory, μ_v extends uniquely to a translation invariant Borel measure. Further, the Haar measure μ_v on κ_v satisfies the property

$$\mu_v(\lambda\Omega) = \|\lambda\|_v \mu_v(\Omega) \tag{7.11}$$

for any $\lambda \in \kappa_v$ and any Borel measurable subset Ω of κ_v. This is trivial for $\Omega = \kappa_v[0; r^n]$. By translation invariance, we get (7.11) for any closed ball and by uniqueness of the extension we get it for all Borel measurable subsets Ω of κ_v.

7.2.2 Adèle rings

Let κ be an algebraic number field. We then write $d = [\kappa : \mathbb{Q}]$ for the degree of κ over $\mathbb{Q}$. We denote by $\mathcal{O}_\kappa$ the ring of integers of κ. In view of Proposition 2.14, the number of Archimedean (or infinite) places of κ does not exceed d. Let $\sigma_1, \dots, \sigma_{r_1}, \dots, \sigma_{r_1+r_2}$ be the embeddings in Proposition 2.14. Then the tuple

$$\sigma = (\sigma_1, \dots, \sigma_{r_1}, \dots, \sigma_{r_1+r_2}) \tag{7.12}$$

defines an embedding of κ into $\mathbb{R}^d$, and any embedding of κ into $\mathbb{C}$ is one of the following

$$\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \dots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}.$$

One can verifies that the image $\Lambda = \sigma(\mathcal{O}_\kappa) \subset \mathbb{R}^d$ is a lattice, which is a free Abelian group generalized by a basis $e_1, \dots, e_d$ of $\mathbb{R}^d$, and

$$D_{\kappa/\mathbb{Q}} = (-4)^{r_2} V(\Lambda)^2, \tag{7.13}$$

where $V(\Lambda)$ is the volume of the fundamental parallelogram

$$\left\{ \sum_{i=1}^{d} x_i e_i \mid 0 \le x_i \le 1,\ i = 1, \dots, d \right\}$$

of the lattice Λ with respect to the ordinary Lebesgue measure on $\mathbb{R}^d$.

For every place v of κ we write κ_v for the completion of κ at v. If v is a finite place of κ we write $\mathcal{O}_v$ for the maximal compact subring of κ_v, that is,

$$\mathcal{O}_v = \{x \in \kappa_v \mid |x|_v \le 1\}.$$

Since all but a finite number of places of κ are non-Archimedean, one defines

$$\kappa_{\mathbb{A}} = \left\{ x = (x_v) \in \prod_{v \in M_\kappa} \kappa_v \mid x_v \in \mathcal{O}_v \text{ for all but a finite number of } v \right\} \tag{7.14}$$

to be the subring of the product $\prod_{v \in M_\kappa} \kappa_v$ consisting of all infinite vectors $x = (x_v)_{v \in M_\kappa}$, $x_v \in \kappa_v$ such that $x_v \in \mathcal{O}_v$ for all but a finite number of v, which is called the *adèle ring*. One gives $\kappa_{\mathbb{A}}$ the topology generated by the open subsets of the type

$$W_S = \prod_{v \in S} W_v \times \prod_{v \notin S} \mathcal{O}_v, \tag{7.15}$$

where S runs through all finite subsets $S \subset M_\kappa$ containing all infinite places, and W_v are open subsets in κ_v. The set W_S has compact closure if all the W_v are bounded. Hence $\kappa_{\mathbb{A}}$ is a locally compact topological ring in which κ is embedded diagonally

$$\kappa \ni x \mapsto (x)_{v \in M_\kappa} \in \kappa_{\mathbb{A}} \subset \prod_{v \in M_\kappa} \kappa_v.$$

The above construction of $\kappa_{\mathbb{A}}$ is called the *restricted topological product* of the topological spaces κ_v with respect to the compact subspaces $\mathcal{O}_v$ defined for all but a finite number of indices v. The convergence of a sequence $\{x_n\}_{n=1}^{\infty}$, $x_n = (x_{n,v}) \in \kappa_{\mathbb{A}}$ to $y = (y_v) \in \kappa_{\mathbb{A}}$ means that for any $\varepsilon > 0$ and any finite set $S \subset M_\kappa$ containing all infinite places, there exists $N \in \mathbb{Z}^+$ such that

(1) $x_{n,v} - y_v \in \mathcal{O}_v$ for each $n > N$, $v \notin S$;

(2) $|x_{n,v} - y_v|_v < \varepsilon$ for each $n > N$, $v \in S$.

Every principal adèle x, i.e.

$$x = (\ldots, x, x, \ldots)_v \in \kappa \subset \kappa_{\mathbb{A}}$$

can be separated from the rest of κ by a neighborhood of type (7.15) with

$$S = \{v \in M_\kappa \mid x \notin \mathcal{O}_v\}.$$

Hence κ is discrete in $\kappa_{\mathbb{A}}$. All the properties of $\kappa_{\mathbb{A}}$ which we will need can be found in Weil [298], Chap. IV.

Since the additive group of $\kappa_{\mathbb{A}}$ is locally compact we can determine a *Haar measure* on $\kappa_{\mathbb{A}}$ which is unique up to a multiplicative constant. We do this as follows:

(i) If $v|p$ we let μ_v denote Haar measure on κ_v normalized so that

$$\mu_v(\mathcal{O}_v) = \mathcal{N}(\mathfrak{d}_v)^{-\frac{1}{2}},$$

where $\mathfrak{d}_v$ is the *local different* of κ at v.

(ii) If $v|\infty$ and $\kappa_v = \mathbb{R}$ we let $\mu_v = dx$ denote the ordinary Lebesgue measure on $\mathbb{R}$.

(iii) If $v|\infty$ and $\kappa_v = \mathbb{C}$ we let $\mu_v = 2dxdy$ denote the ordinary Lebesgue measure on the complex plane $\mathbb{C}$ multiplied by 2.

Now the product measure

$$\mu = \prod_v \mu_v$$

is the required Haar measure on $\kappa_{\mathbb{A}}$ (to be precise, μ determines a Haar measure on all open subgroups $\prod_{v\in S} \kappa_v \times \prod_{v\notin S} \mathcal{O}_v$, where S is any finite set of places containing all infinite places, and the Haar measure on $\kappa_{\mathbb{A}}$ is the unique measure which agrees with the product measure on this family of subgroups).

Recall that we consider κ as a discrete subgroup of $\kappa_{\mathbb{A}}$ by means of the usual diagonal embedding and we denote by φ the canonical homomorphism $\varphi : \kappa_{\mathbb{A}} \longrightarrow \kappa_{\mathbb{A}}/\kappa$ of $\kappa_{\mathbb{A}}$ onto the compact group $\kappa_{\mathbb{A}}/\kappa$ (cf. [14]). By (7.10), we get a uniquely determined Haar measure. The Haar measure induced by φ on $\kappa_{\mathbb{A}}/\kappa$ will also denoted by μ. Alternatively, we can define the measure μ on $\kappa_{\mathbb{A}}/\kappa$ by means of a general notion of fundamental domain: if Γ is a discrete subgroup of a locally compact group G, then a fundamental domain X for G modulo Γ is a complete set of coset representatives for

(left) cosets G/Γ, which has some additional measurability properties. By restricting the Haar measure ν of G onto the subset X, one obtains a uniquely defined measure on G/Γ, which is denoted by the same letter, and $\nu(G/\Gamma) = \nu(X)$.

In order to construct a fundamental domain X for $\kappa_{\mathbb{A}}/\kappa$, we choose a $\mathbb{Z}$-basis $w_1, \dots, w_d$ of the free Abelian group $\mathcal{O}_\kappa \subset \kappa$ of algebraic integers in κ (cf. Theorem 2.18). This is also a basis of the vector space over $\mathbb{R}$

$$\kappa_{\mathbb{R}} = \kappa \otimes \mathbb{R} \cong \prod_{v|\infty} \kappa_v \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \tag{7.16}$$

and it defines an isomorphism $\theta : \mathbb{R}^d \longrightarrow \kappa_{\mathbb{R}}$ by the formula

$$\theta(u_1, \dots, u_d) = \sum_{i=1}^{d} u_i w_i.$$

Denote by I the interval $0 \le t < 1$ in $\mathbb{R}$. Then $\theta(I^d)$ is a fundamental parallelogram for the lattice $\sigma(\mathcal{O}_\kappa)$ in $\kappa_{\mathbb{R}}$. Now take X to be the set

$$X = \theta(I^d) \times \prod_{v\nmid\infty} \mathcal{O}_v. \tag{7.17}$$

To prove that X is a fundamental domain, we note that $\kappa_{\mathbb{R}} + \kappa$ is dense in $\kappa_{\mathbb{A}}$. This statement is known as the *approximation theorem* and it is a version of the *Chinese remainder theorem*. Moreover, $\kappa_{\mathbb{R}} \times \prod_v \mathcal{O}_v$ is an open subgroup in $\kappa_{\mathbb{A}}$, hence for any $x \in \kappa_{\mathbb{A}}$ there exists $\eta \in \kappa$ such that

$$x - \eta \in \kappa_{\mathbb{R}} \times \prod_{v} \mathcal{O}_v.$$

The condition that another element $\eta' \in \kappa$ has the same property is equivalent to saying that $\eta - \eta' \in \mathcal{O}_v$ for all non-Archimedean places v, that is, $\eta - \eta' \in \mathcal{O}_\kappa$. Thus by an appropriate choice of η we may assume that the y_∞-coordinate of $y = x - \eta$ belongs to $\theta(I^d)$; therefore $y_\infty = \theta(u),\ u \in I^d$, where u is uniquely determined. This establishes the statement.

Let us calculate the measure $\mu(\kappa_{\mathbb{A}}/\kappa)$. By (7.10), we have

$$\mu(\kappa_{\mathbb{A}}/\kappa) = \mu(X).$$

The form of the fundamental domain X constructed reduces this calculation to the problem of determining the volume of the fundamental parallelogram $\theta(I^d)$ in $\kappa_{\mathbb{R}}$.

$$\mu(X) = \left(\prod_{v|\infty} \mu_v \right) \big(\theta(I^d)\big) \prod_{v\nmid\infty} \mathcal{N}(\mathfrak{d}_v)^{-\frac{1}{2}}.$$

This volume was already found in (7.13), that is,

$$\left(\prod_{v|\infty}\mu_v\right)\big(\theta(I^d)\big) = |D_{\kappa/\mathbb{Q}}|^{1/2}.$$

Here we have taken into account that the measure $\prod_{v|\infty}\mu_v$ on $\kappa_{\mathbb{R}}$ differs by a multiple of 2 from the Lebesgue measure on those components v such that $\kappa_v \cong \mathbb{C}$, when

$$d\mu_v(z) = 2dxdy = |dz \wedge d\bar{z}|, \;\; z = x + iy \in \kappa_v \cong \mathbb{C}.$$

Therefore we obtain

$$\mu(\kappa_{\mathbb{A}}/\kappa) = |D_{\kappa/\mathbb{Q}}|^{1/2} \prod_{v\nmid\infty} \mathcal{N}(\mathfrak{d}_v)^{-\frac{1}{2}}.$$

Note that

$$|D_{\kappa/\mathbb{Q}}| = \prod_{v\nmid\infty} \mathcal{N}(\mathfrak{d}_v).$$

In view of our normalizations we have

$$\mu(\kappa_{\mathbb{A}}/\kappa) = 1. \tag{7.18}$$

7.2.3 Minkowski's second theorem

Let κ be a number field of degree d and let

$$G = G_1 \times G_2 \times \cdots \times G_n \tag{7.19}$$

be a product of locally compact groups in which each factor G_i is either $\kappa_{\mathbb{A}}$ or $\kappa_{\mathbb{A}}/\kappa$. The Haar measure μ on each factor determines a unique product measure on G. We write V for this product measure and note that V is then a Haar measure on G. Of course there are many different groups G that can be formed in this way. However, there will no confusion if we use V to denote the corresponding Haar measure on each of them.

Let G be a group of the form (7.19) and suppose that the factor G_i is $\kappa_{\mathbb{A}}$. We define a homomorphism φ_i on G by

$$\varphi_i(g_1, \ldots, g_i, \ldots, g_n) = (g_1, \ldots, \varphi(g_i), \ldots, g_n).$$

If each of the factors $G_1, G_2, \ldots, G_i$ is $\kappa_{\mathbb{A}}$ we let Φ_i denote the homomorphism

$$\Phi_i = \varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_i.$$

Since each mapping φ_i or Φ_i is a homomorphism, the Haar measure of a measurable set $X \subseteq G$ is preserved whenever the homomorphism restricted to X is injective. Thus we have

$$V(X) = V(\Phi_i(X))$$

if $X \subseteq G$ is measurable and Φ_i restricted to X is an injection (and similarly for φ_i).

Let $x = (x_v)$ be an element of $\kappa_{\mathbb{A}}$ and let α be a real number. We introduce a scalar multiplication by defining αx to be the point $y = (y_v)$ in $\kappa_{\mathbb{A}}$ determined by

$$y_v = \begin{cases} \alpha x_v, & \text{if } v|\infty, \\ x_v, & \text{if } v \nmid \infty. \end{cases}$$

If $X \subseteq \kappa_{\mathbb{A}}^n$ then $\alpha X \subseteq \kappa_{\mathbb{A}}^n$ is obtained by applying scalar multiplication by α to each $\mathbf{x}$ in X. Clearly we have

$$V(\alpha X) = |\alpha|^{dn} V(X) \tag{7.20}$$

for each measurable subset X in $\kappa_{\mathbb{A}}^n$, where $|\alpha|$ is the Euclidean absolute value of the real number α.

For a finite place v of κ, a *κ_v-lattice* in κ_v^n is an open and compact $\mathcal{O}_v$-submodule of κ_v^n.

Proposition 7.6. *Let Λ_v be an $\mathcal{O}_v$-submodule of κ_v^n. Then Λ_v is a κ_v-lattice in κ_v^n if and only if Λ_v is a finitely generated $\mathcal{O}_v$-module which generates κ_v^n as a κ_v-vector space.*

Proof. See [14], Proposition C.2.2. □

A *κ-lattice* in κ^n is a finitely generated $\mathcal{O}_\kappa$-submodule of κ^n which generates κ^n as a κ-vector space.

Proposition 7.7. *If Λ is a κ-lattice in κ^n, then the closure Λ_v of Λ in κ_v^n is a κ_v-lattice in κ_v^n for any non-Archimedean $v \in M_\kappa$. Moreover, we have $\Lambda_v = \mathcal{O}_v^n$ up to finitely many $v \in M_\kappa$. Conversely, if for any non-Archimedean $v \in M_\kappa$ we have a κ_v-lattice Λ_v in κ_v^n and if $\Lambda_v = \mathcal{O}_v^n$ up to finitely many v, then there is a unique κ-lattice Λ in κ^n such that Λ_v is the closure of Λ in κ_v^n. Moreover, we have*

$$\Lambda = \bigcap_{v \in M_\kappa^0} (\kappa^n \cap \Lambda_v).$$

Proof. See [14], Proposition C.2.6. □

For each infinite place v of κ let $\mathcal{C}_v$ be a nonempty, open, convex subset of κ_v^n, and set

$$\mathcal{C}_\infty = \prod_{v|\infty} \mathcal{C}_v.$$

For each finite place v of κ let $\mathcal{C}_v$ be a κ_v-lattice in κ_v^n. We assume that for almost all v, $\mathcal{C}_v = \mathcal{O}_v^n$. Thus we obtain an open subset $\mathcal{C} \subseteq \kappa_{\mathbb{A}}^n$ by defining

$$\mathcal{C} = \mathcal{C}_\infty \times \prod_{v \nmid \infty} \mathcal{C}_v. \tag{7.21}$$

Lemma 7.8 ([15], [14]). *If $\mathcal{C}$ has the form (7.21) and $\rho \geq 1$, then for each integer i with $1 \leq i \leq n$*

$$V(\Phi_i(\rho\mathcal{C})) \geq \rho^{d(n-i)} V(\Phi_i(\mathcal{C})). \tag{7.22}$$

Proof. First assume that $i = n$ and let $\mathbf{y} \in \mathcal{C}$. Since $0 \in \mathcal{C}$, it follows from the convexity of each $\mathcal{C}_v$, $v|\infty$, that

$$\mathcal{C} - \mathbf{y} \subseteq \rho(\mathcal{C} - \mathbf{y}).$$

Therefore one has

$$\Phi_n(\mathcal{C} - \mathbf{y}) \subseteq \Phi_n(\rho\mathcal{C} - \rho\mathbf{y})$$

and so

$$V(\Phi_n(\mathcal{C} - \mathbf{y})) \leq V(\Phi_n(\rho\mathcal{C} - \rho\mathbf{y})).$$

As V is translation invariant and Φ_n is a homomorphism,

$$V(\Phi_n(\rho\mathcal{C} - \rho\mathbf{y})) = V(\Phi_n(\rho\mathcal{C}))$$

and similarly

$$V(\Phi_n(\mathcal{C} - \mathbf{y})) = V(\Phi_n(\mathcal{C})).$$

This established (7.22) when $i = n$.

Next we suppose that $1 \leq i \leq n-1$. We may identify $\kappa_{\mathbb{A}}^n$ in an obvious way with

$$\kappa_{\mathbb{A}}^i \times \kappa_{\mathbb{A}}^{n-i} = \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x} \in \kappa_{\mathbb{A}}^i, \quad \mathbf{y} \in \kappa_{\mathbb{A}}^{n-i}\}.$$

In this identification the first component of $(\mathbf{x}, \mathbf{y})$ represents the first i coordinates of a vector $\mathbf{z} \in \kappa_{\mathbb{A}}^n$. Then for a fixed vector $\mathbf{y} \in \kappa_{\mathbb{A}}^{n-i}$, let $\mathcal{C}(\mathbf{y}) \subseteq \kappa_{\mathbb{A}}^i$ be defined by

$$\mathcal{C}(\mathbf{y}) = \{\mathbf{x} \in \kappa_{\mathbb{A}}^i \mid (\mathbf{x}, \mathbf{y}) \in \mathcal{C}\}.$$

It follows that

$$\Phi_i(\mathcal{C}(\mathbf{y})) = \{\omega \in (\kappa_{\mathbb{A}}/\kappa)^i \mid (\omega, \mathbf{y}) \in \Phi_i(\mathcal{C})\}.$$

If we replace $\mathcal{C}$ by $\rho\mathcal{C}$, then

$$\begin{aligned} V(\Phi_i(\rho\mathcal{C})) &= \int_{\mathbf{y} \in \kappa_{\mathbb{A}}^{n-i}} \int_{\substack{\omega \in (\kappa_{\mathbb{A}}/\kappa)^i \\ (\omega, \mathbf{y}) \in \Phi_i(\rho\mathcal{C})}} dV(\omega) dV(\mathbf{y}) \\ &= \int_{\mathbf{y} \in \kappa_{\mathbb{A}}^{n-i}} V(\Phi_i((\rho\mathcal{C})(\mathbf{y}))) dV(\mathbf{y}). \end{aligned}$$

We make the change of variable $\mathbf{y} \mapsto \rho\mathbf{y}$ in the last integral, so that

$$V(\Phi_i(\rho\mathcal{C})) = \rho^{d(n-i)} \int_{\mathbf{y}\in\kappa_{\mathbb{A}}^{n-i}} V(\Phi_i((\rho\mathcal{C})(\rho\mathbf{y})))dV(\mathbf{y}). \tag{7.23}$$

Now we observe that

$$(\rho\mathcal{C})(\rho\mathbf{y}) = \{\mathbf{x} \in \kappa_{\mathbb{A}}^i \mid (\mathbf{x}, \rho\mathbf{y}) \in \rho\mathcal{C}\} = \rho(\mathcal{C}(\mathbf{y})). \tag{7.24}$$

Since $\rho \geq 1$ we have

$$V(\Phi_i(\rho(\mathcal{C}(\mathbf{y})))) \geq V(\Phi_i(\mathcal{C}(\mathbf{y}))) \tag{7.25}$$

as before using the facts that V is translation invariant, Φ_i is a homomorphism, and $\mathcal{C}(\mathbf{y}) \subseteq \kappa_{\mathbb{A}}^i$. By combining (7.23), (7.24) and (7.25) we obtain

$$\begin{aligned} V(\Phi_i(\rho\mathcal{C})) &\geq \rho^{d(n-i)} \int_{\mathbf{y}\in\kappa_{\mathbb{A}}^{n-i}} V(\Phi_i(\mathcal{C}(\mathbf{y})))dV(\mathbf{y}) \\ &= \rho^{d(n-i)} V(\Phi_i(\mathcal{C})). \end{aligned}$$

This completes our proof. □

By using Lemma 7.8, one can prove the *Davenport–Estermann theorem* (cf. [15], [14]):

Theorem 7.9. *Let $\mathcal{C}$ be as above. Suppose that*

$$0 < \rho_1 \leq \rho_2 \leq \cdots \leq \rho_n < \infty$$

satisfy the following conditions $x_j = y_j$ for $j = i, i+1, \ldots, n$, if $\mathbf{x}$ and $\mathbf{y}$ are vectors in $\rho_i\mathcal{C}$ with $\mathbf{x} - \mathbf{y} \in \kappa^n$. Then

$$(\rho_1\rho_2 \cdots \rho_n)^d V(\mathcal{C}) \leq 1. \tag{7.26}$$

Proof. For each integer i, $1 \leq i \leq n-1$, we apply Lemma 7.8 to the set $\rho_i\mathcal{C}$ with $\rho = \rho_{i+1}/\rho_i$. We find that

$$V(\Phi_i(\rho_{i+1}\mathcal{C})) \geq (\rho_{i+1}/\rho_i)^{d(n-i)} V(\Phi_i(\rho_i\mathcal{C})). \tag{7.27}$$

Next we claim that

$$\varphi_{i+1} : \Phi_i(\rho_{i+1}\mathcal{C}) \longrightarrow (\kappa_{\mathbb{A}}/\kappa)^{i+1} \times \kappa_{\mathbb{A}}^{n-i-1} \tag{7.28}$$

is injective. To verify this let $\mathbf{x}$ and $\mathbf{y}$ be distinct points in $\Phi_i(\rho_{i+1}\mathcal{C})$. Then there are distinct points $\mathbf{x}'$ and $\mathbf{y}'$ in $\rho_{i+1}\mathcal{C}$ such that $\Phi_i(\mathbf{x}') = \mathbf{x}$ and $\Phi_i(\mathbf{y}') = \mathbf{y}$. Now the equation $\varphi_{i+1}(\mathbf{x}) = \varphi_{i+1}(\mathbf{y})$ implies that

$$x_j = y_j, \;\; j \neq i+1 \tag{7.29}$$

and also implies that

$$\Phi_{i+1}(\mathbf{x}') = \Phi_{i+1}(\mathbf{y}'). \tag{7.30}$$

But (7.30) shows that $\mathbf{x}' - \mathbf{y}' \in \kappa^n$ and so by the hypotheses on $\rho_1, \rho_2, \ldots, \rho_n$ we must have

$$x'_j = y'_j, \;\; j = i+1, i+2, \ldots, n.$$

Since Φ_i is the identity mapping on the $(i+1)$-th coordinate we find that

$$x_j = y_j, \;\; j = i+1. \tag{7.31}$$

Of course (7.29) and (7.31) are inconsistent with the fact that $\mathbf{x}$ and $\mathbf{y}$ are distinct points in $\Phi_i(\rho_{i+1}\mathcal{C})$. Thus our claim that (7.28) is injective has been established. As V is a Haar measure this shows that

$$V(\Phi_i(\rho_{i+1}\mathcal{C})) = V(\Phi_{i+1}(\rho_{i+1}\mathcal{C})). \tag{7.32}$$

By combining (7.27) and (7.32) we have

$$V(\Phi_{i+1}(\rho_{i+1}\mathcal{C})) \geq (\rho_{i+1}/\rho_i)^{d(n-i)} V(\Phi_i(\rho_i\mathcal{C}))$$

for $i = 1, 2, \ldots, n-1$. Next we multiply these inequalities together to obtain

$$V(\Phi_n(\rho_n\mathcal{C})) \geq V(\Phi_1(\rho_1\mathcal{C})) \prod_{i=1}^{n-1} (\rho_{i+1}/\rho_i)^{d(n-i)}.$$

Finally we note that

$$V(\Phi_1(\rho_1\mathcal{C})) = V(\rho_1\mathcal{C}) = \rho_1^{dn} V(\mathcal{C}),$$

since $\Phi_1 = \varphi_1$ applied to $\rho_1\mathcal{C}$ is obviously injective, and also

$$V(\Phi_n(\rho_n\mathcal{C})) \leq V((\kappa_{\mathbb{A}}/\kappa)^n) = 1.$$

Thus we have

$$1 \geq \rho_1^{dn} V(\mathcal{C}) \prod_{i=1}^{n-1} (\rho_{i+1}/\rho_i)^{d(n-i)},$$

which is equivalent to (7.26). □

For each infinite place v of κ, we further assume that $\mathcal{C}_v$ is symmetric subset of κ_v^n. By *symmetric* we mean that $\mathcal{C}_v = -\mathcal{C}_v$. To avoid some minor complications it will be convenient to assume that each $\mathcal{C}_v$ is also bounded. It follows that $\mathcal{C}$ is an open neighborhood of 0 and the closure of $\mathcal{C}$ is compact. As κ^n is a discrete subgroup of $\kappa_{\mathbb{A}}^n$, it is clear that $\mathcal{C} \cap \kappa^n$ is finite. We are now able to define the *successive minima* for $\mathcal{C}$

with respect to the subgroup κ^n. We do this as follows. For each integer j, $1 \le j \le n$, let

$$\lambda_j = \min\{\lambda > 0 \mid \lambda\mathcal{C} \cap \kappa^n \text{ contains at least } j \text{ linearly independent vectors}\}.$$

It is obvious that

$$0 < \lambda_1 \le \lambda_2 \le \cdots \le \lambda_n < \infty. \tag{7.33}$$

In fact, the set

$$\Lambda = \bigcap_{v \nmid \infty} (\kappa^n \cap \mathcal{C}_v)$$

is a κ-lattice, that is, an $\mathcal{O}_\kappa$-module in κ^n containing a basis for κ^n over κ (see [298], Theorem 2, p. 84). If we write

$$E_\infty = \prod_{v \mid \infty} \kappa_v^n,$$

then Λ can be viewed as the projection of

$$\left(E_\infty \times \prod_{v \nmid \infty} \mathcal{C}_v\right) \cap \kappa^n$$

into the first factor E_∞. Thus Λ is a discrete subgroup of E_∞. Since each $\mathcal{C}_v$ is open and bounded for $v|\infty$, it follows that

$$\lambda\mathcal{C}_\infty \cap \Lambda = \{0\}$$

if $\lambda > 0$ is sufficiently small and contains n linearly independent vectors if λ is sufficiently large. In this way, we see that the successive minima λ_j satisfy (7.33). Indeed, it is clear that the numbers λ_j may also be defined by

$$\lambda_j = \min\left\{\lambda > 0 \mid \lambda\mathcal{C}_\infty \cap \Lambda \text{ contains } j \text{ linearly independent vectors}\right\}. \tag{7.34}$$

Now we are ready to prove *Minkowski's second theorem* (cf. [15], [14]):

Theorem 7.10. *The successive minima $\lambda_1, \lambda_2, \ldots, \lambda_n$ satisfy the inequality*

$$(\lambda_1\lambda_2\cdots\lambda_n)^d V(\mathcal{C}) \le 2^{dn}. \tag{7.35}$$

Proof. With each successive minima λ_j we may associate a vector $\mathbf{x}^{(j)}$ in κ^n so that $\{\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(n)}\}$ are linearly independent over κ and for every j, $1 \le j \le n$, and $\lambda > \lambda_j$, we have

$$\{\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(j)}\} \subseteq (\lambda\mathcal{C}) \cap \kappa^n.$$

Now let $A = \left(x_i^{(j)}\right)$ be the $n \times n$ matrix with j-th row $\mathbf{x}^{(j)} = \left(x_1^{(j)}, \ldots, x_n^{(j)}\right)$. It follows that $\mathbf{x} \mapsto \mathbf{x}A$ is an automorphism of $\kappa_{\mathbb{A}}^n$. Since $\det(A) \in \kappa$, the modulus of this automorphism is 1. That is, the automorphism preserves the Haar measure V. The

sets $\mathcal{C}_v A^{-1}$ have exactly the same properties as $\mathcal{C}_v$. Thus the successive minima for $\mathcal{C}A^{-1}$ may be defined as before and are clearly equal to the minima $\lambda_1, \lambda_2, \ldots, \lambda_n$ of $\mathcal{C}$. Now, however, the vectors associated with the successive minima of $\mathcal{C}A^{-1}$ may be taken as

$$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1).$$

Since $\mathcal{C}$ and $\mathcal{C}A^{-1}$ have the same Haar measure, we may assume without loss of generality that $\mathbf{x}^{(j)} = e_j$ to begin with.

Next we wish to apply Theorem 7.9 with

$$\rho_j = \frac{1}{2}\lambda_j,\ \ j = 1, 2, \ldots, n.$$

We must check that the hypotheses of Theorem 7.9 are satisfied and it clearly suffices to consider $j = 1$ and those values of j for which $\lambda_{j-1} < \lambda_j$. Therefore we suppose that $\mathbf{x}$ and $\mathbf{y}$ are distinct points in $\rho_1\mathcal{C}$ with $\mathbf{x} - \mathbf{y} \in \kappa^n$. Since each $\mathcal{C}_v$, $v|\infty$, is convex and symmetric we have

$$\mathbf{x} - \mathbf{y} \in 2\rho_1\mathcal{C} = \lambda_1\mathcal{C}.$$

Also, each of the vectors $e_1, \ldots, e_{j-1}$ and $\mathbf{x} - \mathbf{y}$ is in $(\lambda_j - \delta)\mathcal{C}$ for some $\delta > 0$ since $\lambda_{j-1} < \lambda_j$ and $\mathcal{C}$ is open. It follows that

$$\{e_1, e_2, \ldots, e_{j-1}, \mathbf{x} - \mathbf{y}\}$$

cannot be linearly independent over κ. As $e_1, \ldots, e_{j-1}$ are obviously linearly independent we must have

$$\mathbf{x} - \mathbf{y} = \sum_{i=1}^{j-1} \alpha_i e_i$$

with $\alpha_i \in \kappa$ $(i = 1, 2, \ldots, j-1)$. In other words,

$$x_i = y_i,\ \ i = j, j+1, \ldots, n.$$

We now apply Theorem 7.9 to obtain

$$(\rho_1\rho_2 \cdots \rho_n)^d V(\mathcal{C}) \leq 1.$$

Since $\rho_j = \frac{1}{2}\lambda_j$, this also proves Theorem 7.10. □

The classical form of Minkowski's second main theorem includes a lower bound for the product of the successive minima. This is also true in the context of adèles provided that we modify our hypotheses on the sets $\mathcal{C}_v$ for complex v. Specifically, we must assume that

$$\mathcal{C}_v = \alpha\mathcal{C}_v \text{ for complex } v \text{ and all complex numbers } \alpha \text{ with } |\alpha| = 1. \tag{7.36}$$

For real v we continue to assume that $\mathcal{C}_v$ is symmetric in the sense that $\mathcal{C}_v = -\mathcal{C}_v$, but for complex v our previous requirement that $\mathcal{C}_v$ be symmetric will now be replaced by (7.36).

Theorem 7.11. *Let $\mathcal{C}$ be as in Theorem 7.10 but with the additional requirement that* (7.36) *holds. Then the successive minima $\lambda_1, \lambda_2, \dots, \lambda_n$ satisfy the inequality*

$$\frac{2^{dn}\pi^{nr_2}}{(n!)^{r_1}((2n)!)^{r_2}|D_{\kappa/\mathbb{Q}}|^{\frac{n}{2}}} \le (\lambda_1\lambda_2\cdots\lambda_n)^d V(\mathcal{C}), \tag{7.37}$$

where r_1 is the number of real places, r_2 is the number of complex places and $D_{\kappa/\mathbb{Q}}$ is the discriminant of κ.

Proof. Let $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(n)}$ and A be as in the proof of Theorem 7.10. For complex v, the set $\mathcal{C}_v A^{-1}$ also satisfies (7.36). Thus we may assume, as before, that $\mathbf{x}^{(j)} = e_j$ for $1 \le j \le n$. For each infinite place v we define

$$\mathcal{C}'_v = \left\{ \mathbf{t} \in \kappa_v^n \;\middle|\; \sum_{i=1}^{n} \lambda_i |t_i|_v < 1 \right\}.$$

Since $\lambda e_j \in \mathcal{C}_v$ if $\lambda > \lambda_j$, it follows easily from the convexity and symmetry of $\mathcal{C}_v$ that $\mathcal{C}'_v \subseteq \mathcal{C}_v$. If v is complex the condition of symmetry that we require is exactly (7.36). When we compute the Haar measure of $\mathcal{C}'_v$ we find that

$$\mu_v^n(\mathcal{C}'_v) = \begin{cases} \frac{2^n}{n!\lambda_1\lambda_2\cdots\lambda_n}, & \text{if } v \text{ is real,} \\ \frac{(4\pi)^n}{(2n)!(\lambda_1\lambda_2\cdots\lambda_n)^2}, & \text{if } v \text{ is complex.} \end{cases}$$

If v is a finite place, we know that $e_j \in \mathcal{C}_v$ for each j. As $\mathcal{C}_v$ is an $\mathcal{O}_v$-module it follows that $\mathcal{O}_v^n \subseteq \mathcal{C}_v$. Of course the Haar measure of $\mathcal{O}_v^n$ is $\mathcal{N}(\mathfrak{d}_v)^{-n/2}$.

Let $\mathcal{C}' \subseteq \kappa_{\mathbb{A}}^n$ be defined by

$$\mathcal{C}' = \prod_{v|\infty} \mathcal{C}'_v \times \prod_{v\nmid\infty} \mathcal{O}_v^n.$$

Then the Haar measure of $\mathcal{C}'$ is given by

$$V(\mathcal{C}') = \frac{2^{dn}\pi^{nr_2}}{(n!)^{r_1}((2n)!)^{r_2}(\lambda_1\lambda_2\cdots\lambda_n)^d} \prod_{v\nmid\infty} \mathcal{N}(\mathfrak{d}_v)^{-n/2}. \tag{7.38}$$

As $\mathcal{C}' \subseteq \mathcal{C}$ we have the inequality $V(\mathcal{C}') \le V(\mathcal{C})$. This observation together with (7.38) and

$$\prod_{v\nmid\infty} \mathcal{N}(\mathfrak{d}_v) = |D_{\kappa/\mathbb{Q}}|$$

establish the lower bound (7.37). □

7.3 Successive minima of a length function

Let κ be a number field and let S be a finite set of places of κ. Denote by $\mathcal{O}_{\kappa,S}$ the ring of S-*integers* of κ, i.e.,

$$\mathcal{O}_{\kappa,S} = \{z \in \kappa \mid \|z\|_\rho \le 1,\ \rho \notin S\}. \tag{7.39}$$

For each $v \in S$, let $L_{v,1}, \dots, L_{v,n}$ be n linearly independent linear forms with coefficients in κ, and let $A_{v,1}, \dots, A_{v,n}$ be positive real numbers with

$$\prod_{i=1}^{n} A_{v,i} = 1$$

for each $v \in S$. Set $d = [\kappa : \mathbb{Q}]$ and define a *length function* on κ^n

$$f(\mathbf{x}) = \Big(\prod_{v \in S} \max_{1 \le i \le n} A_{v,i} \|L_{v,i}(\mathbf{x})\|_v \Big)^{\frac{1}{d}}. \tag{7.40}$$

This length function satisfies the following conditions:

(i) $f(\mathbf{x}) \ge 0$ for all $\mathbf{x}$, and $f(\mathbf{x}) > 0$ for some $\mathbf{x}$;

(ii) $f(t\mathbf{x}) = \big(\prod_{v \in S} \|t\|_v \big)^{\frac{1}{d}} f(\mathbf{x})$.

Relative to this length function, following to Vojta [287] one can define the j-*th successive minima* of $\mathcal{O}_{\kappa,S}^n$ as the smallest real number λ_j such that $f(\mathbf{x}) \le \lambda_j$ for at leat j linearly independent points $\mathbf{x} \in \mathcal{O}_{\kappa,S}^n$. In the above, the words "linearly independent" mean linearly independent over κ, so that there are n successive minima.

Let $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}$ be a basis of κ^n with S-integral coordinates such that

$$f\big(\mathbf{x}^{(j)}\big) = \lambda_j,\ \ j = 1, \dots, n.$$

Since $f(\mathbf{x})$ is not affected when $\mathbf{x}$ is multiplied by an S-unit, we may assume the coordinates of $\mathbf{x}^{(j)}$ to be S-integers. Having fixed $\mathbf{x}^{(j)} = \big(x_1^{(j)}, \dots, x_n^{(j)}\big)$, define

$$\lambda_{v,j} = \max_{1 \le i \le n} A_{v,i} \big\| L_{v,i}\big(\mathbf{x}^{(j)}\big) \big\|_v$$

so that

$$\lambda_j^d = \prod_{v \in S} \lambda_{v,j}. \tag{7.41}$$

Lemma 7.12 ([287]). *Let L_v denote the coefficient matrix of $L_{v,1}, \dots, L_{v,n}$. Then*

$$\prod_{v \in S} \varsigma_v \big\| \det\big(x_i^{(j)}\big) \big\|_v \le (\lambda_1 \lambda_2 \cdots \lambda_n)^d \Big(\prod_{v \in S} \big\| \det L_v \big\|_v \Big)^{-1},$$

where

$$\varsigma_v = \begin{cases} 1, & \text{if } v \text{ is non-Archimedean,} \\ 1/n!, & \text{if } v \text{ is real,} \\ 2^n/(2n)!, & \text{if } v \text{ is complex.} \end{cases}$$

Proof. Using (7.41), the inequality can be proved by proving

$$\varsigma_v \big\| \det\left(x_i^{(j)}\right)\big\|_v \le \frac{\prod_{j=1}^n \lambda_{v,j}}{\|\det L_v\|_v} \tag{7.42}$$

for each $v \in S$ and then taking the product over all $v \in S$.

First assume that v is a real place, and let σ be the associated embedding of κ into $\mathbb{R}$. Then the points

$$\pm\frac{\sigma\left(\mathbf{x}^{(j)}\right)}{\lambda_{v,j}}, \quad j = 1, \dots, n, \tag{7.43}$$

lie in the symmetric body

$$\max_{1\le i\le n} A_{v,i}\,|L_{v,i}(\mathbf{x})| \le 1, \tag{7.44}$$

where $L_{v,i}$ is regarded as a form over $\mathbb{R}^n$ by applying σ to its coefficients. The convex body spanned by the points (7.43) lies inside the body (7.44). Since the volumes of these bodies are

$$\frac{2^n\big|\det\left(\sigma\left(x_i^{(j)}\right)\right)\big|}{n!\prod_j \lambda_{v,j}} = \frac{2^n\big\|\det\left(x_i^{(j)}\right)\big\|_v}{n!\prod_j \lambda_{v,j}}$$

and $2^n/\|\det L_v\|_v$, respectively, the inequality (7.42) follows immediately.

Next assume that v is complex. When $|w| \le 1$, the points

$$w\frac{\sigma\left(\mathbf{x}^{(j)}\right)}{\sqrt{\lambda_{v,j}}}, \quad j = 1, \dots, n,$$

lie inside the body (7.44). They span a convex body of volume

$$\frac{(2\pi)^n\big\|\det\left(x_i^{(j)}\right)\big\|_v}{(2n)!\prod_j \lambda_{v,j}}$$

which lies inside the body (7.44) having a volume $\pi^n/\|\det L_v\|_v$. Thus (7.42) holds.

Finally, assume that v is non-Archimedean. Again, this is a volume computation in κ_v using the volume of Mahler [162] (Section 7). The equivalent of (7.43) is now,

$$\left\{ a_1\frac{\sigma\left(\mathbf{x}^{(1)}\right)}{t^{f_1}} + \cdots + a_n\frac{\sigma\left(\mathbf{x}^{(n)}\right)}{t^{f_n}} \;\middle|\; a_j \in \mathcal{O}_v,\ 1 \le j \le n \right\},$$

where t is a uniformizing parameter for κ_v and f_j is an integer for which

$$\left\|t^{f_j}\right\|_v = \lambda_{v,j}, \;\; j = 1, \ldots, n.$$

According to Mahler [162] (Section 8), a linear transformation A changes volumes by a factor of $\|A\|_v$; therefore this body has volume

$$\frac{\left\|\det\left(x_i^{(j)}\right)\right\|_v}{\prod_j \lambda_{v,j}}.$$

It lies inside the body (7.44) which has volume $1/\|\det L_v\|_v$; thus (7.42) holds. □

If $v \in S$ is a finite place of κ, define

$$\mathcal{C}_v = \left\{ \mathbf{x} \in \mathcal{O}_v^n \;\middle|\; \max_{1 \le i \le n} A_{v,i} \|L_{v,i}(\mathbf{x})\|_v \le 1 \right\},$$

and set $\mathcal{C}_v = \mathcal{O}_v^n$ if $v \notin S$. For each infinite place v of κ, define

$$\mathcal{C}_\infty = \left\{ x \in \mathbb{R}^{nr_1} \times \mathbb{C}^{nr_2} \;\middle|\; \sum_{v|\infty} \max_{1 \le i \le n} A_{v,i} \|L_{v,i}^{\sigma_v}(\mathbf{x}_v)\|_v \le d \right\},$$

where $L_{v,i}^{\sigma_v}$ is the form obtained by applying the injection $\sigma_v : \kappa \longrightarrow \mathbb{C}$ to the coefficients of $L_{v,i}$, $\mathbf{x}_v$ are the components of $x = (\ldots, \mathbf{x}_v, \ldots)$ which lie in $\mathbb{R}^n$ or $\mathbb{C}^n$. Write

$$\mathcal{C} = \mathcal{C}_\infty \times \prod_{v \nmid \infty} \mathcal{C}_v.$$

This defines a convex subset of adelic n-space $\kappa_{\mathbb{A}}^n$; it remains only to compare the two notions of successive minima and volumes. Let $\mathbb{R}_+$ act on $\kappa_{\mathbb{A}}^n$ by dilation at the infinite places; it leaves the finite places alone. The *successive minima* relative to this action are

$$\nu_j = \min\{\nu > 0 \mid \nu\mathcal{C} \cap \kappa^n \text{ contains at least } j \text{ linearly independent vectors}\}.$$

First, we know that $\mathcal{C}_\infty$ is contained in the star-body

$$\left\{ x \in \mathbb{R}^{nr_1} \times \mathbb{C}^{nr_2} \;\middle|\; \prod_{v|\infty} \max_{1 \le i \le n} A_{v,i} \|L_{v,i}^{\sigma_v}(\mathbf{x}_v)\|_v \le 1 \right\}.$$

Thus, if $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$ are linearly independent points in κ^n for which $\mathbf{x}^{(j)} \in \nu_j \mathcal{C}$, then the length function satisfies

$$f\left(\mathbf{x}^{(j)}\right) \le \nu_j, \;\; j = 1, \ldots, n.$$

Thus

$$\lambda_j \le \nu_j, \ \ j = 1, \dots, n.$$

Let $C(r_1, r_2, n)$ be the volume of the solid in $\mathbb{R}^{nr_1} \times \mathbb{C}^{nr_2}$ given by

$$\left\{ x \in \mathbb{R}^{nr_1} \times \mathbb{C}^{nr_2} \ \Big| \ \sum_{v|\infty} \max_{1 \le i \le n} |x_{v,i}|^{n_v} \le d \right\},$$

where $\mathbf{x}_v = (x_{v,1}, \dots, x_{v,n})$, and $n_v = 1$ if v is real or $n_v = 2$ if v is complex. Then the volume $V(\mathcal{C})$ in the sense described at Section 7.2 is

$$V(\mathcal{C}) = |D_{\kappa/\mathbb{Q}}|^{-n/2} 2^{nr_2} C(r_1, r_2, n) \prod_{v \in S} \| \det L_v \|_v^{-1}.$$

Thus Theorem 7.10 implies

$$(\lambda_1 \lambda_2 \cdots \lambda_n)^d \le \frac{2^{n(r_1+r_2)} |D_{\kappa/\mathbb{Q}}|^{n/2} \prod_{v \in S} \| \det L_v \|_v}{C(r_1, r_2, n)}.$$

Combining this with Lemma 7.12 gives

Theorem 7.13. *Let $\lambda_1, \dots, \lambda_n$ denote the successive minima of $\mathcal{O}_{\kappa,S}^n$ with respect to the length function* (7.40)*. Then*

$$\left(\frac{1}{n!}\right)^{r_1} \left(\frac{2^n}{(2n)!}\right)^{r_2} \le \frac{(\lambda_1 \lambda_2 \cdots \lambda_n)^d}{\prod_{v \in S} \| \det L_v \|_v} \le \frac{2^{n(r_1+r_2)} |D_{\kappa/\mathbb{Q}}|^{n/2}}{C(r_1, r_2, n)}.$$

Davenport's lemma states:

Lemma 7.14. *Assume that the collection of all $L_{v,i}$, except for duplicates, lies in general position. Let $\Pi(A)$ denote the star-body with length function* (7.40) *and let $\lambda_1, \dots, \lambda_n$ be the successive minima of $\Pi(A)$. Assume that $\rho_1, \dots, \rho_n$ are positive real numbers with*

$$\rho_1 \ge \rho_2 \ge \cdots \ge \rho_n; \tag{7.45}$$

$$\rho_1 \lambda_1 \le \rho_2 \lambda_2 \le \cdots \le \rho_n \lambda_n; \tag{7.46}$$

$$\rho_1 \rho_2 \cdots \rho_n = 1. \tag{7.47}$$

Then for each $v \in S$ and each $1 \le i \le n$, there exists a real constant $\rho_{v,i}$ and constants c_1, c_2 depending only on κ, S, such that the successive minima $\hat{\lambda}_j$ of the length function

$$\hat{f}(\mathbf{x}) = \left(\prod_{v \in S} \max_{1 \le i \le n} \rho_{v,i} A_{v,i} \| L_{v,i}(\mathbf{x}) \|_v \right)^{\frac{1}{d}} \tag{7.48}$$

satisfy

$$c_1 \rho_j \lambda_j \le \hat{\lambda}_j \le c_2 \rho_j \lambda_j. \tag{7.49}$$

Also for each $v \in S$, we have

$$\rho_{v,1}\rho_{v,2}\cdots\rho_{v,n} = 1 \tag{7.50}$$

and

$$\max_{1\le i\le n} \rho_{v,i} = \rho_1^{n_v}, \tag{7.51}$$

where

$$n_v = \begin{cases} 0, & \text{if } v \text{ is non-Archimedean,} \\ 1, & \text{if } v \text{ is real,} \\ 2, & \text{if } v \text{ is complex.} \end{cases}$$

Proof. For convenience of notation, assume $A_{v,i} = 1$ for all v and i. Let $\mathbf{x}^{(j)}$ be a vector in $\mathcal{O}_{\kappa,S}^n$ such that

$$f\big(\mathbf{x}^{(j)}\big) = \lambda_j, \ \ j = 1, \ldots, n.$$

Scaling each $\mathbf{x}^{(j)}$ by some unit, we may assume that

$$c_3\lambda_j^{n_v} \le \max_{1\le i\le n} \left\| L_{v,i}\left(\mathbf{x}^{(j)}\right)\right\|_v \le c_4\lambda_j^{n_v}. \tag{7.52}$$

The constants c_3, c_4 depend only on κ and S.

For $1 \le j \le n$, let E^j be the subspace of κ^n spanned by $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(j)}$. For each $v \in M_\kappa^\infty$, the n linear forms $L_{v,i}$ satisfy a non-trivial linear relation

$$\alpha_{v,1}L_{v,1} + \cdots + \alpha_{v,n}L_{v,n} = 0$$

on E^{n-1}. Reorder the $L_{v,i}$ satisfying

$$\|\alpha_{v,n}\|_v = \max_{1\le i\le n} \|\alpha_{v,i}\|_v. \tag{7.53}$$

Hence when $\mathbf{x} \in E^{n-1}$,

$$L_{v,n}(\mathbf{x}) = -\sum_{i=1}^{n-1} \frac{\alpha_{v,i}}{\alpha_{v,n}} L_{v,i}(\mathbf{x}),$$

and further (7.53) implies

$$\|L_{v,n}(\mathbf{x})\|_v \le \sum_{i=1}^{n-1} \|L_{v,i}(\mathbf{x})\|_v.$$

Thus if $\mathbf{x} \in E^{n-1}$, one obtains

$$\sum_{i=1}^{n-1} \|L_{v,i}(\mathbf{x})\|_v \ge \frac{1}{2}\sum_{i=1}^{n} \|L_{v,i}(\mathbf{x})\|_v.$$

By induction, reorder the remaining $L_{v,i}$ so that on E^j,

$$\sum_{i=1}^{j} \|L_{v,i}(\mathbf{x})\|_v \geq \frac{1}{2^{n-j}} \sum_{i=1}^{n} \|L_{v,i}(\mathbf{x})\|_v. \tag{7.54}$$

Having permuted the $L_{v,i}$ in this manner, define

$$\rho_{v,i} = \rho_i^{n_v}, \quad v \in S, \ \ i = 1, \ldots, n.$$

These choices automatically satisfy (7.50) and (7.51). Now assume $\mathbf{x} \notin E^l$ for some l. Then, for some $j > l$, $\mathbf{x} \notin E^{j-1}$ but $\mathbf{x} \in E^j$. By using (7.45), then

$$\max_{1 \leq i \leq n} \rho_{v,i} \|L_{v,i}(\mathbf{x})\|_v \geq \rho_{v,j} \max_{1 \leq i \leq j} \|L_{v,i}(\mathbf{x})\|_v \geq \frac{\rho_{v,j}}{j} \sum_{i=1}^{j} \|L_{v,i}(\mathbf{x})\|_v,$$

Combining this with (7.54) gives

$$\max_{1 \leq i \leq n} \rho_{v,i} \|L_{v,i}(\mathbf{x})\|_v \geq \frac{\rho_{v,j}}{j2^{n-j}} \sum_{i=1}^{n} \|L_{v,i}(\mathbf{x})\|_v \geq \frac{\rho_{v,j}}{2^n} \max_{1 \leq i \leq n} \|L_{v,i}(\mathbf{x})\|_v,$$

which further yields

$$\max_{1 \leq i \leq n} \rho_{v,i} \|L_{v,i}(\mathbf{x})\|_v \geq \frac{c_3}{2^n} (\rho_j \lambda_j)^{n_v}$$

by using (7.52). Thus for all $\mathbf{x} \notin E^l$,

$$\hat{f}(\mathbf{x}) \geq c_1 \rho_j \lambda_j \geq c_1 \rho_l \lambda_l.$$

This proves the first half of (7.49). The second half follows from (7.47) and Theorem 7.13. □

Take non-negative integers a and b with $a \leq b$. Let $J_{1,a}^b$ be the set of all increasing injective mappings

$$\lambda : \mathbb{Z}[1, a] \longrightarrow \mathbb{Z}[1, b].$$

Let $V = \kappa^n$ be the vector space of dimension n over κ. For each $v \in S$, let $\alpha_{v,1}, \ldots, \alpha_{v,n}$ be vectors in the dual space V^* of V such that

$$L_{v,i}(\mathbf{x}) = \langle \mathbf{x}, \alpha_{v,i} \rangle, \quad \mathbf{x} \in V, \ \ i = 1, \ldots, n.$$

Take $\sigma \in J_{1,p}^n$ and set

$$\begin{aligned} B_{v,\sigma} &= \alpha_{v,\sigma(1)} \wedge \cdots \wedge \alpha_{v,\sigma(p)}, \\ A_{v,\sigma} &= A_{v,\sigma(1)} A_{v,\sigma(2)} \cdots A_{v,\sigma(n)}, \\ \lambda_\sigma &= \lambda_{\sigma(1)} \lambda_{\sigma(2)} \cdots \lambda_{\sigma(n)}. \end{aligned} \tag{7.55}$$

The vectors $B_{v,\sigma}$ define linear forms

$$L_{v,\sigma}(X) = \langle X, B_{v,\sigma} \rangle$$

on $\bigwedge_p V$, which are linearly independent.

Lemma 7.15. *Let* $\det(L_{v,i})$ *denote the determinant of the matrix of the coordinates of the vectors* $\alpha_{v,i}$*. Then*

$$\det(L_{v,\sigma}) = \det(L_{v,i})^{\binom{n-1}{p-1}}.$$

Proof. See Schmidt [231], Ch. IV, Lemma 6E. □

Lemma 7.16 ([287]). *With* $L_{v,\sigma}$ *and* $A_{v,\sigma}$ *as above, and* $X = \mathbf{x}^{(1)} \wedge \cdots \wedge \mathbf{x}^{(p)}$*, one has*

$$A_{v,\sigma} \|L_{v,\sigma}(X)\|_v \le \varsigma_v \prod_{j=1}^{p} \max_{1 \le i \le p} A_{v,\sigma(i)} \left\| L_{v,\sigma(i)}\big(\mathbf{x}^{(j)}\big) \right\|_v,$$

where

$$\varsigma_v = \begin{cases} 1, & \text{if } v \text{ is non-Archimedean,} \\ n!, & \text{if } v \text{ is real,} \\ (n!)^2, & \text{if } v \text{ is complex.} \end{cases}$$

Proof. Immediate from the definitions. □

Proposition 7.17 ([287]). *Order the* σ*'s so that*

$$\lambda_{\sigma_1} \le \cdots \le \lambda_{\sigma_N},$$

where $N = \binom{n}{p}$*. Let* $\nu_1, \ldots, \nu_N$ *be the successive minima of the system* $(A_{v,\sigma}, L_{v,\sigma})$*. Then for all* j*,*

$$\lambda_{\sigma_j} \ll \nu_j \ll \lambda_{\sigma_j}. \tag{7.56}$$

Moreover, $\sigma_1 = (1, 2, \ldots, p)$ *and* $\sigma_2 = (1, 2, \ldots, p-1, p+1)$*.*

Proof. Let f be the length function on κ^n defined by $L_{v,i}$ and $A_{v,i}$; let F be the length function on $\bigwedge_p \kappa^n$ defined by the corresponding $L_{v,\sigma}$ and $A_{v,\sigma}$. Let $\mathcal{O}_{\kappa,S}$ denote the ring of S-integers, and let $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$ be linearly independent vectors in $\mathcal{O}_{\kappa,S}^n$ with

$$f\big(\mathbf{x}^{(j)}\big) = \lambda_j, \;\; j = 1, \ldots, n.$$

Set

$$X^{(\sigma)} = \mathbf{x}^{(\sigma(1))} \wedge \cdots \wedge \mathbf{x}^{(\sigma(p))}, \;\; \sigma \in J_{1,p}^n.$$

Then

$$F\big(X^{(\sigma)}\big) \ll \prod_{i=1}^{p} f\big(\mathbf{x}^{(\sigma(i))}\big)$$

by Lemma 7.16. Since the vectors $X^{(\sigma)}$ are linearly independent, this gives the right-hand half of (7.56). The other half follows from Lemma 7.15, Theorem 7.13, and the fact that

$$\pi_\sigma \lambda_\sigma = (\pi_i \lambda_i)^{\binom{n-1}{p-1}}.$$

The final assertion in this proposition is trivial. □

7.4 Vojta's estimate

Let κ be a number field and let S be a finite set of places of κ. For each $v \in S$, let $L_{v,0}, L_{v,1}, \dots, L_{v,n}$ be $n+1$ linearly independent linear forms on $V = \kappa^{n+1}$ with coefficients in κ. Assume that the collection of all $L_{v,i}$, except for duplicates, lies in general position. To each point $P \in \mathbb{P}^n$ we assign homogeneous coordinates, obtaining a vector $\mathbf{x} \in \mathcal{O}_{\kappa,S}^{n+1}$. Let

$$\overline{H}(\mathbf{x}) = \prod_{v \in S} \|\mathbf{x}\|_v$$

denote the height of a vector $\mathbf{x} \in \mathcal{O}_{\kappa,S}^{n+1}$.

Theorem 7.18. *Let $C_{v,i}$ be a collection of real constants such that $\sum_i C_{v,i} = 0$ for each $v \in S$. Take $\varepsilon > 0$. Then there exists a finite set $\mathcal{T} \subseteq V$ such that if $\mathbf{x} \in \mathcal{O}_{\kappa,S}^{n+1}$ is a vector and $\mathbf{w}_1, \dots, \mathbf{w}_n \in (\mathcal{O}_{\kappa,S}^{n+1})^*$ is a basis for the subspace of V^* which is zero on $\mathbf{x}$, and if*

$$\|L_{v,i}(\mathbf{w}_j)\|_v \le \overline{H}(\mathbf{x})^{C_{v,i}-\varepsilon}, \quad v \in S,\ 0 \le i \le n,\ 1 \le j \le n,$$

then $\mathbf{x} \in \mathcal{T}$.

Proof. If $\mathcal{O}_{\kappa,S} = \mathbb{Z}$, then this is a consequence of Theorems 9A and 10B of Chapter VI of Schmidt [231]. The general case can be proved by essentially the same proof, but we omit the details. See Vojta [287], Theorem 6.4.1. □

Theorem 7.19. *Let ε and $L_{v,i}$ be as above. Let $c > 0$ be constant. Then there exists a finite set $\mathcal{T} \subseteq V$ such that if $\mathbf{x} \in \mathcal{O}_{\kappa,S}^{n+1}$ and $\mathbf{w}_1, \dots, \mathbf{w}_n \in (\mathcal{O}_{\kappa,S}^{n+1})^*$ are as above, such that*

$$\|L_{v,i}(\mathbf{w}_j)\|_v \le \overline{H}(\mathbf{x})^{c}, \quad v \in S,\ 0 \le i \le n,\ 1 \le j \le n;$$

and if

$$\prod_{v\in S}\prod_{i=0}^{n}\max_{1\le j\le n}\|L_{v,i}(\mathbf{w}_j)\|_v \le \overline{H}(\mathbf{x})^{-\varepsilon},$$

then $\mathbf{x}\in\mathcal{T}$.

Proof. This follows from Theorem 7.18 by a compactness argument. See Vojta [287], Theorem 6.4.2. □

Theorem 7.20 ([287]). *Let $\alpha_0,\dots,\alpha_q$ be a set of vectors in V^* in general position. Take $\varepsilon>0$. Then there exists a finite set $\mathcal{T}$ of V such that if $\mathbf{x}\in\mathcal{O}^{n+1}_{\kappa,S}$ is not a scalar multiple of some vector in $\mathcal{T}$, then there exists an $\mathbf{x}'\in\mathcal{O}^{n+1}_{\kappa,S}$ such that $\mathbf{x}\wedge\mathbf{x}'\neq 0$ and*

$$\log\sum_{v\in S}\frac{\|(\mathbf{x}\wedge\mathbf{x}')\angle\alpha_i\|_v}{\|\mathbf{x}\|_v\|\langle\mathbf{x},\alpha_i\rangle\|_v}\le\varepsilon\log\overline{H}(\mathbf{x})$$

for all $i=0,\dots,q$ for which $\langle\mathbf{x},\alpha_i\rangle\neq 0$. If $\langle\mathbf{x},\alpha_i\rangle=0$ then $\langle\mathbf{x}',\alpha_i\rangle=0$.

Proof. It will suffice to prove the theorem under the assumption that $\langle\mathbf{x},\alpha_i\rangle\neq 0$ for all i. Indeed, if $\langle\mathbf{x},\alpha_i\rangle=0$ for some i, then we can reduce to the subspace perpendicular to α_i and use induction on n. We first prove it with a weaker bound,

$$\prod_{v\in S}\frac{\|(\mathbf{x}\wedge\mathbf{x}')\angle\alpha_i\|_v}{\|\mathbf{x}\|_v\|\langle\mathbf{x},\alpha_i\rangle\|_v}\le\overline{H}(\mathbf{x})^{\varepsilon}. \tag{7.57}$$

Let $\mathcal{T}$ be the set of vectors for which (7.57) does not hold, and assume that the theorem is false; i.e. $\mathcal{T}$ is infinite. The strategy will be to apply the theory of successive minima to $V/\langle\mathbf{x}\rangle$, realized as $V\wedge\mathbf{x}\subseteq\bigwedge_2 V$. If no $\mathbf{x}'$ exists, then an appropriate first successive minimum is large; we then dualize and apply a few extra arguments to obtain the situation of Theorem 7.19.

Consider an infinite sequence of $\mathbf{x}$ for which no suitable $\mathbf{x}'$ exists. For each $v\in S$, $0\le i\le q$, and each $\mathbf{x}$ in the sequence, order the vectors α_i to get $\alpha_{v,i,\mathbf{x}}$ so that,

$$\|\langle\mathbf{x},\alpha_{v,0,\mathbf{x}}\rangle\|_v\le\cdots\le\|\langle\mathbf{x},\alpha_{v,q,\mathbf{x}}\rangle\|_v. \tag{7.58}$$

Passing to an infinite subsequence, we may assume $\alpha_{v,i}$ do not depend on $\mathbf{x}$. By assumption, for all $\mathbf{x}'\in\mathcal{O}^{n+1}_{\kappa,S}$ with $\mathbf{x}\wedge\mathbf{x}'\neq 0$,

$$\prod_{v\in S}\frac{\|(\mathbf{x}\wedge\mathbf{x}')\angle\alpha_{v,i}\|_v}{\|\mathbf{x}\|_v\|\langle\mathbf{x},\alpha_{v,i}\rangle\|_v}>\overline{H}(\mathbf{x})^{\varepsilon}$$

for some indices i depending on v and $\mathbf{x}'$. Applying Lemma 3.8, we have indices $j=j(v,\mathbf{x})$ such that

$$\prod_{v\in S}\frac{\|\langle\mathbf{x}\wedge\mathbf{x}',\alpha_{v,j}\wedge\alpha_{v,n}\rangle\|_v}{\|\mathbf{x}\|_v\|\langle\mathbf{x},\alpha_{v,i}\rangle\|_v}\gg\overline{H}(\mathbf{x})^{\varepsilon}. \tag{7.59}$$

On $V \wedge \mathbf{x} \subseteq \bigwedge_2 V$, consider the system of successive minima associated to the parallelepiped given by

$$L_{v,i}(\mathbf{x} \wedge \mathbf{x}') = \langle \mathbf{x} \wedge \mathbf{x}', \alpha_{v,i} \wedge \alpha_{v,n} \rangle, \ \ 0 \le i < n;$$
$$A_{v,i} = 1/\|\mathbf{x}\|_v \|\langle \mathbf{x}, \alpha_{v,i} \rangle\|_v, \ \ 0 \le i < n.$$

Set $d = [\kappa : \mathbb{Q}]$. By (7.59), we then have

$$\lambda_1^d \gg \overline{H}(\mathbf{x})^{\varepsilon}.$$

To compute the relative volume of $\alpha_{v,i} \wedge \alpha_{v,n}$ relative to the lattice $\mathcal{O}_{\kappa,S}^{n+1} \wedge \mathbf{x}$, let $x_0, \dots, x_n$ be the coordinates of $\mathbf{x}$ relative to the standard basis $\{e_i\}$, assume $x_0 \neq 0$. Then $\mathbf{x} \wedge e_1, \dots, \mathbf{x} \wedge e_n$ form a basis for a sublattice of $\mathcal{O}_{\kappa,S}^{n+1} \wedge \mathbf{x}$ of index $\prod_{v \in S} \|x_0\|_v$. Write

$$\xi_i = \mathbf{x} \wedge e_i, \quad \beta_{v,i} = \alpha_{v,n} \wedge \alpha_{v,i-1}$$

for $i = 1, \dots, n$. The volume $\mathcal{V}$ of the $\alpha_{v,i} \wedge \alpha_{v,n}$ relative to this sublattice is

$$\mathcal{V} = \prod_{v \in S} \|\langle \xi_1 \wedge \cdots \wedge \xi_n, \beta_{v,1} \wedge \cdots \wedge \beta_{v,n} \rangle\|_v^{-1}.$$

By Lemma 3.1, one obtains

$$\mathcal{V} = \left\{ \prod_{v \in S} \|\langle \mathbf{x}, \alpha_{v,n} \rangle\|_v^{n-1} \|\langle \mathbf{x} \wedge e_1 \wedge \cdots \wedge e_n, \alpha_{v,0} \wedge \cdots \wedge \alpha_{v,n} \rangle\|_v \right\}^{-1}.$$

Thus

$$\mathcal{V} \ll \left\{ \overline{H}(\mathbf{x})^{n-1} \prod_{v \in S} \|x_0\|_v \| \det \alpha_{v,i} \|_v \right\}^{-1} \ll \mathcal{V}.$$

Therefore, by Theorem 7.13,

$$(\lambda_1 \lambda_2 \cdots \lambda_n)^d \ll \overline{H}(\mathbf{x})^{n-1} \prod_{v,i} A_{v,i} \ll (\lambda_1 \lambda_2 \cdots \lambda_n)^d,$$

or equivalently,

$$(\lambda_1 \lambda_2 \cdots \lambda_n)^d \ll \frac{1}{\prod_v \prod_{i=0}^n \|\langle \mathbf{x}, \alpha_{v,i} \rangle\|_v} \ll (\lambda_1 \lambda_2 \cdots \lambda_n)^d.$$

We now apply Davenport's lemma with $\rho_i = \rho/\lambda_i$, choosing ρ so that

$$\rho_1 \rho_2 \cdots \rho_n = 1.$$

This gives constants $\rho_{v,i}$ such that the successive minima $\hat{\lambda}_j$ relative to

$$\hat{f}(\mathbf{x}) = \left(\prod_{v \in S} \max_{0 \le i \le n-1} \rho_{v,i} A_{v,i} \| \langle \mathbf{x} \wedge \mathbf{x}', \alpha_{v,i} \wedge \alpha_{v,n} \rangle \|_v \right)^{\frac{1}{d}}$$

satisfy

$$\hat{\lambda}_j \ll \left\{ \prod_{v \in S} \prod_{i=0}^{n} \| \langle \mathbf{x}, \alpha_{v,i} \rangle \|_v \right\}^{-\frac{1}{nd}} \ll \hat{\lambda}_j.$$

From (7.51), we also have

$$\rho_{v,i} \ll \left(\frac{\hat{\lambda}_1}{\lambda_1} \right)^{n_v}, \quad v \in S, \ 0 \le i < n,$$

and so

$$\rho_{v,i} \ll \left\{ \overline{H}(\mathbf{x})^{-\varepsilon} \prod_{v \in S} \prod_{i=0}^{n} \| \langle \mathbf{x}, \alpha_{v,i} \rangle \|_v^{-1/n} \right\}^{\frac{n_v}{d}}; \tag{7.60}$$

$$\prod_{v \in S} \max_{0 \le i < n} \rho_{v,i} \ll \overline{H}(\mathbf{x})^{-\varepsilon} \prod_{v \in S} \prod_{i=0}^{n} \| \langle \mathbf{x}, \alpha_{v,i} \rangle \|_v^{-1/n}. \tag{7.61}$$

We now apply Proposition 7.17 to $\bigwedge_{n-1}(\mathbf{x} \wedge V)$. This is isomorphic to the dual of $V/\langle \mathbf{x} \rangle$, i.e. the subspace of V^* consisting of those forms vanishing at $\mathbf{x}$. By Proposition 7.17, the successive minima $\mu_1, \dots, \mu_n$ satisfy

$$\mu_j \ll \left\{ \prod_{v \in S} \prod_{i=0}^{n} \| \langle \mathbf{x}, \alpha_{v,i} \rangle \|_v \right\}^{-\frac{n-1}{nd}} \ll \mu_j.$$

Thus there exists a basis $\Xi_1, \dots, \Xi_n$ of a full sublattice of the lattice $\bigwedge_{n-1}(\mathbf{x} \wedge \mathcal{O}_{\kappa,S}^{n+1})$ such that, after scaling each Ξ_i by a unit, vectors

$$\Phi_{v,m} = \beta_{v,1} \wedge \cdots \wedge \beta_{v,m-1} \wedge \beta_{v,m+1} \wedge \cdots \wedge \beta_{v,n}$$

satisfy

$$\begin{aligned}
\| \langle \Xi_j, \Phi_{v,m} \rangle \|_v &\ll \left(\prod_{i=0}^{n} \| \langle \mathbf{x}, \alpha_{v,i} \rangle \|_v \right)^{-\frac{n-1}{n}} \prod_{\substack{0 \le i \le n-1 \\ i \ne m}} \frac{\rho_{v,i}}{A_{v,i}} \\
&\ll \left(\prod_{i=0}^{n} \| \langle \mathbf{x}, \alpha_{v,i} \rangle \|_v \right)^{-\frac{n-1}{n}} \| \mathbf{x} \|_v^{n-1} \prod_{\substack{0 \le i \le n-1 \\ i \ne m}} \| \langle \mathbf{x}, \alpha_{v,i} \rangle \|_v \rho_{v,i} \\
&\ll \frac{\| \mathbf{x} \|_v^{n-2} \rho_{v,m}}{\| \langle \mathbf{x}, \alpha_{v,m} \rangle \|_v} \prod_{i=0}^{n} \| \langle \mathbf{x}, \alpha_{v,i} \rangle \|_v^{1/n}
\end{aligned} \tag{7.62}$$

since

$$\|\mathbf{x}\|_v \ll \|\langle \mathbf{x}, \alpha_{v,n}\rangle\|_v \ll \|\mathbf{x}\|_v;$$

$$\prod_i \rho_{v,i} = 1, \ \ v \in S.$$

We can write Ξ_j as a finite sum

$$\Xi_j = \sum_{l \in I_j} (\mathbf{x} \wedge \eta_{l1}) \wedge \cdots \wedge (\mathbf{x} \wedge \eta_{l,n-1})$$

with $\eta_{li} \in \mathcal{O}_{\kappa,S}^{n+1}$. By Lemma 3.1, one has

$$\langle \Xi_j, \Phi_{v,m}\rangle = (-1)^{n-1}\langle \mathbf{x}, \alpha_{v,n}\rangle^{n-2}\langle \mathbf{x} \wedge \Theta_j, \Psi_{v,m}\rangle, \tag{7.63}$$

where

$$\Theta_j = \sum_{l \in I_j} \eta_{l1} \wedge \cdots \wedge \eta_{l,n-1} \in \bigwedge_{n-1} \mathcal{O}_{\kappa,S}^{n+1},$$

$$\Psi_{v,m} = \alpha_{v,0} \wedge \cdots \wedge \alpha_{v,m-1} \wedge \alpha_{v,m+1} \wedge \cdots \wedge \alpha_{v,n}.$$

Note that $\mathbf{x} \wedge \Theta_j$ are linearly independent vectors spanning a full sublattice

$$\left\{ \alpha \in \left(\mathcal{O}_{\kappa,S}^{n+1}\right)^* \mid \langle \mathbf{x}, \alpha\rangle = 0 \right\}.$$

Combining (7.62) and (7.63) gives

$$\|\langle \mathbf{x} \wedge \Theta_j, \Psi_{v,m}\rangle\|_v \ll \frac{\rho_{v,m}}{\|\langle \mathbf{x}, \alpha_{v,m}\rangle\|_v} \prod_{i=0}^{n} \|\langle \mathbf{x}, \alpha_{v,i}\rangle\|_v^{1/n}; \tag{7.64}$$

$$\prod_{v \in S} \prod_{m=0}^{n-1} \max_{1 \le j \le n} \|\langle \mathbf{x} \wedge \Theta_j, \Psi_{v,m}\rangle\|_v \ll \prod_{v \in S} \|\langle \mathbf{x}, \alpha_{v,n}\rangle\|_v. \tag{7.65}$$

In order to apply Theorem 7.19, we need a bound for $\|\langle \mathbf{x} \wedge \Theta_j, \Psi_{v,n}\rangle\|_v$. Note that $\bigwedge_n V^* \cong V$, where $\{\Psi_{v,0}, \ldots, \Psi_{v,n}\}$ is the dual basis to $\{\alpha_{v,0}, \ldots, \alpha_{v,n}\}$. Since

$$\Psi_{v,n} \equiv -\frac{1}{\det(\alpha_{v,i})} \sum_{i=0}^{n-1} \frac{\langle \mathbf{x}, \alpha_{v,i}\rangle}{\langle \mathbf{x}, \alpha_{v,n}\rangle} \Psi_{v,i} \ (\mathrm{mod}\ \mathbf{x}),$$

with (7.64) this gives

$$\|\langle \mathbf{x} \wedge \Theta_j, \Psi_{v,n}\rangle\|_v \ll \frac{1}{\|\langle \mathbf{x}, \alpha_{v,n}\rangle\|_v} \left(\prod_{i=0}^{n} \|\langle \mathbf{x}, \alpha_{v,i}\rangle\|_v^{1/n} \right) \max_{0 \le i < n} \rho_{v,i}. \tag{7.66}$$

Further, by (7.61), one has

$$\prod_{v\in S}\max_{1\le j\le n}\|\langle \mathbf{x}\wedge\Theta_j,\Psi_{v,n}\rangle\|_v \ll \left\{\overline{H}(\mathbf{x})^{\varepsilon}\prod_{v\in S}\|\langle \mathbf{x},\alpha_{v,n}\rangle\|_v\right\}^{-1}. \tag{7.67}$$

Combining this with (7.65) gives

$$\prod_{v\in S}\prod_{m=0}^{n}\max_{1\le j\le n}\|\langle \mathbf{x}\wedge\Theta_j,\Psi_{v,m}\rangle\|_v \ll \overline{H}(\mathbf{x})^{-\varepsilon}.$$

Thus the second condition of Theorem 7.19 holds.

To show that the first condition also holds, we first check that if $\langle \mathbf{x},\alpha_{v,i}\rangle\neq 0$, then

$$\|\langle \mathbf{x},\alpha_{v,i}\rangle\|_v \gg \|\mathbf{x}\|_v/\overline{H}(\mathbf{x}). \tag{7.68}$$

We obtain this by a Liouville type argument, as follows. Since $\mathbf{x}$ has integral coordinates relative to the standard basis and $\alpha_{v,i}$ is one of finitely many vectors, we have

$$\prod_{w\in S}\|\langle \mathbf{x},\alpha_{v,i}\rangle\|_w \gg 1;$$

also, if $w\neq v$, then

$$\|\langle \mathbf{x},\alpha_{v,i}\rangle\|_w \ll \|\mathbf{x}\|_w.$$

Dividing these two relations gives (7.68). Combining (7.68) with (7.60) gives

$$\rho_{v,i}\ll\prod_{w\in S}\left(\frac{\overline{H}(\mathbf{x})}{\|\mathbf{x}\|_w}\right)^{\frac{(n+1)n_v}{nd}} = \overline{H}(\mathbf{x})^{\frac{(n+1)n_v}{nd}(\#S-1)};$$

with (7.64) and (7.66) this becomes

$$\|\langle \mathbf{x}\wedge\Theta_j,\Psi_{v,m}\rangle\|_v \ll \frac{\|\mathbf{x}\|_v}{\overline{H}(\mathbf{x})}\|\mathbf{x}\|_v^{\frac{n+1}{n}}\overline{H}(\mathbf{x})^{\frac{(n+1)n_v}{nd}(\#S-1)}.$$

This now implies the first condition of Theorem 7.19, provided that

$$\|\mathbf{x}\|_v \ll \overline{H}(\mathbf{x}).$$

It is no loss of generality to assume this, because it always holds after multiplying $\mathbf{x}$ by an appropriate unit u, and (7.57) is unaffected by this change.

Thus our infinite sequence of $\mathbf{x}$'s satisfies both conditions of Theorem 7.19, a contradiction. We have show the existence of a vector $\mathbf{x}'$ for almost all $\mathbf{x}$, such that (7.57) holds. To obtain the theorem from this, multiply $\mathbf{x}'$ by a scalar unit, making all factors of (7.57) have the same order of magnitude. Then Theorem 7.20 follows (with a different ε). □

7.5 Schmidt subspace theorem

Following Vojta [287], we introduce simply Schmidt subspace theorem, and compare the analogy with Cartan's second main theorem.

7.5.1 Subspace theorem

Let κ be a number field and let S be a finite subset of M_κ. Let $V = V_\kappa$ be a vector space of finite dimension $n+1 > 0$ over κ. We state the *Schmidt subspace theorem* as follows (W. M. Schmidt [230], J. -H. Evertse and H. P. Schlickewei [61]):

Theorem 7.21. *Take $\varepsilon > 0$. Assume that for each $\rho \in S$, the family*

$$\{a_{\rho,0}, \ldots, a_{\rho,n}\} \subset \mathbb{P}(V^*)$$

is in general position. Then there exists a finite set $\{b_1, \ldots, b_s\}$ of $\mathbb{P}(V^*_{\bar\kappa})$ such that the set of solutions $x \in \mathbb{P}(V)$ of

$$\prod_{\rho\in S}\prod_{j=0}^{n} |||x, a_{\rho,j}|||_\rho < \frac{1}{H(x)^{n+1+\varepsilon}}$$

is contained in $\bigcup_i \ddot{E}[b_i]$.

It is possible to obtain quantitative version of the subspace theorem, in which we control the number of subspaces containing all solutions of height exceeding a certain bound. In fact, J. -H. Evertse and H. P. Schlickewei [61] have obtained a strong result of this type.

Take a basis $e = (e_0, \ldots, e_n)$ of V. We will identify $V \cong \mathbb{A}^{n+1}(\kappa)$ by the correspondence relation

$$\xi_0 e_0 + \cdots + \xi_n e_n \in V \longmapsto (\xi_0, \ldots, \xi_n) \in \mathbb{A}^{n+1}(\kappa),\ \ \xi_j \in \kappa.$$

A point $\xi = \xi_0 e_0 + \cdots + \xi_n e_n \in V$ is said to be a *S-integral point* if $\xi_i \in \mathcal{O}_{\kappa,S}$ for all $0 \le i \le n$. An algebraic point $\xi \in V_{\bar\kappa}$ should be *integral* if its coordinates lie in the integral closure of $\mathcal{O}_{\kappa,S}$ in $\bar\kappa$. Denote by $\mathcal{O}_{V,S}$ the set of *S-integral points* of V, that is,

$$\mathcal{O}_{V,S} = \{\xi \in V \mid \|\xi\|_\rho \le 1,\ \ \rho \notin S\}. \tag{7.69}$$

According to the identity $V \cong \mathbb{A}^{n+1}(\kappa)$, we have

$$\mathcal{O}_{V,S} \cong \mathcal{O}^{n+1}_{\kappa,S}. \tag{7.70}$$

Similarly, an affine variety $Z \subset \mathbb{A}^{n+1}$ defined over κ inherits a notion of integral point from the definition for $\mathbb{A}^{n+1}$. The following affine version of the subspace theorem is worth noting.

Theorem 7.22. *Let κ, S be as before with S containing the set M_κ^∞. For $\rho \in S$, $i \in \{0, \dots, n\}$, take $\alpha_{\rho,i} \in V^* - \{0\}$ such that for each $\rho \in S$, $\alpha_{\rho,0}, \dots, \alpha_{\rho,n}$ are linearly independent. Fix $\varepsilon > 0$. Let Q be the set of all $\xi \in \mathcal{O}_{V,S}$ satisfying*

$$\prod_{\rho \in S} \prod_{i=0}^{n} \|\langle \xi, \alpha_{\rho,i} \rangle\|_\rho < \Big(\max_{\rho \in S} \|\xi\|_\rho \Big)^{-\varepsilon}.$$

Then Q is contained in a finite union of hyperplanes of V.

Theorem 7.22 is due to Schmidt ([230], [231]) for the Archimedean case and Schlickewei ([227], [228], [229]) in non-Archimedean cases. The following general form of Subspace Theorem 7.21 will turn out to be equivalent to Theorem 7.22 (see [232], [287], [103] or Section 7.7):

Theorem 7.23. *Let κ, S be as before with S containing the set M_κ^∞. Take $\varepsilon > 0$, $q \geq n$. Assume that for each $\rho \in S$, the family*

$$\mathscr{A}_\rho = \{a_{\rho,0}, \dots, a_{\rho,q}\} \subset \mathbb{P}(V^*)$$

is in general position. Then there exists a finite set $\{b_1, \dots, b_s\}$ of $\mathbb{P}(V_{\bar{\kappa}}^*)$ such that the inequality

$$\sum_{\rho \in S} \sum_{j=0}^{q} \log \frac{1}{|||x, a_{\rho,j}|||_\rho} < (n + 1 + \varepsilon) h(x)$$

holds for all $x \in \mathbb{P}(V) - \bigcup_i \ddot{E}[b_i]$.

A. J. van der Poorten [281] generalized an idea of Schlickewei [228] to obtain the following result:

Theorem 7.24. *Let κ be a number field and let $n \geq 1$ be an integer. Let Γ be a finitely generated subgroup of κ_*. Then all but finitely many solutions of the equation*

$$u_0 + u_1 + \cdots + u_n = 1, \;\; u_i \in \Gamma, \tag{7.71}$$

lie in one of the diagonal hyperplanes H_I defined by the equation $\sum_{i \in I} x_i = 0$, where I is a subset of $\{0, 1, \dots, n\}$ with at least two, but no more than n, elements.

The proof is referred to Vojta [287]. Further, Vojta noted that such infinite families are restricted to finite unions of linear subspaces of dimension $\leq [n/2]$.

A straightforward calculation will show that Theorem 7.22 implies Roth's theorem. In fact, Roth's theorem can be restated in the following symmetric form.

Theorem 7.25. *Let $L_0(x, y) = \alpha x + \beta y$ and $L_1(x, y) = \gamma x + \delta y$ be linearly independent linear forms with algebraic coefficients. Then, for every $\varepsilon > 0$, the inequalities*

$$0 < |L_0(x, y) L_1(x, y)| < \max\{|x|, |y|\}^{-\varepsilon}$$

have only finitely many solutions in integers x, y.

Proof. Theorem 7.25 implies Roth's Theorem 6.1, since the inequality in Roth's Theorem 6.1 implies

$$|y|\,|\alpha y - x| < y^{-\varepsilon}.$$

Essentially this is the same as

$$|y|\,|\alpha y - x| < \max\{|x|, |y|\}^{-\varepsilon}. \tag{7.72}$$

Notice that in (7.72) we have on the left hand side the product of the absolute values of the two linear forms

$$L_0(x, y) = x - \alpha y, \quad L_1(x, y) = y.$$

On the other hand, Roth's Theorem 6.1 implies Theorem 7.25 by the following argument. Assume $|L_1(x, y)| \geq |L_0(x, y)|$. We have

$$|L_0(x, y)| \gg |y| \left| \frac{x}{y} + \frac{\beta}{\alpha} \right|$$

and

$$|L_1(x, y)| \gg |\gamma L_0(x, y) - \alpha L_1(x, y)| = |\alpha\delta - \beta\gamma||y| \gg |y|.$$

Hence

$$\left| -\frac{\beta}{\alpha} - \frac{x}{y} \right| \ll \frac{1}{|y|^2} |L_0(x, y) L_1(x, y)| < \frac{1}{|y|^{2+\varepsilon}},$$

so there can be only finitely many solutions x/y. □

Theorem 6.2 is the special case $n = 1$ of the Subspace Theorem 7.21. It states that, given κ and S as above and given algebraic numbers $a_\rho \in \bar{\kappa}$ for $\rho \in S$, the inequality

$$\prod_{\rho \in S} \min\{1, |||y - a_\rho|||_\rho\} < \frac{1}{H_*(y)^{2+\varepsilon}} \tag{7.73}$$

has only finitely many solution $y \in \kappa$. Note that, by splitting the solutions of (7.73) into finitely many subsets according to the places $\rho \in S$ for which $|||y - a_\rho|||_\rho < 1$, we see immediately that (7.73) is equivalent to the statement that the solutions to

$$\prod_{\rho \in S^*} |||y - a_\rho|||_\rho < \frac{1}{H_*(y)^{2+\varepsilon}}, \quad |||y - a_\rho|||_\rho < 1 \ \ (\rho \in S^*) \tag{7.74}$$

form a finite set for any subset S^* of S.

Take $\xi = \xi_0 e_0 + \xi_1 e_1 \in V$ such that $x = \mathbb{P}(\xi) = [1, y]$ with $y = \xi_1/\xi_0$ and take

$$a_{\rho,i} = \mathbb{P}(\alpha_{\rho,i}) \in \mathbb{P}(V^*) \ \ (i = 0, 1)$$

such that

$$\langle \xi, \alpha_{\rho,0} \rangle = \xi_0, \quad \langle \xi, \alpha_{\rho,1} \rangle = \xi_1 - a_\rho \xi_0.$$

Then $|\alpha_{\rho,0}|_\rho = 1$, and so

$$|x, a_{\rho,0}|_\rho |x, a_{\rho,1}|_\rho = \frac{|y - a_\rho|_\rho}{|\alpha_{\rho,1}|_\rho} \max\{1, |y|_\rho\}^{-2}.$$

Now if $|y - a_\rho|_\rho < 1$, we obtain $|y| < 1 + |a_\rho|_\rho$ and $\max\{1, |y|_\rho\}$ is bounded above independently of y. Therefore, if (7.74) holds, we also have

$$\prod_{\rho \in S^*} |||x, a_{\rho,0}|||_\rho |||x, a_{\rho,1}|||_\rho < \frac{C}{H(x)^{2+\varepsilon}}$$

for some constant C. Thus by Northcott's Theorem 4.29, we obtain

$$C < H(x)^{\varepsilon/2} = H_*(y)^{\varepsilon/2}$$

except for finitely many $y \in \kappa$. Hence we may apply the Subspace Theorem 7.21 with $n = 1$ and $\varepsilon/2$ in place of ε and conclude that the solutions y of (7.74) form a finite set, and so Theorem 6.2 follows.

7.5.2 Proof of subspace theorem

Let κ be a number field and let S be a finite subset of M_κ containing the set M_κ^∞. Let $V = V_\kappa$ be a vector space of finite dimension $n + 1 > 0$ over κ.

Theorem 7.26 ([287]). *Let $\alpha_0, \dots, \alpha_q$ be a set of vectors in V^* in general position. Take $\varepsilon > 0$. Then there exists a finite set $\mathcal{T}$ of V with the following property. Assume that $\alpha_{v,0}, \dots, \alpha_{v,n}$ are distinct elements of $\{\alpha_0, \dots, \alpha_q\}$ for each $v \in S$ and assume that $A_{v,i}$ are positive real constants as in Section 7.3. Let $\lambda_0, \dots, \lambda_n$ be the successive minima relative to the length function*

$$f(\mathbf{x}) = \Big(\prod_{v \in S} \max_{0 \le i \le n} A_{v,i} \|\langle \mathbf{x}, \alpha_{v,i} \rangle\|_v \Big)^{\frac{1}{[\kappa:\mathbb{Q}]}}. \tag{7.75}$$

Then either $f(\mathbf{x}) = \lambda_0$ for some $\mathbf{x} \in \kappa\mathcal{T} \cap \mathcal{O}_{\kappa,S}^{n+1}$, or $\lambda_1 < \lambda_0 H(\mathbf{x})^\varepsilon$.

Proof. Let $\mathcal{T}$ be as Theorem 7.20. Let $\mathbf{x} \in \mathcal{O}_{\kappa,S}^{n+1}$ be such that $f(\mathbf{x}) = \lambda_0$. Assume that $\mathbf{x} \notin \kappa\mathcal{T}$. Then by Theorem 7.20, there exists a vector $\mathbf{x}'$ such that

$$\sum_{v \in S} \frac{\|(\mathbf{x} \wedge \mathbf{x}') \angle \alpha_i\|_v}{\|\mathbf{x}\|_v \|\langle \mathbf{x}, \alpha_i \rangle\|_v} \le H(\mathbf{x})^\varepsilon \tag{7.76}$$

if $\langle \mathbf{x}, \alpha_i \rangle \neq 0$, and $\langle \mathbf{x}', \alpha_i \rangle = 0$ if $\langle \mathbf{x}, \alpha_i \rangle = 0$.

Here $\mathbf{x}'$ is only determined modulo $\mathbf{x}$; let us choose one $\mathbf{x}' \in \mathcal{O}_{\kappa,S}^{n+1}$. For each $v \in S$, permute the vectors $\alpha_{v,i}$ such that

$$\|\langle \mathbf{x}, \alpha_{v,0} \rangle\|_v \le \cdots \le \|\langle \mathbf{x}, \alpha_{v,n} \rangle\|_v. \tag{7.77}$$

It is an elementary fact of number theory that there exists a constant c_1, depending only on κ, such that given constants $a_v \in \kappa_v$ for each $v \in S$, there exists $a \in \mathcal{O}_{\kappa,S}$ such that

$$\|a - a_v\|_v < c_1$$

for each $v \in S$ (cf. Theorem 1.88). Applying this fact with

$$a_v = \frac{\langle \mathbf{x}', \alpha_{v,n} \rangle}{\langle \mathbf{x}, \alpha_{v,n} \rangle},$$

we replace $\mathbf{x}'$ with $\mathbf{x}' - a\mathbf{x}$, so that

$$\|\langle \mathbf{x}', \alpha_{v,n} \rangle\|_v < c_1 \|\langle \mathbf{x}, \alpha_{v,n} \rangle\|_v. \tag{7.78}$$

But

$$\|\langle \mathbf{x} \wedge \mathbf{x}', \alpha_i \wedge \alpha_{v,n} \rangle\|_v \ll \|(\mathbf{x} \wedge \mathbf{x}') \angle \alpha_i\|_v.$$

By (7.76), one obtains

$$\|(\mathbf{x} \wedge \mathbf{x}') \angle \alpha_i\|_v \ll H(\mathbf{x})^{\varepsilon} \|\mathbf{x}\|_v \|\langle \mathbf{x}, \alpha_i \rangle\|_v.$$

Combining this with (7.77), one has

$$\|\langle \mathbf{x} \wedge \mathbf{x}', \alpha_i \wedge \alpha_{v,n} \rangle\|_v \ll H(\mathbf{x})^{\varepsilon} \|\langle \mathbf{x}, \alpha_{v,n} \rangle\|_v \|\langle \mathbf{x}, \alpha_i \rangle\|_v.$$

Note that

$$\|\langle \mathbf{x}', \alpha_i \rangle \langle \mathbf{x}, \alpha_{v,n} \rangle\|_v \le \|\langle \mathbf{x} \wedge \mathbf{x}', \alpha_i \wedge \alpha_{v,n} \rangle\|_v + \|\langle \mathbf{x}, \alpha_i \rangle \langle \mathbf{x}', \alpha_{v,n} \rangle\|_v.$$

Hence by (7.78),

$$\|\langle \mathbf{x}', \alpha_i \rangle\|_v \ll (H(\mathbf{x})^{\varepsilon} + c_1) \|\langle \mathbf{x}, \alpha_i \rangle\|_v \ll H(\mathbf{x})^{\varepsilon} \|\langle \mathbf{x}, \alpha_i \rangle\|_v$$

unless $H(\mathbf{x})$ is small. Enlarging $\mathcal{T}$ to eliminate this possibility, one has

$$f(\mathbf{x}') \ll H(\mathbf{x})^{\varepsilon} f(\mathbf{x}).$$

Thus,

$$\lambda_1 \ll \lambda_0 H(\mathbf{x})^{\varepsilon}$$

(with a different ε), as was to be shown. □

Theorem 7.27 ([287]). *Let $\alpha_0, \dots, \alpha_q$ be a set of vectors in V^* in general position. Take $\varepsilon > 0$ and let $0 \le p \le n-1$. Then there exists a finite set $\mathcal{T}_{p+1}$ of $(p+1)$-dimensional linear subspaces of V with the following property. Let $\alpha_{v,i}, A_{v,i}$, and $\lambda_0, \dots, \lambda_n$ be as in Theorem 7.26. Assume that $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(n)}$ are linearly independent vectors in $\mathcal{O}_{\kappa,S}^{n+1}$ satisfying $f\left(\mathbf{x}^{(j)}\right) = \lambda_j$. Then either*

$$\left\langle \mathbf{x}^{(0)}, \dots, \mathbf{x}^{(p)} \right\rangle \in \mathcal{T}_{p+1},$$

or

$$\lambda_{p+1} < H\left(\mathbf{x}^{(0)} \wedge \cdots \wedge \mathbf{x}^{(p)}\right)^{\varepsilon} \lambda_p.$$

Proof. For $\sigma \in J_p^n$, define $B_{v,\sigma}$ and $A_{v,\sigma}$ as in (7.55). Let $\nu_1, \dots, \nu_{\binom{n+1}{p+1}}$ denote the successive minima of the associated length function on $\bigwedge_{p+1} V$. By Proposition 7.17 and Theorem 7.26,

$$\frac{\lambda_{p+1}}{\lambda_p} \ll \frac{\nu_2}{\nu_1} < H\big(\mathbf{x}^{(0)} \wedge \cdots \wedge \mathbf{x}^{(p)}\big)^{\varepsilon},$$

unless $\mathbf{x}^{(0)} \wedge \cdots \wedge \mathbf{x}^{(p)}$ is a scalar multiple of some element of the finite set $\mathcal{T} \subseteq \bigwedge_{p+1} V$. Let $\mathcal{T}_{p+1}$ be the collection of subspaces of V corresponding to decomposable elements of $\mathcal{T}$. Then the conditions in the theorem hold. □

We will be applying this theorem to the successive minimum problem defined by the length function (7.75), where $\alpha_{v,i}$ are chosen such that

$$\|\langle \mathbf{x}, \alpha_{v,0}\rangle\|_v \le \cdots \le \|\langle \mathbf{x}, \alpha_{v,q}\rangle\|_v \tag{7.79}$$

and

$$A_{v,i} = \frac{A_v}{\|\langle \mathbf{x}, \alpha_{v,i}\rangle\|_v}, \tag{7.80}$$

where A_v is chosen such that

$$\prod_{i=0}^{n} A_{v,i} = 1$$

for all $v \in S$.

Lemma 7.28. *Let $\lambda_0, \dots, \lambda_n$ be the successive minima of the length function defined by* (7.75), (7.79) *and* (7.80). *Let $\mathbf{x}^{(0)}, \dots, \mathbf{x}^{(n)}$ be linearly independent lattice points with $f\left(\mathbf{x}^{(j)}\right) = \lambda_j$. Then there exists constants c_p, $0 \le p \le n-1$, such that*

$$h\big(\mathbf{x}^{(0)} \wedge \cdots \wedge \mathbf{x}^{(p)}\big) < c_p h(\mathbf{x}) + O(1),$$

where the constants c_p depend only on κ, n and p, and the constant in $O(1)$ depends only on κ, n, p and the α_i.

Proof. We have

$$\begin{aligned} h\big(\mathbf{x}^{(0)} \wedge \cdots \wedge \mathbf{x}^{(p)}\big) &\le \sum_{i=0}^{p} h\big(\mathbf{x}^{(i)}\big) + O(1) \\ &\le \sum_{i=0}^{p} \log \lambda_i + \frac{p}{[\kappa : \mathbb{Q}]} \log \max_{0 \le i \le n} A_{v,i} + O(1). \end{aligned}$$

By Theorem 7.13, the first term is negative; it then suffices to show that

$$\sum_{v \in S} \log \max A_{v,i} < c_p' h(\mathbf{x}) + O(1).$$

But this follows from the definition of $A_{v,i}$ and the Liouville estimate (7.68)

$$\frac{\|\mathbf{x}\|_v}{H(\mathbf{x})} \ll \|\langle \mathbf{x}, \alpha_i \rangle\|_v \ll \|\mathbf{x}\|_v. \qquad \square$$

Proof. [Proof of Theorem 7.23] We start with a sequence of vectors $\mathbf{x}$, and immediately throw out all $\mathbf{x}$ such that $\langle \mathbf{x}, \alpha_i \rangle = 0$ for any i, or such that $\mathbf{x}$ lies in one of the subspaces in one of the $\mathcal{T}_{p+1}$. This eliminates only finitely many hyperplanes; we will show that all remaining vectors satisfy the theorem, i.e.

$$\sum_{j=0}^{q} m(x, a_j) \leq (n + 1 + \varepsilon)h(x) + O(1),$$

where $x = \mathbb{P}(\mathbf{x})$, $a_j = \mathbb{P}(\alpha_j)$.

For each vector $\mathbf{x}$, let $\alpha_{v,i}$, $A_{v,i}$, λ_i and $\mathbf{x}^{(i)}$ be defined as in (7.79), (7.80) and Lemma 7.28. Let p_0 be the smallest integer for which

$$\mathbf{x} \in \left\langle \mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(p_0)} \right\rangle.$$

Then Theorem 7.27 holds for all $p \geq p_0$. But by (7.79),

$$\sum_{j=0}^{q} m(x, a_j) = -\frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S} \sum_{j=0}^{q} \log \frac{\|\langle \mathbf{x}, \alpha_{v,j} \rangle\|_v}{\|\mathbf{x}\|_v} + O(1);$$

also

$$\begin{aligned} \log \lambda_{p_0} &\leq \log f(\mathbf{x}) = \frac{1}{[\kappa : \mathbb{Q}]} \sum_{v \in S} \log A_v \\ &= \frac{1}{(n+1)[\kappa : \mathbb{Q}]} \sum_{v \in S} \sum_{i=0}^{n} \log \|\langle \mathbf{x}, \alpha_{v,i} \rangle\|_v \\ &= h(\mathbf{x}) - \frac{1}{n+1} \sum_{j=0}^{q} m(x, a_j) + O(1). \end{aligned}$$

Applying Theorem 7.13, we also have

$$\log \lambda_n \geq \frac{1}{n+1} \sum_{j=0}^{q} m(x, a_j) - h(\mathbf{x}) + O(1).$$

Thus, summing the results of Theorem 7.27 from $p = p_0$ to $n - 1$ gives

$$\begin{aligned}\sum_{j=0}^{q} m(x,a_j) - (n+1)h(x) &\leq \frac{n+1}{2}\log\frac{\lambda_n}{\lambda_{p_0}}\\ &\leq \frac{(n+1)\varepsilon}{2}\sum_{p=p_0}^{n-1}\log H\big(\mathbf{x}^{(0)}\wedge\cdots\wedge\mathbf{x}^{(p)}\big)\\ &\leq \varepsilon\left(\frac{(n+1)[\kappa:\mathbb{Q}]}{2}\sum_{p=p_0}^{n-1}c_p\right)h(x)+O(1)\end{aligned} \tag{7.81}$$

by Lemma 7.28. This concludes the proof (after adjusting ε). □

In particular, Theorem 7.23 has the following form:

Theorem 7.29. *Take $\varepsilon > 0$, $q \geq n$. Assume that the family $\{\alpha_0,\ldots,\alpha_q\} \subset V^*$ is in general position. Then there exists a finite union Q of hyperplanes of V such that*

$$\|\xi\|_\infty^{q-n-\varepsilon} < C\prod_{j=0}^{q}\|\langle\xi,\alpha_j\rangle\|_\infty$$

hold for all $\xi \in \mathcal{O}_{V,S} - Q$.

Thus Conjecture 5.16 is the truncated form of Theorem 7.29.

7.6 Cartan's method

Let κ be a number field and let S be a finite subset of M_κ containing the set M_κ^∞. Let $V = V_\kappa$ be a vector space of finite dimension $n+1 > 0$ over κ. Lemma 4.3 immediately implies the following fact (see [103]):

Lemma 7.30. *For $x \in \mathbb{P}(V)$, we can choose $\xi \in \mathcal{O}_{V,S}$ such that $x = \mathbb{P}(\xi)$, and the relative height of x satisfies*

$$\max\left\{\max_{\rho\in S}\|\xi\|_\rho, \prod_{\rho\in S}\|\xi\|_\rho\right\} \leq cH_\kappa(x) \leq c\left\{\max_{\rho\in S}\|\xi\|_\rho\right\}^{\#S},$$

where c is a constant depending only on S but independent of x.

Take a basis $e = (e_0,\ldots,e_n)$ of V. We will identify $V \cong \mathbb{A}^{n+1}(\kappa)$ by the correspondence relation

$$x_0e_0+\cdots+x_ne_n \in V \longmapsto \mathbf{x} = (x_0,\ldots,x_n) \in \mathbb{A}^{n+1}(\kappa),\ \ x_j \in \kappa.$$

Take

$$\mathbf{x}^{(i)} = \left(x_0^{(i)}, x_1^{(i)}, \dots, x_n^{(i)}\right) \in \mathbb{A}^{n+1}(\kappa), \ \ i = 1, \dots, n.$$

We write

$$\mathbf{W}\big(\mathbf{x}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}\big) = \begin{vmatrix} x_0 & x_1 & \cdots & x_n \\ x_0^{(1)} & x_1^{(1)} & \cdots & x_n^{(1)} \\ \cdots & \cdots & \cdots & \cdots \\ x_0^{(n)} & x_1^{(n)} & \cdots & x_n^{(n)} \end{vmatrix}, \tag{7.82}$$

and define

$$\mathbf{S}\big(\mathbf{x}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}\big) = \frac{\mathbf{W}(\mathbf{x}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)})}{x_0 x_1 \cdots x_n} \tag{7.83}$$

if $x_j \neq 0$ for $j = 0, \dots, n$.

Let $\mathscr{A} = \{a_0, a_1, \dots, a_q\}$ be a family of points $a_j \in \mathbb{P}(V^*)$ in general position. Take $\alpha_i \in V^* - \{0\}$ with $\mathbb{P}(\alpha_i) = a_i$. Write

$$\alpha_i = \alpha_{i0}\epsilon_0 + \cdots + \alpha_{in}\epsilon_n, \ \ i = 0, \dots, q,$$

where $\epsilon = (\epsilon_0, \dots, \epsilon_n)$ is the dual of e. For $i = 0, 1, \dots, q$, set

$$L_i(\mathbf{x}) = \langle \mathbf{x}, \alpha_i \rangle = \alpha_{i0}x_0 + \alpha_{i1}x_1 + \cdots + \alpha_{in}x_n.$$

Take $\varepsilon > 0$. Then there exists a finite set $\mathcal{T}$ of V with the following property. If $\mathbf{x} \in \mathcal{O}_{\kappa,S}^{n+1} - \kappa\mathcal{T}$, then by Theorem 7.20, there exists a vector $\mathbf{x}' \in \mathcal{O}_{\kappa,S}^{n+1}$ such that $\mathbf{x} \wedge \mathbf{x}' \neq 0$ and

$$\sum_{v \in S} \frac{\|(\mathbf{x} \wedge \mathbf{x}')\angle\alpha_i\|_v}{\|\mathbf{x}\|_v \|\langle \mathbf{x}, \alpha_i \rangle\|_v} \leq H(\mathbf{x})^{\varepsilon}$$

for all $i = 0, \dots, q$ for which $\langle \mathbf{x}, \alpha_i \rangle \neq 0$, and $\langle \mathbf{x}', \alpha_i \rangle = 0$ if $\langle \mathbf{x}, \alpha_i \rangle = 0$. Here $\mathbf{x}'$ is only determined modulo $\mathbf{x}$, and so, according to the proof of Theorem 7.26, we can choose one $\mathbf{x}^{(1)} = \mathbf{x}' - a\mathbf{x} \in \mathcal{O}_{\kappa,S}^{n+1}$ for some $a \in \mathcal{O}_{\kappa,S}$ such that $\mathbf{x} \wedge \mathbf{x}^{(1)} \neq 0$, and

$$\|\langle \mathbf{x}^{(1)}, \alpha_i \rangle\|_v \ll H(\mathbf{x})^{\varepsilon} \|\langle \mathbf{x}, \alpha_i \rangle\|_v. \tag{7.84}$$

Based on Theorem 7.20, we make the following hypothesis:

Hypothesis 7.31. *Let $\alpha_0, \dots, \alpha_q$ be a set of vectors in V^* in general position. Take $\varepsilon > 0$. Then there exists a finite set $\mathcal{T}$ of V such that if $\mathbf{x} \in \mathcal{O}_{\kappa,S}^{n+1}$ is not a scalar multiple of some vector in $\mathcal{T}$, then there exist $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)} \in \mathcal{O}_{\kappa,S}^{n+1}$ such that $\mathbf{x} \wedge \mathbf{x}^{(1)} \wedge \cdots \wedge \mathbf{x}^{(n)} \neq 0$ and*

$$\log \sum_{v \in S} \frac{\|(\mathbf{x} \wedge \mathbf{x}^{(j)})\angle\alpha_i\|_v}{\|\mathbf{x}\|_v \|\langle \mathbf{x}, \alpha_i \rangle\|_v} \leq \varepsilon \log \overline{H}(\mathbf{x}), \ \ j = 1, \dots, n$$

for all $i = 0, \dots, q$ for which $\langle \mathbf{x}, \alpha_i \rangle \neq 0$.

Under the Hypothesis 7.31, according to the proof of Theorem 7.26, we can choose $\mathbf{x}^{(j)}$ modulo $\mathbf{x}$ satisfying

$$\|\langle \mathbf{x}^{(j)}, \alpha_i\rangle\|_v \ll H(\mathbf{x})^{\varepsilon}\|\langle \mathbf{x}, \alpha_i\rangle\|_v, \quad 0 \le i \le q, \ \ 1 \le j \le n. \tag{7.85}$$

In particular, we have

$$\mathbf{W} = \mathbf{W}\big(\mathbf{x}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n)}\big) \neq 0.$$

Let $x = \mathbb{P}(\mathbf{x})$ and define

$$N_{\mathrm{Ram}}(x) = -\sum_{v \notin S} \log |||\mathbf{W}|||_v.$$

It is obvious that $N_{\mathrm{Ram}}(x) \ge 0$. Here we follow the method due to Cartan to prove Schmidt subspace theorem again.

Theorem 7.32. *Take $\varepsilon > 0$, $q \ge n$. Let $\mathscr{A} = \{a_0, a_1, \dots, a_q\}$ be a family of points $a_j \in \mathbb{P}(V^*)$ in general position. Under the Hypothesis 7.31, there exists a finite set $\{b_1, \dots, b_s\}$ of $\mathbb{P}(V^*_{\bar{\kappa}})$ such that the inequality*

$$(q-n)h(x) \le \sum_{i=0}^{q} N(x, a_i) - N_{\mathrm{Ram}}(x) + \varepsilon h(x) + O(1) \tag{7.86}$$

holds for all $x \in \mathbb{P}(V) - \bigcup_i \ddot{E}[b_i]$.

Proof. We start with a sequence of vectors $\mathbf{x}$, and immediately throw out all $\mathbf{x}$ such that $\langle \mathbf{x}, \alpha_i\rangle = 0$ for any i, or such that $\mathbf{x}$ lies in the subset $\kappa\mathcal{T}$. This eliminates only finitely many hyperplanes; we will show that all remaining vectors satisfy the theorem. We take $\mathbf{x} \in \mathcal{O}^{n+1}_{\kappa,S}$ such that it is not in the eliminating hyperplanes above and set $x = \mathbb{P}(\mathbf{x})$. Because $\mathscr{A}$ is in general position, we have $c_\lambda = \det\big(\alpha_{\lambda(i)j}\big) \neq 0$ for any $\lambda \in J^q_n$. We abbreviate the determinant

$$\mathbf{W}_\lambda = \mathbf{W}\Big(L_\lambda(\mathbf{x}), L_\lambda\big(\mathbf{x}^{(1)}\big), \dots, L_\lambda\big(\mathbf{x}^{(n)}\big)\Big),$$

and

$$\mathbf{S}_\lambda = \mathbf{S}\Big(L_\lambda(\mathbf{x}), L_\lambda\big(\mathbf{x}^{(1)}\big), \dots, L_\lambda\big(\mathbf{x}^{(n)}\big)\Big),$$

where

$$L_\lambda = (L_{\lambda(0)}, \dots, L_{\lambda(n)}).$$

It follows that $\mathbf{W}_\lambda = c_\lambda \mathbf{W}$. Lemma 3.12 implies

$$\prod_{j=0}^{q} \frac{1}{|||x, a_j|||_v} \le \left(\frac{1}{\Gamma_v(\mathscr{A})}\right)^{q-n} \max_{\lambda \in J^q_n} \prod_{i=0}^{n} \frac{1}{|||x, a_{\lambda(i)}|||_v}.$$

Since

$$\prod_{i=0}^{n}\frac{1}{|||x,a_{\lambda(i)}|||_v}=\prod_{i=0}^{n}\frac{|||\mathbf{x}|||_v|||\alpha_{\lambda(i)}|||_v}{|||L_{\lambda(i)}(\mathbf{x})|||_v}=|||\mathbf{x}|||_v^{n+1}\frac{|||\mathbf{S}_\lambda|||_v}{|||c_\lambda\mathbf{W}|||_v}\prod_{i=0}^{n}|||\alpha_{\lambda(i)}|||_v, \tag{7.87}$$

we have

$$\prod_{j=0}^{q}\frac{1}{|||x,a_j|||_v}\le c_v\frac{|||\mathbf{x}|||_v^{n+1}}{|||\mathbf{W}|||_v}\max_{\lambda\in J_n^q}|||\mathbf{S}_\lambda|||_v,$$

for some constant c_v, which yields

$$\begin{aligned}\sum_{i=0}^{q}m(x,a_i) &\le (n+1)\sum_{v\in S}\log|||\mathbf{x}|||_v-\sum_{v\in S}\log|||\mathbf{W}|||_v\\ &\quad+\sum_{v\in S}\max_{\lambda\in J_n^q}\log|||\mathbf{S}_\lambda|||_v+O(1).\end{aligned} \tag{7.88}$$

By Lemma 7.30, we obtain

$$\sum_{v\in S}\log|||\mathbf{x}|||_v\le h(x)+O(1).$$

The product formula means

$$\sum_{v\in S}\log|||\mathbf{W}|||_v=-\sum_{v\notin S}\log|||\mathbf{W}|||_v=N_{\mathrm{Ram}}(x).$$

Thus the inequality (7.88) becomes

$$\begin{aligned}\sum_{i=0}^{q}m(x,a_i) &\le (n+1)h(x)-N_{\mathrm{Ram}}(x)\\ &\quad+\sum_{v\in S}\max_{\lambda\in J_n^q}\log|||\mathbf{S}_\lambda|||_v+O(1),\end{aligned} \tag{7.89}$$

where

$$|\mathbf{S}_\lambda|_v=\frac{|\mathbf{W}_\lambda|_v}{|L_{\lambda(0)}(\mathbf{x})\cdots L_{\lambda(n)}(\mathbf{x})|_v}=\left|\sum_{i\in\mathcal{J}^n}\mathrm{sign}(i)\frac{L_{\lambda(0)}(\mathbf{x}^{(i_0)})}{L_{\lambda(0)}(\mathbf{x})}\cdots\frac{L_{\lambda(n)}(\mathbf{x}^{(i_n)})}{L_{\lambda(n)}(\mathbf{x})}\right|_v,$$

in which $\mathcal{J}^n$ is the permutation group on $\mathbb{Z}[0,n]$ and $\mathbf{x}^{(0)}=\mathbf{x}$. Hence the conditions (7.85) yields easily

$$\|\mathbf{S}_\lambda\|_v\le\varsigma_{v,r^2}^{n_v}\max_{i\in\mathcal{J}^n}\left\{\frac{\|L_{\lambda(0)}(\mathbf{x}^{(i_0)})\|_v}{\|L_{\lambda(0)}(\mathbf{x})\|_v}\cdots\frac{\|L_{\lambda(n)}(\mathbf{x}^{(i_n)})\|_v}{\|L_{\lambda(n)}(\mathbf{x})\|_v}\right\}\ll H(\mathbf{x})^{n\varepsilon},$$

where $r=\sqrt{(n+1)!}$. Thus Theorem 7.32 follows from (7.89) and the first main theorem (with a different ε). □

Conjecture 7.33. *Take $\varepsilon > 0$, $q \geq n$. Let $\mathscr{A} = \{a_0, a_1, \ldots, a_q\}$ be a family of points $a_j \in \mathbb{P}(V^*)$ in general position. Then there exists a finite set $\{b_1, \ldots, b_s\}$ of $\mathbb{P}(V^*_{\bar{\kappa}})$ such that the inequality*

$$(q-n)h(x) \leq \sum_{i=0}^{q} N_n(x, a_i) + \varepsilon h(x) + O(1) \tag{7.90}$$

holds for all $x \in \mathbb{P}(V) - \bigcup_i \ddot{E}[b_i]$, where

$$N_n(x, a_i) = N_n\big(x, \ddot{E}[a_i]\big).$$

We consider the case $n = 1$. Now we take $V = \kappa^2$. Recall that we have the embeddings

$$x \in \kappa \longmapsto [1, x] \in \mathbb{P}(V),$$
$$a \in \kappa \longmapsto [-a, 1] \in \mathbb{P}(V^*).$$

We write

$$x = \frac{x_1}{x_0}, \quad a_i = -\frac{\alpha_{i0}}{\alpha_{i1}}$$

with $x_0, x_1, \alpha_{i0}, \alpha_{i1} \in \mathcal{O}_\kappa$, and so

$$\mathbf{x} = (x_0, x_1) \in V, \quad \alpha_i = (\alpha_{i0}, \alpha_{i1}) \in V^*$$

such that

$$\langle \mathbf{x}, \alpha_i \rangle = \alpha_{i0} x_0 + \alpha_{i1} x_1.$$

Note that

$$\frac{|\mathbf{x}|_v |\alpha_i|_v}{|\langle \mathbf{x}, \alpha_i \rangle|_v} = \frac{|(1, x)|_v |(-a_i, 1)|_v}{|x - a_i|_v} = \frac{1}{\chi_v(x, a_i)}.$$

Thus the inequality (7.86) means

$$(q-1)h(x) \leq \sum_{i=0}^{q} N(x, a_i) - N_{\mathrm{Ram}}(x) + \varepsilon h(x) + O(1),$$

where $N_{\mathrm{Ram}}(x)$ is the term $N_{\mathrm{Ram}}([1, x])$ in (7.86).

7.7 Subspace theorems on hypersurfaces

Let κ be a number field and let $V = V_\kappa$ be a normed vector space of dimension $n + 1 > 0$ over κ. Let E be a hyperplane on $\mathbb{P}(V_{\bar{\kappa}})$. Take a positive integer d. The dual classification mapping

$$\varphi_{dE} : \mathbb{P}(V_{\bar{\kappa}}) \longrightarrow \mathbb{P}(\amalg_d V_{\bar{\kappa}})$$

is just the *Veronese mapping*, that is,

$$\varphi_{dE}(x) = x^{\amalg d}.$$

Then the absolute (multiplicative) height of $x \in \mathbb{P}(V_{\bar{\kappa}})$ for dE is given by

$$H_{dE}(x) = H(\varphi_{dE}(x)) = H\big(x^{\amalg d}\big) = H(x)^d,$$

and the absolute (logarithmic) height of x for dE is given as

$$h_{dE}(x) = h(\varphi_{dE}(x)) = dh(x).$$

Let S be a finite set of places containing M_κ^∞. Take $\alpha \in \amalg_d V^*$ with $(\alpha) = dE$ and set $a = \mathbb{P}(\alpha)$. For $x \notin dE$, the *proximity function* $m_S(x, dE)$ is given by

$$m_S(x, dE) = m\big(x^{\amalg d}, a\big).$$

Similarly, the *valence function* is given by

$$N_S(x, dE) = N\big(x^{\amalg d}, a\big).$$

Thus the (4.36) yields the following *first main theorem*:

$$m\big(x^{\amalg d}, a\big) + N\big(x^{\amalg d}, a\big) = dh(x) + O(1). \tag{7.91}$$

7.7.1 Statements of theorems

By using Theorem 7.23, we can obtain directly the following result:

Theorem 7.34. *Take $\varepsilon > 0$, $q \geq N = \binom{n+d}{d}$. Assume that for each $\rho \in S$, a family*

$$\{a_{\rho,1}, \ldots, a_{\rho,q}\} \subset \mathbb{P}(\amalg_d V^*)$$

is in general position. Then there exists a finite set $\{b_1, \ldots, b_s\}$ of $\mathbb{P}(\amalg_d V_{\bar{\kappa}}^*)$ such that the inequality

$$\sum_{\rho \in S} \sum_{j=1}^{q} \log \frac{1}{|||x^{\amalg d}, a_{\rho,j}|||_\rho} < d(N + \varepsilon)h(x) + O(1)$$

holds for all $x \in \mathbb{P}(V) - \bigcup_i \ddot{E}^d[b_i]$.

If the families in general position in Theorem 7.34 are replaced by admissible families, then N in the bound of the main inequality of Theorem 7.34 can be replaced by $n + 1$, that is, we have the following *subspace theorem on hypersurfaces*:

Theorem 7.35 ([112]). *Take $\varepsilon > 0$, $q \geq n$. Assume that for $\rho \in S$, a family*

$$\mathscr{A}_\rho = \{a_{\rho,0}, \ldots, a_{\rho,q}\} \subset \mathbb{P}(\amalg_d V^*)$$

is admissible. Then there exist points

$$b_i \in \mathbb{P}(\amalg_{d_i} V_{\bar{\kappa}}^*) \ (1 \leq d_i \in \mathbb{Z}, \ i = 1, \ldots, s < \infty)$$

such that the inequality

$$\sum_{\rho \in S} \sum_{j=0}^{q} \log \frac{1}{\| |x^{\amalg d}, a_{\rho,j}| \|_\rho} < d(n+1+\varepsilon)h(x) + O(1)$$

holds for all $x \in \mathbb{P}(V) - \bigcup_i \ddot{E}^{d_i}[b_i]$.

Originally, Theorem 7.35 is a conjecture proposed by Hu and Yang [103] (or see [108]). It extends the Schmidt's subspace theorem. We will introduce the proof in Section 7.7.2 by using methods of P. Corvaja and U. Zannier [35]. Theorem 7.22 implies the following result:

Theorem 7.36. *For $\rho \in S$, $i \in \{1, \ldots, N\}$, where $N = \binom{n+d}{d}$, take $\alpha_{\rho,i} \in \amalg_d V^* - \{0\}$ such that for each $\rho \in S$, $\alpha_{\rho,1}, \ldots, \alpha_{\rho,N}$ are linearly independent. Then for any $\varepsilon > 0$ there exists a finite set $\{b_1, \ldots, b_s\}$ of $\mathbb{P}(\amalg_d V_{\bar{\kappa}}^*)$ such that the inequality*

$$\prod_{\rho \in S} \prod_{i=1}^{N} \frac{1}{\| \langle \xi^{\amalg d}, \alpha_{\rho,i} \rangle \|_\rho} \leq \Big\{ \max_{\rho \in S} \|\xi\|_\rho \Big\}^{\varepsilon}$$

holds for all S-integral points $\xi \in \mathcal{O}_{V,S} - \bigcup_i E^d[b_i]$.

Related to Theorem 7.36, we have:

Theorem 7.37 ([112]). *For $\rho \in S$, $i = 0, \ldots, n$, take $\alpha_{\rho,i} \in \amalg_d V^* - \{0\}$ such that the system*

$$\langle \xi^{\amalg d}, \alpha_{\rho,i} \rangle = 0, \ \ i = 0, \ldots, n$$

has only the trivial solution $\xi = 0$ in $V_{\bar{\kappa}}$. Then for any $\varepsilon > 0$ there exist points

$$b_i \in \mathbb{P}(\amalg_{d_i} V_{\bar{\kappa}}^*) \ (1 \leq d_i \in \mathbb{Z}, \ i = 1, \ldots, s < \infty)$$

such that the inequality

$$\prod_{\rho \in S} \prod_{i=0}^{n} \frac{1}{\| \langle \xi^{\amalg d}, \alpha_{\rho,i} \rangle \|_\rho} \leq \Big\{ \max_{\rho \in S} \|\xi\|_\rho \Big\}^{\varepsilon}$$

holds for all S-integral points $\xi \in \mathcal{O}_{V,S} - \bigcup_i E^{d_i}[b_i]$.

Hu and Yang suggested Theorem 7.37 in [103] (or see [108]). Obviously, Theorem 7.35 yields immediately Theorem 7.37 by taking $q = n$ and using Lemma 7.30. Conversely, Theorem 7.37 implies also Theorem 7.35. In fact, by Lemma 3.17 and Theorem 7.37, there exist points

$$b_i \in \mathbb{P}(\amalg_{d_i} V_{\bar{\kappa}}^*) \ (1 \le d_i \in \mathbb{Z}, \ i = 1, \dots, s < \infty)$$

such that the inequality

$$\begin{aligned}
\prod_{\rho\in S}\prod_{j=0}^{q}\frac{1}{|||x^{\amalg d}, a_{\rho,j}|||_\rho} &\le \prod_{\rho\in S}\left\{\left(\frac{1}{\Gamma_\rho(\mathscr{A}_\rho)}\right)^{q-n}\prod_{j=0}^{n}\frac{1}{|||x^{\amalg d}, a_{\rho,\sigma_\rho(j)}|||_\rho}\right\} \\
&\le c_1\left(\prod_{\rho\in S}|||\xi|||_\rho^d\right)^{n+1}\left(\prod_{\rho\in S}\prod_{j=0}^{n}\frac{1}{|||\langle\xi^{\amalg d}, \alpha_{\rho,\sigma_\rho(j)}\rangle|||_\rho}\right) \\
&\le c_1\left(\prod_{\rho\in S}|||\xi|||_\rho\right)^{d(n+1)}\left(\max_{\rho\in S}|||\xi|||_\rho\right)^{\varepsilon},
\end{aligned}$$

holds for all points $x = \mathbb{P}(\xi) \in \mathbb{P}(V) - \bigcup_i \ddot{E}^{d_i}[b_i]$, where c_1 is constant, and $\alpha_{\rho,j} \in V^* - \{0\}$ with $a_{\rho,j} = \mathbb{P}(\alpha_{\rho,j})$. By Lemma 7.30, there exists a constant c_2 such that

$$\prod_{\rho\in S}\prod_{j=0}^{q}\frac{1}{|||x^{\amalg d}, a_{\rho,j}|||_\rho} \le c_2 H(x)^{d(n+1)+\varepsilon},$$

and hence Theorem 7.35 follows.

7.7.2 Proof of Theorem 7.35

In this section, we prove Theorem 7.35 based on methods of P. Corvaja and U. Zannier [35]. First of all, we state several lemmas from [35] (or see [224]). We shall use the *lexicographic ordering* on the p-tuples $\nu = (\nu(1), \dots, \nu(p)) \in \mathbb{Z}_+^p$, namely, $\mu > \nu$ if and only if for some $l \in \{1, \dots, p\}$ we have $\mu(k) = \nu(k)$ for $k < l$ and $\mu(l) > \nu(l)$.

Lemma 7.38. *Let A be a commutative ring and let $\{g_1, \dots, g_p\}$ be a regular sequence in A. Suppose that for some $y, x_1, \dots, x_h \in A$ we have an equation*

$$g_1^{\nu(1)} \cdots g_p^{\nu(p)} y = \sum_{k=1}^{h} g_1^{\mu_k(1)} \cdots g_p^{\mu_k(p)} x_k,$$

where $\mu_k > \nu$ for $k = 1, \dots, h$. Then $y \in I_p$.

Proof. We prove Lemma 7.38 by induction on p. Since g_1 is not a zero divisor in A, the assertion is trivial for $p = 1$. Assume that $p > 1$ and that Lemma 7.38 is true up to $p - 1$. Since $\mu_k > \nu$ for $k = 1, \dots, h$, renumbering the indices $1, \dots, h$ we may assume that

$$\mu_k(1) \begin{cases} > \nu(1), & k = 1, \dots, s, \\ = \nu(1), & k = s+1, \dots, h \end{cases}$$

for some $0 \le s \le h$. Since g_1 is not a zero divisor in A we may write

$$g_2^{\nu(2)} \cdots g_p^{\nu(p)} y = g_1 b + \sum_{k=s+1}^{h} g_2^{\mu_k(2)} \cdots g_p^{\mu_k(p)} x_k, \ \ b \in A.$$

Reducing modulo g_1, denoting the reduction with a bar, and working in the ring A/I_1, we have

$$\bar{g}_2^{\nu(2)} \cdots \bar{g}_p^{\nu(p)} \bar{y} = \sum_{k=s+1}^{h} \bar{g}_2^{\mu_k(2)} \cdots \bar{g}_p^{\mu_k(p)} \bar{x}_k.$$

Note that $(\mu_k(2), \dots, \mu_k(p)) > (\nu(2), \dots, \nu(p))$ for $k = s+1, \dots, h$ and that $\{\bar{g}_2, \dots, \bar{g}_p\}$ is a regular sequence in A/I_1. We may apply the inductive assumption with $p - 1$ in place of p and A/I_1 in place of A. Then $\bar{y}$ lies in the ideal of A/I_1 generated by $\bar{g}_2, \dots, \bar{g}_p$, i.e., $y \in I_p$, as required. □

Let κ be a number field and let $\bar{\kappa}$ be an algebraic closure of κ. Let $V = V_{\bar{\kappa}}$ be a normed vector space of dimension $n + 1 > 0$ over $\bar{\kappa}$.

Lemma 7.39. *Let $\tilde{\beta}_1, \dots, \tilde{\beta}_p$ be homogeneous polynomials in $\bar{\kappa}[\xi_0, \dots, \xi_n]$. Assume that they define a subvariety of $\mathbb{P}(V)$ of dimension $n - p$. Then $\{\tilde{\beta}_1, \dots, \tilde{\beta}_p\}$ is a regular sequence.*

Proof. This follows from Hilbert basis theorem and Proposition 1.18. □

Lemma 7.40. *Let $\tilde{\beta}_1, \dots, \tilde{\beta}_n$ be homogeneous polynomials in $\bar{\kappa}[\xi_0, \dots, \xi_n]$. Assume that they define a subvariety of $\mathbb{P}(V)$ of dimension 0. Then, for all large N,*

$$\dim V_{[N]} / \{(\tilde{\beta}_1, \dots, \tilde{\beta}_n) \cap V_{[N]}\} = \deg(\tilde{\beta}_1) \cdots \deg(\tilde{\beta}_n).$$

Proof. It is a classical fact from the theory of Hilbert polynomials that the dimension of the quotient in Lemma 7.40 is constant for large N, equal to the degree of the variety defined by $\tilde{\beta}_1, \dots, \tilde{\beta}_n$ (see [90], Ch. I.7) which is just the product of the degrees of $\tilde{\beta}_i$ (see [239], Ch. IV). □

Take $\rho \in S$ and take a positive integer d. Let $\mathscr{A}_\rho = \{a_{\rho,j}\}_{j=0}^{q}$ be a finite admissible family of points $a_{\rho,j} \in \mathbb{P}\left(\amalg_d V_\kappa^*\right)$ with $q \ge n$. Take $\alpha_{\rho,j} \in \amalg_d V_\kappa^* - \{0\}$ with $\mathbb{P}(\alpha_{\rho,j}) = a_{\rho,j}$, and define

$$\tilde{\alpha}_{\rho,j}(\xi) = \left\langle \xi^{\amalg d}, \alpha_{\rho,j} \right\rangle, \quad \xi \in V, \ \ j = 0, 1, \dots, q.$$

W.l.o.g., assume $|\alpha_{\rho,j}|_\rho = 1$ for $j = 0, \dots, q$. Lemma 3.17 implies

$$\prod_{j=0}^{q} \frac{1}{\|x^{\amalg d}, a_{\rho,j}\|_\rho} \le \left(\frac{1}{\Gamma_\rho(\mathscr{A}_\rho)}\right)^{q+1-n} \max_{\lambda \in J_{n-1}^q} \prod_{i=0}^{n-1} \frac{1}{\|x^{\amalg d}, a_{\rho,\lambda(i)}\|_\rho} \tag{7.92}$$

for $x \in \mathbb{P}(V_\kappa) - \cup_{j=0}^q \ddot{E}^d[a_{\rho,j}]$. P. Corvaja and U. Zannier [35] estimated the terms on the right-hand side of (7.92) as follows.

Now pick $\lambda \in J_{n-1}^q$. Since $\mathscr{A}_\rho$ is admissible, $\tilde{\alpha}_{\rho,\lambda(0)}, \dots, \tilde{\alpha}_{\rho,\lambda(n-1)}$ define a subvariety of $\mathbb{P}(V)$ of dimension 0. Take a multi-index $\nu = (\nu(1), \dots, \nu(n)) \in \mathbb{Z}_+^n$ with the length

$$|\nu| = \nu(1) + \cdots + \nu(n) \le \frac{N}{d}.$$

For any $\gamma = (\gamma(1), \dots, \gamma(n)) \in \mathbb{Z}_+^n$, abbreviate

$$\tilde{\alpha}_{\rho,\lambda}^{\gamma} = \tilde{\alpha}_{\rho,\lambda(0)}^{\gamma(1)} \cdots \tilde{\alpha}_{\rho,\lambda(n-1)}^{\gamma(n)}$$

and define the spaces

$$\mathbf{V}_{N,\nu} = \sum_{\gamma \ge \nu} \tilde{\alpha}_{\rho,\lambda}^{\gamma} V_{[N-d|\gamma|]}$$

with $\mathbf{V}_{N,0} = V_{[N]}$ and $\mathbf{V}_{N,\mu} \subset \mathbf{V}_{N,\nu}$ if $\mu > \nu$. Thus the $\mathbf{V}_{N,\nu}$ define a filtration of $V_{[N]}$.

Next we consider quotients between consecutive spaces in the filtration. Suppose that $\mathbf{V}_{N,\mu}$ follows $\mathbf{V}_{N,\nu}$ in the filtration:

$$V_{[N]} \supset \cdots \supset \mathbf{V}_{N,\nu} \supset \mathbf{V}_{N,\mu} \supset \cdots \supset \{0\}. \tag{7.93}$$

Lemma 7.41. *There is an isomorphism*

$$\mathbf{V}_{N,\nu}/\mathbf{V}_{N,\mu} \cong V_{[N-d|\nu|]}/\{(\tilde{\alpha}_{\rho,\lambda(0)}, \dots, \tilde{\alpha}_{\rho,\lambda(n-1)}) \cap V_{[N-d|\nu|]}\}.$$

Proof. A vector space homomorphism $\varphi : V_{[N-d|\nu|]} \longrightarrow \mathbf{V}_{N,\nu}/\mathbf{V}_{N,\mu}$ is defined as follows: For $\tilde{\beta} \in V_{[N-d|\nu|]}$, we define $\varphi(\tilde{\beta})$ as the class of $\tilde{\alpha}_{\rho,\lambda}^{\nu}\tilde{\beta}$ modulo $\mathbf{V}_{N,\mu}$. Obviously, φ is surjective.

Suppose $\tilde{\beta} \in \ker(\varphi) = \varphi^{-1}(0)$, which means that

$$\tilde{\alpha}_{\rho,\lambda}^{\nu}\tilde{\beta} \in \sum_{\gamma > \nu} \tilde{\alpha}_{\rho,\lambda}^{\gamma} V_{[N-d|\gamma|]}.$$

Thus we may write

$$\tilde{\alpha}_{\rho,\lambda}^{\nu}\tilde{\beta} = \sum_{\gamma > \nu} \tilde{\alpha}_{\rho,\lambda}^{\gamma}\tilde{\beta}_\gamma$$

for elements $\tilde{\beta}_\gamma \in V_{[N-d|\gamma|]}$. Lemma 7.38 implies that $\tilde{\beta}$ lies in the ideal generated by $\tilde{\alpha}_{\rho,\lambda(0)}, \dots, \tilde{\alpha}_{\rho,\lambda(n-1)}$. Therefore

$$\tilde{\beta} = \sum_{i=0}^{n-1} \tilde{\eta}_i \tilde{\alpha}_{\rho,\lambda(i)},$$

where $\tilde{\eta}_i$ $(0 \le i \le n-1)$ are homogeneous with $\deg(\tilde{\eta}_i) = \deg(\tilde{\beta}) - d$, that is,

$$\tilde{\eta}_i \in V_{[N-d(|\nu|+1)]}, \ \ i = 0, \dots, n-1.$$

Hence $\tilde{\alpha}^\nu_{\rho,\lambda}\tilde{\beta}$ is a sum of terms in $\mathbf{V}_{N,\mu}$, which concludes the proof of the lemma. □

By Lemma 7.40 and Lemma 7.41, there exists an integer N_0 depending only on $\tilde{\alpha}_{\rho,\lambda(0)}, \dots, \tilde{\alpha}_{\rho,\lambda(n-1)}$ such that

$$\Delta_\nu := \dim \mathbf{V}_{N,\nu}/\mathbf{V}_{N,\mu} \begin{cases} = d^n, & \text{if } d|\nu| < N - N_0, \\ \le \dim V_{[N_0]}, & \text{others.} \end{cases} \tag{7.94}$$

Now we choose inductively a suitable basis of $V_{[N]}$ in the following way. We start with the last nonzero $\mathbf{V}_{N,\mu}$ in the filtration (7.93) and pick any basis of it. Suppose $\mu > \nu$ are consecutive n-tuples such that $d|\nu|, d|\mu| \le N$. It follows directly from the definition that we may pick representatives $\tilde{\alpha}^\nu_{\rho,\lambda}\tilde{\beta} \in \mathbf{V}_{N,\nu}$ of elements in the quotient space $\mathbf{V}_{N,\nu}/\mathbf{V}_{N,\mu}$, where $\tilde{\beta} \in V_{[N-d|\nu|]}$. We extend the previously constructed basis in $\mathbf{V}_{N,\mu}$ by adding these representatives. In particular, we have obtained a basis for $\mathbf{V}_{N,\nu}$ and our inductive procedure may go on unless $\mathbf{V}_{N,\nu} = V_{[N]}$, in which case we stop. In this way, we obtain a basis $\{\tilde{\psi}_1, \dots, \tilde{\psi}_M\}$ of $V_{[N]}$, where $M = \dim V_{[N]}$.

For a fixed $k \in \{1, \dots, M\}$, assume that $\tilde{\psi}_k$ is constructed with respect to $\mathbf{V}_{N,\nu}/\mathbf{V}_{N,\mu}$. We may write

$$\tilde{\psi}_k = \tilde{\alpha}^\nu_{\rho,\lambda}\tilde{\beta}, \quad \tilde{\beta} \in V_{[N-d|\nu|]}.$$

Then we have a bound

$$\begin{aligned} \|\tilde{\psi}_k(\xi)\|_\rho &= \|\tilde{\alpha}^\nu_{\rho,\lambda}(\xi)\|_\rho \|\tilde{\beta}(\xi)\|_\rho \\ &\le c' \|\tilde{\alpha}^\nu_{\rho,\lambda}(\xi)\|_\rho \|\xi\|_\rho^{N-d|\nu|}, \end{aligned}$$

where c' is a positive constant depending only on $\tilde{\psi}_k$, not on ξ. Observe that there are precisely Δ_ν such functions $\tilde{\psi}_k$ in our basis. Hence, taking the product over all functions in the basis, and then taking logarithms, we get

$$\begin{aligned} \log \prod_{k=1}^{M} \|\tilde{\psi}_k(\xi)\|_\rho &\le \sum_{i=0}^{n-1} \sum_{\nu} \Delta_\nu \nu(i+1) \log \|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho \\ &\quad + \Bigg(\sum_{\nu} \Delta_\nu (N - d|\nu|) \Bigg) \log \|\xi\|_\rho + c, \end{aligned} \tag{7.95}$$

where c is a positive constant depending only on $\tilde{\psi}_k$, not on ξ. Here ν in the summations is taken over the n-tuples in the filtration (7.93) with $|\nu| \le N/d$.

Note that

$$M = \dim V_{[N]} = \binom{n+N}{N} = \frac{N^n}{n!} + O\left(N^{n-1}\right), \tag{7.96}$$

$$\sum_{t=0}^{T} \#J_{n-1,t} = \#J_{n,T} = \binom{n+T}{T}, \ T \in \mathbb{Z}^+,$$

and that, since the sum below is independent of j, we have that, for any positive integer T and for every $0 \le j \le n$,

$$\begin{aligned} \sum_{\nu \in J_{n,T}} \nu(j) &= \frac{1}{n+1} \sum_{\nu \in J_{n,T}} \sum_{j=0}^{n} \nu(j) = \frac{1}{n+1} \sum_{\lambda \in J_{n,T}} T \\ &= \frac{T}{n+1}\binom{n+T}{T} = \binom{n+T}{T-1} \\ &= \frac{T^{n+1}}{(n+1)!} + O\left(T^n\right). \end{aligned} \tag{7.97}$$

Then, for N divisible by d and for every $0 \le i \le n-1$, (7.94) and (7.97) with $T = N/d$ yield

$$\sum_{\nu} \Delta_\nu \nu(i+1) = d^n \sum_{\nu} \nu(i+1) + K_1 = d^n \binom{n+T}{T-1} + K_1, \tag{7.98}$$

where

$$K_1 = \sum_{T - N_0/d \le |\nu| \le T} (\Delta_\nu - d^n)\nu(i+1) = O\left(T^n\right).$$

Therefore, we obtain

$$\sum_{\nu} \Delta_\nu \nu(i+1) = \frac{N^{n+1}}{d(n+1)!} + O\left(N^n\right).$$

Further we have

$$\sum_{\nu} \Delta_\nu |\nu| = \sum_{i=0}^{n-1} \sum_{\nu} \Delta_\nu \nu(i+1) = n d^n \binom{n+T}{T-1} + n K_1, \tag{7.99}$$

and hence

$$\sum_{\nu} \Delta_\nu |\nu| = \frac{n N^{n+1}}{d(n+1)!} + O\left(N^n\right).$$

On the other hand, we have

$$\sum_{\nu} \Delta_\nu T = \sum_{\nu} d^n T + K_2 = d^n T \binom{n+T}{T} + K_2, \tag{7.100}$$

where

$$K_2 = \sum_{T-N_0/d \le |\nu| \le T} (\Delta_\nu - d^n)T = O\left(T^n\right).$$

Hence

$$\sum_{\nu} \Delta_\nu (T - |\nu|) = d^n \binom{n+T}{T-1} + K_2 - nK_1. \tag{7.101}$$

Therefore, by (7.95), (7.98) and (7.101), we have

$$\begin{aligned} \log \prod_{k=1}^{M} \|\tilde{\psi}_k(\xi)\|_\rho &\le \left\{ d^n \binom{n+T}{T-1} + K_1 \right\} \log \prod_{i=0}^{n-1} \|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho \\ &\quad + \left\{ d^n \binom{n+T}{T-1} + K_2 - nK_1 \right\} d \log \|\xi\|_\rho + c \\ &\le K \left\{ \log \prod_{i=0}^{n-1} \|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho + d \log \|\xi\|_\rho \right\} + c, \end{aligned} \tag{7.102}$$

where $K = K(d, n, N)$ is a positive constant such that

$$K = \frac{N^{n+1}}{d(n+1)!} \left(1 + O\left(\frac{1}{N} \right) \right). \tag{7.103}$$

Let $\tilde{\phi}_1, \ldots, \tilde{\phi}_M$ be a fixed basis of $V_{[N]}$ such that when $\xi \in V - \{0\}$,

$$\Xi = (\tilde{\phi}_1(\xi), \ldots, \tilde{\phi}_M(\xi)) \in \bar{\kappa}^M - \{0\}.$$

Then $\tilde{\psi}_k$ can be expressed as a linear form L_k in $\tilde{\phi}_1, \ldots, \tilde{\phi}_M$ so that $\tilde{\psi}_k(\xi) = L_k(\Xi)$. The linear forms $L_1, \ldots, L_M$ are linearly independent. By (7.102), we obtain

$$\begin{aligned} \log \prod_{k=1}^{M} \|L_k(\Xi)\|_\rho &\le K \left\{ \log \prod_{i=0}^{n-1} \|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho + d \log \|\xi\|_\rho \right\} + c \\ &= K \left\{ \log \prod_{i=0}^{n-1} \frac{\|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho}{\|\xi\|_\rho^d} + (n+1) d \log \|\xi\|_\rho \right\} + c, \end{aligned}$$

which implies

$$\begin{aligned} \log \prod_{i=0}^{n-1} \frac{\|\xi\|_\rho^d}{\|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho} &\le \frac{1}{K} \left\{ \log \prod_{k=1}^{M} \frac{1}{\|L_k(\Xi)\|_\rho} + c \right\} \\ &\quad + (n+1) d \log \|\xi\|_\rho, \end{aligned} \tag{7.104}$$

or, equivalently

$$\prod_{i=0}^{n-1} \frac{\|\xi\|_\rho^d}{\|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho} \le \left\{ e^c \prod_{k=1}^{M} \frac{1}{\|L_k(\Xi)\|_\rho} \right\}^{\frac{1}{K}} \|\xi\|_\rho^{(n+1)d}. \tag{7.105}$$

Fix $\varepsilon > 0$. By Theorem 7.22, for all $\lambda \in J^q_{n-1}$, the set Q of all $\Xi \in \mathcal{O}_{V_{[N]},S}$ satisfying

$$\prod_{\rho\in S}\prod_{k=1}^{N} \|L_k(\Xi)\|_\rho < \Big\{ \max_{\rho\in S} \|\Xi\|_\rho \Big\}^{-\varepsilon}$$

is contained in a finite union of hyperplanes of $V_{[N]}$. Note that Q is just a finite union of hypersurfaces of degree N in V, say,

$$Q = \bigcup_{j=1}^{r} E^N[b_j], \quad b_j \in \mathbb{P}\left(\amalg_N V^*\right),$$

and that there is a positive constant $\tilde{c}$ such that

$$\|\Xi\|_\rho \le \tilde{c}\|\xi\|_\rho^N, \quad \rho \in S.$$

Then we have

$$\prod_{\rho\in S}\prod_{i=0}^{n-1} \frac{\|\xi\|_\rho^d}{\|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho} \le \left\{ e^c \Big(\max_{\rho\in S} \tilde{c}\|\xi\|_\rho^N \Big)^{\varepsilon} \right\}^{\frac{1}{K}} \left(\prod_{\rho\in S} \|\xi\|_\rho \right)^{(n+1)d},$$

where

$$\xi \notin \bigcup_{\rho\in S}\bigcup_{j=0}^{q} E^d[a_{\rho,j}] \cup Q.$$

If we choose N large enough such that

$$d \mid N, \quad N_0 + 2d \le N \le K,$$

then Lemma 7.30 implies that there is a constant c depending only on S but independent of ξ such that

$$\prod_{\rho\in S}\prod_{i=0}^{n-1} \frac{|||\xi|||_\rho^d}{|||\tilde{\alpha}_{\rho,\lambda(i)}(\xi)|||_\rho} \le cH(\xi)^{(n+1+\varepsilon)d}. \tag{7.106}$$

Therefore Theorem 7.35 follows from (7.92) and (7.106).

Remark on (7.106). If we take $\lambda \in J^q_n$, Lemma 3.16 means that there exists an index $i_0 \in \{0, 1, \ldots, n\}$ such that

$$\|x^{\amalg d}, a_{\rho,\lambda(i_0)}\|_\rho \ge \Gamma_\rho(\mathscr{A}_\rho), \;\; x = \mathbb{P}(\xi).$$

W.l.o.g., we may assume $i_0 = n$. Thus from (7.105), according to the arguments leading up to (7.106) we can obtain

$$\prod_{\rho\in S}\prod_{i=0}^{n} \frac{1}{\|\tilde{\alpha}_{\rho,\lambda(i)}(\xi)\|_\rho} \le c\Big(\max_{\rho\in S} \|\xi\|_\rho \Big)^{\varepsilon}. \tag{7.107}$$

Hence the above method yields also a proof of Theorem 7.37.

Now we exhibit the original subspace theorem of P. Corvaja and U. Zannier [35] as follows:

Theorem 7.42. *For $\rho \in S$, let $f_{i\rho}$, $i = 1, \dots, n-1$, be polynomials in $k[X_1, \dots, X_n]$ of degrees $\delta_{i\rho} > 0$. Put*

$$\delta_\rho = \max_i \delta_{i\rho}, \quad \mu = \min_{\rho \in S} \sum_{i=1}^{n-1} \frac{\delta_{i\rho}}{\delta_\rho}.$$

Fix $\epsilon > 0$ and consider the Zariski closure $\mathcal{H}$ in $\mathbb{P}^n$ of the set of solutions $x \in \mathcal{O}^n_{\kappa,S}$ of

$$\prod_{\rho \in S} \prod_{i=1}^{n-1} |||f_{i\rho}(x)|||_\rho^{\frac{1}{\delta_\rho}} \le H([1,x])^{\mu - n - \epsilon}. \tag{7.108}$$

Suppose that, for $\rho \in S$, X_0 and the $\overline{f}_{i\rho}$, $i = 1, \dots, n-1$, define a variety of dimension 0. Then $\dim \mathcal{H} \le n-1$.

Here for a polynomial $h \in k[X_1, \dots, X_n]$, we denote by $\overline{h}$ the homogenized polynomial in $k[X_0, \dots, X_n]$; namely, $\overline{h}$ is the unique homogeneous polynomial in $k[X_0, \dots, X_n]$, of the same degree as h and such that $\overline{h}(1, X_1, \dots, X_n) = h(X_1, \dots, X_n)$. For the special cases

$$\delta_{i\rho} = d, \quad 1 \le i < n, \ \ \rho \in S,$$

by setting

$$\overline{f}_{0\rho}(X_0, X_1, \dots, X_n) = X_0^d, \quad \rho \in S,$$

and applying the above argument to $\overline{f}_{i\rho}$ $(0 \le i \le n-1)$ replacing $\tilde{\alpha}_{\rho,\lambda(0)}, \dots, \tilde{\alpha}_{\rho,\lambda(n-1)}$, the proof of Theorem 7.42 follows.

Let $X \subset \mathbb{P}^N$ be a projective subvariety of dimension n defined over κ. Assume that $1 \le n < N$. Further, let $c_{\rho i}$ $(\rho \in S, \ i = 0, \dots, N)$ be nonnegative reals. Faltings and Wüstholz [65] proved that the set of solutions of the following system of inequalities

$$\log \left(\frac{\|x_i\|_\rho}{\|x\|_\rho} \right) \le -c_{\rho i} h(x), \quad \rho \in S, \ \ i = 0, \dots, N, \ \ x = [x_0, \dots, x_N] \in X(\kappa) \tag{7.109}$$

is contained in the union of finitely many proper subvarieties of X if the expectation of a particular probability distribution is large than 1. Ferretti [66] showed that this latter condition is equivalent to

$$\frac{1}{(n+1)\deg(X)} \sum_{\rho \in S} e_X(c_\rho) > 1, \tag{7.110}$$

where $c_\rho = (c_{\rho 0}, \dots, c_{\rho N})$ and $e_X(c_\rho)$ is the Chow weight of X with respect to c_ρ. If X is a linear variety, then the result of Faltings and Wüstholz is equivalent to Schmidt's Subspace Theorem. Whereas Schmidt's proof of his subspace theorem is based on techniques from Diophantine approximation and geometry of numbers, Faltings and Wüstholz developed a totally different method, based on Faltings' product theorem.

Using the method of Faltings and Wüstholz, Ferretti obtained a quantitative version of their result, an equivalent version of which reads as follows. Assume that

$$\frac{1}{(n+1)\deg(X)}\sum_{\rho\in S} e_X(c_\rho) > 1+\delta \tag{7.111}$$

with $\delta > 0$. Then there are explicitly computable constants c_1, c_2, c_3 depending on N, n, δ, κ, S and some geometry invariants of X such that the set of solutions of (7.109) with $h(x) \geq c_1(1 + h(X))$ lies in the union of at most c_2 proper subvarieties of X, each of degree $\leq c_3$. Evertse and Ferretti [60] proved another quantitative version of the result of Faltings and Wüstholz, in which the constant c_1, c_2, c_3 depends only N, n, δ and the degree of X. In particular, if the mapping $\xi \longmapsto [f_{\rho 0}(\xi), \ldots, f_{\rho n}(\xi)]$ is a finite morphism from $\mathbb{P}^n$ to $\mathbb{P}^n$ for each $\rho \in S$, then a version of Theorem 7.37 can be deduced from the result of Evertse and Ferretti.

Chapter 8

Vojta's conjectures

P. Vojta proposed the general conjecture in number theory by comparing the second main theorem in Carlson–Griffiths–King's theory. This conjecture is closely related to several important results and problems in Diophantine geometry.

8.1 Mordellic varieties

In 1909, A. Thue [272] proved the following result: Take $m \in \mathbb{Z}$ and let

$$f(x, y) = a_0 x^d + a_1 x^{d-1} y + \cdots + a_d y^d$$

with $a_i \in \mathbb{Z}$ be a form of degree $d \geq 3$ which is irreducible over $\mathbb{Q}$. Then the Diophantine equation

$$f(x, y) = m \tag{8.1}$$

has only finitely many integer solutions (x, y). A simple proof by using Roth's theorem is referred to Schmidt [232]. An equation of the type (8.1) will be called a *Thue equation*.

Theorem 8.1. *Let $P(x)$ be a polynomial of degree $n \geq 2$ over a number field κ such that its discriminant is not identically zero. Let S be a finite subset of M_κ, containing all of the Archimedean absolute values. Then a superelliptic equation*

$$y^d = P(x) \tag{8.2}$$

with $d \geq 2$ and $(d, n) \neq (2, 2)$ has only finitely many solutions $x, y \in \mathcal{O}_{\kappa,S}$.

The special case of an *elliptic equation*, that is, $d = 2,\ n = 3$, was done by Mordell [189], [190]. The general case is due to Siegel [250]. A proof can be found in [232]. Further, Siegel [251] proved that the number of integer points (x, y) of any irreducible curve of genus > 0 is finite. The same conclusion holds for the affine curve C if $\#(M - C) > 2$, where M is a projective closure of C.

Mordell [190] had originally conjectured that on a curve of genus greater than one there are only finitely many rational points, which was first proved by Faltings [63] in 1983. Faltings' proof in 1983 used a variety of advanced techniques from modern algebraic geometry. Vojta [291] then came up with an entirely new proof of Faltings'

theorem using ideas whose origins lie in the classical theory of Diophantine approximation. However, in order to obtain the precise estimates needed for the delicate arguments involved, he made use of Arakelov arithmetic intersection theory and the deep and technical Riemann–Roch theorem for arithmetic threefolds proven by Gillet and Soulé. Faltings [64] then simplified Vojta's proof by eliminating the use of the Gillet–Soulé theorem and proving a "product lemma". Bombieri [13] has combined Faltings' generalization with Vojta's original proof and with other simplifications of his own to give a comparatively elementary proof of the original Mordell conjecture.

We describe an inequality due to Vojta and show how it leads, via an elementary geometric argument, to a proof of Mordell conjecture. Let M be a smooth projective curve of genus $g \geq 2$ defined over a number field κ. Let Θ be the theta divisor on the Jacobian variety $\mathrm{Jac}(M)$ of M, which is ample. Recall that

$$|x| = \sqrt{\hat{h}_\Theta(x)}$$

is the norm on $\mathrm{Jac}(M)$ associated to the canonical height $\hat{h}_\Theta$ relative to Θ defined by (4.74) and that

$$\langle x, y\rangle = \frac{1}{2}\left(|x+y|^2 - |x|^2 - |y|^2\right)$$

is the bilinear form on $\mathrm{Jac}(M)$, which extends to a Euclidean inner product on the vector space $\mathrm{Jac}(M) \otimes \mathbb{R}$ by Proposition 4.54.

We will assume that $M(\kappa)$ is nonempty. Thus we may choose a rational point in $M(\kappa)$ and use it to fix an embedding $M \mapsto \mathrm{Jac}(M)$ defined over κ. Having done this, we can talk about the norm $|z|$ and inner product $\langle z, w\rangle$ for points $z, w \in M(\bar{\kappa})$. We are now ready for *Vojta's inequality* (cf. [289], [13]):

Theorem 8.2. *With notation as above, there are constants $c_1 = c_1(M)$ and $c_2 = c_2(g)$ such that if $z, w \in M(\bar{\kappa})$ are two points satisfying $|z| \geq c_1$ and $|w| \geq c_2|z|$, then*

$$\langle z, w\rangle \leq \frac{3}{4}|z||w|.$$

Now we state and prove the following more general *Mordell–Faltings theorem*:

Theorem 8.3. *If M is an irreducible algebraic curve of genus greater than one and κ is a number field of finite degree over $\mathbb{Q}$, then the set $M(\kappa)$ of κ-rational points on M is a finite set.*

Proof. Set $A = \mathrm{Jac}(M)$. First we observe that the kernel of the mapping $A(\kappa) \mapsto A(\kappa)\otimes\mathbb{R}$ is the torsion subgroup $A_{\mathrm{tors}}(\kappa)$, which is finite by Theorem 4.58. So in order to prove that $M(\kappa)$ is finite, it suffices to show that the image of $M(\kappa)$ in $A(\kappa) \otimes \mathbb{R}$ is finite. By abuse of notation, we will identify $M(\kappa)$ with its image.

The bilinear form $\langle , \rangle$ makes $A(\kappa) \otimes \mathbb{R}$ into a finite-dimensional Euclidean space, and hence for any two points $x, y \in A(\kappa) \otimes \mathbb{R}$, we can define the angle $\theta(x, y)$ between x and y in the usual way:

$$\cos\theta(x, y) = \frac{\langle x, y\rangle}{|x||y|}, \ \ 0 \le \theta(x, y) \le \pi.$$

For any point x_0 and any angle θ_0, we consider the cone with interior angle $2\theta_0$ whose central axis is the ray from 0 through x_0:

$$\Gamma_{x_0,\theta_0} = \{x \in A(\kappa) \otimes \mathbb{R} \mid \theta(x, x_0) < \theta_0\}.$$

We are going to use Vojta's inequality to show that if θ_0 is small enough, then every cone Γ_{x_0,θ_0} intersects $M(\kappa)$ in only finitely many points. To see this, suppose that we have a cone satisfying

$$\#\{\Gamma_{x_0,\theta_0} \cap M(\kappa)\} = \infty.$$

Since $A(\kappa)$, and a fortiori $M(\kappa)$, contains only finitely many points of bounded norm, we can find a $z \in \Gamma_{x_0,\theta_0} \cap M(\kappa)$ with $|z| \ge c_1$, and then we can find a $w \in \Gamma_{x_0,\theta_0} \cap M(\kappa)$ with $|w| \ge c_2|z|$. Here c_1 and c_2 are the constants appearing in Vojta's inequality. Then Vojta's inequality tells us that

$$\langle z, w\rangle \le \frac{3}{4}|z||w|,$$

or equivalently,

$$\cos\theta(z, w) \le \frac{3}{4},$$

which implies

$$\theta(z, w) \ge \arccos\frac{3}{4} > \frac{\pi}{6}.$$

But by assumption, both z and w are in the cone Γ_{x_0,θ_0}, hence the angle between them is less than $2\theta_0$. Thus we have shown that

$$2\theta_0 > \theta(z, w) > \frac{\pi}{6}.$$

This is equivalent to the statement that $\Gamma_{x_0,\pi/12} \cap M(\kappa)$ is finite for every $x_0 \in A(\kappa) \otimes \mathbb{R}$.

In order to complete the proof that $M(\kappa)$ is finite, we now need merely observe that it is possible to cover $A(\kappa) \otimes \mathbb{R}$ by finitely many cones of the form $\Gamma_{x_0,\pi/12}$. If this is not immediately obvious, consider the intersection of such cones with the unit sphere

$$S = \{x \in A(\kappa) \otimes \mathbb{R} \mid |x| = 1\} \subset A(\kappa) \otimes \mathbb{R}.$$

Clearly,

$$S = \bigcup_{x \in S} \{\Gamma_{x,\pi/12} \cap S\},$$

since $x \in \Gamma_{x,\pi/12}$. Further, each set $\Gamma_{x,\pi/12} \cap S$ is an open subset of S, and we know that S is compact, from which it follows that S is covered by finitely many $\Gamma_{x,\pi/12} \cap S$. Since the Γ's are cones, we conclude that the same finite set of Γ's will cover $A(\kappa) \otimes \mathbb{R}$. This completes the proof of Theorem 8.3. □

Elkies [57] (or see [98]) showed that using an explicit version of the abc-conjecture (that is, with a value assigned to $C(\varepsilon)$ in (5.5) for each ε), one can deduce an explicit version of Mordell–Faltings theorem.

Theorem 8.4. *Let κ be a number field, let M be a smooth curve of genus g over κ, and assume that $M(\kappa)$ is not empty. Then there exist constants a and b, which depend on M/κ and on the height, such that*

$$n(r, M(\kappa)) \sim \begin{cases} ae^{br}, & \text{if } g = 0 \ (a, b > 0), \\ ar^b, & \text{if } g = 1 \ (a > 0,\ b \geq 0), \\ a, & \text{if } g \geq 2. \end{cases}$$

Proof. It follows from Theorem 4.31, Theorem 4.37 and Theorem 8.3. □

Conjecture 8.5. *The statement $\#M(\kappa) < \infty$ for every algebraic number field κ is equivalent to $g > 1$, where g is the genus of X.*

See Shafarevich [240].

Let M be a variety defined over an algebraically closed field of characteristic 0. We shall say that M is *Mordellic* if $M(\kappa)$ is finite for every finitely generated field κ over $\mathbb{Q}$. In this context, it is natural to define a variety M to be *pseudo Mordellic* if there exists a proper Zariski closed subset Y of M such that $M - Y$ is Mordellic. Since the counterpart of algebraic curves of genus > 1 in higher dimensional spaces are Kobayashi hyperbolic varieties, accordingly the analogue of Mordell–Faltings theorem is just the Lang's conjecture (cf. [142], [147], [150]):

Conjecture 8.6. *A projective variety is hyperbolic if and only if it is Mordellic.*

The following problem is referred to Shiffman [241].

Conjecture 8.7. *Let M be a projective algebraic variety that contains no rational or elliptic curves. Then there are no holomorphic curves in M.*

Let M be a projective variety. According to Lang [147], [150], the *algebraic special set* $\mathrm{Sp}_{\mathrm{alg}}(M)$ is defined to be the Zariski closure of the union of all images of nonconstant rational mappings $A \longrightarrow M$, where A is an Abelian variety or $\mathbb{P}^1$. Thus $\mathrm{Sp}_{\mathrm{alg}}(M) = \emptyset$ if and only if every rational mapping of an Abelian variety or $\mathbb{P}^1$ into M is constant. In the case of subvarieties of Abelian varieties, a clear description of this special set is well known, that is, the Ueno–Kawamata fibrations in a subvariety of

an Abelian variety constitute the special set (see Lang [150]). A variety M is said to be *algebraically hyperbolic* if $\mathrm{Sp}_{\mathrm{alg}}(M) = \emptyset$. Then one says that M is *pseudo algebraically hyperbolic* if $\mathrm{Sp}_{\mathrm{alg}}(M)$ is a proper subset. Ballico [6] proved that a generic hypersurface of large degree in $\mathbb{P}^n(\mathbb{C})$ is algebraically hyperbolic.

Conjecture 8.8 ([147], [150]). **(i)** $\mathrm{Sp}_{\mathrm{alg}}(M) = \mathrm{Sp}_{\mathrm{hol}}(M)$.

(ii) *The complements of the special sets are Mordellic.*

(iii) *A projective variety M is Mordellic if and only if the special sets are empty.*

Recall that the holomorphic special set $\mathrm{Sp}_{\mathrm{hol}}(M)$ is the Zariski closure of the union of all image of non-constant holomorphic mappings $f : \mathbb{C} \longrightarrow M$. Observe that the claim (i) would give an algebraic characterization of hyperbolicity. The fundamental Diophantine condition conjecturally satisfied by pseudo canonical varieties is the following problem:

Conjecture 8.9. *Let M be a pseudo canonical variety defined over a number field κ. Then $M(\kappa)$ is not Zariski dense in M.*

Bombieri posed Conjecture 8.9 for pseudo canonical surfaces, and Lang (independently) formulated the general conjecture in its refined form of the exceptional Zariski closed subset. Conjecture 8.8 allows us to state the final form of the Bombieri-Lang conjecture.

Conjecture 8.10 ([147], [150]). *The following conditions are equivalent for a projective variety M.*

(1) *M is pseudo canonical;*

(2) *$\mathrm{Sp}_{\mathrm{alg}}(M)$ is a proper subset;*

(3) *M is pseudo Mordellic. The Zariski closed subset Y can be taken to be $\mathrm{Sp}_{\mathrm{alg}}(M)$.*

In the case of Abelian varieties, there is the following Lang's conjecture over finitely generated fields (cf. Lang [139], [150]):

Conjecture 8.11. *Let M be a subvariety of an Abelian variety over a field κ finitely generated over $\mathbb{Q}$. Then M contains a finite number of translations of Abelian subvarieties which contain all but a finite number of points of $M(\kappa)$.*

The following especially important case from Lang [140] has now been proved by Faltings [64]:

Theorem 8.12. *Let M be a subvariety of an Abelian variety, and suppose that M does not contain any translation of an Abelian subvariety of dimension ≥ 1. Then M is Mordellic.*

Hilbert's tenth problem asks whether there is a general algorithm to determine, given any polynomial in several variables, whether there exists a zero with all coordinates in $\mathbb{Z}$. It was solved in the negative by Yu. Matiyasevich [171] in 1970; for a general reference, see [172]. J. Richard Büchi attempted to prove a similar statement in which there may be any (finite) number of polynomials, but they must be quadratic and of a certain form:

$$\sum_{j=1}^{n} a_{ij}x_j^2 = b_i, \;\; i = 1, \ldots, m$$

with $\{a_{ij}, b_i\} \subset \mathbb{Z}$, $\{m, n\} \subset \mathbb{Z}^+$. Büchi was able to show that a negative resolution of this question would follow from the following "*n-squares problem*":

Conjecture 8.13. *For large enough n, the only integer solutions of the system of equations*

$$x_k^2 + x_{k-2}^2 = 2x_{k-1}^2 + 2, \;\; k = 2, \ldots, n-1 \tag{8.3}$$

satisfy $\pm x_k = \pm x_{k-1} + 1$.

Let M be the projective variety in $\mathbb{P}^n(\mathbb{C})$ defined by the equations

$$x_k^2 + x_{k-2}^2 = 2x_{k-1}^2 + 2x^2, \;\; k = 2, \ldots, n-1$$

in the homogeneous coordinates $[x, x_0, \ldots, x_{n-1}]$. Vojta [295] observed that for $n \geq 6$ the variety M is a pseudo canonical surface, and then showed:

Theorem 8.14. **(i)** *For $n \geq 8$, the only curves on M of geometric genus 0 and 1 are the "trivial" lines*

$$\pm x_k = \pm x_0 + kx, \;\; k = 0, \ldots, n-1.$$

(ii) *Let $n \geq 8$ be an integer and let $f : \mathbb{C} \longrightarrow M$ be a non-constant holomorphic curve. Then the image of f lies in one of the "trivial" lines.*

The statement (i) of Theorem 8.14 has a consequence that if Conjecture 8.9 is true then Büchi's problem has a positive answer. Statement (ii) shows that the analogue of Büchi's problem for holomorphic functions has a positive answer.

8.2 Main conjecture

Let κ be a number field and let $S \subset M_\kappa$ be a finite set containing all Archimedean places. P. Vojta [287] observed that some conditions of the second main theorem in Carlson–Griffiths–King's theory may be relaxed somewhat, and then translated it into the following *main conjecture* in number theory.

Conjecture 8.15. *Let X be a nonsingular complete variety over κ. Let K be the canonical divisor of X, and let D be a normal crossings divisor on X. If $\varepsilon > 0$, and if E is a pseudo ample divisor, then there exists a proper Zariski closed subset $Z = Z(X, D, \kappa, E, \varepsilon, S)$ such that for all $x \in X(\kappa) - Z$,*

$$m(x, D) + h_K(x) \leq \varepsilon h_E(x) + O(1). \tag{8.4}$$

The requirement in Conjecture 8.15 that D have only normal crossings is necessary, since it is easy to produce counterexamples if this condition is dropped. The above inequality is called *Vojta's height inequality*.

Example 8.16. Each hyperplane E of $\mathbb{P}^n(\bar{\kappa})$ is very ample with

$$\dim \mathcal{L}(E) = n + 1,$$

and hence the dual classification mapping φ is the identity. Thus $h_E(x) = h(x)$, and hence

$$h_K(x) = -(n+1)h(x)$$

since $K = -(n+1)E$. Let $D = \sum_i \ddot{E}[a_i]$ be a sum of hyperplanes in general position. Then the conjecture reduces to

$$\sum_i m(x, a_i) < (n + 1 + \varepsilon)h(x)$$

which follows from Schmidt's subspace theorem.

Let $V = V_\kappa$ be a vector space of finite dimension $n+1 > 0$ over κ. Conjecture 8.15 contains the following special case:

Conjecture 8.17. *Take $a_i \in \mathbb{P}(\amalg_d V_{\bar{\kappa}}^*)$ such that $\sum_i \ddot{E}^d[a_i]$ has normal crossings. Then for $\varepsilon > 0$ there exists a proper Zariski closed subset Z such that for all $x \in \mathbb{P}(V) - Z$,*

$$\sum_i m\left(x^{\amalg d}, a_i\right) \leq (n + 1 + \varepsilon)\, h(x).$$

We propose the following conjecture:

Conjecture 8.18. *Take a positive real number $\varepsilon > 0$ and integers $q \geq n \geq r \geq 1$. Assume that for $\rho \in S$, a family*

$$\mathscr{A}_\rho = \{a_{\rho,0}, \ldots, a_{\rho,q}\} \subset \mathbb{P}(\amalg_d V^*)$$

is admissible. Then the set of points of $\mathbb{P}(V) - \bigcup \ddot{E}^d[a_{\rho,j}]$ satisfying

$$\sum_{\rho \in S} \sum_{j=0}^{q} \log \frac{1}{|||x^{\amalg d}, a_{\rho,j}|||_\rho} \geq d(2n - r + 1 + \varepsilon)h(x) + O(1)$$

is contained in a finite union of subvarieties of dimension $\leq r - 1$ of $\mathbb{P}(V_{\bar{\kappa}})$.

In [103] (or see [108]), we proposed this conjecture for the case $r = 1$.

P. Vojta [294] proved that Conjecture 5.3 of Masser and Oesterlé would be derived from a weakening of Conjecture 8.15.

Conjecture 8.15 implies the Bombieri–Lang Conjecture 8.9. Recall that a variety X is said to be pseudo canonical if its canonical bundle K_X is pseudo ample. Indeed, if X is such a variety, we may assume X nonsingular since both the notion of pseudo canonicity and non-denseness in the Zariski topology are birational invariants. Then Conjecture 8.15 with $D = 0$ implies that

$$h_K \leq \varepsilon h_E + O(1) \tag{8.5}$$

on an open dense set. But taking $E = K$ and $\varepsilon < 1$ implies that h_K is bounded, which is a contradiction unless $X(\kappa)$ is contained in a Zariski closed subset of X, that is, $X(\kappa)$ is degenerate.

Conjecture 8.15 also implies the Mordell conjecture since curves are pseudo canonical if and only if their genus is at least two, and degeneracy on curves reduces to finiteness. In fact, Conjecture 8.15 is known for curves.

Theorem 8.19. *Let X be a nonsingular projective curve defined over an algebraic number field κ. Let K be the canonical divisor of X, and let D be an effective divisor on X. If $\varepsilon > 0$, then there exists a finite subset $Z = Z(X, D, \kappa, \varepsilon, S)$ such that for all $x \in X(\kappa) - Z$,*

$$m(x, D) + h_K(x) \leq \varepsilon h(x) + O(1). \tag{8.6}$$

Proof. It is nothing if $X(\kappa)$ is empty, so we may assume that $X(\kappa)$ is non-empty. If the genus of X is zero, then Theorem 3.72 means that the curve X is isomorphic over κ to $\mathbb{P}^1$ if and only if it possesses a κ-rational point. Thus the canonical divisor K has degree -2, $h_K(x) = -2h(x)$, and hence (8.6) becomes

$$\sum_{j=1}^{q} m(x, a_j) - 2h(x) \leq \varepsilon h(x) + O(1)$$

for $D = \sum_{j=1}^{q} a_j$. Theorem 8.19 follows from Roth's theorem.

Now assume that the genus of X is ≥ 1. In 1929 C. L. Siegel applied his theorem on the approximation of algebraic numbers by algebraic numbers from a fixed number field to the situation of algebraic curves. His result, as extended by Mahler, can be reinterpreted as follows. If D is an effective divisor on X (of genus ≥ 1) defined over $\bar{\kappa}$, then, for any $\varepsilon > 0$, we have

$$m(x, D) < \varepsilon h(x)$$

for almost all $x \in X(\kappa)$ (i.e. finitely many exceptional). When X is of genus 1, its canonical divisor is trivial, and hence Theorem 8.19 follows from Siegel–Mahler's theorem.

In the case that the genus of X is greater than or equal to two, we note that the canonical divisor K is positive. Thus if taking $D = \emptyset$, then (8.6) becomes

$$h_K(x) \leq \varepsilon h(x) + O(1)$$

According to the arguments above, this is equivalent to the statement that $X(\kappa)$ is finite. Therefore, Theorem 8.19 follows from Siegel–Mahler's theorem and Faltings' theorem. □

In [290], Vojta has given a direct proof of his height inequality for curves. This gives a unified proof of Faltings's, Roth's, and Siegel's theorems.

Let A denote an Abelian variety and let D be an ample divisor on A. Lang [140] conjectured that A has only finitely many (S, D)-integralizable points. Vojta [287] showed that the Lang's conjecture follows from the main conjecture.

Qualitatively, Conjecture 8.15 also has the following simple consequence.

Conjecture 8.20. *Let X be a nonsingular projective variety defined over a number field κ. Let K be the canonical divisor of X, and D a normal crossings divisor on X. Suppose that $K + D$ is pseudo ample. Then $X - D$ is pseudo Mordellic.*

Related to Conjecture 8.20, A. Levin [158] proposed *main Siegel-type conjecture* as follows:

Conjecture 8.21. *Let X be a projective variety defined over a number field κ. Let $D = D_1 + \cdots + D_q$ be a divisor on X with the D_i's effective Cartier divisors for all i. Suppose that at most m D_i's meet at a point, so that the intersection of any $m + 1$ distinct D_i's is empty. Suppose that $\dim D_i \geq n_0 > 0$ for all i. If $q > m + \frac{m}{n_0}$ then there does not exist a Zariski-dense set of κ-rational (S, D)-integralizable points on X.*

Siegel's theorem [251] is the case $m = n_0 = \dim X = 1$ of Conjecture 8.21, or see [34] for a new proof of Siegel's theorem. When X is a surface, $m \leq 2$, and the D_i's have no irreducible components in common, A. Levin [158] proved Conjecture 8.21. At the extreme of n_0, there is the following special case.

Conjecture 8.22. *Let X be a projective variety defined over a number field κ. Let $D = D_1 + \cdots + D_q$ be a divisor on X with the D_i's effective Cartier divisors for all i. Suppose that at most m D_i's meet at a point. If D_i is pseudo ample for all i and $q > m + \frac{m}{\dim X}$ then $X - D$ is pseudo Mordellic.*

We recall the following theorem, which is a consequence of Mori theory (cf. [191], Lemma 1.7).

Theorem 8.23. *Let N be a nonsingular complex projective variety of dimension n with the canonical divisor K. If $D_1, \ldots, D_{n+2}$ are ample divisors on N, then $K + D_1 + \cdots + D_{n+2}$ is ample.*

When $q > 2m \dim X$, A. Levin [158] proved Conjecture 8.22 based on a formulation of Corvaja–Zannier theorems in [34] and [36]. Further, A. Levin [158] proved that $X - D$ is Mordellic if D_i is ample for all i. By using Theorem 8.23, when X is nonsingular, the D_i's are ample, and $D = D_1 + \cdots + D_q$ has normal crossings, we see that Conjecture 8.22 is a consequence of Conjecture 8.20.

8.3 General conjecture

Let κ be a number field and let S be a finite subset of M_κ containing the Archimedean places. By abuse of notation, let

$$d(x) = d_\kappa(x) := d_{\kappa(x)/\kappa},$$

$$d_S(x) = d_{\kappa,S}(x) := d_{\kappa(x)/\kappa,S}$$

if x is a closed point of a variety. P. Vojta ([287], [293]) proposed the following *general conjecture with ramification*:

Conjecture 8.24. *Let X be a complete nonsingular variety over κ, let K be the canonical divisor of X, let D be a normal crossings divisor on X, let E be a pseudo ample divisor on X, let $\varepsilon > 0$, and let $r \in \mathbb{Z}^+$. Then there exists a proper Zariski closed subset $Z = Z(r, X, D, \kappa, E, \varepsilon, S)$ such that*

$$m(x, D) + h_K(x) \le d(x) + \varepsilon h_E(x) + O(1) \tag{8.7}$$

for all $x \in X(\bar{\kappa}) - Z$ with $[\kappa(x) : \kappa] \le r$.

Under the assumptions of Conjecture 8.24, noting that the first main theorem

$$m(x, D) + N(x, D) = h_D(x) + O(1),$$

then (8.7) is equivalent to

$$h_D(x) + h_K(x) \le d(x) + N(x, D) + \varepsilon h_E(x) + O(1). \tag{8.8}$$

P. Vojta [293] further asked whether $N(x, D)$ could be replaced by the truncated valence function:

Conjecture 8.25. *Conjecture 8.24 holds with* (8.7) *replaced by*

$$h_D(x) + h_K(x) \le d(x) + \overline{N}(x, D) + \varepsilon h_E(x) + O(1). \tag{8.9}$$

We always have the inequality

$$\overline{N}(x, D) \le N(x, D),$$

so Conjecture 8.25 is obviously stronger than Conjecture 8.24.

P. Vojta [293] explained that the inequality (8.9) generalizes that of the abc-conjecture of Masser and Oesterlé. Under the assumptions of Conjecture 5.3, the triple (a, b, c) determine a point

$$x = [a, b, -c] \in \mathbb{P}^2,$$

which lies on the line

$$X : \xi_0 + \xi_1 + \xi_2 = 0.$$

Since $(a, b, c) = 1$, the height of this point is

$$h(x) = \log \sqrt{a^2 + b^2 + c^2}.$$

The relative primeness condition also implies that the curve on $\mathbb{P}^2_{\mathbb{Z}}$ corresponding to x meets the divisor $H_0 = (\xi_0 = 0)$ at a prime p if and only if $p|a$. Similarly, it meets the divisors $H_1 = (\xi_1 = 0)$ and $H_2 = (\xi_2 = 0)$ at p if and only if $p|b$ and $p|c$, respectively. Let H be the divisor

$$H = H_0 + H_1 + H_2$$

on $\mathbb{P}^2$ and set $D = H|_X$. For $S = \{\infty\}$, $\kappa = \mathbb{Q}$, one has

$$\overline{N}(x, D) = \sum_{p|abc} \log p.$$

Thus (5.5) can be written

$$h(x) \leq (1 + \varepsilon)\overline{N}(x, D) + O(1)$$

or (with a different ε)

$$h(x) \leq \overline{N}(x, D) + \varepsilon h(x) + O(1) \tag{8.10}$$

for all abc-points $x \in \mathbb{P}^2$.

Note that D consists of three distinct points, and that

$$K \sim -2E,\ K + D \sim E,$$

where $[E]$ is the restriction of hyperplane line bundle of $\mathbb{P}^2$ on X. Hence

$$h_D(x) + h_K(x) = h_{K+D}(x) + O(1) = h_E(x) + O(1).$$

Since $h_E(x) = h(x)$, then (8.10) becomes

$$h_D(x) + h_K(x) \leq \overline{N}(x, D) + \varepsilon h_E(x) + O(1),$$

which coincides with (8.9) since we are dealing with rational points and therefore $d(x) = 0$ for all x.

In this case, we hope that the exceptional set Z in Conjecture 8.25 is same with the abc-exceptional set E_{abc}.

Next one shows that Conjecture 8.25 also follows from Conjecture 8.24. We start with several lemmas (cf. [293]).

Lemma 8.26. *Let $\pi : X' \longrightarrow X$ be a generically finite morphism of smooth varieties, and let D and D' be normal crossings divisors on X and X', respectively, such that* $\operatorname{supp} D' = (\pi^* D)_{\mathrm{red}}$. *Let K and K' be the canonical divisors on X and X', respectively. Then*

$$K' + D' \geq \pi^*(K + D)$$

relative to the cone of the canonical divisors with $h^0 > 0$. Moreover,

$$[K' + D'] \otimes \pi^*[K + D]^\vee$$

has a global section vanishing only on the support of D' or where π ramifies.

Proof. We have a natural mapping

$$\pi^* \Omega^1_X[\log D] \longrightarrow \Omega^1_{X'}[\log D']$$

which is an isomorphism at generic points of X'; hence taking the maximal exterior power gives an injection of line bundles $\pi^*[K + D] \longrightarrow [K' + D']$. See [117], § 11.4a. □

Consequently, one may use Chow's lemma and resolution of singularities to find a smooth projective variety X' and a proper birational morphism $\pi : X' \longrightarrow X$ such that $D' := (\pi^* D)_{\mathrm{red}}$ has normal crossings; the lemma then shows that

$$h_{K'+D'} \geq h_{K+D} \circ \pi + O(1)$$

outside of a proper Zariski-closed subset. Since

$$\operatorname{supp} D' = \pi^{-1}(\operatorname{supp} D),$$

we have

$$\overline{N}(x, D') = \overline{N}(\pi(x), D) + O(1), \;\; x \in X'(\bar{\kappa});$$

hence Conjecture 8.25 for X' and D' implies the same conjecture for X and D. Thus we may assume that X is projective.

Note that if D and D_1 are effective divisors such that $D + D_1$ has normal crossings, then Conjecture 8.25 for $D + D_1$ implies that the conjecture holds also for D. Indeed,

$$\overline{N}(x, D + D_1) - \overline{N}(x, D) \leq \overline{N}(x, D_1) \leq N(x, D_1) \leq h_{D_1}(x) + O(1),$$

so (8.9) with D replaced by $D + D_1$ implies the original (8.9). Thus, we may assume that D is very ample.

Lemma 8.27. *Take $e \in \mathbb{Z}^+$ and let D_1 be an effective divisor such that $D_1 \sim D$ and $D + D_1$ has normal crossings. Then there is a smooth variety X_1 and a proper generically finite morphism $\pi_1 : X_1 \longrightarrow X$ such that the support of the ramification divisor of π_1 is equal to $\pi_1^{-1}(\operatorname{supp}(D + D_1))$, all components of $\pi_1^*(D + D_1)$ have multiplicity $\geq e$ unless they lie over $D \cap D_1$, $(\pi_1^*(D + D_1))_{\mathrm{red}}$ has normal crossings, and $\bar{\kappa}(X_1) = \bar{\kappa}(X)(\sqrt[e]{f})$ for some $f \in \bar{\kappa}(X)_*$.*

Proof. Take $f \in \bar{\kappa}(X)_*$ such that $(f) = D - D_1$. Let $\pi_0 : X_0 \longrightarrow X$ be the normalization of X in the field $\bar{\kappa}(X)(\sqrt[e]{f})$, let $\pi : X_1 \longrightarrow X_0$ be a desingularization of X_0 such that $(\pi^*(\pi_0^*(D + D_1)))_{\mathrm{red}}$ has normal crossings, and let $\pi_1 = \pi_0 \circ \pi$. We may assume that π_1 is étale outside of $\pi_0^{-1}(\operatorname{supp} D)$. If $x \notin D \cap D_1$, then there is an open neighborhood U of x such that $D|_U = (f)$ and $D_1|_U = 0$, or $D|_U = 0$ and $D_1|_U = (1/f)$. Then $\pi_0^*(D + D_1)$ over U is e times the principal divisor $(\sqrt[e]{f})$ or $(1/\sqrt[e]{f})$. Therefore all components of $\pi_1^*(D + D_1)$ meeting $\pi_1^{-1}(U)$ have multiplicity divisible by e. □

Lemma 8.28. *There exists a normal crossings divisor D^* on X such that*

(i) *$D^* - D$ is effective;*

(ii) *for all $e \in \mathbb{Z}^+$ there exists a smooth variety X' and a proper generically finite morphism $\pi : X' \longrightarrow X$ such that $(\pi^*D)_{\mathrm{red}}$ has normal crossings and all components of π^*D have multiplicity $\geq e$ (or zero);*

(iii) *$\pi : X' \longrightarrow X$ is unramified outside of $\pi^{-1}(\operatorname{supp} D)$; and*

(iv) *$\bar{\kappa}(X') = \bar{\kappa}(X)(\sqrt[e]{f_1}, \ldots, \sqrt[e]{f_n})$ for some $f_1, \ldots, f_n \in \bar{\kappa}(X)_*$.*

Proof. Let $n = \dim X$, and let $D_1, \ldots, D_n$ be effective divisor on X such that $D_i \sim D$ for all i,

$$D^* := D + D_1 + \cdots + D_n$$

has normal crossings, and

$$D \cap D_1 \cap \cdots \cap D_n = \emptyset.$$

Such divisors exist by Bertini's theorem.

Take $e \in \mathbb{Z}^+$. For $i = 1, \ldots, n$, let $\pi_i : X_i \longrightarrow X$ be as in Lemma 8.27, applied to the divisors $D_i \sim D$. Let $\pi : X' \longrightarrow X$ be a desingularization of the normalization of X in the compositum $\bar{\kappa}(X_1) \cdots \bar{\kappa}(X_n)$ such that $(\pi^*D)_{\mathrm{red}}$ has normal crossings and X' dominates $X_1, \ldots, X_n$. We may also assume that π is étale outside of $\pi^{-1}(\operatorname{supp} D)$. Take a component E of π^*D. There exists some i such that

$$\pi(E) \subseteq D \cup D_i, \;\; \pi(E) \nsubseteq D \cap D_i;$$

then the image of E in X_i is contained in a component of $\pi^{-1}(D + D_1)$ of multiplicity $\geq e$. □

After replacing D with D^*, we have the following situation: D has normal crossings, X' is smooth, $D' := (\pi^*D)_{\mathrm{red}}$ has normal crossings, all components of π^*D have multiplicity $\geq e$, and $\pi : X' \longrightarrow X$ is unramified outside of D'.

Lemma 8.29. *Take models $\mathcal{X}$ and $\mathcal{X}'$ for X and X', respectively, for which the divisors D and D' extend to effective divisors on $\mathcal{X}$ and $\mathcal{X}'$, respectively, and π extends to a morphism $\pi : \mathcal{X}' \longrightarrow \mathcal{X}$. Let S be the set of places of κ containing*

(1) *all Archimedean places;*

(2) *all places lying over e;*

(3) *all places of bad reduction for $\mathcal{X}$ and $\mathcal{X}'$;*

(4) *all places where D and D' have vertical components; and*

(5) *all places where π is ramified outside the support of D'.*

Take $r \in \mathbb{Z}^+$. For points $x \in X(\bar{\kappa}) - \operatorname{supp} D$ of degree $\le r$ over κ and points $x' \in \pi^{-1}(x)$, we have

$$d(x') - d(x) + N(x', D') \le \overline{N}(x, D) + \frac{1}{e} h_D(x) + O(1), \tag{8.11}$$

where the constant in $O(1)$ depends only on X, D, e, X', π, r, and S.

Proof. By (4.61), one has

$$d(x') - d(x) = d_S(x') - d_S(x) + O(1). \tag{8.12}$$

Let $K = \kappa(x)$ and $K' = \kappa(x')$. For places $w' \in M_{K'}$ lying over places $w \in M_K$, let $e_{K'/K}(w')$ denote the ramification index of w' over w. By (4.62), one then has

$$d_S(x') - d_S(x) = \sum_{w' \in M_{K'} - S} \frac{e_{K'/K}(w') - 1}{[K' : \mathbb{Q}]} \log \mathcal{N}(\mathfrak{p}_{w'}).$$

If the closure in $\mathcal{X}'$ of x' does not meet D' at w', then K' is unramified over K at w'; if it does meet, then $e_{K'/K}(w') \le e$ because K' is generated over K by e-th roots of elements of K (by condition (iii) in Lemma 8.28). Thus

$$d_S(x') - d_S(x) \le (e-1)\overline{N}(x', D').$$

Combining this with (8.12) then gives

$$d(x') - d(x) \le (e-1)\overline{N}(x', D') + O(1). \tag{8.13}$$

On the other hand,

$$\overline{N}(x, D) - \overline{N}(x', D') \ge (e-1)\overline{N}(x', D')$$

since all components of $\pi^* D$ have multiplicity $\ge e$. Also

$$N(x', D') - \overline{N}(x', D') \le N(x', D') \le \frac{1}{e} N(x, D) \le \frac{1}{e} h_D(x) + O(1).$$

Combining these two inequalities then gives

$$\overline{N}(x, D) - N(x', D') + \frac{1}{e} h_D(x) \ge (e-1)\overline{N}(x', D') + O(1).$$

Combining this with (8.13) then gives (8.11). □

Finally, we prove that Conjecture 8.24 implies Conjecture 8.25. By Kodaira's lemma, we may assume (after adjusting ε) that E is ample. Then

$$h_D \le ch_E + O(1) \tag{8.14}$$

for some constant c depending only X, D, and E. Take $e \in \mathbb{Z}^+$ with $e \ge c/\varepsilon$, and let X' be a generically finite cover of X as in Lemma 8.28. Let D and D' be as discussed following that lemma, and enlarge S so that the conditions of Lemma 8.29 hold. This will ultimately give an inequality (8.9) relative to this larger set S, which trivially implies the same inequality for the original S. Points $x \in X(\bar{\kappa}) - \operatorname{supp} D$ of bounded degree lift to points $x' \in X'(\bar{\kappa})$, also of bounded degree. We now show that Conjecture 8.24 applied to x' and D' implies Conjecture 8.25 for D and X. By the former conjecture (using (8.8)), we have

$$h_{D'}(x') + h_{K'}(x') \le d(x') + N(x', D') + \varepsilon' h_{E'}(x') + O(1), \tag{8.15}$$

provided $x' \notin Z'$, where Z' is a proper Zariski-closed subset (depending also on ε' and E'); here E' is a pseudo ample divisor on X'. We want to show that (8.15) implies Conjecture 8.25; i.e., (8.9).

By Lemma 8.26, $[K' + D'] \otimes \pi^*[K + D]^\vee$ has a global section vanishing nowhere on $X' - \operatorname{supp} D'$; hence, by functoriality of heights and positivity of heights relative to effective divisors,

$$h_{D+K}(x) \le h_{D'+K'}(x') + O(1) \tag{8.16}$$

for all $x \in X'(\bar{\kappa}) - D'$.

By Lemma 8.29,

$$d(x') + N(x', D') \le d(x) + \overline{N}(x, D) + \frac{1}{e} h_D(x) + O(1). \tag{8.17}$$

Let $E' = \pi^* E$; this is pseudo ample on X'; also choose $\varepsilon' > 0$ such that $\varepsilon' < \varepsilon - c/e$. By (8.14), we then have

$$\frac{1}{e} h_D(x) + \varepsilon' h_{E'}(x') \le \varepsilon h_E(x) + O(1). \tag{8.18}$$

Thus, (8.16)–(8.18), combined with (8.15), imply that (8.9) holds if x lies outside the proper Zariski-closed subset $Z := \pi(Z')$.

8.4 Vojta's $(1,1)$-form conjecture

Vojta compares the discriminant term as follows:

Theorem 8.30. *Let $\pi : X \longrightarrow W$ be a generically finite separable surjective morphism of complete nonsingular varieties over a number field κ, with ramification divisor R. Let S be a finite set of absolute values. Then for all $P \in X(\bar{\kappa}) - R$, we have*

$$d(P) - d(\pi(P)) \le N(P, R) + O(1).$$

Vojta's Theorem 8.30 is a generalization to the ramified case of a classical theorem of Chevalley–Weil.

P. Vojta in [287] showed that Conjecture 5.3 of Masser and Oesterlé is an easy consequence of Conjecture 8.24, and in [294] noted that Conjecture 8.15 is possibly weaker than Conjecture 8.24. Conversely, van Frankenhuysen [286] proved that the abc-conjecture implies Vojta's general conjecture for curves, i.e. when X is one-dimensional. Lang [150] conjectures that Vojta's general conjecture is best possible for any curve of nonzero genus over a number field.

A. Levin [158] gave the following conjectural upper bound on the logarithmic discriminant in terms of heights.

Conjecture 8.31. *Let X be a nonsingular projective variety of dimension n defined over a number field κ with canonical divisor K. Let E be a pseudo ample divisor on X. Let r be a positive integer and let $\varepsilon > 0$. Then there exists a proper Zariski closed subset Z such that*

$$d(x) \le h_K(x) + (2[\kappa(x) : \kappa] + n - 1 + \varepsilon)h_E(x) + O(1) \tag{8.19}$$

for all $x \in X(\bar{\kappa}) - Z$ with $[\kappa(x) : \kappa] \le r$.

If E is ample, A. Levin [158] conjectured that the set Z in Conjecture 8.31 is empty. It is a result of Silverman [255] that Conjecture 8.31 is true for $X = \mathbb{P}^n$ with $\varepsilon = 0$ and $r = \infty$, i.e., the inequality holds for all $x \in X(\bar{\kappa})$. For curve, Conjecture 8.31 is true by a result of Song and Tucker [260] (cf. Eq. 2.0.3). They proved the stronger statement.

Theorem 8.32. *Let X be a nonsingular projective curve defined over a number field κ with canonical divisor K. Let E be an ample divisor on X. Let r be a positive integer and let $\varepsilon > 0$. Then*

$$d(x) \le d_a(x) \le h_K(x) + (2[\kappa(x) : \kappa] + \varepsilon)h_E(x) + O(1) \tag{8.20}$$

for all $x \in X(\bar{\kappa})$ with $[\kappa(x) : \kappa] \le r$.

In the inequality (8.20), $d_a(x)$ is the arithmetic discriminant of x. For the definition and properties, see Vojta [288]. Related to the arithmetic discriminant, Vojta [290] proved the following generalization of Falting's theorem on rational points on curves.

Theorem 8.33. *Let X be a nonsingular projective curve defined over a number field κ with canonical divisor K. Let D be an effective divisor on X with no multiple components and E ample divisor on X. Let r be a positive integer and let $\varepsilon > 0$. Then the following inequality*

$$m(x, D) + h_K(x) \le d_a(x) + \varepsilon h_E(x) + O(1) \tag{8.21}$$

holds for all $x \in X(\bar{\kappa}) - D$ with $[\kappa(x) : \kappa] \le r$.

Generalizing the main Siegel-type conjecture, A. Levin [158] further proposed *general Siegel-type conjecture* as follows:

Conjecture 8.34. *Let X be a projective variety defined over a number field κ. Let $D = D_1 + \cdots + D_q$ be a divisor on X with the D_i's effective Cartier divisors for all i. Suppose that at most m D_i's meet at a point. Suppose that $\dim D_i \geq n_0 > 0$ for all i. Let d be a positive integer. If $q > m + \frac{m(2d-1)}{n_0}$ then there does not exist a Zariski-dense set of (S, D)-integralizable points on X of degree d over κ.*

According to the definition, the *degree* of a set $R \subset X(\bar{\kappa})$ over κ is defined to be

$$\deg_\kappa R = \sup_{x \in R} [\kappa(x) : \kappa].$$

Based on Conjecture 8.31, A. Levin [158] shows that Vojta's general conjecture implies general Siegel-type conjecture if D_i is ample for all i and D has normal crossings. Theorem 8.32 and Theorem 8.33 imply that Levin's general Siegel-type conjecture is true for curves.

In [287], Vojta also proposed the following $(1,1)$*-form conjecture*:

Conjecture 8.35. *Let X be a complete nonsingular variety over a number field κ contained in $\mathbb{C}$ and let D be a normal crossings divisor on X. Let ω be a positive $(1,1)$-form on $X - D$ whose holomorphic sectional curvatures are bounded from above by $-c < 0$, i.e. for any nonconstant holomorphic mapping $f : U \longrightarrow X$ ($U \subseteq \mathbb{C}$ is an open subset), one has*

$$\mathrm{Ric}(f^*\omega) \geq c f^*\omega.$$

Also assume that $\omega \geq c_1(L, \rho)$ for some metric ρ on a line bundle L on X. Let E be a pseudo ample divisor on X. Let S be a finite set of absolute values. Let I be a set of (S, D)-integralizable points of bounded degree over κ. Let $\varepsilon > 0$. Then for all points $P \in I$ we have

$$h_L(P) \leq \frac{1}{c} d(P) + \varepsilon h_E(P) + O(1).$$

Vojta [287] applies the $(1,1)$-form conjecture to deduce several number theoretic applications in which he proves that Conjecture 8.35 implies a conjecture of Shafarevich on the finiteness of curves with good reduction, proved by Faltings [62], [63].

We [111] suggested the following problem:

Conjecture 8.36. *Let X be a complete nonsingular variety over a number field κ. Let D be a divisor on X satisfying $|mK - D| \neq \emptyset$ for a positive integer m. Let E be a pseudo ample divisor on X. Let $\varepsilon > 0$. Then there exists a proper Zariski closed subset Z such that for all points $P \in X(\kappa) - Z$ we have*

$$h_D(P) \leq m d(P) + \varepsilon h_E(P) + O(1). \tag{8.22}$$

Recall that $|mK - D|$ is the complete linear system of $mK - D$ in which K is a canonical divisor of X. Conjecture 8.36 could be derived by Conjecture 8.24 simply. In fact, since $|mK-D|$ contains at least one effective divisor, say, D', which is linearly equivalent to $mK - D$, we have

$$mh_K - h_D = h_{D'} + O(1) \geq -O(1).$$

Thus (8.22) follows from (8.7) by taking $D = 0$.

8.5 abc-conjecture implies Vojta's height inequality

Let X be a curve over a number field κ, and let D be a finite set of algebraic points of X, defined over κ. Let $f : X \longrightarrow \mathbb{P}^1$ be a Belyĭ function for D (see Theorem 5.2). The divisors

$$D_0 = f^*(0), \quad D_1 = f^*(1), \quad D_\infty = f^*(\infty)$$

have a decomposition over κ into irreducible divisors

$$\begin{aligned} D_0 &= e_1P_1 + \cdots + e_iP_i, \\ D_1 &= e_{i+1}P_{i+1} + \cdots + e_jP_j, \\ D_\infty &= e_{j+1}P_{j+1} + \cdots + e_kP_k. \end{aligned}$$

According to (5.4), the canonical divisor of X is given by

$$K = f^*(1) - f^{-1}\{0, 1, \infty\} = D_1 - \sum_{\nu=1}^{k} P_\nu.$$

Let x be a point of $X(\bar{\kappa})$, defined over $K = \kappa(x)$, such that $f(x) \neq 0, 1, \infty$. We apply the abc-conjecture to the point $y = [f(x), 1 - f(x), 1]$ to deduce that the height of x is bounded. Note that

$$h(y) = h_{D_1}(x).$$

We estimate the radical of y. We can construct a projective scheme $\pi : \mathcal{X} \longrightarrow \mathrm{Spec}\mathcal{O}_K$, and obtain a section

$$\tilde{x} : \mathbb{M}_K \longrightarrow \mathcal{X}.$$

We can define the closure of D to be its Zariski closure $\bar{D}$ in $\mathcal{X}$. Let $w \notin S$ (i.e. w does not restrict to a multiple of a valuation in S), so that w is non-Archimedean. The prime w contributes

$$\frac{1}{[K : \mathbb{Q}]} \log \mathcal{N}(\mathfrak{p}_w)$$

to the radical $\overline{N}(y, E)$ in Conjecture 5.23 if and only if $w(f(x)) < 0$, $w(1-f(x)) < 0$ or $w(f(x)) > 0$. In other words, w contributes to the radical only if $\deg_w \tilde{x}^* \bar{D}_0$, $\deg_w \tilde{x}^* \bar{D}_1$ or $\deg_w \tilde{x}^* \bar{D}_\infty$ is positive. Since

$$\deg_w \tilde{x}^* \bar{D}_0 = \sum_{\mu=1}^{i} e_\mu \deg_w \tilde{x}^* \bar{P}_\mu,$$

and similarly for D_1 and D_∞, it follows that

$$\deg_w \tilde{x}^* \bar{P}_l > 0$$

for some $l \in \{1, \dots, k\}$. Since $\deg_w \tilde{x}^* \bar{P}_\mu$ is a multiple of $\log \mathcal{N}(\mathfrak{p}_w)$ for every μ, the contribution $r_{K,w}$ of w to the radical of y is bounded by

$$r_{K,w} \le \frac{1}{[K:\mathbb{Q}]} \sum_{\mu=1}^{k} \deg_w \tilde{x}^* \bar{P}_\mu.$$

Write

$$h_{K,w} = \begin{cases} \frac{1}{[K:\mathbb{Q}]} \log \mathcal{N}(\mathfrak{p}_w), & \text{if } w \in M_K^0, \\ 0, & \text{if } w \in M_K^\infty. \end{cases}$$

For $w \in S$, we obtain the stronger bound

$$r_{K,w} \le \frac{1}{[K:\mathbb{Q}]} \sum_{\mu=1}^{k} \deg_w \tilde{x}^* \bar{P}_\mu - \frac{1}{[K:\mathbb{Q}]} \deg_w \tilde{x}^* \bar{D} + h_{K,w}$$

since

$$\deg_w \tilde{x}^* \bar{D} = \sum_{\mu} \deg_w \tilde{x}^* \bar{P}_\mu,$$

where the summation is restricted to those P_μ that are components of D. Note that this also holds for the Archimedean places. Adding these contributions, we find

$$\overline{N}(y, E) \le \sum_{\mu=1}^{k} h_{P_\mu}(x) - m_S(x, D) + \sum_{w \in S} h_{K,w}.$$

By the abc-conjecture with type ψ and (5.54), we obtain

$$h_{D_1}(x) \le \sum_{\mu=1}^{k} h_{P_\mu}(x) - m_S(x, D) + \sum_{w \in S} h_{K,w} + d_{K/\mathbb{Q}} + \psi(h(y)).$$

By (5.4), we have

$$h_K(x) = h_{D_1}(x) - \sum_{\mu=1}^{k} h_{P_\mu}(x).$$

Thus we obtain Vojta's height inequality, with $\varepsilon h_{D_0}(x) + C$ replaced by $\psi(h(f(x))) + \sum_{w \in S} h_{K,w}$. For more details, see [286].

Chapter 9

L-functions

Gauss conjectured that the counting function $\pi(x)$ of prime numbers $p \leq x$ satisfies the asymptotic formula $\pi(x) \sim x/\log x$. Riemann outlined how Gauss's conjecture could be proved by using the Riemann's ζ-function $\zeta(s)$. Riemann's ideas led to the first proof of Gauss's conjecture, the celebrated prime number theorem. Similar cases occur for Dirichlet L-functions, which were used to prove the Dirichlet's prime number theorem. Thus it is nature to hope that distribution problems of algebraic numbers are closely related to valued-properties of some L-functions. In this chapter, we will give an elementary introduction along this direction.

9.1 Dirichlet series

9.1.1 Abscissa of convergence

By a *Dirichlet series* we mean a series of the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{9.1}$$

where the coefficients a_n are any given numbers, and s is a complex variable. The series may converge for all values of s (e.g. $a_n = 1/n!$), or for no values of s (e.g. $a_n = n!$). If the Dirichlet series is convergent, we will denote its sum by $L(s)$.

Theorem 9.1. *If the Dirichlet series* (9.1) *is convergent for $s = s_0$, then it is uniformly convergent throughout the angular region in the complex plane $\mathbb{C}$ defined by the inequality*

$$|\arg(s - s_0)| \leq \frac{\pi}{2} - \varepsilon$$

where ε is any positive number less than $\frac{\pi}{2}$.

Proof. See E. C. Titchmarsh [276], Theorem 9.11. □

In particular, if the Dirichlet series (9.1) is convergent for $s = s_0$, then it is convergent for $s \in \mathbb{C}$, provided that $\mathrm{Re}(s) > \mathrm{Re}(s_0)$. Thus there exists a real number σ_0 such that the series is convergent for $\mathrm{Re}(s) > \sigma_0$, divergent for $\mathrm{Re}(s) < \sigma_0$. The

number σ_0 is called the *abscissa of convergence* of the series, which is given by the formula (cf. [276], 9.14)

$$\sigma_0 = \limsup_{n\to\infty} \frac{\log |A_n|}{\log n},$$

where

$$A_n = \begin{cases} a_{n+1} + a_{n+2} + \cdots, & \text{if } \sum a_n \text{ is convergent,} \\ a_1 + a_2 + \cdots + a_n, & \text{if } \sum a_n \text{ is divergent.} \end{cases}$$

Theorem 9.2. *If σ_0 is the abscissa of convergence of the Dirichlet series* (9.1)*, the sum $L(s)$ is a holomorphic function of s for $\mathrm{Re}(s) > \sigma_0$. In particular, if $a_n \geq 0$ for all n, then $s = \sigma_0$ is a singularity of $L(s)$.*

Proof. The first part follows from Theorem 9.1. For the second part, see E. C. Titchmarsh [276], 9.2. □

In the above notation, we have the following result:

Lemma 9.3. *Assume that there exists a constant c such that*

$$\lim_{n\to\infty} \frac{a_1 + \cdots + a_n}{n} = c.$$

Then, if s approaches 1 (*from $s > 1$*),

$$\lim_{s\to 1} (s-1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} = c.$$

Proof. For a proof, see Hecke [95], Lemma (c) in Section 42. □

The following *Phragmen–Lindelöf principle* (cf. [24], [276], [151], [186]) can be used to obtain estimates on L-functions in vertical strips from ones on their edges:

Theorem 9.4. *Let $f(s)$ be meromorphic in a strip*

$$\Omega = \{s \in \mathbb{C} \mid a \leq \mathrm{Re}(s) \leq b\}, \ \ \{a, b\} \subset \mathbb{R}.$$

Suppose that there exists some $\rho > 0$ such that $f(s)$ satisfies the inequality

$$f(s) = O\big(e^{|s|^\rho}\big)$$

on Ω for $|\mathrm{Im}(s)|$ large and obeys the estimate

$$f(\sigma + it) = O\left(|t|^M\right), \quad \sigma \in \{a, b\}, \ \ |t| \to \infty$$

for some positive integer M. Then

$$f(\sigma + it) = O\left(|t|^M\right), \quad a \leq \sigma \leq b, \ \ |t| \to \infty.$$

An entire function $f(s)$ is said to be of finite order if there is a positive number ρ such that, as $|s| \to \infty$,

$$f(s) = O\big(e^{|s|^\rho}\big).$$

The lower bound λ of numbers ρ for which this is true is called the *order* of $f(s)$. If $f(0)$ is not zero, and if $z_1, z_2, \ldots$ are the zero of $f(s)$, then the series $\sum_n |z_n|^{-\alpha}$ is convergent if $\alpha > \lambda$. The lower bound of positive numbers α for which $\sum_n |z_n|^{-\alpha}$ is convergent is called the *exponent of convergence of the zeros*, and is denoted by λ_1. It is obvious that $\lambda_1 \leq \lambda$, which is a part result of the following *Hadamard's factorization theorem* (cf. [123], [276]):

Theorem 9.5. *If $f(s)$ is an entire function of order λ, with zeros $z_1, z_2, \ldots$ ($f(0) \neq 0$), then the exponent λ_1 of convergence of the zeros z_n is finite such that $\lambda_1 \leq \lambda$,*

$$f(s) = e^{P(s)} \prod_n \left(1 - \frac{s}{z_n}\right) e^{\frac{s}{z_n} + \frac{1}{2}\left(\frac{s}{z_n}\right)^2 + \cdots + \frac{1}{p}\left(\frac{s}{z_n}\right)^p},$$

where $p \geq 0$ is the smallest integer satisfying

$$\sum_n \frac{1}{|z_n|^{p+1}} < +\infty,$$

$P(s)$ is a polynomial with $\deg(P) \leq \lambda$, and we have $\lambda = \max\{\deg(P), \lambda_1\}$. Moreover if, for arbitrary $c > 0$, there exists a sequence $r_m \to \infty$ such that

$$\max_{|s|=r_m} |f(s)| > e^{cr_m^\rho}, \;\; m = 1, 2, \ldots,$$

then $\rho = \lambda_1$, and the series $\sum_n |s_n|^{-\lambda_1}$ diverges.

9.1.2 Riemann's ζ-function

The Riemann's ζ-function is a special example defined by the Dirichlet series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \;\; s \in \mathbb{C}. \tag{9.2}$$

The series is convergent, and the function analytic, for $\mathrm{Re}(s) > 1$. In 1737, Euler [59] discovered the product representation

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \;\; \mathrm{Re}(s) > 1, \tag{9.3}$$

where p runs though all prime numbers. The Euler's product gives a first glance on the intimate connection between the zeta-function and the distribution of prime numbers. A first immediate consequence is Euler's proof of the infinitude of the primes.

By using the substitutions $x \mapsto \pi n^2 x$, $s \mapsto s/2$ in the well-known Γ-*function*

$$\Gamma(s) = \int_0^\infty e^{-x} x^s \frac{dx}{x},$$

it gives

$$\frac{\Gamma_{\mathbb{R}}(s)}{n^s} = \int_0^\infty e^{-\pi n^2 x} x^{\frac{s}{2}} \frac{dx}{x},$$

where

$$\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right).$$

Then Riemann proved that the *completed zeta function*

$$\Lambda(s) = \Gamma_{\mathbb{R}}(s)\zeta(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

has the integral representation

$$\Lambda(s) = \int_0^\infty \left\{ \theta(ix) - \frac{1}{2} \right\} x^{\frac{s}{2}} \frac{dx}{x}, \tag{9.4}$$

where $\theta(ix)$ is given by the classical *Jacobi's theta series*

$$\theta(z) = \frac{1}{2} \sum_{n \in \mathbb{Z}} e^{\pi i n^2 z} = \frac{1}{2} + \sum_{n=1}^{\infty} e^{\pi i n^2 z}.$$

The series converges absolutely and uniformly in $\{z \in \mathbb{C} \mid \mathrm{Im}(z) \geq \varepsilon\}$ for every $\varepsilon > 0$. It therefore represents an analytic function on the upper half-plane

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\},$$

and satisfies the transformation formula

$$\theta\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{\frac{1}{2}} \theta(z).$$

The proof of the functional equation for $\Lambda(s)$ is based on the following general *Mellin principle* (cf. [202], Chapter VII, Theorem 1.4). If $f : \mathbb{R}^+ \longrightarrow \mathbb{C}$ is a continuous function, one defines the *Mellin transform* by

$$\Lambda_f(s) = \int_0^\infty \{f(x) - f(\infty)\} x^s \frac{dx}{x},$$

provided the limit

$$f(\infty) = \lim_{x \to \infty} f(x)$$

and the integral exist. Conversely, f can be obtained by the *Mellin inverse transform*

$$f(x) - f(\infty) = \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma} \Lambda_f(s) x^{-s} ds$$

by the general theory of the Fourier transform.

Theorem 9.6. *Let $f, g : \mathbb{R}^+ \longrightarrow \mathbb{C}$ be continuous functions such that for $x \to \infty$*

$$f(x) = a_0 + O\left(e^{-cx^\alpha}\right), \quad g(x) = b_0 + O\left(e^{-cx^\alpha}\right) \tag{9.5}$$

with positive constants c, α. If they satisfy the equation

$$f\left(\frac{1}{x}\right) = Cx^k g(x) \tag{9.6}$$

for some real number $k > 0$ and some complex number $C \neq 0$, then one has

(a) *The integrals $\Lambda_f(s)$ and $\Lambda_g(s)$ converge absolutely and uniformly if s varies in an arbitrary compact region contained in $D = \{s \in \mathbb{C} \mid \mathrm{Re}(s) > k\}$. They are therefore holomorphic functions on D, and admit holomorphic continuations to $\mathbb{C} - \{0, k\}$.*

(b) *They have no pole at $s = 0$ and $s = k$ if $a_0 = 0$, resp. $b_0 = 0$, otherwise have simple poles at these points with residues*

$$\operatorname*{Res}_{s=0} \Lambda_f(s) = -a_0, \qquad \operatorname*{Res}_{s=k} \Lambda_f(s) = Cb_0,$$
$$\operatorname*{Res}_{s=0} \Lambda_g(s) = -b_0, \qquad \operatorname*{Res}_{s=k} \Lambda_g(s) = \frac{a_0}{C}.$$

(c) *They satisfy the functional equation*

$$\Lambda_f(s) = C\Lambda_g(k - s).$$

Proof. If s varies over a compact subset of $\mathbb{C}$, then the function $e^{-cx^\alpha} x^{\sigma+1}$ ($\sigma = \mathrm{Re}(s)$) is bounded for $x \geq 1$ by a constant which is independent of σ. Hence the condition (9.5) gives the estimates

$$\left|(h(x) - h(\infty))x^{s-1}\right| = O\left(e^{-cx^\alpha} x^{\sigma-1}\right) = O\left(\frac{1}{x^2}\right), \ h \in \{f, g\},$$

for all $x \geq 1$, which means that the integrals

$$\int_1^\infty (h(x) - h(\infty))x^{s-1} dx \ \ (h \in \{f, g\})$$

converge absolutely and uniformly for s in the compact subset.

When $\mathrm{Re}(s) > k$, the substitution $x \mapsto 1/x$ and the equation (9.6) give

$$\int_0^1 (f(x) - a_0)x^{s-1} dx = C \int_1^\infty (g(x) - b_0)x^{k-s-1} dx - \frac{a_0}{s} - \frac{Cb_0}{k - s}.$$

By the above arguments, it converges absolutely and uniformly for $\mathrm{Re}(s) > k$. We therefore obtain

$$\Lambda_f(s) = F(s) - \frac{a_0}{s} - \frac{Cb_0}{k - s}, \ \mathrm{Re}(s) > k,$$

where

$$F(s) = \int_1^\infty \left\{ (f(x) - a_0)x^s + C(g(x) - b_0)x^{k-s} \right\} \frac{dx}{x}.$$

Swapping f and g and noting that

$$g\left(\frac{1}{x}\right) = C^{-1}x^k f(x),$$

we similarly have

$$\Lambda_g(s) = G(s) - \frac{b_0}{s} - \frac{C^{-1}a_0}{k-s}, \ \mathrm{Re}(s) > k,$$

where

$$G(s) = \int_1^\infty \left\{ (g(x) - b_0)x^s + C^{-1}(f(x) - a_0)x^{k-s} \right\} \frac{dx}{x}.$$

The integrals $F(s)$ and $G(s)$ converge absolutely and locally uniformly on $\mathbb{C}$. Thus they represent holomorphic functions satisfying obviously the equation

$$F(s) = CG(k-s).$$

Therefore $\Lambda_f(s)$ and $\Lambda_g(s)$ have been continued to all of $\mathbb{C} - \{0, k\}$ and we have the functional equation in (c). This finishes the proof of the theorem. □

Applied the Mellin principle to the following case

$$f(x) = g(x) = \theta(ix), \quad \Lambda_f(s) = \Lambda(2s),$$

then $\Lambda(2s)$ has a holomorphic continuation to $\mathbb{C} - \{0, 1/2\}$ and simple poles at $s = 0, 1/2$ with residues $-1/2$ and $1/2$, respectively, and it satisfies the functional equation

$$\Lambda(2s) = \Lambda(1-2s).$$

Accordingly, the Riemann's ζ-function admits a meromorphic continuation onto the entire complex plane. The continuation is holomorphic with the exclusion of a simple pole at $s = 1$ with residue 1, and satisfies the following functional equation:

$$\Lambda(s) = \Lambda(1-s), \tag{9.7}$$

or equivalently

$$\zeta(1-s) = 2(2\pi)^{-s}\cos\left(\frac{\pi s}{2}\right)\Gamma(s)\zeta(s). \tag{9.8}$$

It is usual to use the entire function

$$\xi(s) = \frac{s}{2}(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

which satisfies the functional equation

$$\xi(s) = \xi(1-s). \tag{9.9}$$

The *Bernoulli polynomials* $B_n(t)$ are defined by

$$\frac{ze^{tz}}{e^z - 1} = \sum_{n=0}^{\infty} B_n(t)\frac{z^n}{n!}. \tag{9.10}$$

We can find easily the formula

$$B_n(t) = \sum_{k=0}^{n} \binom{n}{k} B_k(0)t^{n-k}, \ \ n = 0, 1, 2, \ldots, \tag{9.11}$$

in which

$$B_0(0) = 1, \quad B_1(0) = -\frac{1}{2}, \quad B_{2n+1}(0) = 0 \ \ (n = 1, 2, \ldots).$$

The *Bernoulli numbers* B_n are defined by

$$B_n = (-1)^{n-1}B_{2n}(0), \ \ n = 1, 2, \ldots. \tag{9.12}$$

The first Bernoulli numbers are

$$B_1 = \frac{1}{6}, \quad B_2 = \frac{1}{30}, \quad B_3 = \frac{1}{42}, \quad B_4 = \frac{1}{30},$$

$$B_5 = \frac{5}{66}, \quad B_6 = \frac{691}{2730}, \quad B_7 = \frac{7}{6}, \quad B_8 = \frac{3617}{510}.$$

Theorem 9.7. *For every integer $n > 0$ one has*

$$\zeta(1-n) = \frac{(-1)^{n-1}}{n}B_n(0).$$

Proof. Since the equation (9.10) can be rewritten into the form

$$\frac{ze^{(1+t)z}}{e^z - 1} = \sum_{n=0}^{\infty}(-1)^n B_n(-t)\frac{z^n}{n!},$$

one obtains

$$\frac{ze^z}{e^z - 1} = \sum_{n=0}^{\infty}(-1)^n B_n(0)\frac{z^n}{n!}.$$

Then the theorem follows from [202], Chapter VII, Theorem 1.8. □

Further, applying the functional equation, it follows that

$$\zeta(2n) = \frac{(2\pi)^{2n}}{2(2n)!} B_n, \ \ n \geq 1. \tag{9.13}$$

From the convergence of the product (9.3) one deduces that $\zeta(s)$ has no zeros for $\mathrm{Re}(s) > 1$. The Γ-function $\Gamma(s)$ is nowhere 0 and has simple poles at $s = 0, -1, -2, \ldots$. The functional equation therefore shows that the only zeros of $\zeta(s)$ in the domain $\mathrm{Re}(s) < 0$ are the poles of $\Gamma(s/2)$. These are called the *trivial zeros* of $\zeta(s)$. Other zeros lie in the *critical strip* $0 \leq \mathrm{Re}(s) \leq 1$. G. H. Hardy proved that there are an infinity of zeros on $\mathrm{Re}(s) = \frac{1}{2}$.

Conjecture 9.8 (Riemann Hypothesis). *The non-trivial zeros of $\zeta(s)$ lie on the line $\mathrm{Re}(s) = \frac{1}{2}$.*

Let ρ_n be the nontrivial zeros in the critical strip $0 \leq \mathrm{Re}(s) \leq 1$ and let s_ν be the zeros of $\zeta(s)$ on the half-line $\mathrm{Re}(s) = \frac{1}{2}$, $\mathrm{Im}(s) > 0$. Assume that ρ_n, s_ν are ordered with respect to increasing absolute values of their imaginary parts. Hadamard's factorization theorem yields (cf. [111])

$$\xi(s) = \frac{1}{2} e^{-\left(1 + \frac{\gamma}{2} - \frac{1}{2}\log(4\pi)\right)s} \prod_{n=1}^{\infty} \left(1 - \frac{s}{\rho_n}\right) e^{\frac{s}{\rho_n}}, \tag{9.14}$$

where γ is *Euler's constant*

$$\gamma = \lim_{n \to \infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right). \tag{9.15}$$

It follow

$$\zeta(\rho_n) = \zeta(1 - \rho_n) = \zeta(\bar{\rho}_n) = \zeta(1 - \bar{\rho}_n) = 0$$

from the functional equation (9.9), in addition with the identity

$$\zeta(\bar{s}) = \overline{\zeta(s)},$$

that is, $\bar{\rho}_n$, $1 - \rho_n$, $1 - \bar{\rho}_n$ are zeros of $\zeta(s)$ too. In other words, non-trivial zeros of $\zeta(s)$ are distributed symmetrically with respect to the real axis and to the vertical line $\mathrm{Re}(s) = \frac{1}{2}$.

Theorem 9.9 ([111]). *The Riemann hypothesis holds if and only if the zeros s_ν of $\zeta(s)$ on the half-line $\mathrm{Re}(s) = \frac{1}{2}$, $\mathrm{Im}(s) > 0$ satisfy*

$$\sum_{\nu=1}^{\infty} \frac{1}{|s_\nu|^2} = 1 + \frac{\gamma}{2} - \frac{1}{2}\log(4\pi). \tag{9.16}$$

Proof. Write

$$b = 1 + \frac{\gamma}{2} - \frac{1}{2}\log(4\pi) = 0.023\cdots .$$

Differentiating logarithmically the Hadamard's factorization (9.14) and the functional equation (9.9) respectively, we obtain

$$b = -\frac{\xi'(0)}{\xi(0)} = \frac{\xi'(1)}{\xi(1)} = -b + \sum_{n=1}^{\infty}\left(\frac{1}{1-\rho_n} + \frac{1}{\rho_n}\right). \tag{9.17}$$

Since $1-\rho_n$, $\bar{\rho}_n$ are zeros of $\zeta(s)$, we have

$$\sum_{n=1}^{\infty}\left(\frac{1}{\bar{\rho}_n} + \frac{1}{\rho_n}\right) = \sum_{n=1}^{\infty}\left(\frac{1}{1-\rho_n} + \frac{1}{\rho_n}\right) = 2b, \tag{9.18}$$

which implies

$$\sum_{\nu=1}^{\infty}\frac{1}{|s_\nu|^2} + \sum_{\mathrm{Re}(\rho_n)\neq 1/2}\frac{\mathrm{Re}(\rho_n)}{|\rho_n|^2} = b,$$

and so Theorem 9.9 follows easily. □

In 1791, Gauss [73] conjectured that the counting function $\pi(x)$ of prime numbers $p \le x$ satisfies the asymptotic formula

$$\pi(x) \sim \frac{x}{\log x}. \tag{9.19}$$

Riemann [219] outlined how Gauss's conjecture (9.19) could be proved by using the function $\zeta(s)$. Riemann's ideas led to the first proof of Gauss's conjecture, the celebrated *prime number theorem*, by J. Hadamard [86] and C. J. de la Vallée-Poussin [280] (independently) in 1896. A very brief sketch is to work with the logarithmic derivative of $\zeta(s)$ which is given by

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}, \ \ \mathrm{Re}(s) > 1, \tag{9.20}$$

where the *von Mangoldt Λ-function* is defined by

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k,\ p \text{ prime},\ k \in \mathbb{Z}^+, \\ 0, & \text{otherwise.} \end{cases} \tag{9.21}$$

A lot of information concerning the prime counting function $\pi(x)$ can be recovered from information about the *Chebyshev's function*:

$$\psi(x) = \sum_{n\le x}\Lambda(n) = \sum_{p\le x}\log p + O\left(\sqrt{x}\log x\right). \tag{9.22}$$

Partial summation gives

$$\pi(x) \sim \frac{\psi(x)}{\log x}. \tag{9.23}$$

We can express $\psi(x)$ in terms of the zeta-function by using the Perron formula, which leads to the exact explicit formula

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right) - \log(2\pi), \tag{9.24}$$

where ρ are the non-trivial zeros of $\zeta(s)$, and so the prime number theorem follows.

9.1.3 Dirichlet's characters

For a positive integer r, we will use the *Euler's φ-function*

$$\varphi(r) = \#\{j \in \mathbb{Z} \mid 0 \le j < r,\ (j, r) = 1\}.$$

The *Euler's theorem* shows

$$a^{\varphi(r)} \equiv 1 \bmod r$$

for all integer $a \in \mathbb{Z}$ with $(a, r) = 1$.

First of all, we consider the case $r = 2^{\alpha}$ for a positive integer α. If n is any odd number, there exist integers γ and γ_0 satisfying

$$n \equiv (-1)^{\gamma} 5^{\gamma_0} \bmod 2^{\alpha},$$

in which γ, γ_0 are called the indexes of n modulo 2^{α}. If one set

$$c = \begin{cases} 1, & \text{if } \alpha = 1, \\ 2, & \text{if } \alpha \ge 2 \end{cases}$$

and

$$c_0 = \begin{cases} 1, & \text{if } \alpha = 1, \\ 2^{\alpha-2}, & \text{if } \alpha \ge 2, \end{cases}$$

one can choose γ, γ_0 such that $0 \le \gamma < c$, $0 \le \gamma_0 < c_0$. Let ζ (resp. ζ_0) be any c-th (resp. c_0-th) root of unit. A *Dirichlet character modulo* 2^{α} is defined by

$$\chi(n) = \chi(n; 2^{\alpha}) = \begin{cases} \zeta^{\gamma}\zeta_0^{\gamma_0}, & \text{if } (n, 2^{\alpha}) = 1, \\ 0, & \text{if } (n, 2^{\alpha}) > 1. \end{cases}$$

If $\zeta = \zeta_0 = 1$, the Dirichlet character modulo 2^{α} is called *trivial* or *principal*, denoted by $\chi^0(n; 2^{\alpha})$.

Take a prime $p > 2$ and consider the case $r = p^\alpha$ for a positive integer α. Then there exists a minimal positive integer g such that $(g, p) = 1$, and

$$g^{\varphi(r)} \equiv 1 \bmod r, \quad g^s \not\equiv 1 \bmod r$$

if $1 \le s < \varphi(r)$. Further, if $n \in \mathbb{Z}$ with $(n, r) = 1$, there exists an integer γ_1 with $0 \le \gamma_1 < \varphi(r)$ such that

$$n \equiv g^{\gamma_1} \bmod r.$$

Let ζ_1 be any $\varphi(r)$-th root of unit. A *Dirichlet character modulo* p^α is defined by

$$\chi(n) = \chi(n; p^\alpha) = \begin{cases} \zeta_1^{\gamma_1}, & \text{if } (n, p^\alpha) = 1, \\ 0, & \text{if } (n, p^\alpha) > 1. \end{cases}$$

If $\zeta_1 = 1$, the Dirichlet character modulo p^α is called *trivial* or *principal*, denoted by $\chi^0(n; p^\alpha)$.

Let r be a positive integer. We can write

$$r = p_1^{\alpha_1} \cdots p_g^{\alpha_g},$$

where $p_1, \ldots, p_g$ are distinct primes, and α_i are positive integers. The *Dirichlet characters modulo* r are defined by

$$\chi(n) = \chi(n; r) = \prod_{i=1}^{g} \chi(n; p_i^{\alpha_i}).$$

In particular, the Dirichlet characters modulo r

$$\chi^0(n) = \chi^0(n; r) = \prod_{i=1}^{g} \chi^0(n; p_i^{\alpha_i})$$

is called *trivial* or *principal*. The Dirichlet characters modulo r form a group with the identity χ^0. When read mod 1, we denote it by $\chi^0 = 1$. It is also called the *principal character* mod 1.

A Dirichlet character χ modulo r is called *nonprimitive* if there exist a proper factor r^* $(\neq r)$ of r and a Dirichlet character χ^* modulo r^* such that

$$\chi(n) = \chi^*(n), \quad (n, r) = 1. \tag{9.25}$$

If there exists no such χ^*, then χ is called a *primitive character*. Each nonprimitive character χ modulo r is induced by a primitive character χ^*, that is, there exists a primitive character χ^* modulo r^* satisfying (9.25) such that r^* is the smallest possible with $r^* | r$, $r^* \neq r$, which is called the *conductor* of χ.

For $n \in \mathbb{Z}$, the *Gauss sum* $\tau(\chi, n)$ associated to the Dirichlet character χ modulo r is defined to be the complex number

$$\tau(\chi, n) = \sum_{m=0}^{r-1} \chi(m) e^{2\pi i m n/r}. \tag{9.26}$$

For $n = 1$, we write

$$\tau(\chi) = \tau(\chi, 1) = \sum_{m=0}^{r-1} \chi(m) e^{2\pi i m/r}. \tag{9.27}$$

Here we list some basic properties of Dirichlet characters χ modulo r:

(1) There are just $\varphi(r)$ distinct Dirichlet characters modulo r.

(2) $\chi(m) = \chi(n)$ if $m \equiv n \bmod r$, $\chi(n) = 0$ if $(n, r) > 1$, and $\chi(n) \neq 0$ if $(n, r) = 1$.

(3) χ is *completely multiplicative*, i. e., $\chi(nm) = \chi(n)\chi(m)$ for any $n, m \in \mathbb{Z}$, particularly, $\chi(1) = 1$.

(4)

$$\frac{1}{\varphi(r)} \sum_{n=0}^{r-1} \chi(n) = \begin{cases} 1, & \text{if } \chi = \chi^0, \\ 0, & \text{if } \chi \neq \chi^0. \end{cases}$$

(5) Given an integer n.

$$\frac{1}{\varphi(r)} \sum_{\chi} \chi(n) = \begin{cases} 1, & \text{if } n \equiv 1 \bmod r, \\ 0, & \text{if } n \not\equiv 1 \bmod r, \end{cases}$$

where χ runs on $\varphi(r)$ distinct Dirichlet characters modulo r.

(6) If χ is a primitive Dirichlet character modulo r, then

$$\tau(\chi, n) = \tau(\chi)\overline{\chi}(n)$$

with $|\tau(\chi)| = \sqrt{r}$.

The property (3) means $\chi(-1)^2 = 1$, that is, $\chi(-1) = \pm 1$. If $\chi(-1) = 1$ (resp. $\chi(-1) = -1$), the character χ is called *even* (resp. *odd*). A main result in elementary number theory shows that the properties (2) and (3) are characteristic of Dirichlet characters modulo r.

Theorem 9.10. *A function $\psi : \mathbb{Z} \longrightarrow \mathbb{C}$ is a Dirichlet character modulo r if and only if ψ satisfy the following conditions:*

(i) $\psi(n) = 0$ *if* $(n, r) > 1$*;*

(ii) ψ *is not identically zero;*

(iii) $\psi(mn) = \psi(m)\psi(n)$*;*

(iv) $\psi(m) = \psi(n)$ *if* $m \equiv n \bmod r$.

9.1.4 Dirichlet's L-functions

Related to a Dirichlet character χ modulo r, one has the *Dirichlet's L-function*:

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \mathrm{Re}(s) > 1.$$

The series $L(\chi, s)$ converges absolutely and uniformly in the region $\mathrm{Re}(s) \geq 1 + \varepsilon$, for any $\varepsilon > 0$. It therefore represents an holomorphic function on the half-plane $\mathrm{Re}(s) > 1$. In particular, for the principal character $\chi = 1$, we get back the Riemann zeta function $\zeta(s)$.

The analog of Euler's formula

$$L(\chi, s) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \quad \mathrm{Re}(s) > 1,$$

is valid. If χ mod r is induced by a primitive character χ^* mod r^*, then

$$L(\chi, s) = L(\chi^*, s) \prod_{p|r} \left(1 - \frac{\chi^*(p)}{p^s}\right). \tag{9.28}$$

In particular, one has

$$L(\chi^0, s) = \zeta(s) \prod_{p|r} \left(1 - \frac{1}{p^s}\right).$$

When $\sigma = \mathrm{Re}(s) > 1$, one has

$$\begin{aligned} \frac{1}{|L(\chi, s)|} &= \left| \prod_p \left(1 - \frac{\chi(p)}{p^s}\right) \right| \leq \prod_p \left(1 + \frac{1}{p^\sigma}\right) \\ &\leq \sum_{n=1}^{\infty} \frac{1}{n^\sigma} < 1 + \int_1^{\infty} \frac{dx}{x^\sigma} = 1 + \frac{1}{\sigma - 1}, \end{aligned}$$

that is,

$$|L(\chi, s)| > \frac{\sigma - 1}{\sigma}.$$

Hence $L(\chi, s) \neq 0$ if $\mathrm{Re}(s) > 1$.

If $\chi \neq \chi^0$, $\mathrm{Re}(s) > 1$, by using Abel's transformation, one obtain

$$\sum_{n=1}^{N} \frac{\chi(n)}{n^s} = 1 + \frac{S(N) - 1}{N^s} + s \int_1^N \{S(x) - 1\} x^{-s-1} dx,$$

where

$$S(x) = \sum_{n \leq x} \chi(n).$$

Let $N \to +\infty$, and so one get

$$L(\chi, s) = s \int_1^{\infty} S(x) x^{-s-1} dx. \tag{9.29}$$

Note that

$$|S(x)| \leq \varphi(r).$$

Therefore the integral in (9.29) converges at the half-plane $\mathrm{Re}(s) > 0$, and hence defines a holomorphic function. In particular, one obtains the estimate

$$|L(\chi, s)| \leq 2|s|\varphi(r), \quad \mathrm{Re}(s) \geq \frac{1}{2}. \tag{9.30}$$

Like the Riemann zeta-function, Dirichlet L-series also admit an analytic continuation to the whole complex plane (with a pole at $s = 1$ in the case $\chi = \chi^0$), and they satisfy a functional equation which relates the arguments s to the argument $1 - s$. We have to distinguish between even and odd Dirichlet characters χ mod r. We define the *exponent* $\delta = \delta_\chi \in \{0, 1\}$ of χ by

$$\delta = \frac{1}{2} \{1 - \chi(-1)\},$$

which means

$$\delta = \begin{cases} 0, & \text{if } \chi(-1) = 1, \\ 1, & \text{if } \chi(-1) = -1. \end{cases}$$

Then the function

$$\Lambda_\chi(s) = \left(\frac{r}{\pi}\right)^{\frac{s+\delta}{2}} \Gamma\left(\frac{s+\delta}{2}\right) L(\chi, s) \tag{9.31}$$

admits the integral representation (cf. [202])

$$\Lambda_\chi(s) = \int_0^{\infty} \left\{\theta(\chi, iy) - \frac{1}{2}\chi(0)\right\} y^{\frac{s+\delta}{2}} \frac{dy}{y} \tag{9.32}$$

with $\chi(0) = 1$, if χ is the trivial character 1, and $\chi(0) = 0$ otherwise, where

$$\theta(\chi, z) = \frac{1}{2}\chi(0) + \sum_{n=1}^{\infty} \chi(n) n^\delta e^{\frac{\pi i n^2 z}{r}}. \tag{9.33}$$

The theta aeries satisfies the transformation formula

$$\theta\left(\chi, -\frac{1}{z}\right) = \frac{\tau(\chi)}{i^\delta \sqrt{r}} \left(\frac{z}{i}\right)^{\delta + \frac{1}{2}} \theta(\bar{\chi}, z), \tag{9.34}$$

where $\bar{\chi}$ is the complex conjugate character to χ, i.e., its inverse, and $\tau(\chi)$ is the *Gauss sum*

$$\tau(\chi) = \sum_{n=0}^{r-1} \chi(n) e^{\frac{2\pi i n}{r}}$$

with $|\tau(\chi)| = \sqrt{r}$ (see [202], Chapter VII, Proposition 2.7).

To study the analytic continuation and functional equation for $L(\chi, s)$, we may restrict ourselves to the case of a primitive character modulo r. For χ is always induced by a primitive character χ^* modulo r^*, where r^* is the conductor of χ, and we clearly have the relation (9.28), so that the analytic continuation and functional equation of $L(\chi, s)$ follows from the one for $L(\chi^*, s)$. We may further exclude the case $r = 1$, this being the case of the Riemann zeta function which was settled in Section 9.1.2.

Assume that χ is a nontrivial primitive character modulo r with $r > 1$. Then $\Lambda_\chi(s)$ admits an analytic continuation to the whole complex plane $\mathbb{C}$ and satisfies the functional equation

$$\Lambda_\chi(s) = \frac{\tau(\chi)}{i^\delta \sqrt{r}} \Lambda_{\bar{\chi}}(1-s). \tag{9.35}$$

The proof of (9.35) is the same as for the original proof of the functional equation due to Riemann and is based on Mellin principle or Poisson summation formula (cf. [41], [202]).

The equation (9.35) translates into

$$L(\bar{\chi}, 1-s) = \frac{i^\delta \sqrt{r}}{\tau(\chi)} \left(\frac{\pi}{r}\right)^{\frac{1}{2}-s} \frac{\Gamma\left(\frac{s+\delta}{2}\right)}{\Gamma\left(\frac{1-s+\delta}{2}\right)} L(\chi, s). \tag{9.36}$$

Legendre's duplication formula yields

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) = \frac{2\sqrt{\pi}}{2^s}\Gamma(s).$$

Substituting $\frac{1-s}{2}$ into the formula

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s},$$

one has

$$\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) = \frac{\pi}{\cos(\pi s/2)}.$$

After taking the quotient, one get

$$\frac{\Gamma\left(\frac{s}{2}\right)}{\Gamma\left(\frac{1-s}{2}\right)} = \frac{2}{2^s\sqrt{\pi}}\Gamma(s)\cos\frac{\pi s}{2}.$$

Therefore, for the case $\delta = 0$ ($\chi(-1) = 1$), the equation (9.36) becomes

$$L(\bar{\chi}, 1-s) = \frac{2}{\tau(\chi)}\left(\frac{2\pi}{r}\right)^{-s} \cos\left(\frac{\pi s}{2}\right)\Gamma(s)L(\chi, s). \tag{9.37}$$

However, for the case $\delta = 1$ ($\chi(-1) = -1$), we have

$$\frac{\Gamma\left(\frac{s+1}{2}\right)}{\Gamma\left(\frac{1-s+1}{2}\right)} = \frac{2\sqrt{\pi}\Gamma(s)}{2^s\Gamma\left(\frac{s}{2}\right)\Gamma\left(1-\frac{s}{2}\right)} = \frac{2}{2^s\sqrt{\pi}}\Gamma(s)\sin\left(\frac{\pi s}{2}\right),$$

and hence the equation (9.36) becomes

$$L(\bar{\chi}, 1-s) = \frac{2i}{\tau(\chi)} \left(\frac{2\pi}{r}\right)^{-s} \sin\left(\frac{\pi s}{2}\right) \Gamma(s) L(\chi, s). \tag{9.38}$$

Two formulae (9.37) and (9.38) can be unified into the form:

$$L(\bar{\chi}, 1-s) = \frac{2}{i^{\delta}\tau(\chi)} \left(\frac{2\pi}{r}\right)^{-s} \cos\left(\frac{\pi(s+\delta)}{2}\right) \Gamma(s) L(\chi, s). \tag{9.39}$$

9.1.5 Zeros of Dirichlet's L-functions

The following facts are well known: If χ is a complex character modulo r, $s = \sigma + it$, then $L(\chi, s)$ has no zeros in the region

$$\mathrm{Re}(s) = \sigma \geq 1 - \frac{c}{\log r(|t|+2)}.$$

If χ is a real character modulo r, $s = \sigma + it$, then $L(\chi, s)$ has no zeros in the region

$$\mathrm{Re}(s) = \sigma \geq 1 - \frac{c}{\log r(|t|+2)}, \ \ |t| > 0.$$

Further, if χ is a real primitive character modulo r, Siegel's theorem claims that for any $\varepsilon > 0$, there exists a constant $c = c(\varepsilon) > 0$ such that a real zero β of $L(\chi, s)$ must satisfy

$$\beta \leq 1 - \frac{c}{r^{\varepsilon}}.$$

For a nontrivial primitive Dirichlet character χ modulo r, the *Bernoulli polynomials* $B_{n,\chi}(t)$ associated to χ are defined by

$$\varphi_{\chi}(z,t) = \sum_{k=1}^{r} \chi(k) \frac{ze^{(r-k+t)z}}{e^{rz}-1} = \sum_{n=0}^{\infty} B_{n,\chi}(t) \frac{z^n}{n!}, \tag{9.40}$$

or equivalently

$$\varphi_{\chi}(-z,-t) = \sum_{k=1}^{r} \chi(k) \frac{ze^{(k+t)z}}{e^{rz}-1} = \sum_{n=0}^{\infty} (-1)^n B_{n,\chi}(-t) \frac{z^n}{n!}.$$

It is easy to show that

$$B_{n,\chi}(t) = \sum_{k=0}^{n} \binom{n}{k} B_{k,\chi}(0) t^{n-k}, \tag{9.41}$$

and

$$B_{n,\chi}(t+r) - B_{n,\chi}(t) = n \sum_{k=1}^{r} \chi(k)(t+r-k)^{n-1}, \ \ n \geq 0.$$

Write

$$\varphi_\chi(z) = \varphi_\chi(z,0) = \sum_{k=1}^{r} \chi(k) \frac{ze^{(r-k)z}}{e^{rz}-1}.$$

Since

$$\varphi_\chi(-z) = \sum_{k=1}^{r} \chi(-1)\chi(r-k) \frac{ze^{kz}}{e^{rz}-1} = \chi(-1)\varphi_\chi(z),$$

we find

$$(-1)^n B_{n,\chi}(0) = \chi(-1) B_{n,\chi}(0),$$

so that $B_{n,\chi}(0) = 0$ if $n \not\equiv \delta \bmod 2$.

Theorem 9.11 (cf. [202]). *For any integer $n \geq 1$, one has*

$$L(\chi, 1-n) = \frac{(-1)^{n-1}}{n} B_{n,\chi}(0).$$

The theorem immediately gives

$$L(\chi, 1-n) = 0, \ \ n \not\equiv \delta \bmod 2,$$

provided that χ is not the principal character $\chi = 1$. From the functional equation (9.35) and the fact that $L(\chi, n) \neq 0$, we deduce for $n \geq 1$ that

$$L(\chi, 1-n) = \frac{(-1)^{n-1}}{n} B_{n,\chi}(0) \neq 0, \ \ n \equiv \delta \bmod 2.$$

In particular, it follows that

$$L(\chi, 0) = B_{1,\chi}(0) = \begin{cases} 0, & \text{if } \chi(-1) = 1, \\ \sum\limits_{k=1}^{r} \left(\frac{1}{2} - \frac{k}{r}\right) \chi(k), & \text{if } \chi(-1) = -1. \end{cases}$$

The functional equation (9.35) also gives for $n \geq 1$ that

$$L(\chi, n) = (-1)^{n+1+\frac{n-\delta}{2}} \frac{\tau(\chi)}{2i^\delta} \left(\frac{2\pi}{r}\right)^n \frac{B_{n,\bar{\chi}}(0)}{n!}, \ \ n \equiv \delta \bmod 2.$$

Based on above facts, if χ is a nontrivial primitive character modulo r, then $L(\chi, s)$ has no zeros in the region $\mathrm{Re}(s) \geq 1$. The functional equation (9.35) shows that $\Lambda_\chi(s)$ has no zeros in the union of region $\mathrm{Re}(s) \geq 1$ and $\mathrm{Re}(s) \leq 0$. Hence when $\delta = 0$, that is, $\chi(-1) = 1$, $L(\chi, s)$ has only the trivial simple zeros in the region $\mathrm{Re}(s) \leq 0$

$$s = 0, -2, -4, \ldots, -2m - \delta, \ldots;$$

when $\delta = 1$, that is, $\chi(-1) = -1$, $L(\chi, s)$ has only the trivial simple zeros in the region $\mathrm{Re}(s) \leq 0$

$$s = -1, -3, -5, \ldots, -2m - \delta, \ldots;$$

in which m is a non-negative integer. Thus the zeros of $\Lambda_\chi(s)$ are all non-trivial zeros of $L(\chi, s)$ in the *critical strip* $0 < \mathrm{Re}(s) < 1$.

Theorem 9.12. *If χ is a nontrivial primitive character modulo r, then $\Lambda_\chi(s)$ is an entire function of order 1, and has infinitely many zeros ρ_n satisfying the conditions: $0 < \mathrm{Re}(\rho_n) < 1$, the series $\sum_{n=1}^{\infty} |\rho_n|^{-1}$ diverges, the series $\sum_{n=1}^{\infty} |\rho_n|^{-1-\varepsilon}$ converges for any $\varepsilon > 0$, and Hadamard's factorization*

$$\Lambda_\chi(s) = e^{a-bs} \prod_{n=1}^{\infty} \left(1 - \frac{s}{\rho_n}\right) e^{\frac{s}{\rho_n}} \tag{9.42}$$

holds, where $a = a(\chi),\ b = b(\chi)$ are constants.

Proof. If $\sigma = \mathrm{Re}(s) \geq \frac{1}{2}$, then (9.30) means

$$|L(\chi, s)| \leq 2|s|\varphi(r) < 2r|s|,$$

which further implies

$$|\Lambda_\chi(s)| \leq 2r|s| \left(\frac{r}{\pi}\right)^{\frac{\sigma+\delta}{2}} \left|\Gamma\left(\frac{s+\delta}{2}\right)\right| \ll r^{\frac{\sigma}{2}+\frac{3}{2}} e^{c|s||\log|s||}.$$

From the functional equation (9.35), this estimate also holds when $\sigma = \mathrm{Re}(s) < \frac{1}{2}$. Since

$$\log \Gamma(s) \sim s \log s, \ \ s \to +\infty,$$

it follows that $\Lambda_\chi(s)$ is an entire function of order 1. Further, by using Hadamard's Factorization Theorem 9.5 it is not difficult to show that the exponent of convergence of the zeros of $\Lambda_\chi(s)$ is equal to the order 1 such that the series

$$\sum_{n=1}^{\infty} |\rho_n|^{-1}$$

diverges. □

The *generalized Riemann hypothesis* states that if $L(\chi, s) = 0$, then either s is a non-positive integer (a "trivial zero") or $\mathrm{Re}(s) = \frac{1}{2}$. It had been shown, for a sufficiently small constant $c > 0$, that if $L(\chi, s) = 0$ with

$$\mathrm{Re}(s) > 1 - \frac{c}{\log r},$$

then s is real, χ is a quadratic real character, and there is at most one such value of r between R and R^2 for any sufficiently large R. Such zeros are known as *Siegel zeros*. In 1995, Granville and Stark proved, assuming the abc-conjecture, that $L(\chi, s)$ has no Siegel zeros for all $\chi \pmod r$ with $r \equiv 3 \pmod 4$.

By using the symbols in Theorem 9.12, it follows

$$L(\chi, \rho_n) = L(\bar{\chi}, 1 - \rho_n) = L(\bar{\chi}, \bar{\rho}_n) = L(\chi, 1 - \bar{\rho}_n) = 0$$

from the functional equation (9.35), that is, $1-\bar{\rho}_n$ are zeros of $L(\chi,s)$ too. In other words, non-trivial zeros of $L(\chi,s)$ are symmetric for the line $\mathrm{Re}(s)=\frac{1}{2}$. Let s_ν be the zeros of $L(\chi,s)$ on the critical line $\mathrm{Re}(s)=\frac{1}{2}$ and assume that ρ_n, s_ν are ordered with respect to increasing absolute values of their imaginary parts.

Theorem 9.13. *Under the notations of Theorem 9.12, we have* $\mathrm{Re}(b)>0$*. Moreover, the generalized Riemann hypothesis holds if and only if the zeros* s_ν *of* $L(\chi,s)$ *on the critical line* $\mathrm{Re}(s)=\frac{1}{2}$ *satisfy*

$$\sum_{\nu}\frac{1}{|s_\nu|^2}=2\mathrm{Re}(b). \tag{9.43}$$

Proof. Differentiating logarithmically the Hadamard's factorization (9.42) and the functional equation (9.35) respectively, we obtain

$$b=-\frac{\Lambda'_\chi(0)}{\Lambda_\chi(0)}=\frac{\Lambda'_{\bar{\chi}}(1)}{\Lambda_{\bar{\chi}}(1)}=-\bar{b}+\sum_{n=1}^{\infty}\left(\frac{1}{1-\bar{\rho}_n}+\frac{1}{\bar{\rho}_n}\right). \tag{9.44}$$

Since $1-\bar{\rho}_n$ are zeros of $L(\chi,s)$, we have

$$\sum_{n=1}^{\infty}\left(\frac{1}{\rho_n}+\frac{1}{\bar{\rho}_n}\right)=\sum_{n=1}^{\infty}\left(\frac{1}{1-\bar{\rho}_n}+\frac{1}{\bar{\rho}_n}\right)=2\mathrm{Re}(b). \tag{9.45}$$

Theorem 9.12 shows

$$\sum_{n=1}^{\infty}\left(\frac{1}{\rho_n}+\frac{1}{\bar{\rho}_n}\right)=\sum_{n=1}^{\infty}\frac{2\mathrm{Re}(\rho_n)}{|\rho_n|^2}>0,$$

and hence $\mathrm{Re}(b)>0$ follows from (9.45).

Further, we rewrite the equation (9.45) into the form

$$\sum_{\nu}\frac{1}{|s_\nu|^2}+\sum_{\mathrm{Re}(\rho_n)\neq 1/2}\frac{2\mathrm{Re}(\rho_n)}{|\rho_n|^2}=2\mathrm{Re}(b),$$

which yields easily the second part of conclusions in Theorem 9.13. □

Dirichlet L-functions were constructed by Dirichlet [49] to tackle the problem of the distribution of primes in arithmetic progressions.

Theorem 9.14 (Dirichlet's prime number theorem). *Every arithmetic progression*

$$a,\ \ a\pm r,\ \ a\pm 2r,\ \ a\pm 3r,\ldots,$$

i.e., every class $a \bmod r$*, contains infinitely many prime numbers, where* $\gcd(a,r)=1$.

Proof. Let χ be a Dirichlet character mod r. One finds

$$\log L(\chi, s) = -\sum_p \log\left\{1 - \chi(p)p^{-s}\right\} = \sum_p \sum_{n=1}^{\infty} \frac{\chi(p^n)}{np^{ns}} = \sum_p \frac{\chi(p)}{p^s} + g_\chi(s)$$

for $\mathrm{Re}(s) > 1$, where $g_\chi(s)$ is holomorphic for $\mathrm{Re}(s) > \frac{1}{2}$. Multiplying by $\chi(a^{-1})$ and summing over all characters mod r, it yields

$$\begin{aligned}\sum_\chi \chi(a^{-1}) \log L(\chi, s) &= \sum_\chi \sum_p \frac{\chi(a^{-1}p)}{p^s} + g(s) \\ &= \sum_{k=1}^{r} \sum_\chi \chi(a^{-1}k) \sum_{p \equiv k(r)} \frac{1}{p^s} + g(s) \\ &= \sum_{p \equiv a(r)} \frac{\varphi(r)}{p^s} + g(s),\end{aligned}$$

where note that

$$\sum_\chi \chi(a^{-1}k) = \begin{cases} 0, & \text{if } a \neq k, \\ \varphi(r), & \text{if } a = k. \end{cases}$$

When we pass to the limit $s \to 1$ ($s > 1$ real), $\log L(\chi, s)$ stays bounded for $\chi \neq \chi^0$ because $L(\chi, 1) \neq 0$, whereas

$$\log L(\chi^0, s) = \sum_{p|r} \log\{1 - p^{-s}\} + \log \zeta(s) \to \infty$$

because $\zeta(s)$ has a pole at $s = 1$. Therefore, the left-hand side of the above equation tends to ∞, and since $g(s)$ is holomorphic at $s = 1$, we find

$$\lim_{s \to 1} \sum_{p \equiv a(r)} \frac{\varphi(r)}{p^s} = \infty.$$

Thus the sum cannot consist of only finitely many terms, and the theorem is proved.□

Further, let $\pi(x; a \bmod r)$ denote the number of primes $p \leq x$ in the residue class a mod r. Using similar techniques as for $\zeta(s)$, then for a coprime with r,

$$\pi(x; a \bmod r) \sim \frac{\pi(x)}{\varphi(r)}. \tag{9.46}$$

This shows that the primes are uniformly distributed in the prime residue classes.

9.2 The Dedekind zeta-function

9.2.1 The ζ-functions of number fields

The Riemann's ζ-function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is associated with the field $\mathbb{Q}$ of rational numbers, and generalizes in the following way to an arbitrary number field κ of degree $n = [\kappa : \mathbb{Q}]$.

Definition 9.15. The *Dedekind's ζ-function* of the number field κ is defined by the series

$$\zeta_\kappa(s) = \sum_{\mathfrak{a}} \frac{1}{\mathcal{N}(\mathfrak{a})^s},$$

where $\mathfrak{a}$ varies over the integral ideals of κ, and $\mathcal{N}(\mathfrak{a})$ denotes the absolute norm of $\mathfrak{a}$.

The unique factorization of ideals, along with the norm computations, imply that there exist only a finite number $a_\kappa(n)$ of integral ideals with norm n. Now, moreover, for two rational integers m, n with $\gcd(m, n) = 1$

$$a_\kappa(mn) = a_\kappa(m)a_\kappa(n). \tag{9.47}$$

In fact, from two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ with $\mathcal{N}(\mathfrak{a}) = m$, $\mathcal{N}(\mathfrak{b}) = n$, an ideal $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ arises with $\mathcal{N}(\mathfrak{c}) = mn$. Conversely, if $\mathfrak{c}$ is an integral ideal with $\mathcal{N}(\mathfrak{c}) = mn$, we set

$$(\mathfrak{c}, m) = \mathfrak{a}, \quad (\mathfrak{c}, n) = \mathfrak{b}, \tag{9.48}$$

and so it follows by multiplication that

$$\mathfrak{a}\mathfrak{b} = (\mathfrak{c}^2, \mathfrak{c}m, \mathfrak{c}n, mn) = \mathfrak{c}\left(\mathfrak{c}, m, n, \frac{mn}{\mathfrak{c}}\right) = \mathfrak{c}.$$

By passage to the conjugate, we obtain from (9.48) that $\mathcal{N}(\mathfrak{a})$ is coprime to n and $\mathcal{N}(\mathfrak{b})$ is coprime to m, while the product $\mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}) = mn$. Consequently, $\mathcal{N}(\mathfrak{a}) = m$, $\mathcal{N}(\mathfrak{b}) = n$, and $\mathfrak{c}$ is thus decomposed into two factors whose norms are m and n respectively. The assertion (9.47) follows from this.

We can write the ζ-function of κ as follows

$$\zeta_\kappa(s) = \sum_{n=1}^{\infty} \frac{a_\kappa(n)}{n^s}.$$

By Theorem 2.37 and Theorem 9.2, we find that the abscissa of convergence of $\zeta_\kappa(s)$ is 1, and so it follows that:

Proposition 9.16. *The series $\zeta_\kappa(s)$ converges absolutely and uniformly in the region $\mathrm{Re}(s) \geq 1+\varepsilon$ for every $\varepsilon > 0$, and one has*

$$\zeta_\kappa(s) = \prod_{\mathfrak{p}} \frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}}, \tag{9.49}$$

where $\mathfrak{p}$ runs through the prime ideals of κ.

The product in (9.49) converges since $\sum_{\mathfrak{p}} 1/\mathcal{N}(\mathfrak{p})^s$ converges as the constituent of the series for $\zeta_\kappa(s)$. For each prime ideal $\mathfrak{p}$ of κ, we obtain a convergent series

$$\frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}} = 1 + \frac{1}{\mathcal{N}(\mathfrak{p})^s} + \frac{1}{\mathcal{N}(\mathfrak{p}^2)^s} + \cdots . \tag{9.50}$$

If we multiply these expressions in a purely formal way for all $\mathfrak{p}$, then we obtain

$$\prod_{\mathfrak{p}} \frac{1}{1-\mathcal{N}(\mathfrak{p})^{-s}} = 1 + \cdots + \frac{1}{\mathcal{N}(\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_r^{a_r})^s} + \cdots , \tag{9.51}$$

where each product of powers of prime ideals appears exactly once in the norm symbol. However, by the fundamental theorem of ideal theory, we obtain each integral ideal of κ exactly once in this form, that is, all terms of the convergent series $\zeta_\kappa(s)$ appear exactly once. Since the series (9.50) converges absolutely for $\mathrm{Re}(s) > 1$ for each prime ideal $\mathfrak{p}$ of κ and the product (9.51) converges for $\mathrm{Re}(s) > 1$, the equality (9.49) follows from the formal agreement of the terms of the series.

The holomorphic function $\zeta_\kappa(s)$ in the domain $\mathrm{Re}(s) > 1$ admits a meromorphic continuation onto the entire complex plane. According to Erich Hecke (1887–1947), or see the arguments in [202], there exist two continuous functions $f, g : \mathbb{R}^+ \longrightarrow \mathbb{C}$ such that for $x \to \infty$

$$f(x) = \frac{2^{r_1+r_2-1}}{w}\mathbf{h}R + O\left(e^{-cx^\alpha}\right), \quad g(x) = \frac{2^{r_1+r_2-1}}{w}\mathbf{h}R + O\left(e^{-cx^\alpha}\right)$$

with positive constants c, α, where r_1 (resp. r_2) is the number of real (resp. complex) places of κ, $\mathbf{h}$ is the class number of κ, R is the regulator of κ, and w denotes the number of roots of unity in κ, which are related by the formula

$$f\left(\frac{1}{x}\right) = x^{\frac{1}{2}} g(x),$$

such that the Mellin transform

$$\Lambda_\kappa(2s) = \int_0^\infty \{f(x) - f(\infty)\} x^s \frac{dx}{x}$$

holds, where

$$\Lambda_\kappa(s) = |D_{\kappa/\mathbb{Q}}|^{s/2} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} \zeta_\kappa(s)$$

in which the function $\Gamma_{\mathbb{C}}(s)$ is defined by

$$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s).$$

Hence $\Lambda_\kappa(s)$ admits an analytic continuation to $\mathbb{C} - \{0, 1\}$ and satisfies functional equation (cf. [164], [202]):

$$\Lambda_\kappa(s) = \Lambda_\kappa(1 - s). \tag{9.52}$$

It has simple poles at $s = 0$ and $s = 1$ with residues

$$-\frac{2^{r_1+r_2}}{w}\mathbf{h}R, \quad \frac{2^{r_1+r_2}}{w}\mathbf{h}R,$$

respectively. It is convenient to use the entire function

$$\xi_\kappa(s) = \frac{s}{2}(s-1)|D_{\kappa/\mathbb{Q}}|^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_\kappa(s)$$

which satisfies the functional equation

$$\xi_\kappa(s) = \xi_\kappa(1 - s). \tag{9.53}$$

Therefore $\zeta_\kappa(s)$ admits a holomorphic continuation with the exclusion of a simple pole at $s = 1$, and satisfies the following functional equation

$$\zeta_\kappa(1-s) = |D_{\kappa/\mathbb{Q}}|^{s-\frac{1}{2}}\left(\cos\frac{\pi s}{2}\right)^{r_1+r_2}\left(\sin\frac{\pi s}{2}\right)^{r_2}\Gamma_{\mathbb{C}}(s)^n\zeta_\kappa(s). \tag{9.54}$$

It follows that $\zeta_\kappa(1-m) = 0$ for odd $m > 1$. If the number field κ is totally real, then we have $\zeta_\kappa(1-m) \neq 0$ for even $m > 1$. If the number field κ is not totally real, then we have $\zeta_\kappa(1-m) = 0$ for all $m = 2, 3, 4, \ldots$.

By Theorem 2.37 and Lemma 9.3, we have the following fact:

Theorem 9.17. *There exists a positive number $\varkappa$, defined by* (2.29)*, such that*

$$\lim_{s\to 1}(s-1)\zeta_\kappa(s) = \varkappa.$$

9.2.2 Selberg class

Many authors have introduced classes of Dirichlet series to find common patterns in their value distribution. However, the most successful class seems to be the class introduced by Selberg [235]. The *Selberg class* $\mathcal{S}$ consists of Dirichlet series

$$L(s) = \sum_{n=1}^{\infty}\frac{a(n)}{n^s}$$

satisfying the following hypotheses:

(1) *Ramanujan hypothesis*. $a(n) = O(n^{\varepsilon})$ for any $\varepsilon > 0$, where the implicit constant may depend on ε.

(2) *Analytic continuation*. There exists a non-negative integer k such that $(s-1)^k L(s)$ is an entire function of finite order.

(3) *Functional equation*. $L(s)$ satisfies a functional equation of type

$$\Lambda_L(s) = \omega\overline{\Lambda_L(1-\bar{s})}, \tag{9.55}$$

where

$$\Lambda_L(s) = Q^s L(s) \prod_{j=1}^{f} \Gamma(\lambda_j s + \mu_j)$$

with positive real numbers Q, λ_j and complex numbers μ_j, ω with $\mathrm{Re}(\mu_j) \geq 0$ and $|\omega| = 1$.

(4) *Euler product*. $L(s)$ has a product representation

$$L(s) = \prod_p L_p(s),$$

where

$$L_p(s) = \exp\left(\sum_{n=1}^{\infty} \frac{b(p^n)}{p^{ns}}\right)$$

with suitable coefficients $b(p^n)$ satisfying $b(p^n) = O(p^{n\theta})$ for some $\theta < \frac{1}{2}$.

The Ramanujan hypothesis implies the absolute convergence of the Dirichlet series $L(s)$ in the half-plane $\mathrm{Re}(s) > 1$, and uniform convergence in every compact subset. Thus $L(s)$ is analytic for $\mathrm{Re}(s) > 1$. The Euler product hypothesis implies that the coefficients $a(n)$ are *multiplicative*, that is, $a(1) \neq 0$ and

$$a(mn) = a(m)a(n)$$

for all coprime integers m, n, and that each Euler factor has the Dirichlet series representation

$$L_p(s) = \sum_{n=0}^{\infty} \frac{a(p^n)}{p^{ns}}$$

absolutely convergent for $\mathrm{Re}(s) > 0$. Comparing two representations of $L_p(s)$, we can obtain $a(p) = b(p)$. Moreover, it turns out that each Euler factor is non-vanishing for $\mathrm{Re}(s) > \theta$.

The *degree* of $L \in \mathcal{S}$ is defined by

$$d_L = 2\sum_{j=1}^{f} \lambda_j.$$

The constant function 1 is the only element of $\mathcal{S}$ of degree zero. Recently, Kaczorowski and Perelli [122] proved that all functions $L \in \mathcal{S}$ with degree $0 < d_L < \frac{5}{3}$ have degree equal to one. It is conjectured that all $L \in \mathcal{S}$ have integral degree (cf. [262]).

By the work of Kaczorowski and Perelli [121], it is known that the functions of degree one in the Selberg class are the Riemann zeta-function and shifts $L(\chi, s + i\varphi)$ of Dirichlet L-functions attached to primitive character χ with $\varphi \in \mathbb{R}$. Examples of degree two are L-functions associated with holomorphic newforms. Other examples in the Selberg class are Dedekind zeta-functions to number fields κ; their degrees are equal to the degrees $[\kappa : \mathbb{Q}]$ of the field extensions $\kappa/\mathbb{Q}$.

In view of the Euler product representation, it is obvious that each element $L(s) \in \mathcal{S}$ does not vanish in the half-plane of absolute convergence $\mathrm{Re}(s) > 1$. The zeros of $L(s)$ located at the poles of Γ-factors appearing in the functional equation are called *trivial*, which all lie in $\mathrm{Re}(s) \leq 0$. All other zeros are said to be *non-trivial*.

Conjecture 9.18 (Grand Riemann Hypothesis). *If $L \in \mathcal{S}$, then $L(s) \neq 0$ for $\mathrm{Re}(s) > \frac{1}{2}$.*

If $N_L(T)$ counts the number of zeros of $L(s) \in \mathcal{S}$ in the rectangle $0 \leq \mathrm{Re}(s) \leq 1$, $|\mathrm{Im}(s)| \leq T$ (according to multiplicities), by standard contour integration one (cf. [262]) can show

$$N_L(T) = \frac{d_L T}{\pi} \log \frac{T}{e} + \frac{T}{\pi} \log(\lambda Q^2) + O(\log T), \tag{9.56}$$

where

$$\lambda = \prod_{j=1}^{f} \lambda_j^{2\lambda_j}.$$

Ye [303] computed the Nevanlinna functions for the Riemann zeta-function. Following Ye [303], Steuding [262] proved that if $L(s)$ satisfies axioms (1)–(3) with $a(1) = 1$, the Nevanlinna characteristic function $T(r, L)$ satisfies the asymptotic formula

$$T(r, L) = \frac{d_L}{\pi} r \log r + O(r), \tag{9.57}$$

and hence when $d_l \neq 0$, $L(s)$ is of order one, that is,

$$\limsup_{r \to \infty} \frac{\log T(r, L)}{\log r} = 1.$$

Similar to Theorem 9.12 and Theorem 9.13, we can prove the following result:

Theorem 9.19. *For a number field κ, $\xi_\kappa(s)$ is an entire function of order 1, and has infinitely many zeros ρ_n satisfying the conditions: $0 \leq \mathrm{Re}(\rho_n) \leq 1$, the series $\sum_{n=1}^{\infty} |\rho_n|^{-1}$ diverges, the series $\sum_{n=1}^{\infty} |\rho_n|^{-1-\varepsilon}$ converges for any $\varepsilon > 0$, and*

Hadamard's factorization

$$\xi_\kappa(s) = \frac{2^{r_1+r_2-1}}{w}\mathbf{h}Re^{-bs}\prod_{n=1}^{\infty}\left(1-\frac{s}{\rho_n}\right)e^{\frac{s}{\rho_n}} \tag{9.58}$$

holds, where b is a positive constant. Moreover, the Grand Riemann Hypothesis for $\zeta_\kappa(s)$ holds if and only if the zeros s_ν of $\zeta_\kappa(s)$ on the critical line $\mathrm{Re}(s) = \frac{1}{2}$ satisfy

$$\sum_\nu \frac{1}{|s_\nu|^2} = 2b. \tag{9.59}$$

9.3 Special linear groups

9.3.1 General linear groups

For any commutative ring A, the *general linear group* $\mathrm{GL}(2, A)$ is defined to be the set of matrices

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that

$$\det(\gamma) = ad - bc \in A_*.$$

The *special linear group* $\mathrm{SL}(2, A)$ is defined to be the subgroup of $\mathrm{GL}(2, A)$ consisting of matrices of determinant 1.

Set $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ which is isomorphic to $\mathbb{P}^1(\mathbb{C})$, and take

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R}),\ \ z \in \bar{\mathbb{C}}.$$

We define

$$\gamma(z) = \begin{cases} \frac{az+b}{cz+d}, & \text{if } z \in \mathbb{C}, \\ \frac{a}{c}, & \text{if } z = \infty, \end{cases} \tag{9.60}$$

and hence $\gamma(-d/c) = \infty$, where we think $\gamma(\infty) = \infty$ if $c = 0$. These mappings $z \mapsto \gamma(z)$ are called *fractional linear transformations* of the Riemann sphere $\bar{\mathbb{C}}$. It is easy to check that (9.60) defines a group action on the set $\bar{\mathbb{C}}$, in other words:

$$\gamma_1(\gamma_2(z)) = (\gamma_1\gamma_2)(z),\ \{\gamma_1, \gamma_2\} \subset \mathrm{GL}(2, \mathbb{R});\ z \in \bar{\mathbb{C}}.$$

Take a subgroup Γ of $\mathrm{GL}(2, \mathbb{R})$. For an element z of $\bar{\mathbb{C}}$ we put

$$\Gamma_z = \{\gamma \in \Gamma \mid \gamma(z) = z\},$$

and call it the *stabilizer* of z. It is obvious that for any element γ of Γ,

$$\Gamma_{\gamma(z)} = \gamma^{-1}\Gamma_z\gamma.$$

An element z of $\bar{\mathbb{C}}$ is called a *fixed point* of $\gamma \in \Gamma$ if $\gamma(z) = z$. This is equivalent to saying $\gamma \in \Gamma_z$.

We consider the fractional linear transformation (9.60) again. Note that

$$\mathrm{Im}(\gamma(z)) = \frac{\det(\gamma)}{|cz+d|^2}\mathrm{Im}(z), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{R}).$$

In particular, for the case $\det(\gamma) > 0$, then $\mathrm{Im}(z) > 0$ implies that $\mathrm{Im}(\gamma(z)) > 0$. Let $\mathbb{H} \subset \mathbb{C}$ denote the upper half plane

$$\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}.$$

We put

$$\mathrm{GL}^+(2,\mathbb{R}) = \{\gamma \in \mathrm{GL}(2,\mathbb{R}) \mid \det(\gamma) > 0\}.$$

Thus, $\mathrm{GL}^+(2,\mathbb{R})$ acts on the set $\mathbb{H}$ by the transformations (9.60).

We classify elements of $\mathrm{GL}^+(2,\mathbb{R})$ by the following way. A non-scalar element γ of $\mathrm{GL}^+(2,\mathbb{R})$ is called *elliptic*, *parabolic* or *hyperbolic*, when it satisfies

$$\mathrm{trace}(\gamma)^2 < 4\det(\gamma), \quad \mathrm{trace}(\gamma)^2 = 4\det(\gamma), \quad \mathrm{trace}(\gamma)^2 > 4\det(\gamma),$$

respectively. The following simple fact explains the geometrical meaning of the classification.

Theorem 9.20. *A non-scalar element γ of $\mathrm{GL}^+(2,\mathbb{R})$ is characterized by its fixed points on $\bar{\mathbb{C}}$ as follows:*

(1) *γ is elliptic if and only if γ has the fixed points z and $\bar{z}$ with $z \in \mathbb{H}$;*

(2) *γ is parabolic if and only if γ has a unique fixed point on $\in \mathbb{R} \cup \{\infty\}$;*

(3) *γ is hyperbolic if and only if γ has two distinct fixed points on $\in \mathbb{R} \cup \{\infty\}$.*

Set

$$\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{R} \cup \{\infty\}.$$

When $z \in \overline{\mathbb{H}}$ is a fixed point of an elliptic, parabolic or hyperbolic element of a subgroup Γ of $\mathrm{GL}^+(2,\mathbb{R})$, we say that z is an *elliptic point*, a *parabolic point* or a *hyperbolic point* of Γ, respectively. We also call a parabolic point of Γ a *cusp* of Γ.

Proposition 9.21. *Let Γ be a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$. If $x \in \mathbb{R} \cup \{\infty\}$ is a cusp of Γ, then*

$$\Gamma_x \subset \{\gamma \in \mathrm{SL}(2,\mathbb{R})_x \mid \gamma \textit{ is parabolic or scalar}\},$$

and

$$\Gamma_x/(\Gamma \cap \{\pm\mathbf{1}\}) \cong \mathbb{Z}.$$

Moreover for $\gamma \in \mathrm{SL}(2,\mathbb{R})$ such that $\gamma(\infty) = x$, we have

$$\gamma^{-1}\Gamma_x\gamma \cdot \{\pm\mathbf{1}\} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m \;\middle|\; m \in \mathbb{Z} \right\}$$

for some $h > 0$, where $\mathbf{1}$ is the unit in Γ.

Proof. See [186], Theorem 1.5.4. □

9.3.2 Modular groups

The subgroup of $\mathrm{SL}(2,\mathbb{R})$ consisting of matrices with integer entries is, by definition, $\mathrm{SL}(2,\mathbb{Z})$. It is called the *modular group* or, more precisely, the *elliptic modular group*. Let N be a positive integer. One defines subgroups of $\mathrm{SL}(2,\mathbb{Z})$ as follows:

$$\Gamma_0(N)=\left\{\left(\begin{array}{cc}a & b\\ c & d\end{array}\right)\in \mathrm{SL}(2,\mathbb{Z})\,\middle|\, c\equiv 0\ (\mathrm{mod}N)\right\}, \tag{9.61}$$

$$\Gamma_1(N)=\left\{\gamma\in \mathrm{SL}(2,\mathbb{Z})\,\middle|\, \gamma\equiv\left(\begin{array}{cc}1 & b\\ 0 & 1\end{array}\right)\ (\mathrm{mod}N)\right\}, \tag{9.62}$$

and

$$\Gamma(N)=\left\{\gamma\in \mathrm{SL}(2,\mathbb{Z})\,\middle|\, \gamma\equiv\left(\begin{array}{cc}1 & 0\\ 0 & 1\end{array}\right)\ (\mathrm{mod}N)\right\}. \tag{9.63}$$

We note

$$\Gamma(1)=\Gamma_1(1)=\Gamma_0(1)=\mathrm{SL}(2,\mathbb{Z}),$$

and

$$\Gamma(N)\subset\Gamma_1(N)\subset\Gamma_0(N)\subset\mathrm{SL}(2,\mathbb{Z}).$$

Further if $M|N$, then

$$\Gamma(N)\subset\Gamma(M),\quad \Gamma_1(N)\subset\Gamma_1(M),\quad \Gamma_0(N)\subset\Gamma_0(M).$$

We call $\Gamma(N)$ a *principal congruence modular group*, and $\Gamma_1(N)$ and $\Gamma_0(N)$ *modular group of Hecke type*. We call N the *level* of $\Gamma(N)$, $\Gamma_1(N)$ and $\Gamma_0(N)$. More generally, for some integer $N\geq 1$, a *congruence subgroup of lebel* N of $\mathrm{SL}(2,\mathbb{Z})$ is defined to be a subgroup Γ of $\mathrm{SL}(2,\mathbb{Z})$ which contains $\Gamma(N)$.

If Γ is a subgroup of $\mathrm{SL}(2,\mathbb{Z})$, we say that two points $\tau,\tau'\in\mathbb{H}$ are Γ-*equivalent* if there exists $\gamma\in\Gamma$ such that $\tau'=\gamma(\tau)$, and denote this relation between τ and τ' by

$$\tau=\tau' \bmod \Gamma. \tag{9.64}$$

Let $\mathfrak{B}$ be a region in $\mathbb{H}$. We say that $\mathfrak{B}$ is a *fundamental region* for Γ if every $\tau\in\mathbb{H}$ is Γ-equivalent to a point in $\mathfrak{B}$, but no two distinct points τ_1,τ_2 in $\mathfrak{B}$ are Γ-equivalent. The most famous example of a fundamental region for $\mathrm{SL}(2,\mathbb{Z})$ is as follows

$$\mathfrak{B}=\left\{x+iy\in\mathbb{H}\,\middle|\, x^2+y^2\geq 1,\ -\frac{1}{2}\leq x<\frac{1}{2}\right\}-l,$$

where

$$l=\left\{x+iy\in\mathbb{H}\,\middle|\, x^2+y^2=1,\ 0<x<\frac{1}{2}\right\}.$$

We identify $\mathbb{Q} \cup \{\infty\}$ with $\mathbb{P}^1(\mathbb{Q})$. Here one should think of the points $[x, 1] \in \mathbb{P}^1(\mathbb{Q})$ as forming the usual copy of $\mathbb{Q}$ in $\mathbb{C}$; and the point $[1, 0] \in \mathbb{P}^1(\mathbb{Q})$ as a point at infinity. Notice that $\mathrm{SL}(2, \mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Q})$ in the usual manner,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : [x, y] \longmapsto [ax + by, cx + dy].$$

Define

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

That is, we add to $\mathbb{H}$ a point at infinity (which should be visualized for up the positive imaginary axis; for this reason we sometimes denote it $i\infty$) and also all of the rational numbers on the real axis. These points $\mathbb{P}^1(\mathbb{Q})$ are called *cusps* of $\mathrm{SL}(2, \mathbb{Z})$. It is easy to see that $\mathrm{SL}(2, \mathbb{Z})$ permutes the cusps transitively. If Γ is a subgroup of $\mathrm{SL}(2, \mathbb{Z})$, then Γ permutes the cusps, but in general not transitively. That is, there is usually more than one Γ-equivalence class among the cusps $\mathbb{P}^1(\mathbb{Q})$. A Γ-equivalence class of cusps is also called a *cusp of* Γ. We may choose any convenient representative of the equivalence class to denote the cusp.

We extend the usual topology on $\mathbb{H}$ to the set $\mathbb{H}^*$ as follows. First, a fundamental system of open neighborhoods of ∞ is

$$U_\infty = \{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) > r\} \cup \{\infty\}$$

for any $r > 0$. Note that if we map $\mathbb{H}$ to the punctured open unit disc by sending

$$\tau \mapsto z = e^{2\pi i \tau}, \tag{9.65}$$

and if we agree to take the point $\infty \in \mathbb{H}^*$ to the origin under this mapping, then U_∞ is the the inverse image of the open disc of radius $e^{-2\pi r}$ centered at the origin, and we have defined our topology on $\mathbb{H} \cup \{\infty\}$ so as to make the mapping (9.65) continuous.

Near a cusp $x \in \mathbb{Q} \subset \mathbb{H}^*$ by writing $x = a/c$ in which a, c are coprime, we define a fundamental system of open neighborhoods by completing a, c to a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$$

by finding solution b and d to the equation $ad - bc = 1$, and using γ to transport the U_∞ to discs in $\mathbb{H}^*$ which are tangent to the real axis at $x = \gamma(\infty)$. According to this topology, a sequence τ_j approaches x means that $\gamma^{-1}(\tau_j)$ approaches $i\infty$, i.e., that $\mathrm{Im}(\gamma^{-1}(\tau_j))$ approaches infinity in the usual sense.

We may use (9.65) to define an analytic structure on $\mathbb{H}^*$. Near ∞, we say that a function f of period 1 on $\mathbb{H}$ is *meromorphic* at ∞ if it can be expressed as a power series in the variable z having at most finitely many negative terms, i.e., f has a Fourier expansion of the form

$$f(\tau) = \sum_{n \geq m} c_n z^n = \sum_{n \geq m} c_n e^{2\pi i n \tau} \tag{9.66}$$

for some integer $m \in \mathbb{Z}$. We say that f is *holomorphic* at ∞ if $m = 0$; and we say that f *vanishes* (or has a *zero*) at ∞ if f is holomorphic at ∞ with $c_0 = 0$. More generally, if f has period N, then we use the mapping

$$\tau \mapsto z^{1/N} = e^{2\pi i\tau/N} \tag{9.67}$$

to map $\mathbb{H} \cup \{\infty\}$ to the open unit disc. We then say that f is *meromorphic* (*holomorphic*; *vanishes*) at ∞ if we can express f as a series in $z^{1/N}$

$$f(\tau) = \sum_{n \geq \mu} a_n z^{n/N} \tag{9.68}$$

for some integer $\mu \in \mathbb{Z}$ (respectively, for $\mu = 0$; for $\mu = 1$). Similarly, we can define analytic structure near any cusp (see Section 9.4).

Let $\bar{\mathfrak{B}}$ denote the fundamental region $\mathfrak{B}$ with $\mathrm{SL}(2,\mathbb{Z})$-equivalent boundary points identified and with the cusp ∞ thrown in. Thus, the points of $\bar{\mathfrak{B}}$ are in one-to-one correspondence with $\mathrm{SL}(2,\mathbb{Z})$-equivalence classes in $\mathbb{H}^*$, and so we have the identification:

$$\bar{\mathfrak{B}} = \mathbb{H}^*/\mathrm{SL}(2,\mathbb{Z}).$$

We take the topology on $\bar{\mathfrak{B}}$ which comes from the topology on $\mathbb{H}^*$. That is, by a small disc around an interior point of $\mathfrak{B}$ we mean a disc in the usual sense; by a small disc around ∞ we mean all points lying above the line $\mathrm{Im}(\tau) = r$, where r is large; by a small disc around a boundary point $-\frac{1}{2} + iy$ we mean the half-disc contained in $\mathfrak{B}$ together with the half-disc of the same radius around $\frac{1}{2} + iy$ which is contained in $\mathfrak{B}$; and so on. Thus, $\bar{\mathfrak{B}}$ has an analytic structure coming from the usual structure on $\mathbb{H}$, except at ∞, where it comes from the usual structure at 0 after the change of variable (9.65). If Γ is a congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$, then Γ acts on $\mathbb{H}^*$, and we can form the quotient space $\mathbb{H}^*/\Gamma$, which has a natural structure as a Riemann surface (see Shimura [245], Sections 1.3 and 1.5).

We may view $1/N$ as a point of order N on the torus $\mathbb{C}/[1,\tau]$. Let Z_N be the cyclic group generated by $1/N$. Then we may consider the pair $(\mathbb{C}/[1,\tau], Z_N)$ as consisting of a torus and a cyclic subgroup of order N. One has the following parametrizations:

(f1) The association $\tau \mapsto (\mathbb{C}/[1,\tau], 1/N)$ gives a bijection between $\mathbb{H}/\Gamma_1(N)$ and isomorphism classes of toruses together with a point of order N.

(f2) The association $\tau \mapsto (\mathbb{C}/[1,\tau], Z_N)$ gives a bijection between $\mathbb{H}/\Gamma_0(N)$ and isomorphism classes of toruses together with a cyclic subgroup of order N.

Furthermore, there exist affine curves $Y_1(N)$ and $Y_0(N)$, defined over $\mathbb{Q}$, such that

$$Y_1(N)(\mathbb{C}) \approx \mathbb{H}/\Gamma_1(N), \quad Y_0(N)(\mathbb{C}) \approx \mathbb{H}/\Gamma_0(N)$$

and such that $Y_1(N)$ parametrizes isomorphism classes of pairs (E,P) algebraically, where E is an elliptic curve and P is a point of order N, in the following sense. If κ is

a field containing $\mathbb{Q}$, then a point of $Y_1(N)(\kappa)$ corresponds to such a pair (E, P) with E defined over κ and P rational over κ. Similarly, $Y_0(N)$ parametrizes pairs (E, Z), where E is defined over κ and Z is invariant under the Galois group $G_{\kappa/\mathbb{Q}}$. The affine curve $Y_1(N)$ can be compactified by adjointing the points which lie above $j = \infty$. Its completion, denoted by $X_1(N)$, is a smooth projective curve which contains $Y_1(N)$ as a dense Zariski open subset. Similarly, we have the completion $X_0(N)$ of $Y_0(N)$. Thus one obtains the holomorphic isomorphisms

$$X_1(N)(\mathbb{C}) \approx \mathbb{H}^*/\Gamma_1(N), \quad X_0(N)(\mathbb{C}) \approx \mathbb{H}^*/\Gamma_0(N).$$

See Shimura [245], or Silverman [256].

9.4 Modular functions

9.4.1 Automorphic forms

Let M be a complex manifold, let $\mathcal{M}(M)$ be the set of meromorphic functions on M, let $\mathcal{A}(M)$ be the set of holomorphic functions on M, let $\mathcal{A}^*(M)$ be the elements in $\mathcal{A}(M)$ vanishing nowhere, and let $\mathrm{Aut}(M)$ be the *group of automorphisms* on M, where the group operation is composition, and where an *automorphism* on M means a biholomorphic self-mapping on M.

Definition 9.22. Let M be a complex manifold and let Γ be a discrete subgroup of $\mathrm{Aut}(M)$. A meromorphic function $f \in \mathcal{M}(M)$ is called a (*multiplicative*) *automorphic function* for Γ if each $\gamma \in \Gamma$ determines an element $j_\gamma \in \mathcal{A}^*(M)$ such that

$$f(\gamma(z)) = j_\gamma(z) f(z), \ \ z \in M.$$

In particular, f is called a *multiplicative function* if all j_γ are constants, an *automorphic function* if $j_\gamma = 1$ for each $\gamma \in \Gamma$, and called an *automorphic form of weight* k if

$$j_\gamma(z) = J_\gamma(z)^{-k}, \ \ \gamma \in \Gamma,$$

where J_γ is the Jacobian determinant of γ.

We have interesting to a discrete subgroup Γ of $\mathrm{SL}(2, \mathbb{R})$ acting on $\mathbb{H}$, called usually a *Fuchsian group*. Take

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \tau \longmapsto \gamma(\tau) = \frac{a\tau + b}{c\tau + d}$$

and define

$$f_{\gamma,k}(\tau) := \left\{ \frac{d\gamma(\tau)}{d\tau} \right\}^{k/2} f(\gamma(\tau)).$$

Note that the Jacobian determinant J_γ of γ is just

$$\frac{d\gamma(\tau)}{d\tau} = \frac{1}{(c\tau+d)^2}.$$

By the definition, an automorphic form f of weight k for Γ satisfies

$$f_{\gamma,2k}(\tau) = f(\tau),\ \ \tau \in \mathbb{H},$$

or equivalently

$$(c\tau+d)^{-2k} f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau),\ \ \tau \in \mathbb{H}. \tag{9.69}$$

We denote by $\mathfrak{M}_k(\Gamma)$ the set of all automorphic forms of weight $k/2$ for Γ. Then $\mathfrak{M}_k(\Gamma)$ is a vector space over $\mathbb{C}$, and generates a graded ring

$$\mathfrak{M}(\Gamma) = \sum_{k=-\infty}^{\infty} \mathfrak{M}_k(\Gamma).$$

The following properties are trivial

$$\mathfrak{M}_k(\Gamma) \subset \mathfrak{M}_k(\Gamma'),\ \text{if } \Gamma \supset \Gamma';$$

$$\mathfrak{M}_k(\Gamma) = \{0\},\ \text{if } k \text{ is odd and } -\mathbf{1} \in \Gamma;$$

$$\mathfrak{M}_k(\Gamma)\mathfrak{M}_l(\Gamma) \subset \mathfrak{M}_{k+l}(\Gamma),$$

where $\mathbf{1}$ means the unit of Γ.

Suppose that k is even and that x is a cusp of Γ. Let γ be an element of $\mathrm{SL}(2,\mathbb{R})$ such that $\gamma(\infty) = x$. Since $f_{\gamma,k} \in \mathfrak{M}_k(\gamma^{-1}\Gamma\gamma)$ for $f \in \mathfrak{M}_k(\Gamma)$, by using Proposition 9.21, there exists $h > 0$ satisfying

$$f_{\gamma,k}(\tau+h) = f_{\gamma,k}(\tau).$$

Therefore there exists a meromorphic function g on the domain

$$D = \{z \in \mathbb{C} \mid 0 < |z| < 1\}$$

such that

$$f_{\gamma,k}(\tau) = g\big(e^{2\pi i\tau/h}\big),\ \ \tau \in \mathbb{H},$$

which yields the Laurent expansion

$$f_{\gamma,k}(\tau) = \sum_{n=\mu}^{\infty} c_n e^{2\pi i n\tau/h}$$

with $\mu \in \mathbb{Z} \cup \{-\infty\}$ on $\{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) > R\}$ for a sufficiently large R. The series is convergent absolutely and uniformly on any compact subset of $\{\tau \in \mathbb{H} \mid \mathrm{Im}(\tau) > R\}$,

and so also are on any compact subset of $\mathbb{H}$ if f is holomorphic on $\mathbb{H}$. By definition, an element f of $\mathfrak{M}_k(\Gamma)$ is *meromorphic*, is *holomorphic*, or has a *zero* at x, if the above function g is meromorphic ($\mu \neq -\infty$), is holomorphic ($\mu \geq 0$), or has a zero ($\mu \geq 1$) at 0, respectively. The above definitions are independent of the choice of γ.

When k is odd and $-\mathbf{1} \notin \Gamma$, we say that f is *meromorphic*, is *holomorphic*, or has a *zero* at x when f^2 is meromorphic, is holomorphic, or has a zero at x, respectively.

For a Fuchsian group Γ, we put

$$\begin{aligned}
\mathscr{M}_k(\Gamma) &= \{f \in \mathfrak{M}_k(\Gamma) \mid f \text{ is meromorphic at all cusps of } \Gamma\};\\
\mathcal{H}_k(\Gamma) &= \{f \in \mathfrak{M}_k(\Gamma) \mid f \text{ is holomorphic both on } \mathbb{H} \text{ and at all cusps of } \Gamma\};\\
\mathcal{S}_k(\Gamma) &= \{f \in \mathfrak{M}_k(\Gamma) \mid f \text{ is holomorphic on } \mathbb{H} \text{ and has a zero at each cusp of } \Gamma\},
\end{aligned}$$

which are vector spaces over $\mathbb{C}$, and generate graded rings

$$\mathscr{M}(\Gamma) = \sum_k \mathscr{M}_k(\Gamma), \quad \mathcal{H}(\Gamma) = \sum_k \mathcal{H}_k(\Gamma), \quad \mathcal{S}(\Gamma) = \sum_k \mathcal{S}_k(\Gamma).$$

Theorem 9.23. *Let $f \in \mathfrak{M}_k(\Gamma)$ be holomorphic on $\mathbb{H}$. If there exists a positive number ν such that*

$$f(\tau) = O\left(\mathrm{Im}(\tau)^{-\nu}\right), \quad \mathrm{Im}(\tau) \to 0$$

uniformly with respect to $\mathrm{Re}(\tau)$, then $f \in \mathcal{H}_k(\Gamma)$. Moreover, if we can take ν so that $\nu < k$, then $f \in \mathcal{S}_k(\Gamma)$.

Proof. See [186], Theorem 2.1.4. □

Theorem 9.24. *Take $f \in \mathfrak{M}_k(\Gamma)$. Then $f \in \mathcal{S}_k(\Gamma)$ if and only if $f(\tau)\mathrm{Im}(\tau)^{k/2}$ is bounded on $\mathbb{H}$.*

Proof. See [186], Theorem 2.1.5. □

9.4.2 Weierstrass $\wp$ function

Take $\omega_1, \omega_2 \in \mathbb{C}$ such that they are linearly independent over $\mathbb{R}$, that is, $\omega_i \neq 0$, $\omega_2/\omega_1 \notin \mathbb{R}$. Let Λ be the discrete subgroup of $\mathbb{C}$ generated by ω_1 and ω_2:

$$\Lambda = [\omega_1, \omega_2] = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\},$$

which is called a *lattice* over $\mathbb{Z}$. Here we simply introduce meromorphic functions on the quotient space $\mathbb{C}/\Lambda$; or equivalently, meromorphic functions on $\mathbb{C}$ which are periodic with respect to the lattice Λ. An *elliptic function* (*relative to the lattice* Λ) is a meromorphic function f on $\mathbb{C}$ which satisfies

$$f(z+\omega) = f(z), \quad z \in \mathbb{C}, \ \omega \in \Lambda.$$

The set of all such functions is clearly the field $\mathcal{M}(\mathbb{C}/\Lambda)$.

The *Eisenstein series of weight* $2k$ (*for* Λ) is the series

$$G_{2k} = G_{2k}(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \omega^{-2k},$$

which is absolutely convergent for all $k > 1$. The *Weierstrass* $\wp$ *function* (*relative to* Λ) is defined by the series

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

which converges absolutely and uniformly on every compact subset of $\mathbb{C} - \Lambda$. It defines an even elliptic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

Theorem 9.25. *Every elliptic function is a rational combination of* $\wp$ *and* $\wp'$*, i.e.,*

$$\mathcal{M}(\mathbb{C}/\Lambda) = \mathbb{C}(\wp, \wp').$$

Proof. Siegel [252], Chapter 1, Section 14, Theorem 6, or Silverman [256]. □

It is standard notation to set

$$g_2 = g_2(\Lambda) = 60G_4, \quad g_3 = g_3(\Lambda) = 140G_6. \tag{9.70}$$

A basic theorem (cf. [252]) in elliptic function theory shows that $g_2^3 - 27g_3^2 \neq 0$, and the inverse function of the *elliptic integral of the first kind* in the Weierstrass normal form

$$z = \int_\infty^w \frac{d\zeta}{\sqrt{4\zeta^3 - g_2\zeta - g_3}}$$

formed with these g_2, g_3 coincides with the Weierstrass $\wp$ function which also is unique even meromorphic function in $\mathbb{C}$ satisfying the differential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3. \tag{9.71}$$

Conversely, one has the following *uniformization theorem*:

Theorem 9.26. *Let* $A, B \in \mathbb{C}$ *satisfy* $A^3 - 27B^2 \neq 0$*. Then there exists a unique lattice* $\Lambda \subset \mathbb{C}$ *such that* $g_2(\Lambda) = A$ *and* $g_3(\Lambda) = B$*.*

Proof. See Apostol [1], Theorem 2.9; Robert [220], I.3.13; Shimura [245], Section 4.2; Serre [237], VII Proposition 5, or Siegel [252], Chapter 1, Sections 11–13. □

9.4.3 Elliptic modular functions

We here use the following form of Theorem 3.76 over $\mathbb{C}$ (cf. [253], [80]):

Theorem 9.27. *Every algebraic curve of genus* 1 *defined over* $\mathbb{C}$ *can be transformed birationally into a cubic curve* E *of the special form*

$$y^2 = 4x^3 - Ax - B \tag{9.72}$$

with constants A, B *satisfying* $\Delta = A^3 - 27B^2 \neq 0$. *Two such cubic curves are birationally equivalent if and only if they agree on the invariant*

$$j = \frac{1728A^3}{A^3 - 27B^2}. \tag{9.73}$$

If this is the case, then the two curves go over into each other under an affine transformation of the form $x \mapsto u^2x,\ y \mapsto u^3y$, *with constant* $u \neq 0$.

Next we study the curve $E/\mathbb{C}$ defined by (9.72). According to Theorem 9.26, there exists a unique lattice $\Lambda = [\omega_1, \omega_2] \subset \mathbb{C}$ such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$. Hence we can rewrite the equation (9.72) into the following form:

$$y^2 = 4x^3 - g_2x - g_3 \tag{9.74}$$

with a solution of functions $x = \wp,\ y = \wp'$. The Riemann surface $E(\mathbb{C})$ of the elliptic curve E is isomorphic to a complex torus, that is, a quotient $\mathbb{C}/\Lambda$ by using a mapping

$$[\wp, \wp', 1] : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}).$$

By possibly reversing the order of ω_1 and ω_2, we can assume that the imaginary part of the ratio $\tau = \omega_2/\omega_1$ is positive. By (9.70), the quantity

$$j = j(\Lambda) = \frac{1728g_2^3}{g_2^3 - 27g_3^2}$$

associated with the algebraic curve (9.74) depends solely on the period lattice and is homogeneous of degree 0 in ω_1, ω_2, that is, it is the same if we replace ω_1, ω_2 by $c\omega_1, c\omega_2$ for any complex number $c \neq 0$. Thus we have $j(c\Lambda) = j(\Lambda)$, and we may define $j(\tau) = j(\Lambda)$. But $\mathbb{C}/\Lambda$ is a complex torus of dimension 1, and the above arguments show that j is the single invariant for isomorphism classes of such toruses. It follows that $j = j(\tau)$, considered in the upper half plane $\mathbb{H}$, is a holomorphic function of τ alone which has the invariance property

$$j(\gamma(\tau)) = j(\tau),\ \ \tau \in \mathbb{H}$$

for $\gamma \in \mathrm{SL}(2, \mathbb{Z})$. Note that the transformation

$$\tau \mapsto \tau' = \gamma(\tau) = \frac{a\tau + b}{c\tau + d}, \quad \{a, b, c, d\} \subset \mathbb{Z},\ \ ad - bc = 1 \tag{9.75}$$

maps $\mathbb{H}$ into itself. In particular, we have

$$j(\tau+1) = j(\tau), \ \ \tau \in \mathbb{H}.$$

Hence $j(\tau)$ is an automorphic function for $\mathrm{SL}(2,\mathbb{Z})$ defined on $\mathbb{H}$.

In view of Theorem 9.27, the function $j(\tau)$ has the important property of separating every two points of $\mathbb{H}$ by its values if these points are not equivalent with respect to the modular group, that is,

$$j(\tau) \neq j(\tau'), \quad \tau \neq \tau' \bmod \mathrm{SL}(2,\mathbb{Z}),$$

which gives a holomorphic isomorphism (cf. [237])

$$j : \mathbb{H}/\mathrm{SL}(2,\mathbb{Z}) \longrightarrow \mathbb{C}.$$

One can show that the j-function then defines a holomorphic isomorphism

$$j : \mathbb{H}^*/\mathrm{SL}(2,\mathbb{Z}) \longrightarrow \mathbb{P}^1(\mathbb{C}).$$

See Shimura [245], Sections 1.3, 1.4 and 1.5 for details.

More generally, we consider an automorphic function $f(\tau)$ of one complex variable τ, which is meromorphic in $\mathbb{H}^*$ and which is invariant under the modular group. More precisely, the condition on the behavior at infinity states that there exists a Laurent expansion

$$f(\tau) = \sum_{n \geq m} c_n z^n$$

which converges for sufficiently small values of $|z|$ and contains only finitely many negative powers of z. Here the variable $z = e^{2\pi i \tau}$, $m \in \mathbb{Z}$. Every function satisfying all these conditions is called a *modular function* or, more precisely, an *elliptic modular function*.

The function $j(\tau)$ is an elliptic modular function, called the *modular invariant*, with (cf. [1], Theorem 1.18, 1.19, 1.20, or [237], VII Proposition 4, 5, 8)

$$j(\tau) = \frac{1}{z} + 744 + \sum_{n=1}^{\infty} c(n) z^n, \ \ c(n) \in \mathbb{Z}, \tag{9.76}$$

where

$$c(1) = 196884, \quad c(2) = 21493760.$$

The expansion (9.76) can be easily derived from (9.94) and (9.101) below.

The elliptic modular functions obviously form a field which consists precisely of the rational functions of $j(\tau)$ (see [252], [253], [254], [256]).

9.4.4 Hecke's theorem

Lemma 9.28. *Let f be a holomorphic function on $\mathbb{H}$ such that f has a Fourier expansion*

$$f(\tau) = \sum_{n=0}^{\infty} c_n e^{2\pi i n\tau},$$

which converges absolutely and uniformly on any compact subset of $\mathbb{H}$. Further there exists $\nu > 0$ such that

$$f(\tau) = O\left(\mathrm{Im}(\tau)^{-\nu}\right), \ \mathrm{Im}(\tau) \to 0$$

uniformly on $\mathrm{Re}(\tau)$. Then we have

$$c_n = O(n^{\nu}). \tag{9.77}$$

Proof. Note that

$$|c_n| = \left| \int_0^1 f(x+iy) e^{-2\pi i n(x+iy)} dx \right| = O\left(y^{-\nu} e^{2\pi n y}\right).$$

In particular, taking $y = 2/n$, we obtain the estimate (9.77). □

This fact is referred to Corollary 2.1.6 and (4.3.8) in [186]. Conversely, one has the following result (cf. [186], Lemma 4.3.3):

Lemma 9.29. *For a sequence $\{c_n\}_{n=0}^{\infty}$ of complex numbers, put*

$$f(\tau) = \sum_{n=0}^{\infty} c_n e^{2\pi i n\tau}, \ \tau \in \mathbb{H}.$$

If $c_n = O(n^{\nu})$ with some $\nu > 0$, then the right-hand side is convergent absolutely and uniformly on any compact subset of $\mathbb{H}$, and f is holomorphic on $\mathbb{H}$. Moreover,

$$f(\tau) = O\left(\mathrm{Im}(\tau)^{-\nu-1}\right), \ \mathrm{Im}(\tau) \to 0,$$

$$f(\tau) - c_0 = O\big(e^{-2\pi \mathrm{Im}(\tau)}\big), \ \mathrm{Im}(\tau) \to \infty$$

uniformly on $\mathrm{Re}(\tau)$.

Proof. By using the Euler–Gauss formula on Γ-function

$$\Gamma(z) = \lim_{n\to\infty} \frac{n^z n!}{z(z+1)\cdots(z+n)}, \ \mathrm{Re}(z) > 0,$$

we have for $\nu > 0$

$$\lim_{n\to\infty} \frac{n^{\nu}}{(-1)^n \binom{-\nu-1}{n}} = \Gamma(\nu+1).$$

Hence there exists a constant $C > 0$ such that

$$|c_n| \leq C(-1)^n \binom{-\nu - 1}{n}, \ \ n \geq 0.$$

Put $\tau = x + iy$, then

$$\begin{aligned} \sum_{n=0}^{\infty} |c_n| \left| e^{2\pi i n \tau} \right| &\leq C \sum_{n=0}^{\infty} (-1)^n \binom{-\nu - 1}{n} e^{-2\pi n y} \\ &= C \left(1 - e^{-2\pi y}\right)^{-\nu - 1}. \end{aligned} \tag{9.78}$$

This implies that f is convergent absolutely and uniformly on any compact subset of $\mathbb{H}$. Since

$$1 - e^{-2\pi y} = O(y), \ \ y \to 0,$$

one has

$$|f(x + iy)| = O\left(y^{-\nu - 1}\right).$$

Moreover (9.78) implies that $f(\tau)$ is bounded when $y \to \infty$. Note that the function

$$g(\tau) = \sum_{n=0}^{\infty} c_{n+1} e^{2\pi i n \tau}$$

also satisfies the assumption, and so it is bounded on a neighborhood of ∞. Therefore one obtains

$$f(\tau) - c_0 = e^{2\pi i \tau} g(\tau) = O\left(e^{-2\pi y}\right), \ \ y \to \infty,$$

and hence the lemma is proved. □

For a holomorphic function

$$f(\tau) = \sum_{n=0}^{\infty} c_n e^{2\pi i n \tau}$$

on $\mathbb{H}$ satisfying the conditions in Lemma 9.28, we put

$$L(f, s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}. \tag{9.79}$$

Since (9.77) holds, then the Dirichlet series $L(f, s)$ converges absolutely and uniformly on any compact subset of $\mathrm{Re}(s) > \nu + 1$, so that it is holomorphic on $\mathrm{Re}(s) > \nu + 1$. We call $L(f, s)$ the *Dirichlet series associated with* f. For $N > 0$, we put

$$\Lambda_f(s) = \Lambda_{f,N}(s) = \left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s) L(f, s). \tag{9.80}$$

Now we can prove the *Hecke's theorem* (cf. [186], Theorem 4.3.5):

Theorem 9.30. *Take two holomorphic functions*

$$f(\tau)=\sum_{n=0}^{\infty}c_ne^{2\pi in\tau},\quad g(\tau)=\sum_{n=0}^{\infty}d_ne^{2\pi in\tau}$$

on $\mathbb{H}$ satisfying the conditions in Lemma 9.28. For positive numbers k and N, the following conditions (i) *and* (ii) *are equivalent.*

(i) *The functions f and g satisfy an equation*

$$g(\tau)=\left(-i\sqrt{N}\tau\right)^{-k}f\left(-\frac{1}{N\tau}\right).$$

(ii) *Both $\Lambda_{f,N}(s)$ and $\Lambda_{g,N}(s)$ can be analytically continued to the whole complex plane $\mathbb{C}$, satisfy the functional equation*

$$\Lambda_{f,N}(s)=\Lambda_{g,N}(k-s),$$

and

$$\Lambda_{f,N}(s)+\frac{c_0}{s}+\frac{d_0}{k-s} \tag{9.81}$$

is holomorphic on $\mathbb{C}$ and bounded on any vertical strip.

Proof. (i)⇒(ii): Note that for $\mathrm{Re}(s)>\nu+1$,

$$\begin{aligned}\Lambda_f(s) &= \sum_{n=1}^{\infty}c_n\left(\frac{2\pi n}{\sqrt{N}}\right)^{-s}\int_0^{\infty}e^{-x}x^{s-1}dx\\ &= \sum_{n=1}^{\infty}\int_0^{\infty}c_ne^{-2\pi nx/\sqrt{N}}x^{s-1}dx\\ &= \int_0^{\infty}\left(\sum_{n=1}^{\infty}c_ne^{-2\pi nx/\sqrt{N}}\right)x^{s-1}dx,\end{aligned}$$

since there there exists $\nu>0$ satisfying

$$c_n=O(n^{\nu}),\quad d_n=O(n^{\nu}),$$

so that

$$\sum_{n=1}^{\infty}|c_n|e^{-2\pi nx/\sqrt{N}}\ \ (x>0)$$

and

$$\sum_{n=1}^{\infty}|c_n|\int_0^{\infty}e^{-2\pi nx/\sqrt{N}}x^{\sigma-1}dx\ \ (\sigma>\nu+1)$$

are convergent. Thus we obtain

$$\Lambda_f(s) = \int_0^\infty \left\{ f\left(ix/\sqrt{N}\right) - c_0 \right\} x^s \frac{dx}{x}.$$

By Lemma 9.29, when x tends to ∞, we have

$$f(ix) - c_0 = O\left(e^{-2\pi x}\right), \quad g(ix) - d_0 = O\left(e^{-2\pi x}\right),$$

and hence Theorem 9.6 yields the conclusion (ii) based on the condition (i).

(ii)⇒(i): By using Mellin inverse transform, we can obtain the formula

$$e^{-x} = \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\sigma} \Gamma(s) x^{-s} ds \ \ (\sigma > 0),$$

which means

$$f(ix) = c_0 + \frac{1}{2\pi i} \sum_{n=1}^{\infty} c_n \int_{\mathrm{Re}(s)=\sigma} \Gamma(s) (2\pi n x)^{-s} ds \tag{9.82}$$

for any $\sigma > 0$. If $\alpha > \nu + 1$, then the series $L(f, s)$ is uniformly convergent and bounded on $\mathrm{Re}(s) = \alpha$, so that by Stirling's estimate

$$\Gamma(\sigma + it) \sim \sqrt{2\pi} t^{\sigma - \frac{1}{2}} e^{-\pi |t|/2} \ \ (|t| \to \infty)$$

uniformly on any vertical strip $a \le \sigma \le b$, $\Lambda_f(s)$ is absolutely integrable on $\mathrm{Re}(s) = \alpha$. Therefore, for the case $\sigma = \alpha$ we can exchange the order of summation and integration in (9.82) to get

$$f(ix) = c_0 + \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=\alpha} \Lambda_f(s) (\sqrt{N} x)^{-s} ds. \tag{9.83}$$

Furthermore we assume that $\alpha > \max\{k, \nu + 1\}$. Since $L(f, s)$ is bounded on $\mathrm{Re}(s) = \alpha$, for any $\mu > 0$ we see

$$|\Lambda_f(s)| = O\left(|\mathrm{Im}(s)|^{-\mu}\right), \ \ |\mathrm{Im}(s)| \to \infty \tag{9.84}$$

on $\mathrm{Re}(s) = \alpha$ by Stirling's estimate. Next take $\beta < 0$ so that $k - \beta > \nu + 1$. A similar argument implies that for any $\mu > 0$,

$$|\Lambda_f(s)| = |\Lambda_g(k - s)| = O\left(|\mathrm{Im}(s)|^{-\mu}\right), \ \ |\mathrm{Im}(s)| \to \infty$$

on $\mathrm{Re}(s) = \beta$. Since the function (9.81) is bounded on the region

$$\Omega = \{ s \in \mathbb{C} \mid \beta \le \mathrm{Re}(s) \le \alpha \},$$

Theorem 9.4 implies that for any $\mu > 0$, (9.84) holds uniformly on the region Ω. Further, since $\Lambda_f(s)\left(\sqrt{N}x\right)^{-s}$ has simple poles at $s = 0$ and $s = k$ with the residue

$-c_0$ and $d_0\big(\sqrt{N}x\big)^{-k}$, respectively, we can change the integral path $\mathrm{Re}(s) = \alpha$ in (9.83) to $\mathrm{Re}(s) = \beta$ and obtain

$$f(ix) = \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\beta} \Lambda_f(s)(\sqrt{N}x)^{-s}ds + d_0\big(\sqrt{N}x\big)^{-k}.$$

By the functional equation,

$$\begin{aligned} f(ix) &= d_0\big(\sqrt{N}x\big)^{-k} + \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\beta} \Lambda_g(k-s)(\sqrt{N}x)^{-s}ds \\ &= d_0\big(\sqrt{N}x\big)^{-k} + \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=k-\beta} \Lambda_g(s)(\sqrt{N}x)^{s-k}ds \\ &= \big(\sqrt{N}x\big)^{-k} g\left(\frac{i}{Nx}\right), \end{aligned}$$

which yields

$$f(\tau) = \big(-i\sqrt{N}\tau\big)^{-k} g\left(-\frac{1}{N\tau}\right),$$

since $f(\tau)$ and $g(\tau)$ are holomorphic on $\mathbb{H}$, and so the case (i) follows. □

For a positive integer N, we put

$$\gamma_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}. \tag{9.85}$$

Then

$$f_{\gamma_N,k}(\tau) = \left\{\frac{d\gamma_N(\tau)}{d\tau}\right\}^{k/2} f(\gamma_N(\tau)) = \big(\sqrt{N}\tau\big)^{-k} f\left(-\frac{1}{N\tau}\right).$$

We can restate the above theorem as follows:

Theorem 9.31. *Take two holomorphic functions*

$$f(\tau) = \sum_{n=0}^{\infty} c_n e^{2\pi i n\tau}, \quad g(\tau) = \sum_{n=0}^{\infty} d_n e^{2\pi i n\tau}$$

on $\mathbb{H}$ satisfying the conditions in Lemma 9.28. For positive numbers k and N, the following conditions (i) *and* (ii) *are equivalent.*

(i) *The functions f and g satisfy an equation*

$$f_{\gamma_N,k}(\tau) = g(\tau).$$

(ii) *Both $\Lambda_{f,N}(s)$ and $\Lambda_{g,N}(s)$ can be analytically continued to the whole complex plane $\mathbb{C}$, satisfy the functional equation*

$$\Lambda_{f,N}(s) = i^k \Lambda_{g,N}(k-s),$$

and

$$\Lambda_{f,N}(s) + \frac{c_0}{s} + \frac{i^k d_0}{k-s}$$

is holomorphic on $\mathbb{C}$ and bounded on any vertical strip.

9.5 Modular forms

9.5.1 Modular forms for $\mathrm{SL}(2,\mathbb{Z})$

Let k be an integer. An automorphic form $f \in \mathcal{M}(\mathbb{H})$ of weight $\frac{k}{2}$ for $\mathrm{SL}(2,\mathbb{Z})$ is said to be a *modular function of weight k for* $\mathrm{SL}(2,\mathbb{Z})$ if f also is meromorphic at infinity. Recall that f being meromorphic at infinity means a Fourier expansion of the form

$$f(\tau) = \sum_{n \geq m} c_n z^n = \sum_{n \geq m} c_n e^{2\pi i n \tau} \tag{9.86}$$

for some integer $m \in \mathbb{Z}$. If, in addition, f is actually holomorphic on $\mathbb{H}$ and at infinity (i.e., $m = 0$), then f is called a *modular form of weight k* for $\mathrm{SL}(2,\mathbb{Z})$. If we further have $c_0 = 0$, i.e., the modular form vanishes at infinity, then f is called a *cusp form of weight k* for $\mathrm{SL}(2,\mathbb{Z})$. See [143], [186], [210].

Take

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : \tau \longmapsto \gamma(\tau) = \frac{a\tau + b}{c\tau + d}.$$

Note that the Jacobian determinant J_γ of γ is just

$$\frac{d\gamma}{d\tau} = \frac{1}{(c\tau + d)^2}.$$

By the definition, a modular function f of weight k for $\mathrm{SL}(2,\mathbb{Z})$ satisfies

$$f_{\gamma,k}(\tau) = f(\tau), \ \ \tau \in \mathbb{H}, \tag{9.87}$$

where

$$f_{\gamma,k}(\tau) = (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right). \tag{9.88}$$

In particular, for the elements

$$\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \tag{9.89}$$

then (9.87) gives respectively

$$f(\tau+1)=f(\tau); \tag{9.90}$$

$$f\left(-\frac{1}{\tau}\right)=\tau^k f(\tau). \tag{9.91}$$

If k is odd, there are no nonzero modular functions of weight k for $\mathrm{SL}(2,\mathbb{Z})$. We see this by substituting

$$\gamma=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$

in (9.87). The sets of modular functions, forms, and cusp forms of weight k are complex vector spaces. The complex vector space of all modular (resp. cusp) forms of weight k with respect to $\mathrm{SL}(2,\mathbb{Z})$ is denoted by $\mathcal{H}_k(\mathrm{SL}(2,\mathbb{Z}))$ (resp. $\mathcal{S}_k(\mathrm{SL}(2,\mathbb{Z}))$). Since $\mathrm{SL}(2,\mathbb{Z})$ is generated by two elements (9.89), we can easily characterize an element f of $\mathcal{H}_k(\mathrm{SL}(2,\mathbb{Z}))$ by the functional equation of $L(f,s)$ and obtain

Theorem 9.32. *Let $k\geq 2$ be an even integer. Let f be a holomorphic function on $\mathbb{H}$ satisfying the conditions in Lemma 9.28. Then $f\in\mathcal{H}_k(\mathrm{SL}(2,\mathbb{Z}))$ if and only if*

$$\Lambda_f(s)=(2\pi)^{-s}\Gamma(s)L(f,s)$$

can be analytically continued to the whole s-plane,

$$\Lambda_f(s)+\frac{c_0}{s}+\frac{(-1)^{k/2}c_0}{k-s} \tag{9.92}$$

is holomorphic on $\mathbb{H}$ and bounded on any vertical strip, and satisfies the functional equation

$$\Lambda_f(s)=(-1)^{k/2}\Lambda_f(k-s). \tag{9.93}$$

Let k be an even integer with $k\geq 4$. The Eisenstein series $G_k(\tau)=G_k(\Lambda)$ of weight k for the lattice $\Lambda=[1,\tau]$ is a modular form of weight k for $\mathrm{SL}(2,\mathbb{Z})$. Its Fourier series is given by

$$G_k(\tau)=2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)e^{2\pi i n\tau}, \tag{9.94}$$

where $\sigma_{k-1}(n)$ is the *divisor function*

$$\sigma_{k-1}(n)=\sum_{d|n}d^{k-1}.$$

See [1], Theorem 1.18, 1.19, 1.20, or [237], VII Proposition 4, 5, 8.

It is obvious that $G_k(\tau)$ is holomorphic on $\mathbb{H}$, and that

$$G_k(\tau+1) = G_k(\tau).$$

We easily check that

$$\tau^{-k} G_k\left(-\frac{1}{\tau}\right) = G_k(\tau)$$

by the definition of $G_k(\tau)$, and so $G_k(\tau) \in \mathcal{H}_k(\mathrm{SL}(2,\mathbb{Z}))$. Further, the space $\mathcal{H}_k(\mathrm{SL}(2,\mathbb{Z}))$ has a basis (cf. [186], Theorem 4.1.8)

$$\{G_4(\tau)^m G_6(\tau)^n \mid 4m+6n=k;\ m,n\geq 0\},$$

which yields immediately

$$\dim \mathcal{H}_k(\mathrm{SL}(2,\mathbb{Z})) = \begin{cases} [k/12], & \text{if } k \equiv 2 \bmod 12, \\ [k/12]{+}1, & \text{if } k \not\equiv 2 \bmod 12. \end{cases} \tag{9.95}$$

Using the Fourier coefficients of (9.94), we put

$$L_k(s) = \sum_{n=1}^{\infty} \frac{\sigma_{k-1}(n)}{n^s}. \tag{9.96}$$

Then one has

$$L_k(s) = \zeta(s)\zeta(s-k+1), \tag{9.97}$$

and therefore, $L_k(s)$ is convergent on $\mathrm{Re}(s) > k$, and has an Euler product

$$L_k(s) = \prod_p \left\{ \left(1-p^{-s}\right)\left(1-p^{k-1-s}\right) \right\}^{-1}.$$

The analytic continuity and the functional equation of $\zeta(s)$ induce those of $L_k(s)$.

Related to the definition of $G_{2k}(\tau)$, here one introduces the following function

$$E(\tau,s) = \frac{1}{2\zeta(2s)} \sum_{(m,n)\in\mathbb{Z}^2-\{0\}} \frac{y^s}{|m+n\tau|^{2s}}, \quad \tau = x+iy \in \mathbb{H}. \tag{9.98}$$

This series converges absolutely and uniformly in any compact subset of the region $\mathrm{Re}(s) > 1$. Selberg [234] proved that $E(\tau,s)$ has a meromorphic continuation to the whole complex s-plane and satisfies the functional equation

$$E(\tau,s) = \frac{\xi(2s-1)}{\xi(2s)} E(\tau, 1-s). \tag{9.99}$$

For an even integer $k \geq 2$, we have (cf. [186], Corollary 4.1.4)

$$\dim \mathcal{S}_k(\mathrm{SL}(2,\mathbb{Z})) = \begin{cases} 0, & \text{if } k=2; \\ [k/12]{-}1, & \text{if } k \equiv 2 \bmod 12,\ k>2, \\ [k/12], & \text{if } k \not\equiv 2 \bmod 12. \end{cases} \tag{9.100}$$

The discriminant function $\Delta(\tau)$ is a classic cusp form of weight 12 for $\mathrm{SL}(2,\mathbb{Z})$. Its Taylor expansion in $z = e^{2\pi i\tau}$ assumes the form

$$\Delta(\tau) = (2\pi)^{12} z \prod_{n=1}^{\infty} (1-z^n)^{24} = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) z^n \tag{9.101}$$

with $\tau(n) \in \mathbb{Z}$ (see [1], Theorem 1.18, 1.19, 1.20, or [237], VII Proposition 4, 5, 8). The integer-valued function $n \mapsto \tau(n)$ is called the *Ramanujan τ-function*. Its first few values are

$$\tau(1) = 1, \ \ \tau(2) = -24, \ \ \tau(3) = 252, \ \ \tau(4) = -1472.$$

Ramanujan [213] conjectured that the coefficients $\tau(n)$ are *multiplicative*, that is,

$$\tau(mn) = \tau(m)\tau(n) \quad \text{for } m, n \text{ relatively prime;}$$

and satisfy the estimate

$$|\tau(p)| \le 2p^{11/2}$$

for every prime number p. The multiplicativity was proved by Mordell [188], in particular by the beautiful formula

$$\tau(m)\tau(n) = \sum_{d|\gcd(m,n)} d^{11} \tau\left(\frac{mn}{d^2}\right).$$

The estimate was shown by Deligne [44].

Ramanujan also conjectured that the *Hecke's L-series* associated to Δ has an *Euler product*:

$$L(\Delta, s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} = \prod_{p} \left(1 - \frac{\tau(p)}{p^s} + \frac{1}{p^{2s-11}}\right)^{-1}. \tag{9.102}$$

This was proved by Mordell [188]. Further $L(\Delta, s)$ satisfies the functional equation

$$\Lambda_\Delta(s) = \Lambda_\Delta(12-s), \tag{9.103}$$

where

$$\Lambda_\Delta(s) = (2\pi)^{-s}\Gamma(s)L(\Delta, s). \tag{9.104}$$

9.5.2 Modular forms for congruence subgroups

Let f be a meromorphic function on $\mathbb{H}$, and let $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ be a congruence subgroup of level N, i.e., $\Gamma \supseteq \Gamma(N)$. Take $k \in \mathbb{Z}$. We call f a *modular function* of weight k for Γ if

$$f_{\gamma,k}(\tau) = f(\tau), \ \ \tau \in \mathbb{H} \tag{9.105}$$

for all $\gamma \in \Gamma$, and if

$$f_{\gamma,k}(\tau) = \sum_{n \geq \mu} a_n(\gamma) e^{2\pi i n\tau/N} \tag{9.106}$$

for some integer $\mu = \mu(\gamma) \in \mathbb{Z}$ and for all $\gamma \in \mathrm{SL}(2,\mathbb{Z})$. We call such an f a *modular form* of weight k for Γ if it is holomorphic on $\mathbb{H}$ and if we have $\mu = 0$ in (9.106). We call a modular form a *cusp form* if in addition $a_0(\gamma) = 0$ in (9.106). See [133], [164].

Thus a modular function is allowed to have poles, a modular form must be holomorphic at all points including the cusps, and a cusp form must vanish at all cusps. The complex vector space of all modular (resp. cusp) forms of weight k with respect to Γ is denoted by $\mathcal{H}_k(\Gamma)$ (resp. $\mathcal{S}_k(\Gamma)$). A basic fact from the theory of modular forms is that the space of modular forms are finite dimensional. Also, one has

$$\mathcal{H}_k(\Gamma)\mathcal{H}_l(\Gamma) \subset \mathcal{H}_{k+l}(\Gamma).$$

The direct sum

$$\mathcal{H}(\Gamma) = \bigoplus_{k \geq 0} \mathcal{H}_k(\Gamma)$$

turns out to be a graded algebra over $\mathbb{C}$ with a finite number of generators.

Any cusp $x \in \mathbb{Q} \cup \{\infty\}$ can be written in the form $x = \gamma(\infty)$ for some

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

by writing $x = a/c$ for two coprime integers $a,\ c$, and finding solution b and d to the equation $ad - bc = 1$. The behavior of $f_{\gamma,k}$ near ∞ is a reflection of the behavior of f near x. Thus, the condition (9.106) is really a set of conditions, one corresponding to each cusp x of Γ.

In particular, the condition (9.105) means

$$f(\tau + N) = f(\tau),\ \ \tau \in \mathbb{H},$$

that is, f has period N. Further, if $\Gamma \supseteq \Gamma_1(N)$, then f has period 1. It is easy to show that (9.106) then implies the expression:

$$f(\tau) = \sum_{n \geq m} c_n e^{2\pi i n\tau},$$

where $c_n = a_{nN}(I)$ in which I is the unit matrix of $\mathrm{SL}(2,\mathbb{Z})$, $m = \mu/N$ if $N \mid \mu$, and $m = [\mu/N] + 1$ if $N \nmid \mu$.

Let $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ be a congruence subgroup of level N. Then $\Gamma \supseteq \Gamma(N)$ means

$$\mathcal{H}_k(\Gamma) \subseteq \mathcal{H}_k(\Gamma(N)).$$

Therefore the investigation of $\mathcal{H}_k(\Gamma)$ is reduced to that of $\mathcal{H}_k(\Gamma(N))$. Note that

$$\lambda_N^{-1}\Gamma(N)\lambda_N = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \middle| \, c \equiv 0 (\mathrm{mod}\, N^2), a \equiv d \equiv 1 (\mathrm{mod}\, N) \right\}, \tag{9.107}$$

where

$$\lambda_N = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix},$$

that is,

$$\Gamma_1\left(N^2\right) \subset \lambda_N^{-1}\Gamma(N)\lambda_N.$$

Hence, if $f \in \mathcal{H}_k(\Gamma(N))$,

$$f(N\tau) = N^{-k/2} f_{\lambda_N,k}(\tau) \in \mathcal{H}_k(\Gamma_1(N^2)).$$

Therefore the study of modular forms with respect to congruence subgroups is reduced to that of $\mathcal{H}_k(\Gamma_1(N))$.

9.5.3 Hecke operator

The study of modular forms is facilitated by the existence of certain linear operators. For each integer $m \geq 1$, we define the *Hecke operator* T_m on modular forms of weight k for $\mathrm{SL}(2,\mathbb{Z})$ by the formula

$$T_m(f)(\tau) = m^{k-1} \sum_{ad=m} \frac{1}{d^k} \sum_{b=0}^{d-1} f\left(\frac{a\tau + b}{d}\right). \tag{9.108}$$

For a more intrinsic definition, see Apostol [1], Section 6.8; Serre [237], VII, Section 5.1; or Shimura [245], Ch. 3.

The Hecke operator satisfies the following basic properties:

(g1) If f is a modular form (respectively cusp form) of weight k for $\mathrm{SL}(2,\mathbb{Z})$, then $T_n(f)$ is also.

(g2) For all integers m and n, $T_m T_n = T_n T_m$.

(g3) If m and n are relatively prime, then $T_{mn} = T_m T_n$.

See Apostol [1], Theorem 6.11 and 6.13; Serre [237], VII, Section 5.1 and 5.3.

Let f be a modular form of weight k for $\mathrm{SL}(2,\mathbb{Z})$ which can be expressed by a Fourier expansion of the form

$$f(\tau) = \sum_{n=0}^{\infty} c_n z^n, \ \ \tau \in \mathbb{H}, \tag{9.109}$$

where $z = e^{2\pi i\tau}$. One defines two operators V_m and U_m as follows:

$$V_m(f)(\tau) = \sum_{n=0}^{\infty} c_n z^{mn} = f(m\tau); \tag{9.110}$$

$$U_m(f)(\tau) = \sum_{n=0}^{\infty} c_{mn} z^n = \frac{1}{m} \sum_{i=0}^{m-1} f\left(\frac{\tau + i}{m}\right). \tag{9.111}$$

From (9.108), we obtain easily the formula:

$$T_m = \sum_{d|m} d^{k-1} U_{m/d} \circ V_d. \tag{9.112}$$

We note that

$$f\left(\frac{a\tau+b}{d}\right) = \sum_{n=0}^{\infty} c_n e^{2\pi i n(a\tau+b)/d}.$$

Then by (9.108) and the equality

$$\sum_{b=0}^{d-1} e^{2\pi i n b/d} = \begin{cases} d, & \text{if } d|n, \\ 0, & \text{if } d \nmid n, \end{cases}$$

we get

$$T_m(f)(\tau) = \sum_{n=0}^{\infty} \left(\sum_{d|\gcd(m,n)} d^{k-1} c_{mn/d^2} \right) z^n. \tag{9.113}$$

Most of the most important examples of modular forms turn out to be eigenvectors, called *eigenforms* here, for the action of all of the T_m on the given space of modular forms. If $f \in \mathcal{H}_k(\mathrm{SL}(2,\mathbb{Z}))$ is such an eigenform for all of the operators T_m with eigenvalues λ_m:

$$T_m f = \lambda_m f, \ \ m = 1, 2, \ldots.$$

Using (9.113) with $n = 1$, we find the coefficient of the first power of z in $T_m f$ is c_m. Since $T_m f = \lambda_m f$, then this coefficient is also equal to $\lambda_m c_1$. Thus we obtain

$$c_m = \lambda_m c_1, \ \ m = 1, 2, \ldots.$$

In addition, $c_1 \neq 0$ unless $k = 0$ and f is a constant. If we compare the constant terms in $T_m f = \lambda_m f$ and use (9.113) with $n = 0$, we have

$$\lambda_m c_0 = \sum_{d|m} d^{k-1} c_0.$$

If $c_0 \neq 0$, the eigenform $c_0^{-1} f$ is called *normalized*. Now we find

$$\lambda_m = \sum_{d|m} d^{k-1} = \sigma_{k-1}(m).$$

The Hecke operators defined above also act on the space of modular forms relative to congruence subgroups. We explain this case for the congruence subgroup $\Gamma_1(N)$. Let χ be a Dirichlet character modulo N. We define a *character* χ of $\Gamma_0(N)$ by

$$\chi(\gamma) = \chi(d), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \tag{9.114}$$

The complex vector space $\mathcal{H}_k(\Gamma_1(N))$ of all modular forms of weight k with respect to $\Gamma_1(N)$ has the decomposition (cf. [133], Proposition 28 in Chapter III):

$$\mathcal{H}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{H}_k(N, \chi),$$

where the sum is over all Dirichlet characters modulo N, and

$$\mathcal{H}_k(N, \chi) = \{f \in \mathcal{H}_k(\Gamma_1(N)) \mid f_{\gamma,k} = \chi(\gamma) f,\ \gamma \in \Gamma_0(N)\}.$$

In particular, if $\chi = 1$ is the trivial character, then

$$\mathcal{H}_k(N, 1) = \mathcal{H}_k(\Gamma_0(N)).$$

The Hecke operators T_m defined on $\mathcal{H}_k(N, \chi)$ can be gave by (cf. [133], Proposition 38 in Chapter III):

$$T_m = \sum_{d|m} \chi(d) d^{k-1} U_{m/d} \circ V_d, \tag{9.115}$$

which means

$$T_m(f)(\tau) = \sum_{n=0}^{\infty} \left(\sum_{d|\gcd(m,n)} \chi(d) d^{k-1} c_{mn/d^2} \right) z^n \tag{9.116}$$

for each

$$f(\tau) = \sum_{n=0}^{\infty} c_n z^n \in \mathcal{H}_k(N, \chi),\ z = e^{2\pi i \tau}.$$

Proposition 9.33. *Let Γ be a congruence subgroup of $\mathrm{SL}(2, \mathbb{Z})$, say $\Gamma \supset \Gamma(N)$ and let f be a modular form of weight k for Γ. Then for each integer $n \geq 1$ relatively prime to N, the function $T_n(f)$ is again a modular form of weight k for Γ. Further, if f is a cusp form, then so is $T_n(f)$.*

Proof. See Shimura [245], Proposition 3.37. □

We also introduce the notation $\mathcal{S}_k(N, \chi)$ to denote the subspace of cusp forms:

$$\mathcal{S}_k(N, \chi) = \mathcal{H}_k(N, \chi) \cap \mathcal{S}_k(\Gamma_1(N)).$$

One then has the following decomposition

$$\mathcal{S}_k(\Gamma_1(N)) = \bigoplus_{\chi \bmod N} \mathcal{S}_k(N, \chi).$$

For a modular form $f \in \mathcal{H}_k(N, \chi)$, the *Petersson inner product* of f with $g \in \mathcal{S}_k(N, \chi)$ is defined by the formula

$$\langle g, f \rangle_N = \int_{\mathbb{H}/\Gamma_0(N)} \overline{g(\tau)} f(\tau) y^{k-2} dx dy,$$

where $\tau = x+iy$, $\mathbb{H}/\Gamma_0(N)$ is a fixed fundamental region for $\mathbb{H}$ modulo $\Gamma_0(N)$. Then one has the following orthogonal decomposition

$$\mathcal{H}_k(N,\chi) = \mathcal{S}_k(N,\chi) \oplus \mathcal{E}_k(N,\chi),$$

where $\mathcal{E}_k(N,\chi)$ is the subspace of Eisenstein series.

A basis of $\mathcal{S}_k(N,\chi)$ consisting of eigenforms for Hecke operators can be found using the Petersson inner product. One verifies that the operators T_m on $\mathcal{S}_k(N,\chi)$ are normal with respect to this inner product for $\gcd(m,N)=1$. Moreover, the operators are χ-Hermitian: for all $f,g \in \mathcal{S}_k(N,\chi)$, the following equation holds:

$$\langle g, T_m(f)\rangle_N = \chi(m)\langle T_m(g), f\rangle_N. \tag{9.117}$$

By a general theorem of linear algebra on families of commuting normal operators, there is an orthogonal basis of $\mathcal{S}_k(N,\chi)$ consisting of eigenforms of all T_m with $\gcd(m,N)=1$ (cf. [133], Proposition 51 in Chapter III). A basis with this property is called a *Hecke basis*.

9.5.4 Hecke's *L*-series

The growth condition (9.77) is quite natural since for any $\varepsilon > 0$, we have

$$c_n = \begin{cases} O\left(n^{k-1+\varepsilon}\right), & \text{if } f \in \mathcal{H}_k(N,\chi), \\ O\left(n^{\frac{k-1}{2}+\varepsilon}\right), & \text{if } f \in \mathcal{S}_k(N,\chi). \end{cases} \tag{9.118}$$

These estimates use some fine arithmetical properties of the coefficients c_n. Especially, the estimate for the coefficients of cusp forms is famous which was known as the *Petersson–Ramanujan conjecture* before being proved by Deligne (cf. [44]) using Grothendieck's étale l-adic cohomology.

Since any element f of $\mathcal{H}_k(N,\chi)$ satisfies the conditions in Lemma 9.28, we obtain the following fact:

Theorem 9.34. *For any element $f \in \mathcal{H}_k(N,\chi)$, the function*

$$\Lambda_{f,N}(s) = \left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s) L(f,s)$$

is holomorphic on $\mathbb{C}$ and satisfies the functional equation

$$\Lambda_{f,N}(s) = i^k \Lambda_{f_{\gamma_N},k,N}(k-s).$$

The situation for $\mathcal{S}_k(\Gamma_1(N))$ is much clear. A cusp form of weight k for $\Gamma_1(N)$ is also called a *cusp form of weight k* and *level N*, which is a holomorphic function f on $\mathbb{H}$ such that by using Theorem 9.24,

(h1) $f_{\gamma,k}(\tau) = f(\tau)$ for all $\tau \in \mathbb{H}$ and all $\gamma \in \Gamma_1(N)$;

(h2) $f(\tau)\mathrm{Im}(\tau)^{k/2}$ is bounded on $\mathbb{H}$.

The space $\mathcal{S}_k(\Gamma_1(N))$ of cusp forms of weight k and level N is a finite-dimensional complex vector space. Take $f \in \mathcal{S}_k(\Gamma_1(N))$. Recall that f has a Taylor expansion in $e^{2\pi i\tau}$:

$$f(\tau) = \sum_{n=1}^{\infty} c_n e^{2\pi i n\tau},$$

which converges absolutely and uniformly on any compact subset of $\mathbb{H}$, and the *Hecke's L-series* of f is defined to be

$$L(f,s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

As a direct application of Lemma 9.28, it follows that

$$c_n = O\big(n^{\frac{k}{2}}\big).$$

If f is an eigenform such that it does not come from a space of lower level and is normalized to have $c_1 = 1$, then f is called a *newform*.

If f is a newform, it turns out that c_n are multiplicative. Hence, in the half-plane of absolute convergence, there is an Euler product representation

$$L(f,s) = \prod_{p|N} \left(1 - \frac{c_p}{p^s}\right)^{-1} \prod_{p\nmid N} \left(1 - \frac{c_p}{p^s} + \frac{1}{p^{2s-k+1}}\right)^{-1}. \tag{9.119}$$

Further, if k is even, Hecke [94], respectively, Atkin and Lehner [3] proved that $L(f,s)$ has an analytic continuation to an entire function and satisfies the functional equation

$$\Lambda_{f,N}(s) = \omega(-1)^{k/2}\Lambda_{f,N}(k-s), \tag{9.120}$$

where $\omega = \pm 1$.

9.5.5 Modular representations

For any prime $\mathfrak{p}$ over p, we let $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ denote respectively the decomposition and inertia groups of $\mathfrak{p}$. Thus

$$D_{\mathfrak{p}} = \{\sigma \mid \sigma(\mathfrak{p}) = \mathfrak{p}\},$$

and $I_{\mathfrak{p}}$ is the kernel of the reduction mapping $D_{\mathfrak{p}} \longrightarrow G_{\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p}$. This reduction mapping is surjective, and we let Frob_p denote an element of $D_{\mathfrak{p}}$ that maps to the *Frobenius* $\alpha \mapsto \alpha^p$. It is well defined up to an element of $I_{\mathfrak{p}}$ (and up to conjugation).

Let λ be a place of the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ above a rational prime ℓ and let $\overline{\mathbb{Q}}_\lambda$ denote the algebraic closure of $\mathbb{Q}_\ell$ thought of as a $\overline{\mathbb{Q}}$ algebra via λ. If $f \in$

$\mathcal{S}_k(\Gamma_1(N))$ is an eigenform, then there is a unique continuous irreducible representation

$$\rho_{f,\lambda} : G_{\overline{\mathbb{Q}}/\mathbb{Q}} \longrightarrow \mathrm{GL}(2, \overline{\mathbb{Q}}_\lambda)$$

such that for any prime $p \nmid N\ell$, $\rho_{f,\lambda}$ is unramified at p and

$$\mathrm{tr}\rho_{f,\lambda}(\mathrm{Frob}_p) = a_p(f).$$

The existence of $\rho_{f,\lambda}$ is due to Shimura [245] if $k = 2$, to Deligne [43] if $k > 2$ and to Deligne and Serre [45] if $k = 1$. Its irreducibility is due to Ribet [216] if $k > 1$ and to Deligne and Serre [45] if $k = 1$. Moreover $\rho_{f,\lambda}$ is potentially semi-stable at ℓ in the sense of Fontaine.

Let $\rho : G_{\overline{\mathbb{Q}}/\mathbb{Q}} \longrightarrow \mathrm{GL}(2, \overline{\mathbb{Q}}_\ell)$ be a continuous representation which is unramified outside finitely many primes and for which the restriction of ρ to a decomposition group at ℓ is potentially semi-stable in the sense of Fontaine. It is known by work of Carayol and others that the following two conditions are equivalent:

(i1) $\rho \sim \rho_{f,\lambda}$ for some eigenform f and some place $\lambda|\ell$;

(i2) $\rho \sim \rho_{f,\lambda}$ for some eigenform f of level $N(\rho)$ and weight $k(\rho)$ and some place $\lambda|\ell$.

In (i2), $N(\rho)$ and $k(\rho)$ are respectively the *conductor* and the *weight* of ρ. When these equivalent conditions are met we call ρ *modular*.

9.6 Hasse–Weil L-functions

We assume that E is an elliptic curve over $\mathbb{Q}$ defined by (3.58), that is,

$$y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{Z}$. By (3.59), since $A = -4a$ and $B = -4b$ satisfies

$$A^3 - 27B^2 = -16(4a^3 + 27b^2) = \Delta \neq 0,$$

the uniformization theorem shows that there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that

$$g_2 = g_2(\Lambda) = -4a, \quad g_3 = g_3(\Lambda) = -4b.$$

Hence the equation (3.58) has non-constant meromorphic solutions $x = \wp,\ y = \frac{1}{2}\wp'$.

Let κ be a number field. According to the Mordell–Weil's theorem, we can write

$$E(\kappa) = \mathbb{Z}^r \oplus E_{\mathrm{tors}}(\kappa),$$

where the *torsion subgroup* $E_{\mathrm{tors}}(\kappa)$ is finite and the *rank* r of $E(\kappa)$ is a non-negative integer. A deep theorem of Mazur [174], [175] states which finite groups can occur as torsion subgroups of elliptic curves:

Theorem 9.35. *If E is an elliptic curve, then $E_{\mathrm{tors}}(\mathbb{Q})$ is one of the following* 15 *groups:*

(A1) $\mathbb{Z}/n\mathbb{Z}$, *with* $1 \leq n \leq 10$ *or* $n = 12$,

(A2) $\mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, *with* $1 \leq m \leq 4$.

Each of the groups in Theorem 9.35 occurs infinitely often as the torsion subgroup of an elliptic curve over $\mathbb{Q}$. For an example of each possible group, see exercise 8.12 in Silverman [256]. For arbitrary number fields, there is the following result of Manin [163]:

Theorem 9.36. *Let κ be a number field and $p \in \mathbb{Z}$ a prime. There is a constant $N = N(\kappa, p)$ so that for all elliptic curves E/κ, the p-primary component of $E(\kappa)$ has order dividing p^N.*

For those torsion subgroups which are allowed in Mazur's Theorem 9.35, it is a classical result that the elliptic curves E/κ having the specified torsion subgroup all lie in a 1-parameter family. See exercise 8.13a, b in Silverman [256]. A complete list is given in Kubert [137]. Taken together, Theorem 9.35 and Theorem 9.36 provide the best evidence to date for the following longstanding conjecture (cf. Silverman [256]):

Conjecture 9.37. *Let κ be a number field. There is a constant N depending on κ so that for all elliptic curves E/κ,*

$$|E_{\mathrm{tors}}(\kappa)| \leq N.$$

The rank of $E(\mathbb{Q})$ is called the *rank* of E and is written $\mathrm{rank}(E)$. The rank of the Mordell–Weil group is much more mysterious and much more difficult to compute. There are infinitely many elliptic curves E over $\mathbb{Q}$ with $\mathrm{rank}(E) = 0$ (see [256], Corollary 6.2.1), but there are many elliptic curves E such that $\mathrm{rank}(E) \geq 1$ (see [225]). The following conjecture is referred to Lang [149], Silverman [256], or Hindry and Silverman [98]:

Conjecture 9.38. *There exist elliptic curves E over $\mathbb{Q}$ whose Mordell–Weil rank $\mathrm{rank}(E)$ is arbitrarily large.*

Fix an elliptic curve E defined by (3.58) over $\mathbb{Q}$. For every prime number p not dividing $\Delta = -16(4a^3 + 27b^2)$, we can reduce a and b modulo p and view E as an elliptic curve over the finite field $\mathbb{F}_p$. For every prime number p not dividing Δ let

$$N_p = \#E(\mathbb{F}_p) = 1 + \#\{0 \leq x, y \leq p-1 \mid y^2 \equiv x^3 + ax + b \,(\mathrm{mod}\, p)\},$$

and set

$$a_p = 1 + p - N_p.$$

H. Hasse proved the following remarkable result (cf. [91], [92], [93]):

$$-2\sqrt{p} < a_p < 2\sqrt{p}. \tag{9.121}$$

For a review of the elementary methods, see [261]. Define the *Hasse–Weil L-function* of E by

$$L(E,s) = \prod_{p\nmid\Delta}\left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} \prod_{p|\Delta} l_p(E,s)^{-1} = \sum_{n=1}^{\infty}\frac{a_n}{n^s}, \tag{9.122}$$

where $l_p(E,s)$ is of the form

$$l_p(E,s) = 1 - \frac{a_p}{p^s}$$

for some well-defined integer $a_p = 1, -1$, or 0 (cf. [150], p. 97; [256], p. 240; [270], p. 196), which is defined as follows:

$$a_p = \begin{cases} 1, & \text{if } E \text{ has split multiplicative reduction over } \mathbb{Q} \text{ at } p, \\ -1, & \text{if } E \text{ has non-split multiplicative reduction over } \mathbb{Q} \text{ at } p, \\ 0, & \text{if } E \text{ has additive reduction over } \mathbb{Q} \text{ at } p. \end{cases}$$

The coefficients a_n are constructed easily from a_p for prime p. It follows from (9.121) that $L(E,s)$ converges absolutely and uniformly on compact subsets of the complex half-plane $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 3/2\}$.

Let $N(E)$ be the *conductor* of the elliptic curve E

$$N(E) = \prod_{p} p^{f(p)} = \prod_{p|\Delta} p^{f(p)},$$

in which $f(p)$ is 0 if $p \nmid \Delta$ and ≥ 1 if $p|\Delta$ (see [150], p. 97; [256], p. 361; [270], p. 196), called the *exponent of the conductor of E at p* . In particular, $f(p) = 1$ if E has a multiplicative reduction over $\mathbb{Q}$ at p; $f(p) = 2$ if E has an additive reduction over $\mathbb{Q}$ at p with $p \geq 5$. If E has an additive reduction over $\mathbb{Q}$ at $p = 2$ or 3, the definition of $f(p)$ is more complicated, but in any case we always have $f(2) \leq 8$ and $f(3) \leq 5$.

Let $\rho_{E,\ell}$ denote the representation of $G_{\overline{\mathbb{Q}}/\mathbb{Q}}$ on the ℓ-adic Tate module of $E(\overline{\mathbb{Q}})$. The following conditions are equivalent (cf. [16]):

(B1) The L-function $L(E,s)$ of E equals the L-function $L(f,s)$ for some eigenform f.

(B2) The L-function $L(E,s)$ of E equals the L-function $L(f,s)$ for some eigenform f of weight 2 and level $N(E)$.

(B3) For some prime ℓ, the representation $\rho_{E,\ell}$ is modular.

(B4) For all primes ℓ, the representation $\rho_{E,\ell}$ is modular.

(B5) There is a non-constant holomorphic mapping $X_1(N)(\mathbb{C}) \longrightarrow E(\mathbb{C})$ for some positive integer N.

(B6) There is a non-constant morphism $X_1(N(E)) \longrightarrow E$ which is defined over $\mathbb{Q}$.

The implications (B2) $\Rightarrow$ (B1), (B4) $\Rightarrow$ (B3) and (B6) $\Rightarrow$ (B5) are tautological. The implication (B1) $\Rightarrow$ (B4) follows from the characterization of $L(E,s)$ in terms of $\rho_{E,\ell}$. The implications (B3) $\Rightarrow$ (B2) follows from a theorem of Carayol [23]. The implications (B2) $\Rightarrow$ (B6) follows from a construction of Shimura [245] and a theorem of Faltings [63]. The implications (B5) $\Rightarrow$ (B3) follows from Mazur [176]. When these equivalent conditions are satisfied we call E *modular*.

Theorem 9.39. *If E is an elliptic curve over $\mathbb{Q}$, then E is modular.*

It has become a standard conjecture that all elliptic curves over $\mathbb{Q}$ are modular. Taniyama made a suggestion along the line (B1) as one of a series of problems collected at the Tokyo-Nikko conference in September 1955. However his formulation did not make clear whether the function f defined by coefficients of $L(E,s)$ should be a cusp form or some more general automorphic form. He also suggested that constructions as in (B5) and (B6) might help attack this problem at least for some elliptic curves. In private conversations with a number of mathematicians (including Weil) in the early 1960's, Shimura suggested that assertions along the lines of (B5) and (B6) might be true (see Shimura [246] and Weil [299]). However, it only became widely known through its publication in a paper of Weil [297] in 1967, in which Weil gave conceptual evidence for the conjecture. That assertion (B1) is true for CM elliptic curves follows at once from work of Hecke and Deuring. Shimura [244] went on to check the assertion (B5) for these curves. The Shimura–Taniyama–Weil conjecture (Theorem 9.39) was finally proved by Breuil, Conrad, Diamond, and Taylor [16] by extending work of Wiles [301], Taylor and Wiles [271].

In 1985, Frey [67] made the remarkable observation that the Shimura–Taniyama–Weil conjecture should imply Fermat's last theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986, which enabled Ribet to show that the conjecture only for semistable elliptic curves implies Fermat's last theorem (see [217], [150]). However, one still needed to know that the curve in question would have to be modular, and this is accomplished by Wiles [301], Taylor and Wiles [271] via studying associated Galois representations of elliptic curves.

Theorem 9.39 implies the following long-standing conjecture of Hasse and Weil (cf. Silverman [256]): $L(E,s)$ has an analytic continuation to all of $\mathbb{C}$ and satisfies a functional equation

$$\Lambda_E(s) = w_E \Lambda_E(2-s), \tag{9.123}$$

where $w_E = \pm 1$, called the *sign of the functional equation*, and

$$\Lambda_E(s) = \left(\frac{2\pi}{\sqrt{N(E)}}\right)^{-s} \Gamma(s) L(E,s). \tag{9.124}$$

By using this fact, one can prove that the series (9.122) for $L(E,s)$ actually converges for $\mathrm{Re}(s) > \frac{5}{6}$, and in particular in a neighborhood of $s = 1$. See [28] and [197].

Goldfeld [76] proved that if there exist constants $C \in \mathbb{R}^+$ and $r \in \mathbb{R}$ such that

$$\prod_{p \le x, p \nmid \Delta} \frac{N_p}{p} \backsim C(\log x)^r,$$

then $r = \operatorname*{ord}_{s=1} L(E,s)$, the order of vanishing of $L(E,s)$ at $s = 1$, and

$$\lim_{s \to 1} \frac{L(E,s)}{(s-1)^r} = \sqrt{2} e^{r\gamma} C^{-1} \prod_{p|\Delta} l_p(E,1)^{-1},$$

where γ is Euler's constant. In particular, if $r = 0$ then

$$L(E,1) = \sqrt{2} \left(\prod_{p \nmid \Delta} \frac{N_p}{p} \times \prod_{p|\Delta} l_p(E,1) \right)^{-1}.$$

We may ask for the behavior of $L(E,s)$ near some special value of s, for example $s = 1$. The famous conjecture of Birch and Swinnerton-Dyer gives an answer. we first set some notation. The *real period* of E is the integral

$$\Omega_E = \Big| \int_{E(\mathbb{R})} \omega \Big|,$$

where ω is the invariant differential for $E/\mathbb{Q}$.

For each prime p, let $E_0(\mathbb{Q}_p)$ denote the subgroup of $E(\mathbb{Q}_p)$ that reduces to the identity component of the Néron model of E, and let c_p be the index of $E_0(\mathbb{Q}_p)$ in $E(\mathbb{Q}_p)$. In particular, $c_p = 1$ for primes of good reduction, so $c_p = 1$ for all but finitely many primes.

Note that $E(\mathbb{Q})/E_{\mathrm{tors}}(\mathbb{Q})$ is a lattice in $\mathbb{R} \otimes E(\mathbb{Q})$. By using the pairing $\langle , \rangle$ associated to the canonical height on E, we can define the *elliptic regulator of* $E/\mathbb{Q}$, denoted $R_{E/\mathbb{Q}}$, being the volume of the lattice $E(\mathbb{Q})/E_{\mathrm{tors}}(\mathbb{Q})$. In other words, choose $P_1, \ldots, P_r$ to generate $E(\mathbb{Q})/E_{\mathrm{tors}}(\mathbb{Q})$. Then

$$R_{E/\mathbb{Q}} = \sqrt{\det(\langle P_i, P_j \rangle)}.$$

If $r = 1$, we set $R_{E/\mathbb{Q}} = 1$.

Conjecture 9.40 (Birch and Swinnerton–Dyer [12]). **(1)** *$L(E,s)$ has a zero of order equal to the rank of $E(\mathbb{Q})$ at $s=1$, that is,*

$$\operatorname{rank}(E) = \operatorname*{ord}_{s=1} L(E,s).$$

(2) *Let $r = \operatorname{rank}(E)$. Then with notation as above,*

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{\#Ш(E/\mathbb{Q})R_{E/\mathbb{Q}}}{(\#E_{\mathrm{tors}}(\mathbb{Q}))^2}\Omega_E \prod_p c_p.$$

The following theorem, a combination of work of Kolyvagin [135], [136], Gross and Zagier [82], Coates and Wiles [32], and others, is the best result to date in the direction of the Birch and Swinnerton-Dyer conjecture.

Theorem 9.41. **(C1)** $\operatorname*{ord}_{s=1} L(E,s) = 0 \Longrightarrow \operatorname{rank}(E) = 0$,

(C2) $\operatorname*{ord}_{s=1} L(E,s) = 1 \Longrightarrow \operatorname{rank}(E) = 1$,

(C3) $\operatorname{rank}(E) \geq 1 \Longrightarrow \operatorname*{ord}_{s=1} L(E,s) \geq 1$.

The sign w_E in the functional equation (9.123) for $L(E,s)$ determines the parity of the integer $\operatorname{ord}_{s=1} L(E,s)$, that is, $\operatorname{ord}_{s=1} L(E,s)$ is even when $w_E = 1$, and is odd when $w_E = -1$. Thus the following *parity conjecture* is a consequence of the Birch and Swinnerton–Dyer conjecture.

Conjecture 9.42. *The integer $\operatorname{rank}(E)$ is even when $w_E = 1$, and is odd when $w_E = -1$.*

There may be many parametrization $\varphi : X_0(N(E)) \longrightarrow E$. An interesting question is to find one of the ones of smallest degree, or at least to determine its degree. The following *modular parametrization conjecture* is referred to Hindry and Silverman [98]:

Conjecture 9.43. *There is an absolute constant d such that for all elliptic curves $E/\mathbb{Q}$, there is a finite covering $\varphi : X_0(N(E)) \longrightarrow E$ such that $\deg(\varphi) \leq N(E)^d$.*

9.7 L-functions of varieties

Let κ be a number field and set $d = [\kappa : \mathbb{Q}]$. Let X be a projective variety defined over κ and let D be an ample divisor on X. For a positive integer n, set

$$a_n(X(\kappa), D) = \#\left\{x \in X(\kappa) \mid n-1 < H_D(x) \leq n\right\},$$

and consider a Dirichlet series

$$\sum_{n=1}^{\infty} \frac{a_n(X(\kappa), D)}{n^s}. \tag{9.125}$$

Let σ_0 be the abscissa of convergence of (9.125) if it exists. We define the *L-function of* $X(\kappa)$

$$L(X(\kappa), s) = \sum_{n=1}^{\infty} \frac{a_n(X(\kappa), D) n^{1-\sigma_0}}{n^s}, \tag{9.126}$$

which is holomorphic in the half plane $\mathrm{Re}(s) > 1$.

If $\#X(\kappa) < \infty$, then there are only finite many of non-zero terms in (9.125), and so it defines an entire function on $\mathbb{C}$.

Next we consider the case $\#X(\kappa) = \infty$. Without loss of generality, we assume that D is very ample. Then we have the associated dual classification mapping $\varphi_D : X \longrightarrow \mathbb{P}(V^*)$, where $V = \mathcal{L}(D)$. The *absolute* (*multiplicative*) *height* of $x \in X$ for D is defined by $H_D(x) = H(\varphi_D(x))$. Take a field extension K of κ if it is necessary such that $\varphi_D(X(\kappa)) \subseteq \mathbb{P}^N(K)$, where $N = \dim V - 1$. Thus

$$A_n = a_1(X(\kappa), D) + \cdots + a_n(X(\kappa), D) \leq n \left(\log n, \mathbb{P}^N(K)\right).$$

By Theorem 4.31, we know that the abscissa of convergence of (9.125) satisfies

$$0 \leq \sigma_0 = \limsup_{n\to\infty} \frac{\log |A_n|}{\log n} \leq (N+1)[K : \mathbb{Q}],$$

and so Theorem 9.2 means that the Dirichlet series (9.125) defines a holomorphic function of s for $\mathrm{Re}(s) > \sigma_0$ such that $s = \sigma_0$ is its singular point.

Assume that X is contained in $\mathbb{P}^N$. Then a point $x \in X(\kappa)$ has some projective coordinates $[\xi_0, \ldots, \xi_N] \in \mathbb{P}^N(\kappa)$ with $\xi_i \in \mathcal{O}_\kappa$ for each $i = 0, \ldots, N$, and so determine some ideals $(\xi_0, \ldots, \xi_N)$ of $\mathcal{O}_\kappa$. Write

$$\mathfrak{I}_{X(\kappa)} = \bigcup_{x \in X(\kappa)} \mathfrak{I}_x,$$

where

$$\mathfrak{I}_x = \{(\xi_0, \ldots, \xi_N) \mid [\xi_0, \ldots, \xi_N] = x,\ \xi_i \in \mathcal{O}_\kappa,\ 0 \leq i \leq N\},$$

and let $\bar{\mathfrak{I}}_{X(\kappa)}$ be the set consisting of all distinct ideals in $\mathfrak{I}_{X(\kappa)}$. For each function $\lambda : \bar{\mathfrak{I}}_{X(\kappa)} \longrightarrow \mathbb{Z}$, we obtain a series

$$\sum_{\mathfrak{a} \in \bar{\mathfrak{I}}_{X(\kappa)}} \frac{\lambda(\mathfrak{a})}{\mathcal{N}(\mathfrak{a})^s}.$$

In particular, the series

$$\sum_{\mathfrak{a}\in\tilde{\mathfrak{I}}_{X(\kappa)}} \frac{1}{\mathcal{N}(\mathfrak{a})^s}$$

defines a holomorphic function in the domain $\mathrm{Re}(s) > 1$.

On the other hand, for each $x \in X(\kappa)$ there exists an ideal $\mathfrak{a}_x \in \mathfrak{I}_x$ such that

$$\mathcal{N}(\mathfrak{a}_x) = \min_{\mathfrak{a}\in\mathfrak{I}_x} \mathcal{N}(\mathfrak{a}).$$

Thus for each function $\psi : X(\kappa) \longrightarrow \mathbb{Z}$, we obtain a series

$$\sum_{x\in X(\kappa)} \frac{\psi(x)}{\mathcal{N}(\mathfrak{a}_x)^s}.$$

In particular, the series

$$\sum_{x\in X(\kappa)} \frac{1}{\mathcal{N}(\mathfrak{a}_x)^s}$$

defines a holomorphic function in the domain $\mathrm{Re}(s) > 1$.

9.7.1 L-functions of $\mathbb{P}^N$

We consider the case $X = \mathbb{P}^N$ and take $D = H$ being the hyperplane in $\mathbb{P}^N$. Then

$$a_n(\mathbb{P}^N(\kappa), H) = \#\left\{x \in \mathbb{P}^N(\kappa) \mid n-1 < H(x) \le n\right\}.$$

Note that

$$A_n = a_1(\mathbb{P}^N(\kappa), H) + \cdots + a_n(\mathbb{P}^N(\kappa), H) = n\left(\log n, \mathbb{P}^N(\kappa)\right).$$

By Theorem 4.31, we obtain the abscissa of convergence

$$\sigma_0 = \limsup_{n\to\infty} \frac{\log|A_n|}{\log n} = d(N+1),$$

and so Theorem 9.2 means that the Dirichlet series (9.125) defines a holomorphic function of s for $\mathrm{Re}(s) > d(N+1)$ such that $s = d(N+1)$ is its singular point.

We define the *L-function of* $\mathbb{P}^N(\kappa)$

$$L(\mathbb{P}^N(\kappa), s) = \sum_{n=1}^{\infty} \frac{a_n(\mathbb{P}^N(\kappa), H) n^{1-d(N+1)}}{n^s}$$

which is holomorphic in the half plane $\mathrm{Re}(s) > 1$.

9.7.2 L-functions of Abelian varieties

Let A be an Abelian variety and let H_D be the height on A relative an ample divisor $D \in \mathrm{Div}(A)$. Note that

$$A_n = a_1(A(\kappa), D) + \cdots + a_n(A(\kappa), D) = n\left(\log n, A(\kappa)\right).$$

By Theorem 4.37, we obtain the abscissa of convergence

$$\sigma_0 = \limsup_{n\to\infty} \frac{\log |A_n|}{\log n} = 0,$$

and so Theorem 9.2 means that the Dirichlet series (9.125) defines a holomorphic function of s for $\mathrm{Re}(s) > 0$ such that $s = 0$ is its singular point.

We define the *L-function of $A(\kappa)$*

$$L(A(\kappa), s) = \sum_{n=1}^{\infty} \frac{a_n(A(\kappa), D)n}{n^s}$$

which is holomorphic in the half plane $\mathrm{Re}(s) > 1$.

Bibliography

[1] Apostol, T., Modular functions and Dirichlet series in number theory, Springer-Verlag, 1976.

[2] Atiyah, M. F. and Macdonald, I. G., Introduction to commutative algebra, Addison-Wesley, 1969.

[3] Atkin, A. O. L. and Lehner, J., Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970), 134–160.

[4] Baily, W. and Borel, A., Compactification of arithmetic quotients of bounded symmetric domains, Ann. of Math. 84 (1966), 442–528.

[5] Baker, A., Logarithmic forms and the abc-conjecture, Number Theory: Diophantine, Computational and Algebraic Aspects, 37–44. Györy, Kálmán et al (eds), Proceedings of the international conference (Eger, Hungary, 1996), De Gruyter, Berlin 1998.

[6] Ballico, E., Algebraic hyperbolicity of generic high degree hypersurfaces, Arch. Math. 63 (1994), 282–283.

[7] Bass, H., Connell, E. H. and Wright, D., The Jacobian conjecture: reduction of degree and formal expansion of the inverse, Bull. Amer. Math. Soc. 7 (1982), 287–330.

[8] Beckenbach, E. F. and Bellman, R., Inequalities, Springer, Berlin–Heidelberg–New York, 1971.

[9] Belyĭ, G. V., On Galois extensions of a maximal cyclotomic field, Math. USSR Izvestija 14 (1980), No. 2, 247–256.

[10] Bilu, Yu. F., Catalan's conjecture (after Mihăilescu), Séminaire Bourbaki, Exposé 909, Vol. 2002/03, Astérisque 294 (2004), 1–26.

[11] Birch, B. J., Chowla, S., M. Hall Jnr. and Schinzel, A., On the difference $x^3 - y^2$, Norske Vid. Selsk. Forh. (Trondheim) 38 (1965), 65–69.

[12] Birch, B., and Swinnerton-Dyer, H. P. F., Notes on elliptic curves. II, J. Reine Angew. Math. 218 (1965), 79–108.

[13] Bombieri, E., The Mordell conjecture revisited, Ann. Scuola Norm. Sup. Pisa Cl. Sci. 17 (1990), 615–640.

[14] Bombieri, E. and Gubler, W., Heights in Diophantine geometry, Cambridge, 2006.

[15] Bombieri, E. and Vaaler, J., On Siegel's lemma, Inv. Math. 73 (1983), 11–32; Addendum, Inv. Math. 75 (1984), p.377.

[16] Breuil, C., Conrad, B., Diamond, F. and Taylor, R., On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001), 843–939.

[17] Broberg, N., Some examples related to the abc-conjecture for algebraic number fields, Mathematics of Computation 69 (2000), no. 232, 1707–1710.

[18] Brody, R., Compact manifolds and hyperbolicity, Trans. Amer. Math. Soc. 235 (1978), 213–219.

[19] Brody, R. and Green, M., A family of smooth hyperbolic hypersurfaces in $\mathbb{P}_3$, Duke Math. J. 44 (1977), 873–874.

[20] Browkin, J. and Brzezinski, J., Some remarks on the abc-conjecture, Mathematics of Computation 62 (1994), 931–939.

[21] Bryuno, A. D., Continued fraction expansion of algebraic numbers, USSR Comput. Math. and Math. Phys 4 (1964), 1–15.

[22] Bump, D., Automorphic forms and representations, Cambridge Studies in Advanced Mathematics, Vol. 55, Cambridge University Press, Cambridge, 1997.

[23] Carayol, H., Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, Ann. Sci. Éc. Norm. Sup. 19 (1986), 409–468.

[24] Cartwright, M. L., Integral functions, Cambridge University Press, 1956.

[25] Cassels, J. W. S., An introduction to the geometry of numbers, Grundlehren der Mathematischen Wissenschaften 99, Springer-Verlag, Berlin–Göttingen–Heidelberg, 1959.

[26] Cassels, J. W. S., On the equation $a^x - b^y = 1$, II, Proc. Cambridge Philos. Soc. 56 (1960), 97–103.

[27] Catalan, E., Note extraite d'une lettre adressee a l'editeur, J. reine angew. Math. 27 (1844), p. 192.

[28] Chandrasekharan, K. and Narasimhan, R., Functional equations with multiple Gamma factors and the average of arithmetical functions, Annals of Math. 76 (1962), 93–136.

[29] Chein, E. Z., A note on the equation $x^2 = y^q + 1$, Proc. Amer. Math. Soc. 56 (1976), 83–84.

[30] Chen, W., Cartan's conjecture: defect relations for meromorphic maps from parabolic manifold to projective space, University of Notre Dame Thesis, 1987.

[31] Ciliberto, C. and Zaidenberg, M., 3-fold symmetric products of curves as hyperbolic hypersurfaces in $\mathbb{P}^4$, International J. Math. 14 (4) (2003), 413–436.

[32] Coates, J. and Wiles, A., On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39, no. 3 (1977), 223–251.

[33] Cohn, P. M., Algebraic numbers and algebraic functions, Chapman & Hall, 1991.

[34] Corvaja, P. and Zannier, U., A subspace theorem approach to integral points on curves, C. R. Acad. Sci. Paris (Ser. I, Math.) 334(4) (2002), 267–271.

[35] Corvaja, P. and Zannier, U., On a general Thue's equation, Amer. J. Math. 126 (5) (2004), 1033–1055.

[36] Corvaja, P. and Zannier, U., On integral points on surfaces, Ann. of Math. 160(2) (2004), 705–726.

[37] Danilov, L. V., Diophantine equation $x^3 - y^2 = k$ and Hall's conjecture, Mat. Zametki 32 (1982), 273–275; English translation, Math. Notes of the USSR 32 (1982), 617–618.

[38] Darmon, H. and Granville, A., On the equation $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (1995), 513–543.

[39] Davenport, H., Minkowski's inequality for the minima associated with a convex body, Quart. Journ. Math. (Oxford Ser.) 10 (1939), 119–121.

[40] Davenport, H., On $f^3(t) - g^2(t)$, Norske Vid. Selsk. Forh. (Trondheim) 38 (1965), 86–87.

[41] Davenport, H., Multiplicative number theory, Springer Verlag, G. T. M., 1974.

[42] Davies, D., A note on the limit points associatedd with the generalized abc-conjecture for $\mathbb{Z}[t]$, Colloquium Mathematicum 71 (2) (1996), 329–333.

[43] Deligne, P., Forms modulaires et représentatione ℓ-adiques, Lecture Notes in Math. 179, Springer-Verlag, 1971.

[44] Deligne, P., La conjecture de Weil, I. Pub. Math. IHES 43 (1974), 273–307; 52 (1981), 313–428.

[45] Deligne, P. and Serre, J. P., Forms modulaires de poids 1, Ann. Sci. Ec. Norm. Sup. 7 (1974), 507–530.

[46] Demailly, J.-P., Algebraic criteria for Kobayashi hyperbolic projective varieties and jet differentials, Proc. Sympos. Pure Math. 62, Part 2, Amer. Math. Soc., Providence, RI, 1997, 285–360.

[47] Demailly, J.-P. and El Goul, J., Hyperbolicity of generic surfaces of high degree in projective 3-space, Amer. J. Math. 122 (2000), 515–546.

[48] Dickson, L. E., History of the theory of numbers, Vol. 2 (Chelsea, 1966), pp. 513–520.

[49] Dirichlet, L. G. P., Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, Abhdl. Königl. Preuss. Akad. Wiss. (1837), 45–81.

[50] Dirichlet, L. G. P., Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen, S. B. Preuss. Akad. Wiss., 1842, 93–95.

[51] Dobrowolski, E., On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. 34 (1979), 391–401.

[52] Donoghue, W. F., Distributions and Fourier transforms, Academic Press, New York, 1969.

[53] Duval, J., Une sextique hyperbolique dans $\mathbf{P}^3(\mathbf{C})$, Math. Ann. 330 (2004), no. 3, 473–476.

[54] Dyson, F. J., The approximation to algebraic numbers by rationals, Acta Math. 79 (1947), 225–240.

[55] El Goul, J., Algebraic families of smooth hyperbolic surfaces of low degree in P^3_C, Manuscripta Math. 90 (1996), 521–532.

[56] Elkies, N., On $A^4 + B^4 + C^4 = D^4$, Math. Comp. 51, No. 184 (1988), 825–835.

[57] Elkies, N., ABC implies Mordell, Int. Math. Res. Not. 7 (1991), 99–109; Duke Math. J. 64 (1991).

[58] Eremenko, A. E. and Sodin, M. L., The value distribution of meromorphic functions and meromorphic curves from the point of view of potential theory, St. Petersburg Math. J. 3 (1) (1992), 109–136.

[59] Euler, L., Variae observationes circa series infinitas, Comment. Acad. Sci. Petropol 9 (1737), 160–188.

[60] Evertse, J.-H. and Ferretti, Roberto G., Diophantine inequalities on projective varieties, International Mathematics Research Notices No. 25 (2002), 1295–1330.

[61] Evertse, J.-H and Schlickewei, H. P., A quantitative version of the Absolute Subspace Theorem, J. reine angew. Math. 548 (2002), 21–127.

[62] Faltings, G., Arakelov's theorem for abelian varieties, Invent. Math. 73 (1983), 337–347.

[63] Faltings, G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), 349–366.

[64] Faltings, G., Diophantine approximation on abelian varieties, Ann. of Math. (2) 133 (1991), no. 3, 549–576.

[65] Faltings, G. and Wüstholz, G., Diophantine approximations on projective spaces, Invent. Math. 116 (1994), 109–138.

[66] Ferretti, R. G., Mumford's degree of contact and Diophantine approximations, Compositio Math. 121 no. 3 (2000), 247–262.

[67] Frey, G., Links between stable elliptic curves and certain Diophantine equations, Annales Universitatis Saraviensis, Series Mathematicae, 1 (1986), 1–40.

[68] Frey, G., Links between elliptic curves and solutions of $A - B = C$, J. Indian Math. Soc. 51 (1987), 117–145.

[69] Fujimoto, H., Value distribution theory of the Gauss map of minimal surfaces in $\mathbb{R}^m$, Aspects of Mathematics E21, Vieweg, 1993.

[70] Fujimoto, H., A family of hyperbolic hypersurfaces in the complex projective space, Complex Variables Theory Appl. 43 (2001), 273–283.

[71] Fulton, W., Algebraic curves, Benjamin, 1969.

[72] Fulton, W., Intersection theory, Springer-Verlag, 1984.

[73] Gauss, C. F., Asymptotische Gesetze der Zahlentheorie, Werke, vol. 101 (1791), 11–16, Teubner 1917.

[74] Gelfond, A. O., Transcendental and algebraic numbers (Russian), Moscow, 1952; English transl. (1969), Dover Publications, New York.

[75] Gel'fond, A. O. and Linnik, Yu. V., On Thue's method in the problem of effectiveness in quadratic fields (Russian), Doklady Akad. Nauk SSSR (N.S.) 61 (1948), 773–776.

[76] Goldfeld, D., Sur les produits partiels eulériens attachés aux courbes elliptiques, C. R. Acad. Sci.Paris Sér. I Math. 294 (1982), 471–474.

[77] Gouvêa, F. Q., p-adic numbers, Springer, 1997.

[78] Granville, A. and Stark, H. M., abc implies no "Siegel zeros" for L-functions of characters with negative discriminant, Invent. Math. 139 (2000), no. 3, 509–523.

[79] Granville, A. and Tucker, T. J., It's as easy as abc, Notices Amer. Math. Soc. 49 (2002), 1224–1231.

[80] Griffiths, P., Algebraic curves (Chinese), Beijing Univ. Press, 1981.

[81] Griffiths, P. and Harris, J., Principles of algebraic geometry, John Wiley and Sons,1978.

[82] Gross, B. H. and Zagier, D. B., Heegner points and derivatives of L-series, Invent. Math. 84 (1986), 225–320.

[83] Gundersen, G. G. and Hayman, W. K., The strength of Cartan's version of Nevanlinna theory, preprint.

[84] Hà, Huy Khóai, Hyperbolic surfaces in $\mathbf{P}^3(\mathbf{C})$, Proc. Amer. Math. Soc. 125 (1997), 3527–3532.

[85] Hadamard, J., Resolution d'une question relative aux determinants, Bull. Sci. Math. 2 (1893), 240–248.

[86] Hadamard, J., Sur les zéros de la fonction $\zeta(s)$ de Riemann, Comptes Rendus Acad. Sci. Paris 122 (1896), 1470–1473.

[87] Hadamard, J., The psychology of invention in the mathematical field, Princeton, N. J., Princeton University Press, 1949.

[88] Hall, Jr., Marshall, The diophantine equation $x^3 - y^2 = k$, in Computers in Number Theory, ed. by A. O. L. Atkin and B. J. Birch, Academic Press, London, 1971, pp. 173–198.

[89] Hardy, G. H. and Wright, E. M., An introduction to the theory of numbers, Oxford Univ. Press, London/New York, 1960, pp. 325–328.

[90] Hartshorne, R., Algebraic geometry, Springer-Verlag, 1977.

[91] Hasse, H., Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorläufige Mitteilung, Nachr. Ges. Wiss. Göttingen I, Math.-phys. Kl. Fachgr. I Math. Nr. 42 (1933), 253–262 (# 38 in H. Hasse, Mathematische Abhandlungen, Band 2, Walter de Gruyter, Berlin–New York, 1975).

[92] Hasse, H., Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Sem. Univ. Hamburg. 10 (1934), 325–348 (# 40 in H. Hasse, Mathematische Abhandlungen, Band 2, Walter de Gruyter, Berlin–New York, 1975).

[93] Hasse, H., The Riemann hypothesis in function fields, C. R. Congr. Int. Math. 1 (1937), 189–206. Philadelphia: Pennsylvania State University Press, 1989.

[94] Hecke, E., Über die Bestimmung Dirichletscher L-Reihen durch ihre Funktionalgleichung, Math. Ann. 112 (1936), 664–699.

[95] Hecke, E., Lectures on the theory of algebraic numbers, Graduate Texts in Mathematics 77, Springer-Verlag, 1981.

[96] Hecke, E., Lectures on Dirichlet series, modular functions and quadratic forms, Vandenhoeck & Ruprecht, Göttingen, 1983, Edited by Bruno Schoeneberg.

[97] Hecke, E., Mathematische Werke, 3rd ed., Vandenhoeck & Ruprecht, Göttingen, 1983.

[98] Hindry, M. and Silverman, J. H., Diophantine geometry: An introduction, GTM 201, Springer, 2000.

[99] Hironaka, H., Resolution of singularities of an algebraic variety over a field of characteristic zero, I, II, Ann. Math. 79 (1964), 109–326.

[100] Hirzebruch, F., Topological methods in algebraic geometry, Springer-Verlag, 1966.

[101] Hu, P. C., Li, P. and Yang, C. C., Unicity of meromorphic mappings, Advances in Complex Analysis and Its Applications, Kluwer Academic Publishers, 2003.

[102] Hu, P. C. and Yang, C. C., Differentiable and complex dynamics of several variables, Mathematics and Its Applications 483, Kluwer Academic Publishers, 1999.

[103] Hu, P. C. and Yang, C. C., Meromorphic functions over non-Archimedean fields, Mathematics and Its Applications 522, Kluwer Academic Publishers, 2000.

[104] Hu, P. C. and Yang, C. C., The "abc" conjecture over function fields, Proc. Japan Acad. 76, Ser. A(2000), 118–120.

[105] Hu, P. C. and Yang, C. C., Notes on a generalized abc-conjecture over function fields, Annales Mathematiques Blaise Pascal 8 (1) (2001), 61–71.

[106] Hu, P. C. and Yang, C. C., A generalized abc-conjecture over function fields, Journal of Number Theory 94 (2002), 286–298.

[107] Hu, P. C. and Yang, C. C., A note on the abc-conjecture, Communications on Pure and Applied Mathematics, Vol. LV (2002), 1089–1103.

[108] Hu, P. C. and Yang, C. C., Some progress in non-Archimedean analysis, Contemporary Mathematics Vol. 303 (2002), 37–50.

[109] Hu, P. C. and Yang, C. C., Generalized Fermat and Hall's conjectures, Methods of Complex and Clifford Analysis (Proceedings of ICAM, Hanoi, 2004).

[110] Hu, P. C. and Yang, C. C., A note on Browkin–Brzeziński conjecture, Contemporary Mathematics 384 (2005), 101–109.

[111] Hu, P. C. and Yang, C. C., Value distribution theory related to number theory, Birkhäuser, 2006.

[112] Hu, P. C. and Yang, C. C., Subspace theorems for homogeneous polynomial forms, Israel Journal of Mathematics 157 (2007), 47–61.

[113] Hu, P. C. and Yang, C. C., Hyperbolic hypersurfaces of lower degrees, Some Topics on Value Distribution and Differentiability in Complex and p-adic Analysis, edited by A. Escassut, W. Tutschke and C. C. Yang, Mathematics Monograph Series 11, Science Press, Beijing, 2008, 219–234.

[114] Iitaka, S., On D-dimensions of algebraic varieties, J. Math. Soc. Japan 23 (1971), 356–373.

[115] Iitaka, S., Logarithmic forms of algebraic varieties, J. Fac. Sci. Univ. Tokyo Sect. IA Math 23 (1976), 525–544.

[116] Iitaka, S., On logarithmic Kodaira dimension of algebraic varieties, Complex analysis and algebraic geometry, Iwanami Shoten, Tokyo, 1977, 175–189.

[117] Iitaka, S., Algebraic geometry, Grad. Texts Math. 76, Springer-Verlag, 1982.

[118] Iwaniec, H., Fourier coefficients of modular forms of half-integral weight, Invent. Math. 87 (1987), 385–401.

[119] Janusz, G. J., Algebraic Number Fields, Graduate Studies in Mathematics 7, AMS, 1996.

[120] Jung, H. W. E., Über ganze birationale Transformationen der Ebene, J. Reine Angew. Math. 184 (1942), 161–174.

[121] Kaczorowski, J. and Perelli, A., On the structure of the Selberg class, I: $0 \leq d \leq 1$, Acta Math. 182 (1999), 207–241.

[122] Kaczorowski, J. and Perelli, A., On the structure of the Selberg class, V: $1 < d < \frac{5}{3}$, Invent. Math. 150 (2002), 485–516.

[123] Karatsuba, A. A., Fundamentals of analytic number theory (Chinese), Science Press, Beijing, 1984.

[124] Karatsuba, A. A., Complex analysis in number theory, CRC Press, 1995.

[125] Kawamata, Y., On Bloch's conjecture, Invent. Math. 57 (1980), 97–100.

[126] Khintchine, A., Zur metrischen Theorie der diophantischen Approximationen, Math. Z. 24 (1926), 706–714.

[127] Kiernan, P. and Kobayashi, S., Holomorphic mappings into projective space with lacunary hyperplanes, Nagoya Math. J. 50 (1973), 199–216.

[128] Ko, C., On the Diophantine equation $x^2 = y^n + 1,\ xy \neq 0$, Sci. Sinica 14 (1964), 457–460.

[129] Kobayashi, S., Hyperbolic manifolds and holomorphic mappings, New York, Marcel Dekker, 1970.

[130] Kobayashi, S., Hyperbolic complex spaces, Springer, 1998.

[131] Kobayashi, S. and Ochiai, T., Mappings into compact complex manifolds with negative first Chern class, J. Math. Soc. Japan 23 (1971), 137–143.

[132] Kobayashi, S. and Ochiai, T., Meromorphic mappings into compact complex spaces of general type, Invent. Math. 31 (1975), 7–16.

[133] Koblitz, N., Introduction to elliptic curves and modular forms, GTM 97, Springer-Verlag, 1984.

[134] Kodaira, K., On holomorphic mappings of polydiscs into compact complex manifolds, J. Differ. Geom. 6 (1971), 33–46.

[135] Kolyvagin, V. A., Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves, Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 522–540, 670–671 (= Math. USSR - Izvestija 32 (1989), 523–541).

[136] Kolyvagin, V. A., Euler systems, in The Grothendieck Festschrift (Vol. II), P. Cartier et al., eds., Prog. in Math. 89, Birkhäuser, Boston (1990), 435–483.

[137] Kubert, D., Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc. 33 (1976), 193–237.

[138] Lander, L. and Parkin, T., Conterexamples to Euler's conjecture on sums of the powers, Bull. Amer. Math. Soc. 72 (1966), p. 1079.

[139] Lang, S., Integral points on curves, Pub. Math. IHES, 1960.

[140] Lang, S., Some theorems and conjectures in diophantine equations, Bull. Amer. Math. Soc. 66 (1960), 240–249.

[141] Lang, S., Report on Diophantine approximations, Bull. Soc. Math. France 93 (1965), 177–192.

[142] Lang, S., Higher dimensional Diophantine problems, Bull. Amer. Math. Soc. 80 (1974), 779–787.

[143] Lang, S., Introduction to modular forms, New York–Berlin–Heidelberg, Springer-Verlag, 1976.

[144] Lang, S., Fundamentals of Diophantine geometry, Springer-Verlag, New York, 1983.

[145] Lang, S., Conjectured Diophantine estimates on elliptic curves, in Arithmetic and Geometry, M. Artin and J. Tate, eds., Birkhäuser, Boston, 1983; pp. 155–172.

[146] Lang, S., Algebra, Addison–Wesley Publishing Company, Inc., 1984.

[147] Lang, S., Hyperbolic and Diophantine analysis, Bull. Amer. Math. Soc. 14 (1986), no. 2, 159–205.

[148] Lang, S., Introduction to complex hyperbolic spaces, Springer-Verlag, 1987.

[149] Lang, S., Old and new conjectured Diophantine inequalities, Bull. Amer. Math. Soc. 23 (1990), 37–75.

[150] Lang, S., Number theory III, Encyclop. Math. Sc. vol. 60 (1991), Springer-Verlag.

[151] Lang, S., Complex analysis, 4th ed., Graduate Texts in Mathematics, Vol. 103, Springer-Verlag, New York, 1999.

[152] Lang, S., Algebra, revised third edition, Springer-Verlag, New York, 2002.

[153] Langevin, M., Partie sans facteur carre d'un produit d'entiers voisins. (Square-free divisor of a product of neighbouring integers). Approximations diophantiennes et nombres transcendants, C.-R. Colloq., Luminy/ Fr. 1990, (1992), 203–214.

[154] Langevin, M., Cas d'egalite pour le theoreme de Mason et applications de la conjecture (abc). (Extremal cases for Mason's theorem and applications of the (abc) conjecture). C. R. Acad. Sci., Paris, Ser. I 317, No.5, (1993), 441–444.

[155] Lebesgue, V. A., Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, Nouv. Ann. Math. 9 (1850), 178–181.

[156] Lehmer, D. H., Factorization of certain cyclotomic functions, Ann. Math. 34(2) (1933), 461–479.

[157] Lehmer, D. H., On the Diophantine equation $x^3 + y^3 + z^3 = 1$, J. London Math. Soc. 31 (1965), 275–280.

[158] Levin, A., Generalizations of Siegel's and Picard's theorem, preprint.

[159] Liouville, J., Sur des classes très-étendues de quantités dont la irrationelles algébriques, C. R. Acad. Sci. Paris 18 (1844), 883–885 and 910–911.

[160] Maclaurin, C., A second letter to Martin Folges, Esq.; concerning the roots of equations with the demonstration of other rules in algebra, Phil. Trans. 36 (1729), 59–96.

[161] Mahler, K., Zur Approximation algebraischer Zahlen, Math. Ann. 107 (1933), 691–730.

[162] Mahler, K., An analogue to Minkowski's geometry of numbers in a field of series, Ann. Math. 42 (1941), 488–522.

[163] Manin, Ju., The p-torsion of elliptic curves is uniformly bounded, Izv. Akad. Nauk SSSR 33 (1969), AMS Transl., 433–438.

[164] Manin, Yu. I. and Panchishkin, A. A., Introduction to modern number theory, Second Edition, Springer, 2005.

[165] Mason, R. C., The hyperelliptic equation over function fields, Math. Proc. Cambridge Philos. Soc. 93 (1983), 219–230.

[166] Mason, R. C., Equations over function fields, Lecture Notes in Math. 1068 (1984), 149–157, Springer.

[167] Mason, R. C., Diophantine equations over function fields, London Math. Soc. Lecture Note Series, Vol. 96, Cambridge University Press, United Kingdom, 1984.

[168] Mason, R. C., Norm form equations I, J. Number Theory 22 (1986), 190–207.

[169] Masser, D. W., Open problems, Proc. Symp. Analytic Number Th., W. W. L. Chen (ed), London: Imperial College, 1985.

[170] Masuda, K. and Noguchi, J., A construction of hyperbolic hypersurface of $\mathbb{P}^n(\mathbb{C})$, Math. Ann. 304 (1996), 339–362.

[171] Matiyasevich, Yu. V., Enumerable sets are diophantine, Soviet Math. Dokl. 11 (1970), 354–358.

[172] Matiyasevich, Yu. V., Hilbert's tenth problem, Foundations of Computing Series, MIT Press, Cambridge, Mass., 1993.

[173] Matsumura, H., Commutative algebra, W. A. Benjamin Co., New York, 1970.

[174] Mazur, B., Modular curves and the Eisenstein ideal, Publ. Math. IHES 47 (1977), 33–186.

[175] Mazur, B., Rational isogenies of prime degree, Invent. Math. 44 (1978), 129–162.

[176] Mazur, B., Number theory as gadfly, Amer. Math. Monthly 98 (1991), 593–610.

[177] McQuillan, M., Diophantine approximations and foliations, Inst. Hautes Études Sci. Publ. Math. No. 87 (1998), 121–174.

[178] McQuillan, M., Holomorphic curves on hyperplane sections of 3-folds, Geom. Funct. Anal. 9 (1999), 370–392.

[179] Metsänkylä, T., Catalan's conjecture: another old Diophantine problem solved, Bull. Amer. Math. Soc. 41 (1) (2004), 43–57.

[180] Mihăilescu, P., A class number free criterion for Catalan's conjecture, J. Number Theory 99 (2003), 225–231.

[181] Mihăilescu, P., Primary cyclotomic units and a proof of Catalan's conjecture, preprint.

[182] Milne, J., Jacobian varieties, In Arithmetic Geometry, Cornell, Silverman, eds., Springer-Verlag, 1986, 167–212.

[183] Milovanović, G. V., Mitrinović, D. S. and Rassias, Th. M., Topics in polynomials: extremal problems, inequalities, zeros, World Scientific Publishing Co. Pte. Ltd., 1994.

[184] Minkowski, H., Diophantische approximationen, Leipzig, B. G. Teubner, 1907.

[185] Minkowski, H., Geometrie der Zahlen, Leipzig, 1910.

[186] Miyake, Toshitsune, Modular forms, Transl. from the Japanese by Yoshitaka Maeda., Berlin etc.: Springer-Verlag, 1989.

[187] Moh, T. T., Algebra, Series on University Mathematics Vol. 5, World Scientific Publishing Co. Pte. Ltd., 1992.

[188] Mordell, L. J., On Mr. Ramanujan's Empirical Expansions of Modular Functions, Proc. Cambridge Phil. Soc. 19 (1917), 117–124.

[189] Mordell, L. J., Note on the integer solutions of the equation $Ey^2 = Ax^3+Bx^2+Cx+D$, Messenger Math. 51 (1922), 169–171.

[190] Mordell, L. J., On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Cambridge Philos. Soc. 21 (1922), 179–192.

[191] Mori, S., Threefolds whose canonical bundles are not numerically effective (2), Ann. of Math. 116 (1) (1982), 133–176.

[192] Mori, S., Classification of higher dimensional varieties, Proc. of Symp. in Pure Math. AMS 46 (1987), 269–288.

[193] Mori, S. and Mukai, S., The uniruledness of the moduli space of curves of genus 11, Algebraic Geometry Conference, Tokyo–Kyoto, 1982; Lecture Notes in Mathematics, Vol. 1016, 334–353.

[194] Muir, T. and Metzler, W. H., A treatise on the theory of determinants, Dover, 1960.

[195] Mumford, D., A remark on Mordell's conjecture, Amer. J. Math. 87 (1965), 1007–1016.

[196] Mumford, D., Algebraic geometry I. Complex projective varieties, Springer-Verlag, 1976.

[197] Murty, K., Modular elliptic curves, Seminar on Fermat's Last Theorem, K. Murty, eds., AMS, 1995, 1–38.

[198] Musili, C., Algebraic geometry for beginners, Texts and Readings in Mathematics 20, Hindustan Book Agency (India), 2001.

[199] Nadel, A. M., Hyperbolic surfaces in $\mathbb{P}^3$, Duke Math. J. 58 (1989), 749–771.

[200] Nadel, A. M., The nonexistence of certain level structures on abelian varieties over complex function fields, Ann. Math. 129 (1989), 161–178.

[201] Nathanson, M. B., Elementary methods in number theory, Springer-Verlag, New York, 2000.

[202] Neukirch, J., Algebraic number theory, Science Press, Beijing, 2007.

[203] Nochka, E. I., Defect relations for meromorphic curves, Izv. Akad. Nauk. Moldav. SSR Ser. Fiz.-Teklam. Mat. Nauk 1 (1982), 41–47.

[204] Nochka, E. I., On a theorem from linear algebra, Izv. Akad. Nauk. Moldav. SSR Ser. Fiz.-Teklam. Mat. Nauk 3 (1982), 29–33.

[205] Nochka, E. I., On the theory of meromorphic curves, Dokl. Akad. Nauk SSSR 269 (1983), 377–381.

[206] Northcott, D. G., An inequality in the theory of arithmetic on algebraic varieties, Proc. Cambridge Philos. Soc. 45 (1949), 502–509.

[207] Northcott, D. G., A further inequality in the theory of arithmetic on algebraic varieties, Proc. Cambridge Philos. Soc. 45 (1949), 510–518.

[208] Northcott, D. G., Periodic points of an algebraic variety, Annals of Math. 51 (1950), 167–177.

[209] Oesterlé, J., Nouvelles approches du "theoreme" de Fermat (New approaches to Fermat's last theorem), Semin. Bourbaki, 40eme Annee, Vol. 1987/88, Exp. No.694, Asterisque 161/162 (1988), 165–186.

[210] Ogg, A., Modular forms and Dirichlet series, W. A. Benjamin, Inc., New York, 1969.

[211] Ostrowski, A., Untersuchungen zur arithmetischen Theorie der Körper, Math. Zeit. 39 (1935), 269–404.

[212] Pillai, S. S., On the equation $2^x - 3^y = 2^X + 3^Y$, Bull. Calcutta Math. Soc. 37 (1945), 15–20.

[213] Ramanujan, S., On certain arithmetical functions, Trans. Camb. Phil. Soc. 22 (1916), 159–184.

[214] Reznick, B., Patterns of dependence among powers of polynomials, in "Algorithmic and quantitative real algebraic geometry", DIMACS: Series in Discrete Mathematics and Theoretical Computer Science, Vol. 60, pp. 101–121, AMS, 2003.

[215] Ribenboim, P., The theory of classical valuations, Springer Monographs in Mathematics, Springer, 1999.

[216] Ribet, K. A., The ℓ-adic representations attached to an eigenform with Nebentypus: a survey, Lecture Notes in Math. 601, Springer-Verlag, 1977.

[217] Ribet, K. A., On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Invent. Math. 100 (1990), 431–476.

[218] Richtmyer, R., Devaney, M. and Metropolis, N., Continued fraction expansions of algebraic numbers, Numer. Math. 4 (1962), 68–84.

[219] Riemann, B., Über die Anzahl der Primzahlen unter einer gegebenen Grösse, Mon. Not. Berlin Akad (Nov. 1859), 671–680.

[220] Robert, A., Elliptic curves, Lecture Notes in Math. 326, Springer-Verlag, 1973.

[221] Rogers, K., Swinnerton-Dyer, H. P. F., The geometry of numbers over algebraic number fields, Trans. AMS 88 (1958), 227–242.

[222] Rosser, J. B., Yohe, J. M. and Schoenfeld, L., Rigorous computation and the zeros of the Riemann zeta-function, Information Processing 68 (Proc. IFIP Congress, Edinburgh, 1968), vol. 1, North-Holland, Amsterdam, 1969, pp. 70–76. Errata: Math. Comp. 29 (1975), p. 243.

[223] Roth, K. F., Rational approximations to algebraic numbers, Mathematika 2 (1955), 1–20.

[224] Ru, M., A defect relation for holomorphic curves intersecting hypersurfaces, Amer. J. Math. 126 (2004), 215–226.

[225] Rubin, K. and Silverberg, A., Ranks of elliptic curves, Bull. Amer. Math. Soc. 39 (2002), 455–474.

[226] Schanuel, S., Heights in number fields, Bull. Soc. Math. France 107 (1979), 433–449.

[227] Schlickewei, H. P., Linearformen mit algebraischen koeffizienten, Manuscripta Math. 18 (1976), 147–185.

[228] Schlickewei, H. P., On products of special linear forms with algebraic coefficients, Acta Arith. 31 (1976), 389–398.

[229] Schlickewei, H. P., The $\wp$-adic Thue–Siegel–Roth–Schmidt theorem, Archiv der Math. 29 (1977), 267–270.

[230] Schmidt, W. M., Norm form equations, Ann. of Math. 96 (1972), 526–551.

[231] Schmidt, W. M., Diophantine approximation, Lecture Notes in Math. 785 (1980), Springer.

[232] Schmidt, W. M., Diophantine approximations and Diophantine equations, Lecture Notes in Math. 1467 (1991), Springer.

[233] Schmitt, S. and Zimmer, H. G., Elliptic curves: A computational approach, de Gruyter Studies in Mathematics 31, Walter de Gruyter, Berlin, 2003.

[234] Selberg, A., Discontinuous groups and harmonic analysis, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag–Leffler, Djursholm, 1963, pp. 177–189.

[235] Selberg, A., Old and new conjectures and results about a class of Dirichlet series, Proceedings of the Amalfi Conference on Analytic Number Theory, Maiori 1989, E. Bombieri et al. (Eds.), Università di Salerno (1992), 367–385.

[236] Serre, J. P., Groupes Algébriques et Corps de Classes, Hermann, 1959.

[237] Serre, J. P., A course in arithmetic, Springer-Verlag, 1973.

[238] Serre, J. P., Lectures on the Mordell–Weil Theorem, 2nd ed., Aspects of Mathematics, Vieweg, Wiesbaden, 1990.

[239] Shafarevich, I. R., Basic algebraic geometry, Springer-Verlag, 1994.

[240] Shafarevich, I. R., On some arithmetic properties of algebraic varieties, Proceedings of the Second Asian Mathematical Conference (1995; Editors: S. Tangmanee, E. Schulz), World Scientific, 1998, 231–241.

[241] Shiffman, B., Holomorphic curves in algebraic manifolds, Bull. Amer. Math. Soc. 83 (1977), 553–568.

[242] Shiffman, B. and Zaidenberg, M., Two classes of hyperbolic surfaces in $\mathbb{P}^3$, International J. Math. 11 (1) (2000), 65–101.

[243] Shiffman, B. and Zaidenberg, M., Hyperbolic hypersurfaces in $\mathbb{P}^n$ of Fermat–Waring type, Proc. Amer. Math. Soc. 130 (2002), 2031–2035.

[244] Shimura, G., On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields, Nagoya Math. J. 43 (1971), 199–208.

[245] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Princeton Univ. Press, Princeton, 1971.

[246] Shimura, G., Response to 1996 Steele Prize, Notes of the AMS 43 (1996), 1344–1347.

[247] Shirosaki, M., Hyperbolic hypersurfaces in the complex projective spaces of low dimensions, Kodai Math. J. 23 (2000), 224–233.

[248] Shirosaki, M., A hyperbolic hypersurface of degree 10, Kodai Math. J. 23 (2000), 376–379.

[249] Siegel, C. L., Approximation algebraischer Zahlen, Math. Z. 10 (1921), 173–213.

[250] Siegel, C. L., The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. London Math. Soc. 1 (1926), 66–68.

[251] Siegel, C. L., Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. d. Wiss., Math. Phys. Kl., Nr. 1 = Ges. Abh. I (1929), 209–266.

[252] Siegel, C. L., Topics in complex function theory, Vol. I, Elliptic functions and uniformization theory, John Wiley & Sons Inc., 1969.

[253] Siegel, C. L., Topics in complex function theory, Vol. II, Automorphic functions and Abelian integrals, John Wiley & Sons Inc., 1971.

[254] Siegel, C. L., Topics in complex function theory, Vol. III, Abelian functions and modular functions of several variables, John Wiley & Sons Inc., 1973.

[255] Silverman, J. H., Lower bounds for height functions, Duke Math. J. 51 (2) (1984), 395–403.

[256] Silverman, J. H., The arithmetic of elliptic curves, Springer-Verlag, 1986.

[257] Siu, Y. T. and Yeung, S. K., Defects for ample divisors of Abelian varieties, Schwarz lemma, and hyperbolic hypersurfaces of low degrees, Amer. J. Math. 119 (1997), 1139–1172.

[258] Siu, Y. T. and Yeung, S. K., Addendum to "Defects for ample divisors of Abelian varieties, Schwarz lemma, and hyperbolic hypersurfaces of low degrees", Amer. J. Math. 125 (2003), 441–448.

[259] Smyth, C. J., On the product of the conjugates outside the unit circle of an algebraic integer, Bull. London Math. Soc. 3 (1971), 169–175.

[260] Song, X. J. and Tucker, T. J., Dirichlet's theorem, Vojta's inequality, and Vojta's conjecture, Compositio Math. 116 (2) (1999), 219–238.

[261] Stepanov, S. A., Arithmetic of algebraic curves, Monographs in Contemporary Mathematics, New York: Consultants Bureau, 1994.

[262] Steuding, J., Value-distribution of L-functions, Lecture Notes in Mathematics 1877, Springer, 2007.

[263] Stewart, C. L. and Tijdeman, R., On the Oesterlé–Masser conjecture, Monatsh. Math. 102 (1986), 251–257.

[264] Stewart, C. L. and Yu, Kunrui, On the abc conjecture, Math. Ann. 291(2) (1991), 225–230.

[265] Stewart, C. L. and Yu, Kunrui, On the abc conjecture. II, Duke Math. J. 108 (1) (2001), 169–181.

[266] Stewart, Ian and Tall, David, Algebraic number theory and Fermat's last theorem, A K Peters, Ltd., Natick, Massachusetts, 2002.

[267] Stoll, W., Value distribution theory of meromorphic maps, Aspects of Math. E 7 (1985), pp. 347, Vieweg-Verlag.

[268] Stothers, W. W., Polynomial identities and Hauptmoduln, Quart. J. Math. Oxford Ser. (2) 32 (1981), no. 127, 349–370.

[269] Study, E., Kürzeste Wege im komplexen Gebiete, Math. Ann. 60 (1905), 321–377.

[270] Tate, J. T., The arithmetic of elliptic curves, Invent. Math. 23 (1974), 179–206.

[271] Taylor, R. and Wiles, A., Ring-theoretic properties of certain Hecke algebras, Ann. of Math. 141 (1995), 553–572.

[272] Thue, A., Über Annäherungswerte algebraischer Zahlen, J. reine angew. Math. 135 (1909), 284–305.

[273] Thue, A., Selected mathematical papers, Edited by T. Nagell, A. Selberg, S. Selberg, K. Thalberg, Universitetsforlaget Oslo-Bergen-Troms∅, 1977.

[274] Tijdeman, R., On the equation of Catalan, Acta Arith. 29 (1976), 197–209.

[275] Tijdeman, R., In Number Theory and Applications, ed. by R. A. Mollin, Kluwer, 1989, p.234.

[276] Titchmarsh, E. C., The theory of functions, 2nd edition, Oxford, 1939.

[277] Totaro, B., Proof of a conjecture of Lang, preprint, 1986.

[278] Ueno, K., Classification of algebraic varieties I, Comp. Math. 27 (1973), 277–342.

[279] Ueno, K., Classification theory of algebraic varieties and compact complex spaces, Lecture Notes in Math. 439, Springer, 1975.

[280] Vallée–Poussin, C. J. de la, Recherches analytiques sur la théorie des nombres premiers, I–III, Ann. Soc. Sci. Bruxelles 20 (1896), 183–256, 281–362, 363–397.

[281] van der Poorten, A. J., Additive relations in number fields, Seminar on number theory, Paris 1982–83, 259–266, Progr. Math. 51, Birkhäuser Boston, Boston, MA, 1984.

[282] Van der Waerden, B. L., Algebra, Vol. 2, 7-th ed., Springer-Verlag, 1991.

[283] van Frankenhuysen, M., Hyperbolic spaces and the abc conjecture, Katholieke Universiteit Nijmegen, Thesis, 1995.

[284] van Frankenhuysen, M., The abc conjecture implies Roth's theorem and Mordell's conjecture, Math. Contemporanea 16 (1999), 45–72.

[285] van Frankenhuysen, M., A lower bound in the ABC conjecture, J. Number Theory 82 (2000), 91–95.

[286] van Frankenhuysen, M., The abc conjecture implies Vojta's height inequality for curves, J. Number Theory 95 (2002), no. 2, 289–302.

[287] Vojta, P., Diophantine approximation and value distribution theory, Lecture Notes in Math. 1239, Springer, 1987.

[288] Vojta, P., Arithmetic discriminants and quadratic points on curves, In Arithmetic algebraic geometry (Texel, 1989), volume 89 of Progr. Math., pages 359–376, Birkhäuser Boston, Boston, MA, 1991.

[289] Vojta, P., Siegel's theorem in the compact case, Annals of Math. 133 (1991), 509–548.

[290] Vojta, P., A generalization of theorems of Faltings and Thue–Siegel–Roth–Wirsing, J. Amer. Math. Soc. 5(4) (1992), 763–804.

[291] Vojta, P., Integral points on subvarieties of semi-Abelian varieties, Invent. Math. 126 (1996), 133–181.

[292] Vojta, P., On Cartan's theorem and Cartan's conjecture, Amer. J. Math. 119 (1997), 1–17.

[293] Vojta, P., A more general abc conjecture, International Mathematics Research Notices 1998 (1998), 1103–1116.

[294] Vojta, P., On the ABC conjecture and Diophantine approximation by rational points, Amer. J. Math. 122 (2000), 843–872.

[295] Vojta, P., Diagonal quadratic forms and Hilbert's Tenth Problem, Contemporary Mathematics 270 (2000), 261–274.

[296] Voutier, P., An effective lower bound for the height of algebraic numbers, Acta. Arith. 74 (1996), no. 1, 81–95.

[297] Weil, A., Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann. 168 (1967), 149–156.

[298] Weil, A., Basic number theory, Berlin-Heidelberg-New York, Springer, 1973.

[299] Weil, A., Scientific works. Collected papers. III (1964–1978), Springer-Verlag, 1979.

[300] Weil, A., Number theory, an approach through history, Birkhäuser, Boston, 1984.

[301] Wiles, A., Modular elliptic curves and Fermat's Last Theorem, Ann. of Math. 141 (1995), 443–551.

[302] Wu, H., The equidistribution theory of holomorphic curves, Princeton University Press, Princeton, New Jersey, 1970.

[303] Ye, Z., The Nevanlinna functions of the Riemann zeta-function, J. Math. Analysis Appl. 233 (1999), 425–435.

[304] Zagier, D., Algebraic numbers close to both 0 and 1, Math. Computation 61 (1993), 485–491.

[305] Zaidenberg, M., Stability of hyperbolic embeddedness and construction of examples, Math. USSR-Sb. 63 (1989), 351–361.

[306] Zannier, U., Some remarks on the S-unit equation in function fields, Acta Arithmetica LXIV.1 (1993), 87–98.

[307] Zariski, O. and Samuel, P., Commutative algebra (Vol. I, II), Van Nostrand, Princeton (1958, 1960).

[308] Zhang, S., Positive line bundles on arithmetic surfaces, Ann. of Math. 136 (1992), 569–587.

Symbols

$|$, 9, 22, 22, 61, 83
$\ll$, 309
$\#$, 145
$D \sim D'$, 169
$\angle$, 131
r^+, 332
r^-, 332
$r^\vee$, 135
$|\mathbf{i}|$, 250
$|\xi|_{*,v}$, 240, 332
$\|\xi\|_v$, 103, 133
$|||\xi|||_v$, 106, 133
$|x, a|_v$, 133
$\|x, a\|_v$, 133
$|||x, a|||_v$, 133
$\binom{i}{j}$, 136
(f), 168, 227
$[x]$, 195
$\lceil r \rceil$, 347
$\partial_{\mathbf{i}} f$, 250
$\otimes_m V$, 144
$\bigwedge_k V$, 130
$\amalg_m V$, 144
$\mathbb{A}^n$, 150
A_{tors}, 167
$\mathcal{A}(M)$, 464
$\mathcal{A}^*(M)$, 464
$A[n]$, 167
$A[O; r]$, 263, 273
A_{red}, 12
$\mathrm{Ann}(\mathfrak{b})$, 12, 210
$\mathrm{Aut}(M)$, 158, 464
$\mathbb{C}$, 1
$\mathrm{CaDiv}(X)$, 169
$\mathrm{char}(\kappa)$, 43
$\mathrm{Cl}(D)$, 169
$\mathrm{Cl}(X)$, 169, 227
$\mathrm{codim}(Y)$, 160
$\mathrm{Coker}(\varphi)$, 200
$d_{K/\kappa}$, 293
$d_{K/\kappa,S}$, 293
$D_{K/\kappa}$, 52, 110
$\mathfrak{D}_{K/\kappa}$, 90
$\mathfrak{d}_{K/\kappa}$, 125, 85
D_{red}, 167
$\deg(\mathbf{D})$, 228, 287, 289
$\deg_v(\mathbf{D})$, 287
$\deg(f)$, 35, 312
$\deg^{(1)}(f)$, 304
$\deg^{(k)}(f)$, 312
$\deg_{X_h}(f)$, 250
$\dim(X)$, 153, 160, 175
$\mathrm{Div}(X)$, 167, 169, 226
$\mathrm{Div}^0(X)$, 172
$\mathrm{dom}(\varphi)$, 159
$e_{\mathfrak{P}/\mathfrak{p}}$, 46
$E[a]$, 130
$E^d[a]$, 147
$\ddot{E}[a]$, 130
$\ddot{E}^d[a]$, 147
$f_{\mathfrak{P}/\mathfrak{p}}$, 46
$\mathbb{F}_p$, 26, 66, 106
$\mathbb{F}_v(\kappa)$, 26
$\mathcal{F}(Y, \bar{\kappa})$, 151
$\gcd(a_0, \ldots, a_n)$, 312
$G_{K/\kappa}$, 45
$\mathrm{GL}(2, A)$, 459
$h(\xi)$, 240, 284

$h_D(x)$, 265, 266, 271
$h_*(\xi)$, 240, 251
$h_\vee(f)$, 252
$\hbar_D(x)$, 278, 290
$\hbar_{D,f}(x)$, 294
$\hbar_{D,\mathcal{X}}(x)$, 283, 288
$\hbar_{\mathcal{L},\mathcal{X},S}(x)$, 289
$\mathbb{H}$, 437, 460, 468
$\mathbb{H}^*$, 462
$H(\xi)$, 240, 251
$H_D(x)$, 265
$H_\kappa(\xi)$, 239, 251
$H_*(\xi)$, 240, 251
$H_{*,\kappa}(\xi)$, 240
$H_\vee(f)$, 252
$H_{\vee,\kappa}(f)$, 251
$\mathcal{H}_k(\Gamma)$, 466, 476, 479
$I(Y)$, 150, 155
$\mathfrak{I}_A$, 19, 30, 73
$\mathrm{Im}(\varphi)$, 200
$\mathrm{Ind}(P)$, 335
J_a^b, 131
$J_{1,a}^b$, 384
$J_{n,d}$, 145
$J_l(\mathscr{A})$, 141
$J(P)$, 98
$\mathrm{Jac}(C)$, 196
$\mathcal{J}_d$, 144
K_X, 171
$[K:\kappa]$, 36
$[K:\kappa]_s$, 42
$\mathrm{Ker}(\varphi)$, 30, 200
$\ell(D)$, 173
$\mathcal{L}(D)$, 173
$\mathrm{length}(M)$, 209, 211
$\log^+ r$, 282
$m(x,D)$, 280, 282
$m(x,a)$, 281
$\mathbf{m}_{\kappa,v}$, 26
$\mathcal{M}(M)$, 464
M_κ, 61, 105
M_κ^0, 24
M_κ^∞, 61, 105
$\mathbb{M}_\kappa$, 286
$\tilde{M}$, 224
$\mathfrak{M}_k(\Gamma)$, 465
$\mathscr{M}_k(\Gamma)$, 466
$\mathrm{Mah}(f)$, 255
$n_\nu(t)$, 263, 273
$n(r, A(\kappa))$, 263, 273
$N(x,D)$, 280, 282
$N(x,a)$, 281
$N_m(x,D)$, 292
$N_\nu(r)$, 263, 273
$\mathbf{N}_{K/\kappa}$, 48
$\overline{N}(x,D)$, 292
$\mathcal{N}(\mathfrak{a})$, 99, 112
$o(1)$, 245
$O(1)$, 276, 245
$\mathcal{O}(X)$, 157, 157
$\mathcal{O}_X(x)$, 157, 157
$\mathcal{O}_\kappa$, 91
$\mathcal{O}_{\kappa,S}$, 379, 392
$\mathrm{ord}(z)$, 28
$\mathrm{ord}_Y(f)$, 168, 168
$\wp$, 467
$\mathbb{P}(A)$, 130
$\mathbb{P}_A^n$, 218, 223
$\mathrm{Pic}(X)$, 169
$\mathrm{Pic}^0(X)$, 172
$\mathrm{Proj}\ S$, 217
$\mathbb{Q}$, 1
$\mathbb{Q}_p$, 57
$\bar{\mathbb{Q}}$, 91
$r(x)$, 306
$r_k(x)$, 313
$R_{K/\kappa}$, 292
$\mathbb{R}$, 1
$\mathcal{S}_k(\Gamma)$, 466, 476, 479
$\mathfrak{Sch}(S)$, 218
$\mathrm{SL}(2,A)$, 459
$\mathrm{SL}(2,\mathbb{Z})$, 461
$\mathrm{Sp}_{\mathrm{alg}}(M)$, 418
$\mathrm{Spec}A$, 212

$\mathrm{supp}(D)$, 167
$\mathbf{Tr}_{K/\kappa}$, 48
$\mathfrak{Var}(\kappa)$, 218
$V_{[d]}$, 146
$X_0(N)$, 464
$X_1(N)$, 464
X_{red}, 220
X^{sch}, 219
$\mathbb{Z}$, 1
$\bar{\mathbb{Z}}$, 91
$Z(S)$, 150
$\Gamma(N)$, 461
$\Gamma_0(N)$, 461
$\Gamma_1(N)$, 461
$\Gamma(X, \mathcal{F})$, 199
δ_{ij}, 50
$\kappa(\alpha)$, 36, 152, 155, 156
$\kappa[\alpha]$, 36, 151
κ^+, 1
κ_+, 1
κ_*, 24
$\kappa_{\mathbb{A}}$, 368
$\kappa_{\mathbb{R}}$, 333, 370
κ_v, 61, 274
$\overline{\kappa}$, 43
$\varkappa$, 123
λ_D, 275
$\lambda_{D,v}$, 274
$\mu_{C_0}(p)$, 178
$\mu_f^0(p)$, 178
$\xi^{\amalg m}$, 145
$\varsigma_{v,r}$, 136
φ_D, 174
φ_L, 174
$\chi(C)$, 183
$\chi_\kappa(x)$, 263, 273
$\chi_v(x, a)$, 135
$\Omega_{B/A}$, 20, 224
$\Omega^r[X]$, 164, 164
$\Omega^r(X)$, 165

Index

$(1,1)$-form conjecture, 431

A

$\mathfrak{a}$-adic completion, 18
$\mathfrak{a}$-adic topology, 18
$\mathfrak{a}$-topology, 18
abc-conjecture, 306, 313
abc-point, 318
abc-theorem, 306
Abelian variety, 166
abscissa of convergence, 435
absolute discriminant, 293
absolute height, 240, 252, 264
absolute heights, 251
absolute value, 55
abstract curve, 227
abstract differential form, 163, 164
abstract variety, 223
additive M_κ-constant, 274
additive reduction, 194
adèle ring, 368
admissible, 147
affine n-space, 150
affine algebraic variety, 150
affine bounded, 274
affine coordinate ring, 151
affine curve, 151
affine dimension theorem, 161
affine scheme, 215
affine variety, 150
algebraic, 36, 91
algebraic closure, 37
algebraic extension, 40
algebraic group, 165
algebraic integer, 91
algebraic point, 155
algebraic set, 150, 154
algebraic special set, 418
algebraically equivalent, 172
algebraically hyperbolic, 419
ample, 175
annihilator, 12, 210
anti-symmetrizer, 139
antisymmetric divisor, 296
Apostol, 467, 480
approximation theorem, 56, 370
Arakelov degree, 289
Arakelov divisor, 286
Archimedean, 56
Archimedean property, 6
arithmetic progression, 452
arithmetic scheme, 286
ascending chain condition, 14
associated divisor, 288
associated line bundle, 207
associated sheaf, 199
associated vector space, 173
Atiyah, 13, 15, 18, 28, 35, 153
Atkin, 484
automorphic form, 464, 475
automorphic function, 464
automorphism, 41, 158, 464

B

Büchi, 420
bad reduction, 194, 283
Baily, 231
Baker, 307
Ballico, 419
base extension, 222

base point, 173
base point free, 173
base scheme, 222
basepoint, 187
basis, 2
Belyĭ, 305
Bergman metric, 231
Bernoulli number, 440
Bernoulli polynomial, 440, 449
birational mapping, 159
birationally equivalent, 159
Birch, 490
Bombieri, 416, 419
Bombieri-Lang conjecture, 419
Borel, 231
bounded, 275
bounded from above, 275
bounded from below, 275
branch point, 228
Breuil, 488
Brody, 231, 238
Brody hyperbolic, 231
Browkin, 313, 315
Bryuno, 328
Brzeziński, 313, 315

C
canonical, 176
canonical class, 171
canonical divisor, 171
canonical extension, 35
canonical height, 294, 297, 299
canonical set, 106
Carayol, 488
cardinality, 145
Cartier divisor, 169
Cassels, 124, 324
Catalan, 323
Catalan's conjecture, 323
Catalan's equation, 323
ceiling, 347
center, 263, 273
chain, 9
character, 481
characteristic function, 263, 273
Chebyshev's function, 442
Chein, 323
Chen, 142
Chevalley, 430
Chinese remainder theorem, 370
Chow's lemma, 223
Ciliberto, 238
class number, 117
closed, 223
closed immersion, 220
closed point, 213, 219
closed subscheme, 220
coboundary, 8
cocycle, 8
codimension, 160
codimension one, 226
Cohen–Macaulay ring, 13
coherent, 224
coherent sequence, 17
Cohn, 45
cohomologous, 8
cohomology group, 8
cokernel, 200
combinatorial lemma, 337
compactified divisor, 286
compatible, 276
complete, 17, 56, 156, 223
complete intersection, 161
complete linear system, 173
complete multiplicative, 445
completed zeta function, 437
completion, 16, 57
conductor, 128, 444, 485, 487
congruence subgroup, 461
conjugate, 37, 39
connected scheme, 219
conorm mapping, 83
Conrad, 488
constant sheaf, 198

content of polynomial, 98
continuous, 275
convex body, 114, 124, 360
convex set, 114, 360
coprime, 11
Corvaja, 405, 406, 408, 412, 424
cotangent bundle, 206
cotangent space, 162
counting function, 273
counting norm, 99
Crelle, 323
critical strip, 441, 450
curve, 161
cusp, 188, 460, 462
cusp form, 475, 479, 483

D
D-dimension, 175
Danilov, 311
Davenport, 124
Davenport's theorem, 316
Davenport-Estermann theorem, 374
decomposable, 15
decomposition group, 108, 484
Dedekind domain, 28, 91
degree, 36, 151, 155, 160, 166, 181, 211, 216, 227, 228, 289, 431, 457
degree of divisor, 287
Deligne, 483, 485
Demailly, 238
dense, 27
dependent, 56
depth, 13
derivation, 19
descending chain condition, 152
determinant bundle, 203
Deuring, 488
Devaney, 328
diagonal morphism, 222
Diamond, 488
different, 84, 85
differential, 163
dimension, 10, 153, 155, 160, 161, 173, 175, 221
Diophantine, 306
direct image, 201
direct sum, 203
Dirichlet, 328, 452
Dirichlet character, 443, 444
Dirichlet series, 434, 471
Dirichlet's L-function, 446
Dirichlet's unit theorem, 121
discrete, 27, 112
discrete valuation ring, 27
discriminant, 52, 84, 90, 110, 188
distance, 133
distance function, 58, 124, 360
divide, 61, 83
divides, 9
divisible, 22
divisor, 73, 168, 171, 183, 227
divisor class group, 77, 169, 227
divisor function, 476
divisor group, 73
Dobrowolski, 247
domain, 9
domain of definition, 159
domain of regularity, 165
dominant, 159
double, 178
double point, 178
dual, 84, 203
dual classification mapping, 174
Duval, 238
Dyson, 328

E
effective, 167, 169, 226
eigenform, 481
Eisenstein polynomial, 89
Eisenstein series, 467
El Goul, 238
elementary mapping, 158

Elkies, 327, 418
elliptic, 415, 460
elliptic curve, 186
elliptic function, 466
elliptic integral, 467
elliptic modular function, 469
elliptic modular group, 461
elliptic point, 460
elliptic regulator, 489
embedding, 41
entire, 9
equivalent, 17, 24, 30, 56, 58, 461
Erdös, 307
Eremenko, 147
étale morphism, 226
Euler, 323, 327, 436
Euler characteristic, 183
Euler formulae, 128
Euler product, 478
Euler's φ-function, 443
Euler's constant, 441
Euler's theorem, 443
even character, 445
Evertse, 392
exact, 200
exponent, 447
exponent of conductor, 487
exponent of convergence, 436
extension, 60
extension field, 36
exterior power, 203
exterior product, 130

F
factorial, 9
factorization theorem, 28
Faltings, 415, 419, 431, 488
family of schemes, 222
Fermat, 326, 327
Fermat's conjecture, 323
Fermat's equation, 323
Fermat–Catalan conjecture, 324
fibre, 222
fibred product, 221
field, 9
field of fractions, 9
filtration, 209, 210
finite extension, 36
finite group, 1
finite length, 209
finite morphism, 159, 220
finite place, 61
finite prime, 61
finite type, 220
finitely generated, 40
first exact sequence, 20
first main theorem, 281, 404
first minimum, 123
fixed component, 174
fixed field, 45
fixed point, 460
flat, 223
Fontaine, 485
form, 155
forward orbit, 294
fractional ideal, 18
fractional linear transformation, 459
frame, 205
free, 134
Frey, 306, 310, 488
Frobenius, 484
Fubini–Study metric, 291
Fuchsian group, 464
Fujimoto, 143, 238
Fulton, 170, 177, 181, 183
function field, 152, 156, 226
fundamental mesh, 113
fundamental region, 461
fundamental units, 122

G
Galois extension, 45
Galois group, 45
Γ-equivalent, 461

Γ-function, 437
gauge, 134, 137, 140, 143, 148, 149
Gauss, 442
Gauss norm, 251
Gauss sum, 445, 447
Gauss' theorem, 34, 92
Gaussian extension, 35
Gelfand's inequality, 258
Gelfond, 328
general distance function, 360
general linear group, 459
general position, 141, 147
general type, 176
generalized Fermat–Catalan equation, 324
generalized inverse, 12, 18
generalized Riemann hypothesis, 451
generalized Szpiro conjecture, 309
generalized Wronskian determinant, 341
generic fibre, 222
generic point, 213, 216, 219, 222
generically finite, 222
genus, 181
geometric point, 219
geometrically regular of dimension n, 225
germ, 199
global field, 283
global section, 199
Goldfeld, 489
good reduction, 194, 283
graded module, 210
graded ring, 154, 216
Granville, 451
greatest common divisor, 9, 22, 95, 312
Green, 238
Green function, 287
Griffiths, 176
group of ideals, 30
group of units, 30, 77

H
Hà, 238
Haar measure, 366, 369
Hadamard, 442
Hadamard's determinant inequality, 140
Hadamard's factorization theorem, 436
Hall, 311, 317
Hall's conjecture, 311
Hartshorne, 14, 153, 159, 161, 163, 170, 173, 175, 177, 181, 199, 202, 206, 214, 217, 220, 222, 223, 225, 226
Hasse, 487, 488
Hasse-Weil L-function, 487
Hecke, 98, 117, 120, 123, 125, 435, 484, 488
Hecke basis, 483
Hecke operator, 480
Hecke's L-series, 478, 484
Hecke's theorem, 471
height, 10, 239, 240, 251, 265, 283, 288, 289, 491
Hensel, 57
Hensel's lemma, 36
Henselian, 35, 61
Hermitian metric, 135, 229
Hermitian product, 135
Hermitian vector space, 135
Hilbert, 13, 34, 185, 420
Hilbert basis theorem, 13
Hilbert polynomial, 211
Hilbert's Nullstellensatz, 34
Hindry, 160, 161, 163, 168, 169, 172, 173, 175, 177, 183, 325, 486, 490
Hironaka, 176
Hirzebruch, 234
holomorphic, 463, 466
holomorphic chain, 230
holomorphic differential, 231
holomorphic special set, 231, 419
homogeneous coordinate ring, 155, 211

homogeneous coordinates, 134
homogeneous element, 154, 216
homogeneous function field, 155
homogeneous ideal, 154, 155, 211, 216
horizontal divisor, 284
Hu, 143, 313, 405, 406
Hurwitz, 185
Hurwitz formula, 171
hyperbolic, 230, 460
hyperbolic modulo a subset, 231
hyperbolic point, 460
hyperelliptic, 194
hyperplane, 130, 155
hypersurface, 147, 151

I
ideal, 9
ideal basis, 92
ideal class, 30
ideal class group, 30
ideal of set, 150
ideal sheaf, 224
identity element, 165
Iitaka, 176
image, 9, 200
index, 2
index of polynomial, 335
inertia group, 108, 484
inertial degree, 46, 67
infinite extension, 36
infinite group, 1
infinite place, 61
infinite prime, 61
injective, 200
inner product, 130
inseparable, 43
integral, 21, 22
integral closure, 22
integral divisor, 73
integral domain, 9
integral ideal, 19
integral scheme, 220
integralizable point, 280
integrally closed, 22
interior product, 131
intersect number, 179
intersect properly, 179
intersection multiplicity, 212
intersection of ideals, 11
invariant differential, 188
invariant field, 45
inverse image, 201
inverse limit, 17
inverse system, 17
invertible, 12, 19
invertible sheaf, 201
irreducible, 9, 14, 150
irreducible component, 152
irreducible scheme, 219
isogeny, 166
isomorphic, 158
isomorphism, 158, 199

J
j-invariant, 188
Jacobi's theta series, 437
Jacobian, 196
Jacobian conjecture, 159
Jacobian determinant, 170
Jacobian embedding, 196
Jacobson radical, 12
Janusz, 45–47, 52, 55, 108, 109

K
Kähler differential, 20
Kaczorowski, 458
κ-lattice, 372
κ-rational point, 150, 152, 155
κ_v-lattice, 372
Kawamata's structure theorem, 176
kernel, 9, 200
Khintchine, 329
Kiernan, 231
Ko, 323
Kobayashi, 229, 231, 235–238

Kobayashi hyperbolic, 230
Kobayashi measure, 233
Kobayashi pseudo distance, 230
Kodaira, 235, 237
Kodaira dimension, 175
Kolyvagin, 490
Krull dimension, 10, 221
Kubert, 486
Kummer pairing, 302

L
ℓ-adic representation, 193
L-function, 491–493
L^2-norm, 255
Lagrange interpolation formula, 128
Lander, 327
Lang, 13, 35, 172, 175, 176, 191, 229, 231, 237, 306, 311, 317, 328, 418, 419, 423, 430, 486
Langevin, 308
lattice, 113, 466
lattice point, 361
Lebesgue, 323
left translation, 165
Lehmer, 247, 259
Lehmer polynomial, 247
Lehmer's question, 258
Lehner, 484
length, 10, 209
length function, 379, 382, 395
length of index, 250
length of module, 210
level, 461, 483
Levin, 423, 424, 430, 431
lexicographic ordering, 406
lie over, 61
lifting, 35
line bundle, 202
line sheaf, 201
linear system, 173
linearly equivalent, 169, 227, 278
linearly independent, 321
Liouville, 328
Liouville's inequality, 242
local coordinate, 164
local defining function, 168
local degree, 80, 105
local different, 86, 369
local discriminant, 90
local equation, 168
local homomorphism, 214
local parameter, 164, 228
local ring, 10, 157
local trivialization, 202
localization, 11, 13
localization of ring, 213
locally bounded, 209, 275
locally free, 201
locally Noetherian scheme, 220
locally ringed space, 214
logarithmic discriminant, 293

M
Macdonald, 13, 15, 18, 28, 35, 153
Mahler, 329, 360, 380, 381
Mahler measure, 255
Manin, 486
Mason, 304, 306
Masser, 306
Masuda, 238
Matiyasevich, 420
Matsumura, 13, 14, 32, 153, 161, 216
maximal, 10
maximal condition, 14
maximal ideal, 157
maximal tamely ramified, 71
maximal unramified, 70, 89
Mazur, 485, 488
McQuillan, 238
measure hyperbolic, 233
Mellin inverse transform, 437
Mellin principle, 437
Mellin transform, 437
meromorphic, 462, 463, 466

metric, 208, 288
metrized height, 289
metrized line bundle, 209, 288
Metropolis, 328
Mihăilescu, 324
Milne, 197
minimal, 15
minimal (Weierstrass) equation, 193
minimal polynomial, 36
minimal prime, 210
minimal prime ideal, 15
Minkowski, 114
Minkowski's bound, 116
Minkowski's first theorem, 114
Minkowski's second theorem, 123, 376
mixed group, 4
M_κ-constant, 104, 274
model, 177, 283
modular, 485, 488
modular form, 475, 479
modular function, 469, 475, 478
modular group, 461
modular invariant, 469
modular parametrization conjecture, 490
module, 2
Mordell, 303, 415, 478
Mordell-Faltings theorem, 416
Mordell-Weil group, 303
Mordell-Weil theorem, 302
Mordellic, 418
Mori, 176, 237, 423
morphism, 158, 214, 216
μ-fold point, 178
Mukai, 237
multiple, 177
multiplicative, 457, 478
multiplicative M_κ-constant, 104
multiplicative function, 464
multiplicative reduction, 194
multiplicatively closed subset, 10
multiplicity, 163, 167, 178, 180, 211
Mumford, 175, 274
Mumford's formula, 296
Musili, 161

N

n-coboundary, 8
n-cocycle, 8
n-squares problem, 420
Néron, 172, 273
Néron function, 287
Néron-Severi group, 172
Nadel, 238
negatively curved, 231
newform, 484
nilpotent, 12
nilradical, 12
Nochka constant, 143
Nochka weight, 143
node, 188
Noetherian, 14, 152
Noetherian ring, 13
Noetherian scheme, 220
Noguchi, 238
non-Archimedean, 56, 61
non-singular, 162
non-split, 194
non-trivial zero, 458
nondegenerate, 55
nonprimitive, 444
nonsingular, 226, 227
norm, 48, 51, 58, 99, 135, 231
norm of ideal, 112
normal, 43, 158
normal crossings, 168
normal scheme, 220
normalization, 176, 177
normalized, 27, 481
normed vector space, 58
Northcott, 295
number field, 91

O

Ochiai, 235, 237
odd character, 445

Oesterlé, 306
open immersion, 220
open subscheme, 220
order, 1, 2, 28, 168, 436
order function, 27
ordinary, 178
ordinary multiple point, 180
ordinary singularity, 163
origin, 187
Ostrowski's first theorem, 57
Ostrowski's second theorem, 58
$\mathcal{O}_X$-module, 201

P
p-adic, 61
p-adic absolute value, 57
p-adic integer, 57
p-adic numbers, 57
$\mathfrak{p}$-adic valuation, 31
p-adic valuation, 24
palindromic polynomial, 247
parabolic, 460
parabolic point, 460
Parkin, 327
Perelli, 458
perfect, 44
periodic, 294
Petersson inner product, 482
Petersson–Ramanujan conjecture, 483
Phragmen–Lindelöf principle, 435
Picard group, 169
Picard variety, 172
Pick, 229
Pillai, 324
Pillai's conjecture, 324
place, 24
Poincaré, 185
Poincaré metric, 230
Poincaré–Bergman metric, 230
point at infinity, 177
pole, 226
pole set, 157
polynomial function, 151
positive, 167
powerful, 309
preperiodic, 294
presheaf, 197
presheaf cokernel, 199
presheaf image, 199
presheaf kernel, 199
primary decomposition, 15
primary ideal, 9
prime, 24
prime divisor, 24, 226
prime ideal, 9
prime number theorem, 442, 452
primitive, 34, 35, 444
primitive element, 44
principal, 19, 169, 443, 444
principal Cartier divisor, 169
principal character, 444
principal class, 30
principal compactified divisor, 287
principal congruence modular group, 461
principal divisor, 227
principal ideal, 9
product, 19
product formula, 57, 103, 105
product of ideals, 11
projection, 130
projection morphism, 221
projective, 223
projective n-space, 218, 223
projective algebraic variety, 155
projective dimension theorem, 161
projective hypersurface, 155
projective space, 130
projective variety, 155
proper, 9, 156, 223
proximity function, 280–282, 404
pseudo algebraically hyperbolic, 419
pseudo ample, 175
pseudo Brody hyperbolic, 231
pseudo canonical, 176

pseudo distance, 230
pseudo Kobayashi hyperbolic, 231
pseudo Mordellic, 418
pure dimension, 161
purely inseparable, 44
purely ramified, 70

Q
quasi-affine variety, 150
quasi-coherent, 224
quasi-projective, 223
quasi-projective variety, 155, 231
quotient bundle, 204
quotient field, 9
quotient of ideals, 111
quotient ring, 9
quotient sheaf, 200

R
radical, 12, 212, 306
Ramanujan hypothesis, 457
Ramanujan τ-function, 478
ramification divisor, 172, 227, 292
ramification index, 46, 67, 171, 228
ramified, 46, 67, 171, 228
rank, 201, 202, 303, 485, 486
rational algebraic curve, 185
rational differential form, 165
rational function, 152, 156
rational mapping, 159
rational section, 204
real period, 489
reciprocal polynomial, 247
reduced divisor, 167
reduced representation, 319
reduced scheme, 219, 220
reduction, 194, 283
reduction modulo, 35
regular, 156–158, 162, 177, 226
regular differential 1-form, 164
regular differential form, 164
regular function, 184
regular local ring, 13
regular sequence, 13, 406
regulator, 123
relative degree, 46, 101
relative differential, 224
relative differential form, 20
relative height, 264
relatively prime, 96
residue characteristic, 26
residue class degree, 67
residue class field, 13, 26, 155
residue field, 10, 222
residue-class ring, 9
resolution of singularity, 176
restricted topological product, 369
restriction mapping, 197
Ribenboim, 7
Ribet, 485
Richtmyer, 328
Riemann, 442
Riemann metric, 229
Riemann surface, 161
Riemann-Hurwitz formula, 183
Riemann-Roch space, 173
Riemann-Roch theorem, 181
right translation, 165
rigidity, 158
ring, 9
ring of fractions, 10, 11
ring of integers, 71
ringed space, 214
Robert, 467
Rogers, 114
Roth, 328
Roth's lemma, 342

S
S-integer, 379
S-integral point, 392
S-morphism, 218
S-scheme, 218
Salem number, 259
Salem polynomial, 259

Samuel, 35, 44, 161, 216
scheme, 215
scheme over S, 218
Schlickewei, 392, 393
Schmidt, 114, 314, 385, 386, 392, 393, 415
Schwarz, 229
Schwarz inequality, 133, 136
Schwarz-Pick lemma, 229
second minimum, 123
section, 197, 204
Segre mapping, 160, 265
Selberg, 456, 477
Selberg class, 456
Selmer group, 301
semi-stable reduction, 194
separable, 227
separable algebraic element, 43
separable algebraic extension, 44
separable degree, 42
separable polynomial, 43
separably generated, 44
separated, 222
separating element, 45
separating transcendence base, 44
Serre, 80, 181, 305, 467, 480, 485, 488
Severi, 172
Shafarevich, 160–162, 168, 173, 202, 206, 418, 431
Shafarevich-Tate group, 301
sheaf, 197
sheaf of ideals, 224
sheaf of regular functions, 198
Shiffman, 238, 418
Shimura, 463, 464, 467, 469, 480, 482, 485, 488
Shirosaki, 238
Siegel, 323, 328, 415, 467
Siegel zero, 451
Siegel's lemma, 331, 333
Siegel-type conjecture, 423, 431
sign of functional equation, 489
Silverman, 160, 161, 163, 168, 169, 172, 173, 175, 177, 183, 191, 430, 464, 467, 486, 488, 490
simple, 178, 209
simple point, 177
singular, 162, 177
Siu, 238
smooth, 162
smooth of relative dimension n, 225
Smyth, 259
Sodin, 147
Song, 430
special distance function, 360
special fibre, 222
special linear group, 459
specialization, 213
spectrum, 213
spherical image, 263, 273
split, 194
splitting field, 42, 43
stabilizer, 459
stable reduction, 194
stalk, 198
Stark, 191, 451
Steuding, 458
Stewart, 307
Stoll, 130
Stothers, 304, 306
Stothers–Mason's theorem, 304
strong approximation property, 30
structure sheaf, 214
subbundle, 204
subgeneral position, 142
subsheaf, 200
subspace theorem, 392, 404
subvariety, 158
successive minima, 123, 364, 375, 379, 381
sum of ideals, 11
superelliptic, 415
support, 167, 169
surface, 151, 161

surjective, 200
surjective system, 18
Swinnerton-Dyer, 114, 490
symmetric, 114, 144, 375
symmetric divisor, 296
symmetric polynomial, 247
symmetric polynomial theorem, 32
symmetric tensor power, 145
symmetric tensor product, 144, 145
symmetrizer, 145
Szpiro, 306, 309, 311

T
tame, 171, 228
tamely ramified, 71, 88
tangent bundle, 206
tangent line, 177, 178, 180
tangent mapping, 163
tangent space, 162
Taniyama, 488
Tate module, 192
Tate-Shafarevich group, 301
Taylor, 323, 488
tensor product, 80, 144, 203
Thue, 328, 331, 415
Thue equation, 415
Tijdeman, 307, 323, 324
Titchmarsh, 434, 435
topological ring, 18
Torelli's theorem, 197
torsion, 167
torsion sheaf, 228
torsion subgroup, 485
torsion-free group, 4
totally ordered, 6
totally ramified, 46, 70, 89
Totaro, 236, 237
trace, 48
transcendence base, 44
transcendence degree, 44
transcendental, 36
transition function, 206
transition matrices, 202
translation, 165
triple point, 178
trivial, 24, 56, 443, 444
trivial bundle, 202
trivial zero, 441, 458
truncated valence function, 292, 319, 320
Tucker, 430

U
Ueno, 176
Ueno fibration, 176
Ueno's theorem, 176
ultrametric, 56
uniform abc-conjecture, 320
uniformization theorem, 467
uniformizing parameter, 28
unique factorization domain, 9
unit, 9, 22
universally closed, 223
unramified, 46, 67, 70, 171, 226, 228
unstable reduction, 194

V
v-integer, 26
valence function, 280–282, 404
valuation, 24, 226
valuation group, 27
valuation ideal, 26
valuation integer, 26
valuation ring, 23, 24
value, 156, 157
van der Monde, 55, 109
van der Poorten, 393
Van der Waerden, 35
van Frankenhuysen, 305, 430
vector bundle, 202
Veronese mapping, 145, 404
vertical divisor, 284
very ample, 175
very canonical, 176

Vojta, 293, 314, 328, 386, 387, 392, 393, 415, 420, 423–425, 430, 431
Vojta's height inequality, 421
Vojta's inequality, 416
volume, 114
volume of convex body, 362
von Mangoldt Λ-function, 442

W
Waldschmidt, 311, 317
Weierstrass $\wp$ function, 467
Weierstrass coordinate function, 187
Weierstrass equation, 186, 190, 191
weight, 467, 475, 483, 485
weight function, 263, 273
Weil, 302, 369, 430, 487, 488
Weil divisor, 167, 226
Weil function, 274, 275
Weil's height machine, 266
wild, 171, 228
wildly ramified, 71, 88
Wiles, 323, 326, 488
Woods, 307
Wronskian determinant, 341
Wu, 132, 138

Y
Yang, 143, 313, 405, 406
Ye, 458
Yeung, 238
Yu, 307

Z
Zagier, 247
Zaidenberg, 238
Zannier, 405, 406, 408, 412, 424
Zariski, 35, 44, 161, 216
Zariski topology, 150, 155
Zariski's connectedness principle, 222
zero, 226, 463, 466
zero divisor, 9
zero ideal, 9
zero set, 150, 154
Zhang, 247