A.J. ENGLER · A. PRESTEL

# Valued Fields

Springer Monographs in Mathematics

Springer

**S***pringer* **M***onographs in* **M***athematics*

Antonio J. Engler
Alexander Prestel

# Valued Fields

Springer

Antonio J. Engler
Departamento de Matemática
IMECC-UNICAMP
Cx. Postal 6065
13083-970 Campinas
Brazil
E-mail: engler@ime.unicamp.br

Alexander Prestel
Fak. Mathematik
Fachbereich Mathematik und Statistik
Postfach 5560
78457 Konstanz
Germany
E-mail: alex.prestel@uni-konstanz.de

Library of Congress Control Number: 2005930440

Mathematics Subject Classification (2000): 12J10, 12J20

ISSN 1439-7382
ISBN-10 3-540-24221-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-24221-5 Springer Berlin Heidelberg New York



Springer is a part of Springer Science+Business Media
springeronline.com

Printed in The Netherlands



Typesetting: by the authors and TechBooks using a Springer LaTeX macro package

Cover design: *design & production* GmbH, Heidelberg

Printed on acid-free paper SPIN: 10996843 41/TechBooks 5 4 3 2 1 0

To the memory of Otto Endler
(17.9.1929–12.5.1988)

# Preface

The purpose of this book is to give a self-contained and comprehensive introduction to the theory of general valuations, in contrast to classical absolute values. In particular, we present some applications of the general theory going beyond the use of absolute values. The book does not aim for an encyclopaedic presentation, but rather prefers a streamlined style, leading eventually to deep results of recent research.

While the classical theory of absolute values can be found in many books, in particular those on number theory, there are few textbooks devoted to the general theory of valuations. To our knowledge, these are O. Schilling (1950, [27]), P. Ribenboim (1965, [23]), and O. Endler (1972, [6]). Besides those, one can find, however, chapters on general valuation theory in several books, such as in O. Zariski – P. Samuel (1960, [33]) or Y. Ershov (2001, [8]). Concerning the history of valuation theory, the reader is referred to P. Roquette [25].

Both authors of this book have been deeply influenced by the late Otto Endler – the first author as a student, the second as a colleague. It was at the IMPA in Rio de Janeiro where we all met in the mid seventies. Since then we became followers of Krull's development of henselian valued fields, and since then we have tried to convince other mathematicians of the beauty of this theory.

The book is based on courses given by the first author in Brazil, and by the second author in Pisa, Freiburg and Konstanz. We are grateful to K. Becher, M. Illengo, I. Klep, J. Koenigsmann, J. Schmid and T. Unger for reading parts of the book and making many valuable comments. We are also grateful to C. N. Delzell for checking the layout and the use of the English language.

Last not least we thank Mrs. Otterbeck for preparing the manuscript of this book.

Campinas, Brazil — *Antonio J. Engler*
Konstanz, Germany — *Alexander Prestel*
May 2005

# Contents

# Introduction

Absolute values of a field and their completions – like the $p$-adic number fields – played an important role in the development of number theory in the beginning of the 20th century. In the 1930's Krull generalized the notion of an absolute value to that of a valuation. This generalization made possible applications in other branches of mathematics, such as algebraic and real algebraic geometry. In the theory of valuations, the notion of a completion had to be replaced by that of the so-called henselization. In this book, the theory of valuations as well as of henselizations is developed, and applications are given that could not be obtained by the use of absolute values only.

To be more precise, let us start by recalling the notion of an absolute value on a field $K$. It is a map

$$|\ |: K \longrightarrow \mathbb{R}$$

satisfying for all $x, y \in K$ the axioms

$$\begin{array}{ll} (i) & |x| = 0 \iff x = 0\ , \\ (ii) & |xy| = |x||y|\ , \\ (iii) & |x+y| \leq |x| + |y|\ . \end{array}$$

In case the following, stronger version of $(iii)$,

$$|x+y| \leq \max\,(|x|, |y|)\ ,$$

holds, $|\ |$ is called a non-archimedean absolute value.

The archimedean absolute values turn out to be induced by the canonical absolute value of the field $\mathbb{C}$ of complex numbers; more precisely, in this case $K$ may be identified with a subfield of $\mathbb{C}$ together with the induced absolute value.

Every absolute value $|\ |$ canonically defines a metric, by taking $|x-y|$ as the distance between $x$ and $y$. The completion of $K$ with respect to this metric yields again a field $\widehat{K}$ to which the absolute value $|\ |$ of $K$ extends canonically and which contains $K$ as a dense subfield. In the archimedean case the only completions possible are $\mathbb{R}$ and $\mathbb{C}$.

The non-archimedean absolute values of the field $\mathbb{Q}$ of rational numbers are in one-to-one correspondence with the prime numbers $p$. The absolute value $|\ |_p$ corresponding to $p$ assigns to $p$ the value $e^{-1}$ (where $e$ is the base of the natural logarithm) and $e^0 = 1$ to any other prime $q$. The completion of $\mathbb{Q}$ with respect to $|\ |_p$ is known as the field $\mathbb{Q}_p$ of $p$-adic numbers. With its use we can formulate the famous and very useful local-global principle of Hasse-Minkowski concerning quadratic forms: Let $f(X_1, \ldots, X_n)$ be a homogeneous polynomial of degree 2 over $\mathbb{Q}$. Then $f$ has a non-trivial zero in $\mathbb{Q}$ if it has one in $\mathbb{R}$ and one in each $\mathbb{Q}_p$.

The reason this principle is so useful lies in the fact that solving equations is much easier in $\mathbb{R}$ and in $\mathbb{Q}_p$ than in $\mathbb{Q}$. For $\mathbb{R}$ this is pretty clear. Let us explain this fact for $\mathbb{Q}_p$, or more generally for a field $K$ that is complete with respect to a non-archimedean absolute value $|\ |$. In such a field (even without being complete) the set

$$\mathcal{O} = \{x \in K \mid |x| \leq 1\}$$

forms a subring of $K$ with

$$\mathcal{M} = \{x \in K \mid |x| < 1\}$$

as its unique maximal ideal. The field $\mathcal{O}/\mathcal{M}$ is called the residue class field of $|\ |$ and is denoted by $\overline{K}$. This field is usually much simpler than $K$ itself. For instance, if $|\ |_p$ is the $p$-adic absolute value of $\mathbb{Q}$ or of $\mathbb{Q}_p$ then $\overline{K}$ is just the finite field $\mathbb{F}_p$ consisting of only $p$ elements. Now if $K$ is complete, "Hensel's Lemma" holds, saying that a polynomial over $\mathcal{O}$ that has a simple zero in $\overline{K}$, already has a zero in $K$. By this lemma, many algebraic problems of $K$ are reduced to $\overline{K}$. It is this lemma that matters for the completion $\widehat{K}$ of $K$, and not the fact that $K$ is dense in $\widehat{K}$.

Now let us come to valuations of a field $K$. Before doing so, let us, however, replace a non-archimedean absolute value $|\ |$ on a field $K$ by the map

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}\ ,$$

defined by $v(x) := -\ln|x|$. Now the properties $(i)$-$(iii)$ read as follows

$$\begin{array}{ll} (i') & v(x) = \infty \iff x = 0\ , \\ (ii') & v(xy) = v(x) + v(y)\ , \\ (iii') & v(x+y) \geq \min\,(v(x), v(y))\ . \end{array}$$

Accordingly, we get

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$$

and

$$\mathcal{M} = \{x \in K \mid v(x) > 0\}\ .$$

One should observe that the map $v$ uses only the additive structure and the ordering of $\mathbb{R}$. Thus when searching for a generalization of absolute values, we

may replace $(\mathbb{R}, +, \leq)$ by an arbitrary ordered abelian group $\Gamma$. This is what Krull did.

We now define a valuation of $K$ to be a map

$$v : K \longrightarrow \Gamma \cup \{\infty\}$$

satisfying the axioms $(i')$ to $(iii')$. The definitions of $\mathcal{O}$ and $\mathcal{M}$ and of the residue class field $\overline{K}$ remain the same as above.

Unfortunately, the notion of a completion now becomes more involved, and, as it turns out, is not very useful. The reason for this is that Hensel's Lemma no longer holds in general. As a substitute one therefore introduces a certain algebraic extension field $K^h$ of $K$ that canonically extends the valuation of $K$ and satisfies Hensel's Lemma. This extension, which is unique up to value isomorphism, is called the henselization of $(K, v)$. Although $K$ need no longer be dense in $K^h$, the henselization still has the same residue class field and takes the same values as $K$, a property which, for the completion, is a consequence of the density. It is the henselization that will open up to us the opportunity for further applications.

After presenting the basic facts about absolute values in Chap. 1, we shall introduce valuations in Chap. 2. In Chap. 3 we study extensions of valuations from one field $K$ to a bigger one, and in Chap. 4 we deal with fields satisfying Hensel's Lemma. In Chap. 5, finally, we study henselizations and the structure of their algebraic extension fields. Chapter 6 is devoted to three interesting applications of the general theory developed so far.

As a first application we give Ax-Kochen's solution of 'Artin's Conjecture' about the $p$-adic number fields $\mathbb{Q}_p$. This conjecture deals with the solvability of certain diophantine equations over $\mathbb{Q}_p$, and thus does not involve any valuations except the $p$-adic absolute value in the definition of $\mathbb{Q}_p$. The solution, however, makes essential use of quite general valuation theory, in particular of the theory of henselian fields. No proof avoiding this is known.

In the second application we use the notion of (general) valuations and henselizations in order to give a description of those fields that share with $\mathbb{Q}_p$ all its 'algebraic' properties (like the real closed fields do with $\mathbb{R}$).

Finally, in the third application we give a general local-global principle for 'weak' isotropy of quadratic forms over a given field $K$. Here again general valuation theory is needed, as the 'local' objects are henselizations of valuations that do not admit a useful completion.

In Appendix B we give one more justification for the consideration of valuations besides the absolute values. Both, the absolute values as well as the valuations on a field $K$, canonically induce a topology on $K$ for which all field operations are continuous, with the extra property that the product of two elements can be small only if at least one of the factors is already small. Such field topologies are called $V$-topologies. It turns out that, conversely, every $V$-topology on $K$ must be induced by an absolute value or a valuation. Thus the valuations complement the absolute values in a natural way.

# 1

# Absolute Values

In this chapter we give a short introduction to the classical theory of absolute values as it can be found in many books on basic algebra, e.g., [15]. In particular we introduce the $p$-adic number field $\mathbb{Q}_p$, $p$ a rational prime, and the field $\mathbb{F}_p((X))$ of formal Laurent series over the finite field $\mathbb{F}_p$ of $p$ elements.

## 1.1 Absolute Values – Completions

Let $K$ be a field. An *absolute value* on $K$ is a map

$$|\ |: K \longrightarrow \mathbb{R}$$

satisfying the following axioms for all $x, y \in K$:

$$\begin{array}{ll} (1) & |x| > 0 \text{ for all } x \neq 0, \text{ and } |0| = 0 \\ (2) & |xy| = |x||y| \\ (3) & |x+y| \leq |x| + |y| \end{array} \tag{1.1.1}$$

The absolute value sending all $x \neq 0$ to 1 is called the *trivial* absolute value on $K$.

We observe that $|1|^2 = |1^2| = |1|$, whence $|1| = 1$. Similarly $|-1|^2 = |(-1)(-1)| = |1| = 1$ implies $|-1| = 1$. Thus we obtain $|-x| = |x|$, for all $x \in K$. Since $|\ |$ is a homomorphism on $K^\times$ we also have $|x^{-1}| = |x|^{-1}$ for $x \neq 0$.

**Proposition 1.1.1.** *The set $\{|n \cdot 1| \mid n \in \mathbb{Z}\}$ is bounded if and only if $|\ |$ satisfies the "ultrametric" inequality*

$$|x+y| \leq \max\{|x|, |y|\} \tag{1.1.2}$$

*for all $x, y \in K$.*

*Proof.* If $|\ |$ satisfies (1.1.2), then by induction, the set $\{|n \cdot 1| \mid n \in \mathbb{Z}\}$ is bounded by 1.

Conversely, let $|n \cdot 1| \leq C$. Then

$$|x+y|^n = |(x+y)^n| \leq \sum_\nu \left| \binom{n}{\nu} x^\nu y^{n-\nu} \right| \leq (n+1)C\max(|x|,|y|)^n \ .$$

Taking $n$-th roots and letting $n$ go to infinity proves the assertion of the proposition. □

If an absolute value satisfies (1.1.2), it is called *non-archimedean*; otherwise it is called *archimedean*. Clearly, if char $K \neq 0$, $K$ cannot carry any archimedean absolute value.

A typical example of an archimedean absolute value is

$$|x|_0 = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x \leq 0 \ , \end{cases}$$

for all $x \in \mathbb{R}$; we shall call $|\ |_0$ the *usual* absolute value on $\mathbb{R}$. In fact, the set

$$\{|n \cdot 1|_0 \mid n \in \mathbb{Z}\} = \mathbb{N}$$

is unbounded in $\mathbb{R}$.

Next, let us consider the most basic examples of non-archimedean absolute values.

For every rational prime $p$, the *$p$-adic* absolute value $|\ |_p$ on $\mathbb{Q}$ is defined by $|0|_p = 0$ and

$$\left| p^\nu \frac{m}{n} \right|_p = \frac{1}{e^\nu} \ , \tag{1.1.3}$$

where $e$ is the base of the natural logarithms, $\nu \in \mathbb{Z}$, and $n, m \in \mathbb{Z} \smallsetminus \{0\}$ are not divisible by $p$. In this case the set

$$\{\, |n \cdot 1|_p \mid n \in \mathbb{Z} \,\} = \{\, e^{-\nu} \mid \nu \in \mathbb{N} \,\}$$

in bounded in $\mathbb{R}$.

Similarly we define for every irreducible polynomial $p \in k[X]$, $k$ a field, the following absolute value $|\ |_p$ on the rational function field $K = k(X)$: Let $|0|_p = 0$ and

$$\left| p^\nu \frac{f}{g} \right|_p = \frac{1}{e^\nu} \ , \tag{1.1.4}$$

where $\nu \in \mathbb{Z}$, and $f, g \in k[X] \smallsetminus \{0\}$ are not divisible by $p$. Hence the set $\{|n \cdot 1|_p \mid n \in \mathbb{Z}\}$ contains only 0, and thus is bounded in $\mathbb{R}$.

An absolute value $|\ |$ on $K$ defines a metric by taking $|x-y|$ as distance, for $x, y \in K$. In particular, $|\ |$ induces a topology on $K$. If two absolute values induce the same topology on $K$, they are called *dependent* (otherwise *independent*).

**Proposition 1.1.2.** *Let* $|\ |'$ *and* $|\ |''$ *be two non-trivial absolute values on* $K$. *They are dependent if and only if for all* $x \in K$,

$$|x|' < 1 \text{ implies } |x|'' < 1 \ .$$

*If they are dependent, then there exists a real number* $\lambda > 0$ *such that* $|x|' = (|x|'')^\lambda$ *for all* $x \in K$.

*Proof.* For $|\ |'$ and $|\ |''$ non-trivial and dependent absolute values on $K$ there exists $\varepsilon > 0$ such that $\{x \in K \mid |x|' < \varepsilon\} \subseteq \{x \in K \mid |x|'' < 1\}$. If $|x|' < 1$, there is $m \geq 1$ such that $|x^m|' = (|x|')^m < \varepsilon$. Hence $(|x|'')^m = |x^m|'' < 1$ and consequently $|x|'' < 1$, as required.

Conversely, by the non-triviality of $|\ |'$, there exists $z \in K$ with $|z|' > 1$. Thus $|z^{-1}|' < 1$ and so $|z^{-1}|'' < 1$, by assumption. Hence $|z|'' > 1$, too.

Claim: for every $x \in K$, $x \neq 0$,

$$\frac{\log |x|'}{\log |x|''} = \frac{\log |z|'}{\log |z|''} \ .$$

In fact, for $m, n \in \mathbb{Z}$, $n > 0$, such that

$$\frac{m}{n} > \frac{\log |x|'}{\log |z|'} \ ,$$

it follows that $(|z|')^m > (|x|')^n$. Consequently, $|x^n z^{-m}|' < 1$ and then, by assumption, $|x^n z^{-m}|'' < 1$. Walking back the steps of the last argument one gets

$$\frac{m}{n} > \frac{\log |x|''}{\log |z|''} \ .$$

Therefore

$$\frac{\log |x|'}{\log |z|'} \geq \frac{\log |x|''}{\log |z|''} \ .$$

Similarly one proves the reverse inequality. So

$$\frac{\log |x|'}{\log |z|'} = \frac{\log |x|''}{\log |z|''}$$

implying the claim.

Therefore for

$$\lambda = \frac{\log |z|'}{\log |z|''}$$

it follows that $|x|' = (|x|'')^\lambda$, for every $x \in K$, as required. Finally, the last equation implies that $|\ |'$ and $|\ |''$ are dependent. □

By taking into account the axioms (1.1.1), one gets $|x| = |x - y + y| \leq |x - y| + |y|$. Thus $|x| - |y| \leq |x - y|$. Permuting $x$ and $y$ and recalling that $|y - x| = |x - y|$, it follows that $||x| - |y||_0 \leq |x - y|$, where $|\ |_0$ is again the

usual absolute value on the real numbers. Consequently, an absolute value $|\ |$ is a uniformly continuous map from $K$, provided with the topology given by $|\ |$, to $\mathbb{R}$ with the usual topology defined by $|\ |_0$.

The next theorem deals with independent absolute values on $K$.

**Approximation Theorem 1.1.3.** (Artin-Whaples) *Let $K$ be a field and $|\ |_1, \ldots, |\ |_n$ non-trivial pairwise-independent absolute values on $K$. Moreover let $x_1, \ldots, x_n \in K$, and $0 < \varepsilon \in \mathbb{R}$. Then there exists $x \in K$ such that*

$$|x - x_i|_i < \varepsilon$$

*for all $i$.*

*Proof.* The proof will be achieved in three steps.

*Step 1.* We shall prove that for every $1 \leq i \leq n$ there exists $a_i \in K$ such that $|a_i|_i > 1$ and $|a_i|_j < 1$, for all $j \neq i$. We may fix $i = 1$ without loss of generality, and write $a = a_1$.

Proceeding by induction on $n$, for $n = 2$, Proposition 1.1.2 implies the existence of $b, c \in K$ such that

$$\begin{aligned} |b|_1 < 1 \quad &\text{and} \quad |b|_2 \geq 1 \\ |c|_1 \geq 1 \quad &\text{and} \quad |c|_2 < 1\ . \end{aligned}$$

Thus $a = b^{-1}c$ has the desired properties.

Assume next that there is $y \in K$ such that $|y|_1 > 1$ and $|y|_j < 1$ for all $j = 2, \ldots, n-1$. Applying the first case to $|\ |_1$ and $|\ |_n$, one has $|z|_1 > 1$ and $|z|_n < 1$, for some $z \in K$. Therefore, if $|y|_n \leq 1$, then $|zy^\nu|_1 > 1$ and $|zy^\nu|_n < 1$ for every integer $\nu \geq 1$. On the other hand, for a sufficiently large integer $\nu \geq 1$, $|zy^\nu|_j < 1$ for every $j = 2, \ldots, n-1$. For such a $\nu$, $a = zy^\nu$ satisfies the requirements.

Consider now the case $|y|_n > 1$, and form the sequence

$$w_\nu = \frac{y^\nu}{1 + y^\nu}, \quad \nu \in \mathbb{N}\ .$$

The usual properties of sequences of ordinary real numbers imply that

$$\lim_{\nu \to \infty} |w_\nu|_j = 0 \text{ for } j = 2, \ldots, n-1$$

and

$$\lim_{\nu \to \infty} |w_\nu - 1|_j = 0 \text{ for } j = 1, \ldots, n\ .$$

Consequently,

$$\lim_{\nu \to \infty} |zw_\nu|_j = 0 \text{ for } j = 2, \ldots, n-1$$

and

$$\lim_{\nu \to \infty} |zw_\nu|_j = |z|_j \text{ for } j = 1, \ldots, n\ .$$

Hence, for sufficiently large $\nu$, $a = zw_\nu$ has the required properties.

*Step 2.* Now we prove that for any real number $\varepsilon > 0$ and every $i$ such that $1 \le i \le n$, there exists $c_i \in K$ such that $|c_i - 1|_i < \varepsilon$ and $|c_i|_j < \varepsilon$, for all $j \ne i$. As in Step 1, it is enough to consider the case $i = 1$.

Let $a \in K$ satisfy the conditions of Step 1. Then the sequence

$$\Big|\frac{a^\nu}{1+a^\nu}\Big|_j$$

converges to 1 for $j = 1$, and converges to 0 if $j > 1$. Thus for sufficiently large $\nu$,

$$c_1 = \frac{a^\nu}{1+a^\nu}$$

has the required property.

*Final step.* According to Step 2 there exist elements $c_1, \dots, c_n$ in $K$ such that $c_i$ is close to 1 at $|\ |_i$, and for every $j \ne i$, $c_i$ is close to 0 at $|\ |_j$. The element $x = c_1x_1 + \cdots + c_nx_n$ is then arbitrarily close to $x_i$ at $|\ |_i$, for every $i = 1, \dots, n$, and therefore satisfies the requirements of the theorem. □

Since a non-trivial absolute value $|\ |$ defines a metric on $K$, we may consider the completion of $K$ with respect to $|\ |$. In what follows, $|\ |$ is fixed.

A sequence $(x_n)_{n\in\mathbb{N}}$ of elements of $K$ is called a *Cauchy sequence* if to every $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $n, m > N$ we have

$$|x_n - x_m| < \varepsilon\ .$$

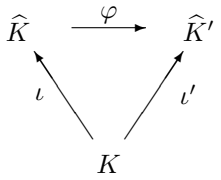
Similarly, we say that a sequence $(x_n)_{n\in\mathbb{N}}$ *converges* to $x \in K$, and we write $\lim_{n\to\infty} x_n = x$, if for every $\varepsilon > 0$ there is an $N \in \mathbb{N}$ such that for all $n > N$ we have

$$|x_n - x| < \varepsilon\ .$$

$K$ is called *complete* if every Cauchy sequence from $K$ converges to some element of $K$.

The next theorem will show that every field $K$ with a non-trivial absolute value can be densely embedded into a field complete with respect to an absolute value extending the given one on $K$. (Note that $K$ is always complete with respect to the trivial absolute value.) Before we do so, let us recall that $\mathbb{Q}$ is not complete with respect to the usual absolute value $|\ |_0$. Moreover, $\mathbb{Q}$ is not complete with respect to the $p$-adic absolute value $v_p$.

**Theorem 1.1.4.** *There exists a field $\widehat{K}$, complete under an absolute value $|\widehat{\ }|$, and an embedding $\iota : K \longrightarrow \widehat{K}$, such that $|x| = \big|\widehat{\iota(x)}\big|$ for all $x \in K$. The image $\iota(K)$ is dense in $\widehat{K}$. If $\big(\widehat{K}', \iota'\big)$ is another such pair, then there exists a unique continuous isomorphism $\varphi : \widehat{K} \longrightarrow \widehat{K}'$ preserving the absolute value and making the diagram*




*commutative.*

*Proof.* The existence of $\widehat{K}$ is proved by standard arguments. Let $\mathcal{C}$ be the set of all Cauchy sequences $(x_n)_{n\in\mathbb{N}}$ of elements of $K$. Componentwise addition and multiplication make $\mathcal{C}$ with these operations a commutative ring with $1 = (1)_{n\in\mathbb{N}}$. The set

$$\mathcal{N} = \left\{ (x_n)_{n\in\mathbb{N}} \;\middle|\; \lim_{n\to\infty} x_n = 0 \right\}$$

is an ideal of $\mathcal{C}$. In fact, the sum of two sequences in $\mathcal{N}$ clearly lies in $\mathcal{N}$. To check the multiplicative property of $\mathcal{N}$, observe first that if $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$, then there exists an $N \in \mathbb{N}$ such that $|a_m - a_{N+1}| < 1$ for every $m > N$. Thus

$$|a_m| = |a_m - a_{N+1} + a_{N+1}| \leq |a_m - a_{N+1}| + |a_{N+1}| < 1 + |a_{N+1}| \,,$$

for every $m > N$ (i.e., each Cauchy sequence is bounded from above). Given $(b_n)_{n\in\mathbb{N}} \in \mathcal{N}$ and $\varepsilon > 0$, there is $N' \in \mathbb{N}$ such that

$$|b_n| < \frac{\varepsilon}{1 + |a_{N+1}|}$$

for every $n > N'$. Consequently, for every $n > \max\{N, N'\}$ it follows that $|a_n b_n| < \varepsilon$. Hence $(a_n b_n)_{n\in\mathbb{N}} \in \mathcal{N}$. In particular, we see that every sequence from $\mathcal{N}$ admits an upper bound.

On the other hand, each $(a_n)_{n\in\mathbb{N}} \in \mathcal{C} \setminus \mathcal{N}$ has a positive lower bound. Indeed, suppose, for the sake of obtaining a contradiction, that for every real $\eta > 0$ and every $N \in \mathbb{N}$, $|a_m| < \eta$ for some $m > N$. Then, given $\varepsilon > 0$, take $N' \in \mathbb{N}$ such that $p, q > N'$ implies $|a_p - a_q| < \varepsilon/2$. Let $m > N'$ be an integer for which $|a_m| < \varepsilon/2$. Then for every $p > N'$ it follows that

$$|a_p| = |a_p - a_m + a_m| \leq |a_p - a_m| + |a_m| < \varepsilon \,,$$

contrary to the assumption that $(a_n)_{n\in\mathbb{N}} \notin \mathcal{N}$. Consequently, for $(a_n)_{n\in\mathbb{N}} \in \mathcal{C} \setminus \mathcal{N}$, an $M \in \mathbb{N}$ and a real number $\eta > 0$ must exist such that

$$|a_n| > \eta \text{ for every } n > M \,.$$

Setting $c_n = 1$ for every $n = 1, \ldots, M$ and $c_n = a_n^{-1}$ for every $n > M$, by the usual arguments one sees that $(c_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. In fact, given a real number $\varepsilon > 0$, let $N \in \mathbb{N}$ and $\eta > 0$ be such that $|a_p - a_q| < \varepsilon\eta^{-2}$ for all

$p, q > N$. Now, if $p, q > \max\{N, M\}$, then $|c_p - c_q| = |a_q - a_p||a_p|^{-1}|a_q|^{-1} < \varepsilon$, as desired. Finally, it is clear that $(a_n)_{n\in\mathbb{N}}(c_n)_{n\in\mathbb{N}} - (1)_{n\in\mathbb{N}} \in \mathcal{N}$. Therefore the ideal $\mathcal{N}$ is a maximal ideal (actually the unique such ideal) of $\mathcal{C}$, and the quotient ring $\widehat{K}$ is a field.

The map $\iota : K \longrightarrow \widehat{K}$ defined by $\iota(x) = (x_n)_{n\in\mathbb{N}}$, where $x_n = x$ for every $n$, embeds $K$ in $\widehat{K}$.

Now for $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$ the sequence $(|a_n|)_{n\in\mathbb{N}}$ is a Cauchy sequence of real numbers, because $||a_p| - |a_q||_0 \leq |a_p - a_q|$, for all $p, q$, as we observed before Theorem 1.1.3. Moreover, for every sequence $(a_n)_{n\in\mathbb{N}} \in \mathcal{N}$ the sequence of real numbers $(|a_n|)_{n\in\mathbb{N}}$ has limit 0. Consequently, for $\xi = (a_n)_{n\in\mathbb{N}} + \mathcal{N}$ the value

$$\big|\widehat{\xi}\big| = \lim_{n\to\infty} |a_n|$$

does not depend on the representative $(a_n)_{n\in\mathbb{N}}$ of $\xi$. Combining the properties of $|\ |$ and limits it follows that $|\widehat{\ }|$ is an absolute value on $\widehat{K}$ that induces $|\ |$ on $K$.

Next, we prove that $\iota(K)$ is dense in $\widehat{K}$ with respect to $|\widehat{\ }|$. For $\zeta \in \widehat{K}$ let $(a_n)_{n\in\mathbb{N}}$ be a representative sequence of $\zeta$. Given a real number $\varepsilon > 0$, take $N \in \mathbb{N}$ such that $|a_p - a_q| < \varepsilon$ for all $p, q > N$. Then

$$\big|\widehat{\zeta - \iota(a_n)}\big| = \lim_{p\to\infty} |a_p - a_n| < \varepsilon$$

for every $n > N$. Hence

$$\lim_{n\to\infty} \iota(a_n) = \zeta\ .$$

It follows also from the last limit that given a Cauchy sequence $(a_n)_{n\in\mathbb{N}}$, $a_n \in K$, the sequence $(\iota(a_n))_{n\in\mathbb{N}}$ converges to the residue class $(a_n)_{n\in\mathbb{N}} + \mathcal{N}$, with respect to $|\widehat{\ }|$. This remark is the key to seeing that $\widehat{K}$ is complete with respect to $|\widehat{\ }|$. Take a Cauchy sequence $(\xi_n)_{n\in\mathbb{N}}$ in $\widehat{K}$, $|\widehat{\ }|$. As $\iota(K)$ is dense in $\widehat{K}$, we can choose $x_n \in K$, for each number $n$, such that

$$\big|\widehat{\xi_n - \iota(x_n)}\big| < 1/n\ .$$

For any real number $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that for $p, q > N$, the inequalities

$$1/p < \varepsilon/3, \qquad 1/q < \varepsilon/3, \qquad \big|\widehat{\xi_p - \xi_q}\big| < \varepsilon/3$$

hold. Thus

$$|x_p - x_q| \leq \big|\widehat{\iota(x_p) - \xi_p}\big| + \big|\widehat{\xi_p - \xi_q}\big| + \big|\widehat{\xi_q - \iota(x_q)}\big| < \varepsilon$$

for all $p, q > N$. Hence $(x_n)_{n\in\mathbb{N}} \in \mathcal{C}$. Moreover, for $\xi = (x_n)_{n\in\mathbb{N}} + \mathcal{N} \in \widehat{K}$, it follows from $\lim_{n\to\infty} \iota(x_n) = \xi$ that

$$\big|\widehat{\xi_n - \xi}\big| \leq \big|\widehat{\xi_n - \iota(x_n)}\big| + \big|\widehat{\iota(x_n) - \xi}\big| < \varepsilon\ ,$$

for $\varepsilon > 0$ and all $n$ sufficiently large. Consequently, $(\xi_n)_{n\in\mathbb{N}}$ converges to $\xi$, and so $\widehat{K}$ is complete.

Finally, let $\left(\widehat{K}', \iota'\right)$ be any other pair with the same properties. For every $\xi = (a_n)_{n\in\mathbb{N}} + \mathcal{N} \in \widehat{K}$, the sequence $(\iota'(a_n))_{n\in\mathbb{N}}$ is a Cauchy sequence of $\widehat{K}'$. Let $\xi'$ be its limit in $\widehat{K}'$. Define $\varphi(\xi) = \xi'$. From the uniqueness of limits it follows that $\varphi$ is a map. As $\iota'(K)$ is dense in $\widehat{K}'$, $\varphi$ is surjective. The assumption that $\iota$ and $\iota'$ are homomorphisms and again the uniqueness of limits imply that $\varphi$ is a homomorphism. Clearly $\varphi$ makes the required diagram commutative, and by standard strictly topological arguments $\varphi$ is continuous. Finally, as a non-trivial ring homomorphism, $\varphi$ is injective, which completes the proof of the uniqueness of the completion. □

Note that for the trivial absolute value on $K$, every Cauchy sequence is eventually constant, and thus $K$ is complete. We are not interested in this case.

A pair $\left(\widehat{K}, |\widehat{\ }|\right)$ as in Theorem 1.1.4 is called a *completion* of the valued field $(K, |\ |)$. We shall see examples in the next two sections.

## 1.2 Archimedean Complete Fields

In this section let $K$ be a field complete with respect to an archimedean absolute value $|\ |$. Since the set $\{\, |n \cdot 1| \mid n \in \mathbb{Z}\}$ is not bounded, $\operatorname{char} K = 0$. Thus $K$ contains the field $\mathbb{Q}$ of rationals. We shall first show that $|\ |$ restricted to $\mathbb{Q}$ is dependent on the usual absolute value of $\mathbb{Q}$. Thus the complete field $K$ contains the completion of $\mathbb{Q}$ with respect to the ordinary absolute value, i.e., $K$ contains $\mathbb{R}$ as a closed subfield. We shall then show that $K$ must be equal to $\mathbb{R}$ or to $\mathbb{C}$. Consequently, every field $K$ admitting an archimedean absolute value may be considered as a subfield of $\mathbb{C}$ or even $\mathbb{R}$ with the absolute value dependent on the induced one from $\mathbb{C}$ (or from $\mathbb{R}$).

**Proposition 1.2.1.** *Every archimedean absolute value on $\mathbb{Q}$ is dependent on the usual one.*

*Proof.* Let $|\ |$ be an archimedean absolute value on $\mathbb{Q}$. Denote by $|\ |_0$ the usual absolute value on $\mathbb{Q}$.

Next, for integers $m, n \geq 2$ and $t \geq 1$ expand $m^t$ in powers of $n$:

$$m^t = c_0 + c_1 n + \cdots + c_s n^s \text{ where } 0 \leq c_0, \ldots, c_s < n \text{ and } c_s \neq 0\ .$$

Since $|c_i| \leq c_i < n$, for each $i$ such that $0 \leq i \leq s$, it follows that

$$|m|^t \leq \sum_{0\leq i\leq s} |c_i||n|^i \leq n \sum_{0\leq i\leq s} |n|^i \leq n(s+1)\max\{1, |n|^s\}\ .$$

As $n^s \leq m^t$, $s \leq t(\log m)/\log n$. Thus

$$|m|^t \le n\left(\frac{t\log m}{\log n}+1\right)\max\{1,|n|\}^{t(\log m)/\log n}$$

or equivalently,

$$|m| \le n^{1/t}\left(\frac{t\log m}{\log n}+1\right)^{1/t}\max\{1,|n|\}^{(\log m)/\log n}\ .$$

Letting $t$ go to infinity and taking limits, one gets

$$|m| \le \max\{1,|n|\}^{(\log m)/\log n}\ .$$

Now, if $|n|<1$ for some $n\in\mathbb{N}$, the above inequality implies $|m|<1$ for every integer $m\ge 2$, contradicting the archimedeanness of $|\ |$.

Therefore, $|n|>1$ for all integers $n\ge 2$, and thus

$$|m| \le |n|^{(\log m)/\log n}\ .$$

Interchanging the roles of $m$ and $n$ in the above inequality gives the reverse inequality. Hence

$$|m| = |n|^{(\log m)/\log n}\ .$$

Therefore, if $m>n\ge 2$, then $(\log m)/\log n>1$ and so $|m|>|n|$. Since $|-m|=|m|$ for all $m\in\mathbb{Z}$, it follows that $|m|_0>|n|_0$ implies $|m|>|n|$, for non-zero $m,n\in\mathbb{Z}$. Consequently, if $m/n\in\mathbb{Q}$ satisfies $|m/n|_0<1$, then $|m/n|<1$. By Proposition 1.1.2, $|\ |_0$ and $|\ |$ are dependent. □

For the next proposition we do not require the absolute value $|\ |$ on $K$ to be archimedean. Thus for the time being let $|\ |$ be just a non-trivial absolute value on $K$. Then if $E$ is a vector space over $K$, by a *norm* $\|\ \|$ on $E$ (compatible with $|\ |$ on $K$) we understand a map

$$\|\ \| : E \longrightarrow \mathbb{R}$$

satisfying the following axioms for all $\xi,\eta\in E$ and $x\in K$:

$$\begin{aligned}&(1)\ \|\xi\|>0 \text{ for } \xi\neq 0 \text{ and } \|0\|=0\\ &(2)\ \|x\xi\| = |x|\|\xi\|\\ &(3)\ \|\xi+\eta\| \le \|\xi\|+\|\eta\|\end{aligned} \tag{1.2.1}$$

A norm $\|\ \|$ on $E$ defines a metric on $E$ by taking $\|x-y\|$ as distance. For $r\in\mathbb{R}$, the "open ball" of radius $r$ and center $x_0\in E$ is $\{\,x\in E\mid \|x-x_0\|<r\,\}$.

Two norms $\|\ \|_1$ and $\|\ \|_2$ are called *equivalent* if there exist numbers $C_1,C_2>0$ such that for all $\xi\in E$ we have

$$C_1\|\xi\|_1 \le \|\xi\|_2 \le C_2\|\xi\|_1\ .$$

If $E$ is finite dimensional, and $\omega_1,\dots,\omega_n$ is a basis of $E$ over $K$, the most basic norm on $E$ is obtained by setting

$$\|x_1\omega_1 + \cdots + x_n\omega_n\| := \max_i |x_i|.$$

It may be worth mentioning that the above norm induces the "product topology" on $E$. Indeed, once a basis $\omega_1, \ldots, \omega_n$ is fixed, there is a canonical isomorphism from $E$ onto the vector space $K^n$. This isomorphism is clearly a homeomorphism when $E$ is endowed with the topology induced by this "max-norm", and $K^n$ with the product topology, where we take on $K$ the topology induced by the absolute value $|\ |$. Observe also that if $K$ is complete with respect to $|\ |$, then $E$ is complete with respect to the max-norm.

In case $E$ is a field extension of $K$, every absolute value $|\ |'$ of $E$ that restricts to $|\ |$ on $K$ is a norm of $E$ compatible with $|\ |$. If $E$ has finite degree over $K$ and $K$ is complete with respect to $|\ |$, the next proposition will imply that up to equivalence of norms (and hence up to dependence as absolute values, by Proposition 1.1.2), $E$ admits only one absolute value $|\ |'$ restricting to $|\ |$ on $K$. Moreover, $E$ is complete with respect to $|\ |'$.

**Proposition 1.2.2.** *Let $K$ be a field complete with respect to a non-trivial absolute value $|\ |$. Then every two norms (compatible with $|\ |$) of a finite dimensional $K$-vector space $E$ are equivalent.*

*Proof.* We shall prove that any such norm on $E$ is equivalent to the max-norm of the previous example. This will be done by induction on the dimension $n$ of the $K$-vector space $E$. For $n = 1$ the statement is obvious. Assume the proposition is proved for $n-1$, $n \geq 2$. One inequality is very simple to prove. Fix a basis $\omega_1, \ldots, \omega_n$ of $E$ over $K$, and for $\xi = x_1\omega_1 + \cdots + x_n\omega_n \in E$, denote

$$\|\xi\|_{\max} = \max_i |x_i| \ .$$

Then

$$\|\xi\| \leq \sum_{1 \leq i \leq n} |x_i| \|\omega_i\| \leq C\|\xi\|_{\max} \quad \text{for} \quad C = n \max_i \|\omega_i\|$$

We must now prove that there exists a number $C' > 0$ such that for all $\xi \in E$,

$$\|\xi\|_{\max} \leq C'\|\xi\| \ .$$

Suppose no such number exists. Then, for every positive integer $m$ there exists $\xi \in E$ such that

$$\|\xi\|_{\max} > m\|\xi\| \ . \tag{1.2.2}$$

Let $j$ be such that

$$|x_j| = \max_{1 \leq i \leq n} |x_i| \ .$$

Letting $\xi_m = x_j^{-1}\xi$, we get $\|\xi_m\|_{\max} = 1$ and thus $\|\xi_m\| < 1/m$, by (1.2.2).

For every $m \geq 1$, one of the components of $\xi_m$ equals 1. Thus there must be an infinite subset $T$ of $\mathbb{N}$ and a fixed number $j$ such that the $j$-th component of $\xi_m$ equals 1 for all $m \in T$. We fix this number $j$ from now until the end of the proof.

Consider the subspace $E_1$ of $E$ consisting of all vectors whose $j$-th coordinate is equal to 0, equipped with the norm induced by $\| \ \|$. By induction, the restrictions of $\| \ \|$ and max-norm $\| \ \|_{\max}$ to $E_1$ are equivalent. In particular, a sequence of elements of $E_1$ converges to $\zeta \in E_1$ with respect to $\| \ \|_{\max}$ if and only if it converges to $\zeta$ with respect to $\| \ \|$.

For each $m \in T$ we can write $\xi_m = \omega_j + \zeta_m$, for some $\zeta_m \in E_1$. Now, for every $\varepsilon > 0$, take $N \in \mathbb{N}$ such that $2/N < \varepsilon$. If $m, n \geq N$, $m, n \in T$, then

$$\|\zeta_m - \zeta_n\| = \|\zeta_m + \omega_j - \omega_j - \zeta_n\| \leq \|\xi_m - \xi_n\| \leq \|\xi_m\| + \|\xi_n\| < \frac{1}{m} + \frac{1}{n} \leq \frac{2}{N} < \varepsilon \ .$$

Consequently, $(\zeta_m)_{m \in T}$, is a Cauchy sequence with respect to the restriction of $\| \ \|$ to $E_1$. From the induction hypothesis, it follows that this sequence is also a Cauchy sequence with respect to the max-norm. Since $E_1$ is complete with respect to the max-norm, this sequence converges to some $\zeta \in E_1$ (with respect to the max-norm).

The choice of $T$ implies

$$\|\omega_j + \zeta_m\| < 1/m \ ,$$

for each $m \in T$.

Since the restrictions of $\| \ \|$ and the max-norm to $E_1$ are equivalent,

$$\|\zeta_m - \zeta\| \leq C \|\zeta_m - \zeta\|_{\max} \ ,$$

for some number $C > 0$. Therefore,

$$\|\omega_j + \zeta\| \leq \|\omega_j + \zeta_m\| + \|\zeta - \zeta_m\| \leq \frac{1}{m} + C \|\zeta_m - \zeta\|_{\max} \ .$$

Letting $m \in T$ go to infinity, the right-hand side of the preceding inequality tends to 0. Hence $\omega_j + \zeta = 0$. But, this cannot occur, because $\zeta \in E_1$ has the $j$-th coordinate equal to 0 and $\omega_1, \ldots, \omega_n$ is a basis of $E$ over $K$. This contradiction finishes the proof of the proposition. □

**Theorem 1.2.3.** *Let $K$ be a field containing $\mathbb{R}$ and having an absolute value that induces the ordinary one on $\mathbb{R}$. Then $K = \mathbb{R}$ or $K = \mathbb{C}$.*

In particular, the only fields complete with respect to an archimedean absolute value $| \ |$ are (up to isomorphism) $\mathbb{R}$ and $\mathbb{C}$ with $| \ |$ dependent on the ordinary absolute value.

This theorem is a consequence of the following proposition:

**Proposition 1.2.4.** (Gelfand-Mazur) *Let $A$ be a commutative algebra with an identity element 1 over the real numbers. Suppose that $A$ has a norm compatible with the absolute value of $\mathbb{R}$ satisfying*

$$\|1\| = 1 \quad \textit{and} \quad \|xy\| \leq \|x\| \|y\|$$

*for all $x, y \in A$. Moreover, assume that $A$ contains an element $j$ such that $j^2 = -1$, and let $\mathbb{C} = \mathbb{R} + j\mathbb{R} \subseteq A$ (identifying $\mathbb{R} \cdot 1$ with $\mathbb{R}$). Then for every $x_0 \in A \setminus \{0\}$, there exists an element $c \in \mathbb{C}$ such that $x_0 - c$ is not invertible in $A$.*

*Proof.* Suppose that $x_0 - z$ is invertible for all $z \in \mathbb{C}$. The map $f : \mathbb{C} \longrightarrow A$, $z \mapsto (x_0 - z)^{-1}$, is then well defined. Moreover, we shall see that taking inverses is a continuous operation on the group of units of $A$, from which it will follow that $f$ is continuous.

In order to show that $x \mapsto x^{-1}$ is continuous on the group of units of $A$, note that for any units $a$ and $x$ in $A$,

$$\|x^{-1} - a^{-1}\| = \|(a - x)a^{-1}x^{-1}\| \leq \|x - a\| \, \|a^{-1}\| \, \|x^{-1}\| \, .$$

Thus it remains to show that $\|x^{-1}\|$ is bounded as $x$ varies through units near $a$. Let $\|a^{-1}\| \, \|x - a\| \leq \frac{1}{2}$, and set $w = a^{-1}(x - a)$. Then clearly $\|w\| \leq \frac{1}{2}$. Hence we get

$$\left\| \frac{1}{1+w} \right\| = \left\| 1 - \frac{w}{1+w} \right\| \leq 1 + \|w\| \left\| \frac{1}{1+w} \right\| \leq 1 + \frac{1}{2} \left\| \frac{1}{1+w} \right\| \, .$$

This implies $\|(1 + w)^{-1}\| \leq 2$. Thus finally we get

$$\|x^{-1}\| = \|a^{-1}(1 + w)^{-1}\| \leq 2\|a^{-1}\| \, .$$

Back to the proof of the proposition, observe that for $0 \neq z \in \mathbb{C}$,

$$f(z) = \frac{1}{z} \left( \frac{1}{x_0/z - 1} \right) \, .$$

Since $z^{-1}$ and $x_0 z^{-1}$ approach 0 when $z$ goes to infinity in $\mathbb{C}$, it follows that $f(z) \to 0$ when $z \to \infty$. On the other hand, the map $z \mapsto \|f(z)\|$ is continuous, being the composition of two continuous maps. Consequently, $\|f(z)\| \to 0$ when $z \to \infty$. Hence this map may be considered as a real valued continuous map on the one-point compactification $\widetilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ of $\mathbb{C}$. Hence $\|f\|$ has a maximum $M \in \mathbb{R}$, $M > 0$. Let $D$ be the set of elements $z \in \mathbb{C}$ such that $\|f(z)\| = M$. $D$ is a non-empty, bounded, and closed subset of $\mathbb{C}$. We shall prove that it is also open, a contradiction.

For $z_0 \in D$ we shall see that if $r > 0$ is a sufficiently small real number, then all points in the open ball of center $z_0$ and radius $r$ lie in $D$.

To this end, write $y = x_0 - z_0$, and consider the sum

$$S(n) = \frac{1}{n} \sum_{j=1}^{n} \frac{1}{y + \varsigma^j r} \, ,$$

where $\varsigma \in \mathbb{C}$ is a primitive $n$-th root of unity. Let

$$h(X) = X^n - r^n = \prod_{j=1}^{n} (X - \varsigma^j r) \ ,$$

whence

$$\frac{h'(X)}{h(X)} = \frac{nX^{n-1}}{X^n - r^n} = \sum_{j=1}^{n} \frac{1}{X - \varsigma^j r} \ ,$$

where $h'(X)$ is the formal derivative of the polynomial $h(X)$. Dividing by $n$ and replacing every occurrence of $X$ by $y$, we obtain

$$\frac{1}{y - r(r/y)^{n-1}} = S(n) \ .$$

Thus $f(z_0 + r(r/y)^{n-1}) = S(n)$. If $r < \|y^{-1}\|^{-1}$, then

$$\lim_{n\to\infty} (z_0 + r(r/y)^{n-1}) = z_0$$

and so

$$\lim_{n\to\infty} \|S(n)\| = \lim_{n\to\infty} \|f(z_0 + r(r/y)^{n-1})\| = \|f(z_0)\| = M \ ,$$

by the continuity of $f$.

We now claim that every $z \in \mathbb{C}$ such that $\|z_0 - z\| < r$ lies in $D$. This inequality means that $z$ can be written in the form $z_0 + cs$, where $c$ is a complex number of absolute value 1, and $0 < s < r$ is real. If the claim were false, then there would exist such $c$ and $s$ for which $\|f(z)\| = \|f(z_0 + cs)\| < M$. From this we shall obtain a contradiction.

Let $\mathcal{S}$ be the circle of center $z_0$ and radius $s$. The arc $\mathcal{A} = \mathcal{S} \cap D$ is a closed subset of $\mathbb{C}$, and $z \in \mathcal{S} \setminus \mathcal{A}$. Taking $m$ points equally spaced on $\mathcal{S}$ for a sufficiently large $m$, a closed arc $\mathcal{S}_1$ of length $2s\pi/m$ is contained in $\mathcal{S} \setminus \mathcal{A}$ and $z$ lies on it. Since $\mathcal{S}_1$ is also compact, $f$ has a maximum $M_1$ on this arc. As $\mathcal{S}_1 \cap D = \emptyset$, we have that $0 < M_1 < M$. Now for every $q$, if we consider the points $z_0 + \varsigma^j s$, $1 \le j \le mq$, we have $q$ of them in the arc $\mathcal{S}_1$. We can rewrite $S(mq)$ in the form:

$$S(mq) = \frac{1}{mq} \left( \sum_{\mathrm{I}} \frac{1}{y + \varsigma^j s} + \sum_{\mathrm{II}} \frac{1}{y + \varsigma^j s} \right) \ ,$$

where the first sum is taken over those roots of unity $\varsigma^j$ corresponding to the points lying in $\mathcal{S}_1$, and the second sum is taken over the others.

Each term in the second sum has norm $\le M$, because $M$ is the maximum. Hence we obtain

$$\begin{aligned} \|S(mq)\| &\le \frac{1}{mq} \left( \left\| \sum_{\mathrm{I}} \frac{1}{y + \varsigma^j s} \right\| + \left\| \sum_{\mathrm{II}} \frac{1}{y + \varsigma^j s} \right\| \right) \\ &\le \frac{1}{mq} (qM_1 + (mq - q)M) \\ &\le M - \frac{M - M_1}{m} = M' < M \ . \end{aligned}$$

Thus $\|S(mq)\| \leq M'$ for every $q$. This contradicts the fact that the limit of $\|S(n)\|$ is equal to $M$. □

*Proof of Theorem 1.2.3.* We apply Proposition 1.2.4 to the $\mathbb{R}$-algebra $K$, and let the given absolute value serve as norm. If $K$ contains $\mathbb{C}$, then $K = \mathbb{C}$, because every element of $K$ is invertible.

If $K$ does not contain $\mathbb{C}$, let $L = K(j)$, where $j^2 = -1$. Define a norm on $L$ by putting $\|x + yj\| = |x| + |y|$ for $x, y \in K$. This clearly makes $L$ a normed $\mathbb{R}$-algebra. Moreover, by standard calculations one proves that $\|1\| = 1$ and $\|zz'\| \leq \|z\|\|z'\|$. Now, applying Proposition 1.2.4 to $A = L$, we obtain $L = \mathbb{C}$ as before. Thus $K$ must be $\mathbb{R}$. □

## 1.3 Non-Archimedean Complete Fields

Since the trivial absolute value makes any field complete, we assume in this section that $|\ |$ is a non-trivial, non-archimedean absolute value on the field $K$.

In Chap. 2 we shall generalize the notion of a non-archimedean absolute value. For this generalization it is more convenient to use the so-called "additive" presentation of the absolute value $|\ |$. One simply defines

$$v(x) := -\ln |x| \ .$$

In the case of the $p$-adic absolute value $|\ |_p$ on $\mathbb{Q}$, we obtain from (1.1.3)

$$v_p\Big(p^\nu \frac{m}{n}\Big) = \nu \ . \tag{1.3.1}$$

$v_p$ is called the *p-adic valuation* on $\mathbb{Q}$. We proceed similarly in (1.1.4). Note that in case $k = \mathbb{C}$ and $p = X$, $v_p$ of a rational function $\varrho$ just gives the "order" of $\varrho$ at 0, i.e., if $v_p(\varrho) = \nu > 0$, then $\varrho$ has a zero of order $\nu$ at 0, and if $v_p(\varrho) = \nu < 0$, then $\varrho$ has a pole of order $\nu$ at 0.

Using the additive notation, the axioms of a non-archimedean absolute value

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}$$

now read as follows for all $x, y \in K$:

$$\begin{aligned} &(1)\ \ v(x) \in \mathbb{R} \text{ for } x \neq 0, \text{ and } v(0) = \infty \\ &(2)\ \ v(xy) = v(x) + v(y) \\ &(3)\ \ v(x+y) \geq \min\{v(x), v(y)\} \ . \end{aligned} \tag{1.3.2}$$

Two observations are important here. First we note that only the additive structure of $\mathbb{R}$ together with the ordering on $\mathbb{R}$ is used. In the next chapter we shall therefore generalize (1.3.2) by requiring only that $v$ takes its values

in a given ordered abelian group. Secondly, we note that $\infty$ is a symbol (the value of 0) that satisfies, for all $\gamma \in \mathbb{R}$, the following axiom:

$$\infty = \infty + \infty = \gamma + \infty = \infty + \gamma \tag{1.3.3}$$

For the rest of this section, $v$ will continue to denote a non-archimedean absolute value. After making the generalization in Chap. 2, $v$ will then be called a "valuation of rank 1."

Note that for $v$ the trivial absolute value, $v$ would take only the value 0 in $\mathbb{R}$.

Now let us assume that $v$ is a non-archimedean absolute value on $K$, i.e., $v$ satisfies (1.3.2). Then the set

$$\mathcal{O}_v := \{\, x \in K \mid v(x) \geq 0 \,\}$$

is a subring of $K$. Indeed, for all $x, y \in \mathcal{O}_v$ we have

$$v(x \pm y) \geq \min\{v(x), v(\pm y)\} \geq 0$$

and

$$v(xy) = v(x) + v(y) \geq 0\ .$$

Hence $x \pm y, xy \in \mathcal{O}_v$. (Recall that $|-y| = |y|$.) From $v(x^{-1}) = -v(x)$ (recall $|x^{-1}| = |x|^{-1}$), we find that $x$ is a unit in $\mathcal{O}_v$ if and only if $v(x) = 0$, and that for every $x \in K$, either $x$ or $x^{-1}$ or both lie in $\mathcal{O}_v$. A subring $\mathcal{O}$ of $K$ satisfying

$$x \in \mathcal{O} \ \text{ or } \ x^{-1} \in \mathcal{O}$$

for all $x \in K^\times$ is called a *valuation ring* of $K$. Thus $\mathcal{O}_v$ is a valuation ring of $K$. Moreover, one easily sees that

$$\mathcal{M}_v := \{\, x \in K \mid v(x) > 0 \,\}$$

is an ideal of $\mathcal{O}_v$. Since $\mathcal{M}_v$ consists exactly of the non-units of $\mathcal{O}_v$, $\mathcal{M}_v$ is a maximal ideal, and in fact the only maximal ideal of $\mathcal{O}_v$. Thus $\mathcal{O}_v$ is a local ring. Its residue class field

$$\overline{K}_v := \mathcal{O}_v/\mathcal{M}_v$$

is called the *residue class field* of $v$. The residue class of $a \in \mathcal{O}_v$ is denoted by $\overline{a}$. Note that $v$ is trivial if and only if $\mathcal{O}_v = K$, and hence also $\overline{K}_v = K$. The group $v(K^\times)$ will be called the *value group* of $v$.

Next, let us determine the valuation ring, the maximal ideal and the residue class field in the concrete case $K = \mathbb{Q}$ and $v = v_p$, the $p$-adic valuation at the beginning of this section. From definition (1.3.1) we easily see that

$$\mathcal{O}_{v_p} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \text{ not divisible by } p \right\}$$
$$\mathcal{M}_{v_p} = \left\{ \frac{pa}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \text{ not divisible by } p \right\}\ .$$

Clearly $\mathcal{O}_{v_p}$ is the localization $\mathbb{Z}_{(p)}$ of the ring $\mathbb{Z}$ at the prime ideal $(p) = p\mathbb{Z}$, and $\mathcal{M}_{v_p}$ is $p\mathbb{Z}_{(p)}$. Thus the residue class field $\overline{K}_{v_p}$ is isomorphic to the finite prime field $\mathbb{F}_p$.

Similarly, for the example in (1.1.4), we get for the valuation ring the localization $k[X]_{(p)}$ of $k[X]$ at the prime ideal $(p) = pk[X]$; $pk[X]_{(p)}$ is the maximal ideal, and the residue class field is canonically isomorphic to $k[X]/(p)$.

So far we have not made use of the fact that $v(K)$ is a subgroup of the additive reals. The next theorem, however, heavily depends on that fact. Before we come to the theorem, let us note the following, frequently used implication:

$$v(x) < v(y) \text{ implies } \ v(x+y) = v(x)\ . \tag{1.3.4}$$

For if we had $v(x+y) > v(x)$, then we find

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

a contradiction.

Let us also recall that for $b \in \mathcal{O}_v$, we have

$$\overline{b} = 0 \text{ if and only if } v(b) > 0\ ,$$
$$\overline{b} \neq 0 \text{ if and only if } v(b) = 0\ .$$

These little facts are important when making computations with valuations, but they may cause some confusion at the beginning.

Now we come to an important property of a field $K$ complete with respect to a (non-trivial) non-archimedean absolute value $v$. This theorem is widely known as *Hensel's Lemma*.

**Theorem 1.3.1.** (Hensel's Lemma) *Let $K$ be a field complete with respect to a non-archimedean absolute value $v$. Let $f \in \mathcal{O}_v[X]$ be a polynomial, and let $a_0 \in \mathcal{O}_v$ be such that $v(f(a_0)) > 2v(f'(a_0))$. Then there exists some $a \in \mathcal{O}_v$ with $f(a) = 0$ and $v(a_0 - a) > v(f'(a_0))$.*

*Proof.* The natural way to reach the conclusions of the theorem is to construct a suitable Cauchy sequence which must converge to a root $a$ of $f$ (recall that every polynomial $f$ is a continuous map).

Let $b_0 = f'(a_0)$, and choose $\varepsilon > 0$ so that

$$v(f(a_0)) \geq v(b_0^2) + \varepsilon\ .$$

Then $f(a_0) = b_0^2 c_0$, where $c_0 = f(a_0)/b_0^2 \in K$ and $v(c_0) \geq \varepsilon$. Set $a_1 := a_0 - b_0 c_0$. Using the fact that $f$ is a polynomial and $a_0, b_0, c_0 \in \mathcal{O}_v$, we find $d_0 \in \mathcal{O}_v$ such that

$$f(a_1) = f(a_0 - b_0 c_0) = f(a_0) - b_0 c_0 f'(a_0) + b_0^2 c_0^2 d_0 = b_0^2 c_0^2 d_0\ .$$

Hence

$$v(f(a_1)) \geq v(b_0^2) + 2\varepsilon \ . \tag{1.3.5}$$

Applying the same procedure to $f'$, it follows that

$$\begin{aligned} f'(a_1) &= f'(a_0) - b_0 c_0 b, \text{ for some } b \in \mathcal{O}_v \\ &= b_0(1 - c_0 b) =: b_1 \ . \end{aligned}$$

Then $v(b_1) = v(b_0)$, since by (1.3.4) $v(1 - c_0 b) = 0$. Therefore, (1.3.5) implies $f(a_1) = b_1^2 c_1$, where $c_1 \in K$ and $v(c_1) \geq 2\varepsilon$. By repeating "verbatim" the above arguments with $\varepsilon$, $b_0$ and $a_1$ replaced by $2\varepsilon$, $b_1$ and $a_2 = a_1 - b_1 c_1$, respectively, we get $f'(a_2) = b_2$, for some $b_2$ such that

$$v(b_2) = v(b_0), \quad \text{and} \quad f(a_2) = b_2^2 c_2, \text{ for some } c_2 \text{ with } v(c_2) \geq 4\varepsilon \ .$$

Iterating this process we get a sequence $a_{n+1} = a_n - b_n c_n$, where

$$\begin{aligned} f'(a_{n+1}) &= b_{n+1} & v(b_{n+1}) &= v(b_0) \\ f(a_{n+1}) &= b_{n+1}^2 c_{n+1} & v(c_{n+1}) &\geq 2^{n+1}\varepsilon \ . \end{aligned}$$

Since $2^n\varepsilon \to \infty$ as $n \to \infty$, the sequence $(a_n)_{n\in\mathbb{N}}$ is Cauchy: for $m \leq n$,

$$\begin{aligned} v(a_n - a_m) &= v\left(\sum_{i=m}^{n-1}(a_{i+1} - a_i)\right) \\ &\geq \min_{m\leq i<n}\{v(a_{i+1} - a_i)\} \\ &\geq v(b_0) + 2^m\varepsilon \ . \end{aligned} \tag{1.3.6}$$

Let

$$a = \lim_{n\to\infty} a_n \ .$$

Recalling that polynomials are continuous maps, we see that

$$f(a) = \lim_{n\to\infty} f(a_n) \ ,$$

and $(b_n)_{n\in\mathbb{N}}$ is also a Cauchy sequence. Moreover

$$f'(a) = \lim_{n\to\infty} f'(a_n) = \lim_{n\to\infty} b_n \ .$$

Since $v(f(a_n)) = v(b_0^2) + v(c_n) \geq 2^n\varepsilon$ for every $n \in \mathbb{N}$, the first limit is given the value $\infty$; i.e., $f(a) = 0$.

From the other limit we can deduce that $v(f'(a)) = v(b_0)$. In fact, since $v(f(a_0)) > 2v(b_0)$, we get $b_0 \neq 0$. Then, for $\delta > v(b_0) \neq \infty$, there is some $n$ such that

$$v(f'(a - b_n)) > \delta > v(b_0) = v(b_n) \ .$$

By (1.3.4), this inequality implies $v(f'(a)) = v(b_n) = v(b_0)$, as required.

Furthermore, it follows from (1.3.6) that $v(a_n - a_0) \geq v(b_0) + \varepsilon$. Therefore,

$$v(a - a_0) = v((a - a_n) + (a_n - a_0)) \geq v(b_0) + \varepsilon \ ,$$

for a sufficiently large $n$. Consequently $v(a - a_0) > v(b_0) = v(f'(a))$, as desired. □

For a polynomial $f \in \mathcal{O}_v[X]$ written as

$$f = c_0 + c_1 X + \cdots + c_n X^n \,,$$

we call

$$\bar{f} = \overline{c}_0 + \overline{c}_1 X + \cdots \overline{c}_n X^n$$

the residue polynomial of $f$.

The next corollary is an easy consequence of Theorem 1.3.1.

**Corollary 1.3.2.** *Let $K$, $v$ be as in Theorem* 1.3.1. *If $f \in \mathcal{O}_v[X]$ has a simple zero $\overline{a}_0$ in the residue class field $\overline{K}_v$, i.e., $\overline{f}(\overline{a}_0) = 0$ and $\overline{f}'(\overline{a}_0) \neq 0$, then $f$ has a zero $a \in \mathcal{O}_v$ such that $\overline{a} = \overline{a}_0$.*

The proof of Theorem 1.3.1 clearly shows that under the assumption of Theorem 1.3.1 (or of Corollary 1.3.2), the sequence $(f(a_n))_{n\in\mathbb{N}}$ converges to 0. At this point, essential use is made of the fact that $v(K^\times)$ is a subgroup of the additive reals. Thus even without the completeness of $K$, we could still notice:

*Remark 1.3.3.* Let $v$ be a non-archimedean absolute value on $K$. Then for every $f \in \mathcal{O}_v[X]$, if $\overline{f}$ has a simple zero in $\overline{K}_v$, then $f(K)$ approximates 0.

As we shall see, for the generalizations considered in Chap. 2 this need no longer be true.

Now consider the completion $\big(\widehat{K}, \widehat{v}\big)$ of the field with respect to a non-archimedean absolute value $v$ as stated in Theorem 1.1.4, but now using the additive notation for absolute values. The density of $K$ in $\widehat{K}$ has the following important consequence.

**Theorem 1.3.4.** *Denote by $\mathcal{O}_{\widehat{v}}$, $\overline{K}_{\widehat{v}}$ and $\mathcal{O}_v$, $\overline{K}_v$ the valuation ring and the residue class field of $\widehat{v}$ and $v$, respectively. Then the residue class fields $\overline{K}_v$ and $\overline{K}_{\widehat{v}}$, as well as the groups $v(K^\times)$ and $\widehat{v}\big(\widehat{K}^\times\big)$, are canonically isomorphic.*

*Proof.* It follows from the constructions that $\mathcal{O}_{\widehat{v}} \cap K = \mathcal{O}_v$ and $\mathcal{M}_{\widehat{v}} \cap \mathcal{O}_v = \mathcal{M}_v$, where $\mathcal{M}_{\widehat{v}}$ and $\mathcal{M}_v$ are the respective maximal ideals. Thus the map that sends the residue class of $a \in \mathcal{O}_v$ to the residue class $\overline{a} \in \mathcal{O}_{\widehat{v}}/\mathcal{M}_{\widehat{v}}$ is well defined; and it is clearly a ring homomorphism. It remains to be seen that it is surjective. For every $x \in \mathcal{O}_{\widehat{v}}$, the set $x + \mathcal{M}_{\widehat{v}}$ is an open neighbourhood of $x$. It consists of all elements $z$ such that $\widehat{v}(z-x) > 0$, or $\widehat{|z-x|} < 1$ in terms of the absolute value. Thus the set $(x+\mathcal{M}_{\widehat{v}}) \cap K$ is non-empty, by the density property. Hence the residue class of $y \in (x + \mathcal{M}_{\widehat{v}}) \cap K$ is sent by the map above to $\overline{x}$, as required.

Similarly, the map $v(K^\times) \to \widehat{v}\big(\widehat{K}^\times\big)$ sending $v(x)$ to $\widehat{v}(x)$ for every $x \in K^\times$ is an order-preserving group monomorphism. In order to show surjectivity, let $x \in \widehat{K}^\times$ be given. By the density of $K$ in $\widehat{K}$ there exists $z \in K$ with $\widehat{v}(z-x) > v(x)$, or $\widehat{|z-x|} < |x|$ in terms of the absolute value. But then $\widehat{v}(z) = v(x)$. □

Let us return to the examples in (1.1.3) (or in (1.3.1) in the additive notation) and (1.1.4). In these examples, the value group $v(K^\times)$ is the additive group $\mathbb{Z}$ of rational integers. Such an absolute value is called *discrete* (*of rank* 1, as we shall add later). Any element $\pi \in K$ with $v(\pi) = 1$ is called a *uniformizer* for $v$, or a *local parameter*.

Every element $x$ of $K^\times$ can be written as a product

$$x = u\pi^\nu ,$$

where $u$ is a unit of $\mathcal{O}_v$ and $\nu$ is from $\mathbb{Z}$. Indeed, if $\nu = v(x)$, then

$$v(x\pi^{-\nu}) = v(x) - \nu v(\pi) = 0 .$$

Thus $u = x\pi^{-\nu}$ is a unit in $\mathcal{O}_v$. In particular, the maximal ideal $\mathcal{M}_v$ is principal, generated by $\pi$. It is easy to see that every ideal of $\mathcal{O}_v$ is generated by some power $\pi^n$, with $n = 0, 1, 2, \ldots$. Hence $\mathcal{O}_v$ is factorial.

In the case of (1.3.1), the completion of $(\mathbb{Q}, v_p)$ is denoted by $\mathbb{Q}_p$, and is called the *field of p-adic numbers*. The valuation ring of $\mathbb{Q}_p$, denoted by $\mathbb{Z}_p$, is the *ring of p-adic integers*; it is the topological closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, as we shall see below. According to our previous discussion of this example, Theorem 1.3.4 implies that the residue class field of $\mathbb{Z}_p$ is $\mathbb{F}_p$. Observe also that $p$ is a local parameter for $v_p$ in both fields, $\mathbb{Q}$ and $\mathbb{Q}_p$.

If we fix $X$ as the irreducible polynomial $p$ in the example in (1.1.4), then the completion of $(k(X), v_X)$ is the field $k((X))$ of formal Laurent series over $k$, and the valuation ring is $k[[X]]$, the ring of formal power series (see below).

The last two examples above are special cases of the following more general result:

**Proposition 1.3.5.** *Let $v$ be a discrete absolute value on the field $K$, with uniformizer $\pi$. Then every element $x \in K^\times$ can be written uniquely as a convergent series*

$$x = r_\nu\pi^\nu + r_{\nu+1}\pi^{\nu+1} + r_{\nu+2}\pi^{\nu+2} + \cdots = \lim_{n\to\infty} \sum_{i=\nu}^{n} r_i\pi^i ,$$

*where $\nu = v(x)$, $r_\nu \neq 0$, and the coefficients $r_i$ are taken from a set $R \subseteq \mathcal{O}_v$ of representatives of the residue classes in the field $\overline{K}_v$ (i.e., the canonical map $\mathcal{O}_v \longrightarrow \overline{K}_v$ induces a bijection of $R$ onto $\overline{K}_v$).*

*Proof.* We proceed by induction. As observed above, $u = x\pi^{-\nu}$ is a unit in $\mathcal{O}_v$. Choose $r_\nu \in R$ such that $\overline{r}_\nu = \overline{u}$. Then clearly $v(x\pi^{-\nu} - r_\nu) > 0$ or, equivalently,

$$v(x - r_\nu\pi^\nu) > \nu(\pi^\nu) = \nu .$$

Let $x_1 = x - r_\nu\pi^\nu$ and $\mu = v(x_1) > \nu$. Then by the same argument we get $r_\mu \in R$ such that

$$v(x - (r_\nu\pi^\nu + r_\mu\pi^\mu)) = v(x_1 - r_\mu\pi^\mu) > \mu .$$

Repeating this argument and adding "zero coefficients" (i.e. a representative for zero in $\overline{K}_v$) if necessary, we obtain the existence of the "series"

$$r_\nu \pi^\nu + r_{\nu+1}\pi^{\nu+1} + \cdots \ .$$

At the same time we see that it converges to $x$.

The uniqueness of the coefficients is clear. Indeed, otherwise 0 would have a representation

$$0 = (r_m - r'_m)\pi^m + (r_{m+1} - r'_{m+1})\pi^{m+1} + \cdots$$

with $r_m \neq r'_m \in R$, and hence $\overline{r_m - r'_m} \neq \overline{0}$, for some $m \in \mathbb{N}$. Thus $v(0) = m$, a contradiction. □

Returning once more to our typical examples, any $p$-adic number $z \in \mathbb{Q}_p^\times$ has a unique representation in the form

$$z = \sum_{i=m}^{\infty} a_i p^i \ ,$$

where $m = v_p(z),\ 0 \leq a_i < p$ for every $i$, and $a_m \neq 0$. The set of representatives chosen here is then $R = \{0, \ldots, p-1\}$. If $z \in \mathbb{Z}_p$, i.e., if $v(z) \geq 0$, then $z = \sum_{i=0}^{\infty} a_i p^i = \lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i$. This shows, in particular, that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. The reader should be aware of the fact that addition of two "series" of the form $\sum_{i=m}^{\infty} a_i p^i$ is not coefficientwise, as the set $R$ is not closed under addition. As a simple example observe that (choosing $p = 7$)

$$5p^i + 4p^i = p^{i+1} + 2p^i \ .$$

For the $X$-adic valuation of $k(X)$, we can take the elements of $k$ itself as representatives of the residue class field. In this case every $z \in k((X))^\times$ has a unique representation in the form

$$z = \sum_{i=m}^{\infty} a_i X^i \ ,$$

where $v_X(z) = m \in \mathbb{Z}$ and $a_i \in k$ for every $i$. This time, addition of two such series is coefficientwise. These series are called formal Laurent series. They form a field $k((X))$, the *field of formal Laurent series*. The canonical discrete absolute value on $k((X))$ is just given by

$$v\left(\sum_{i=m}^{\infty} a_i X^i\right) = m \quad \text{if} \quad a_m \neq 0 \ .$$

Clearly its valuation ring consists of the ring $k[[X]]$ of formal power series, i.e., series of the type $\sum_{i=0}^{\infty} a_i X^i$.

# 2

# Valuations

In this chapter we introduce Krull's generalization of non-archimedean absolute values – the valuations. In Sect. 2.2 we shall give three important methods for constructing a valuation. All of them will be used in later chapters.

Every valuation induces a topology on its field $K$ of definition. As we did for absolute values, we shall give a characterization of those valuations inducing the same topology. Moreover, we shall generalize the Approximation Theorem, and also study the completion of $K$ with respect to a valuation. For valuations, however, the completion turns out not to have such good properties as the completion of absolute values. In Remark 2.4.6 we shall see that Hensel's Lemma need not always be true. This is the reason why we shall replace later the completion by the so-called "henselization".

In Appendix B we shall present a characterization of those topologies on a field $K$ that come from a valuation or an absolute value.

## 2.1 Ordered Abelian Groups – Valuations

As already explained in Sect. 1.3, we shall generalize non-archimedean absolute values $v$ on a field $K$ by relaxing the conditions on the value group $v(K^\times)$. In order to do so, let us first recall the notion of an ordered abelian group.

By an *ordered abelian group* we understand an abelian group $(\Gamma, +, 0)$, together with a binary relation $\leq$ on $\Gamma$, satisfying the following axioms:
for all $\gamma, \delta, \lambda \in \Gamma$,

$$\begin{aligned}
&(1) \quad \gamma \leq \gamma \\
&(2) \quad \gamma \leq \delta,\ \delta \leq \gamma \implies \gamma = \delta \\
&(3) \quad \gamma \leq \delta,\ \delta \leq \lambda \implies \gamma \leq \lambda \\
&(4) \quad \gamma \leq \delta \ \text{ or } \ \delta \leq \gamma \\
&(5) \quad \gamma \leq \delta \implies \gamma + \lambda \leq \delta + \lambda\,.
\end{aligned} \tag{2.1.1}$$

The first four axioms simply say that $\leq$ is a linear ordering on $\Gamma$. Axiom (5) expresses the monotonicity of addition. As usual, we shall write merely $\Gamma$ for $(\Gamma, +, 0)$.

A subgroup $\Delta$ of an ordered abelian group $\Gamma$ is called *convex* in $\Gamma$ if each $\gamma \in \Gamma$ with $0 \leq \gamma \leq \delta \in \Delta$ already belongs to $\Delta$. Clearly, the collection of all proper convex subgroups of $\Gamma$ is linearly ordered by inclusion. The order type of this collection is called the *rank* of $\Gamma$. Thus, if there are exactly $n$ proper convex subgroups of $\Gamma$, we shall say that $\Gamma$ is of rank $n$. In particular, if $\{0\}$ is the only proper convex subgroup of $\Gamma$, we say that $\Gamma$ is of rank 1.

An ordering $\leq$ of an abelian group $\Gamma$ is called *archimedean* if the following condition holds:

for all $\gamma, \varepsilon \in \Gamma$ such that $\varepsilon > 0$, there exists $n \in \mathbb{N}$ such that $\gamma \leq n\varepsilon$ .

It is clear that an archimedean ordered group has no non-trivial convex subgroup. Hence it is of rank 1. Every subgroup $\Delta$ of the additive group $(\mathbb{R}, +, 0)$ of the reals is archimedean with respect to the canonical ordering $\leq$ induced from $\mathbb{R}$. Thus $\Delta$ has rank 1, exept for $\Delta = \{0\}$. The converse to this observation is also true.

**Proposition 2.1.1.** *An ordered abelian group $\Gamma$ is of rank* 1 *if and only if it is order-isomorphic to a non-trivial subgroup of $(\mathbb{R}, +, 0)$ with the canonical ordering induced from $\mathbb{R}$.*

*Proof.* The proof will be achieved in several steps. Let us first prove that a rank-one ordered group is archimedean. Given $\varepsilon \in \Gamma$ with $\varepsilon > 0$, we shall prove that for every $\gamma \in \Gamma$, there is some $n \in \mathbb{N}$ such that $-\gamma, \gamma < n\varepsilon$.

Set $\Delta := \{\, \gamma \in \Gamma \mid \gamma, -\gamma \leq n\varepsilon \text{ for some } n \in \mathbb{N} \,\}$. Clearly, $0 \in \Delta$, and $-\gamma \in \Delta$ for every $\gamma \in \Delta$. Moreover, for $\gamma_1, \gamma_2 \in \Delta$ and $n_1, n_2 \in \mathbb{N}$ such that $\gamma_1, -\gamma_1 < n_1\varepsilon$ and $\gamma_2, -\gamma_2 < n_2\varepsilon$, it follows that $(\gamma_1 + \gamma_2), -(\gamma_1 + \gamma_2) < (n_1 + n_2)\varepsilon$. Thus $\Delta$ is a subgroup of $\Gamma$. Clearly $\Delta$ is convex, i.e., $0 \leq \gamma \leq \delta \in \Delta$ and $\gamma \in \Gamma$ imply $\gamma \in \Delta$. Since $0 \neq \varepsilon \in \Delta$, it follows from the rank-one property of $\Gamma$ that $\Delta = \Gamma$. Thus $\Gamma$ is archimedean ordered as desired.

For the rest of this proof, fix any positive element $\varepsilon \in \Gamma$.

For each $\alpha \in \Gamma$, let

$$L(\alpha) = \{\, m/n \in \mathbb{Q} \mid n > 0 \text{ and } m\varepsilon \leq n\alpha \,\} ,$$
$$U(\alpha) = \{\, m/n \in \mathbb{Q} \mid n > 0 \text{ and } m\varepsilon \geq n\alpha \,\} .$$

We shall prove that for each $\alpha \in \Gamma$, $L(\alpha) \neq \emptyset$, $U(\alpha) \neq \emptyset$, $L(\alpha) \cup U(\alpha) = \mathbb{Q}$, and, if $\beta \in L(\alpha)$ and $\beta' \in U(\alpha)$, then $\beta \leq \beta'$. Consequently, $L(\alpha)$ and $U(\alpha)$ will define a Dedekind cut in $\mathbb{Q}$.

Since $\Gamma$ is ordered, either $m\varepsilon \leq n\alpha$ or $m\varepsilon \geq n\alpha$. Therefore every $m/n \in \mathbb{Q}$ lies in $L(\alpha)$ or $U(\alpha)$. Thus $L(\alpha) \cup U(\alpha) = \mathbb{Q}$. Hence, if $L(\alpha) = \emptyset$, we would have $U(\alpha) = \mathbb{Q}$ and $m\varepsilon \leq \alpha$ for all $m \in \mathbb{Z}$, which is impossible since $\Gamma$ is archimedean. Similarly we can prove $U(\alpha) \neq \emptyset$. Finally, $m\varepsilon \leq n\alpha$ and $m'\varepsilon \geq$

$n'\alpha$ together imply $mn'\varepsilon \leq n'n\alpha = nn'\alpha \leq nm'\varepsilon$. Therefore $mn' \leq nm'$, since $\varepsilon > 0$. Hence $m/n \leq m'/n'$, as required.

Consequently, there is a mapping $\alpha \mapsto r(\alpha)$ from $\Gamma$ into the additive group $(\mathbb{R}, +, 0)$, where $r(\alpha)$ is the real number corresponding to the Dedekind cut $L(\alpha)$, $U(\alpha)$. Clearly, $\alpha \leq \beta$ implies $r(\alpha) \leq r(\beta)$. We now prove that $r$ is a group monomorphism. For $\alpha, \beta \in \Gamma$ let $m/n \in L(\alpha)$ and $m'/n' \in L(\beta)$. By modifying $m$ and $m'$ conveniently, we may assume $n' = n$. Since $m\varepsilon \leq n\alpha$ and $m'\varepsilon \leq n\beta$, $(m + m')\varepsilon \leq n(\alpha + \beta)$ and so $(m + m')/n \in L(\alpha + \beta)$. Thus $r(\alpha+\beta) \geq r(\alpha)+r(\beta)$. Similarly, one proves $U(\alpha)+U(\beta) \subseteq U(\alpha+\beta)$. Since the last inclusion implies $r(\alpha+\beta) \leq r(\alpha)+r(\beta)$, the equality $r(\alpha+\beta) = r(\alpha)+r(\beta)$ holds. Therefore $r$ is a group homomorphism.

To finish the proof it remains only to show that the kernel of $r$ is trivial. If $r(\alpha) = 0$, then for any positive integer $n$ it follows that $-1/n \in L(\alpha)$ and $1/n \in U(\alpha)$. Hence $-\varepsilon \leq n\alpha \leq \varepsilon$ for all $n > 0$. Because the group $\Gamma$ is archimedean, this implies $\alpha = 0$. □

Let $\Gamma$ be an ordered abelian group and $\Delta \subseteq \Gamma$ a convex subgroup. Then the quotient group $\Gamma/\Delta$ can also be made an ordered group. Indeed, let $\gamma + \Delta$ and $\gamma' + \Delta$ be two different cosets. We can order them by defining

$$\gamma + \Delta < \gamma' + \Delta \text{ iff } \gamma < \gamma' .$$

One easily checks that this definition is independent of the representatives $\gamma$ and $\gamma'$, and gives an ordering on $\Gamma/\Delta$. We then take

$$\gamma + \Delta \leq \gamma' + \Delta \quad \text{iff} \quad \gamma + \Delta = \gamma' + \Delta \text{ or } \gamma + \Delta < \gamma' + \Delta .$$

If $\Gamma$ and $\Delta$ are two ordered abelian groups, we can order the direct product *lexicographically* by taking, for $\gamma, \gamma' \in \Gamma$ and $\delta, \delta' \in \Delta$,

$$(\gamma, \delta) \leq (\gamma', \delta') \quad \text{iff} \quad \gamma < \gamma' \text{ or } (\gamma = \gamma' \text{ and } \delta \leq \delta') .$$

Clearly $\{0\} \times \Delta$ becomes a convex subgroup of $\Gamma \times \Delta$, order-isomorphic to $\Delta$.

The additive group of the rational integers $\mathbb{Z}$ is ordered of rank 1. The lexicographic product $\mathbb{Z} \times \mathbb{Z}$, or more generally $\mathbb{Z} \times \cdots \times \mathbb{Z}$, $n$-times, is of rank 2, respectively $n$. We may give, however, the direct product $\mathbb{Z} \times \mathbb{Z}$ another ordering that makes it a rank 1 ordered abelian group. Indeed, we may just identify $\mathbb{Z} \times \mathbb{Z}$ with the subgroup $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ of the additive reals and take the ordering induced from $\mathbb{R}$.

With respect to the lexicographic ordering, $\mathbb{Z} \times \mathbb{Z}$ is *discrete*[1], i.e., an ordered abelian group that admits a minimal positive element, with respect to the ordering induced from $\mathbb{R}$, $\mathbb{Z} \times \mathbb{Z}$ is densely ordered.

Now, after this short excursion into ordered abelian groups, let us define valuations. For this, let $\Gamma$ be an ordered abelian group, and $\infty$ a symbol

[1] In classical valuation theory 'discrete' very often stands for 'isomorphic to $\mathbb{Z}$'. In this book, however, we use 'discrete of rank 1' in that case.

satisfying the rules (1.3.3). We then define a *valuation* $v$ on a field $K$ to be a surjective map

$$v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$$

satisfying the following axioms: for all $x, y \in K$,

$$\begin{aligned} &(1)\ \ v(x) = \infty \Longrightarrow x = 0 \\ &(2)\ \ v(xy) = v(x) + v(y) \\ &(3)\ \ v(x+y) \geq \min\{v(x), v(y)\}\ . \end{aligned} \tag{2.1.2}$$

Clearly this definition generalizes that of a non-archimedean absolute value. It should be noted, however, that surjectivity was not required in (1.3.2).

If $\Gamma = \{0\}$, we call $v$ the *trivial valuation*; if $\Gamma$ has rank 1, we call $v$ a *rank*-1 *valuation*. More generally, we define the *rank of* $v$ as the rank of the *value group* $\Gamma = v(K^\times)$.

As in Sect. 1.3, we get for all $x, y \in K$:

$$\begin{gathered} v(1) = 0, \qquad v(x^{-1}) = -v(x), \qquad v(-x) = v(x)\ , \\ v(x) < v(y) \implies v(x+y) = v(x)\ . \end{gathered}$$

Moreover, the set

$$\mathcal{O}_v := \{\, x \in K \mid v(x) \geq 0 \,\}$$

is a valuation ring of $K$, i.e., a subring of $K$ such that for all $x \in K^\times$,

$$x \in \mathcal{O}_v \quad \text{or} \quad x^{-1} \in \mathcal{O}_v\ .$$

The group $\mathcal{O}_v^\times$ of units of $\mathcal{O}_v$ is given by

$$\mathcal{O}_v^\times = \{\, x \in K \mid v(x) = 0 \,\}\ ,$$

and the set of non-units

$$\mathcal{M}_v = \{\, x \in K \mid v(x) > 0 \,\}$$

forms a maximal ideal of $\mathcal{O}_v$—in fact, the only such. As in Sect. 1.3, we call the quotient

$$\overline{K}_v := \mathcal{O}_v / \mathcal{M}_v$$

the *residue class field of* $v$.

If $K$ is a subfield of $L$, $v$ a valuation on $K$, and $w$ a valuation on $L$, we say that $w$ *extends* $v$, if $w$ *restricts* to $v$, i.e., $w|_K = v$.

As we saw above, every valuation $v$ on $K$ determines a valuation ring $\mathcal{O}_v$ in $K$. Now we show that, conversely, every valuation ring $\mathcal{O}$ in $K$ determines a valuation $v$ on $K$.

**Proposition 2.1.2.** *Let $\mathcal{O} \subseteq K$ be a valuation ring of $K$. There exists a valuation $v$ on $K$ such that $\mathcal{O} = \mathcal{O}_v$.*

*Proof.* Denote by $\mathcal{O}^\times$ the group of units of $\mathcal{O}$. The multiplicative quotient group $\Gamma = K^\times/\mathcal{O}^\times$ is an abelian group. We rewrite it additively by setting for the cosets $x\mathcal{O}^\times$ and $y\mathcal{O}^\times$:

$$x\mathcal{O}^\times + y\mathcal{O}^\times := xy\mathcal{O}^\times \ .$$

Furthermore we define a binary relation $\leq$ on $\Gamma$ by

$$x\mathcal{O}^\times \leq y\mathcal{O}^\times \quad \text{iff} \quad \frac{y}{x} \in \mathcal{O} \ .$$

It is easily checked that this turns $\Gamma$ into an ordered abelian group. The linearity (2.1.1)(4) of this ordering follows from the defining property of a valuation ring. The desired valuation is now defined by

$$v(x) = x\mathcal{O}^\times \in \Gamma$$

for $x \in K^\times$, and $v(0) = \infty$. Indeed, $v(xy) = v(x) + v(y)$ is trivial. If $v(x) \leq v(y)$, then $y/x \in \mathcal{O}$. Hence also $(x+y)/x = 1 + y/x \in \mathcal{O}$. Thus $v(x+y) \geq v(x) = \min\{v(x), v(y)\}$. Obviously,

$$\mathcal{O}_v = \{\, x \in K \mid v(x) \geq 0 \,\} = \left\{\, x \in K \;\middle|\; \frac{x}{1} \in \mathcal{O} \,\right\} = \mathcal{O}. \qquad \square$$

This proposition implies that the set $\mathcal{M} = \mathcal{O} \setminus \mathcal{O}^\times$ is an ideal of the valuation ring $\mathcal{O}$. Actually, the unique maximal one. Extending the concept of rank to valuation rings, we call rank $\Gamma$ the *rank of* $\mathcal{O}$.

The valuation ring $\mathcal{O} = K$ clearly corresponds to the trivial valuation, thus will be called the *trivial* valuation ring. Let us mention at this point that the only valuation ring of a finite field is the trivial one. In fact, for a corresponding valuation, the value group has to be a finite ordered group, hence must be $\{0\}$.

We now call two valuations $v_i : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma_i \cup \{\infty\}$ $(i = 1, 2)$ *equivalent* if they define the same valuation ring in $K$, i.e., $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$.

**Proposition 2.1.3.** *Two valuations $v_i : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma_i \cup \{\infty\}$ on $K$ are equivalent if and only if there exists an order-preserving isomorphism $\varrho : \Gamma_1 \longrightarrow \Gamma_2$ such that $\varrho \circ v_1 = v_2$.*

*Proof.* If such a $\varrho : \Gamma_1 \to \Gamma_2$ exists, then clearly $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$. Conversely, since $v_i : K^\times \longrightarrow\!\!\!\!\!\rightarrow \Gamma_i$ is a group homomorphism having kernel $\mathcal{O}_{v_i}^\times$, for $i = 1, 2$, there exists an isomorphism $\tau_i : K^\times/\mathcal{O}_{v_i}^\times \longrightarrow \Gamma_i$ satisfying $\tau_i(x\mathcal{O}_{v_i}^\times) = v_i(x)$, for $i = 1, 2$. From $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$ we get $K^\times/\mathcal{O}_{v_1}^\times = K^\times/\mathcal{O}_{v_2}^\times$. Thus $\varrho = \tau_2 \circ \tau_1^{-1}$ is the required isomorphism. $\square$

Using Proposition 2.1.3 we may say that valuation rings of $K$ correspond one-to-one to valuations of $K$ up to an order-isomorphism of the value group. In this sense, we will identify valuations with valuation rings in the rest of this book. We use whatever is more convenient.

The first non-trivial examples of valuations that we saw in Sect. 1.3 were the p-adic valuation $v_p$ on $\mathbb{Q}$ where $p$ is a rational prime, and similarly the $p$-adic valuation $v_p$ on the rational function field $k(X)$ where $p$ is any irreducible polynomial from $k[X]$, $k$ being an arbitrary field. In the second case, $v_p$ restricted to $k$ is trivial.

There is one more interesting valuation on $k[X]$, trivial on $k$. This is the *degree valuation* $v_\infty$ defined by $v_\infty(0) = \infty$ and, for non-zero polynomials $f, g \in k[X]$, by

$$v_\infty\left(\frac{f}{g}\right) = \deg g - \deg f \ .$$

One easily checks the axioms of a valuation. $\frac{f}{g}$ is a unit in the valuation ring $\mathcal{O}_{v_\infty}$ if and only if $\deg f = \deg g$. Thus if

$$f = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_0 \ ,$$

with $c_i \in k$ and $c_n \neq 0$, then we see that $f(X)/X^n$ is a unit that maps to $c_n$ in the residue class field. Hence it follows that the residue class field is exactly $k$. In fact, if $\deg f = \deg g = n$, we simply use the identity

$$\frac{f}{g} = \frac{f(X)/X^n}{g(X)/X^n} \ .$$

The next theorem shows that there are no valuations $v$ on $\mathbb{Q}$ and $k(X)$ other than the ones just mentioned, assuming in the second case triviality on $k$.

**Theorem 2.1.4.**
*(a) Every non-trivial valuation on $\mathbb{Q}$ is a p-adic valuation for some rational prime $p$.*
*(b) Every non-trivial valuation on $k(X)$, trivial on $k$, is either the degree valuation $v_\infty$ or a p-adic valuation for some irreducible polynomial $p \in k[X]$.*

*Proof.* Let $K$ be either $\mathbb{Q}$ or $k(X)$ and $v$ some non-trivial valuation on $K$. Then the valuation ring $\mathcal{O}_v$ is different from $K$. In the second case $v$ is assumed to be trivial on $k$. This means that $k \subseteq \mathcal{O}_v$. Let us simply write $\mathcal{O}$ for $\mathcal{O}_v$.

(a) Since $1 \in \mathcal{O}$, we have $\mathbb{Z} \subseteq \mathcal{O}$. As $\mathcal{O} \neq \mathbb{Q}$, at least one prime $p$ must lie in $\mathcal{M}$. If $q$ is a prime different from $p$, we have

$$ap + bq = 1 \ ,$$

for some $a, b \in \mathbb{Z}$. This shows that $q \notin \mathcal{M}$. Hence all primes $q \neq p$ are units in $\mathcal{O}$. Using the factorization of integers we therefore see that for $a, b \in \mathbb{Z}$, relatively prime, we have

$$\frac{a}{b} \in \mathcal{O} \quad \text{iff} \quad p \nmid b \ .$$

This proves that $\mathcal{O} = \mathbb{Z}_{(p)}$, i.e., $v$ is equivalent to the $p$-adic valuation $v_p$.

(b) If $X \in \mathcal{O}$, then $k[X] \subseteq \mathcal{O}$ and we can argue as in case (a) replacing $\mathbb{Z}$ by $k[X]$. If $X \notin \mathcal{O}$, then $X^{-1} \in \mathcal{M}$. In this case $v(X) < 0$ and

$$v(X^m) < v(X^n)$$

whenever $0 \leq n < m$. Since $v(a) = 0$ for every $a \in k^\times$, we get

$$v(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0) = v(a_n X^n) = nv(X)$$

in case $a_n \neq 0$. Hence the value group $v(k(X)^\times)$ is $\mathbb{Z}v(X)$. By sending $v(X)$ to $-1$, we therefore get an order-preserving isomorphism with $\mathbb{Z}$, showing that $v$ is equivalent to the degree valuation. □

## 2.2 Constructions of Valuations

In this section we shall discuss some ways to construct valuations and therefore also give more examples. We first deal with the case of a rational function field $F = K(X)$ in one variable, where $K$ already carries a valuation $v$, and we give many ways to extend $v$ to $F$. Next we shall study orderings on a field $K$, since they are naturally linked to valuations of $K$. This linkage is very useful; it works both ways. From orderings we can construct certain valuations, and conversely from valuations we can construct certain orderings. Finally we construct valuations from so-called rigid elements in a quite unusual way. This construction will be important in Sect. 5.4.

### 2.2.1 Rational Function Fields

**Theorem 2.2.1.** *Suppose $K$ is a field, $\Gamma$ is an ordered subgroup of an ordered group $\Gamma'$, $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ is a valuation, and $\gamma \in \Gamma'$. For $f = \sum_{i=0}^n a_i X^i \in K[X]$, define*

$$w(f) := \begin{cases} \infty & \text{if } f = 0\,, \\ \min\limits_{0 \leq i \leq n} \{v(a_i) + i\gamma\} & \text{otherwise}\,. \end{cases} \tag{2.2.1}$$

*For $f, g \in K[X] \setminus \{0\}$ let $w(f/g) = w(f) - w(g)$. The above equations define a valuation $w : K(X) \longrightarrow \Gamma' \cup \{\infty\}$ on $K(X)$ that extends $v$.*

*Proof.* For $f, g \in K[X] \setminus \{0\}$, let $n = \max\{\deg f, \deg g\}$, and write $f = \sum_{i=0}^n a_i X^i$ and $g = \sum_{i=0}^n b_i X^i$, $a_i, b_i \in K$. Then $f + g = \sum_{i=0}^n (a_i + b_i) X^i$, and

$$\begin{aligned} v(a_i + b_i) + i\gamma &\geq \min\{v(a_i), v(b_i)\} + i\gamma \\ &= \min\{v(a_i) + i\gamma,\ v(b_i) + i\gamma\} \\ &\geq \min\{w(f), w(g)\}\,, \quad \text{whence} \\ w(f+g) &\geq \min\{w(f), w(g)\}\,. \end{aligned} \tag{2.2.2}$$

Next we show that for $f, g \in K[X] \setminus \{0\}$, $w(fg) = w(f) + w(g)$. This time write $f = \sum_{i=0}^{n} a_i X^i$ and $g = \sum_{j=0}^{m} b_j X^j$. Then

$$fg = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j X^{i+j} = \sum_{k=0}^{n+m} \Big( \sum_{i+j=k} a_i b_j \Big) X^k = \sum_{k=0}^{n+m} c_k X^k \ ,$$

where $c_k = \sum_{i+j=k} a_i b_j$. For $i + j = k$ we have

$$v(a_i b_j) + k\gamma = v(a_i) + i\gamma + v(b_j) + j\gamma \geq w(f) + w(g) \ .$$

Thus

$$v(c_k) + k\gamma \geq \min\{ v(a_i b_j) \mid i + j = k \} + k\gamma \geq w(f) + w(g) \ .$$

Therefore

$$w(f) + w(g) \leq \min_{0 \leq k \leq n+m} \{ v(c_k) + k\gamma \} = w(fg) \ ,$$

whence

$$w(f) + w(g) \leq w(fg) \ . \tag{2.2.3}$$

To show the opposite inequality, let

$$\begin{aligned} i_0 &= \min\{ i \mid v(a_i) + i\gamma = w(f) \} \ , \\ j_0 &= \min\{ j \mid v(b_j) + j\gamma = w(g) \} \ , \\ k_0 &= i_0 + j_0 \ . \end{aligned}$$

Then

$$c_{k_0} = \sum_{i+j=k_0} a_i b_j = \Bigg( \sum_{\substack{i+j=k_0 \\ i<i_0}} a_i b_j \Bigg) + a_{i_0} b_{j_0} + \sum_{\substack{i+j=k_0 \\ i>i_0}} a_i b_j \ . \tag{2.2.4}$$

In the summation in parentheses we always have $i < i_0$, whence $v(a_i) + i\gamma > w(f)$, by the definition of $i_0$. Thus for each summand $a_i b_j$ in that summation,

$$v(a_i b_j) + k_0\gamma = \underbrace{v(a_i) + i\gamma}_{> w(f)} + \underbrace{v(b_j) + j\gamma}_{\geq w(g)} > w(f) + w(g) \ .$$

Symmetrically for the last summation in (2.2.4). Since $i > i_0$, then $j < j_0$. Whence $v(b_j) + j\gamma > w(g)$, by the definition of $j_0$. Thus for each summand $a_i b_j$ in that summation,

$$v(a_i b_j) + k_0\gamma = \underbrace{v(a_i) + i\gamma}_{\geq w(f)} + \underbrace{v(b_j) + j\gamma}_{> w(g)} > w(f) + w(g) \ .$$

Consequently,

$$v\left(\sum_{\substack{i+j=k_0\\ i<i_0}} a_i b_j\right) > w(f)+w(g)-k_0\gamma = v(a_{i_0}b_{j_0})$$

and

$$v\left(\sum_{\substack{i+j=k_0\\ i>i_0}} a_i b_j\right) > w(f)+w(g)-k_0\gamma = v(a_{i_0}b_{j_0})\ .$$

Thus $v(c_{k_0}) = v(a_{i_0}b_{j_0})$[2] and therefore $v(c_{k_0})+k_0\gamma = w(f)+w(g)$. Hence

$$w(fg) \le v(c_{k_0})+k_0\gamma = w(f)+w(g)\ ,$$

which, together with (2.2.3), gives

$$w(fg) = w(f)+w(g)\ , \tag{2.2.5}$$

as promised.

The map $w : K(X) \longrightarrow \Gamma' \cup \{\infty\}$ is well defined: if $f_1/g_1 = f_2/g_2$, then $f_1g_2 = f_2g_1$. Hence (2.2.5) implies $w(f_1)+w(g_2) = w(f_2)+w(g_1)$ and so $w(f_1)-w(g_1) = w(f_2)-w(g_2)$.

It remains to extend (2.2.2) and (2.2.5) from the case of $f, g \in K[X]\setminus\{0\}$ to the case of arbitrary elements $h_1, h_2$ of $K(X)\setminus\{0\}$. For this, let $g$ be a common denominator of $h_1$ and $h_2$: $h_i = f_i/g$, where $f_1, f_2, g \in K[X]\setminus\{0\}$. Then

$$\begin{aligned} w(h_1+h_2) &= w\left(\frac{f_1+f_2}{g}\right) = w(f_1+f_2)-w(g)\\ &\ge \min\{w(f_1),\, w(f_2)\}-w(g)\\ &= \min\{w(f_1)-w(g),\ w(f_2)-w(g)\}\\ &= \min\{w(h_1),\, w(h_2)\}\ . \end{aligned}$$

Finally,

$$\begin{aligned} w(h_1h_2) &= w\left(\frac{f_1f_2}{g^2}\right) = w(f_1f_2)-w(g^2)\\ &= w(f_1)-w(g)+w(f_2)-w(g)\\ &= w(h_1)+w(h_2)\ , \end{aligned}$$

as required. □

The valuation considered in the next corollary is commonly known as the *Gauss extension* of $v$ from $K$ to the rational function field $K(X)$.

[2] If $x_1, \dots, x_n \in K$ are such that $\min\{v(x_1), \dots, v(x_n)\}$ is assumed for a unique $i$, then $v(x_1+\cdots+x_n) = \min\{v(x_1), \dots, v(x_n)\}$.

**Corollary 2.2.2.** *Suppose $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ is a valuation on $K$. Then there is exactly one extension $w$ of $v$ to $K(X)$ such that $w(X) = 0$ and $\overline{X}$ is transcendental over $\overline{K}$. For this $w$, we have $\overline{K(X)} = \overline{K}(\overline{X})$ and $w(K(X)^\times) = \Gamma$.*

*Proof.* For the uniqueness, let $f = \sum_{i=0}^n a_i X^i \in K[X] \setminus \{0\}$. Pick $k \le n$ such that

$$v(a_k) = \min_{0 \le i \le n} v(a_i) \; .$$

Then

$$f = a_k \underbrace{\sum_{i=0}^{n} b_i X^i}_{=:\, g}, \quad \text{where } b_i = \frac{a_i}{a_k} \text{ and } v(b_i) \ge 0 \; . \tag{2.2.6}$$

Then $w(g) \ge 0$, since $w(X) = 0$. Moreover,

$$\overline{g} = \sum_{i=0}^{n} \overline{b_i}\, \overline{X}^i \ne 0 \; ,$$

since $b_k = 1$ and $\overline{X}$ is transcendental over $\overline{K}$. Therefore $g \in \mathcal{O}_w^\times$, i.e., $w(g) = 0$, whence $w(f) = v(a_k)$, i.e.,

$$w(f) = \min_{0 \le i \le n} v(a_i) \; .$$

For the existence, let $f \in K[X]$, and define $w(f)$ by (2.2.1), taking $\Gamma' = \Gamma$ and $\gamma = 0$. Then $w(X) = 0$. To see that $\overline{X}$ is transcendental, suppose $\sum_{i=0}^n \overline{a_i}\overline{X}^i = 0$, for some $a_i \in \mathcal{O}_v$. Then

$$0 < w\left(\sum_{i=0}^{n} a_i X^i\right) = \min_{0 \le i \le n} v(a_i) \; ,$$

whence $v(a_i) > 0$ for each $i$; i.e., each $\overline{a}_i = 0$.

Next, $w(K(X)^\times) = \Gamma$ is clear.

The last property to show is that $\overline{K(X)} = \overline{K}(\overline{X})$. For this, let $h \in \mathcal{O}_w^\times$, and write $h = f_1/f_2$, with $f_1, f_2 \in K[X] \setminus \{0\}$. As in 2.2.6, for each $i = 1, 2$ write $f_i = c_i g_i$, where $c_i \in K^\times$, and $g_i \in \mathcal{O}_w^\times$. Therefore $h = c\, g_1/g_2$, where $c = c_1/c_2 \in K^\times$. Also, $c \in \mathcal{O}_w^\times$, since $h \in \mathcal{O}_w^\times$. Then $\overline{h} = \overline{cg_1}/\overline{g_2} \in \overline{K}(\overline{X})$. □

**Corollary 2.2.3.** *Suppose $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ is a valuation of the field $K$, $\Gamma$ is an ordered subgroup of an ordered group $\Gamma'$, and $\gamma \in \Gamma'$ has the property:*

$$\text{if } n \in \mathbb{Z} \text{ satisfies } n\gamma \in \Gamma, \text{ then } n = 0 \; .$$

*Under these conditions, there is exactly one valuation $w$ on $K(X)$ extending $v$, with $w(X) = \gamma$. For this $w$, we have $\overline{K(X)} = \overline{K}$ and $w(K(X)^\times) = \Gamma \oplus \mathbb{Z}\gamma$ with the ordering induced from $\Gamma'$.*

*Proof.* The existence of $w$ follows from Theorem 2.2.1. To prove uniqueness, let $w$ be any such extension. Consider an $f \in K[X]$, say, $f = a_0 + a_1X + \cdots + a_nX^n$, with $a_i \in K$. Then for each $i \leq n$, $w(a_iX^i) = v(a_i) + iw(X) = v(a_i) + i\gamma$. For $i \neq j$ and $a_i \neq 0 \neq a_j$ we claim that $w(a_iX^i) \neq w(a_jX^j)$. Indeed, $v(a_i) + i\gamma = v(a_j) + j\gamma$ implies that $(i-j)\gamma = v(a_j) - v(a_i) \in \Gamma$. Whence by hypothesis $i - j = 0$, i.e., $i = j$.

Now the claim above yields

$$w(f) = \min\{w(a_0), \ldots, w(a_nX^n)\} = \min_{0\leq i\leq n} (v(a_i) + i\gamma) ,$$

which implies that $w$ is uniquely determined on $K[X]$, and hence on $K(X)$.

It is now clear that $w(K(X)^\times) = \Gamma \oplus \mathbb{Z}\gamma$; and it remains to show that $\overline{K(X)} = \overline{K}$.

First we show that every $f \in K[X] \setminus \{0\}$ is of the form $f = aX^m(1+u)$, where $a \in K^\times$, $m \in \mathbb{N}$, $u \in K(X)$, and $w(u) > 0$. For this, write $f = \sum_{i=0}^n a_iX^i$, with $a_i \in K$. We have seen above that there is exactly one $i_0$ such that $w(f) = v(a_{i_0}) + i_0\gamma = w(a_{i_0}X^{i_0})$. Therefore

$$f = a_{i_0}X^{i_0}\Bigg(1 + \underbrace{\sum_{\substack{i=0\\ i\neq i_0}}^{n} \frac{a_iX^i}{a_{i_0}X^{i_0}}}_{=:\, u}\Bigg) .$$

Observe that

$$w\left(\frac{a_iX^i}{a_{i_0}X^{i_0}}\right) = w(a_iX^i) - w(a_{i_0}X^{i_0}) > 0$$

for $i \neq i_0$, whence $w(u) > 0$.

Second, we consider any $h \in K(X) \setminus \{0\}$, and write $h = f/g$, with $f, g \in K[X] \setminus \{0\}$. Write $f = aX^m(1+u)$ and $g = bX^n(1+u')$, with $a, b \in K^\times$, $m, n \in \mathbb{N}$, and $w(u), w(u') > 0$. Then

$$h = \frac{f}{g} = \frac{a}{b}\, X^{m-n}\, \frac{1+u}{1+u'} = cX^r\Big(1 + \frac{u-u'}{1+u'}\Big) ,$$

where $c = a/b \in K^\times$ and $r = m - n \in \mathbb{Z}$. Since $w(u') > 0$, $w(1+u') = 0$; therefore $w(u - u'/1+u') > 0$. Consequently, there exists $u'' \in K(X)$ with $w(u'') > 0$ such that $h = cX^r(1+u'')$.

We now show that $\overline{K(X)} = \overline{K}$. Let $h \in \mathcal{O}_w^\times$ be written in the form $h = cX^r(1+u'')$ as described above. We then have

$$0 = w(h) = w(cX^r(1+u'')) = v(c) + r\gamma ,$$

whence $r\gamma = -v(c) \in \Gamma$. By assumption, $r = 0$. Consequently, $v(c) = 0$. Therefore $\overline{h} = \overline{c}(\overline{1} + \overline{u''}) = \overline{c} \in \overline{K}$ (since $\overline{u''} = 0$). □

### 2.2.2 Ordered Fields

Next we deal with orderings on a field $K$. An ordering $\geq$ on $K$ is a binary relation that makes the additive group of $K$ an ordered abelian group, and in addition satisfies the following: for all $x, y \in K$,

$$0 \leq x, y \implies 0 \leq xy \,.$$

A field $K$ is called *real* if it admits some ordering $\leq$. The set

$$P_{\leq} := \{\, x \in K \mid 0 \leq x \,\}$$

is called the *positive cone* of $\leq$. For a subring $R$ of $K$, we define the $\leq$-*convex hull of* $R$ *in* $K$ by

$$\mathcal{O}_R(\leq) := \{\, x \in K \mid x, -x \leq a \text{ for some } a \in R \,\} \,.$$

One easily sees that $\mathcal{O}_R(\leq)$ is a subring of $K$ containing $R$.

We say that a subring $R$ of $K$ is $\leq$-*convex* if $\mathcal{O}_R(\leq) = R$.

Clearly, $R$ is $\leq$-convex if and only if $R$ is a convex subgroup of the additive group $K$. Moreover, any $\leq$-convex subring $\mathcal{O}$ of $K$ containing 1, is a valuation ring of $K$. Indeed, let $0 < x \notin \mathcal{O}$. Then $1 < x$, and hence $0 < x^{-1} < 1$, proving that $x^{-1} \in \mathcal{O}$. If $R = \mathbb{Z}$, we simply write $\mathcal{O}(\leq)$ for $\mathcal{O}_{\mathbb{Z}}(\leq)$. The ring $\mathcal{O}(\leq)$ is the minimal $\leq$-convex subring of $K$ containing 1.

In dealing with orderings $\leq$ on $K$ it is sometimes more convenient to use their positive cones $P_{\leq}$. In fact, there is a one-to-one correspondence between orderings $\leq$ and *positive cones* $P \subseteq K$ defined by the axioms

$$\begin{aligned} &(1) \quad P + P \subseteq P, \quad P \cdot P \subseteq P \\ &(2) \quad -1 \notin P \\ &(3) \quad P \cup -P = K \end{aligned} \tag{2.2.7}$$

If $\leq$ is an ordering, then clearly $P_{\leq}$ satisfies these axioms. Conversely, if $P \subseteq K$ is a positive cone, a little exercise shows that

$$x \leq y \;\text{ iff }\; y - x \in P$$

defines an ordering on $K$ with $P_{\leq} = P$. Because of this correspondence we simply call $P$ as well an ordering. Similarly we say that a valuation ring $\mathcal{O}$ is $P$-*convex* if $\mathcal{O}$ is $\leq$-convex for the ordering $\leq$ defined by $P$.

**Proposition 2.2.4.** *Let $P$ be an ordering of $K$ and let $\mathcal{O}$ be a valuation ring of $K$ with maximal ideal $\mathcal{M}$. The following conditions are equivalent:*

*(1) $\mathcal{O}$ is $P$-convex;*
*(2) $\mathcal{M}$ is a $P$-convex subgroup of the additive group of $\mathcal{O}$;*
*(3) $\overline{P} := \{p + \mathcal{M} \mid p \in P \cap \mathcal{O}\}$ is an ordering of the residue class field $\overline{K}$ of $\mathcal{O}$;*

*(4)* $1 + \mathcal{M} \subseteq P$.

*Proof.* (1) $\Longrightarrow$ (2) For $x \in \mathcal{O}$ and $y \in \mathcal{M}$ such that $0 < x < y \in \mathcal{M}$, it follows that $0 < y^{-1} < x^{-1}$. Since $y^{-1} \notin \mathcal{O}$, also $x^{-1} \notin \mathcal{O}$. Thus $x \in \mathcal{M}$, as required.

(2) $\Longrightarrow$ (3) The only condition to check is (2) of (2.2.7). Assume that $-1+\mathcal{M} \in \overline{P}$. Then there exists $p \in P$ such that $p+1 \in \mathcal{M}$. Now $0 < 1 \leq p+1$ and the convexity of $\mathcal{M}$ imply $1 \in \mathcal{M}$, a contradiction.

(3) $\Longrightarrow$ (4) Arguing by contradiction, take $x \in \mathcal{M}$ such that $1 + x \notin P$. But then $-(1 + x) \in P \cap \mathcal{O}$ implies $-1 \in \overline{P}$, a contradiction.

(4) $\Longrightarrow$ (1) Suppose there is $0 < x < y \in \mathcal{O}$ such that $x \notin \mathcal{O}$. Then $x^{-1} \in \mathcal{M}$. Hence $-x^{-1}y \in \mathcal{M}$ and by (4), $1 - x^{-1}y \in P$. Multiplying by $x$, one gets $x - y \in P$, contradicting the assumption $x < y$. □

The next theorem is known as the *Baer-Krull Representation Theorem*. In order to formulate it, let $K$ be a field and $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ a valuation with valuation ring $\mathcal{O}$. The quotient group $\overline{\Gamma} := \Gamma/2\Gamma$ becomes, in a canonical way, an $\mathbb{F}_2$-vector space. Let $\{ \pi_i \mid i \in I \}$ be a family of elements of $K^\times$ such that $\{ \overline{v(\pi_i)} \mid i \in I \}$ is an $\mathbb{F}_2$-basis of $\overline{\Gamma}$. (Here $\overline{v(\pi_i)}$ denotes the coset $v(\pi_i) + 2\Gamma$ of $\Gamma/2\Gamma$.) Such a family is called a *quadratic system of representatives* of $K$ with respect to $v$.

**Theorem 2.2.5.** *Let $\mathrm{X}(K)$ and $\mathrm{X}\big(\overline{K}_v\big)$ denote the set of all orderings of $K$ and $\overline{K}_v$, respectively, and fix a quadratic system $\{\pi_i | i \in I\}$ of representations of $K$. Then there exists is a bijective correspondence*

$$\{ P \in \mathrm{X}(K) \mid \mathcal{O} \text{ is } P\text{-convex} \} \overset{\approx}{\longleftrightarrow} \{-1, 1\}^I \times \mathrm{X}\big(\overline{K}_v\big) \tag{2.2.8}$$

*described as follows:*

*Given an ordering $P$ on $K$ such that $\mathcal{O}$ is $P$-convex, let $\eta_P : I \to \{-1, 1\}$, where $\eta_P(i) = 1$ iff $\pi_i \in P$. Then the map $P \mapsto \big(\eta_P, \overline{P}\big)$ is the above bijection.*

*Proof.* We shall show that the above correspondence is bijective, by constructing the inverse map.

The choice of $\{ \pi_i \mid i \in I \}$ implies that for each $a \in K^\times$, there exist uniquely determined indices $i_1, \ldots, i_r \in I$ such that $\overline{v(a)} = \overline{v(\pi_{i_1})} + \cdots + \overline{v(\pi_{i_r})}$. Thus for some $b \in K$ one has $v(a) = v(\pi_{i_1}) + \cdots + v(\pi_{i_r}) + 2v(b)$. Hence there exists $u \in \mathcal{O}^\times$ for which $a = ub^2\pi_{i_1} \cdots \pi_{i_r}$. Since $b$ is determined only up to a unit, $u$, too, is determined only up to a unit square.

Now, given a mapping $\eta : I \to \{-1, 1\}$ and an ordering $Q$ on $\overline{K}_v$, define $P(\eta, Q) \subseteq K$ by $0 \in P(\eta, Q)$ and for each $a \in K^\times$:

$$a \in P(\eta, Q) \text{ if and only if } \eta(i_1) \cdots \eta(i_r)\overline{u} \in Q \, .$$

By what we said about $u$ and $i_1 \ldots, i_r$ above, $P(\eta, Q)$ is well-defined.

We have to show that $P(\eta, Q)$ is an ordering on $K$ such that $\mathcal{O}$ is $P(\eta, Q)$-convex and $\overline{P(\eta, Q)} = Q$. Take $a, a' \in P(\eta, Q)$, $a, a' \neq 0$, and write

$$a = u \ \ b^2 \ \ \pi_1^{\varepsilon_1} \cdots \pi_n^{\varepsilon_n} \ ,$$
$$a' = u'(b')^2 \pi_1^{\varepsilon'_1} \cdots \pi_n^{\varepsilon'_n} \ ,$$

where $\varepsilon_1, \ldots, \varepsilon_n, \varepsilon'_1, \ldots, \varepsilon'_n \in \{0, 1\}$.

If $v(a) \neq v(a')$, say $v(a) < v(a')$, then $v(a + a') = v(a)$. Hence $a + a' = ca$ for some $c \in \mathcal{O}^\times$. Dividing both sides of this equation by $a$, and taking the residue class, one gets $\overline{1} = \overline{c}$. Therefore $a + a' = cub^2\pi_1^{\varepsilon_1} \cdots \pi_n^{\varepsilon_n} \in P(\eta, Q)$. The case $v(a) = v(a')$ occurs only if $\varepsilon_j = \varepsilon'_j$, for every $j = 1, \ldots, n$, because $\overline{v(\pi_1)}, \ldots, \overline{v(\pi_n)}$ is an $\mathbb{F}_2$-linearly independent family of elements of $\overline{\Gamma}$. Consequently, also $b' = bu''$ with $u'' \in \mathcal{O}^\times$ and $a + a' = (u + u'(u'')^2)b^2\pi_1^{\varepsilon_1} \cdots \pi_n^{\varepsilon_n}$. Finally, $\overline{u}, \overline{u}' \in \pm Q$ implies $\overline{0} \neq \overline{u} + \overline{u'}(\overline{u''})^2 \in \pm Q$. Therefore $a + a' \in P(\eta, Q)$, by the very definition of $P(\eta, Q)$. Hence, we have already shown that $P(\eta, Q) + P(\eta, Q) \subseteq P(\eta, Q)$.

In order to prove that $P(\eta, Q)$ is closed under multiplication, we first extend $\eta$ to an $\mathbb{F}_2$-linear map from $\overline{\Gamma}$ to $\{-1, 1\}$. (This is clearly possible since $\left\{ \overline{v(\pi_i)} \;\middle|\; i \in I \right\}$ is an $\mathbb{F}_2$-basis of $\overline{\Gamma}$.) By composing

$$K^\times \xrightarrow{v} \Gamma \longrightarrow \overline{\Gamma} \xrightarrow{\eta} \{-1, 1\} \ ,$$

we have a group homomorphism $K^\times \to \{-1, 1\}$, which we shall also denote by $\eta$. Observe now that $a \in P(\eta, Q)$ if and only if $\eta(a)\overline{u} \in Q$. It follows from this that $P(\eta, Q)P(\eta, Q) \subseteq P(\eta, Q)$, as required.

It remains to show that $P(\eta, Q) \cup -P(\eta, Q) = K$ and $-1 \notin P(\eta, Q)$. Both conditions, however, are immediate by the definition of $P(\eta, Q)$.

It is also clear that $1 + \mathcal{M} \subseteq P(\eta, Q)$. Hence Proposition 2.2.4 implies that $\mathcal{O}$ is $P(\eta, Q)$-convex. Finally, if $u \in \mathcal{O}^\times \cap \overline{P(\eta, Q)}$, it follows from the very definition of $P(\eta, Q)$ that $\overline{u} \in Q$. Therefore $\overline{P(\eta, Q)} = Q$, as required.

What we have done so far shows that the ordering $P(\eta, Q)$ is sent to the pair $(\eta, Q)$ by the map (2.2.8) This proves surjectivity. Injectivity is seen as follows. If $P$ is mapped to $(\eta, Q)$ by (2.2.8), the construction of $P(\eta, Q)$ shows that $P(\eta, Q) \subseteq P$. But inclusion of two positive cones implies equality. □

An ordering $\leq$ of a field $K$ is called *archimedean* if it is an archimedean ordering of the additive group. Thus for every $\varepsilon \in K$ with $\varepsilon > 0$, every $\gamma \in K$ can be exceeded by some multiple $n\varepsilon$, with $n \in \mathbb{N}$. Since we are working with a field ordering, it clearly suffices to require this for $\varepsilon = 1$. Thus $\leq$ is archimedean on $K$ if and only if to every $\gamma \in K$ there exists $n \in \mathbb{N}$ such that $\gamma \leq n$.

The next corollary gives an interesting characterization of fields that admit a non-archimedean ordering.

**Corollary 2.2.6.** *The field $K$ admits a non-archimedean ordering if and only if $K$ carries a non-trivial valuation with a real residue class field $\overline{K}$.*

*Proof.* Assume that $\leq$ is a non-archimedean ordering of $K$. Then the valuation ring $\mathcal{O}(\leq)$ defined above is non-trivial and $\leq$-convex. Thus by Theorem 2.2.5

the positive cone $P$ of $\leq$ corresponds to the pair $(\eta_P, \overline{P})$. In particular, $\overline{K}$ admits an ordering, and thus is real.

Conversely, let $\mathcal{O}$ be a non-trivial valuation ring of $K$, and let $Q$ be an ordering of $\overline{K}$. Choosing for $\eta$ the constant map 1 yields an ordering $P$ of $K$ for which $\mathcal{O}$ is convex and such that $\eta = \eta_P$ and $Q = \overline{P}$. Clearly, the ordering $\leq$ defined by $P$ is non-archimedean as $\mathcal{O}(\leq) \subseteq \mathcal{O}$, and therefore $\mathcal{O}(\leq)$ cannot be the whole field $K$. □

As a simple consequence of this corollary we see that every valuation $v$ of a field extension $K$ of $\mathbb{R}$ (e.g., a function field over $\mathbb{R}$) with real residue class field must be trivial on $\mathbb{R}$. In fact, if $v|_{\mathbb{R}}$ were not trivial, then by the last corollary $\mathbb{R}$ would admit a non-archimedean ordering, an absurdity.

### 2.2.3 Rigid Elements

The ultrametric triangle inequality (2.1.2) (3) for a valuation $v$ on a field $K$ implies that for $x \in K^\times \setminus \mathcal{O}_v^\times$,

$$\mathcal{O}_v^\times + x\mathcal{O}_v^\times \subseteq \mathcal{O}_v^\times \cup x\mathcal{O}_v^\times \ .$$

The same 'rigidity' holds when $\mathcal{O}_v^\times$ is replaced by any subgroup $T$ of $K^\times$ with $\mathcal{O}_v^\times \subseteq T$. In fact, let $a, b \in T$ and $x \in K^\times \setminus T$. Then $v(a) \neq v(xb)$ and thus

$$v(a + xb) = \min\{v(a), v(xb)\} \ .$$

We shall now show that, conversely, subgroups of $K^\times$ with the above property may give rise to valuations. Given a subgroup $T$ of $K^\times$, any $x \in K^\times \setminus T$ will be called $T$-*rigid* if

$$T + xT \subseteq T \cup xT \ .$$

If $T = \mathcal{O}_v^\times$, then every $x \in K^\times \setminus T$ actually is $T$-rigid. We shall show that a subgroup $T \subseteq K^\times$ with 'many' $T$-rigid elements comes from some valuation. To be more precise, let us define

$$\begin{aligned} \mathsf{O}_1(T) &= \{\, x \in K \setminus T \mid 1 + x \in T \,\} \\ \mathsf{O}_2(T) &= \{\, x \in T \mid x\mathsf{O}_1(T) \subseteq \mathsf{O}_1(T) \,\} \\ \mathcal{O}(T) &= \mathsf{O}_1(T) \cup \mathsf{O}_2(T) \ . \end{aligned}$$

In the next theorem we shall see that under certain conditions on $T$, the set $\mathcal{O}(T)$ turns out to be a non-trivial valuation ring of $K$. Although the definition of $\mathcal{O}(T)$ looks quite strange and the proof of the theorem is by no means straight forward, the theorem has an important application in Sect. 5.4 where we deduce from certain assumptions on the structure of the absolute Galois group $G(K^s/K)$ of $K$ the existence of a non-trivial "henselian" valuation on $K$.

**Theorem 2.2.7.** *Fix a rational prime $p$. Let $K$ be a field and $T \subseteq K^\times$ a subgroup with $(K^\times)^p \subseteq T$ such that every element $x \in K^\times \setminus T$ is $T$-rigid.*

*(1) For $p \neq 2$, $\mathcal{O}(T)$ is a valuation ring of $K$ with $\mathcal{O}(T)^\times \subseteq T$.*
*(2) In case $p = 2$ assume also $-1 \in T$. Then there exists a subgroup $T_1$ containing $T$ such that $(T_1 : T) \leq 2$ and $\mathcal{O}(T_1)$ is a valuation ring of $K$ with $\mathcal{O}(T_1)^\times \subseteq T_1$.*

*Proof.* We simplify the notation and just write $\mathsf{O}_1$, $\mathsf{O}_2$ and $\mathcal{O} = \mathsf{O}_1 \cup \mathsf{O}_2$. Observe that, trivially $0 \in \mathsf{O}_1$ and $1 \in \mathsf{O}_2$.

First we suppose $T$ has additionally the property:

$$\text{for all } x,\, y \in \mathsf{O}_1, \quad 1 - xy \in T\,. \tag{2.2.9}$$

We then prove that $\mathcal{O}$ is the required valuation ring.

*Step 1.* $1 + \mathsf{O}_1 \subseteq \mathsf{O}_2$.

Let $x,\, y \in \mathsf{O}_1$. Since $1 + (-y)(1+y)^{-1} = (1+y)^{-1} \in T$ it follows that $-y(1+y)^{-1} \in \mathsf{O}_1$. Thus property (2.2.9) applies to $x$ and $-y(1+y)^{-1}$, i.e., $1 + xy(1+y)^{-1} \in T$. Consequently,

$$1 + (1+x)y = (1+y)\left(1 + \frac{xy}{1+y}\right) \in T\,,$$

and so $(1+x)y \in \mathsf{O}_1$, showing that $1 + x \in \mathsf{O}_2$, as contended.

*Step 2:* $\mathcal{O} \cdot \mathcal{O} \subseteq \mathcal{O}$.

By definition $\mathsf{O}_2 \cdot \mathsf{O}_1 \subseteq \mathsf{O}_1$ and $\mathsf{O}_2 \cdot \mathsf{O}_2 \subseteq \mathsf{O}_2$. It remains to be seen that $\mathsf{O}_1 \cdot \mathsf{O}_1 \subseteq \mathcal{O}$. We shall prove for $x,\, y \in \mathsf{O}_1$ that $xy \in \mathsf{O}_1$ if $xy \notin T$, and $xy \in \mathsf{O}_2$ otherwise.

Case 1: $xy \notin T$. Suppose $-x \in \mathsf{O}_1$ or $-y \in \mathsf{O}_1$ occurs for at least one of the elements $x, y$. Say $-x \in \mathsf{O}_1$. It then follows from (2.2.9) that $1 + xy = 1 - (-x)y \in T$. Thus $xy \in \mathsf{O}_1$, as desired.

We shall now prove that $-x \in \mathsf{O}_1$ or $-y \in \mathsf{O}_1$ is in fact true, and so Case 1 is done. By contradiction let us assume that $-x,\, -y \notin \mathsf{O}_1$. As $x,\, y$ are rigid, $1 - x \in xT$ and $1 - y \in yT$ (observe that $-1 \in T$). On the other hand, by (2.2.9), $1 - xy \in T$. Hence

$$1 - xy = (1-x) + x(1-y) \in T \cap (xT \cup xyT) = \emptyset\,,$$

a contradiction.

Case 2: $xy \in T$.

Observe first that for all $a \in \mathsf{O}_1$ we have that $-a(1+a)^{-1} \in \mathsf{O}_1$. In fact, $-a(1+a)^{-1} \notin T$ and $1 + (-a(1+a)^{-1}) = (1+a)^{-1} \in T$.

Since by Step 1, $1 + x \in \mathsf{O}_2$ we get $(1+x)(-y)(1+y)^{-1} \in \mathsf{O}_1$. Once again Step 1 says that $1 + y$ and $1 + (1+x)(-y)(1+y)^{-1}$ are in $\mathsf{O}_2$. Since $\mathsf{O}_2 \cdot \mathsf{O}_2 \subseteq \mathsf{O}_2$, we get

$$1 - xy = (1+y)\left(1 + (1+x)\left(\frac{-y}{1+y}\right)\right) \in \mathsf{O}_2\,.$$

Now take any $z \in \mathsf{O}_1$. As proved above, $-z(1+z)^{-1} \in \mathsf{O}_1$. Hence

$$(1-xy)(-z)(1+z)^{-1} \in \mathsf{O}_1 \ .$$

Therefore

$$1+xyz = (1+z)\left(1+(1-xy)\frac{-z}{1+z}\right) \in T \ .$$

Thus $xyz \in \mathsf{O}_1$ and $xy \in \mathsf{O}_2$, as desired.

*Step 3.* For $x \in K^\times$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. In particular, $-1 \in \mathsf{O}_2$.
Case 1. $x \notin T$. If $x \notin \mathsf{O}_1$, then $1+x \notin T$. But $x$ is $T$-rigid. Thus $1+x \in xT$. Hence $1+x^{-1} \in T$ and $x^{-1} \in \mathsf{O}_1$.
Case 2: $x \in T$. If $x \notin \mathsf{O}_2$, there exists $y \in \mathsf{O}_1$ such that $xy \notin \mathsf{O}_1$. Since $xy \notin T$, $(xy)^{-1} \in \mathsf{O}_1$, by Case 1. Thus, by Case 2 of Step 2, $x^{-1} = (xy)^{-1}y \in \mathsf{O}_2$.

*Step 4.* $1+\mathsf{O}_2 \subseteq \mathcal{O}$. More precisely, for $x \in \mathsf{O}_2$ we have $1+x \in \mathsf{O}_1$ if $1+x \notin T$, and $1+x \in \mathsf{O}_2$ otherwise.
Case 1: $1+x \notin T$. Since $-(1+x) \notin T$ and $1-(1+x) = -x \in T$, it follows that $-(1+x) \in \mathsf{O}_1$. By Step 2 and Step 3, $1+x = (-1)(-(1+x)) \in \mathsf{O}_1$ as required.
Case 2: $1+x \in T$. Observe first that $-x = (-1)x \in \mathsf{O}_2$ (Step 2 and Step 3). Moreover, we saw in the proof of Case 2 of Step 2 that for each $y \in \mathsf{O}_1$ it follows that $-y(1+y)^{-1} \in \mathsf{O}_1$. Then $(-x)\left(-y(1+y)^{-1}\right) \in \mathsf{O}_1$, and so

$$1+(1+x)y = (1+y)\left(1+(-x)\frac{-y}{1+y}\right) \in T \ .$$

Consequently, $(1+x)y \in \mathsf{O}_1$ and $1+x \in \mathsf{O}_2$, as claimed.

*Final Step.* $\mathcal{O}$ is a valuation ring of $K$ satisfying $\mathcal{O}^\times \subseteq T$, and so the result is proved in this case:

By Step 2, $\mathcal{O}\cdot\mathcal{O} \subseteq \mathcal{O}$. Since Step 3 implies $-1 \in \mathcal{O}$, it follows that $-x \in \mathcal{O}$ for every $x \in \mathcal{O}$. To prove that $\mathcal{O}$ is a subring of $K$, it remains to be seen that $\mathcal{O}+\mathcal{O} \subseteq \mathcal{O}$. Take any $x, y \in \mathcal{O}$. From Step 3, either $xy^{-1} \in \mathcal{O}$ or $yx^{-1} \in \mathcal{O}$. Say $xy^{-1} \in \mathcal{O}$. Then Step 1 and Step 4 imply $1+xy^{-1} \in \mathcal{O}$. Finally, Step 2 yields $x+y = y(1+xy^{-1}) \in \mathcal{O}$. Moreover, Step 3 says that $\mathcal{O}$ is a valuation ring of $K$.

To show $\mathcal{O}^\times \subseteq T$, note that if $x \in \mathsf{O}_1$, then $1+x^{-1} \in x^{-1}T$. Therefore, $x^{-1} \notin \mathsf{O}_1$. Additionally, $x^{-1} \notin T$ implies $x^{-1} \notin \mathcal{O}$. Hence $\mathcal{O}^\times \subseteq \mathsf{O}_2 \subseteq T$, as contended.

To complete the proof we shall show next for every prime $p \neq 2$ that $T$ has the property (2.2.9). For $p = 2$ we shall see that if (2.2.9) does not hold for $T$, then there exists a subgroup $T_1$ of $K^\times$ containing $T$, with $(T_1 : T) = 2$, for which (2.2.9) holds.

Indeed, if there exists $d, e \in \mathsf{O}_1$ such that $1-de \notin T$, then

$$\begin{aligned} 1-de &= (1+d)-d(1+e) \in T \cup dT \\ &= (1+e)-e(1+d) \in T \cup eT \ , \\ &\text{consequently, } 1-de \in dT = eT \ . \end{aligned} \tag{2.2.10}$$

On the other hand, if $p \neq 2$ and $dT = eT$, then $de \notin T$. Indeed, if $de \in T$, then $\frac{d}{e}de = d^2 \in T$, and as $p$ is odd, also $d \in T$. Thus $de$ is $T$-rigid. Hence $1 - de \in T \cup deT$, contradicting $1 - de \in dT$. We may therefore conclude for $p \neq 2$ that $1 - xy \in T$ for all $x, y \in \mathsf{O}_1$.

Consider now the case $p = 2$. Defining $T_1 = T \cup eT$ we get a subgroup of $K^\times$ such that $(T_1 : T) = 2$, and clearly each $x \in K \setminus T_1$ is $T_1$-rigid. Moreover, $\mathsf{O}_1(T_1) = \{\, x \in \mathsf{O}_1(T) \mid x \notin eT \,\}$. We shall prove next that condition (2.2.9) holds for $T_1$, i.e., for all $x$, $y \in \mathsf{O}_1(T_1)$ we have that $1 - xy \in T_1$. Then $\mathcal{O}(T_1)$ would be the required valuation ring.

Pick $x, y \in \mathsf{O}_1(T_1)$. In order to prove that $1 - xy \in T_1$ we have to use the $T$-rigidity of $x, y, e$ and $d$. We first claim that $-dy \in \mathsf{O}_1(T)$. Indeed, from $x, y \notin eT = dT \subseteq T_1$, it follows $-ey^{-1}$, $-dy \notin T$ (recall that $-1 \in T$) and also $1 - dy \in T$, as a conclusion of (2.2.10). Proving the claim.

Next, looking for a contradiction, assume that $1-xy \notin T_1$. Then $1-xy \notin T$, too. As $x$, $y \in \mathsf{O}_1(T_1) \subseteq \mathsf{O}_1(T)$, arguing as in (2.2.10) we see that $xT = yT = (1 - xy)T$.

From $-ey^{-1} \notin T$, it follows that $-ey^{-1}$ is $T$-rigid. Therefore, either $1 - ey^{-1} \in T$ or $1-e^{-1}y \in T$. We shall prove that both possibilities cannot occur, which gives the desired contradiction.

Suppose $1-ey^{-1} \in T$. Then $-ey^{-1} \in \mathsf{O}_1(T)$, and since $1-(-ey^{-1})(-dy) = 1 - ed \notin T$, the argument in (2.2.10) implies

$$(-dy)T = (1 - (-ey^{-1})(-dy))T = (1 - ed)T = dT \ .$$

Since $dyT = dT$ implies $y \in T \subseteq T_1$, we get a contradiction.

On the other hand, if $1 - e^{-1}y \in T$, then $-e^{-1}y \in \mathsf{O}_1(T)$. Observe now that $1 - (-ex)(-e^{-1}y) = 1 - xy \notin T$. Again as in (2.2.10), it follows that

$$(-ex)T = (1 - (-ex)(-e^{-1}y))T = (1 - xy)T = xT \ .$$

Finally, $exT = xT$ contradicts $e \notin T$. □

## 2.3 Dependent Valuations – Induced Topology

Below we shall study the topology induced by a valuation on a field $K$. It will then turn out that the dependence of valuation rings we are going to introduce now means nothing else than inducing the same topology on $K$.

Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two valuation rings on $K$. We call $\mathcal{O}_1$ and $\mathcal{O}_2$ *dependent* if their product $\mathcal{O}_1\mathcal{O}_2$ (= the smallest subring of $K$ containing both $\mathcal{O}_1$ and $\mathcal{O}_2$) is different from $K$. By the elements of the *dependence class* $[\mathcal{O}]$ of $\mathcal{O}$ we just mean all non-trivial valuation rings $\mathcal{O}'$ of $K$, dependent on $\mathcal{O}$. Note that by the very definition of a valuation ring $\mathcal{O}$, every overring $\mathcal{O}'$ of $\mathcal{O}$ in $K$ is as well a valuation ring of $K$. Such an overring $\mathcal{O}'$ of $\mathcal{O}$ is called a *coarsening* of $\mathcal{O}$. Thus two dependent valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ of $K$ always have a lowest common coarsening with respect to inclusion–namely, their product $\mathcal{O}_1\mathcal{O}_2$.

We are now going to show that the set of overrings $\mathcal{O}'$ of $\mathcal{O}$ in $K$ is linearly ordered by inclusion. Moreover, the non-trivial valuation rings above $\mathcal{O}$ are in one-to-one correspondence with the proper convex subgroups of the value group $\Gamma$ of $\mathcal{O}$. Thus the rank of $\Gamma$ is as well the order type of the set of non-trivial valuation rings of $K$ above $\mathcal{O}$. In particular, $\Gamma$ has rank 1 if and only if $\mathcal{O}$ is maximal.

Furthermore, we see from this fact that the dependence relation is an equivalence relation. Indeed, if $\mathcal{O}_1$ and $\mathcal{O}_2$ are dependent and also $\mathcal{O}_2$ and $\mathcal{O}_3$ are dependent, then $\mathcal{O}_1\mathcal{O}_2$ and $\mathcal{O}_2\mathcal{O}_3$ are both overrings of $\mathcal{O}_2$. Thus there is some inclusion, say $\mathcal{O}_1\mathcal{O}_2 \subseteq \mathcal{O}_2\mathcal{O}_3$. But then $\mathcal{O}_1$ and $\mathcal{O}_3$ are both contained in $\mathcal{O}_2\mathcal{O}_3$. Hence they are dependent.

In what follows, let $\mathcal{O}$ be a fixed non-trivial valuation ring of $K$ (i.e., $\mathcal{O} \neq K$). Let $\mathcal{O}' \subseteq K$ be an overring of $\mathcal{O}$, and hence a valuation ring. We then have

$$\mathcal{M}' \subseteq \mathcal{M} \,,$$

where $\mathcal{M}$ and $\mathcal{M}'$ denote the maximal ideals of $\mathcal{O}$ and $\mathcal{O}'$ respectively. Indeed, $x \in \mathcal{M}'$ implies $x^{-1} \notin \mathcal{O}'$. Thus also $x^{-1} \notin \mathcal{O}$. But then $x \in \mathcal{M}$.

Since $\mathcal{M}'$ is a prime ideal in $\mathcal{O}'$, it is also prime in $\mathcal{O}$. Localizing $\mathcal{O}$ at $\mathcal{M}'$ we actually get back $\mathcal{O}'$:

$$\mathcal{O}' = \mathcal{O}_{\mathcal{M}'} \,.$$

To prove this it suffices to show that every element $x$ in $\mathcal{O}'$ has the form $a/b$ with $a, b \in \mathcal{O}$ and $b \notin \mathcal{M}'$. If $x \in \mathcal{O}$, write $x = x/1$. If $x \notin \mathcal{O}$, we have $x^{-1} \in \mathcal{M} \setminus \mathcal{M}'$. Now write $x = 1/x^{-1}$. Since we did not exclude the case $\mathcal{O}' = K$, this argument also shows that $K$ is the quotient field for every valuation ring $\mathcal{O}$ of $K$, a fact that we did already mention earlier.

Conversely, if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$, the localization $\mathcal{O}_\mathfrak{p}$ is an overring of $\mathcal{O}$ with maximal ideal $\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Thus we have shown that the overrings $\mathcal{O}'$ of $\mathcal{O}$ correspond 1-1 with the prime ideals $\mathfrak{p}$ of $\mathcal{O}$. The next lemma will give the promised linearity.

**Lemma 2.3.1.** *Let $\mathcal{O}$ be a non-trivial valuation ring of $K$ corresponding to the valuation $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$. Then there is a 1–1 correspondence of convex subgroups $\Delta$ of $\Gamma$ with prime ideals $\mathfrak{p}$ of $\mathcal{O}$, and hence with overrings $\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}$. This correspondence is given by*

$$\begin{aligned} \Delta &\mapsto \mathfrak{p}_\Delta = \{\, x \in K \mid v(x) > \delta \text{ for all } \delta \in \Delta \,\} \\ \mathfrak{p} &\mapsto \Delta_\mathfrak{p} = \{\, \gamma \in \Gamma \mid \gamma, -\gamma < v(x) \text{ for all } x \in \mathfrak{p} \,\} \,. \end{aligned}$$

*In particular, if $\mathcal{O}$ has finite rank, this rank coincides with the Krull dimension of $\mathcal{O}$.*

*Proof.* Clearly the set $\mathfrak{p}_\Delta$ is an ideal of $\mathcal{O}$. It remains to show that $\mathfrak{p}_\Delta$ is prime. Thus let $x, y \in \mathcal{O}$, and let $v(xy) > \delta$ for all $\delta \in \Delta$. Assume that $v(x), v(y) \leq \delta$ for some $\delta \in \Delta$. Then $v(xy) = v(x) + v(y) \leq 2\delta \in \Delta$, a contradiction.

The convexity of the set $\Delta_\mathfrak{p}$ is clear at once. Moreover, $-\Delta_\mathfrak{p} = \Delta_\mathfrak{p}$ follows from the construction. Thus it remains to show that $\Delta_\mathfrak{p}$ is closed under addition. Since two elements of $\Delta_\mathfrak{p}$ are always comparable, and $\Delta_\mathfrak{p}$ is convex, it actually suffices to show that $0 \leq \delta \in \Delta_\mathfrak{p}$ implies $\delta + \delta \in \Delta_\mathfrak{p}$. Let $\delta = v(x)$ for some $x \in \mathcal{O}$ and assume that $v(x^2) = \delta + \delta \notin \Delta_\mathfrak{p}$. Thus $v(y) \leq v(x^2)$ for some $y \in \mathfrak{p}$. Since $v(x^2y^{-1}) \geq 0$, $x^2y^{-1} \in \mathcal{O}$ and hence $x^2 = y(x^2y^{-1}) \in \mathfrak{p}$. As $\mathfrak{p}$ is a prime ideal, also $x \in \mathfrak{p}$. This, however, gives $\delta = v(x) \notin \Delta_\mathfrak{p}$, a contradiction.

Actually, the two operations are inverse to each other, i.e., for all $\Delta$ and $\mathfrak{p}$ one gets

$$\Delta = \Delta_{(\mathfrak{p}_\Delta)} \qquad \text{and} \qquad \mathfrak{p} = \mathfrak{p}_{(\Delta_\mathfrak{p})} \qquad \square$$

From this lemma and Proposition 2.1.1 we immediately get

**Corollary 2.3.2.** *Let $\mathcal{O}$ be a non-trivial valuation ring of $K$. Then $\mathcal{O}$ has rank 1 if and only if $\mathcal{O}$ is a maximal subring of $K$.*

Let us return to the non-trivial valuation ring $\mathcal{O}$ of $K$ and a corresponding valuation $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$. Assume again that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ with corresponding convex subgroup $\Delta$ in $\Gamma$. The canonical valuation corresponding to $\mathcal{O}_\mathfrak{p}$ induces an order-preserving group homomorphism

$$K^\times/\mathcal{O}^\times \longrightarrow K^\times/\mathcal{O}_\mathfrak{p}^\times \ ,$$

by sending for each $x \in K^\times$ the coset $x\mathcal{O}^\times$ to $x\mathcal{O}_\mathfrak{p}^\times$. The kernel consists of the elements $x \in K^\times$ such that

$$x = \frac{a}{b} \ ,$$

with $a, b \in \mathcal{O} \setminus \mathfrak{p}$. Hence $0 \leq v(a), v(b) \in \Delta$. Thus also $v(x) = v(a) - v(b) \in \Delta$. This shows that the valuation $v_\mathfrak{p}$ of $\mathcal{O}_\mathfrak{p}$ is obtained from $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ simply by dividing $\Gamma$ by the convex subgroup $\Delta$:

$$v_\mathfrak{p} : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma/\Delta \cup \{\infty\}$$

where $v_\mathfrak{p}(x) = v(x) + \Delta$.

The residue homomorphism

$$\varphi_\mathfrak{p} : \mathcal{O}_\mathfrak{p} \longrightarrow \mathcal{O}_\mathfrak{p}/\mathfrak{p} = \overline{K}_\mathfrak{p}$$

sends the valuation ring $\mathcal{O}$ to a valuation ring $\overline{\mathcal{O}}$ in $\overline{K}_\mathfrak{p}$. One easily checks that

$$\overline{v} : \overline{K}_\mathfrak{p} \longrightarrow\!\!\!\!\!\rightarrow \Delta \cup \{\infty\}$$

with $\overline{v}(\overline{x}) := v(x)$ is well-defined and yields a valuation on $\overline{K}_\mathfrak{p}$ corresponding to $\overline{\mathcal{O}}$. The residue class field of the latter valuation $\overline{v}$ is actually $\mathcal{O}/\mathcal{M} = \overline{K}$ as

$$\overline{\mathcal{O}}/\overline{\mathcal{M}} = (\mathcal{O}/\mathfrak{p})/(\mathcal{M}/\mathfrak{p}) = \mathcal{O}/\mathcal{M} \ .$$

Thus, passing from a non-trivial valuation ring $\mathcal{O}$ to some coarsening $\mathcal{O}_\mathfrak{p}$ of $\mathcal{O}$, we obtain from a valuation $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$, corresponding to $\mathcal{O}$, two other valuations, namely

$$v_\mathfrak{p} : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma/\Delta_\mathfrak{p} \cup \{\infty\}$$

with valuation ring $\mathcal{O}_\mathfrak{p}$, and the valuation

$$\overline{v} : \overline{K}_\mathfrak{p} \longrightarrow\!\!\!\!\!\rightarrow \Delta_\mathfrak{p} \cup \{\infty\}$$

on the residue class field of $v_\mathfrak{p}$.

This last process can also be reversed. Given a valuation $v' : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma' \cup \{\infty\}$ and another one on its residue class field, say $\overline{v} : \overline{K}_{v'} \longrightarrow\!\!\!\!\!\rightarrow \Delta' \cup \{\infty\}$, we can define a 'composition' of $v'$ with $\overline{v}$ as follows: we simply let

$$\mathcal{O} = \varphi^{-1}(\mathcal{O}_{\overline{v}}) \ ,$$

the pre-image of the valuation ring $\mathcal{O}_{\overline{v}}$ via the canonical residue homomorphism $\varphi : \mathcal{O}_{v'} \longrightarrow \overline{K}_{v'}$. $\mathcal{O}$ is a valuation ring of $K$ and $\mathcal{O}_{v'}$ a coarsening of $\mathcal{O}$ as described above. Let $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ be the canonical valuation corresponding to $\mathcal{O}$. There exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ such that

$$\mathcal{O}_{v'} = \mathcal{O}_\mathfrak{p} \ .$$

From what we have explained above we see that $\Delta'$ is isomorphic to a convex subgroup $\Delta$ of $\Gamma$, and $\Gamma' \cong \Gamma/\Delta$. We call $v$ the *composition* of $v'$ with $\overline{v}$.

We shall now study the topology induced by a valuation on a field $K$. As in the case of absolute values (cf. Sect. 1.1), also valuations of a field $K$ induce topologies on $K$ making all field operations continuous and satisfying one more property, saying that "a product can only be small, if one of the factors is small." Such field topologies are called $V$-topologies. A classical theorem, proved in Appendix B, says that every $V$-topology comes from either an archimedean absolute value or a valuation.

Returning to the dependency relation introduced above, we shall see that two valuations are dependent if and only if they induce the same topology.

Let $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ be a valuation of $K$. For each $\gamma \in \Gamma$ and each $a \in K$ we define the set

$$\mathcal{U}_\gamma(a) := \{\, x \in K \mid v(x-a) > \gamma \,\} \ .$$

These sets form a basis of open neighborhoods of $a$:

(1) $a \in \mathcal{U}_\gamma(a)$;
(2) $\mathcal{U}_\gamma(a) \cap \mathcal{U}_\lambda(a) = \mathcal{U}_\delta(a)$, where $\delta = \max\{\gamma, \lambda\}$;
(3) $b \in \mathcal{U}_\gamma(a)\,,\ b \neq a\,,\ v(b-a) = \gamma' > \gamma$ implies $\mathcal{U}_{\gamma'}(b) \subseteq \mathcal{U}_\gamma(a)$.

Indeed, $v(x-b) > \gamma' = v(b-a)$ implies $v(x-a) = v((x-b)+(b-a)) = v(b-a) = \gamma' > \gamma$.

One easily sees that the topology constructed above has the Hausdorff property. Moreover $\Gamma = \{0\}$ if and only if $\mathcal{U}_\gamma(a) = \{a\}$ for every $a \in K$ and every $\gamma \in \Gamma$. Thus $v$ is trivial if and only if the induced topology is discrete.

*Remark 2.3.3.* (1) The sets $\{ x \mid v(x-a) \geq \gamma \}$, $\{ x \mid v(x-a) \leq \gamma \}$, and $\{ x \mid v(x-a) = \gamma \}$ are open. For since $v(x-b) > v(b-a)$ implies $v(x-a) = v(b-a)$, we have, for example,

$$\{ x \mid v(x-a) \leq \gamma \} = \bigcup_{v(b-a) \leq \gamma} \mathcal{U}_{v(b-a)}(b) \, .$$

Therewith are all of these sets (and naturally also $\mathcal{U}_\gamma(a)$) both open and closed. This applies, for example, to $\mathcal{O} = \{ x \mid v(x) \geq 0 \}$ and $\mathcal{M} = \{ x \mid v(x) > 0 \}$.

(2) The field operations are continuous with respect to this topology. For example, $v(x+y) \geq \min\{v(x),\ v(y)\}$ implies $\mathcal{U}_\gamma(a) + \mathcal{U}_\gamma(b) \subseteq \mathcal{U}_\gamma(a+b)$. Moreover, since

$$xy - ab = (x-a)(y-b) + (x-a)b + (y-b)a \, ,$$

it follows that $\mathcal{U}_\gamma(a)\mathcal{U}_\gamma(b) \subseteq \mathcal{U}_\delta(ab)$, where $\delta = \min\{2\gamma, \gamma + v(a), \gamma + v(b)\}$.

(3) Moreover, we observe that the topology induced by $v$ satisfies the characteristic property of a $V$-topology (cf. Appendix B). For all $x, y \in K$ we have

$$xy \in \mathcal{U}_{2\gamma}(0) \ \text{ implies } \ x \in \mathcal{U}_\gamma(0) \text{ or } y \in \mathcal{U}_\gamma(0) \, .$$

Indeed, if $x, y \notin \mathcal{U}_\gamma(0)$, then $v(x),\ v(y) \leq \gamma$. Hence $v(xy) = v(x) + v(y) \leq 2\gamma$.

**Theorem 2.3.4.** *Two nontrivial valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ of $K$ are dependent if and only if they induce the same topology on $K$.*

*Proof.* Since two dependent valuation rings have a common non-trivial coarsening, to show that they induce the same topology it is enough to consider the particular case $\mathcal{O}_1 \subseteq \mathcal{O}_2$.

Let $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ be a valuation corresponding to $\mathcal{O}_1$. By Lemma 2.3.1 and its consequences there exists a convex subgroup $\Delta$ of $\Gamma$ connected with $\mathcal{O}_2$ in such a way that $K^\times \longrightarrow\!\!\!\!\!\rightarrow \Gamma \longrightarrow\!\!\!\!\!\rightarrow \Gamma/\Delta = \Gamma_2$ is a valuation $v_2$ corresponding to $\mathcal{O}_2$. Since $\mathcal{O}_2 \neq K$, $\Gamma_2 \neq \{0\}$. Write

$$\begin{aligned} \mathcal{U}_\gamma(0) &= \{ a \in K \mid v(a) > \gamma \} \quad \text{and} \\ \mathcal{U}_{\gamma+\Delta}(0) &= \{ a \in K \mid v_2(a) > \gamma + \Delta \} \\ &= \{ a \in K \mid v(a) > \lambda \text{ for all } \lambda \text{ with } \lambda \equiv \gamma \bmod \Delta \} \, . \end{aligned}$$

Therefore $\mathcal{U}_{\gamma+\Delta}(0) \subseteq \mathcal{U}_\gamma(0)$.

On the other hand, $v(a) > 2\gamma$ implies $v_2(a) \geq 2\gamma + \Delta$. Thus for $\gamma > 0$, if in addition $v_2(a) \leq \gamma + \Delta$, then $\gamma + \Delta \geq 2\gamma + \Delta$. Hence $\gamma \in \Delta$. Consequently, for $0 < \gamma \notin \Delta$ it follows that $\mathcal{U}_{2\gamma}(0) \subseteq \mathcal{U}_{\gamma+\Delta}(0)$.

Therefore the topologies induced by $\mathcal{O}_1$ and $\mathcal{O}_2$ are identical.

Conversely, let $\mathcal{M}_1$ and $\mathcal{M}_2$ be the maximal ideals of $\mathcal{O}_1$ and $\mathcal{O}_2$. If $\mathcal{O}_1$ and $\mathcal{O}_2$ induce the same topology on $K$, then $\mathcal{M}_2$ is an open neighbourhood

of 0 in the topology induced by $\mathcal{O}_1$. Consequently, there exists an $a \in K^\times$ with $a\mathcal{M}_1 \subseteq \mathcal{M}_2$.

As $\mathcal{M}_2$ is the maximal ideal of the valuation ring $\mathcal{O}_2$, the set $K \setminus \mathcal{M}_2$ is multiplicatively closed. Thus we can form the ring

$$\mathcal{O}_3 = \left\{ \frac{x}{y} \mid x \in \mathcal{O}_1, y \in \mathcal{O}_1 \setminus \mathcal{M}_2 \right\} .$$

Since $\mathcal{O}_3$ contains $\mathcal{O}_1$, it is a valuation ring too. $\mathcal{O}_3$ also contains $\mathcal{O}_2$. In fact, if $x \in \mathcal{O}_2 \setminus \{0\}$, then $x^{-1} \notin \mathcal{M}_2$. Hence $x = \frac{1}{x^{-1}} \in \mathcal{O}_3$ in case $x^{-1} \in \mathcal{O}_1$. If, however, $x^{-1} \notin \mathcal{O}_1$, we have $x \in \mathcal{O}_1$ and thus $x \in \mathcal{O}_3$. Finally, $\mathcal{O}_3 \neq K$. Indeed, let $z \in \mathcal{M}_1 \setminus \{0\}$. Then $\frac{1}{az} \notin \mathcal{O}_3$. To see this let $\frac{1}{az} = \frac{x}{y}$ with $x \in \mathcal{O}_1$ and $y \in \mathcal{O}_1 \setminus \mathcal{M}_2$. Then $y = a(zx) \in a\mathcal{M}_1 \subseteq \mathcal{M}_2$, a contradiction.

Hence we have proved that $\mathcal{O}_1$ and $\mathcal{O}_2$ are dependent. □

The last theorem is another way to see that the dependence relation among the valuation rings of a field $K$ is an equivalence relation, as we already saw above. Let $\mathcal{O}$ be a non-trivial valuation ring of $K$ and take the dependence class $[\mathcal{O}]$ of all non-trivial valuation rings of $K$ dependent on $\mathcal{O}$. Clearly $[\mathcal{O}]$ is an upwardly directed set with respect to the partial order of inclusion.

**Proposition 2.3.5.** *Let $\mathcal{O}$ be any non-trivial valuation ring of $K$. Then we have the following case distinction:*

*(1) $[\mathcal{O}]$ has a maximal valuation ring $\mathcal{O}_1$ which is a maximal non-trivial overring of $\mathcal{O}$; moreover $\mathcal{O}_1$ has rank 1 and its maximal ideal is the intersection of all non-zero prime ideals of $\mathcal{O}$, or*

*(2) there is no maximal non-trivial overring of $\mathcal{O}$. Then the maximal ideals $\mathcal{M}'$ of valuation rings $\mathcal{O}' \in [\mathcal{O}]$ form a neighborhood system of 0 for the topology induced by $\mathcal{O}$. In this case the set of all non-zero prime ideals of $\mathcal{O}$ is also a neighborhood system of 0.*

*Proof.* The first item is a consequence of Lemma 2.3.1.

For the second item suppose we are given a positive $\delta \in \Gamma$. We seek a valuation ring $\mathcal{O}' \supseteq \mathcal{O}$ such that $\mathcal{O}' \neq K$ and whose maximal ideal $\mathcal{M}'$ satisfies $\mathcal{M}' \subseteq \mathcal{U}_\delta(0)$. Let $\Delta$ be the convex hull of the subgroup generated by $\delta$ in $\Gamma$, i.e.,

$$\Delta = \{ \gamma \in \Gamma \mid \gamma, -\gamma < n\delta \text{ for some } n \in \mathbb{N} \} .$$

$\Delta$ is a convex subgroup of $\Gamma$, and defines by Lemma 2.3.1 a valuation ring $\mathcal{O}' \supseteq \mathcal{O}$ with $\mathcal{M}' \subseteq \mathcal{U}_\delta(0)$. It remains to show that $\mathcal{O}' \neq K$.

If $\mathcal{O}' = K$, then $\Delta = \Gamma$ and thus $\delta$ is an element of $\Gamma$ such that $\Gamma$ is the convex hull of $\mathbb{Z}\delta$. Let $\Delta^*$ be the largest convex subgroup of $\Gamma$ not containing $\delta$. Then $\Gamma^* = \Gamma/\Delta^*$ is archimedean ordered and thus the overring $\mathcal{O}^*$ of $\mathcal{O}$, corresponding to $\Delta^*$ by Lemma 2.3.1, is maximal according to Corollary 2.3.2. This contradicts our assumption. □

## 2.4 Approximation – Completion

The next theorem extends Theorem 1.1.3 to non-archimedean valuations of arbitrary rank.

**Approximation Theorem 2.4.1.** *Suppose $\mathcal{O}_1, \ldots, \mathcal{O}_n$ are pairwise independent valuation rings of $K$. For every $i$ such that $1 \leq i \leq n$, let*

$$v_i : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma_i \cup \{\infty\}$$

*be a valuation corresponding to $\mathcal{O}_i$. Then for any $a_1, \ldots, a_n \in K$ and $\gamma_1 \in \Gamma_1, \ldots, \gamma_n \in \Gamma_n$, there exists an $x \in K$ with*

$$v_i(x - a_i) > \gamma_i, \quad \textit{for all } i \in \{1, \ldots, n\} .$$

*Proof.* For each $i$ such that $1 \leq i \leq n$, we pick $\delta_i \in \Gamma_i$ satisfying $\delta_i \geq \gamma_i$ and $-\delta_i \leq v_i(a_1), \ldots, v_i(a_n)$. Some new restrictions will be imposed on each $\delta_i$ in the course of argumentation.

Next take the open sets

$$\begin{aligned} M_i &= \{\, x \in K \mid \quad 2\delta_i < v_i(x) \,\} \quad \text{and} \\ A_i &= \{\, x \in K \mid -2\delta_i \leq v_i(x) \,\} . \end{aligned}$$

(1) We may choose the $\delta_i$ so that

$$M_1 \cap \bigcap_{j=2}^{n} (K \setminus A_j) \neq \emptyset .$$

*Proof of (1)*: Induction on $n$.

$n = 2$: If $M_1 \cap (K \setminus A_2) = \emptyset$, then $M_1 \subseteq A_2$.

Choosing $c_i \in M_i$ $(i = 1, 2)$, we find that $c_i A_i \subseteq \mathcal{M}_i$ and $c_i \mathcal{M}_i \subseteq M_i$. Therefore $M_1 \subseteq A_2$ implies

$$(c_2 c_1)\mathcal{M}_1 = c_2(c_1 \mathcal{M}_1) \subseteq c_2 M_1 \subseteq c_2 A_2 \subseteq \mathcal{M}_2 .$$

Taking $a = c_2 c_1$ yields $a\mathcal{M}_1 \subseteq \mathcal{M}_2$, and we are exactly in the situation of the proof of Theorem 2.3.4. Thus we obtain that $\mathcal{O}_1$ and $\mathcal{O}_2$ are dependent, a contradiction.

$n > 2$: By the induction hypothesis there exists $r \in M_1 \cap (K \setminus A_2)$. We choose the $\delta_3, \ldots, \delta_n$ large enough so that $r \in A_j$, for all $j = 3, \ldots, n$.

By the induction hypothesis there further exists an

$$s \in M_1 \cap \bigcap_{3 \leq j \leq n} (K \setminus A_j) .$$

If $s \notin A_2$, we're done. In the case $s \in A_2$, since all $M_i$ and $A_i$ are closed under addition and subtraction,

$$s + r \in M_1 \cap \bigcap_{2 \le j \le n} (K \setminus A_j) \ ,$$

proving (1).

Analogously we find via "belated improvement" of the $\delta_\nu$ that

$$M_i \cap \bigcap_{j \neq i} (K \setminus A_j) \neq \emptyset \ .$$

An element from this intersection "approximates infinity" with respect to $v_j$ for each $j \neq i$, and it approximates 0 with respect to $v_i$.

(2) It now follows that

$$(1 + M_i) \cap \bigcap_{j \neq i} M_j \neq \emptyset$$

(i.e., we can approximate 1 with respect to $v_i$, and 0 with respect to $v_j$ for all $j \neq i$); indeed,

$$x \in M_i \quad \Rightarrow \quad \frac{1}{1+x} = 1 - \frac{x}{1+x} \in 1 + M_i \ ,$$

and

$$x \in K \setminus A_j \quad \Rightarrow \quad v_j(1+x) = v_j(x), \quad \text{whence } \frac{1}{1+x} \in M_j \ .$$

(3) Then we choose

$$d_i \in (1 + M_i) \cap \bigcap_{j \neq i} M_j$$

and finally set

$$x := a_1 d_1 + \cdots + a_n d_n \ .$$

Since $d_i - 1 \in M_i$ and $d_j \in M_i$ for all $j \neq i$, $v_i(d_i - 1), v_i(d_j) > 2\delta_i$. Therewith follows

$$\begin{aligned} v_i(x - a_i) &= v_i(a_1 d_1 + \cdots + a_i(d_i - 1) + \cdots + a_n d_n) \\ &> \min_{1 \le j \le n} \{v_i(a_j) + 2\delta_i\} \ge -\delta_i + 2\delta_i = \delta_i \ge \gamma_i \ , \end{aligned}$$

as desired. □

*Remark 2.4.2.* The above Approximation Theorem for valuations does apply to non-archimedean absolute values, but does not apply to archimedean absolute values. Hence it does not really generalize the Approximation Theorem 1.1.3 for absolute values. If one wants the archimedean absolute values to be included, one should look at the paper [29] of A. L. Stone. Another possibility is to "transform" them by model theoretic arguments also into valuations and then apply Theorem 2.4.1. This approach can be found in [22].

Once again let $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ be a non-trivial valuation on $K$. We are now going to introduce the completion of $K$ with respect to $v$. In case $\Gamma$ has rank 1 (i.e. $\Gamma$ is a subgroup of the additive reals), $v$ is a non-archimedean absolute value and the more general definition below will coincide with that of Sect. 1.

As we shall see later (Remark 2.4.6) the completion with respect to a higher rank valuation will in general not satisfy Hensel's Lemma (i.e., the statement of Theorem 1.3.1). This is the reason why the completion will be replaced by the so-called "henselization" (cf. Sect. 5.2), a uniquely determined algebraic extension of $K$ that satisfies Hensel's Lemma. Nevertheless, we shall introduce[3] the completion, but shall only sketch the proofs for its existence and uniqueness.

Let $\kappa$ be the smallest cardinal number serving as the index set of a sequence $\gamma_\nu \quad (\nu < \kappa, \quad \gamma_\nu \in \Gamma)$ that is "cofinal" in $\Gamma$ (i.e., to each $\delta \in \Gamma$ there exists a $\nu < \kappa$ with $\delta < \gamma_\nu$). The cardinal $\kappa$ is called the *cofinality* of $\Gamma$. As the rationals are dense in $\mathbb{R}$ we see that the cofinality of every subgroup $\Gamma$ of $\mathbb{R}$ is $\aleph_0$.

Similar to what we did in Sect. 1.1, we now consider sequences $(a_\nu)_{\nu<\kappa}$ of *length* $\kappa$. We define *convergence* and *Cauchy sequences* as follows:

$$\lim_{\nu<\kappa} a_\nu = a$$

if and only if for every $\gamma \in \Gamma$ there exists $\nu_0 < \kappa$ such that for all $\nu \geq \nu_0$,

$$v(a - a_\nu) > \gamma \ .$$

And $(a_\nu)_{\nu<\kappa}$ is a *Cauchy sequence* if and only if for every $\gamma \in \Gamma$ there exists $\nu_0 < \kappa$ such that for all $\nu, \mu \geq \nu_0$,

$$v(a_\nu - a_\mu) > \gamma \ .$$

$K$ is called *complete* if every Cauchy sequence converges in $K$. If we restrict to the case where $\kappa = \aleph_0$ (so that $(y_i)_{i<\kappa} = (y_i)_{i\in\mathbb{N}}$), then we have the ordinary concepts of convergence, Cauchy sequence, and completeness.

**Theorem 2.4.3.** *Every valued field $(K, v)$ possesses one and (up to valuation isomorphism) only one valued extension $\left(\widehat{K}, \widehat{v}\right)$ that is complete and in which $K$ is dense.*

$\left(\widehat{K}, \widehat{v}\right)$ is called the *completion* of $(K, v)$.

*Proof.* As in the proof of Theorem 1.1.4, the set $\mathcal{C}$ of all Cauchy sequences $(a_\nu)_{\nu<\kappa}$ of elements of $K$ with componentwise addition and multiplication is a commutative ring. The set

[3] In this introduction we shall assume some familiarity with basic fact about ordinals and cardinals. In the course of the book we shall, however, not return to this general notion of completions.

$$\mathcal{N} = \left\{ (a_\nu)_{\nu<\kappa} \;\middle|\; \lim_{\nu<\kappa} a_\nu = 0 \right\}$$

is a maximal ideal of $\mathcal{C}$. Thus the quotient ring $\widehat{K} = \mathcal{C}/\mathcal{N}$ is a field.

The ultrametric triangle inequality implies for any Cauchy sequence $(a_\nu)_{\nu<\kappa}$ that either:

(*i*) there is (exactly) one $\gamma \in \Gamma$ such that, for some $\eta < \kappa$, $v(a_\nu) = \gamma$ for all $\nu \geq \eta$; or

(*ii*) for all $\gamma \in \Gamma$, there exists $\eta < \kappa$ such that $v(a_\nu) > \gamma$ for every $\nu > \eta$.

It is pretty clear that case (ii) occurs if and only if $(a_\nu)_{\nu<\kappa} \in \mathcal{N}$.

The above remark shows that there is a well defined function

$$\widehat{v} : \mathcal{C} \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$$

given by

$$\widehat{v}((a_\nu)_{\nu<\kappa}) := \begin{cases} \gamma & \text{where } \gamma \text{ is given in (i)} . \\ \infty & \text{in case (ii)} . \end{cases}$$

Next, one can construct a valuation on $\widehat{K}$ (also denoted by $\widehat{v}$) as follows: for $\widehat{a} = (a_\nu)_{\nu<\kappa} + \mathcal{N} \in \widehat{K}$ set

$$\widehat{v}(\widehat{a}) = \widehat{v}((a_\nu)_{\nu<\kappa}) .$$

Let $(a_\nu)_{\nu<\kappa}, (b_\nu)_{\nu<\kappa} \in \mathcal{C}$ and denote $\gamma = \widehat{v}((a_\nu)_{\nu<\kappa}), \lambda = \widehat{v}((b_\nu)_{\nu<\kappa}) \in \Gamma \cup \{\infty\}$. By a "three-triangle-inequality" argument one sees that

$$\widehat{v}((a_\nu + b_\nu)_{\nu<\kappa}) \begin{cases} = \min\{\gamma, \lambda\} & \text{if } \gamma < \lambda \\ \geq \min\{\gamma, \lambda\} & \text{if } \gamma = \lambda \end{cases}$$

It follows from this that $\widehat{v} : \widehat{K} \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ is well defined and satisfies the ultrametric triangle condition. To show that $\widehat{v}$ preserves multiplication is an easy exercise. Thus $\widehat{v}$ is a valuation on $\widehat{K}$.

The map which associates to each $x \in K$ the class $(x_\nu)_{\nu<\kappa} + \mathcal{N}$ of the constant sequence $x_\nu = x$ for every $\nu$, embeds $K$ in a canonical way in $\widehat{K}$. It is also true that $\widehat{v}$ restricts to $v$ on the image of $K$.

Every Cauchy sequence $(a_\nu)_{\nu<\kappa}$ in $K$ has $\widehat{a} = (a_\nu)_{\nu<\kappa} + \mathcal{N}$ as its limit in $\widehat{K}$. Whence $K$ is dense in $\widehat{K}$.

To show the completeness of $\widehat{K}$, note first that there is a monotonically increasing sequence $(\gamma_t)_{t<\kappa}$ that is cofinal in $\Gamma$. Now take $(\widehat{a}_\nu)_{\nu<\kappa}$ a Cauchy sequence in $\widehat{K}$. For each $t < \kappa$, we can find an element $x_t \in K$ such that $\widehat{v}(\widehat{a}_t - x_t) > \gamma_t$. Then one verifies immediately that $(x_t)_{t<\kappa}$ is a Cauchy sequence in $K$. Put $\widehat{x} = (x_t)_{t<\kappa} + \mathcal{N}$. One shows that $(\widehat{a}_\nu)_{\nu<\kappa}$ converges to $\widehat{x}$, thus proving the completeness of $\widehat{K}$.

If $\widehat{K}$ and $\widehat{K}'$ are completions of the valued field $K$, then by standard arguments one verifies that there exists exactly one isomorphism $\phi : \widehat{K} \to \widehat{K}'$ of valued fields whose restriction to $K$ is the identical map. (In fact, there does exist a commutative diagram like in 1.1.4.) □

A valued field $(K, v)$ is called *relatively complete* if $K$ is relatively separably closed in $\widehat{K}$. For a valued field $(K, v)$, we write $(K^a, v^a)$ for the relative separable closure of $K$ in $\widehat{K}$, where $v^a$ is the restriction of $\widehat{v}$ to $K^a$.

**Proposition 2.4.4.** *$(K, v) \subseteq (K^a, v^a) \subseteq (\widehat{K}, \widehat{v})$ are immediate extensions, i.e., all residue class fields and all value groups are canonically isomorphic (cf. Theorem 1.3.4).*

*Proof.* For $\widehat{a} \in \widehat{K}$, the density of $K$ in $\widehat{K}$ implies the existence of $a \in K$ satisfying $\widehat{v}(\widehat{a} - a) > \widehat{v}(\widehat{a})$. Then $v(a) = \widehat{v}((\widehat{a} - a) - \widehat{a}) = \widehat{v}(\widehat{a})$. Thence $\widehat{v}$ and $v$ have the same value group. Moreover, if $\widehat{v}(\widehat{a}) = 0$, it follows from $\widehat{v}(\widehat{a} - a) > 0$ that $\widehat{a}$ and $a$ have the same residue class. Thus $\widehat{v}$ has $\overline{K}$ as its residue class field. □

**Theorem 2.4.5.** *A valued field $(K, v)$ is relatively complete if and only if every separable[4] polynomial $f \in K[X]$ that comes arbitrarily close to 0 over $K$ (i.e., that is such that 0 is in the closure of $f(K)$) has a zero in $K$.*

*Proof.* Suppose $(K, v) \neq (K^a, v^a)$ and let $\widehat{a} \in K^a \setminus K$. Take an irreducible polynomial $f \in K[X]$ such that $f(\widehat{a}) = 0$. Let $(a_\nu)_{\nu<\kappa}$ be a sequence in $K$ that converges to $\widehat{a}$. The continuity of the function defined by the polynomial $f$ implies that $(f(a_\nu))_{\nu<\kappa}$ converges to 0 over $K$. Yet $f$ has no zero in $K$.

Conversely, suppose $K = K^a$, and let $f \in K[X]$ be a separable polynomial which comes arbitrarily close to 0 over $K$. Denote $d = \deg f$. We may assume $f$ is monic. Consider next a cofinal sequence $(\gamma_\nu)_{\nu<\kappa}$ in $\Gamma$. Then for each $\nu < \kappa$ there exists an $a_\nu \in K$ with $v(f(a_\nu)) > d\gamma_\nu$.

As before, $\widehat{v}$ denotes the canonical extension of $v$ to $\widehat{K}$. By Theorem 3.1.2 there exists a valuation $w$ of a separable closure $\widehat{K}^s$ of $\widehat{K}$ whose restriction to $\widehat{K}$ equals $\widehat{v}$. From Theorem 3.2.4 (1) we shall see that the value group $\Gamma^s$ of $w$ is contained in the divisible hull of $\Gamma$. In particular, $(\gamma_\nu)_{\nu<\kappa}$ is still cofinal in $\Gamma^s$.

In $\widehat{K}^s$ we have $f(X) = (X - \widehat{a}_1) \cdots (X - \widehat{a}_d)$. From

$$d\gamma_\nu < v(f(a_\nu)) = \sum_{i=1}^{d} w(a_\nu - \widehat{a}_i)$$

it follows that for at least one $i$,

$$\gamma_\nu < w(a_\nu - \widehat{a}_i) \ .$$

Since we have only finitely many zeros $\widehat{a}_i$ of $f(X)$ there exists an $i$ and a subsequence of $(a_\nu)_{\nu<\kappa}$ that converges to $\widehat{a}_i$. From the completeness of $\widehat{K}$ it follows that $\widehat{a}_i \in \widehat{K}$. Since $K$ is relatively complete, $\widehat{a}_i$ even lies in $K$. □

[4] In this book, by a *separable* polynomial we always mean a polynomial without multiple zeros.

Clearly, every complete valued field $(K, v)$ is relatively complete. Thus if we want the statement of Corollary 1.3.2 to hold, every polynomial $f \in \mathcal{O}_v[X]$ that has a simple zero $\overline{a_0}$ in the residue class field $\overline{K_v}$ (i.e., $\overline{f}(\overline{a_0}) = 0$ and $\overline{f}'(\overline{a_0}) \neq 0$), should approach 0, i.e., 0 should belong to the closure of $f(K)$. This is always true if $v$ is a rank 1 valuation (see Remark 1.3.3). For higher rank valuations, however, this need no longer be true. Here is a counterexample:

*Remark 2.4.6.* Let $v_Y : \mathbb{R}(Y) \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z} \cup \{\infty\}$ be the $Y$-adic valuation on the rational function field $\mathbb{R}(Y)$. Clearly the residue class field is $\mathbb{R}$. We identify $\mathbb{Z}$ with the subgroup $\{0\} \times \mathbb{Z}$ of $\mathbb{Z} \times \mathbb{Z}$, ordered lexicographically. Thus the element $\gamma = (1, 0)$ is greater than any element $(0, \delta)$ from $\{0\} \times \mathbb{Z}$. In particular $(\{0\} \times \mathbb{Z}) \cap \mathbb{Z}\gamma = \{(0, 0)\}$. Thus by Corollary 2.2.3, $v_Y$ extends uniquely to a valuation $w : \mathbb{R}(X, Y) \longrightarrow\!\!\!\!\!\rightarrow (\mathbb{Z} \times \mathbb{Z}) \cup \{\infty\}$ with $w(X) = \gamma$. The residue class field of $w$ remains to be $\mathbb{R}$.

Now consider the polynomial $f = Z^2 - (1+Y) \in K[Z]$ where $K = \mathbb{R}(X, Y)$. Obviously, $a_0 = 1$ yields the simple zero $\overline{a_0} = \overline{1}$ of $\overline{f}$ in the residue class field. However, 0 is not in the closure of $f(K)$.

*Proof.* We shall show that

$$w(a^2 - (1 + Y)) < (1, 0) \qquad (*)$$

for every $a \in K$. Thus $f(K)$ cannot approach 0.

In order to show $(*)$, observe that $w$ is the composition of the $X$-adic valuation $v_X$ on the rational function field $k(X)$ with residue class field $k = \mathbb{R}(Y)$, and the $Y$-adic valuation $v_Y$ on $\mathbb{R}(Y)$. In fact,

$$v_X : K \longrightarrow (\mathbb{Z} \times \mathbb{Z})/(\{0\} \times \mathbb{Z}) \,,$$

with $v_X(a) = w(a) + (\{0\} \times \mathbb{Z})$. Therefore, showing that $v_X(a^2 - (1+Y)) \leq 0$ implies $(*)$. Now, if $v_X(a) < 0$, then $v_X(a^2 - (1 + Y)) < 0$, too. If $v_X(a) \geq 0$, then by passing to the residue class field $\mathbb{R}(Y)$ of $v_X$, we obtain

$$\overline{a}^2 - (1 + Y) \neq 0$$

(as $1 + Y$ is not a square in $\mathbb{R}(Y)$), showing that $v_X(a^2 - (1 + Y)) = 0$. □

We end this section with a result that deals with the *continuity of roots* of a separable polynomial.

**Theorem 2.4.7.** *Let $(K, v)$ be a valued field and let*

$$f(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in K[X]$$

*be a polynomial with distinct roots $x_1, \ldots, x_n \in K$. To every $\alpha \in v(K)$ there exists $\gamma \in v(K)$ such that whenever $y_1, \ldots, y_n \in K$,*

$$g(X) = \prod_{i=1}^{n}(X - y_i) = b_0 + \cdots + b_{n-1}X^{n-1} + X^n \ ,$$

*and*

$$\min_{0\le i<n} v(a_i - b_i) > \gamma \ ,$$

*then to every $x_i$ there is at least one $y_j$ with $v(x_i - y_j) > \alpha$. Moreover, if $\alpha \ge \max_{i\ne j} v(x_i - x_j)$, then there exists only one $y_j$ with $v(x_i - y_j) > \alpha$.*

*Proof.* Let $\beta := \min\{\, v(x_j) \mid 1 \le j \le n \,\}$, and assume that

$$\alpha \ge \max_{i\ne j} v(x_i - x_j) \ .$$

Observe that $\alpha \ge v(x_i - x_j) \ge \min\{v(x_i), v(x_j)\} \ge \beta$. Now let $\gamma > \max\{n\alpha, n(\alpha - \beta)\}$.

For every $y \in K$ such that $v(y - x_j) \le \alpha$ for all $1 \le j \le n$ it follows that

$$v(f(y)) = \sum_{j=1}^{n} v(y - x_j) \le n\alpha \ .$$

On the other hand, if $g(y) = 0$ and $v(y) \ge 0$, we get

$$\begin{aligned} v(f(y)) = v(f(y) - g(y)) &= v\left(\sum_{k=0}^{n-1}(a_k - b_k)y^k\right) \\ &\ge \min_{0\le k<n}\{v(a_k - b_k) + kv(y)\} > \gamma. \end{aligned}$$

Hence $n\alpha < \gamma < v(f(y)) \le n\alpha$, a contradiction. Therefore, $v(y - x_j) > \alpha$ for at least one zero $x_j$ of $f$.

If, however, $g(y) = 0$ and $v(y) < 0$, we consider

$$\begin{aligned} f(y)y^{-n} &= a_0y^{-n} + a_1y^{-(n-1)} + \cdots + a_{n-1}y^{-1} + 1 \ , \\ g(y)y^{-n} &= b_0y^{-n} + b_1y^{-(n-1)} + \cdots + b_{n-1}y^{-1} + 1 \ , \end{aligned}$$

and obtain

$$\begin{aligned} v(f(y)y^{-n}) = v(f(y)y^{-n} - g(y)y^{-n}) &= v\left(\sum_{k=0}^{n-1}(a_k - b_k)y^{-n+k}\right) \\ &\ge \min_{0\le k<n}\{v(a_k - b_k) + (n-k)(-v(y))\} > \gamma. \end{aligned}$$

On the other hand, since $v(f(y)y^{-n}) = v(f(y)) - nv(y) \le n\alpha - nv(y)$, we get

$$n(\alpha - \beta) < \gamma < v(f(y)y^{-n}) \leq n\alpha - nv(y) \ . \qquad (*)$$

Thus $n\beta > nv(y)$, and hence $\beta > v(y)$. Therefore $v(y - x_i) = v(y)$ for all $i$ with $1 \leq i \leq n$, and thus

$$v(f(y)) = \sum_{j=1}^{n} v(y - x_j) = nv(y) \ .$$

This together with $(*)$ yields

$$n(\alpha - \beta) < v(f(y)y^{-n}) = v(f(y)) - nv(y) = 0 \ ,$$

contradicting the inequality $\alpha \geq \beta$, observed at the very beginning of the proof. Thus also in the case $v(y) < 0$ we find $v(y - x_j) > \alpha$ for some $j$.

Finally, assume that there are $x_i \neq x_j$ and $v(y - x_i), v(y - x_j) > \alpha$. Then

$$v(x_i - x_j) = v((x_i - y) + (y - x_j)) \geq \min\{v(x_i - y), v(y - x_j)\} > \alpha \ ,$$

a contradiction to the choice of $\alpha$. □

## 2.5 Exercises

**Exercise 2.5.1.**
(a) Show that all local subrings of $\mathbb{Q}$ are valuation rings of $\mathbb{Q}$.
(b) Is this also true for the rational function field $\mathbb{F}_p(X)$?

**Exercise 2.5.2.**
Let $\mathcal{O}$ be a non-trivial valuation ring of $K$. Show the equivalence of the following conditions:
(i) $\mathcal{O}$ is factorial,
(ii) $\mathcal{O}$ is a principal ideal domain,
(iii) $K^\times/\mathcal{O}^\times \cong \mathbb{Z}$, i.e., the value group is discrete of rank 1.

**Exercise 2.5.3.**
Let $(K, \mathcal{O})$ be a valued field with residue class field $\overline{K}$. Show that $\overline{K}$ is real if and only if for all $a_1, \ldots, a_n \in K$,

$$v(a_1^2 + \cdots + a_n^2) = \min\{v(a_i^2) \mid 1 \leq i \leq n\}$$

**Exercise 2.5.4.**
Let $K$ and $L$ be fields. A map $\varphi : K \longrightarrow L \cup \{\infty\}$ is a *place* of $K$, if for all $x, y \in K$ :
(i) $\varphi(x + y) = \varphi(x) + \varphi(y)$,

(ii) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$,
(iii) $\varphi(1) = 1$.

Here for all $a \in L$ the following operations are defined:

$$a + \infty = \infty + a = \infty, \quad a \cdot \infty = \infty \cdot a = \infty \cdot \infty = \infty \, .$$

The operations $\infty + \infty$, $0 \cdot \infty$ and $\infty \cdot 0$ are *not* defined.

(a) Show that $\mathcal{O} = \varphi^{-1}(L)$ is a valuation ring of $K$ with maximal ideal $\mathcal{M} = \varphi^{-1}(\{0\})$ and residue class field $\overline{K} \cong \varphi(K)$.
(b) For every valuation ring $\mathcal{O}$ of $K$ with maximal ideal $\mathcal{M}$, the map $\varphi(x) = x + \mathcal{M}$ for all $x \in \mathcal{O}$ and $\varphi(x) = \infty$ for all $x \in K \setminus \mathcal{O}$ defines a place $\varphi : K \longrightarrow \cup\{\infty\}$ with $L = \mathcal{O}/\mathcal{M}$.

**Exercise 2.5.5.**
Let $K(X, Y)$ be the rational function field in $X$ and $Y$ over the field $K$. Define $\varphi : K(X) \longrightarrow K \cup \{\infty\}$ by

$$\varphi\left(\frac{f(X)}{g(X)}\right) = \frac{f(0)}{g(0)} \text{ with } f, g \in K[X] \text{ coprime}$$

(as usual, we let $\frac{a}{0} = \infty$ if $a \neq 0$; note that $\frac{0}{0}$ does not occur).
Similarly define $\psi : L(Y) \longrightarrow L \cup \{\infty\}$ with $L = K(X)$ by

$$\psi\left(\frac{p(Y)}{q(Y)}\right) = \frac{p(0)}{q(0)} \text{ with } p, q \in L[Y] \text{ coprime} \, .$$

Show that $\varphi, \psi$ and $\chi = \varphi \circ \psi$ (with $\varphi(\infty) = \infty$) are places of $K(X, Y)$. Describe the valuations, valuation rings, value groups, and residue class field corresponding to $\varphi, \psi$ and $\chi$.

# 3

# Extension of Valuations

In this chapter we discuss the question whether, and in how many ways, a valuation $v$ of a field $K$ can be extended to another field $L$ containing $K$.

We have seen in Sect. 1.1 that for a rank-1 valuation there exists an extension of $v$ to the completion $\widehat{K}$. If $L$ is the rational function field $K(X)$, we also constructed extensions of $v$ in Sect. 2.2. We shall now show that a valuation $v$ on a field $K$ always allows at least one extension to every field $L$ containing $K$ (Sect. 3.1).

In Sect. 3.2 and 3.3 we study the collection of all extensions $w$ of a valuation $v$ of $K$ to an algebraic extension field $L$. The most important fact is the Conjugation Theorem, stating that in a normal extension $L/K$ (finite or infinite), two extensions of $v$ are always conjugate. Moreover, we prove the Fundamental Inequality yielding in particular that for a finite extension $L/K$ there are only finitely many extensions of $v$ to $L$.

In Sect. 3.4 we treat transcendental extensions $L/K$ and prove the so-called Dimension Inequality.

## 3.1 Chevalley's Extension Theorem

We prove in this section that for every valuation $v$ of a field $K$ and every extension $L$ of $K$ there is a valuation $w$ of $L$ lying over $v$, i.e., such that the restriction of $w$ to $K$ equals $v$. This is a direct consequence of Chevalley's Theorem, our first result. We shall also apply Chevalley's Theorem to characterize the integral closure of a domain $D$ by means of the valuation rings containing $D$.

**Theorem 3.1.1.** (Chevalley) *For a field $K$, let $R \subseteq K$ be a subring and let $\mathfrak{p} \subseteq R$ be a prime ideal of $R$. Then there exists a valuation ring $\mathcal{O}$ of $K$ such that*

$$R \subseteq \mathcal{O} \quad \textit{and} \quad \mathcal{M} \cap R = \mathfrak{p}\ ,$$

*where $\mathcal{M}$ is the maximal ideal of $\mathcal{O}$.*

*Proof.* We use the standard notation $R_{\mathfrak{p}}$ for the localization of $R$ at $\mathfrak{p}$. Let

$$\Sigma = \{\, (A, I) \mid R_{\mathfrak{p}} \subseteq A \subseteq K,\ \mathfrak{p}R_{\mathfrak{p}} \subseteq I \subseteq A,\ A \text{ a ring},\ I \text{ a proper ideal of } A \,\} .$$

Then $\Sigma \neq \emptyset$, since $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}}) \in \Sigma$. Moreover, $\Sigma$ may be partially ordered as follows: for all $(A_j, I_j) \in \Sigma$ $(j = 1, 2)$, we declare

$$(A_1, I_1) \leq (A_2, I_2) \quad :\Leftrightarrow \quad A_1 \subseteq A_2,\ I_1 \subseteq I_2 .$$

Each chain $\{\, (A_j, I_j) \mid j \in J \,\}$ of such pairs (where $J$ is a nonempty index set) possesses an upper bound in $(\Sigma, \leq)$, namely,

$$\left( \bigcup_{j \in J} A_j,\ \bigcup_{j \in J} I_j \right) .$$

By Zorn's Lemma, $\Sigma$ has a maximal element $(\mathcal{O}, \mathcal{M})$.

Observe now that $R \subseteq R_{\mathfrak{p}} \subseteq \mathcal{O}$, and since $\mathfrak{p}R_{\mathfrak{p}}$ is the maximal ideal of $R_{\mathfrak{p}}$, $\mathcal{M} \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$. Hence $\mathcal{M} \cap R = \mathfrak{p}$. Therefore, to complete the proof it remains to show that $\mathcal{O}$ is a valuation ring. From the maximality of $(\mathcal{O}, \mathcal{M})$ we first conclude that $\mathcal{O}$ is a local ring.

Assume now that $\mathcal{O}$ is not a valuation ring. Then there exists an $x \in K^\times$ such that $x, x^{-1} \notin \mathcal{O}$. Then $\mathcal{O} \subsetneqq \mathcal{O}[x], \mathcal{O}[x^{-1}]$. The maximality of $(\mathcal{O}, \mathcal{M})$ implies therefore $\mathcal{M}\mathcal{O}[x] = \mathcal{O}[x]$ and $\mathcal{M}\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}]$. Thus there exist $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathcal{M}$ such that

$$1 = \sum_{i=0}^{n} a_i x^i \ \text{ and } 1 = \sum_{i=0}^{m} b_i x^{-i} , \tag{3.1.1}$$

with $n$, $m$ minimal. Suppose, first, that $m \leq n$. As $b_0 \in \mathcal{M}$, we have

$$\sum_{i=1}^{m} b_i x^{-i} = 1 - b_0 \in \mathcal{O}^\times = \mathcal{O} \setminus \mathcal{M} .$$

Hence

$$1 = \sum_{i=1}^{m} c_i x^{-i}, \quad c_i = \frac{b_i}{1 - b_0} \in \mathcal{M} .$$

Multiplying this equation by $x^n$, one gets

$$x^n = \sum_{i=1}^{m} c_i x^{n-i} .$$

Combining this with the first part of (3.1.1) yields

$$1 = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n-1} a_i x^i + \sum_{i=1}^{m} c_i a_n x^{n-i};$$

since $m \leq n$, this contradicts the minimality of $n$. If, on the other hand, $n \leq m$, then arguing in a similar way one gets a contradiction to the minimality of $m$. □

Let $K_2/K_1$ be a field extension, and $\mathcal{O}_1 \subseteq K_1$, $\mathcal{O}_2 \subseteq K_2$ be valuation rings. We say that $\mathcal{O}_2$ is a *prolongation* of $\mathcal{O}_1$ if $\mathcal{O}_2 \cap K_1 = \mathcal{O}_1$. We denote this statement by $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$. We shall also use expressions like "$\mathcal{O}_2$ is an *extension* of $\mathcal{O}_1$," or "$\mathcal{O}_2$ *lies over* $\mathcal{O}_1$," as synonyms of this expression.

Suppose $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ as above, and let $\mathcal{M}_1$, $\mathcal{M}_2$ be the maximal ideals of $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively. Then

$$\mathcal{M}_2 \cap K_1 = \mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_1$$
$$\mathcal{O}_2^\times \cap K_1 = \mathcal{O}_2^\times \cap \mathcal{O}_1 = \mathcal{O}_1^\times \ .$$

For a field extension $K_1 \subseteq K_2$ and a valuation ring $\mathcal{O}_2$ of $K_2$, one also sees that $\mathcal{O}_1 = \mathcal{O}_2 \cap K$ is a valuation ring of $K_1$ such that $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$.

**Theorem 3.1.2.** *Let $K_2/K_1$ be a field extension, and let $\mathcal{O}_1 \subseteq K_1$ be a valuation ring. Then there is an extension $\mathcal{O}_2$ of $\mathcal{O}_1$ in $K_2$.*

*Proof.* Since $\mathcal{O}_1$ is a subring of $K_2$, according to Chevalley's Theorem there exists a valuation ring $\mathcal{O}_2$ of $K_2$ with $\mathcal{O}_1 \subseteq \mathcal{O}_2$ and $\mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_1$ for the maximal ideals. Since $\mathcal{O}_2 \cap K_1$ and $\mathcal{O}_1$ are valuation rings with the same maximal ideal they must coincide. □

Next we prove the other promised consequence of Chevalley's Theorem.

**Theorem 3.1.3.**

(1) *Every valuation ring $\mathcal{O}$ of a field $K$ is integrally closed in $K$.*

(2) *Let $D$ be a subring of a field $K$, and denote by $\mathbb{V}$ the set of all valuation rings $\mathcal{O}$ in $K$ with maximal ideal $\mathcal{M}$ such that $D \subseteq \mathcal{O}$ and $\mathcal{M} \cap D$ is a maximal ideal of $D$. Then the integral closure $R$ of $D$ in $K$ equals the intersection*

$$R_1 := \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O} \ .$$

*Proof.* (1) Suppose $x \in K$ satisfies $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n = 0$, for some $a_0, \ldots, a_{n-1} \in \mathcal{O}$. If $x \notin \mathcal{O}$, then $x^{-1} \in \mathcal{M}$, whence

$$-1 = a_0 x^{-n} + \cdots + a_{n-1} x^{-1} \in \mathcal{M} \ ,$$

a contradiction.

(2) By (1) above, each $\mathcal{O} \in \mathbb{V}$ is integrally closed in $K$. Thus $R \subseteq R_1$.

Conversely, if $x \in K \setminus R$ we shall show that $x \notin R_1$. We first claim that $x \notin R[x^{-1}]$. In fact, otherwise $x = b_0 + b_1 x^{-1} + \cdots + b_m x^{-m}$, for some $b_0, \ldots, b_m \in R$. Multiplying this equation by $x^m$, one gets that $x$ is integral over $R$, and by transitivity, integral over $D$, a contradiction.

Consequently, we conclude that $x^{-1} \in \mathfrak{m}$, for some maximal ideal $\mathfrak{m}$ of $R[x^{-1}]$. According to Chevalley's Theorem, 3.1.1, there exists a valuation ring $\mathcal{O}$ of $K$ such that $R[x^{-1}] \subseteq \mathcal{O}$ and $\mathcal{M} \cap R[x^{-1}] = \mathfrak{m}$. Since $x^{-1} \in \mathcal{M}$, it follows that $x \notin \mathcal{O}$. Therefore it remains only to show that $\mathcal{O} \in \mathbb{V}$, i.e., that the ideal $\mathcal{M} \cap D$ of $D$ is maximal.

To this end, observe first that the canonical map $R \longrightarrow R[x^{-1}]/\mathfrak{m}$ is a surjective homomorphism. Indeed, for $z = c_0 + c_1 x^{-1} + \cdots + c_s x^{-s} \in R[x^{-1}]$, we find $z + \mathfrak{m} = c_0 + \mathfrak{m}$, as $x^{-1} \in \mathfrak{m}$. Thus $\mathcal{M} \cap R = \mathfrak{m} \cap R$ is a maximal ideal of $R$.

Next, $\mathfrak{m} \cap D$ is a prime ideal of $D$. Thus considering $D/(\mathfrak{m} \cap D) \subseteq R/(\mathfrak{m} \cap R)$, it follows from $R$ being integral over $D$ that $R/(\mathfrak{m} \cap R)$ is integral over $D/(\mathfrak{m} \cap D)$. Since $R/(\mathfrak{m} \cap R)$ is a field, so is $D/(\mathfrak{m} \cap D)$. Consequently $\mathfrak{m} \cap D$ is a maximal ideal. Hence $\mathcal{O} \in \mathbb{V}$. □

**Corollary 3.1.4.** *Let $L/K$ be any field extension, and let $\mathcal{O}$ be a valuation ring of $K$. Let $R$ be the integral closure of $\mathcal{O}$ in $L$. Then $R = \bigcap \mathcal{O}'$, where $\mathcal{O}'$ ranges over the set of all prolongations of $\mathcal{O}$ to $L$.*

*Proof.* For each prolongation $\mathcal{O}'$ of $\mathcal{O}$ to $L$, write $\mathcal{M}'$ for its maximal ideal. Then we have $\mathcal{M}' \cap \mathcal{O} = \mathcal{M}$, the maximal ideal of $\mathcal{O}$. Conversely, if $\mathcal{O}'$ is a valuation ring of $L$ containing $\mathcal{O}$, with maximal ideal $\mathcal{M}'$ satisfying $\mathcal{M}' \cap \mathcal{O} = \mathcal{M}$, then $\mathcal{O}' \cap K = \mathcal{O}$. Thus the result follows from the above Theorem 3.1.3. □

For later use we shall note one more result about extensions of valuations.

**Lemma 3.1.5.** *Let $L/K$ be an extension of fields, and let $\mathcal{O}'$ be a valuation ring of $L$. Then every valuation ring $\mathcal{O} \supseteq \mathcal{O}' \cap K$ of $K$ can be extended to some valuation ring $\mathcal{O}'' \supseteq \mathcal{O}'$ on $L$.*

*Proof.* Let the value group of $\mathcal{O}'$ be $\Gamma'$, and denote by $\Gamma \subseteq \Gamma'$ the value group of $\mathcal{O}' \cap K$. Now by Lemma 2.3.1, the valuation ring $\mathcal{O}$ corresponds to a convex subgroup $\Delta$ of $\Gamma$. More precisely, if $v$ denotes the valuation corresponding to $\mathcal{O}' \cap K$, then

$$\mathcal{O} = \{\, x \in K \mid v(x) \geq \delta \text{ for some } \delta \in \Delta \,\} .$$

If we now set

$$\mathcal{O}'' = \{\, x \in L \mid v'(x) \geq \delta \text{ for some } \delta \in \Delta \,\} ,$$

where $v'$ corresponds to $\mathcal{O}'$, then clearly $\mathcal{O}'' \supseteq \mathcal{O}'$ and $\mathcal{O}'' \cap K = \mathcal{O}$. □

## 3.2 Algebraic Extensions

In this section, for a valued extension $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ with $K_2$ algebraic over $K_1$ we are concerned with the relationship between $\mathcal{O}_1$ and $\mathcal{O}_2$. We shall describe the relations between the value groups and the residue class fields. Moreover, we are also interested in the set $\mathbb{V}$ of all extensions of $\mathcal{O}_1$ to $K_2$. According to Theorem 3.1.2, $\mathbb{V} \neq \emptyset$. Although $\mathbb{V}$ need not be finite for infinite extensions $K_2/K_1$, its cardinality is always limited by the degree of separability of $K_2$ over $K_1$. This will imply that $\mathbb{V}$ has just one element for

purely inseparable extensions. Two different elements of $\mathbb{V}$ are never comparable by inclusion. However, if $K_2$ is a normal extension of $K_1$, the elements of $\mathbb{V}$ are pairwise $K_1$-conjugate in the sense that they are isomorphic by some $\sigma \in \mathrm{Aut}(K_2/K_1)$.

We start with an arbitrary extension of valued fields $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$. To each $\mathcal{O}_i$, $i = 1, 2$, corresponds a valuation $v_i : K_i \longrightarrow\!\!\!\!\!\rightarrow \Gamma_i \cup \{\infty\}$. Recall from Sect. 2.1 that $v_i|_{K_i^\times} : K_i^\times \longrightarrow\!\!\!\!\!\rightarrow \Gamma_i$ is a group homomorphism with kernel $\mathcal{O}_i^\times$ and $K_i^\times/\mathcal{O}_i^\times \cong \Gamma_i$. Moreover, the composite mapping

$$K_1^\times \overset{\mathrm{id}}{\hookrightarrow} K_2^\times \longrightarrow\!\!\!\!\!\rightarrow K_2^\times/\mathcal{O}_2^\times \cong \Gamma_2$$

has kernel $\mathcal{O}_2^\times \cap K_1^\times = \mathcal{O}_1^\times$, whence $\Gamma_1 \cong K_1^\times/\mathcal{O}_1^\times \hookrightarrow K_2^\times/\mathcal{O}_2^\times \cong \Gamma_2$, by the homomorphism theorem. Therefore we may regard $\Gamma_1$ as a ordered subgroup of $\Gamma_2$. Let us call $e := e(\mathcal{O}_2/\mathcal{O}_1) := [\Gamma_2 : \Gamma_1]$ the *ramification index* of this extension.

Similarly, denoting the maximal ideals by $\mathcal{M}_1$, $\mathcal{M}_2$, the composite mapping

$$\mathcal{O}_1 \overset{\mathrm{id}}{\hookrightarrow} \mathcal{O}_2 \longrightarrow\!\!\!\!\!\rightarrow \mathcal{O}_2/\mathcal{M}_2 = \overline{K_2}$$

has kernel $\mathcal{M}_2 \cap \mathcal{O}_1 = \mathcal{M}_1$. Thus, $\overline{K_1} = \mathcal{O}_1/\mathcal{M}_1 \hookrightarrow \mathcal{O}_2/\mathcal{M}_2 = \overline{K_2}$. Therefore we may regard $\overline{K_1}$ as a subfield of $\overline{K_2}$. Now, we define $f := f(\mathcal{O}_2/\mathcal{O}_1) := \left[\overline{K_2} : \overline{K_1}\right]$ as the *residue degree* of this extension.

In particular, if $e(\mathcal{O}_2/\mathcal{O}_1) = 1$ and $f(\mathcal{O}_2/\mathcal{O}_1) = 1$, the extension $\mathcal{O}_2/\mathcal{O}_1$ is called *immediate*.

For example, a completion $\left(\widehat{K}, \mathcal{O}_{\widehat{v}}\right)$ of a rank-one valued field $(K, \mathcal{O}_v)$ is an immediate extension, by Theorem 1.3.4.

*Remark 3.2.1.* The ramification index and the residue degree are multiplicative. If $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2) \subseteq (K_3, \mathcal{O}_3)$ are valued extensions of fields, then

$$\begin{aligned} e(\mathcal{O}_3/\mathcal{O}_1) &= e(\mathcal{O}_3/\mathcal{O}_2)\, e(\mathcal{O}_2/\mathcal{O}_1) \quad \text{and} \\ f(\mathcal{O}_3/\mathcal{O}_1) &= f(\mathcal{O}_3/\mathcal{O}_2) f(\mathcal{O}_2/\mathcal{O}_1)\,. \end{aligned}$$

Next we shall study the connections between the value groups $\Gamma_1 \subseteq \Gamma_2$ and the residue class fields $\overline{K_1} \subseteq \overline{K_2}$ as discussed above.

**Lemma 3.2.2.** *Suppose* $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$, *and, for* $i = 1, 2$,

$$v_i : K_i \longrightarrow\!\!\!\!\!\rightarrow \Gamma_i \cup \{\infty\}$$

*is the valuation corresponding to* $\mathcal{O}_i$. *Choose* $\omega_1, \ldots, \omega_f \in \mathcal{O}_2$ *and* $\pi_1, \ldots, \pi_e \in K_2^\times$ *so that:*

*(1) the residues* $\overline{\omega_1}, \ldots, \overline{\omega_f} \in \overline{K_2}$ *are linearly independent over* $\overline{K_1}$*;*
*(2) the values* $v_2(\pi_1), \ldots, v_2(\pi_e)$ *are representatives of the distinct cosets of* $\Gamma_2/\Gamma_1$.

*Then for all* $a_{ij} \in K_1$,

$$v_2\Big(\sum_{i=1}^{f}\sum_{j=1}^{e} a_{ij}\omega_i\pi_j\Big) = \min\{\, v_2(a_{ij}\omega_i\pi_j) \mid 1 \le i \le f,\ 1 \le j \le e \,\}\,. \quad (3.2.1)$$

*In particular, the products* $\{\, \omega_i\pi_j \mid i = 1,\dots,f,\ j = 1,\dots,e \,\}$ *are linearly independent over* $K_1$.

*Proof.* Let $a_{ij} \in K_1$, not all zero, and pick any $I \in \{1,\dots,f\}$ and $J \in \{1,\dots,e\}$ such that

$$v_2(a_{IJ}\pi_J) = \min\{v_2(a_{ij}\pi_j) \mid (i,j) \in \{1,\dots,f\} \times \{1,\dots,e\}\}\,,$$

and observe first that $v_2(a_{IJ}\pi_J) < v_2(a_{ij}\pi_j)$ for all $j \neq J$. Otherwise,

$$v_2(\pi_J) - v_2(\pi_j) = v_2(a_{ij}) - v_2(a_{IJ}) \in \Gamma_1\,,$$

for some $j \neq J$, which would contradict assumption 2.

Next, write $z = \sum_{i=1}^{f}\sum_{j=1}^{e} a_{ij}\omega_i\pi_j$, and assume, for the sake of obtaining a contradiction, that $v_2(z) > \min\{\, v_2(a_{ij}\omega_i\pi_j) \mid 1 \le i \le f,\ 1 \le j \le e \,\}$. Then $z(a_{IJ}\pi_J)^{-1} \in \mathcal{M}_2$. According to the previous paragraph, $a_{ij}\pi_j(a_{IJ}\pi_J)^{-1} \in \mathcal{M}_2$ for all $j \neq J$, too. Dividing everything by $a_{IJ}\pi_J$ one gets

$$\sum_{i=1}^{f} a_{iJ}a_{IJ}^{-1}\omega_i = z(a_{IJ}\pi_J)^{-1} - \sum_{i=1}^{f}\sum_{\substack{j=1\\ j\neq J}}^{e} a_{ij}\pi_j(a_{IJ}\pi_J)^{-1}\omega_i \in \mathcal{M}_2\,.$$

Consequently,

$$\sum_{i=1}^{f} \overline{a_{iJ}a_{IJ}^{-1}}\,\overline{\omega_i} = 0\,,$$

contradicting assumption 1. □

The above proposition has the following immediate consequence:

**Corollary 3.2.3.** *Suppose* $(K_1,\mathcal{O}_1) \subseteq (K_2,\mathcal{O}_2)$, *and set* $n = [K_2 : K_1]$, $e = e(\mathcal{O}_2/\mathcal{O}_1)$, *and* $f = f(\mathcal{O}_2/\mathcal{O}_1)$. *If* $n < \infty$, *then* $e, f < \infty$ *and* $ef \le n$.

More generally, we can state:

**Theorem 3.2.4.** *For* $(K_1,\mathcal{O}_1) \subseteq (K_2,\mathcal{O}_2)$ *with* $K_2$ *algebraic over* $K_1$ *the following statements hold:*

*(1) for every* $\gamma \in \Gamma_2$ *there is an* $n \in \mathbb{N}$ *such that* $n\gamma \in \Gamma_1$; *i.e.,* $\Gamma_2/\Gamma_1$ *is a torsion group;*
*(2)* $\overline{K_2}$ *is an algebraic extension of* $\overline{K_1}$.

*Proof.* (1) Pick $x \in K_2$ such that $v_2(x) = \gamma \in \Gamma_2$. Set $L = K_1(x)$, $\mathcal{O} = \mathcal{O}_2 \cap L$, and $v = v_2|_L$, the restriction of $v_2$ to $L$. Let $\Gamma = v(L^\times) \subseteq \Gamma_2$. By Corollary 3.2.3, the quotient $\Gamma/\Gamma_2$ is a finite group. Hence for $\gamma = v(x) \in \Gamma$ there is $n \in \mathbb{N}$ satisfying $n\gamma \in \Gamma_2$, as desired.

(2) Similarly, for $x \in \mathcal{O}_2^\times$ we take $L$ and $\mathcal{O}$ as above. It follows from Corollary 3.2.3 that the residue class field $\overline{L}$ is a finite extension of $\overline{K_2}$. Therefore $\overline{x} \in \overline{L} \subseteq \overline{K_2}$ is algebraic over $\overline{K_1}$. □

**Corollary 3.2.5.** *Let $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ be an extension as in Theorem 3.2.4. Then $\Gamma_2$ and $\Gamma_1$ (resp. $\mathcal{O}_2$ and $\mathcal{O}_1$) have the same rank.*

*Proof.* From the fact that $\Gamma_2/\Gamma_1$ is a torsion group it follows that the map $\Delta \mapsto \Delta \cap \Gamma_1$ is a bijective, inclusion-preserving correspondence between the set of convex subgroups of $\Gamma_2$ and $\Gamma_1$. □

Next, we state some results needed to study the set of valuation rings of an algebraic extension of a field $K$ lying over a fixed valuation ring of $K$.

**Lemma 3.2.6.** *Suppose $\mathcal{O}_1, \ldots, \mathcal{O}_n$ are valuation rings of a field $K$ with maximal ideals $\mathcal{M}_1, \ldots, \mathcal{M}_n$. Let*

$$R := \bigcap_{i=1}^{n} \mathcal{O}_i \quad \text{and} \quad \mathfrak{p}_i := R \cap \mathcal{M}_i \ .$$

*Then for $1 \le i \le n$, $\mathcal{O}_i = R_{\mathfrak{p}_i}$.*

*Proof.* Clearly $R_{\mathfrak{p}_i} \subseteq \mathcal{O}_i$. To prove the other inclusion, take $a \in \mathcal{O}_i$, and let $I_a = \{\, j \mid a \in \mathcal{O}_j \,\}$. Write $\alpha_j = a + \mathcal{M}_j \in \overline{K_j}$ for each $j \in I_a$. Choose a prime number $p \in \mathbb{N}$ such that, for all $j \in I_a$: $p > \operatorname{char} \overline{K_j}$, and $\alpha_j$ is not a primitive $p$-th root of 1.

Set $b = 1 + a + \cdots + a^{p-1}$, and observe that

$$\alpha_j = 1 \text{ implies } \overline{b} = 1 + \cdots + 1 = p \neq 0 \text{ in } \overline{K_j}, \quad \text{and}$$
$$\alpha_j \neq 1 \text{ implies } \overline{b} = \frac{1 - \alpha_j^p}{1 - \alpha_j} \neq 0 \text{ in } \overline{K_j} \ .$$

Thus, either way, $b \in \mathcal{O}_j^\times$ for all $j \in I_a$.

For $j \in \{1, \ldots, n\} \smallsetminus I_a$, $a \notin \mathcal{O}_j$, whence $a^{-1} \in \mathcal{M}_j$. Hence

$$1 + a^{-1} + \cdots + a^{-(p-1)} \in \mathcal{O}_j^\times \ ,$$

implying

$$b^{-1} = a^{-(p-1)}(1 + a^{-1} + \cdots + a^{-(p-1)})^{-1} \in \mathcal{O}_j, \quad \text{and}$$
$$ab^{-1} = a^{-(p-2)}(1 + a^{-1} + \cdots + a^{-(p-1)})^{-1} \in \mathcal{O}_j \ .$$

Thus for all $j = 1, \ldots, n$ we have $b^{-1}$, $ab^{-1} \in \mathcal{O}_j$. So $b^{-1}$, $ab^{-1} \in R$, and $b^{-1} \notin \mathcal{M}_i \cap R = \mathfrak{p}_i$, since $b \in \mathcal{O}_i^\times$. Hence $a = ab^{-1}/b^{-1} \in R_{\mathfrak{p}_i}$. □

**Theorem 3.2.7.** *With the assumptions and notations of Lemma 3.2.6, suppose that $\mathcal{O}_i \not\subseteq \mathcal{O}_j$, for all $i \neq j$. Then*

(1) *for all $i \neq j$, $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$;*
(2) *$\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ is the set of all maximal ideals of $R$;*
(3) *for each $n$-tuple $(a_1, \ldots, a_n) \in \mathcal{O}_1 \times \cdots \times \mathcal{O}_n$, there exists an $a \in R$ with $a - a_i \in \mathcal{M}_i$;*

Observe that item (3) of the above theorem is a weak version of the Approximation Theorem 2.4.1 in case $\mathcal{O}_1, \ldots, \mathcal{O}_n$ are pairwise independent. The importance of Theorem 3.2.7, however, lies in the fact that independence is not necessary in (3).

*Proof.* (1) If $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ then $\mathcal{O}_j = R_{\mathfrak{p}_j} \subseteq R_{\mathfrak{p}_i} = \mathcal{O}_i$, by Lemma 3.2.6.

In order to prove (2), we shall show that every ideal $\mathfrak{a} \neq R$ is contained in some $\mathfrak{p}_i$, $i = 1, \ldots, n$. For the sake of obtaining a contradiction, assume that there exists an ideal $\mathfrak{a} \neq R$ such that for each $i = 1, \ldots, n$, there exists $a_i \in \mathfrak{a} \setminus \mathfrak{p}_i$. For each $i \neq j$, use (1) to pick $b_{ij} \in \mathfrak{p}_i \setminus \mathfrak{p}_j$. Then

$$c_j := \prod_{i \neq j} b_{ij} \in \mathfrak{p}_i \setminus \mathfrak{p}_j \ ,$$

for every $i \neq j$. Consequently, $a_j c_j \in \mathfrak{p}_i$ for all $i \neq j$ and $a_j c_j \notin \mathfrak{p}_j$. Therefore

$$d := \sum_{j=1}^{n} a_j c_j \notin \mathfrak{p}_i, \text{ for all } i = 1, \ldots, n \ ,$$

implying $d^{-1} \in \mathcal{O}_i$ for every $i$ such that $1 \leq i \leq n$. Hence $d^{-1} \in R$, implying $1 = dd^{-1} \in \mathfrak{a}$, a contradiction.

(3) For $i \neq j$, $\mathfrak{p}_i + \mathfrak{p}_j = R$, by (2) and (1). Therefore, the Chinese Remainder Theorem implies that the canonical map

$$R \longrightarrow R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_n$$

is surjective. Since for each $i$, $R_{\mathfrak{p}_i}/\mathfrak{p}_i R_{\mathfrak{p}_i} \cong R/\mathfrak{p}_i$, and, by Lemma 3.2.6, $R_{\mathfrak{p}_i} = \mathcal{O}_i$, it follows that $R \longrightarrow \mathcal{O}_1/\mathcal{M}_1 \times \cdots \times \mathcal{O}_n/\mathcal{M}_n$ is surjective. □

**Lemma 3.2.8.** *Suppose $K_2/K_1$ is an algebraic extension of fields, $\mathcal{O}$ is a valuation ring of $K_1$, and $\mathcal{O}'$, $\mathcal{O}''$ are valuation rings of $K_2$ lying over $\mathcal{O}$. If $\mathcal{O}' \subseteq \mathcal{O}''$, then $\mathcal{O}' = \mathcal{O}''$.*

*Proof.* The valuation ring $\mathcal{O}'$ maps to a valuation ring $\overline{\mathcal{O}'} \cong \mathcal{O}'/\mathcal{M}''$ of the residue class field $\overline{K''} = \mathcal{O}''/\mathcal{M}''$ of $\mathcal{O}''$. Since $\mathcal{O}'$ is an extension of $\mathcal{O}$, it follows that $\overline{K} = \mathcal{O}/\mathcal{M} \hookrightarrow \overline{\mathcal{O}'}$. According to Theorem 3.2.4, $\overline{K''}$ is an algebraic extension of $\overline{K}$. Moreover, since $\overline{K''}$ is the field of fractions of $\overline{\mathcal{O}'}$ it follows that $\overline{\mathcal{O}'}$ is also a field. But $\overline{\mathcal{O}'}$ is a valuation ring of $\overline{K''}$. Thus $\overline{\mathcal{O}'} = \overline{K''}$, and so $\mathcal{O}' = \mathcal{O}''$. This last equality follows from $\mathcal{M}'' \subseteq \mathcal{M}'$. □

Given an algebraic extension $K_2$ of $K_1$ and a valuation ring $\mathcal{O}_1$ of $K_1$, there may exist infinitely many valuation rings of $K_2$ lying over $\mathcal{O}_1$. Sometimes, however, their number has a natural bound. This is the content of the next result.

Let $K_2 \cap K_1^s = \{x \in K_2 \mid x \text{ is separable over } K_1\}$. The field $K_2 \cap K_1^s$ is a separable extension of $K_1$, and $[K_2 \cap K_1^s : K_1]$ is called the *degree of separability* of $K_2$ over $K_1$. Moreover, $[K_2 : K_2 \cap K_1^s]$ is called the *degree of inseparability* of $K_2$ over $K_1$. Every $x \in K_2 \setminus K_2 \cap K_1^s$ is purely inseparable over $K_2 \cap K_1^s$. We use the following notations:

$$[K_2 : K_1]_s = [K_2 \cap K_1^s : K_1] \qquad \text{and} \qquad [K_2 : K_1]_i = [K_2 : K_2 \cap K_1^s] \; .$$

**Theorem 3.2.9.** *Let $K_2$ be algebraic over $K_1$, and $[K_2 : K_1]_s < \infty$. Let $\mathcal{O}$ be a valuation ring of $K_1$. Then the number $n$ of all prolongations of $\mathcal{O}$ to $K_2$ is finite, and*

$$n \leq [K_2 : K_1]_s \; .$$

*Proof.* Let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be some distinct prolongations of $\mathcal{O}$ to $K_2$, with maximal ideals $\mathcal{M}_1, \ldots, \mathcal{M}_m$, respectively. Our previous Lemma 3.2.8 implies that these prolongations are pairwise incomparable. Therefore, Theorem 3.2.7 (3) applies, and there exist $c_1, \ldots, c_m$ such that for all $i, j \in \{1, \ldots, m\}$,

$$c_j - 1 \in \mathcal{M}_j \quad \text{and} \quad c_i \in \mathcal{M}_j \text{ for } i \neq j \; .$$

If $\operatorname{char} K_1 = p > 0$, pick $k$ large enough to guarantee that

$$c_1^{p^k}, \ldots, c_m^{p^k} \in K_2 \cap K_1^s \; .$$

In case $\operatorname{char} K_1 = 0$, replace $p^k$ by 1. We claim that the $m$ elements just listed are $K_1$-linearly independent. Consequently, $m \leq [K_2 : K_1]_s$, and the result follows.

We shall prove the claim by contradiction. For $a_1, \ldots, a_m \in K_1$, not all zero, such that

$$\sum_{i=1}^{m} a_i c_i^{p^k} = 0 \; ,$$

pick $j$ such that $1 \leq j \leq m$ and

$$v(a_j) = \min\{\, v(a_1), \ldots, v(a_m) \,\} \; .$$

Then $a_j \neq 0$ and

$$c_j^{p^k} = -\sum_{i \neq j} a_j^{-1} a_i c_i^{p^k} \in \mathcal{M}_j \; .$$

Since this would imply $c_j \in \mathcal{M}_j$ and hence $1 \in \mathcal{M}_j$, we get the desired contradiction. □

The last theorem has the following immediate consequence.

**Corollary 3.2.10.** *Suppose $K_2$ is a purely inseparable extension of $K_1$. Then every valuation ring $\mathcal{O}$ of $K_1$ has exactly one extension to $K_2$.*

**Theorem 3.2.11.** *Suppose $K$ is a separably closed field and $\mathcal{O}$ is a proper valuation ring of $K$. Let $\widetilde{K}$ be an algebraic closure of $K$ and let $\widetilde{\mathcal{O}}$ be the unique extension of $\mathcal{O}$ to $\widetilde{K}$. Then $\widetilde{\mathcal{O}}/\mathcal{O}$ is an immediate extension. In particular, the residue class field $\overline{K}$ of $\mathcal{O}$ is algebraically closed, and the value group $\Gamma$ of $\mathcal{O}$ is divisible (i.e., for every $\gamma \in \Gamma$ and any $n \in \mathbb{N} \setminus \{0\}$, there exists $\delta \in \Gamma$ such that $n\delta = \gamma$).*

For the proof of this theorem we shall need the following technical lemma.

**Lemma 3.2.12.** *Suppose $K$ is a field with a non-trivial valuation $v$. For every polynomial $g(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in K[X]$ and every $\gamma$ in the value group $\Gamma$ of $v$, there exists a separable polynomial $h(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + X^n \in K[X]$ such that $v(a_i - b_i) > \gamma$ for every $i$ with $0 \le i < n$.*

Using the Gauss extension of Corollary 2.2.2 this condition would be written as $w(g - h) > \gamma$. Therefore, this lemma means that the set of *separable*, monic polynomials is dense in the set of all monic polynomials.

*Proof.* Let $Y_0, \ldots, Y_{n-1}$ be indeterminates over $K$. Construct

$$\begin{aligned} f_Y(X) &= f_{Y_0,\ldots,Y_{n-1}}(X) \\ &= (a_0 + Y_0) + (a_1 + Y_1)X + \cdots + (a_{n-1} + Y_{n-1})X^{n-1} + X^n \\ &\in K(Y_0, \ldots, Y_{n-1})[X] \,, \end{aligned}$$

and consider the resultant $\mathrm{Res}(f_Y(X), f_Y'(X))$ of $f$ and its formal derivative with respect to the variable $X$ (this is also called the *discriminant* of $f$). Since $Y_0, \ldots, Y_{n-1}$ are algebraically independent over $K$, $\mathrm{Res}(f_Y, f_Y')$ is a nontrivial polynomial $R(Y_0, \ldots, Y_{n-1}) \in K[Y_0, \ldots, Y_{n-1}]$.

Since $v$ is non-trivial, $K$ cannot be a finite field. Thus for every $\gamma \in \Gamma$, the set $\{\, x \in K \mid v(x) > \gamma \,\}$ has infinitely many elements. Consequently, there are

$$c_0, \ldots, c_{n-1} \in K \text{ with } v(c_i) > \gamma$$

such that $R(c_0, \ldots, c_{n-1}) \neq 0$.[1] Hence for

$$h(X) = (a_0 + c_0) + (a_1 + c_1)X + \cdots + (a_{n-1} + c_{n-1})X^{n-1} + X^n \,,$$

it follows that $\mathrm{Res}(h, h') \neq 0$. Therefore $h$ and $h'$ have no common roots, i.e., $h(X)$ has no multiple roots. Thus $h$ fulfills the requirement of the lemma. □

[1] For a non-constant polynomial $g(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ and an infinite subset $M \subseteq K$, one shows by induction on $n$ that there exists $(x_1, \ldots, x_n) \in M^n$ such that $g(x_1, \ldots, x_n) \neq 0$.

*Proof of Theorem 3.2.11.* Let us denote by $\widetilde{\Gamma}$ and $\overline{\widetilde{K}}$ the value group and the residue class field of $\widetilde{\mathcal{O}}$, respectively. Observe first that the multiplicative group $\widetilde{K}^\times$ of $\widetilde{K}$ is divisible. Indeed, for every $a \in \widetilde{K}^\times$ and every $n \in \mathbb{N}$, the polynomial $X^n - a$ has its roots in $\widetilde{K}$. Consequently $\widetilde{\Gamma}$, as a quotient of $\widetilde{K}^\times$, is also divisible. Similarly, for $a_0, \ldots, a_n \in \widetilde{\mathcal{O}}$, $n > 0$, $a_n \in \widetilde{\mathcal{O}}^\times$, the polynomial $\overline{f} = \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n \in \overline{\widetilde{K}}[X]$ necessarily has a root in $\overline{\widetilde{K}}$, since $f = a_0 + a_1X + \cdots + a_nX^n$ has a root in $\widetilde{\mathcal{O}}$ (recall that $\widetilde{\mathcal{O}}$ is integrally closed in $\widetilde{K}$).

We next prove $\overline{K} = \overline{\widetilde{K}}$. Take $x \in \widetilde{\mathcal{O}}^\times$, and let

$$g(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in \mathcal{O}[X]$$

be a monic polynomial such that $\overline{g}$ is the minimal polynomial of $\overline{x}$ over $\overline{K}$.

By Lemma 3.2.12, pick a separable polynomial

$$h(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + X^n \in K[X]$$

such that $v(a_i - b_i) > 0$ for every $i$ such that $0 \leq i < n$. Since $g \in \mathcal{O}[X]$, it follows also that $h \in \mathcal{O}[X]$. Since $h$ is separable, it has a root $z$ in $K$. By Theorem 3.1.3 (1), $\mathcal{O}$ is integrally closed in $K$; so $z \in \mathcal{O}$. Consequently

$$\overline{g}(\overline{z}) = \overline{g(z)} = \overline{g(z) - h(z)} = \sum_{i=1}^{n} \overline{(a_i - b_i)}\overline{z}^i = 0\ .$$

As $\overline{g}$ is the minimal polynomial of $\overline{x}$, it follows that $\overline{g}$ has degree one, and $\overline{x} \in \overline{K}$, as required.

In order to prove $\Gamma = \widetilde{\Gamma}$, let $\delta \in \widetilde{\Gamma}$. By Theorem 3.2.4 there are $n > 1$ and $a \in K$ such that $n\delta = v(a) \in \Gamma$, where $v$ is a valuation corresponding to $\mathcal{O}$. Without loss of generality we may take $\delta > 0$, and so $a \in \mathcal{O}$. We now take $g(X) = X^n - a$. By Lemma 3.2.12 we can approximate $g(X) = a_0 + a_1X + \cdots + X^n$ by a separable polynomial $h(X) = b_0 + b_1X + \cdots + X^n$ such that $v(a_i - b_i) > n\delta$ for every $i = 0, \ldots, n$. Since $K$ is separably closed and $\mathcal{O}$ is integrally closed in $K$, $h$ has a root $z \in \mathcal{O}$. Moreover,

$$v(g(z)) = v(g(z) - h(z)) \geq \min_{0 \leq i < n} \{v(a_i - b_i) + iv(z)\} > n\delta = v(a)\ .$$

Now $v(z^n - a) > v(a)$ implies that $v(z^n) = v(a) = n\delta$. Hence $\delta = v(z) \in \Gamma$. □

Next we shall show that the integral closure of a valuation ring in an algebraic extension of its quotient field has a "localization property" like the one in Lemma 3.2.6.

**Theorem 3.2.13.** *Let $L$ be an algebraic extension of a field $K$, and let $\mathcal{O}$ be a valuation ring of $K$. Denote by $R$ the integral closure of $\mathcal{O}$ in $L$ and let $\mathcal{O}'$ be an extension of $\mathcal{O}$ to $L$. If $\mathcal{M}'$ is the maximal ideal of $\mathcal{O}'$ and $\mathfrak{m} = \mathcal{M}' \cap R$, then $R_\mathfrak{m} = \mathcal{O}'$.*

*Proof.* The inclusion $R_{\mathfrak{m}} \subseteq \mathcal{O}'$ is clear. For $x \in \mathcal{O}'$, let $K_2 = K(x)$, and adopt the following notations: $R_2 = R \cap K_2$, $\mathfrak{m}_2 = \mathfrak{m} \cap K_2$, $\mathcal{O}_2 = \mathcal{O}' \cap K_2$ and $\mathcal{M}_2 = \mathcal{M}' \cap K_2$. Clearly $R_2$ is the integral closure of $\mathcal{O}$ in $K_2$. According to Corollary 3.1.4, $R_2 = \bigcap \mathcal{O}^*$, where $\mathcal{O}^*$ ranges over the set of all prolongations of $\mathcal{O}$ to $K_2$. By Theorem 3.2.9, $\mathcal{O}$ has only finitely many extensions to $K_2$. Hence Lemma 3.2.6 applies. Therefore, since $\mathcal{M}_2 \cap R_2 = \mathfrak{m}_2$, it follows that $\mathcal{O}_2$ is the localization of $R_2$ with respect to $\mathfrak{m}_2$. Consequently, there exist $a, b \in R_2$ with $b \notin \mathfrak{m}_2$ such that $x = ab^{-1}$. Obviously $ab^{-1} \in R_{\mathfrak{m}}$, proving the theorem. □

Next we shall consider the set of all prolongations of a fixed valuation ring of a field $K$ to normal extensions of $K$.

**Theorem 3.2.14.** *Suppose $L/K$ is a finite normal extension of fields, with $G = \mathrm{Aut}(L/K)$. Suppose $\mathcal{O}$ is a valuation ring of $K$, and $\mathcal{O}'$ and $\mathcal{O}''$ are valuation rings in $L$ extending $\mathcal{O}$. Then $\mathcal{O}'$ and $\mathcal{O}''$ are conjugate over $K$, i.e., there exists $\sigma \in G$ with $\sigma\mathcal{O}' = \mathcal{O}''$.*

*Proof.* First, split the extension $L/K$ into the steps $K \subseteq L \cap K^s$ and $L \cap K^s \subseteq L$. Corollary 3.2.10 implies that every extension of $\mathcal{O}$ to $L \cap K^s$ has just one prolongation to $L$. Furthermore, $\mathrm{Aut}(L \cap K^s/K)$ and $G$ can be canonically identified. Therefore, we see that it is enough to consider the case where $L$ is separable over $K$. In this case let

$$H' = \{\, \sigma \in G \mid \sigma\mathcal{O}' = \mathcal{O}' \,\} \quad \text{and}$$
$$H'' = \{\, \tau \in G \mid \tau\mathcal{O}'' = \mathcal{O}'' \,\} .$$

Then $H'$ and $H''$ are subgroups of $G$. Moreover, for every $\sigma \in H'$, it follows that $\sigma(\mathcal{M}') = \mathcal{M}'$, for the maximal ideal of $\mathcal{O}'$. Indeed, it is enough to observe that $\sigma(\mathcal{M}')$ must be the maximal ideal of $\sigma(\mathcal{O}')$. Analogously for the maximal ideal $\mathcal{M}''$ of $\mathcal{O}''$, it follows that $\tau(\mathcal{M}'') = \mathcal{M}''$ for all $\tau \in H''$. Next write $G$ as disjoint unions of cosets of $H'$ and $H''$, respectively:

$$G = \bigcup_{i=1}^{n} H'\sigma_i^{-1} \quad \text{and} \quad G = \bigcup_{j=1}^{m} H''\tau_j^{-1} ,$$

for suitable $\sigma_i, \tau_j \in G$. These partitions will be crucial in studying the set of all extensions of $\mathcal{O}$ to $L$.

Suppose now, for the sake of contradiction, that $\sigma_i\mathcal{O}' \not\subseteq \tau_j\mathcal{O}''$ and $\tau_j\mathcal{O}'' \not\subseteq \sigma_i\mathcal{O}'$ for all $i, j$.

Since $\sigma_1^{-1}, \ldots, \sigma_n^{-1}$ is a complete set of representatives of cosets of $H'$, for all $k \neq t$, $\sigma_k(\mathcal{O}') \not\subseteq \sigma_t(\mathcal{O}')$. In fact, if $\sigma_k\mathcal{O}' \subseteq \sigma_t\mathcal{O}'$ for some $k, t$ such that $1 \leq k, t \leq n$, then $\sigma_k\mathcal{O}' = \sigma_t\mathcal{O}'$ by Lemma 3.2.8. Thus $\sigma_t^{-1}\sigma_k \in H'$, implying $k = t$, as required. Similarly, $\tau_k(\mathcal{O}'') \not\subseteq \tau_t(\mathcal{O}'')$ for every $k \neq t$ such that $1 \leq k, t \leq m$.

Now take

$$R = \bigcap_{i=1}^{n} \sigma_i \mathcal{O}' \ \cap \ \bigcap_{j=1}^{m} \tau_j \mathcal{O}'' \ .$$

According to Theorem 3.2.7 (3), there exists an $a \in R$ satisfying

$$\begin{aligned} a - 1 \in \sigma_i(\mathcal{M}') \text{ for } i = 1, \ldots, n, \text{ and} \\ a \in \tau_j(\mathcal{M}'') \text{ for } j = 1, \ldots, m \ . \end{aligned}$$

As a consequence, for $\sigma \in G$, writing $\sigma = \rho\sigma_i^{-1}$, with $1 \le i \le n$ and $\rho \in H'$, it follows that $\sigma(a-1) \in \rho\sigma_i^{-1}(\sigma_i(\mathcal{M}')) = \rho(\mathcal{M}') = \mathcal{M}'$. Analogously, $\sigma(a) \in \mathcal{M}''$ for every $\sigma \in G$.

Taking norms, it then follows

$$\begin{aligned} N_{L/K}(a) &= \prod_{\sigma \in G} \sigma(a) \in (\mathcal{M}' + 1) \cap K = \mathcal{M} + 1, \quad \text{and} \\ N_{L/K}(a) &= \prod_{\sigma \in G} \sigma(a) \in \mathcal{M}'' \cap K = \mathcal{M} \ . \end{aligned}$$

The above contradiction implies therefore $\sigma_i\mathcal{O}' \subseteq \tau_j\mathcal{O}''$ or $\tau_j\mathcal{O}'' \subseteq \sigma_i\mathcal{O}'$, for some $i, j$. Thus, by Lemma 3.2.8, $\sigma_i\mathcal{O}' = \tau_j\mathcal{O}''$. Hence $\mathcal{O}'' = \tau_j^{-1}\sigma_i\mathcal{O}'$. □

In the next theorem we prove that the last result holds for arbitrary normal extensions.

**Conjugation Theorem 3.2.15.** *Suppose $L/K$ is an arbitrary normal extension of fields, $\mathcal{O}$ is a valuation ring of $K$, and $\mathcal{O}'$ and $\mathcal{O}''$ are valuation rings in $L$ extending $\mathcal{O}$. Then there exists $\sigma \in \mathrm{Aut}(L/K)$ with $\sigma(\mathcal{O}') = \mathcal{O}''$.*

*Proof.* Consider the set of ordered pairs $(K_1, \sigma_1)$, where $K_1$ is an intermediate normal extension of $L/K$, $\mathcal{O}_1' = \mathcal{O}' \cap K_1$, $\mathcal{O}_1'' = \mathcal{O}'' \cap K_1$, and $\sigma_1$ is an automorphism of $K_1/K$ with $\sigma_1(\mathcal{O}_1') = \mathcal{O}_1''$. Clearly this set contains $(K, \mathrm{id})$. We endow it with the partial ordering

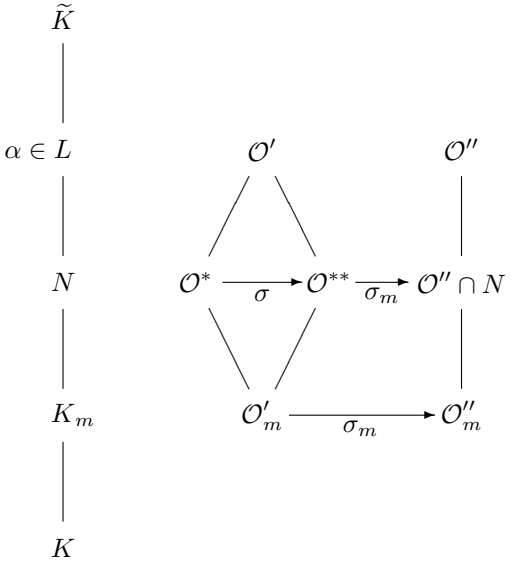
$$(K_1, \sigma_1) \le (K_2, \sigma_2) \quad :\Leftrightarrow \quad K_1 \subseteq K_2 \text{ and } \sigma_1 = \sigma_2|_{K_1} \ .$$

By Zorn's lemma there exists a maximal such pair $(K_m, \sigma_m)$ with $K \subseteq K_m \subseteq L$ and $\sigma_m(\mathcal{O}_m') = \mathcal{O}_m''$, where $\mathcal{O}_m' := \mathcal{O}' \cap K_m$ and $\mathcal{O}_m'' := \mathcal{O}'' \cap K_m$.

We have to show that $K_m = L$. Otherwise, we could pick $\alpha \in L \setminus K_m$. Let $f$ be the minimal polynomial of $\alpha$ with respect to $K$, and let $N$ be the splitting field of $f$ over $K_m$ inside $L$. We extend $\sigma_m$ to an automorphism (still denoted by $\sigma_m$) of the algebraic closure $\widetilde{K}$ of $K$.

Then $\sigma_m(L) = L$ and $\sigma_m(N) = N$. In fact, $L/K$ is normal by assumption, and $N$ is the compositum of $K_m$ and the splitting field of $\alpha$ over $K$ inside $L$.

Let $\mathcal{O}^* := \mathcal{O}' \cap N$ and $\mathcal{O}^{**} := \sigma_m^{-1}(\mathcal{O}'' \cap N)$. Following the picture below one sees that $\mathcal{O}^* \cap K_m = \mathcal{O}^{**} \cap K_m = \mathcal{O}_m'$.




Application of Theorem 3.2.14 to $\mathcal{O}^*$ and $\mathcal{O}^{**}$ gives a $\sigma \in \mathrm{Aut}(N/K_m)$ with $\mathcal{O}^{**} = \sigma(O^*)$. Then $\sigma_m \circ \sigma(\mathcal{O}' \cap N) = \sigma_m(\mathcal{O}^{**}) = \mathcal{O}'' \cap N$. Thus $(N, \sigma_m \circ \sigma) > (K_m, \sigma_m)$, contradicting the maximality of $(K_m, \sigma_m)$. □

The next proposition collects very useful properties of normal extensions.

**Proposition 3.2.16.** *Let $N$ be a normal extension of a field $K$, $\mathcal{O}$ a valuation ring of $K$, and $\mathcal{O}'$ a valuation ring of $N$ lying over $\mathcal{O}$. Write $\mathcal{M}'$ for the maximal ideal of $\mathcal{O}'$. Let $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ and $v' : N \longrightarrow\!\!\!\!\!\rightarrow \Gamma' \cup \{\infty\}$ be valuations corresponding to $\mathcal{O}$ and $\mathcal{O}'$, respectively, and assume that the restriction of $v'$ to $K$ is $v$. Denote the residue class field of $\mathcal{O}'$ by $\overline{N}$, and write $x \mapsto \overline{x}$ for the corresponding quotient map.*

*(1) For $\sigma \in \mathrm{Aut}(N/K)$, the map $v' \circ \sigma$ is the unique valuation of $N$ that corresponds to $\sigma^{-1}(\mathcal{O}')$ and $\Gamma'$. In particular, if $\sigma(\mathcal{O}') = \mathcal{O}'$, then $v' \circ \sigma = v'$.*

*(2) $\overline{N}$ is a normal extension of $\overline{K}$.*

*(3) The map $x \mapsto \overline{\sigma(x)}$ is a ring homomorphism from $\sigma^{-1}(\mathcal{O}')$ onto $\overline{N}$. This homomorphism induces a $\overline{K}$-isomorphism from $\sigma^{-1}(\mathcal{O}')/\sigma^{-1}(\mathcal{M}')$ onto $\overline{N}$ which satisfies $\overline{\sigma}(u + \sigma^{-1}(\mathcal{M}')) = \overline{\sigma(u)}$ for every $u \in \sigma^{-1}(\mathcal{O}')$. In particular, if $\sigma(\mathcal{O}') = \mathcal{O}'$, then $\overline{\sigma} \in \mathrm{Aut}(\overline{N}/\overline{K})$.*

*(4) $e(\sigma^{-1}(\mathcal{O}')/\mathcal{O}) = e(\mathcal{O}'/\mathcal{O})$ and $f(\sigma^{-1}(\mathcal{O}')/\mathcal{O}) = f(\mathcal{O}'/\mathcal{O})$, for every $\sigma \in \mathrm{Aut}(N/K)$.*

*Proof.* (1) Clearly $v' \circ \sigma : N \longrightarrow\!\!\!\!\!\rightarrow \Gamma' \cup \{\infty\}$ is a valuation on $N$ satisfying

$$\{\, x \in N \mid v' \circ \sigma(x) \geq 0 \,\} = \sigma^{-1}(\mathcal{O}') \,.$$

Next let $w : N \longrightarrow\!\!\!\!\!\rightarrow \Gamma' \cup \{\infty\}$ be a valuation on $N$ having $\sigma^{-1}\mathcal{O}'$ as valuation ring. Then $v' \circ \sigma$ and $w$ are equivalent valuations. According to Proposition 2.1.3 there exists an order-preserving isomorphism $\varrho : \Gamma' \longrightarrow \Gamma'$ such that $\varrho \circ w = v' \circ \sigma$. Thus $\varrho(\gamma) = \gamma$ for every $\gamma \in \Gamma$ (= the value group of $v$). In general, for $\delta \in \Gamma'$, by Theorem 3.2.4, there is $n > 1$ such that $n\delta \in \Gamma$. Hence $n\varrho(\delta) = \varrho(n\delta) = n\delta$, yielding $\varrho(\delta) = \delta$, since $\Gamma'$ is torsion-free.

(2) Let $\overline{f} \in \overline{K}[X]$ be an irreducible polynomial with a root $\alpha \in \overline{N}$.

Let $R$ be the integral closure of $\mathcal{O}$ in $N$ and write $\mathfrak{m} = \mathcal{M}' \cap R$. By Theorem 3.2.13, $\mathcal{O}' = R_{\mathfrak{m}}$. Hence the map $x \mapsto \overline{x}$ induces a surjective map $R \longrightarrow \overline{N}$. Observe next that for every $\sigma \in \mathrm{Aut}(N/K)$, $\sigma(R) = R$. Indeed, each $\sigma$ permutes the valuation rings of $N$ that lie over $\mathcal{O}$. Thus for $x \in R$ it follows that $\sigma(x) \in R$ for every $\sigma \in \mathrm{Aut}(N/K)$. Now take $x \in R$ such that $\overline{x} = \alpha$ and let $g \in \mathcal{O}[X]$ be the minimal polynomial of $x$ over $K$. Since $N/K$ is normal, $g = (X - x_1) \cdots (X - x_n)$, for $n = \deg g$ and $x = x_1, \ldots, x_n \in R$. From $\overline{g}(\alpha) = 0$, it follows that $\overline{f}$ divides $\overline{g}$. But $\overline{g} = (X - \overline{x_1}) \cdots (X - \overline{x_n})$ in $\overline{N}$. Hence $\overline{f}$ has all its roots in $\overline{N}$, proving (2).

(3) As a composition of ring homomorphisms, the map $x \mapsto \overline{\sigma(x)}$ is a ring homomorphism. The other statements are proved by standard computations.

(4) An immediate consequence of (3). □

*Remark 3.2.17.* Let $L/K$ be a finite Galois extension with $[L : K] = n$, and write $N : L \longrightarrow K$ for the norm map. Suppose that a valuation ring $\mathcal{O}$ of $K$ has a unique prolongation $\mathcal{O}'$ to $L$, and let $v$ be a valuation on $K$ corresponding to $\mathcal{O}$. Then

$$w(x) = \frac{1}{n} v(N(x))$$

is the unique valuation of $L$ extending $v$.

Actually, we can drop the finiteness assumption. In fact, in case $L$ is the separable closure of $K$, for $x \in L$ let $f(X) = a_n + a_{n-1}X + \cdots + X^n$ be its minimal polynomial over $K$. Then

$$w(x) = \frac{1}{n} v(a_n) \ .$$

*Proof.* Let $x = x_1, \ldots, x_n$ be all the conjugates of $x$. Then $w(x) = w(x_i)$, by (1) of Proposition 3.2.16. Hence

$$v(N(x)) = w(x_1 x_2 \cdots x_n) = nw(x). \qquad \square$$

## 3.3 The Fundamental Inequality

Let $(K, \mathcal{O})$ be a valued field, and assume $L/K$ is a finite extension. We would then like to know as much as possible about all prolongations of $\mathcal{O}$ to $L$. In the last section we saw (Theorem 3.2.9) that the number $r$ of prolongations is bounded by the degree $n = [L : K]$. We also saw (Corollary 3.2.3) that $ef \leq n$, where $e = e(\mathcal{O}_1/\mathcal{O})$ is the ramification index and $f = f(\mathcal{O}_1/\mathcal{O})$ the

residue degree of a prolongation $\mathcal{O}_1$ of $\mathcal{O}$ to $L$. In this section we shall prove even more, namely

$$\sum_{i=1}^{r} e(\mathcal{O}_i/\mathcal{O}) f(\mathcal{O}_i/\mathcal{O}) \leq n \ ,$$

where $\mathcal{O}_1, \ldots, \mathcal{O}_r$ are all the prolongations of $\mathcal{O}$ to $L$. This inequality is called the *fundamental inequality*. In case the value group of $\mathcal{O}$ is $\mathbb{Z}$, and $L/K$ is separable, even equality will be proved.

We shall first treat the case of a Galois extension $L/K$. This can be done with what we have developed so far. For the general case, however, we have to refer to some results that need the structure theory of Chap. 5. Let us start with a lemma that is also basic for the theory of henselian fields.

**Lemma 3.3.1.** *Let $(K, \mathcal{O}) \subseteq (N, \mathcal{O}^*)$ be an extension of valued fields. Assume that $N/K$ is a finite Galois extension with Galois group $G(N/K)$. Let $L$ be the fixed field of the subgroup $H = \{\, \sigma \in G(N/K) \mid \sigma(\mathcal{O}^*) = \mathcal{O}^* \,\}$, and set $\mathcal{O}' = \mathcal{O}^* \cap L$. Then $(L, \mathcal{O}')$ is an immediate extension of $(K, \mathcal{O})$. Moreover, $\mathcal{O}^*$ is the unique extension of $\mathcal{O}'$ to $N$.*

*Proof.* Let $\mathcal{O}^* = \mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m$ be the collection of all extensions of $\mathcal{O}$ to $N$, with corresponding maximal ideals $\mathcal{M}_1, \ldots, \mathcal{M}_m$. Moreover, let $\mathcal{O}'_i = \mathcal{O}_i \cap L$ for $1 \leq i \leq m$. We then consider the subring

$$R = \mathcal{O}'_1 \cap \cdots \cap \mathcal{O}'_m$$

of $L$. By Theorem 3.2.7 and Lemma 3.2.8, the maximal ideals of $R$ are given by $\mathfrak{p}_i = R \cap \mathcal{M}_i$. Note, however, that for $i \neq j$ we may have $\mathfrak{p}_i = \mathfrak{p}_j$. This is not the case if $i = 1$. In fact, if $\mathfrak{p}_1 = \mathfrak{p}_j$, then

$$\mathcal{O}^* \cap L = \mathcal{O}'_1 = R_{\mathfrak{p}_1} = R_{\mathfrak{p}_j} = \mathcal{O}'_j = \mathcal{O}_j \cap L \ .$$

Hence by the Conjugation Theorem 3.2.15, $\mathcal{O}_j = \sigma\mathcal{O}^*$ for some $\sigma \in G(N/L) = H$. But then $\mathcal{O}_j = \mathcal{O}^*$, by the definition of $H$.

Let us next prove that $\mathcal{O}$ and $\mathcal{O}'$ have the same residue class field. Given $\alpha \in \mathcal{O}'$, by the approximation condition (3) of Theorem 3.2.7, we can find $\beta \in R$ such that $\beta - \alpha \in \mathcal{M}_1$ and $\beta \in \mathcal{M}_i$ for all $i$ with $1 < i \leq m$. Let $\beta = \beta_1, \beta_2, \ldots, \beta_n$ be the collection of all distinct $K$-conjugates of $\beta$ in $N$, and assume

$$\mathrm{Irr}(\beta, K) = X^n + a_1 X^{n-1} + \cdots + a_n \ .$$

Then clearly $a_1 = -(\beta_1 + \cdots + \beta_n)$. We shall show that

$$\alpha + a_1 = (\alpha - \beta_1) - \beta_2 - \cdots - \beta_n \in \mathcal{M}_1 \ .$$

Then $\overline{\alpha} = -\overline{a_1} \in \overline{K}$, showing that $\overline{L} = \overline{K}$. Since $\alpha - \beta_1 \in \mathcal{M}_1$, it remains to show that $\beta_j \in \mathcal{M}_1$ for every $j \geq 2$. Since $\beta_j \neq \beta_1$, we get $\beta_j = \tau(\beta)$ for some $\tau \in G(N/K) \setminus H$, as $\beta \in L$. Hence $\tau^{-1}(\mathcal{O}_1) = \mathcal{O}_i$ for some $i$ with

$1 < i \leq m$. Since by the approximation condition $\beta \in \mathcal{M}_i = \tau^{-1}(\mathcal{M}_1)$, we get $\beta_j = \tau(\beta) \in \mathcal{M}_1$.

Now let us prove that $\mathcal{O}$ and $\mathcal{O}'$ have the same value group. Write $w$ for the valuation corresponding to $\mathcal{O}^*$, and let $\alpha \in L^\times$ be given. We have to find some $a \in K^\times$ such that $w(a) = w(\alpha)$.

As above we use the approximation property for $R$ to find $\beta \in R$ with $\beta - 1 \in \mathcal{M}_1$ and $\beta \in \mathcal{M}_i$ for all $2 \leq i \leq m$. From $\beta - 1 \in \mathcal{M}_1$ it follows that $w(\tau(\beta)) = 0$ for all $\tau \in H$, and as above, $\beta \in \mathcal{M}_i$ for all $2 \leq i \leq m$ yields $w(\tau(\beta)) > 0$ for all $\tau \in G(N/K) \setminus H$. Since $\{\, w(\tau(\alpha)) \mid \tau \in G(N/K) \,\}$ is finite, it is possible to choose $\nu \in \mathbb{Z}$ such that

$$w(\beta^\nu \alpha) \neq w(\tau(\beta^\nu \alpha))$$

for all $\tau \in G(N/K) \setminus H$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the collection of distinct conjugates of $\beta^\nu \alpha = \alpha_1$ in $N$. Note that for every $j$ with $1 < j \leq n$ we have $\alpha_j = \tau(\alpha_1)$ for some $\tau \in G(N/K) \setminus H$, and thus $w(\alpha_j) \neq w(\alpha_1)$. For the irreducible polynomial $X^n + a_1 X^{n-1} + \cdots + a_n$ of $\alpha_1$ over $K$ we have

$$a_t = (-1)^t \cdot \sum_{1 \leq i_1 < \cdots < i_t \leq n} \alpha_{i_1} \cdots \alpha_{i_t} \ .$$

Suppose now that $j_1 < \cdots < j_r$ are the indices $j \geq 2$ for which $w(\alpha_j) < w(\alpha_1)$. In case there is no such $j$, obviously $w(a_1) = w(\alpha_1) = w(\alpha)$, and we are done. Otherwise we see that

$$w(a_r) = w(\alpha_{j_1} \cdots \alpha_{j_r}) \ ,$$

since all other summands of $a_r$ have higher value. Similarly we see that

$$w(a_{r+1}) = w(\alpha_1 \alpha_{j_1} \cdots \alpha_{j_r}) \ .$$

Thus we obtain

$$w(a_{r+1}) - w(a_r) = w(\alpha_1) = w(\alpha) \ .$$

Hence we may take $a = a_{r+1}/a_r \in K$ in order to get $w(\alpha) = w(a)$.

Thus we have finally obtained that $(L, \mathcal{O}')$ is an immediate extension of $(K, \mathcal{O})$. The last statement of the Lemma is clear from the proof. □

From Proposition 3.2.16(4) we know that, for a Galois extension $N/K$, all prolongations $\mathcal{O}_1, \ldots, \mathcal{O}_r$ of the valuation ring $\mathcal{O}$ from $K$ to $L$ have equal ramification indices and equal residue degrees, i.e., $e = e(\mathcal{O}_i/\mathcal{O})$ and for $f = f(\mathcal{O}_i/\mathcal{O})$ for all $1 \leq i \leq r$. Thus, in the Galois case we expect $ref \leq n$ to hold.

**Lemma 3.3.2.** *Let $N/K$ be a finite Galois extension of degree $n$. Assume that $\mathcal{O}_1, \ldots, \mathcal{O}_r$ are all prolongations of the valuation ring $\mathcal{O}$ from $K$ to $N$. Then $ref \leq n$, where $e = e(\mathcal{O}_i/\mathcal{O})$ and $f = f(\mathcal{O}_i/\mathcal{O})$ for all $i$ with $1 \leq i \leq r$.*

*Proof.* Let $H = \{\, \sigma \in G(N/K) \mid \sigma(\mathcal{O}_1) = \mathcal{O}_1 \,\}$, and consider the decomposition

$$G = G(N/K) = \bigcup_{i=1}^{r} \sigma_i H \ ,$$

where we choose $\sigma_1 = \mathrm{id}$. According to the Conjugation Theorem 3.2.15, $\sigma_1(\mathcal{O}_1), \ldots, \sigma_r(\mathcal{O}_1)$ are exactly all prolongations of $\mathcal{O}$ to $N$.

Now let $L$ be the fixed field of $H$ and set $\mathcal{O}_L = \mathcal{O}_1 \cap L$. Then $N/L$ is a Galois extension with Galois group $H$ and $[N : L] = |H| = n/r$. Applying Corollary 3.2.3 to the extension $N/L$ gives

$$e(\mathcal{O}_1/\mathcal{O}_L) f(\mathcal{O}_1/\mathcal{O}_L) \leq [N : L] = \frac{n}{r} \ .$$

By Lemma 3.3.1, $e(\mathcal{O}_L/\mathcal{O}) = 1 = f(\mathcal{O}_L/\mathcal{O})$. This together with the multiplicativity of $e$ and $f$ (Remark 3.2.1) finally gives

$$ref = r \cdot e(\mathcal{O}_1/\mathcal{O}) f(\mathcal{O}_1/\mathcal{O}) = r \cdot e(\mathcal{O}_1/\mathcal{O}_L) f(\mathcal{O}_1/\mathcal{O}_L) \leq r\frac{n}{r} = n \qquad \square$$

For a Galois extension $N/K$, more can be said than just "$ref \leq n$". Actually $ref$ divides $n$ and the quotient is a power of $p$ in case $\mathrm{char}\, \overline{K} = p$, where $\overline{K}$ is the residue class field of $(K, \mathcal{O})$. If $\mathrm{char}\, \overline{K} = 0$, then we simply get $ref = n$. From these improvements for Galois extensions we shall then deduce the fundamental inequality in full generality. Before we can do so, however, we need to refer to some specific results from Chap. 5. Although we don't use the improvement in the Galois case (and the general fundamental inequality) before Chap. 5, we think that even those readers who will not make it to Chap. 5 should already here be introduced to the (general) fundamental inequality.

In Chap. 5 we shall fix a valued field $(K, \mathcal{O})$, extend $\mathcal{O}$ to a valuation ring $\mathcal{O}^s$ of the separable closure $K^s$ of $K$, and consider a certain sequence of valued fields:

$$(K, \mathcal{O}) \subseteq (K^h, \mathcal{O}^h) \subseteq (K^t, \mathcal{O}^t) \subseteq (K^v, \mathcal{O}^v) \subseteq (K^s, \mathcal{O}^s) \ .$$

$(K^h, \mathcal{O}^h)$ will be called the "henselization" of $(K, \mathcal{O})$, while $(K^t, \mathcal{O}^t)$ and $(K^v, \mathcal{O}^v)$ will be called the "inertia field" and the "ramification field" of $(K, \mathcal{O})$.

Intersecting all fields from the sequence $K \subseteq K^h \subseteq K^t \subseteq K^v \subseteq K^s$ with the Galois extension $N$ of $K$, we obtain

$$K \subseteq K_h \subseteq K_t \subseteq K_v \subseteq N$$

where $K_h := K^h \cap N = L, K_t := K^t \cap N$, and $K_v := K^v \cap N$. The results of Chap. 5 (collected in Corollary 5.3.8) we are going to use here, are the following facts (since it is always clear to which valuation ring we refer, we only mention the corresponding fields in $e$ and $f$):

(0) $e(K_h/K) = 1$ and $f(K_h/K) = 1$

(1) $e(K_t/K_h) = 1$ and $f(K_t/K_h) = [K_t : K_h]$

(2) $f(K_v/K_t) = 1$ and $e(K_v/K_t) = [K_v : K_t]$

(3) $[N : K_v], e(N/K_v), f(N/K_v)$ are powers of $p$, where $p = 1$ if $\operatorname{char} \overline{K} = 0$, and $p = \operatorname{char} \overline{K}$, otherwise.

Using the multiplicativity of $e$ and $f$, we therefore get

$$e(K_v/K_h)f(K_v/K_h) = [K_v : K_h] .$$

Using (3) and applying Corollary 3.2.3 to $N/K_v$, we obtain

$$d \cdot e(N/K_h)f(N/K_h) = [N : K_h] ,$$

where $d = 1$ if $\operatorname{char} \overline{K} = 0$, and a certain power of $p$ if $\operatorname{char} \overline{K} = p$.

Entering with this extra information into the proof of Lemma 3.3.2 and observing that $L = K_h$ (as is shown in the proof of Theorem 5.2.5), we get

**Theorem 3.3.3.** *Let $N/K$ be a finite Galois extension of degree $n$. Assume that $\mathcal{O}_1, \ldots, \mathcal{O}_r$ are the distinct prolongations of the valuation ring $\mathcal{O}$ from $K$ to $N$. Then $n = refd$, where $e = e(\mathcal{O}_i/\mathcal{O}), f = f(\mathcal{O}_i/\mathcal{O})$ for all $1 \leq i \leq r$, and $d$ is a power of $p$ if $p = \operatorname{char} \overline{K}$, and $d = 1$ otherwise.*

In the situation of Theorem 3.3.3, the quotient

$$d = \frac{[N : K]}{re(N/K)f(N/K)}$$

is called the *defect* of $\mathcal{O}$ in the Galois extension $N/K$. If $d = 1$ the extension is called *defectless* .

From Theorem 3.3.3 we finally obtain

**Theorem 3.3.4.** (Fundamental Inequality) *Let $L/K$ be a finite extension of the valued field $(K, \mathcal{O})$, and assume that $\mathcal{O}_1, \ldots, \mathcal{O}_r$ are all prolongations of $\mathcal{O}$ to $L$. Then*

$$\sum_{i=1}^{r} e(\mathcal{O}_i/\mathcal{O})f(\mathcal{O}_i/\mathcal{O}) \leq [L : K] .$$

*Proof.* Let $F$ be the relative separable closure of $K$ in $L$. Every valuation ring of $F$ has a unique prolongation to $L$ (Corollary 3.2.10). Then using Corollary 3.2.3 for the extension $L/F$, one sees that it suffices to prove the fundamental inequality for the separable extension $F/K$. Thus without loss of generality we may assume that the extension $L/K$ is already separable.

Let $N/K$ be the Galois closure of $L/K$ (taking $N$ as the splitting field of the minimal polynomial of a generating element of $L$ over $K$). We shall then compare the Galois extension $N/K$ with the Galois extension $N/L$.

From the definition of the "ramification field" $K^v$ in Sect. 5.3, it follows immediately that $K^v \subseteq L^v$. Thus we have

$$K_v = K^v \cap N \subseteq L^v \cap N = L_v \ ,$$

and hence in particular that $[N : L_v]$ divides $[N : K_v]$.

Now we shall first apply Theorem 3.3.3 to the Galois extension $N/K$, obtaining

$$[N : K] = sefd, \tag{$*$}$$

where $s$ is the number of all prolongations of $\mathcal{O}$ to $N$, and $e, f, d$ are the obvious terms. Next we apply Theorem 3.3.3 to the Galois extension $N/L$ together with the valuation ring $\mathcal{O}_i$ of $L$, assuming that $\mathcal{O}_{i1}, \ldots, \mathcal{O}_{it_i}$ are all prolongations of $\mathcal{O}_i$ to $N$. Hence we obtain

$$[N : L] = t_i e_i f_i d_i, \tag{$**$}$$

where the terms $e_i, f_i, d_i$ refer to the valuation ring $\mathcal{O}_i$, i.e., $e_i = e(\mathcal{O}_{i1}/\mathcal{O}_i)$, $f_i = f(\mathcal{O}_{i1}/\mathcal{O}_i)$, and $d_i$ refers to a prolongation of $\mathcal{O}_i$ to $K^s$. From the inclusion $K_v \subseteq L_v$ for the corresponding $i$, we get (as explained above) that $d_i$ divides $d$ for all $i$ with $1 \leq i \leq r$. Using the multiplicativity of $e$ and $f$, we get from $(**)$

$$[N : L] \cdot e(\mathcal{O}_i/\mathcal{O}) f(\mathcal{O}_i/\mathcal{O}) \frac{d}{d_i} = t_i efd \ .$$

Since $s = \sum_{i=1}^{r} t_i$, the identity $(*)$ above gives

$$[N : K] = \left( \sum_{i=1}^{r} t_i \right) \cdot efd = [N : L] \cdot \sum_{i=1}^{r} e(\mathcal{O}_i/\mathcal{O}) f(\mathcal{O}_i/\mathcal{O}) \frac{d}{d_i} \ .$$

Dividing by $[N : L]$ and observing that $d/d_i \geq 1$ we get the desired inequality. □

The next theorem shows that in case $\mathcal{O}$ has value group $\mathbb{Z}$ and $L/K$ is separable, even equality holds in Theorem 3.3.4. Let us point out that the proof of this equality does not use the fundamental inequality and hence also no result from Chap. 5. The proof is completely selfcontained and elementary.

**Theorem 3.3.5.** *Let $(K, \mathcal{O})$ be a valued field with value group $\mathbb{Z}$, and let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be all extensions of $\mathcal{O}$ to a finite separable extension $L$ of $K$. Then*

$$[L : K] = \sum_{i=1}^{m} e(\mathcal{O}_i/\mathcal{O}) f(\mathcal{O}_i/\mathcal{O}) \ .$$

*Proof.* Let $\Gamma$ be the value group of $\mathcal{O}$ and let $\Gamma_i$ be the value group of $\mathcal{O}_i$. Since $\Gamma \cong \mathbb{Z}$ also $\Gamma_i \cong \mathbb{Z}$ ($\Gamma_i$ is torsion-free and $\Gamma_i/\Gamma$ is finite) and $\Gamma_i/\Gamma$ is a cyclic group of order $e_i$. Let $\pi$ be an element of $\mathcal{O}$ having the smallest positive value and for every $i$ let $\pi_i$ be some element of $\mathcal{O}_i$ with the same property. By Corollary 3.1.4, $R = \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_m$ is the integral closure of $\mathcal{O}$ in $L$. We shall prove the following three facts which imply the result:

(a) $\mathcal{O}_i/\pi\mathcal{O}_i$ is a $\overline{K}$-vector space of dimension $e_i f_i$.
(b) $R/\pi R \cong \prod_{i=1}^{m}(\mathcal{O}_i/\pi\mathcal{O}_i)$, as $\overline{K}$-vector spaces.
(c) $R/\pi R$ has $\overline{K}$-dimension $[L : K]$.

(a): Observe that

$$\mathcal{M}_i = \pi_i\mathcal{O}_i \supsetneqq \pi_i^2\mathcal{O}_i \supsetneqq \cdots \supsetneqq \pi_i^{e_i}\mathcal{O}_i = \pi\mathcal{O}_i \ .$$

For every $1 \leq j \leq e_i - 1$ the additive quotient group

$$\overline{L}_j = \pi_i^j\mathcal{O}_i/\pi_i^{j+1}\mathcal{O}_i$$

naturally is a $\overline{K}$-vector space for which the map

$$\pi_i^j x + \pi_i^{j+1}\mathcal{O}_i \longmapsto x + \mathcal{M}_i$$

from $\overline{L}_j$ to $\mathcal{O}_i/\mathcal{M}_i$ is an isomorphism. Consequently $\overline{L}_j$ has $\overline{K}$-dimension $f_i$ for every $1 \leq j \leq e_i$. Thus, $\mathcal{O}_i/\pi\mathcal{O}_i$ has dimension $e_i f_i$ as a $\overline{K}$-vector space.

(b): By Theorem 3.2.7 (3), the map $\Theta(x) = (x + \pi\mathcal{O}_1, \ldots, x + \pi\mathcal{O}_m)$ from $R$ to $\prod_{i=1}^{m}(\mathcal{O}_i/\pi\mathcal{O}_i)$ is surjective. Then, to see that $\Theta$ induces the desired isomorphism it suffices to show that $\pi R$ is its kernel. Clearly $\pi R \subseteq \ker(\Theta)$. Conversely, take $x \in R$ such that $x \in \pi\mathcal{O}_i$ for every $1 \leq i \leq m$. Then $\pi^{-1}x \in \mathcal{O}_1 \cap \cdots \cap \mathcal{O}_m = R$ and so $x \in \pi R$, as required.

(c): It follows from (a) and (b) that $R/\pi R$ is a $\overline{K}$-vector space of dimension $n = \sum_{i=1}^{m} e_i f_i$. Let $x_1, \ldots, x_n \in R$ such that $\overline{x_1}, \ldots, \overline{x_n}$ is a $\overline{K}$-basis of $R/\pi R$. We first show that $x_1, \ldots, x_n$ are linearly independent over $K$. In fact, suppose that $a_1, \ldots, a_n \in K$ are not all zero and $a_1x_1 + \cdots + a_nx_n = 0$. Write $a_i = \pi^{\nu_i}u_i$, where $\nu_i \in \mathbb{Z}$ and $u_i \in \mathcal{O}^\times \cup \{0\}$, for every $i = 1, \ldots, n$. For $1 \leq j \leq n$ such that $\nu_j = \min\{\nu_1, \ldots, \nu_n\}$ we get

$$\pi^{\nu_1 - \nu_j}u_1x_1 + \cdots + \pi^{\nu_n - \nu_j}u_nx_n = 0 \ .$$

Thus $\overline{\pi^{\nu_1-\nu_j}}\,\overline{u_1x_1} + \cdots + \overline{\pi^{\nu_n-\nu_j}}\,\overline{u_nx_n} = 0$ with some $\overline{u_j} \neq 0$, a contradiction.

We shall next prove that $x_1, \ldots, x_n$ is a $K$-basis of $L$. From [32, Corollary 1, p. 265] we know that $R$ is a finitely generated $\mathcal{O}$-module. Since $\pi\mathcal{O}$ is the Jacobson radical of $\mathcal{O}$, by [1, Proposition 2.8], $x_1, \ldots, x_n$ generate $R$ as $\mathcal{O}$-module.

Take now $y \in L^\times$ and let $a_r + \cdots + a_1X^{r-1} + X^r$ be the minimal polynomial of $y$ over $K$. Write $a_j = \pi^{\eta_j}u_j$ as above, for each $j = 1, \ldots, r$. Set

$$\eta = \begin{cases} \min\{\,\eta_j \mid \eta_j < 0\} & \text{if there exists } j \text{ such that } \eta_j < 0 \\ 1 & \text{otherwise} \end{cases}$$

Then $y\pi^{-\eta}$ is a root of $\pi^{\eta_r - r\eta}u_r + \cdots + \pi^{\eta_1-\eta}u_1X^{r-1} + X^r$. Since $R$ is the integral closure of $\mathcal{O}$, $y\pi^{-\eta} \in R$. As we have proved that $R = \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$, we may conclude that $y \in Kx_1 + \cdots + Kx_n$. Hence $[L : K] = n$. □

## 3.4 Transcendental Extensions

In Sect. 2.2 we already studied the extension of a valuation $v$ of a field $K$ to the rational function field $K(X)$. Now we continue this study to field extensions of finite transcendence degree over $K$. In particular we shall prove the very important "Dimension inequality" Theorem 3.4.3.

We start this section by introducing an invariant for abelian groups that is connected with the rank for ordered abelian groups.

Consider an abelian group $G$ as a $\mathbb{Z}$-module and write $G_d = G \otimes_{\mathbb{Z}} \mathbb{Q}$ for the tensor product. $G_d$ is a $\mathbb{Q}$-vector space in the obvious way. We define its dimension over $\mathbb{Q}$ to be the *rational rank* of $G$. We write $\mathrm{rr}(G)$ for the rational rank. Alternatively, the rational rank of $D$ is the maximal number (finite or infinite) of elements of $G$ that are linearly independent over $\mathbb{Z}$.

Observe first that $\mathrm{rr}(G) = 0$ if and only if $G$ is a torsion group. In fact the map $\iota : G \to G_d$ defined by $\iota(g) = g \otimes 1$ is a group homomorphism; the quotient group $G_d/\iota(G)$ is a torsion group. We shall call $G_d$ the *divisible hull* of $G$, since this group is in some sense the smallest group with the above property. Every homomorphism $\varphi : G \longrightarrow G'$ to a divisible group $G'$ such that $G'/\varphi(G)$ is a torsion group has a unique "extension" $G_d \longrightarrow G'$ satisfying $g \otimes 1 \mapsto \varphi(g)$, for all $g \in G$.

Every element of $G_d$ has a representation in the form:

$$g \otimes \frac{1}{n} \,,$$

for some $g \in G$ and $n \in \mathbb{N}$. Indeed, for $g_1, \ldots, g_r \in G$ and $a_1/b_1, \ldots, a_r/b_r \in \mathbb{Q}$ take $b \in \mathbb{N}$ such that $a_i/b_i = c_i/b$ for some $c_i \in \mathbb{Z}$ and every $i = 1, \ldots, r$. Then

$$g_1 \otimes \frac{a_1}{b_1} + \cdots + g_r \otimes \frac{a_r}{b_r} = g_1 \otimes \frac{c_1}{b} + \cdots + g_r \otimes \frac{c_r}{b} = (c_1g_1 + \cdots + c_rg_r) \otimes \frac{1}{b} \,.$$

Now, if $G$ is an ordered abelian group, we endow $G_d$ with an ordering defined by

$$g \otimes \frac{1}{m} \;\leq\; g' \otimes \frac{1}{n} \quad \Longleftrightarrow \quad ng \leq mg' \,.$$

An easy exercise shows that this definition does not depend on the representations of $g \otimes (1/m)$ and $g' \otimes (1/n)$, and produces an ordering on $G_d$ extending the one of $G$. Additionally, as an ordered group, $G$ is torsion free; thus, we may consider $G \subseteq G_d$, and so the name "divisible hull" is even more appropriate.

Moreover, the above discussion together with Theorem 3.2.4 and Corollary 3.2.11 shows that if we extend a valuation ring $\mathcal{O}$ in $K$ to $\widetilde{\mathcal{O}}$ in the

algebraic closure $\widetilde{K}$ of $K$, then the value group $\widetilde{\Gamma}$ of $\widetilde{\mathcal{O}}$ is the divisible hull of the value group $\Gamma$ of $\mathcal{O}$.

Returning to the rational rank, we observe that $\mathrm{rr}(\mathbb{Z}) = 1$, $\mathrm{rr}(\mathbb{Q}) = 1$, $\mathrm{rr}(\mathbb{Z}^n) = n$, and $\mathrm{rr}(\mathbb{R}) = \infty$. Furthermore, an easy calculation shows that if $H$ is a subgroup of an abelian group $G$, then $\mathrm{rr}(G) = \mathrm{rr}(H) + \mathrm{rr}(G/H)$. (Note that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.)

Let us now denote by $\mathrm{rk}(G)$ the rank of an ordered abelian group as defined in Sect. 2.1. Since $G_d/G$ is a torsion group, $\mathrm{rk}(G_d) = \mathrm{rk}(G)$. More generally:

**Proposition 3.4.1.** *Let $G$ be an ordered abelian group and let $H$ be a subgroup of $G$. Then*

$$\mathrm{rk}(G) \leq \mathrm{rk}(H) + \mathrm{rr}(G/H) \ .$$

*In particular, taking $H = \{0\}$ we conclude that* $\mathrm{rk}(G) \leq \mathrm{rr}(G)$.

*Proof.* Let $G_0 \subsetneqq G_1 \subsetneqq \cdots \subsetneqq G_r = G$ be a chain of convex subgroups of $G$. We shall show by induction on $r$ that $r \leq \mathrm{rk}(H) + \mathrm{rr}(G/H)$. The statement is clearly true for $r = 0$. Assume $r \geq 1$. By the inductive hypothesis,

$$r - 1 \leq \mathrm{rk}(G_{r-1} \cap H) + \mathrm{rr}(G_{r-1}/(G_{r-1} \cap H)) \ .$$

If $H \subseteq G_{r-1}$, then $r \leq \mathrm{rk}(H) + \mathrm{rr}(G_{r-1}/H) + 1$. Since $G/G_{r-1}$ is an ordered group, it is torsion-free. Thus $\mathrm{rr}(G/G_{r-1}) \neq 0$, which implies

$$\mathrm{rr}(G/H) = \mathrm{rr}(G/G_{r-1}) + \mathrm{rr}(G_{r-1}/H) \geq \mathrm{rr}(G_{r-1}/H) + 1 \ ,$$

and the result holds in this case.

In the other case, $G_{r-1} \cap H$ is a proper convex subgroup of $H$. Thus $\mathrm{rk}(H) > \mathrm{rk}(G_{r-1})$. Since $\mathrm{rr}(G/H) \geq \mathrm{rr}(G_{r-1}/(G_{r-1} \cap H))$, we may also conclude the inequality. □

**Theorem 3.4.2.** *Suppose $L/K$ is a field extension, $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ is a valuation on $K$, and $w : L \longrightarrow\!\!\!\!\!\rightarrow \Delta \cup \{\infty\}$ is an extension of $v$ to $L$. Let $\mathcal{O}$ be the valuation ring of $L$ corresponding to $w$.*

*Let $x_1, \ldots, x_r \in \mathcal{O}$ be such that $\overline{x_1}, \ldots, \overline{x_r} \in \overline{L}$ are algebraically independent over $\overline{K}$. Further let $y_1, \ldots, y_s \in L^\times$ be such that $\overline{w(y_1)}, \ldots, \overline{w(y_s)} \in \Delta/\Gamma$ are $\mathbb{Z}$-linearly independent. Then $x_1, \ldots, x_r, y_1, \ldots, y_s$ are algebraically independent over $K$. Moreover, the restriction $v'$ of $w$ to $K' = K(x_1, \ldots, x_s, y_1, \ldots, y_r)$ has $\overline{K}(\overline{x_1}, \ldots, \overline{x_r})$ as residue class field and $\Gamma + \mathbb{Z}v'(y_1) + \cdots + \mathbb{Z}v'(y_s)$ as value group.*

*Proof.* We first show the result in the cases $r = 1$, $s = 0$ and $r = 0$, $s = 1$ (the case $r = 0 = s$ is trivial). Next we shall work step by step adding one element each time.

Applying Theorem 3.2.4 to $K(x_1)$ in the case $r = 1$ and $s = 0$, we see that $x_1$ cannot be algebraic over $K$. The other statements follow from Corollary 2.2.2. In the case $s = 1$ and $r = 0$, Theorem 3.2.3 also shows that $y_1$ is transcendental over $K$, while Corollary 2.2.3 provides the other conclusions.

Now we prove the result by induction on $r+s$. The case $r+s=1$ is the content of what we just did. Suppose the result holds for every pair $m,n$ such that $m+n<k$, and assume $r+s=k$, with $s\neq 0$. Since $x_1,\dots,x_r,y_1,\dots,y_{s-1}\in L_1=K(x_1,\dots,x_r,y_1,\dots,y_{s-1})$ satisfy the assumptions of the induction hypothesis, they are algebraically independent over $K$, and the valuation ring $\mathcal{O}_1=\mathcal{O}\cap L_1$ has residue field $\overline{L_1}$ and value group $\overline{\Gamma_1}$ as described in the theorem. Since by the case $r+s=1$ we have $y_s$ transcendental over $L_1$, it follows that $x_1,\dots,x_r,y_1,\dots,y_s$ are algebraically independent over $K$ as desired.

The other statements follow by induction and by the case $r+s=1$ applied to the extension $L/L_1$; observe the picture below.

$$\begin{array}{lll}
L & \overline{L} & \Delta \\
\vert & \vert & \vert \\
K' & \overline{K'}=\overline{L_1} & \Delta'=\Delta_1+\mathbb{Z}v'(y_s) \\
\vert & \vert & \vert \\
L_1 & \overline{L_1}=\overline{K}(\overline{x_1},\dots,\overline{x_r}) & \Delta_1=\Gamma+\mathbb{Z}v_1(y_1)+\cdots+\mathbb{Z}v_1(y_{s-1}) \\
\vert & \vert & \vert \\
K & \overline{K} & \Gamma
\end{array}$$

In case $r\neq 0$ we proceed analogously. □

For every extension of fields $E/F$, let tr.deg.$(E/F)$ denote the transcendence degree of $E$ over $F$.

**Theorem 3.4.3.** (Dimension Inequality) *Keeping the notation as in Theorem 3.4.2, it follows that*

$$\text{tr.deg.}\big(\overline{L}/\overline{K}\big)+\text{rr}(\Delta/\Gamma)\leq\text{tr.deg.}(L/K)\ . \tag{3.4.1}$$

*Moreover, if $L$ is finitely generated over $K$, and equality holds in 3.4.1, then $\Delta/\Gamma$ is a finitely generated $\mathbb{Z}$-module and $\overline{L}$ is finitely generated over $\overline{K}$.*

*Proof.* For every pair of numbers $r\leq\text{tr.deg.}\big(\overline{L}/\overline{K}\big)$ and $s\leq\text{rr}(\Delta/\Gamma)$, we can pick elements $x_1,\dots,x_r,y_1,\dots,y_s\in L$ satisfying the assumptions of Theorem 3.4.2. Hence $r+s\leq\text{tr.deg.}(L/K)$, and so the inequality (3.4.1) is proved.

If $L$ is finitely generated over $K$, then tr.deg.$(L/K)$ is finite. Thus, (3.4.1) implies that $r:=\text{tr.deg.}\big(\overline{L}/\overline{K}\big)$ and $s:=\text{rr}(\Delta/\Gamma)$ are finite, too. Now, if $r+s=\text{tr.deg.}(L/K)$ and we choose $x_1,\dots,x_r,y_1,\dots,y_s\in L$ satisfying the assumptions of Theorem 3.4.2, then $x_1,\dots,x_r,y_1,\dots,y_s\in L$ is a transcendence basis for $L$ over $K$. Hence $L$ is an algebraic extension of $K'=K(x_1,\dots,x_r,y_1,\dots,y_s)$, and by assumption, a finite extension. Write

$v'$ for the restriction of $w$ to $K'$ and let $\Gamma'$ and $\overline{K}'$ be the value group and residue class field of $v'$, respectively. By Theorem 3.4.2, $\overline{K}' = \overline{K}(\overline{x_1}, \ldots, \overline{x_r})$ and $\Gamma' = \Gamma + \mathbb{Z}v'(y_1) + \cdots + \mathbb{Z}v'(y_s)$. Since by Corollary 3.2.3, $\Delta/\Gamma'$ is a finite group and $\overline{L}$ is a finite extension of $\overline{K}'$, the proof is complete. □

Combining Proposition 3.4.1 and Theorem 3.4.3, one gets

**Corollary 3.4.4.** *Keeping the notation of Theorem 3.4.2, we have*

$$\text{tr.deg.}\big(\overline{L}/\overline{K}\big) + \text{rk}(\Delta) \leq \text{tr.deg.}(L/K) + \text{rk}(\Gamma)\ . \tag{3.4.2}$$

**Corollary 3.4.5.** *Assume in Theorem 3.4.2 that $v$ is trivial. Then*

$$\text{tr.deg.}\big(\overline{L}/K\big) + \text{rk}(\Delta) \leq \text{tr.deg.}(\overline{L}/K) + \text{rr}(\Delta) \leq \text{tr.deg.}(L/K)\ . \tag{3.4.3}$$

*Proof.* In this case $\overline{K} = K$ and $\Gamma = \{0\}$. The first inequality follows by Proposition 3.4.1 and the second by Theorem 3.4.3. □

**Corollary 3.4.6.** *Suppose $L/K$ is a field extension, $\mathcal{O}$ is a valuation ring of $K$, and $\mathcal{O}_1 \subsetneqq \cdots \subsetneqq \mathcal{O}_n$ are extensions of $\mathcal{O}$ to $L$. Then* $\text{tr.deg.}(L/K) \geq n-1$.

*Proof.* To $\mathcal{O}$ belongs a valuation $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ and to $\mathcal{O}_1$ belongs a valuation $w : L \longrightarrow\!\!\!\!\!\rightarrow \Delta \cup \{\infty\}$ with $\Gamma \subseteq \Delta$. Choose

$$y_2 \in \mathcal{O}_2 \setminus \mathcal{O}_1,\ y_3 \in \mathcal{O}_3 \setminus \mathcal{O}_2,\ \ldots,\ y_n \in \mathcal{O}_n \setminus \mathcal{O}_{n-1}\ .$$

Since $y_i \notin \mathcal{O}_{i-1},\ y_i^{-1} \in \mathcal{O}_{i-1} \subseteq \mathcal{O}_i$. Whence $y_i \in \mathcal{O}_i^\times \subseteq \mathcal{O}_n^\times$.

According to Theorem 3.4.2, it suffices to prove that $\overline{w(y_2)}, \ldots, \overline{w(y_n)} \in \Delta/\Gamma$ are $\mathbb{Z}$-linearly independent. Let us show this by contradiction. Suppose there exist $\nu_2, \ldots, \nu_n \in \mathbb{Z}$, not all 0, such that $\nu_2 w(y_2) + \cdots + \nu_n w(y_n) \in \Gamma$. Then

$$\nu_2 w(y_2) + \cdots + \nu_n w(y_n) = w(a),\ \text{for some } a \in K^\times\ .$$

Hence $b = a^{-1} y_2^{\nu_2} \cdots y_m^{\nu_n} \in \mathcal{O}_1^\times$, and it follows that

$$a = b^{-1} y_2^{\nu_2} \cdots y_m^{\nu_n} \in K^\times \cap \mathcal{O}_n^\times\ .$$

Since $\mathcal{O}_n \cap K = \mathcal{O}$, it therefore follows that $a \in \mathcal{O}^\times$.

Let now $m$ be the biggest number in $\{2, \ldots, n\}$ such that $\nu_m \neq 0$. Then

$$y_m^{\nu_m} = bay_2^{-\nu_2} \cdots y_{m-1}^{-\nu_{m-1}} \in \mathcal{O}_{m-1}^\times\ .$$

Since $\nu_m \neq 0$ and $\mathcal{O}_{m-1}$ is integrally closed, $y_m \in \mathcal{O}_{m-1}^\times$ contradicting the choice of $y_m$. □

Let us point out that we may have proper inequality in equation (3.4.1) even for a finitely generated extension $L/K$. In fact there are prolongations of a valuation $v$ of a field $K$ to the pure transcendental extension $K(X)$ different from the ones we constructed in Corollaries 2.2.2 and 2.2.3. For example, for a prime $p$ consider the $p$-adic valuation $v_p$ of $\mathbb{Q}$ from (1.3.1). Take a $p$-adic number $x \in \mathbb{Q}_p$ transcendental over $\mathbb{Q}$. Let $\widehat{v}_p$ be the $p$-adic valuation of $\mathbb{Q}_p$, and denote by $w$ its restriction to $K(x)$. Since $(\mathbb{Q}_p, \widehat{v}_p)$ is an immediate extension of $(\mathbb{Q}, v_p)$ by Theorem 1.3.4, $(\mathbb{Q}(x), w)$ is also an immediate extension of $(\mathbb{Q}, v_p)$.

## 3.5 Exercises

**Exercise 3.5.1.**
(a) Show that every valuation of the algebraic closure of a finite field is trivial.
(b) Which fields allow only the trivial valuation?

**Exercise 3.5.2.**
Construct valuations on $\mathbb{C}$ of rank $\kappa$ for every cardinal $\kappa \leq 2^{\aleph_0}$.

**Exercise 3.5.3.**
Show that every non-trivial valuation of $\mathbb{R}$ has divisible value group and algebraically closed residue class field.

**Exercise 3.5.4.**
Let $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$ be a finite extension of valued fields. Assume that $n = [K_2 : K_1]$.
(a) Let $z \in \mathcal{O}_2$ and $h \in \mathcal{O}_1[X]$ such that $\overline{h}(\overline{z}) = 0$, $\deg \overline{h} = n$ and $\overline{h}$ irreducible. Conclude that $\mathcal{O}_2$ is the unique extension of $\mathcal{O}_1$ to $K_2$ and satisfies $f(\mathcal{O}_2/\mathcal{O}_1) = n$ and $e(\mathcal{O}_2/\mathcal{O}_1) = 1$.
(b) Let $z \in K_2^\times$ such that $v_2(z) + v_1(K_1)$ has order $n$ in the quotient group $v_2(K_2)/v_1(K_1)$. Conclude that $\mathcal{O}_2$ is the unique extension of $\mathcal{O}_1$ to $K_2$ and satisfies $e(\mathcal{O}_2/\mathcal{O}_1) = n$ and $f(\mathcal{O}_2/\mathcal{O}_1) = 1$.

**Exercise 3.5.5.**
Let $(K, v)$ be a non-trivially valued field, and let $\alpha, \beta, \gamma, \delta, \nu, \mu, \lambda, \varrho$ denote ordinal numbers. A sequence $s = (a_\nu)_{\nu<\varrho}$ ($\varrho$ a limit ordinal) of elements of $K$ is called a *pseudo-Cauchy sequence* if for all $\alpha < \beta < \gamma < \varrho$ we have

$$v(a_\gamma - a_\beta) > v(a_\beta - a_\alpha) \ .$$

An element $b$ of $K$ is called a *pseudo-limit* of the sequence $s$, if for all $\nu < \varrho$

$$v(b - a_\nu) = v(a_{\nu+1} - a_\nu) \ .$$

The valued field $(K, v)$ is called *pseudo-complete* if every pseudo-Cauchy sequence of $(K, v)$ has a pseudo-limit in $K$.

Show that every pseudo-complete field $(K, v)$ is maximal valued, i.e., does not allow any proper immediate extension $(K', v')$.

*Hint*: Assume that $(K', v')$ is an immediate extension of $(K, v)$ with $K' = K(z)$ and $z \in K' \setminus K$. Consider the subset

$$\Delta = \{v'(z - a) \mid a \in K\}$$

of the value group $\Gamma = v'(K')$. Choose a strictly increasing cofinal sequence $(\delta_\nu)_{\nu<\varrho}$ from $\Delta$, i.e., $\delta_\nu < \delta_\mu$ if $\nu < \mu$, and to every $\delta \in \Delta$ there exists $\nu < \varrho$ such that $\delta \leq \delta_\nu$. Let $a_\nu \in K$ be such that $v'(z - a_\nu) = \delta_\nu$. Show that $\varrho$ has to be a limit ordinal (by looking at the proof of Theorem 4.1.10), and that $(a_\nu)_{\nu<\varrho}$ is a pseudo-Cauchy sequence without pseudo limit in $K$.

**Exercise 3.5.6.**
Let $K$ be a field and $\Gamma$ an ordered abelian group. Denote by $K((\Gamma))$ the set of *formal power series*

$$f = \sum_{\gamma\in\Gamma} a_\gamma t^\gamma$$

where $a_\gamma \in K$ for all $\gamma \in \Gamma$, the *support* $\{\gamma | a_\gamma \neq 0\}$ of $f$ is well-ordered (i.e., every non-empty subset has a least element, or equivalently, there is no infinite strictly decreasing sequence of elements in the support), and $t$ is a symbol. If $g = \sum_{\gamma\in\Gamma} b_\gamma t^\gamma$ is also a formal power series, we define addition and multiplication by

$$f + g = \sum_\gamma (a_\gamma + b_\gamma)t^\gamma, \quad f \cdot g = \sum_\gamma \Big( \sum_{\delta+\varepsilon=\gamma} a_\delta b_\varepsilon \Big) t^\gamma \ .$$

Show that multiplication is well-defined: for this one has to show that $\sum_{\delta+\varepsilon=\gamma} a_\delta b_\varepsilon$ is a finite sum for each $\gamma \in \Gamma$ and that the set of $\gamma$'s occurring non-trivially, is well-ordered. This makes $K((\Gamma))$ a commutative domain. The map $v : K((\Gamma)) \longrightarrow \Gamma \cup \{\infty\}$ defined by $v(0) = \infty$ and

$$v(f) = \text{ least } \gamma \text{ such that } a_\gamma \neq 0$$

satisfies the axioms of a valuation. Show that $(K((\Gamma)), v)$ is a pseudo-complete field. (Hence it is maximal valued by Exercise 3.5.5.)

*Hint*: Prove first that $(K((\Gamma)), v)$ is pseudo-complete as follows: Let $(f_\nu)_{\nu<\varrho}$ be a pseudo-Cauchy sequence of formal power series

$$f_\nu = \sum_\gamma a_{\nu,\gamma} t^\gamma \ .$$

Thus defining $\gamma_\nu = v(f_{\nu+1} - f_\nu)$, we obtain $\gamma_\nu < \gamma_\mu$ for all $\nu < \mu < \varrho$. Define now the series $g = \sum_\gamma b_\gamma t^\gamma$ by taking

$$b_\gamma = \begin{cases} a_{\nu,\gamma} & \text{if there is some } \gamma_\nu > \gamma \\ 0 & \text{otherwise.} \end{cases}$$

Show that $b_\gamma$ does not depend on the choice of $\gamma_\nu > \gamma$. Now show that the support of $g$ is well ordered and that $g$ is a pseudo-limit of the sequence $(f_\nu)_{\nu<\varrho}$.

Next prove that $K((\Gamma))$ is a field as follows: It suffices to show that every formal power series $f$ with $a_{v(f)} = 1$ is invertible. Define the set

$$\Sigma = \{v(1 - fg) \mid g \in K((\Gamma)), \quad 1 - fg \neq 0\} .$$

Show that $\Sigma$ cannot have a maximal element. Now choose a strictly increasing sequence $(\gamma_\nu)_{\nu<\varrho}$ of elements of $\Sigma$ that is cofinal in $\Sigma$, i.e., to every $\gamma \in \Sigma$ there exists some $\nu < \varrho$ such that $\gamma \leq \gamma_\nu$. Moreover choose $g_\nu \in K((\Gamma))$ such that $v(1 - fg_\nu) = \gamma_\nu$. Conclude that $\varrho$ is a limit ordinal and show that $(g_\nu)_{\nu<\varrho}$ is a pseudo-Cauchy sequence. Let $h \in K((\Gamma))$ be a pseudo-limit of the sequence $(g_\nu)_{\nu<\varrho}$. Show that $1 - fh = 0$.

# 4

# Henselian Fields

In this chapter we shall study a very important class of valued fields – the so-called "henselian" fields. They got their name from the fact that Hensel's Lemma (cf. Theorem 1.3.1) holds in such fields. Moreover, they are even characterized by the validity of this lemma. As we saw in Chap. 1, Hensel's Lemma holds in the completion of a field with respect to a non-archimedean absolute value, or equivalently, a rank 1 valuation. As we saw in Remark 2.4.6, however, Hensel's Lemma need no longer hold in the completion of a field with respect to a valuation of rank greater than 1. For that reason, in the higher rank case we turn away from complete fields and instead concentrate on henselian fields.

As we shall see later (Sect. 5.2) every valued field allows an algebraic extension, unique up to value-preserving isomorphism, that satisfies Hensel's Lemma. This extension will be called the "henselization" of the given valued field.

In Sect. 4.1 we shall study many properties of valued fields, all equivalent to the validity of Hensel's Lemma. The most striking one (which we actually shall take as our definition of a henselian field) is that the valuation ring $\mathcal{O}$ on our field $K$ has a unique extension to the separable closure $K^s$ of $K$. It is this uniqueness of the extension of $\mathcal{O}$ that interests us most in the present chapter.

One can easily generalize the notion of a henselian field by replacing the Galois extension $K^s/K$ by any other one. Thus let $N/K$ be an arbitrary Galois extension (finite or infinite). We then call a valuation ring $\mathcal{O}$ of $K$ *$N$-henselian* if it has a unique extension to $N$. Besides $K^s$ we shall be mainly interested in the maximal Galois $p$-extension $K(p)$ of $K$ ($p$ a rational prime). In that case, $\mathcal{O}$ will be called *$p$-henselian* (Sect. 4.2).

The extension $K^s/K$ (resp. $K(p)/K$) is always infinite unless $K^s = K$ (resp. $K(p) = K$) or $K$ is real closed (resp. $p = 2$ and $K$ is euclidean). These classical field theoretic facts will be explained in Sect. 4.3, where we also give a valuation theoretic characterization of real closed (resp. euclidean) fields whose ordering is non-archimedean.

In Sect. 4.4 we study the interrelationship of all henselian valuation rings on a fixed field $K$. They will form a dependence class with one distinguished element – the so-called "canonical" henselian valuation ring.

Using the canonical henselian valuation, we prove that the property of admitting a henselian valuation "goes down" any Galois extension $N/K$ and every finite extension $L/K$ unless $K$ is real closed and $L = K^s$. Besides these classical results we also present a most recent one (by J. Koenigsmann [12]): if $L$ is the fixed field of a $p$-Sylow subgroup of the absolute Galois group $G(K^s/K)$ of $K$, then the property of being henselian always goes down from $L$ to $K$, unless $p = 2$ and $L$ is real closed.

## 4.1 Henselian Fields

We have seen (by Proposition 1.2.2) that every rank-one valuation $v$ of a complete field $K$ has a unique prolongation to each algebraic extension $E$ of $K$. By Corollary 3.2.10, also every valuation of a separably closed field $K$ has this property. Valuation rings, or valuations, with this property are very important. They are the so-called "henselian" valuation rings. In this section we introduce these rings; we shall see that they are the suitable substitute for rank-one valuation rings of complete fields. In particular, they are the valuation rings for which Hensel's Lemma holds.

A valued field $(K, \mathcal{O})$ is called *henselian* if $\mathcal{O}$ has a unique prolongation to every algebraic extension $L$ of $K$. It clearly suffices to require unique prolongations only to all finite extensions.

We see from the definition that the property of being henselian is hereditary, i.e., for any algebraic extension of valued fields $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$, if $(K_1, \mathcal{O}_1)$ is henselian, then so is $(K_2, \mathcal{O}_2)$.

Let $\widetilde{K}$ be an algebraic closure of $K$ and set

$$K^s := \{\, \alpha \in \widetilde{K} \mid \alpha \text{ is separable over } K \,\}$$

for the separable closure of $K$.

We then have the following apparently easier characterization of henselian valuations.

**Lemma 4.1.1.** *A valuation ring $\mathcal{O}$ of a field $K$ is henselian if and only if it extends uniquely to $K^s$.*

*Proof.* If $(K, \mathcal{O})$ is henselian, $\mathcal{O}$ extends uniquely to $K^s$ by definition.

Conversely, take an algebraic extension $L$ of $K$. Every extension of $\mathcal{O}$ to $L \cap K^s$ has a prolongation to $K^s$ which lies over $\mathcal{O}$. By assumption, $\mathcal{O}$ extends uniquely to $L \cap K^s$. Since by Corollary 3.2.10 every valuation ring of $L \cap K^s$ extends uniquely to $L$, by transitivity, $\mathcal{O}$ has a unique prolongation to $L$. □

The next theorem will highlight the importance of henselian valuation rings. Comparing with completions we see that rank-one complete valuation rings are a particular case of henselian valuation rings. Before stating the theorem we need a little preparation.

Let $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ be a valuation of the field $K$. By Corollary 2.2.2, the Gauss extension $w$ of $v$ to the rational function field $K(X)$ is given by $w : K(X) \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$, where, for $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$,

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

Let us call a polynomial $f$ *primitive* if $w(f) = 0$.

*Remark 4.1.2.* Denoting by $\mathcal{O}$ the valuation ring of $v$, we see that if $f$ is primitive, then $f \in \mathcal{O}[X]$. We have moreover the following properties:

(1) If two polynomials $f$ and $g$ are primitive, then so is their product $fg$.
(2) Every $f \in K[X]$ admits a decomposition $f = af_1$ with $a \in K$ and $f_1 \in K[X]$ primitive.
(3) If $f \in \mathcal{O}[X]$ decomposes as $f = g_1 \cdots g_m$ with irreducible factors $g_1, \ldots, g_m \in K[X]$, then there are $h_1, \ldots, h_m \in \mathcal{O}[X]$, irreducible in $K[X]$, such that $f = h_1 \cdots h_m$.

Statements (1) and (2) are clearly true. To see (3), write $f = af_1$, $g_i = b_i g_{1,i}$, $1 \le i \le m$, where $a, b_1, \ldots, b_m \in K$ and $f_1, g_{1,1}, \ldots, g_{1,m}$ are primitive. Then

$$v(b_1 \cdots b_m) = \sum_{i=1}^{m} w(g_i) = w(f) = v(a) \ .$$

Hence $b = b_1 \cdots b_m \in \mathcal{O}$ and defining $h_1 = bg_{1,1}$ and $h_i = g_{1,i}$ for each $i = 2, \ldots, m$, we get the desired decomposition.

**Theorem 4.1.3.** *For a valued field $(K, \mathcal{O})$ let $\mathcal{M}$, $\overline{K}$, and $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ be, respectively, the maximal ideal of $\mathcal{O}$, the residue class field of $\mathcal{O}$, and a valuation corresponding to $\mathcal{O}$. Set also $a \mapsto \overline{a}$ for the residue homomorphism and $f \mapsto \overline{f}$ for the corresponding map from $\mathcal{O}[X]$ to $\overline{K}[X]$. The following statements are equivalent:*

*(1) $(K, \mathcal{O})$ is henselian.*
*(2) For each irreducible polynomial $f \in \mathcal{O}[X]$ with $\overline{f} \notin \overline{K}$, there exists $g \in \mathcal{O}[X]$ such that $\overline{g}$ is irreducible in $\overline{K}[X]$, and $\overline{f} = \overline{g}^s$, for some $s \ge 1$.*
*(3) Let $f, g, h \in \mathcal{O}[X]$ satisfy $\overline{f} = \overline{g}\overline{h}$, with $\overline{g}$, $\overline{h}$ relatively prime in $\overline{K}[X]$. Then there exist $g_1, h_1 \in \mathcal{O}[X]$ with $f = g_1h_1$, $\overline{g_1} = \overline{g}$, $\overline{h_1} = \overline{h}$, and $\deg g_1 = \deg \overline{g}$.*
*(4) For each $f \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ with $\overline{f}(\overline{a}) = 0$ and $\overline{f}\,'(\overline{a}) \ne 0$,[1] there exists an $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and $\overline{\alpha} = \overline{a}$.*

[1] The latter will follow, for example, if $\overline{f}$ is separable.

*(5) For each $f \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ with $v(f(a)) > 2v(f'(a))$, there exists an $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and $v(a - \alpha) > v(f'(a))$.*[2]

*(6) Every polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}[X]$ with $a_{n-1} \notin \mathcal{M}$ and $a_{n-2}, \ldots, a_0 \in \mathcal{M}$ has a zero in $K$.*

*(7) Every polynomial $X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in \mathcal{O}[X]$ with $a_{n-2}, \ldots, a_0 \in \mathcal{M}$ has a zero in $K$.*

*Proof.* (1) $\Rightarrow$ (2): Denote by $\mathcal{O}'$ the unique extension of $\mathcal{O}$ to $\widetilde{K}$, the algebraic closure of $K$. Write $\mathcal{M}'$ for the maximal ideal, $v' : \widetilde{K} \longrightarrow\!\!\!\!\!\rightarrow \Gamma' \cup \{\infty\}$ for a valuation corresponding to $\mathcal{O}'$, and $\overline{K}'$ for the residue class field of $\mathcal{O}'$.

Since $\mathcal{O}'$ is the unique valuation ring of $\widetilde{K}$ lying over $\mathcal{O}$, for every $K$-automorphism $\sigma$ of $\widetilde{K}$, it follows that $\sigma(\mathcal{O}') = \mathcal{O}'$ and, of course, $\sigma(\mathcal{M}') = \mathcal{M}'$. By Proposition 3.2.16, $v' \circ \sigma = v'$ for all $K$-automorphisms $\sigma$ of $\widetilde{K}$.

Write

$$f(X) = \prod_{j=1}^{n} (aX - x_j) \,,$$

where $a, x_1, \ldots x_n \in \widetilde{K}$ and $a$ is an $n$-th root of the leading coefficient of $f$. Thus $a \in \mathcal{O}'$. Also $(-1)^n x_1 \cdots x_n = f(0) \in \mathcal{O}$.

The roots $x_1/a, \ldots, x_n/a$ of $f$ are all $K$-conjugate, i.e., for $1 \leq i, j \leq n$ there exists a $K$-automorphism $\sigma$ such that $\sigma(x_i/a) = x_j/a$. Consequently, there exists $\gamma \in \Gamma'$ such that $v'(x_j/a) = \gamma$ for all $1 \leq j \leq n$. So, for $\delta = \gamma + v'(a)$, we have that $v'(x_j) = \delta$ for each $1 \leq j \leq n$. Therefore, $x_1 \cdots x_n \in \mathcal{O}$ implies $\delta \geq 0$, and thus $x_j \in \mathcal{O}'$ for all $1 \leq j \leq n$. Actually, from $v'(x_j) = \delta$ for every $j$ with $1 \leq j \leq n$, it follows that either $x_1, \ldots, x_n \in \mathcal{M}'$ or $x_1, \ldots, x_n \in \mathcal{O}' \setminus \mathcal{M}'$.

In the first case $\overline{f} = (\overline{a}X)^n$ and the result is proved. In the second case $x_1, \ldots, x_n \in \mathcal{O}' \setminus \mathcal{M}'$, we obtain

$$\overline{f} = \prod_{i=1}^{n} (\overline{a}X - \overline{x_j}) \qquad \text{with } \overline{x_j} \neq \overline{0} \,.$$

By assumption $\overline{f} \notin \overline{K}$, hence $\overline{a} \neq 0$.

For the sake of seeking a contradiction, let us assume that $\overline{f} = \overline{g}\overline{h}$ for some relatively prime polynomials $\overline{g}$ and $\overline{h}$ with $g, h \in \mathcal{O}[X]$. Let $\overline{x_i/a}$ be a root of $\overline{g}$ and take some $x_j \neq x_i$ such that $\overline{x_j/a}$ is a root of $\overline{h}$. Hence $g(x_i/a) \in \mathcal{M}'$ and $h(x_j/a) \in \mathcal{M}'$. Take $\sigma \in \mathrm{Gal}(\widetilde{K}/K)$ such that $\sigma(x_i/a) = x_j/a$. Then

$$g(x_j/a) = g(\sigma(x_i/a)) = \sigma(g(x_i/a)) \in \sigma(\mathcal{M}') = \mathcal{M}' \,.$$

Thus $\overline{g}$ has also $\overline{x_j/a}$ as a root, contradiction.

(2) $\Rightarrow$ (3): Let $f = g_1 \cdots g_m$ be a factorization of $f$ with irreducible factors $g_1, \ldots, g_m \in \mathcal{O}[X]$ (note Remark 4.1.2 (3)). Our assumption implies that for

[2] Note that for complete rank one valued fields, this property was called 'Hensel's Lemma' in Theorem 1.3.1.

every $i$ with $1 \le i \le m$, either $\overline{g_i} \in \overline{K}$ or there exists $f_i \in \mathcal{O}[X]$ such that $\overline{f_i}$ is irreducible and $\overline{g_i} = \overline{f_i}^{t_i}$ for some $t_i \ge 1$. Clearly, we may assume that $f_i$ has no non-zero coefficient in $\mathcal{M}$. Renumbering conveniently the polynomials $g_1, \dots, g_m$, we may assume that

$$\prod_{i=1}^{k} \overline{f_i}^{t_i} = \overline{a}\,\overline{g}, \quad \prod_{i=k+1}^{\ell} \overline{f_i}^{t_i} = \overline{b}\,\overline{h}, \quad \prod_{i=\ell+1}^{m} \overline{g_i} = \overline{c}$$

for some $a, b, c \in \mathcal{O} \setminus \mathcal{M}$, because $\overline{g}$ and $\overline{h}$ are relatively prime. Define now

$$g_1 = a^{-1} \prod_{i=1}^{k} f_i^{t_i} \quad \text{and} \quad h_1 = \left( b^{-1} \prod_{i=k+1}^{\ell} f_i^{t_i} \right) \left( c^{-1} \prod_{i=\ell+1}^{m} g_i \right) .$$

Clearly $g_1$ and $h_1$ satisfy all the requirements.

(3) $\Rightarrow$ (4): Set $g(X) = X - a$ and $\overline{h} = \overline{f}/\overline{g} \in \overline{K}[X]$. Then $\overline{f} = \overline{g}\overline{h}$. Since $\overline{f'}(\overline{a}) \neq 0$, $\overline{g}$ and $\overline{h}$ are relatively prime. Hence there exist $g_1, h_1 \in \mathcal{O}[X]$ with $f = g_1 h_1$, $\overline{g_1} = \overline{g} = X - \overline{a}$, and $\deg g_1 = 1 = \deg \overline{g}$, by (3). It then follows that $g_1 = e(X - b)$ with $e \in \mathcal{O}^\times$ and $b \in \mathcal{O}$. Then $\overline{e} = 1$, $f(b) = 0$, and $\overline{b} = \overline{a}$.

(4) $\Rightarrow$ (5): By well-known computations one gets $f(a - X) = f(a) - f'(a)X + X^2 g(X)$, for some $g \in \mathcal{O}[X]$. Since $v(f'(a)) = \infty$ cannot occur, $f'(a) \neq 0$ and we may change variables putting $X = f'(a)Y$. Thus

$$\frac{f(a - f'(a)Y)}{f'(a)^2} = \frac{f(a)}{f'(a)^2} - Y + Y^2 g(f'(a)Y) .$$

Let $h(Y) = g(f'(a)Y)$ and

$$f_1(Y) = f(a)/(f'(a))^2 - Y + Y^2 h(Y) .$$

Since $v(f(a)) > v(f'(a)^2)$ and $f'(a) \in \mathcal{O}$, one has $h, f_1 \in \mathcal{O}[Y]$. Now $\overline{f_1} = Y(Y\overline{h}(Y) - 1)$, which has the simple zero $\overline{0}$ in the residue class field. Therefore $f_1$ has a zero $b \in \mathcal{M}$, by (4). Then $f$ has the zero $\alpha = a - f'(a)b \in \mathcal{O}$. Since $b \in \mathcal{M}$, $v(\alpha - a) > v(f'(a))$.

(5) $\Rightarrow$ (6): Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ as in (6). Then

$$\overline{f} = X^n + \overline{a_{n-1}} X^{n-1} = X^{n-1}(X + \overline{a_{n-1}}) .$$

Hence $-\overline{a_{n-1}}$ $(\neq 0)$ is a simple zero of $\overline{f}$. In particular,

$$v(f(-a_{n-1})) > 0 = v(f'(-a_{n-1})) .$$

Then $f$ has a zero in $\mathcal{O}$, by (5).

(6) $\Rightarrow$ (7): Trivial.

(7) $\Rightarrow$ (6): Suppose $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with $a_{n-1} \in \mathcal{O}^\times$ and $a_{n-2}, \dots, a_0 \in \mathcal{M}$. Replace $X$ by $a_{n-1}Y$ and divide by $a_{n-1}^n$; we obtain

$$g(Y) = Y^n + Y^{n-1} + \frac{a_{n-2}}{a_{n-1}^2} Y^{n-2} + \cdots + \frac{a_0}{a_{n-1}^n} .$$

Apply (7) to $g(Y)$ to obtain a zero $b \in K$ of $g$. Then $a = a_{n-1}b$ is a zero of $f$.

(6) $\Rightarrow$ (1): Suppose $(K, \mathcal{O})$ were not henselian. Then there would be a finite Galois extension $N/K$ with Galois group $G(N/K)$ in which $\mathcal{O}$ has more than one extension. Let $\mathcal{O}^*$ be a prolongation of $\mathcal{O}$ to $N$ and set $H = \{\sigma \in G(N/K) \mid \sigma(\mathcal{O}^*) = \mathcal{O}^* \}$, as in Lemma 3.3.1.

As $\mathcal{O}^*$ is not the only prolongation of $\mathcal{O}$ to $N$, the group $H$ is a proper subgroup of $G(N/K)$, and thus the fixed field $L$ of $H$ is a proper extension of $K$. Following the proof of Lemma 3.3.1, we let $\mathcal{O}^* = \mathcal{O}_1, \ldots, \mathcal{O}_m$ be all conjugates of $\mathcal{O}^*$ in $N$, define $\mathcal{O}_i' = \mathcal{O}_i \cap L$ for $1 \leq i \leq m$, and consider the subring

$$R = \mathcal{O}_1' \cap \cdots \cap \mathcal{O}_m'$$

of $L$. As in the proof of the lemma, we find $\beta \in R$ such that $\beta - 1 \in \mathcal{M}_1$ and $\beta \in \mathcal{M}_i$ for all $i$ such that $2 \leq i \leq m$. Since $m > 1$, $\beta$ cannot lie in $K$. Therefore

$$f = \mathrm{Irr}(\beta, K) = X^n + a_1 X^{n-1} + \cdots + a_n$$

cannot have a zero in $K$. This, however, contradicts (6), since according to the proof of Lemma 3.3.1 (with $\alpha = 1$), $1 + a_1 \in \mathcal{M}_1$ and $a_2, \ldots, a_n \in \mathcal{M}_1$. □

The last theorem has the following very important consequences:

**Corollary 4.1.4.** *Let $\mathcal{O} \subseteq \mathcal{O}_1$ be two valuation rings of $K$ with corresponding maximal ideals $\mathcal{M}_1 \subseteq \mathcal{M}$. Then $\overline{\mathcal{O}} = \mathcal{O}/\mathcal{M}_1$ is a valuation ring of $\overline{K} = \mathcal{O}_1/\mathcal{M}_1$. The composition $(K, \mathcal{O})$ is henselian if and only if both $(K, \mathcal{O}_1)$ and $\left(\overline{K}, \overline{\mathcal{O}}\right)$ are henselian.*

*Proof.* ($\Rightarrow$): Suppose $(K, \mathcal{O})$ is henselian. Then $(K, \mathcal{O}_1)$ is also henselian, using $\mathcal{M}_1 \subseteq \mathcal{M} \subseteq \mathcal{O} \subseteq \mathcal{O}_1$ and Theorem 4.1.3 (7). To show that $\left(\overline{K}, \overline{\mathcal{O}}\right)$ is henselian, let $\overline{f} = X^n + \overline{X^{n-1}} + \overline{a_{n-2}} X^{n-2} + \cdots \overline{a_0}$, with $\overline{a_i} \in \overline{\mathcal{M}}$ we must show that $\overline{f}$ has a zero in $\overline{K}$ (again using Theorem 4.1.37). The polynomial

$$f = X^n + X^{n-1} + a_{n-2} X^{n-2} + \cdots + a_0 \in \mathcal{O}[X]$$

has a zero $x \in \mathcal{O}$ (yet again by (4.1.3 (7)), since $a_i \in \mathcal{M}$); therefore $\overline{x} \in \overline{\mathcal{O}}$ is a zero of $\overline{f}$.

($\Leftarrow$): Let $f = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in \mathcal{O}[X]$, and suppose that $\overline{f}$ has a simple zero in the residue class field $\mathcal{O}/\mathcal{M}$. As $\mathcal{O}/\mathcal{M}$ is also the residue class field of $(\overline{K}, \overline{\mathcal{O}})$, and $(\overline{K}, \overline{\mathcal{O}})$ is henselian, this simple zero of $\overline{f}$ lifts to $\overline{K} = \mathcal{O}_1/\mathcal{M}_1$. As the field $(K, \mathcal{O}_1)$ is also henselian, the zero (which is again simple) can be lifted further to $K$. Note that we have used twice Theorem 4.1.3 (4). □

**Corollary 4.1.5.** *Let $(K_2, \mathcal{O}_2)$ be henselian, $K_1 \subseteq K_2$, and $\mathcal{O}_1 = K_1 \cap \mathcal{O}_2$. If $K_1$ is relatively separably closed in $K_2$, then $(K_1, \mathcal{O}_1)$ is henselian.*

*Proof.* Observing that in the proof of (6) ⇒ (1) in Theorem (4.1.3) we have only used separable polynomials, let

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_1[X]$$

be separable with $a_{n-1} \notin \mathcal{M}_1$, and $a_{n-2}, \ldots, a_0 \in \mathcal{M}_1$. Then $f$ has a zero in $K_2$, hence also in $K_1$. □

For later use we note one more corollary.

**Corollary 4.1.6.** *Let $(K, \mathcal{O})$ be a henselian valued field with residue class field $\overline{K}$. Then every finite Galois extension of $\overline{K}$ can be "lifted" to $K$, more precisely, if $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}[X]$, $\overline{f}$ is irreducible in $\overline{K}[X]$ and $\overline{K}[X]/(\overline{f})$ is a Galois extension of $\overline{K}$, then $K[X]/(f)$ is a Galois extension of $K$ too.*

*Proof.* As $\overline{f}$ is irreducible, also $f$ is irreducible. Let $L = K(\alpha)$ with $f(\alpha) = 0$. The valuation ring $\mathcal{O}$ extends uniquely to $L$, and $L$ together with this extension ring $\mathcal{O}'$ is again henselian. Since $\overline{f}$ splits into linear factors over $\overline{L} = \overline{K}[X]/(\overline{f})$, by Theorem 4.1.3, (3), it splits correspondingly over $L$. Thus $L/K$ is a Galois extension. □

Henselian valued fields can also be characterized as the class of valued fields satisfying "Krasner's Lemma". We next prove that a henselian valued field satisfies this lemma and we leave it to the reader to show the converse (see Exercise 4.5.2).

**Theorem 4.1.7.** (Krasner's Lemma) *Let $\mathcal{O}$ be a henselian valuation ring of a field $K$ and let $v$ be a valuation of $\widetilde{K}$ whose restriction to $K$ corresponds to $\mathcal{O}$. Let $x \in \widetilde{K}$ with $f(X) = (X - x_1) \cdots (X - x_n)$, $x = x_1$, as its minimal polynomial over $K$. Suppose $y \in \widetilde{K}$ satisfies:*

$$v(y - x) > \max\{\, v(x_i - x) \mid x_i \neq x \,\} .$$

*Then $K(x, y)$ is purely inseparable over $K(y)$. In particular, if $x$ is separable over $K$, then $x \in K(y)$.*

*Proof.* If $\sigma(x) = x$ for every $K(y)$-automorphism of $\widetilde{K}$, the statements follow from Galois theory. Going for a contradiction let us assume that $\sigma(x) \neq x$ for some $K(y)$-automorphism of $\widetilde{K}$. Let $N$ be a finite normal extension of $K(y)$ containing $K(x, y)$. Keep the notation $v$ for the restriction of $v$ to $N$. The assumption $\sigma(x) \neq x$ implies that

$$\delta = \max\{\, v(x_i - x) \mid x_i \in N, x_i \neq x \,\} \geq v(\sigma(x) - x) .$$

Next, let $\mathcal{O}'$ be the unique extension of $\mathcal{O}$ to $N$. Hence $\sigma(\mathcal{O}') = \mathcal{O}'$ and then Proposition 3.2.16 implies that $v = v \circ \sigma$. Therefore, observing that $v(y - \sigma(x)) = v(\sigma(y - x))$, we obtain

$$v(\sigma(x)-x) = v((y-x)-(y-\sigma(x))) \\ \geq \min\{v(y-x), v(y-\sigma(x))\} > \delta \geq v(\sigma(x)-x)\ ,$$

a contradiction. □

*Remark 4.1.8.* From Lemma 3.3.1 together with Theorem 3.2.14 we see that an *algebraically maximal* valued field $(K,\mathcal{O})$, i.e., $(K,\mathcal{O})$ does not allow any proper separable immediate extension $(K',\mathcal{O}')$, must be henselian. Clearly the same applies, if $(K,\mathcal{O})$ does not allow any proper immediate extension, algebraic or not. In this case $(K,\mathcal{O})$ is called *maximal* valued. Examples of such fields are the so-called "formal power series fields" treated in Exercise 3.5.6.

A henselian valued field $(K,\mathcal{O})$ need in general not be algebraically maximal, as Exercise 4.5.6 shows. There is, however, the following sufficient condition which makes a henselian field even algebraically maximal. Let us call a valued field $(K,\mathcal{O})$ *finitely ramified* if either $\operatorname{char}\overline{K}=0$, or $\operatorname{char}\overline{K}=p>0$ and there are only finitely many values between 0 and $v(p)$. Here are two examples of such fields:

(1) Let $\leq$ be an ordering of $K$, and take $\mathcal{O}(\leq)$. By Proposition 2.2.4 (iii) the residue class field $\overline{K}$ is ordered, whence $\operatorname{char}\overline{K}=0$.

(2) If $\Gamma_{\mathcal{O}} \cong \mathbb{Z}$, then $(K,\mathcal{O})$ is finitely ramified.

*Remark 4.1.9.* Suppose $(K,\mathcal{O})$ is a non-trivially valued field that is finitely ramified. Then $\operatorname{char}K=0$ and for every $n\in\mathbb{Z}\setminus\{0\}$, there are only finitely many values between 0 and $v(n)$. To see this, we consider the two cases, $\operatorname{char}\overline{K}=p$ and $\operatorname{char}\overline{K}=0$. If $\operatorname{char}\overline{K}=p$, write $n=p^e s$ with $p\nmid s$; then $v(n)=ev(p)$, so that there are $e$ times as many values between 0 and $v(n)$ as between 0 and $v(p)$. Now suppose $\operatorname{char}\overline{K}=0$. Since in this case $\mathbb{Q}\subseteq K$ and $\mathcal{M}\cap\mathbb{Q}=(0)\subseteq\mathcal{O}$, we find $v(n)=0$ for every $n\in\mathbb{Z}\setminus\{0\}$.

**Theorem 4.1.10.** *Suppose $(K,\mathcal{O})$ is finitely ramified. Then $(K,\mathcal{O})$ is henselian if and only if $(K,\mathcal{O})$ is algebraically maximal.*

*Proof.* ($\Leftarrow$) See Remark 4.1.8

($\Rightarrow$) Let $(K',\mathcal{O}')\supseteq(K,\mathcal{O})$ be a separable algebraic, immediate extension. Suppose $\alpha\in K'\setminus K$. Without loss of generality, let $K'/K$ be finite, and let $L$ be the normal closure of $K'/K$. The valuation ring $\mathcal{O}'$ extends uniquely to $L$. Let $v$ be a valuation corresponding to this extension. Then by Proposition 3.2.16 (1)

$$v(\beta)=v(\sigma(\beta)),\quad \text{for all } \beta\in L \ \text{ and } \ \sigma\in G=\operatorname{Gal}(L/K)\ . \tag{*}$$

Let us consider the element

$$a:=\frac{1}{n}\sum_{\sigma\in G}\sigma(\alpha)\in K\ ,$$

where $n = [L : K]$. (Recall that $\operatorname{char} K = 0$ by Remark 4.1.9.) We have $\alpha \neq a$ and thus $v(\alpha - a) = \gamma \in v(K')$. Since $\mathcal{O}'/\mathcal{O}$ is immediate, there exists $c \in K$ with $v(c) = \gamma$, whence

$$v\Big(\frac{\alpha - a}{c}\Big) = 0 \; .$$

In addition, there exists a $d \in K$ with

$$v\Big(\frac{\alpha - a}{c} - d\Big) > 0 \; .$$

It therefore follows that

$$v(\alpha - (\underbrace{a + cd}_{b \in K})) > v(c) = v(\alpha - a) \; .$$

Repeating this argument with $\alpha - a$ replaced by $\alpha - b$, after finitely many steps we find some $b \in K$ with

$$v(\alpha - b) > v(\alpha - a) + v(n) \; , \tag{$\dagger$}$$

using Remark 4.1.9. Then, in particular,

$$v(a - b) = v((\alpha - b) - (\alpha - a)) = v(\alpha - a) \; . \tag{$\ddagger$}$$

Summarizing, we get

$$\begin{aligned} v(n) + v(a - b) &= v(n(a - b)) \\ &= v\Big(\sum_{\sigma} \big(\sigma(\alpha) - b\big)\Big) \\ &\geq v(\alpha - b) && \text{(by } (*)\text{)} \\ &> v(\alpha - a) + v(n) && \text{(by } (\dagger)\text{)} \\ &= v(a - b) + v(n), && \text{(by } (\ddagger)\text{)} \end{aligned}$$

contradiction. □

## 4.2 $p$-Henselian Fields

Let $(K, \mathcal{O})$ be a valued field. Assume $N/K$ is a Galois extension (finite or infinite), i.e., the extension is algebraic, separable, and normal. We then call $(K, \mathcal{O})$ *$N$-henselian* if $\mathcal{O}$ has exactly one extension to $N$.

In the last section we always considered the case $N = K^s$, the separable closure of $K$. In this section we shall study the case where $N$ is the compositum

$K(p)$ of all finite Galois extensions of $p$-power degree[3] (i.e., the degree is $p^\nu$ for some $\nu \in \mathbb{N}$), where $p$ is a fixed rational prime. Clearly $K(p)$ is a Galois extension of $K$, and every finite subextension $L/K$ of $K(p)/K$ has a $p$-power degree over $K$. $K(p)$ is maximal with this property. Therefore $K(p)$ is also called the *maximal Galois $p$-extension* of $K$. Valuation rings $\mathcal{O}$ of $K$ that are $K(p)$-henselian are simply called *$p$-henselian*.

The extension $K(p)/K$ is always trivial or infinite unless $K$ is a *euclidean* field (i.e., an ordered field where every positive element is a square) and $K(p) = K(\sqrt{-1})$. This field theoretic fact will be explained in Sect. 4.3 below. We shall not use it here.

**Lemma 4.2.1.** *For every field $K$ and every prime $p$ we have $(K(p))(p) = K(p)$.*

*Proof.* Let $L = K(p)$ and $N/L$ be a Galois extension of $p$-power degree. Let $K_1/K$ be a finite Galois subextension of $L/K$ containing the coefficients of an irreducible polynomial $f \in L[X]$ such that $N = L(\alpha)$ and $f(\alpha) = 0$.

For every $\sigma \in \mathrm{Gal}(K_1/K)$, the image $f^\sigma$ of $f$ generates a Galois extension

$$L^\sigma = K_1[X]/(f^\sigma)$$

of $K_1$ of $p$-power degree. The compositum of those finitely many extensions of $K_1$ clearly is a Galois $p$-extension of $K$, thus contained in $L = K(p)$. But then $\alpha \in L$. □

**Theorem 4.2.2.** *A valued field $(K, \mathcal{O})$ is $p$-henselian if and only if $\mathcal{O}$ extends uniquely to every Galois extension $L/K$ with $[L : K] = p$.*

*Proof.* Assume that $\mathcal{O}$ extends uniquely to every Galois extension $L/K$ of degree $p$. Suppose that $M/K$ is a finite Galois $p$-extension to which $\mathcal{O}$ has two different extensions $\mathcal{O}' \neq \mathcal{O}''$. By Theorem 3.2.14 there exists an automorphism $\sigma \in G = G(M/K)$ with $\mathcal{O}'' = \sigma(\mathcal{O}')$. Thus $\sigma$ cannot be a member of the group

$$D = \{\, \tau \in G \mid \tau(\mathcal{O}') = \mathcal{O}' \,\} .$$

Since $G$ is a $p$-group, we can find a normal subgroup $N$ of $G$ of index $p$ containing $D$. The fixed field $L$ of $N$ is a Galois extension of $K$ of degree $p$. Thus $\mathcal{O}' \cap L = \mathcal{O}'' \cap L$ by assumption. Hence again by Theorem 3.2.14 (applied to the Galois extension $M/L$) there exists $\tau \in N$ such that $\tau(\mathcal{O}'') = \mathcal{O}'$. Therefore $\tau\sigma \in D$, and hence $\sigma \in N$.

The argument just given works for every $\sigma \notin D$, in particular for $\sigma \notin N$, which is impossible. Thus $\mathcal{O}$ extends uniquely to $M$. Hence $\mathcal{O}$ also extends uniquely to $K(p)$. □

Just as we obtained many equivalent characterizations of henselian fields in Theorem 4.1.3, we can also obtain many equivalent characterizations of

[3] Such extensions are simply called *$p$-extensions*.

$p$-henselian fields. One need only go through the proof of 4.1.3 and restrict consideration to those polynomials $f$ that split in $K(p)$. The corresponding condition for the Galois extension $K^s/K$ is always satisfied, hence, of course, was not mentioned in Theorem 4.1.3. Let us state a few such equivalences.

**Theorem 4.2.3.** *For a valued field $(K, \mathcal{O})$, the following statements are equivalent:*

(1) *$(K, \mathcal{O})$ is $p$-henselian.*

(2) *For each $f \in \mathcal{O}[X]$ splitting in $K(p)$, and any $a \in \mathcal{O}$ with $\overline{f}(\overline{a}) = 0$ and $\overline{f}'(\overline{a}) \neq 0$, there exists an $\alpha \in \mathcal{O}$ such that $f(\alpha) = 0$ and $\overline{\alpha} = \overline{a}$.*

(3) *Every polynomial $X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in \mathcal{O}[X]$ with $a_{n-2}, \ldots, a_0 \in \mathcal{M}$ has a zero in $K$, if it splits in $K(p)$.*

*Proof.* Just follow the proof of Theorem 4.1.3 and try to work exclusively in the Galois extension $K(p)/K$. In the implication (1) $\Rightarrow$ (2) of 4.1.3 we used the $n$-th root $a$ of the leading coefficient of $f \in \mathcal{O}[X]$. This element need not lie in $K(p)$. Thus one should extend $\mathcal{O}$ to some valuation ring $\mathcal{O}'$ of the algebraic closure $\widetilde{K}$ of $K$. Then clearly $a \in \mathcal{O}'$, and all computations work as in 4.1.3. The reader should note that the zeros $y_i = x_i/a$ of $f$ belong to $K(p)$ by assumption, and uniqueness of the extension of $\mathcal{O}$ is therefore used only inside $K(p)$. □

**Corollary 4.2.4.** *Let $(K, \mathcal{O})$ be a valued field with $\operatorname{char} \overline{K} \neq p$, and assume that $K$ contains a primitive $p$-th root of unity $\zeta_p$. Then $(K, \mathcal{O})$ is $p$-henselian if and only if $1 + \mathcal{M}$ is contained in $K^p$, the set of $p$-th powers of $K$.*

*Proof.* Assume first that $(K, \mathcal{O})$ is $p$-henselian. Since $\zeta_p \in K$, for any $\mu \in \mathcal{M}$, the polynomial $f = X^p - (1 + \mu)$ splits in $K(p)$. Clearly $\overline{f}(\overline{1}) = 0$ and $\overline{f}'(\overline{1}) = \overline{p} \neq 0$. Hence by Theorem 4.2.3, $f$ has a zero in $K$, i.e., $1 + \mu \in K^p$.

Conversely, assume that $1 + \mathcal{M} \subseteq K^p$. By Theorem 4.2.2, it suffices to show that $\mathcal{O}$ extends uniquely to every Galois extension $L/K$ of degree $p$. Since $\zeta_p \in K$, such an extension is obtained by adjoining a $p$-th root. Hence

$$L = K(\sqrt[p]{a}) ,$$

for some $a \in K$.

If $v(a)$ is not divisible by $p$, i.e., $v(a) \notin pv(K)$, we see that

$$p \leq (v(L) : v(K)) = e .$$

Hence it follows from Lemma 3.3.2 that $\mathcal{O}$ has only one extension to $L$. If $p | v(a)$, say $v(a) = v(b^p)$ for some $b \in K$, we may replace $a$ by $ab^{-p}$ and thus assume that $a$ is a unit of $\mathcal{O}$. If $\overline{a} \notin \overline{K}^p$, we find that $p \leq [\overline{L} : \overline{K}]$. Again Lemma 3.3.2 implies that $\mathcal{O}$ extends uniquely to $L$. If $\overline{a} \in \overline{K}^p$, say $\overline{a} = \overline{c}^p$, we may replace $a$ by $ac^{-p}$, and thus assume that $\overline{a} = \overline{1}$. In that case, however, $a \in 1 + \mathcal{M} \subseteq K^p$, and hence $\sqrt[p]{a}$ would not yield an extension of degree $p$. □

Similar to the henselian case we obtain here a $p$-version of Krasner's Lemma 4.1.7:

**Theorem 4.2.5.** *Let $(K, \mathcal{O})$ be a $p$-henselian field and $v$ be a valuation of $K(p)$ whose restriction to $K$ corresponds to $\mathcal{O}$. For $x \in K(p)$ let*

$$f := (X - x_1) \cdots (X - x_n) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$$

*be the minimal polynomial of $x = x_1$ over $K$. Suppose $y \in K(p)$ satisfies*

$$v(y - x) > \max\{\, v(x_i - x) \mid i \neq 1 \,\} .$$

*Then $x \in K(y)$. In particular, if $g = X^n + b_{n-1}X^{n-1} + \cdots + b_0 \in K[X]$ is close enough to $f$ (i.e., $\min v(a_i - b_i)$ is big enough), and splits in $K(p)$, then $K(x) = K(y)$ for some zero $y$ of $g$.*

*Proof.* The first assertion follows as in the proof of 4.1.7. The second assertion follows from the first by using Theorem 2.4.7. □

It is a very easy matter to see that the residue class field of an algebraically closed field is again algebraically closed (see Corollary 3.2.11). To prove the corresponding fact for *$p$-closed* fields $K$ (i.e., $K = K(p)$), however, is much more difficult. It amounts to lifting Galois extensions of degree $p$ from the residue class field $\overline{K}$ of a valued field $(K, \mathcal{O})$ to the field $K$ itself. For that reason we shall need here the notion of a "generic" polynomial.

Let $K$ be any field. A polynomial $g \in K[T_1, \ldots, T_r, X]$ is called *$p$-generic* (or $C_p$-generic, where $C_p$ is the cyclic group of order $p$) over $K$, if

(i) $K(T_1, \ldots, T_r)[X]/(g)$ is a Galois extension of order $p$, and
(ii) every Galois extension $N/L$ of degree $p$ of an extension field $L$ of $K$ is obtained as $N = L[X]/(g(t_1, \ldots, t_r, X))$ for some $t_1, \ldots, t_r \in L$.

In case we restrict ourselves to fields $K$ containing a primitive $p$-th root of unity, the polynomial

$$g = X^p - T_1$$

has these properties.

In particular, for $p = 2$ this polynomial is 2-generic. On the other hand, if we consider only fields $K$ with $\operatorname{char} K = p$, conditions (i) and (ii) are satisfied by the *Artin-Schreier polynomial*

$$g = X^p - X - T_1 .$$

In general, $p$-generic polynomials are quite complicated to compute. We simply take their existence from the literature (see [10]). Here is an example of a 3-generic polynomial:

$$g = X^3 - T_1X^2 + (T_1 - 3)X + 1 .$$

**Theorem 4.2.6.** *Let $(K, \mathcal{O})$ be a valued field and $L/\overline{K}$ a Galois extension of the residue class field $\overline{K}$ of degree $p$. Then there exists a Galois extension $L'/K$ of degree $p$ such that $\overline{L'} = L$ for the (unique) extension of $\mathcal{O}$ to $L'$.*

*In particular, if $K = K(p)$, then $\overline{K}(p) = \overline{K}$.*

*Proof.* The uniqueness of the extension of $\mathcal{O}$ to $L'$ follows simply from Proposition 3.2.16(5).

The existence of $L'$ will be proved by case distinction on the characteristics of $K$ and $\overline{K}$.

*Case 1:* $\operatorname{char} \overline{K} = p = \operatorname{char} K$.

In this case $L$ is obtained from $\overline{K}$ by adjoining a root of a suitable 'Artin-Schreier' polynomial

$$\overline{g} = X^p - X - \overline{a},\ a \in \mathcal{O}$$

to $\overline{K}$. But then the polynomial $g = X^p - X - a$ yields the desired Galois extension $L'/K$.

*Case 2:* $\operatorname{char} \overline{K} = \operatorname{char} K \neq p$. In this case let $g(T_1, \ldots, T_r, X)$ be a $p$-generic polynomial over the prime field of $K$. Then $L$ is obtained by adjoining a root of $g(\overline{a}_1, \ldots, \overline{a}_r, X)$ to $\overline{K}$, for a suitable choice of $a_1, \ldots, a_r \in \mathcal{O}$. But then

$$g(a_1, \ldots, a_r, X) \in \mathcal{O}[X]$$

has to be irreducible, and thus a root $x$ of $g$ generates the desired Galois extension $L'$ over $K$.

*Case 3:* $\operatorname{char} \overline{K} = q > 0$, $\operatorname{char} K = 0$. Let $\Gamma = v(K^\times)$ be the value group of a valuation $v$ corresponding to $\mathcal{O}$, and $K_0 = \overline{K}$ the residue class field of $v$. We are going to write $v$ as a composition of three valuations such that

(1) $K_0$ is the residue class field of a valuation $v_1$ on $K_1$ with $\operatorname{char} K_0 = q = \operatorname{char} K_1$,

(2) $K_1$ is the residue class field of a valuation $v_2$ on $K_2$ with $\operatorname{char} K_1 = q$, $\operatorname{char} K_2 = 0$, and $v_2$ has rank 1,

(3) $K_2$ is the residue class field of a valuation $v_3$ on $K_3 = K$ with $\operatorname{char} K_2 = 0 = \operatorname{char} K_3$.

After that we shall lift the given Galois extension $L/K_0$ of degree $p$ first to $K_1$, then to $K_2$, and finally to $K_3$. We already know how to proceed in (1) and (3). In (2) we seem to have the same conditions as at the beginning of Case 3. What we gained, however, by our decomposition, is the rank 1 property of $v_2$. Thus we may assume in Case 3 right from the beginning that $v$ has rank 1. But before we do this let us show how to obtain the desired decomposition of $v$.

First let $\Delta_2$ be the convex hull of $\mathbb{Z}v(q)$ in $\Gamma$ (note that $v(q) > 0$). Defining $v_3$ on $K_3 = K$ by

$$v_3(x) = v(x) + \Delta_2 \in \Gamma/\Delta_2$$

yields a valuation $v_3$ on $K$ with the residue class field $K_2$ and a valuation

$$v_2' : K_2 \longrightarrow \Delta_2 \cup \{\infty\}$$

on $K_2$. Since $v(q) \in \Delta_2$, $\operatorname{char} K_2 = 0$. The residue class field of $v_2'$ is $K_0 = \overline{K}$ (cf. Sect. 2.3).

Next let $\Delta_1$ be the maximal convex subgroup of $\Delta_2$ not containing $v(q)$. Then

$$v_2(x) = v_2'(x) + \Delta_1 \in \Delta_2/\Delta_1$$

defines a valuation on $K_2$ with value group $\Delta_2/\Delta_1$, which obviously is of rank 1. As explained in Sect. 2.3, the residue class field $K_1$ of $v_2$ carries a valuation

$$v_1 : K_2 \longrightarrow \Delta_1 \cup \{\infty\}$$

with residue class field $K_0$. Since $v(q) \notin \Delta_1$, we have $\operatorname{char} K_1 = q$.

Now let us return to the proof of case 3, assuming in addition that $\Gamma = v(K^\times)$ has rank 1. At this point we use the fact that the completion $(\widehat{K}, \widehat{v})$ of the rank 1 valued field $(K, v)$ is henselian (Theorem 1.3.1), and thus by Corollary 4.1.6 we can lift our Galois extension $L/\overline{K}$ from the residue class field $\overline{K}$ to a Galois extension $L'/\widehat{K}$ of the completion $\widehat{K}$. Using once more a $p$-generic polynomial $g \in \mathbb{Q}[T_1, \ldots, T_r, X]$, $L'$ is generated by a zero of $g_t = g(t_1, \ldots, t_r, X)$ for a suitable choice of $t_1, \ldots, t_r \in \widehat{K}$. Since $K$ is dense in $\widehat{K}$, we may choose $\tau_1, \ldots, \tau_r \in K$ so close to $t_1, \ldots, t_r$ that a root $x$ of the polynomial $g_\tau = g(\tau_1, \ldots, \tau_r, X)$ generates $L'/\widehat{K}$ as well (see Theorem 4.2.5). But then $K[X]/(g_\tau)$ yields the desired Galois extension of $K$. □

Corollary 4.1.4 on henselian valuations has the following $p$-henselian analog:

**Corollary 4.2.7.** *Let $\mathcal{O} \subseteq \mathcal{O}_1$ be two valuation rings of $K$ with corresponding maximal ideals $\mathcal{M} \supseteq \mathcal{M}_1$. Then $\overline{\mathcal{O}} = \mathcal{O}/\mathcal{M}_1$ is a valuation ring of $\overline{K} = \mathcal{O}_1/\mathcal{M}_1$, and $(K, \mathcal{O})$ is $p$-henselian if and only if $(K, \mathcal{O}_1)$ and $(\overline{K}, \overline{\mathcal{O}})$ are both $p$-henselian.*

*Proof.* Recall that $(K, \mathcal{O})$ is the composition of the valued field $(K, \mathcal{O}_1)$ with the valuation $\overline{\mathcal{O}}$ on the residue class field $\overline{K}$ of $(K, \mathcal{O}_1)$. This is reflected by the factorization

$$\mathcal{O} \longrightarrow \mathcal{O}/\mathcal{M}_1 \longrightarrow \mathcal{O}/\mathcal{M}$$

of the residue map $\mathcal{O} \longrightarrow \mathcal{O}/\mathcal{M}$.

First let $(K, \mathcal{O})$ be $p$-henselian, and consider the polynomial

$$f = X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_o \in \mathcal{O}_1[X]$$

with $a_i \in \mathcal{M}_1$. Assuming that $f$ splits in $K(p)$, it follows from $\mathcal{M}_1 \subseteq \mathcal{M}$ and (3) of Theorem 4.2.3 that $f$ has a zero in $K$. Thus $(K, \mathcal{O}_1)$ is $p$-henselian. To show that $\big(\overline{K}, \overline{\mathcal{O}}\big)$ is $p$-henselian, assume that $\overline{a}_i \in \overline{\mathcal{M}} = \mathcal{M}/\mathcal{M}_1$ and that $\overline{f}$ splits in $\overline{K}(p) = \overline{K(p)}$. Of course, we may as well replace $f$ by a pre-image of $\overline{f}$

that splits[4] in $K(p)$. Hence let $f$ split in $K(p)$. Then by (3) of Theorem 4.2.3, $f$ has a zero $a \in K$. Since $\mathcal{O}_1$ is integrally closed, $a \in \mathcal{O}_1$. Hence $\overline{f}(\overline{a}) = 0$ in $\overline{K}$.

Next assume that $(K, \mathcal{O}_1)$ and $\left(\overline{K}, \overline{\mathcal{O}}\right)$ are both $p$-henselian. We now use criterion (2) of Theorem 4.2.3 twice. Thus let $f \in \mathcal{O}[X]$ be split in $K(p)$. Then by Theorem 4.2.6, the image of $f$ also splits in the $p$-closure of $\overline{K} = \mathcal{O}_1/\mathcal{M}_1$ and in the $p$-closure of the residue class field $\mathcal{O}/\mathcal{M}$ of $\left(\overline{K}, \overline{\mathcal{O}}\right)$, which is at the same time also the residue class field of the composition $(K, \mathcal{O})$. Now a simple zero of $f$ in $\mathcal{O}/\mathcal{M}$ can be lifted first to $\mathcal{O}_1/\mathcal{M}_1$ (as $\left(\overline{K}, \overline{\mathcal{O}}\right)$ is $p$-henselian), and then to $K$ (as $(K, \mathcal{O}_1)$ is $p$-henselian). □

## 4.3 Ordered Henselian Fields

In this section we shall continue with the study of ordered fields from Sect. 2.2. Let us first collect some elementary facts about ordered fields that can be found in many basic algebra books (see [15], [9], or more specifically [20]).

**Fact 4.3.1.** *Let $\leq$ be an ordering of the field $K$. Assume that $L/K$ is a field extension. Then $\leq$ extends to $L$ in case*

*(i)* $L = K(\sqrt{a})$ *and* $0 \leq a$ *in* $K$*;*
*(ii)* $L/K$ *is algebraic of odd degree; or*
*(iii)* $L$ *is purely transcendental over* $K$*.*

Given an ordered field $(K, \leq)$, by Zorn's Lemma there always exists a maximal algebraic ordered extension $(K^*, \leq^*)$ of $(K, \leq)$, i.e., $a \leq b$ iff $a \leq^* b$ for all $a, b \in K$.

**Fact 4.3.2.** *For an ordered field $(K, \leq)$ the following are equivalent:*

*(i)* $(K, \leq)$ *has no proper ordered algebraic extension;*
*(ii)* *in $(K, \leq)$ every positive element is a square and every odd-degree polynomial $f \in K[X]$ has a zero in $K$;*
*(iii)* *the set of squares $\{ a^2 \mid a \in K \}$ is a positive cone of $K$ and every odd-degree polynomial from $K[X]$ has a zero in $K$;*
*(iv)* $K\left(\sqrt{-1}\right)$ *is algebraically closed and* $K \neq K\left(\sqrt{-1}\right)$.

Thus, in particular, as in the case $K = \mathbb{R}$, the algebraic closure of a field $K$ satisfying one of the equivalent conditions of Fact 4.3.2 has degree 2 over $K$. One should further note that the ordering of such a field $K$ is uniquely determined, as the positive elements are exactly the squares in $K$. The fields of Fact 4.3.2 are called *real closed* fields since they have many properties

[4] In case $\overline{f}$ is irreducible and $\overline{f}(\overline{\alpha}) = 0$ for some $\overline{\alpha} \in \overline{K(p)}$, lift the splitting field $\overline{F}$ of $\overline{f}$ over $\overline{K}$ by Theorem 4.2.6 to an extension $F/K$, choose $\alpha$ from $F$ and let $f = \mathrm{Irr}(\alpha, K)$. If $\overline{f}$ is reducible, do the same for every factor.

in common with the reals $\mathbb{R}$. From condition *(i)* and the above mentioned application of Zorn's Lemma, we see that every ordered field $(K, \leq)$ admits at least one real closed algebraic extension. Such an extension is called a *real closure* of $(K, \leq)$.

**Fact 4.3.3.** *Every ordered field $(K, \leq)$ has, up to isomorphism over $K$, exactly one real closure; i.e., if $(K^*, \leq^*)$ and $(K^{**}, \leq^{**})$ are real closures of $(K, \leq)$, then there exists an isomorphism $\sigma : K^* \longrightarrow K^{**}$ such that $\sigma|_K = \mathrm{id}_K$.*

Note that the isomorphism $\sigma$ automatically is order-preserving, as the positive elements of $K^*$ and $K^{**}$ are squares and $\sigma$ clearly preserves squares.

An ordered field $(K, \leq)$ whose positive elements are exactly the squares is called *euclidean.* As we already mentioned, a euclidean field has exactly one ordering. If a euclidean field has no odd-degree extensions, it is real-closed by 4.3.2. If we adjoin $\sqrt{-1}$ to a euclidean field, it need not become algebraically closed. The resulting field $L = K\big(\sqrt{-1}\big)$, however, is 2-closed, i.e., $L(2) = L$.

**Proposition 4.3.4.** *If $K$ is euclidean, then the quadratic extension $L = K\big(\sqrt{-1}\big)$ is 2-closed.*

*Proof.* Every element of $L$ has a representation $x + iy$ with $x, y \in K$ and $i = \sqrt{-1}$. We have to solve the equation

$$x + iy = (u + iv)^2 = (u^2 - v^2) + i2uv \ ,$$

i.e., $x = u^2 - v^2$, $y = 2uv$ for some $u, v \in K$. This amounts to solving

$$v = \sqrt{\frac{\sqrt{x^2 + y^2} - x}{2}}$$

in $K$. Since $x^2 + y^2$ is positive we get $z \in K$ such that $x^2 + y^2 = z^2$. Moreover $z$ may be taken positive. Then $z \geq x$ and thus also $z - x = w^2$ for some $w \in K$. □

Let us now prove the "converse":

**Theorem 4.3.5.**
*(a) Let $p$ be a prime and assume that $[L(p) : L]$ is finite. Then either $L(p) = L$ or $p = 2$, $[L(p) : L] = 2$, and $L$ is euclidean.*
*(b) Let $M/L$ be a finite field extension. If $M$ is separably closed, then also $L$ is separably closed or $L$ is real closed and $[M : L] = 2$.*

*Proof.* Case (a) will not be used in this book; for its proof we refer to [4].
(b): Assume that $L$ is not separably closed. We may replace $M$ by the separable closure $L^s$ of $L$. Thus $L^s/L$ is a non-trivial finite Galois extension with Galois group denoted by $G$. We shall first show that $G$ is a 2-group.

Let the prime number $p$ divide the order of $G$. Then there exists an intermediate extension $L \subseteq K \subseteq L^s$ with $[L^s : K] = p$. We show that $\operatorname{char} L \neq p$.

If $\operatorname{char} L = p$, we get $L^s = K(\alpha)$ with $\alpha^p - \alpha - a = 0$ for some $a \in K$. This clearly implies

$$\left(\frac{1}{\alpha}\right)^p + \frac{1}{a}\left(\frac{1}{\alpha}\right)^{p-1} - \frac{1}{a} = 0 \,.$$

Computing the trace $T$ from $L^s/K$ this yields

$$T\left(\frac{1}{\alpha}\right) = -\frac{1}{a} \,.$$

Now choose $\beta \in L^s$ such that $\beta^p - \beta + \frac{a^2}{\alpha} = 0$. (Recall that $L^s$ is separably closed.) Let $\beta_1, \ldots, \beta_p$ be all the conjugates of $\beta$ over $K$. Then

$$T(\beta)^p - T(\beta) = \left(\sum_{i=1}^{p} \beta_i\right)^p - \sum_{i=1}^{p} \beta_i = \sum_{i=1}^{p} (\beta_i^p - \beta_i) = T(\beta^p - \beta) = T(-\frac{a^2}{\alpha}) = a \,.$$

Thus $t = T(\beta)$ is a zero of the polynomial $f = X^p - X - a$. Since with $t$ also $t+1$ is a zero of $f$, this shows that all zeros of $f$ lie in $K$, contradicting $\alpha \notin K$.

Next we may assume that a $p$-th root of unity is contained in $K$. This holds because adjoining such a root to $K$ would give an extension inside $L^s$ of degree prime to $p$. Now by Kummer theory, $L^s = K(\sqrt[p]{a})$ for some $a \in K \setminus K^p$. The norm map $N : L^s \to K$ then yields

$$(-1)^{p-1} \cdot a = N(\sqrt[p]{a}) = N(\sqrt[p^2]{a})^p \in K^p \,,$$

as $\sqrt[p^2]{a}$ also lies in $L^s$. Thus we find that $p = 2$ and $-1 \notin K^2$. Hence $G$ is a 2-group and $L^s = K(\sqrt{-1})$. It remains to show that $K$ is real closed and that $L = K$.

Since $\operatorname{char} L \neq 2$, $L^s$ is quadratically closed. Thus to $a, b \in K$ there exist $c, d \in K$ such that

$$a^2 + b^2 = N(a + b\sqrt{-1}) = N((c + d\sqrt{-1})^2) \in K^2 \,.$$

Now we clearly see that the set of squares $K^2$ is a positive cone of an ordering $\leq$ on $K$. Thus $\operatorname{char} L = 0$ and $L^s$ is algebraically closed. Therefore $K$ is real closed by Fact 4.3.2 (iv).

Finally assume that $L \subsetneq K$. Since $G(L^s/L)$ is a 2-group, we can find an intermediate extension $L \subseteq K' \subseteq K$ with $[K : K'] = 2$. Thus $K = K'(\sqrt{a})$ for some $a \in K'$. Since $a = (\sqrt{a})^2 \geq 0$ in $K$ and $K$ is real closed, also $\sqrt[4]{a} \in K$. But $[K'(\sqrt[4]{a}) : K'] = 4$, a contradiction. Thus we proved $L = K$. □

Let us now continue the study of orderings on a valued field $(K, \mathcal{O})$ from Subsect. 2.2.2. There we already gave a structure theorem for the set of those orderings of $K$ for which $\mathcal{O}$ is convex ring (Theorem 2.2.5). In our study of ($p$-)henselian fields, the next lemma is basic.

**Lemma 4.3.6.** *Let $(K, \mathcal{O})$ be a 2-henselian field. Then $\mathcal{O}$ is convex with respect to every ordering of $K$. In particular, if $K$ is ordered, then $\overline{K}$ is ordered too.*

*Proof.* We show that the maximal ideal $\mathcal{M}$ of $O$ is convex (using Proposition 2.2.4). If $\mathcal{M}$ were not convex, there would exist some $\mu \in \mathcal{M}$ and $\nu \in \mathcal{O}$ such that $0 < \nu < \mu$ and yet $\nu \notin \mathcal{M}$. Hence $0 < \mu/\nu \in \mathcal{M}$. Thus the residue polynomial of

$$X^2 + X + \frac{\mu}{\nu}$$

is $X^2 + X = (X+1)X$. Therefore by Theorem 4.2.3 (2) we find $a, b \in K$ such that

$$(X+a)(X+b) = X^2 + X + \frac{\mu}{\nu}\,.$$

Hence $a+b = 1$ and $ab = \mu/\nu > 0$. Thus $0 \leq a, b \leq 1$. Therefore $\mu/\nu = ab \leq 1$. Hence $\mu \leq \nu$, a contradiction. □

Next assume that $(K, \mathcal{O})$ is a valued field and $\leq$ is a fixed ordering of $K$ for which $\mathcal{O}$ is convex. If $\leq$ is archimedean (i.e., for every $a \in K$ there exists $n \in \mathbb{N}$ with $a \leq n$), then $\mathcal{O}$ is necessarily trivial. Thus the existence of a non-trivial $\leq$-convex valuation ring $\mathcal{O}$ on $K$ entails that $\leq$ be non-archimedean (cf. Corollary 2.2.6).

**Theorem 4.3.7.** *Let $\mathcal{O}$ be a non-trivial valuation ring of $K$ with value group $\Gamma$. Assume $\mathcal{O}$ to be convex with respect to the ordering $\leq$. Then $K$ is real closed (resp. euclidean) if and only if*

*(i) $\overline{K}$ is real closed (resp. euclidean),*
*(ii) $\Gamma$ is divisible (resp. 2-divisible), and*
*(iii) $(K, \mathcal{O})$ is henselian (resp. 2-henselian).*

*Proof.* Assume first that $K$ is real closed (resp. euclidean). Then in the unique ordering $\leq$ of $K$, every positive element is a square. Thus every element $\gamma$ of $\Gamma$ is divisible by 2. In fact, let $v(x) = \gamma$ and assume without restriction that $0 \leq x$. Now $x = y^2$ yields $v(x) = 2v(y)$. In the real closed case, $x$ is even a $p$-th power for every odd prime $p$. Thus $\gamma = v(x)$ is divisible by $p$. This clearly implies $(ii)$.

Since $\mathcal{O}$ is convex with respect to $\leq$, the ordering $\leq$ on $K$ induces canonically an ordering on $\overline{K}$ (Proposition 2.2.4). If $\overline{K}$ did have a proper, ordered extension $L$ of finite degree, then we could first lift $L$ to an algebraic extension $L'$ of $K$ of the same degree (recall that a monic polynomial $f \in \mathcal{O}[X]$ is irreducible over $K$ if $\overline{f}$ is irreducible over $\overline{K}$), and then lift the ordering of $L$ to $L'$ using Theorem 2.2.5. This proves $(i)$.

In order to prove that $(K, \mathcal{O})$ is 2-henselian, it suffices to show (by Corollary 4.2.4) that every $x \in 1 + \mathcal{M}$ is square in $K$. Since $\mathcal{O}$ is convex with respect to $\leq$, it follows from Proposition 2.2.4 that $0 < x$. Hence $x = y^2$ in $K$ by the definition of a euclidean field. Now assume that $K$ is even real closed.

Then $(K, \leq)$ cannot have a proper ordered extension $L$ of finite degree. Hence $(K, \mathcal{O})$ cannot have a proper immediate extension $(K', \mathcal{O}')$ of finite degree. In fact, such an extension would have the same residue class field as $(K, \mathcal{O})$ and also the same value group. But then by Theorem 2.2.5 we could find an extension of $\leq$ to $K'$. Now by Theorem 4.1.10, $(K, \mathcal{O})$ is henselian.

Next we assume $(i), (ii)$ and $(iii)$ and show that $K$ is real closed (resp. euclidean). Let us first treat the euclidean case. Assume that $x \in K$ is positive. By $(ii)$ there exists $y \in K$ such that $v(xy^2) = 0$. Since $0 < xy^2 = z$, the residue $\overline{z}$ of the unit $z$ is positive in the unique ordering of $\overline{K}$. Hence $\overline{z} = \overline{u}^2$ by $(i)$. By $(iii)$ and Corollary 4.2.4,

$$zu^{-2} \in 1 + \mathcal{M} \subseteq K^2 \, .$$

This shows that $x$ is a square in $K$.

Now let us treat the real closed case. We shall show that $K$ does not allow any proper algebraic and ordered extension $K'$. Assume there exists an algebraic extension $K'$ of $K$ of degree $n$ together with an ordering $\leq'$. Since we already proved that $K$ is euclidean, $\leq'$ has to extend the ordering $\leq$ of $K$. Now let $\mathcal{O}'$ be the convex hull of $\mathcal{O}$ in $K'$ with respect to $\leq'$. Clearly, $\mathcal{O}'$ is a valuation ring of $K'$ such that $\mathcal{O}' \cap K = \mathcal{O}$. Moreover, $\mathcal{O}'$ induces an ordering on the residue class field $\overline{K'}$. Thus by $(i)$ and Fact 4.3.2, $\overline{K'} = \overline{K}$. From $(ii)$ and Theorem 3.2.4 we see that the value group of $\mathcal{O}'$ has to coincide with that of $\mathcal{O}$. Hence $(K', \mathcal{O}')$ is an immediate extension of $(K, \mathcal{O})$. But then $(iii)$ and Theorem 4.1.10 imply that $n = 1$. □

## 4.4 The Canonical Henselian Valuation

By the very definition of a henselian valuation ring of a field $K$, every such ring of an algebraically closed field $K$ is henselian. Observing Corollary 3.2.10, the same can be said for a separably closed field. Thus by Chevalley's Extension Theorem 3.1.1, a separably closed field may carry infinitely many henselian valuation rings, dependent and independent. The next theorem will show that this is an exceptional case. In fact, no other field can carry even two independent henselian valuation rings. The henselian valuation rings of a non-separably closed field $K$ always form a dependence class. We shall further see that there is a distinguished ring in this dependence class – the so-called "canonical" henselian valuation ring.

Our first theorem generalizes a classical result of F.K. Schmidt, stating that a field complete with respect to two absolute values must be separably closed.

**Theorem 4.4.1.** (F.K. Schmidt) *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two independent henselian valuation rings of the field $K$. Then $K$ is separably closed, i.e., $K = K^s$.*

*Proof.* Assume that $K$ is not separably closed. Then there exists an irreducible, separable polynomial

$$g = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$$

of degree $n > 1$. Let

$$h = X^n + b_{n-1}X^{n-1} + \cdots + b_0 \in K[X]$$

be a polynomial with $n$ different zeros in $K$. Note that by assumption the valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ are independent and hence in particular non-trivial. Thus $K$ cannot be finite. Now we choose a polynomial

$$f = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in K[X]$$

such that for every $i$ the coefficient $c_i$ is very close to $a_i$ for the valuation $v_1$ corresponding to $\mathcal{O}_1$ and at the same time very close to $b_i$ for the valuation $v_2$ corresponding to $\mathcal{O}_2$. Hence $v_1(c_i - a_i) > \gamma_1$ and $v_2(c_i - b_i) > \gamma_2$ for suitably chosen $\gamma_1 \in v_1(K)$ and $\gamma_2 \in v_2(K)$. Such a polynomial exists by the Approximation Theorem 2.4.1, as $\mathcal{O}_1$ and $\mathcal{O}_2$ are independent.

Approximating closely enough and choosing a zero $x_1 \in K^s$ of $g$, $f$ becomes separable and one of the zeros of $f$, say $y_1$, comes as close as we wish to $x_1$ (Theorem 2.4.7). But then by Theorem 4.1.7 we find $K(x_1) \subseteq K(y_1)$. In particular, $f$ is irreducible in $K[X]$. We then repeat this argument, replacing $g$ by $f$ and $f$ by $h$. Hence one of the zeros of $h$, say $z_1$, will satisfy $K(y_1) \subseteq K(z_1)$, a contradiction to $z_1 \in K$. □

For the following definition we fix the field $K$ and consider the totality of all henselian valuation rings $\mathcal{O}$ of $K$. Since we shall consider several such rings at the same time, we prefer to write $\mathcal{O}/\mathcal{M}$ for the residue class field of $\mathcal{O}$, where $\mathcal{M}$ always denotes the maximal ideal of $\mathcal{O}$ (similarly we write $\mathcal{M}_i$ and $\mathcal{M}'$ for the maximal ideal of $\mathcal{O}_i$ and $\mathcal{O}'$). The former notation $\overline{K}$ is not suitable here as it does not explicitly refer to $\mathcal{O}$. Note that $\mathcal{O} = K$ always is a henselian valuation ring of $K$. Thus the totality of all henselian valuation rings of $K$ is non-empty.

Now set

$$H_1 = \{\, \mathcal{O} \mid \mathcal{O} \text{ henselian, } \mathcal{O}/\mathcal{M} \text{ not separably closed} \,\}$$
$$H_2 = \{\, \mathcal{O} \mid \mathcal{O} \text{ henselian and } \mathcal{O}/\mathcal{M} \text{ separably closed} \,\}\,.$$

Recall that two valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ are called *comparable* if $\mathcal{O}_1 \subseteq \mathcal{O}_2$ or $\mathcal{O}_2 \subseteq \mathcal{O}_1$. In case $\mathcal{O}_1 \subseteq \mathcal{O}_2$, we call $\mathcal{O}_2$ *coarser* than $\mathcal{O}_1$ (or a *coarsening* of $\mathcal{O}_1$) and $\mathcal{O}_1$ *finer* than $\mathcal{O}_2$.

**Theorem 4.4.2.** *Any two valuation rings from $H_1$ are comparable. If $H_2 \neq \emptyset$, then $H_2$ contains a valuation ring $\mathcal{O}^{**}$ that is coarser than every valuation ring from $H_2$ and strictly finer than every valuation ring from $H_1$. If $H_2 = \emptyset$, then there is a finest valuation ring $\mathcal{O}^*$ in $H_1$.*

*Proof.* Let us first recall that if we have an inclusion $\mathcal{O} \subseteq \mathcal{O}_1$ of valuation rings of the same field $K$, then the residue class field $\mathcal{O}_1/\mathcal{M}_1$ contains the valuation ring $\mathcal{O}/\mathcal{M}_1$, and the residue class field of $\mathcal{O}/\mathcal{M}_1$ is the field $\mathcal{O}/\mathcal{M}$, which is, of course, also the residue class field of $\mathcal{O}$. Thus if $\mathcal{O}_1/\mathcal{M}_1$ is separably closed, so is $\mathcal{O}/\mathcal{M}$ (by Theorem 3.2.11, $\mathcal{O}/\mathcal{M}$ is even algebraically closed in case the inclusion $\mathcal{O} \subseteq \mathcal{O}_1$ is proper). Hence the property of having a separably closed residue class field always passes from a coarser valuation ring to a finer one. Recall also from Corollary 4.1.4 that $\mathcal{O}$ is henselian if and only if $\mathcal{O}_1$ and $\mathcal{O}/\mathcal{M}_1$ are henselian.

Now assume that $\mathcal{O}_1$ and $\mathcal{O}_2$ are two non-comparable henselian valuation rings of $K$, i.e., neither $\mathcal{O}_1 \subseteq \mathcal{O}_2$ nor $\mathcal{O}_2 \subseteq \mathcal{O}_1$ holds. Then $\mathcal{O} = \mathcal{O}_1\mathcal{O}_2$ is a proper coarsening of $\mathcal{O}_1$ and $\mathcal{O}_2$ and, of course, the finest such coarsening. Hence in the residue class field $\mathcal{O}/\mathcal{M}$ of $\mathcal{O}$, the induced valuation rings $\mathcal{O}_1/\mathcal{M}$ and $\mathcal{O}_2/\mathcal{M}$ are independent. Since both of them are henselian by Corollary 4.1.4, Theorem 4.4.1 implies that the residue class field $\mathcal{O}/\mathcal{M}$ is separably closed. By what we remarked above, the residue class field of $\mathcal{O}_1$ and $\mathcal{O}_2$ then are separably closed too. This shows that $\mathcal{O}_1$ and $\mathcal{O}_2$ both belong to $H_2$. Therefore, two rings from $H_1$ are always comparable, and if $\mathcal{O}_1 \in H_1$ and $\mathcal{O}_2 \in H_2$, we must have $\mathcal{O}_2 \subseteq \mathcal{O}_1$.

If $H_1 \neq \emptyset$, then $H_1$ forms a linear chain by inclusion. Therefore the intersection

$$\mathcal{O}^* = \bigcap_{\mathcal{O}_1 \in H_1} \mathcal{O}_1$$

is again a valuation ring of $K$. Using the fact that $\mathcal{M}^* = \bigcup_{\mathcal{O}_1 \in H_1} \mathcal{M}_1$ and Theorem 4.1.3 (7), we see that $\mathcal{O}^*$ is again henselian. Thus $\mathcal{O}^*$ is finer than each valuation ring from $H_1$. In particular, if $H_2 = \emptyset$, then $\mathcal{O}^*$ is the finest valuation ring in $H_1$.

In case $H_2$ is non-empty, the valuation ring $\mathcal{O}^*$ just defined may belong to $H_2$ or not, depending on whether its residue class field is separably closed or not. In any case $H_2$ has a maximal element $\mathcal{O}$, by Zorn's Lemma. In fact, we only have to check that every non-empty chain (= linearly ordered subset) $C$ of $H_2$ has an upper bound in $H_2$. This is clear if the chain $C$ already has a maximal element. Otherwise we consider the union

$$\mathcal{O}_1 = \bigcup_{\mathcal{O} \in C} \mathcal{O} \,.$$

$\mathcal{O}_1$ clearly is a henselian valuation ring of $K$ (by Corollary 4.1.4). It remains to show that the residue class field $\mathcal{O}_1/\mathcal{M}_1$ of $\mathcal{O}_1$ is separably closed. Observe that

$$\mathcal{O}_1/\mathcal{M}_1 = \bigcup_{\mathcal{O} \in C} \mathcal{O}/\mathcal{M}_1 \quad \text{and} \quad \mathcal{M}_1 = \bigcap_{\mathcal{O} \in C} \mathcal{M} \,.$$

Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_1[X]$ be a polynomial with discriminant $\delta \in \mathcal{O}_1^\times$ and assume that

$$\overline{f} = X^n + \overline{a}_{n-1}X^{n-1} + \cdots + \overline{a}_0$$

is a separable polynomial in the residue class field $\mathcal{O}_1/\mathcal{M}_1$ (where $\overline{a}_i = a_i + \mathcal{M}_1$). We have to show that $\overline{f}$ has a zero in $\mathcal{O}_1/\mathcal{M}_1$. Choose any $\mathcal{O} \in C$ such that $a_i, \delta \in \mathcal{O}$ and $\delta \notin \mathcal{M}$. Then the image of $f$ in the residue class field $k = \mathcal{O}/\mathcal{M}$ is still a separable polynomial. By assumption $\overline{f}$ has a zero in $k$ which, of course, has to be simple. Now observe that $\mathcal{O}/\mathcal{M}_1$ is a henselian valuation ring of $\mathcal{O}_1/\mathcal{M}_1$ (by Corollary 4.1.4). But then $\overline{f}$ has a zero in $\mathcal{O}_1/\mathcal{M}_1$, as required. This proves that $\mathcal{O}$ belongs to $H_2$.

Finally, we observe that $H_2$ cannot have two different maximal elements $\mathcal{O}_1$ and $\mathcal{O}_2$. Indeed, the valuation ring $\mathcal{O} = \mathcal{O}_1\mathcal{O}_2$ would have $\mathcal{O}_1/\mathcal{M}$ and $\mathcal{O}_2/\mathcal{M}$ as independent and henselian valuation rings in its residue class field $\mathcal{O}/\mathcal{M}$. Thus by Theorem 4.4.1, $\mathcal{O}/\mathcal{M}$ is separably closed and hence $\mathcal{O} \in H_2$. We denote the uniquely determined maximal element of $H_2$ by $\mathcal{O}^{**}$. □

Now we define the *canonical henselian valuation* $\mathcal{O}_c$ of $K$ to be $\mathcal{O}^{**}$ if $H_2 \neq \emptyset$ and $\mathcal{O}^*$ if $H_2 = \emptyset$. One should keep in mind that both cases $\mathcal{O}^* \neq \mathcal{O}^{**}$ and $\mathcal{O}^* = \mathcal{O}^{**}$ may occur. Thus in general $\mathcal{O}_c$ need not belong to $H_1$. For that reason we define

$$H = H_1 \cup \{\mathcal{O}_c\} .$$

Let us point out some properties of the canonical henselian valuation that we are going to use in what will follow:

(1) $\mathcal{O}_c$ is non-trivial iff $K$ admits a non-trivial henselian valuation and $K \neq K^s$;
(2) $\mathcal{O}_c$ is comparable with every henselian valuation ring of $K$, and so is each $\mathcal{O} \in H_1$;
(3) if the residue class field of $\mathcal{O}_c$ is not separably closed, no henselian valuation ring of $K$ has separably closed residue class field;
(4) if $\mathcal{O}$ is strictly coarser than $\mathcal{O}_c$, the residue class field $\mathcal{O}/\mathcal{M}$ is not separably closed;
(5) conversely, for any $\mathcal{O}$ finer than $\mathcal{O}_c$, the residue class field $\mathcal{O}/\mathcal{M}$ is separably closed;
(6) if $K$ is separably closed, then $\mathcal{O}_c$ is trivial, hence $H = \{K\}$.

We shall now prove three theorems showing that under certain conditions, the property of being henselian "goes down" an algebraic extension $L/K$, i.e., if $\mathcal{O}'$ is a non-trivial henselian valuation ring of $L$, then $\mathcal{O} = \mathcal{O}' \cap K$ is a (non-trivial) henselian valuation ring of $K$. Since we shall deal with the canonical henselian valuation of $L$ as well as of $K$, we shall use the notations

$$H_1(F), \quad H_2(F), \quad H(F), \quad \text{and} \quad \mathcal{O}_c(F) ,$$

indicating to which field $F$ the operations refer.

**Theorem 4.4.3.** *Let $L/K$ be a normal extension (finite or infinite) and let $\mathcal{O}' \in H(L)$. Then $\mathcal{O} = \mathcal{O}' \cap K \in H(K)$.*

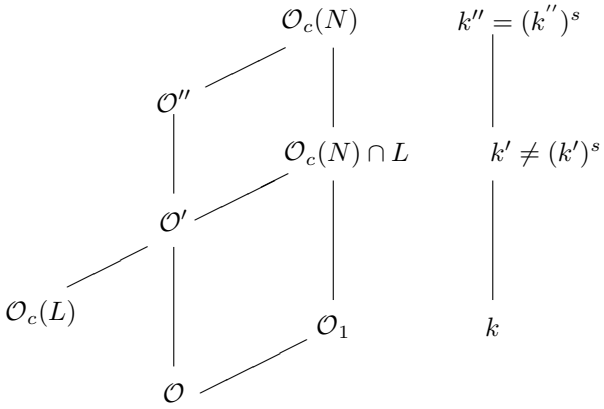
*Proof.* If $L = L^s$, then $\mathcal{O}'$ is trivial as well as $\mathcal{O}$. Now let $\mathcal{O}'$ be non-trivial (and thus $L \neq L^s$). Assume that $\mathcal{O}''$ is another extension of $\mathcal{O}$ to $L$. By Theorem 3.2.15, $\mathcal{O}'' = \sigma\mathcal{O}'$ for some $\sigma \in \mathrm{Aut}(L/K)$. Thus $\mathcal{O}''$ is as well henselian, and hence by (2) must be comparable with $\mathcal{O}'$. Then by Lemma 3.2.8, $\mathcal{O}'' = \mathcal{O}'$. Therefore $\mathcal{O}$ has a unique extension to $L$. Thus $\mathcal{O}$ is henselian in $K$. We still have to show that $\mathcal{O}_c(K) \subseteq \mathcal{O}$.

Assume that $\mathcal{O}$ is strictly contained in $\mathcal{O}_c(K)$ and hence $\mathcal{O} \in H_2(K)$. Take an extension $\mathcal{O}''$ of $\mathcal{O}_c(K)$ to $L$ containing $\mathcal{O}'$ and hence $\mathcal{O}_c(L)$. This is possible by Lemma 3.1.5. Since $\mathcal{O}''$ strictly contains $\mathcal{O}_c(L)$, the residue class field of $\mathcal{O}''$ is not separably closed. But then by Theorem 3.2.4 (2) the same applies[5] to $\mathcal{O}'' \cap K = \mathcal{O}_c(K)$, and hence $H_2(K)$ must be empty, a contradiction to the assumption $\mathcal{O} \in H_2(K)$ just made. □

**Theorem 4.4.4.** *Let $L \neq L^s$ and let $L/K$ be a finite extension. If $\mathcal{O}' \in H(L)$, then $\mathcal{O} = \mathcal{O}' \cap K \in H(K)$.*

*Proof.* Let $N/K$ be the normal hull of $L/K$. This is a finite extension, and thus by Theorem 4.3.5, $N \neq N^s$. (Note that $K \neq K^s$, as $L \neq L^s$.) Let $\mathcal{O}''$ be the unique extension of $\mathcal{O}'$ to $N$. We are going to compare $\mathcal{O}''$ with $\mathcal{O}_c(N)$.

If $\mathcal{O}''$ is coarser than $\mathcal{O}_c(N)$, then by Theorem 4.4.3 the restriction $\mathcal{O}'' \cap K = \mathcal{O}' \cap K = \mathcal{O}$ is henselian on $K$ and $\mathcal{O} \in H(K)$. If, however, $\mathcal{O}''$ is strictly finer than $\mathcal{O}_c(N)$, then $H_2(N) \neq \emptyset$. In particular, the residue class field $k''$ of $\mathcal{O}_c(N)$ is separably closed, while the residue class field $k'$ of $\mathcal{O}_c(N) \cap L$ cannot be separably closed, as $\mathcal{O}_c(N) \cap L$ now strictly contains $\mathcal{O}_c(L)$ (see diagram below).




[5] Note that any algebraic extension of a separably closed field is again separably closed.

Then clearly the residue class field $k$ of $\mathcal{O}_1 = \mathcal{O}_c(N) \cap K$ is also not separably closed. Since $[k'' : k]$ is finite by Corollary 3.2.3, Theorem 4.3.5 tells us that $k$ is real closed, and consequently $k' = k$ and $k'' = k'\big(\sqrt{-1}\big)$. We now see that $\mathcal{O} = \mathcal{O}' \cap K$ is henselian, by use of Corollary 4.1.4. In fact, $\mathcal{O}_1$ is henselian by Theorem 4.4.3, and the valuation ring $\mathcal{O}/\mathcal{M}_1$ in the residue class field $k$ of $\mathcal{O}_1$ is henselian by the following argument: since $k = k'$, the ring $\mathcal{O}/\mathcal{M}_1$ coincides with the image of $\mathcal{O}'$ in the residue class field $k'$ of $\mathcal{O}_c(N) \cap L$. By assumption, $\mathcal{O}'$ is henselian, hence also its image in the residue class field of a coarser valuation (Corollary 4.1.4).

We still have to conclude that $\mathcal{O} \in H(K)$. This now follows from the fact that the residue class field $k$ of $\mathcal{O}_1$ is real closed and that $\mathcal{O}/\mathcal{M}_1$ is a henselian valuation ring on $k$. Thus the residue class field of $\mathcal{O}/\mathcal{M}_1$, which coincides with that of $\mathcal{O}$, carries an ordering by Lemma 4.3.6, hence cannot be separably closed. □

In the final "going down" theorem we shall use a result from Chap. 5. Let us call a separable extension $L/K$ a *$p$-Sylow extension* ($p$ a rational prime) if no finite subextension $F/K$ of $L/K$ has a degree $[F : K]$ divisible by $p$, and all finite separable extensions $F/L$ have a $p$-power degree. Such fields are exactly the fixed fields of pro-$p$-Sylow subgroups of the absolute Galois group $G(K^s/K)$. As a result from (infinite) Galois theory (Sect. 5.1) one gets that two $p$-Sylow extensions $L_1/K$ and $L_2/K$ are always conjugate over $K$, i.e., there exists an automorphism $\sigma$ of $K^s$ over $K$ such that $L_2 = \sigma L_1$. We shall use this fact in the proof of the next theorem.[6]

Unlike Theorems 4.4.3 and 4.4.4, the next theorem needs an extra condition. This condition comes from the fact that a real closure $L$ of some field $K$ ordered by a non-archimedean ordering $\leq$ may be a 2-Sylow extension of $K$. As we saw in Sect. 4.3, the convex hull of $\mathbb{Z}$ in $K$ is a valuation ring $\mathcal{O}$ of $K$, as is the convex hull $\mathcal{O}'$ of $\mathbb{Z}$ in $L$. Clearly $\mathcal{O} = \mathcal{O}' \cap K$. By Theorem 4.3.7, $\mathcal{O}'$ is henselian. but there is no reason for $\mathcal{O}$ to be henselian too. Moreover, $\mathcal{O}'$ is even the canonical henselian valuation ring $\mathcal{O}_c(L)$. In fact, every henselian valuation ring $\mathcal{O}_1$ of $L$ is convex with respect to $\leq$ by Lemma 4.3.6, and $\mathcal{O}'$ is the smallest such valuation ring. Thus $H_2(L) = \emptyset$ and $\mathcal{O}' = \mathcal{O}_c(L)$.

In this last argument we never used that $L$ should be a 2-Sylow extension of $K$. We needed only the existence of a non-archimedean ordering $\leq$ on $L$. If $L$ is real closed, the residue class field of each henselian valuation ring $\mathcal{O}_1 \in H(L)$ also has a real closed residue class field. More generally, if $\mathcal{O} \subseteq \mathcal{O}_1$ are two henselian valuation rings on an arbitrary field $L$, and $\mathcal{O}_1$ has a real closed residue class field (like the trivial valuation ring on a real closed field), then so does $\mathcal{O}$. Indeed, $\mathcal{O}/\mathcal{M}_1$ is a henselian valuation ring on $k_1 = \mathcal{O}_1/\mathcal{M}_1$ (by

[6] To prove this fact, we could alternatively just follow the strategy of the proof of the Conjugation Theorem 3.2.15. By Zorn's Lemma we take a maximal Galois extension $N/K$ with $L_1 \cap N$ conjugate to $L_2 \cap N$, and then go a finite step further (if $N \neq K^s$) by using Sylow's theorem for finite groups.

Corollary 4.1.4). Now by Lemma 4.3.6, $\mathcal{O}/\mathcal{M}_1$ is convex in the unique ordering of $k_1$, and thus by Theorem 4.3.7 has itself a real closed residue class field. Thus real closed residue class fields are inherited from coarser valuation rings $\mathcal{O}_1 \in H_1(L)$. Actually, there is a maximal valuation ring $\mathcal{O}^+ \in H_1(L)$ with real closed residue class field. In fact, $\mathcal{O}^+$ is just the union of all $\mathcal{O}' \in H_1(L)$ with this property. One easily checks this by using the characterization (ii) of real closed fields in Fact 4.3.2 and the arguments we used in the proof of Theorem 4.4.2, showing that the union of a chain of henselian valuation rings of a field $L$ with separably closed residue class fields has itself a separably closed residue class field.

We shall refer to the ring $\mathcal{O}^+$ in the next theorem. In case $H(L)$ does not contain any ring $\mathcal{O}$ with real closed residue class field, we simply set $\mathcal{O}^+ = \mathcal{O}_c(L)$.

**Theorem 4.4.5.** (Koenigsmann) *Let $L/K$ be a $p$-Sylow extension, and let $\mathcal{O}' \in H(L)$. In case $p = 2$ we also assume that $\mathcal{O}'$ is coarser than the valuation ring $\mathcal{O}^+$ defined above. Then $\mathcal{O} = \mathcal{O}' \cap K \in H(K)$.*

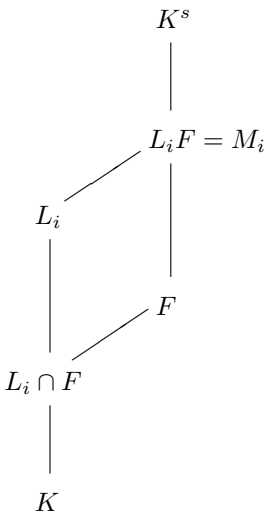
*Proof.* Assume that $\mathcal{O}'$ is non-trivial. Then, in particular, $L$ is neither separably nor real closed. We let $\mathcal{O}^s$ be the unique extension of $\mathcal{O}$ to $L^s$.

Now let $M$ be a finite extension of $L$, and let $\mathcal{O}_1 = \mathcal{O}^s \cap M$. Clearly $\mathcal{O}_1$ is henselian. We claim that $\mathcal{O}_1$ is the only henselian valuation ring of $M$ restricting to $\mathcal{O} = \mathcal{O}' \cap K$. Assume there is a second henselian valuation ring $\mathcal{O}_2$ on $M$ with $\mathcal{O}_2 \cap K = \mathcal{O}$. Then $\mathcal{O}_1$ and $\mathcal{O}_2$ cannot be independent, since otherwise $M$ would be separably closed and, as $[M : L]$ is finite, by Theorem 4.3.5, $L$ would be separably or real closed. Hence the valuation ring $\mathcal{O}_3 = \mathcal{O}_1\mathcal{O}_2$ is non-trivial and has the independent henselian valuation rings $\mathcal{O}_1/\mathcal{M}_3$ and $\mathcal{O}_2/\mathcal{M}_3$ in its residue class field $k = \mathcal{O}_3/\mathcal{M}_3$ (using Corollary 4.1.4). Note that $\mathcal{O}_1$ and $\mathcal{O}_2$ cannot be comparable, by Lemma 3.2.8, since they both restrict to $\mathcal{O}$ on $K$. Then by Theorem 4.4.1, $k$ is separably closed. The restriction $\mathcal{O}'' = \mathcal{O}_3 \cap L$ is strictly coarser than $\mathcal{O}_c(L)$, and thus cannot have separably closed residue class field $k''$. By Corollary 3.2.3, $[k : k'']$ is finite. Hence by Theorem 4.3.5, $[k : k''] = 2$ and $k''$ is real closed. In Theorem 3.3.3 we saw that $[k : k'']$ actually divides $[M : L]$, since $\operatorname{char} k'' = 0$. Therefore $p$ must be 2. In this case we have the extra assumption $\mathcal{O}^+ \subseteq \mathcal{O}'$. Since $\mathcal{O}''$ is strictly coarser than $\mathcal{O}'$, it cannot have a real closed residue class field, a contradiction. This proves our claim.

Let us now assume that $\mathcal{O} = \mathcal{O}' \cap K$ is not henselian. Then there exists a finite Galois extension $F/K$ together with two different prolongations $\mathcal{O}_1$ and $\mathcal{O}_2$ of $\mathcal{O}$ to $F$. For each $i = 1, 2$, let us fix a prolongation $\mathcal{O}_i^s$ of $\mathcal{O}_i$ to $K^s$. By the Conjugation Theorem 3.2.15, for each $i$ there exists a $\sigma_i \in G(K^s/K)$ such that $\mathcal{O}_i^s = \sigma_i\mathcal{O}^s$. Then for each $i$, $L_i := \sigma_i(L)$ is a $p$-Sylow extension of $K$, and $\mathcal{O}_i' = \sigma_i\mathcal{O}'$ is a henselian valuation ring of $L_i$. Now let $M_i = FL_i$. Observe that $[M_i : L_i]$ is finite, and that $\mathcal{O}_i'' = \mathcal{O}_i^s \cap M_i$ is a henselian valuation ring of $M_i$ extending $\mathcal{O}$ from $K$. Below we shall show that $M_i$ is a $p$-Sylow extension of

$F$. Hence there exists $\tau \in G(K^s/F)$ mapping $M_1$ to $M_2$ over $F$. But then $M_2$ would carry two different henselian valuation rings (note that $\mathcal{O}_2'' \cap F = \mathcal{O}_2$ and $\tau\mathcal{O}_1'' \cap F = \mathcal{O}_1$), both restricting to $\mathcal{O}$ on $K$. This contradicts the claim we have proved before. Thus $\mathcal{O}$ must be henselian. The fact that $\mathcal{O} \in H(K)$ follows exactly as in the proof of Theorem 4.4.3.

It remains to see that each $M_i/F$ is a $p$-Sylow extension. For that purpose, consider the diagram




Since $F/F \cap L_i$ is Galois and linearly disjoint to $L_i$, $M_i/F$ cannot have a subextension with degree divisible by $p$, since $L_i/F \cap L_i$ does not allow such a subextension. This already finishes the proof. □

## 4.5 Exercises

**Exercise 4.5.1.**
Let $(K, \mathcal{O})$ be henselian and $\operatorname{char} K = 0$. Show that for all $n \in \mathbb{N}$, the set $K^n \setminus \{0\}$ of non-zero $n$-th powers of elements of $K$ is open.

**Exercise 4.5.2.**
Let $(K, \mathcal{O})$ be a valued field and let $v$ be a valuation of $\widetilde{K}$ whose restriction to $K$ corresponds to $\mathcal{O}$. Suppose that for all $x, y \in \widetilde{K}$ the extension $K(x, y)/K(y)$ is purely inseparable whenever

$$v(y-x) > \max\{v(\sigma(x)-x) \mid \sigma \in \mathrm{Aut}(\widetilde{K}/K), \sigma(x) \neq x\}\,. \qquad (*)$$

Prove that $(K, \mathcal{O})$ is henselian.

*Hint:* Verify condition (6) of Theorem 4.1.3: Consider $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}[X]$ with $a_{n-1} \notin \mathcal{M}$ and $a_{n-2}, \ldots, a_0 \in \mathcal{M}$. Let $x_1$ be the unique zero of $f$ with $v(x_1) = 0$ and let $X^m + b_{m-1}X^{m-1} + \cdots + b_0$ be the minimal polynomial of $x_1$ over $K$. Now $x = x_1$ and $y = -b_{m-1}$ satisfy $(*)$. Conclude that $x_1 \in K$.

**Exercise 4.5.3.**
Let $(K, \mathcal{O})$ be henselian, and let $f \in K[X, Y]$ define the curve

$$C = \{(x, y) \in \widetilde{K} \times \widetilde{K} \mid f(x, y) = 0\}\,.$$

Assume that $(a, b) \in C \cap K \times K$ satisfies $\frac{\partial f}{\partial Y}(a, b) \neq 0$. Show that there exist neighbourhoods $U$ of $a$ and $V$ of $b$ in $K$ such that for every $x \in U$ there is exactly one $y \in V$ with $(x, y) \in C$.

Try to generalize this statement to an affine variety $V \subseteq \widetilde{K}^n$, defined over $K$, and a regular point $(a_1, \ldots, a_n) \in V \cap K^n$.

**Exercise 4.5.4.**
Show that the only henselian valuation on $\mathbb{R}$ is trivial.

**Exercise 4.5.5.**
Let $F$ be an ordered field and let $K = F(\sqrt{-1})$. Suppose that $(K^\times : (K^\times)^2) = 2$. Then the following statements hold:

(a) $F$ has exactly two orderings $\leq$ and $\leq'$, and $F$ is *pythagorean*, i.e., the sum of two squares in $F$ is again a square.

(b) Let $\mathcal{O}(\leq)$ and $\mathcal{O}(\leq')$ be a convex hulls of $\mathbb{Z}$ in $(F, \leq)$ and in $(F, \leq')$, respectively. Then $\mathcal{O}(\leq) = \mathcal{O}(\leq')$ if and only if both valuation rings are 2-henselian. (Note that $\mathcal{O}(\leq)$ may be trivial.)

(c) Let $F_0 = \mathbb{Q}(X)$ and fix two different orderings $\leq$ and $\leq'$ on $F_0$. Further let $R$ and $R'$ be the real closures of $(F_0, \leq)$ and $(F_0, \leq')$, respectively. Then $K = F(\sqrt{-1})$ with $F = R \cap R'$ satisfies $(K^\times : (K^\times)^2) = 2$.

**Exercise 4.5.6.**
Let $K$ be obtained from the $p$-adic number field $\mathbb{Q}_p$ by adjoining all $p^k$-th roots of unity ($k \in \mathbb{N}$), and let $\mathcal{O}$ be the unique extension of the (henselian) $p$-adic valuation ring $\mathbb{Z}_p$ from $\mathbb{Q}_p$ to $K$. Show that the residue class field remains $\mathbb{F}_p$ and that the value group becomes $p$-divisible. Deduce from these facts that the unique extension of $\mathcal{O}$ to $K(\sqrt[p]{p})$ is immediate.

*Hint:* Observe that $Y^{p-1} + \cdots + 1 = \prod_{p \nmid r}(X - \zeta^r)$ where $Y = X^{p^{k-1}}$, $\zeta$ is a primite $p^k$-th root of unity, and $r$ runs from 0 to $p^k - 1$. Consequently, $p = \prod_{p \nmid r}(1 - \zeta^r)$.

**Exercise 4.5.7.**
Let $(K, \mathcal{O})$ be a henselian valued field, and assume that $\operatorname{char} \overline{K} = 0$. Prove that there exists an embedding $\varepsilon : \overline{K} \to K$ such that $\varepsilon(\overline{a}) = a$ for all $\overline{a} \in \overline{K}$.

*Hint*: Since $\operatorname{char} \overline{K} = 0, \mathbb{Q}$ is a subfield of $\overline{K}$, embedding canonically into $K$. Look for a maximal such subfield of $\overline{K}$.

# 5

# Structure Theory

In the last chapter we have seen many useful properties of henselian fields. The usefulness of such fields will become even more clear in the next chapter, where we give some non-trivial applications. The reason why henselian fields are so useful lies in the fact that problems about a henselian field $K$ very often can be reduced to problems about the residue class field $\overline{K}$ and the value group $\Gamma$. This reduction property is also reflected in the absolute Galois group $G(K^s/K)$ of $K$. Its structure relates to $\overline{K}$ and $\Gamma$ as well. Let us explain this in more detail.

Given a valued field $(K, \mathcal{O})$ we shall fix an extension $\mathcal{O}^s$ of $\mathcal{O}$ to the separable closure $K^s$ of $K$ and always refer to it. We then introduce three distinguished subgroups of $G = G(K^s/K)$, namely the decomposition group $G^h$, the inertia group $G^t$, and the ramification group $G^v$. These groups form a descending chain

$$G \supseteq G^h \supseteq G^t \supseteq G^v \ .$$

By infinite Galois theory (introduced in Sect. 5.1), the corresponding fixed fields form an ascending chain

$$K \subseteq K^h \subseteq K^t \subseteq K^v \ .$$

$K^h$ will be a henselian field (the henselization of $K$), and $K$ is henselian if and only if $K = K^h$. The valued field $K^h$ is an immediate extension of $(K, \mathcal{O})$. From $K^h$ to $K^t$ the value group does not change, but the residue class field gets separably closed. This is reflected in the *first exact sequence* (Sect. 5.2)

$$1 \longrightarrow G^t \longrightarrow G^h \longrightarrow G(\overline{K}^s/\overline{K}) \longrightarrow 1 \ .$$

In particular, $G^t$ is a normal subgroup of $G^h$.

From $K^t$ to $K^v$ the residue class field remains the separable closure $\overline{K}^s$ of $\overline{K}$, while the value group will become $q$-divisible by every prime $q$ different from $\operatorname{char} \overline{K}$ (in case $\operatorname{char} \overline{K} \neq 0$). This is expressed in the *second exact sequence* (Sect. 5.3)

$$1 \longrightarrow G^v \longrightarrow G^t \longrightarrow \mathrm{Hom}(\Delta/\Gamma, \Omega) \longrightarrow 1 \,,$$

where $\Delta$ is the value group of $K^v$ and $\Omega$ is the group of roots of unity in $\overline{K}^s$. In particular, $G^t/G^v$ is abelian.

If we now consider the case of a 'tamely ramified' henselian field, i.e., $G = G^h$ and $G^v = \{1\}$, then $G^t$ is an abelian normal subgroup of $G$. In the interesting cases, one actually has in addition that $G^t$ is a non-trivial subgroup of $G$. This situation is very typical for the absolute Galois group $G$ of many henselian fields: $G$ contains an abelian normal subgroup $H \neq \{1\}$. In Sect. 5.4 we shall prove that, apart from very few exceptions, the converse holds for $p$-groups. Thus if $P$ is a $p$-Sylow subgroup of $G = G(K^s/K)$, one can tell from the structure of $P$ that the fixed field $L$ of $P$ has a henselian valuation. But then by the 'going down' Theorem 4.4.5 one can tell that $K$ has a henselian valuation.

Before we start with the structure theory, we shall offer the reader not familiar with infinite Galois theory and the language of profinite groups a short introduction to this subject in Sect. 5.1. For more information about profinite groups we refer the reader to the books [24] and [31].

## 5.1 Infinite Galois Groups

Let $N$ be an arbitrary Galois extension of a field $K$. This means that $N/K$ is separable algebraic and normal, but need not be of finite degree. In order to produce a $K$-automorphism $\sigma$ of $N$ we may consider the set of all ordered pairs $(F, \sigma_F)$, where $F/K$ is a finite intermediate Galois extension of $N/K$ and $\sigma_F$ is a $K$-automorphism of $F$, and such that every time $E \subseteq F$, for any two such extensions, the restriction of $\sigma_F$ to $E$ coincides with $\sigma_E$. Then $\sigma : N \longrightarrow N$, defined as $\sigma(x) = \sigma_F(x)$ if $x \in F$, will be a $K$-automorphism of $N$ whose restriction to each $F$ equals $\sigma_F$. In fact this procedure gives all the $K$-automorphisms of $N$, and allows us to understand the Galois group $G(N/K) = \mathrm{Aut}(N/K)$ as an "inverse limit" of the finite Galois groups $G(F/K)$. In order to make this precise, we need a little excursion to the land of profinite groups.

Take an indexed set of finite groups $G_i$, $i \in I$, where $I$ is a directed partially ordered set, i.e., $I$ is equipped with a partial order $\leq$, and for all $i, j \in I$ there exists $k \in I$ such that $i, j \leq k$. Consider next a collection of triples $(G_i, G_j, \psi_{i,j})$, where $j \leq i$ and $\psi_{i,j} : G_i \longrightarrow G_j$ is a surjective group homomorphism. Suppose that $\psi_{i,i} = \mathrm{id}$, the identity map of $G_i$, and if $k \leq j \leq i$ then $\psi_{i,k} = \psi_{j,k} \circ \psi_{i,j}$. Such a collection is usually called an *inverse system*(*projective system*) of finite groups.

Now set

$$\varprojlim G_i = \left\{ (g_i) \in \prod_{i \in I} G_i \;\middle|\; \psi_{i,j}(g_i) = g_j \text{ for } j \leq i \right\} .$$

Taking $\prod_{i\in I} G_i$ endowed with the coordinatewise operation, induced by the operations of the groups $G_i$, clearly makes $\varprojlim G_i$ a subgroup of $\prod_{i\in I} G_i$, which is called the *inverse limit* (*projective limit*) of the inverse system.

Additionally, taking each $G_i$ with the discrete topology and $\prod_{i\in I} G_i$ with the product topology, it follows that $\varprojlim G_i$ is a closed subset of $\prod_{i\in I} G_i$. Indeed, for $(x_i) \notin \varprojlim G_i$, there exist $k \leq j$ such that $\psi_{j,k}(x_j) \neq x_k$. Then

$$X := \left\{ (g_i) \in \prod_{i\in I} G_i \;\middle|\; \psi_{j,k}(g_j) = \psi_{j,k}(x_j) \text{ and } g_k = x_k \right\}$$

is an open set in $\prod_{i\in I} G_i$ containing the sequence $(x_i)$. Clearly $X \cap \varprojlim G_i = \emptyset$.

Since each $G_i$ is a Hausdorff compact totally disconnected (every point is its own connected component) topological space, it follows that $\prod_{i\in I} G_i$, and hence also $\varprojlim G_i$, are Hausdorff compact totally disconnected topological spaces. Moreover, for each $i$, the group operation $G_i \times G_i \longrightarrow G_i$ and taking inverses in $G_i$ are continuous maps as well as the homomorphisms $\psi_{i,j}$. Hence the same is true for $\prod_{i\in I} G_i$ and its subgroup $\varprojlim G_i$. Conversely one can show that a Hausdorff compact and totally disconnected topological group is an inverse limit of an inverse system of finite groups. Topological groups with a Hausdorff compact and totally disconnected topology are called *profinite*. In particular, every finite group is a profinite group. Profinite groups receive more precise denominations according to the nature of the groups $G_i$ in the inverse system. For example, if all $G_i$ are $p$-groups, for a fixed prime $p$, then $\varprojlim G_i$ is called a *pro-p group*. In a similar way *prosolvable*, *pronilpotent*, *procyclic*, (etc.) *groups* are introduced.

The inverse limit can be characterized by the following universal property, which makes it unique:

**Lemma 5.1.1.** *The profinite group $G$ is the inverse limit of the inverse system of finite groups $\{ (G_i, G_j, \psi_{i,j}) \mid i, j \in I \}$ if and only if the following conditions hold:*

*(1) For every $i$ there exists a continuous group homomorphism $\psi_i : G \longrightarrow G_i$ such that $\psi_{i,j} \circ \psi_i = \psi_j$ for all $j \leq i$.*
*(2) If $G'$ is any profinite group such that for every $i$ there exists a continuous homomorphism $\varphi_i : G' \longrightarrow G_i$ satisfying $\psi_{i,j} \circ \varphi_i = \varphi_j$ for all $j \leq i$, then there exists a unique continuous homomorphism $\varphi : G' \longrightarrow G$ such that $\psi_i \circ \varphi = \varphi_i$, for every $i$.*

*If in (2) we assume, additionally, that $\varphi_i$ is surjective for every $i \in I$, then $\varphi$ is also surjective.*

Consequently, any two groups $G$ and $G'$ satisfying the above conditions (1) and (2) are topologically isomorphic.

*Proof.* For item (1) take $\psi_i$ as the restriction to $\varprojlim G_i$ of the natural projections

$$\prod_{i\in I} G_i \longrightarrow G_i \ .$$

(2) The compatibility condition $\psi_{i,j}\circ\varphi_i = \varphi_j$ implies for each $g \in G'$ that $(\varphi_i(g))_{i\in I} \in \varprojlim G_i$. Then $\varphi(g) = (\varphi_i(g))_{i\in I}$ will do the desired job.

Since $G'$ is compact and $\varphi$ is a continuous map, $\varphi(G')$ is a closed subgroup of $\varprojlim G_i$. We claim that $\varphi(G')$ is a dense subgroup of $\varprojlim G_i$, provided that all $\varphi_i$ are surjective. Then this will imply $\varphi(G') = \varprojlim G_i$, as contended.

To prove the density, take a basic open subset $\mathcal{U} \subseteq \prod_{i\in I} G_i$. I.e., for some finite subset $\{i_1, \ldots, i_n\} \subseteq I$ there exist non-empty open subsets $\mathcal{U}_{i_j} \subseteq G_{i_j}$, $1 \le j \le n$, such that

$$(g_i)_{i\in I} \in \mathcal{U} \qquad \Leftrightarrow \qquad g_{i_j} \in \mathcal{U}_{i_j}, \quad \text{for every} \quad j = 1, \ldots, n \ .$$

We have to show that

$$\left(\varprojlim G_i \cap \mathcal{U}\right) \cap \varphi(G') \neq \emptyset \ .$$

Take $i_0 \in I$ satisfying $i_0 \ge i_j$ for every $j = 1, \ldots, n$, and take any $(g_i)_{i\in I} \in \varprojlim G_i \cap \mathcal{U}$. Then $\psi_{i_0,i_j}(g_{i_0}) = g_{i_j}$ for every $j = 1, \ldots, n$. Choose next $g \in G'$ such that $\varphi_{i_0}(g) = g_{i_0}$. From the compatibility conditions of (2) it follows that $\varphi_{i_j}(g) = g_{i_j} \in \mathcal{U}_{i_j}$ for every $j = 1, \ldots, n$. Hence $\varphi(g) \in \varprojlim G_i \cap \mathcal{U}$, completing the proof. □

The above lemma has a corresponding version for pro-$p$ groups, proabelian groups, and so on.

Let $G = \varprojlim G_i$ be a profinite group. Given $n \in \mathbb{N}$ and a prime number $p$, we say that $p^n$ *divides the order* of $G$ if $p^n$ divides the order $|G_i|$ of $G_i$ for some $i$. If $p^n$ divides the order of $G$ for every $n \in \mathbb{N}$, we say that $p^\infty$ divides the order of $G$. Consequently we define the *order* of a profinite group $G$ as:

$$|G| = \prod_p p^{\nu_p}, \ \text{where } \nu_p = \max\{\, n \in \mathbb{N} \cup \{\infty\} \mid p^n \text{ divides the order of } G\} \ .$$

The order of a profinite group is a so-called *supernatural* number, and of course the order of a pro-$p$ group is a "supernatural" power of $p$.

Let us present the simplest examples of non-finite profinite groups, namely, the procylic groups. Let $\mathbb{P}'$ be a set of rational primes, and write $\mathbb{M}$ for the set consisting of all products of primes in $\mathbb{P}'$. Consider then the collection of all triples

$$(\mathbb{Z}/s\mathbb{Z}, \mathbb{Z}/r\mathbb{Z}, \vartheta_{s,r}) \ ,$$

where $r, s \in \mathbb{M}$, the partial order $r \le s$ is defined by $r|s$, and $\vartheta_{s,r}$ is the canonical projection from $\mathbb{Z}/s\mathbb{Z}$ to $\mathbb{Z}/r\mathbb{Z}$ ($\vartheta_{s,s} = id$). For $r$, $s$, $t \in \mathbb{M}$ satisfying

$t|r$ and $r|s$, we obviously have $\vartheta_{s,t} = \vartheta_{r,t} \circ \vartheta_{s,r}$. Thus $(\mathbb{Z}/s\mathbb{Z}, \mathbb{Z}/r\mathbb{Z}, \vartheta_{s,r})$ is a projective system of finite additive groups. Let

$$\widehat{Z}_{\mathbb{P}'} = \varprojlim \mathbb{Z}/n\mathbb{Z}, \quad n \in \mathbb{M} .$$

The group $\widehat{Z}_{\mathbb{P}'}$ is called the $\mathbb{P}'$-*procyclic* group and has order $\prod_{p\in\mathbb{P}'} p^\infty$. This name makes sense because the natural embedding $\mathbb{Z} \hookrightarrow \widehat{Z}_{\mathbb{P}'}$ sends the integers to a dense subgroup of $\widehat{Z}_{\mathbb{P}'}$, or equivalently, $\widehat{Z}_{\mathbb{P}'}$ is topologically generated by 1. Moreover, for every $m \in \mathbb{M}$ we have that $m\widehat{Z}_{\mathbb{P}'} \cap \mathbb{Z} = m\mathbb{Z}$ and $\widehat{Z}_{\mathbb{P}'}/m\widehat{Z}_{\mathbb{P}'} \cong \mathbb{Z}/m\mathbb{Z}$. Clearly the map sending $\hat{a} \in \widehat{Z}_{\mathbb{P}'}$ to $m\hat{a} \in m\widehat{Z}_{\mathbb{P}'}$ is a topological isomorphism. Therefore each $m\widehat{Z}_{\mathbb{P}'}$ is also a $\mathbb{P}'$-procyclic group.

In particular, if $\mathbb{P}'$ contains all rational primes, we just write $\widehat{\mathbb{Z}}$. This group is known as the *Prüfer completion* of $\mathbb{Z}$ or simply the *Prüfer group*. Another important case is when $\mathbb{P}' = \{p\}$. In this case, $\widehat{Z}_{\mathbb{P}'}$ is known as the *pro-p completion* of $\mathbb{Z}$, and is isomorphic to the additive group of the $p$-adic integers, $\mathbb{Z}_p$. Indeed, recall from Proposition 1.3.5 that every non-zero $z \in \mathbb{Z}_p$ has a unique representation

$$z = \sum_{i=0}^{\infty} a_i p^i ,$$

where $a_m \neq 0$ for some $m \geq 0$, and $0 \leq a_i < p$ for every $i$. Thus for every $n \geq 1$ we have an epimorphism $\varphi_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ given by

$$\varphi_n(z) = a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} + p^n\mathbb{Z} .$$

According to Lemma 5.1.1 there exists an epimorphism $\varphi : \mathbb{Z}_p \longrightarrow \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. Since $\varphi$ is clearly injective, compactness implies that it is a topological isomorphism.

The most basic properties of profinite (resp. pro-$p$) groups $G$ are:

- Every open subgroup of $G$ is also closed:
  Take a set $\{ g_\lambda \mid \lambda \in \Lambda \}$ of representatives of the cosets determined by $H$ in $G$. Then
  $$H = G \setminus \bigcup_{\substack{\lambda\in\Lambda \\ g_\lambda \notin H}} Hg_\lambda$$
  is closed.
- If $H$ is a closed subgroup of $G$, then $G/H$ is finite if and only if $H$ is open: recall that $G$ is compact.

Let us return for a moment to the $\mathbb{P}'$-procyclic groups. Take $H$ an open subgroup of $\widehat{Z}_{\mathbb{P}'}$ such that $\widehat{Z}_{\mathbb{P}'}/H$ has $r \in \mathbb{N}$ elements. Then $r \cdot 1 \in H$. Thus $r\mathbb{Z} \subseteq H \cap \mathbb{Z}$. On the other hand, the density of $\mathbb{Z}$ within $\widehat{Z}_{\mathbb{P}'}$ yields for every $\hat{z} \in \widehat{Z}_{\mathbb{P}'}$ a $z \in \mathbb{Z}$ such that $z \in \hat{z} + H$. This means that the restriction to $\mathbb{Z}$ of the natural projection $\widehat{Z}_{\mathbb{P}'} \longrightarrow \widehat{Z}_{\mathbb{P}'}/H$ is surjective. Consequently, $r\mathbb{Z} = H \cap \mathbb{Z}$, $r \in \mathbb{M}$, and $H = r\widehat{Z}_{\mathbb{P}'}$. So the $\mathbb{P}'$-procyclic groups have the following distinguished property:

- Every open subgroup of $\widehat{Z}_{\mathbb{P}'}$ has the form $r\widehat{Z}_{\mathbb{P}'}$, for some $r \in \mathbb{M}$, and thus is $\mathbb{P}'$-procyclic, too.

Further properties of profinite groups are:

- Every closed subgroup $H$ of $G$ is also a profinite (pro-$p$) group:
  This follows from
  $$H = \varprojlim HU/U \ ,$$
  where $U$ ranges over the set of all open normal subgroups of $G$. In particular,
  $$G = \varprojlim G/U \ .$$
- For a closed subgroup $H \subseteq G$, we have that $|H|$ divides $|G|$, in the sense that
  $$|G| = \prod_p p^{\nu_p} \qquad \text{and} \qquad |H| = \prod_p p^{\mu_p} \ ,$$
  where $\mu_p \leq \nu_p$ for every $p$.
- For a closed subgroup $H \subseteq G$ the *index* of $H$ in $G$, denoted by $(G : H)$, is defined to be the product of all powers $p^\nu$ of prime numbers, where $\nu$ is either $\infty$, or the largest number $\nu \in \mathbb{N}$ for which there is an open normal subgroup $U \subseteq G$ such that $p^\nu$ divides the index $(G/U : HU/U)$.
- The above definition implies that Lagrange's Theorem remains true for profinite groups:
  $$|G| = (G : H)|H| \ ,$$
  where the product of supernatural numbers is defined by adding exponents of the powers of prime numbers (where $\infty + \infty = \infty$ and $\nu + \infty = \infty + \nu = \infty$ for $\nu \in \mathbb{N}$).
- If a prime number $p$ divides $|G|$, then there exists a maximal closed subgroup $S_p$ with order a supernatural number $p^\nu$. Moreover, $p$ does not divide $(G : S_p)$, and any other maximal closed subgroup of $G$ with order a power of $p$ is conjugate to $S_p$ in $G$. These maximal pro-$p$ subgroups of $G$ are called the *$p$-Sylow subgroups* of $G$. We also have
  $$|G| = \text{l.c.m.}\{\, |S_p| \mid p \text{ prime and } S_p \text{ a } p\text{-Sylow subgroup of } G \,\} \ .$$

Looking at the $\mathbb{P}'$-procyclic group $\widehat{Z}_{\mathbb{P}'}$ introduced above, we see that $\mathbb{Z}_p$ is the $p$-Sylow subgroup of $\widehat{Z}_{\mathbb{P}'}$ for every $p \in \mathbb{P}'$. Moreover, we also have the decomposition
$$\widehat{Z}_{\mathbb{P}'} \cong \prod_{p \in \mathbb{P}'} \mathbb{Z}_p \ .$$

Now let $H$ and $K$ be closed subgroups of a profinite group $G$, and let $H$ be a normal subgroup. Then $H \times K$ is compact in the product topology on $G \times G$. Since the map $(x, y) \mapsto xy$ is continuous, the image
$$HK = \{\, hk \mid h \in H,\ k \in K \,\}$$

of $H \times K$ is a closed subset of $G$. Moreover, the normality of $H$ implies that $HK$ is a subgroup of $G$. This closed subgroup $G_1$ is called the *semidirect product* of $H$ and $K$ in $G$, and $K$ is called a *complement* to $H$ in $G_1$. We write $H \rtimes K$ for $G_1 = HK$.

Suppose that $f : G \to G'$ is a continuous epimorphism of profinite groups with kernel $H$. Then $H$ has a complement in $G$ if and only if there exists a continuous homomorphism $g : G' \to G$ such that $f \circ g = \mathrm{id}$. In this case the exact sequence

$$1 \to H \to G \to G' \to 1$$

splits, and $K = g(G')$ is a complement to $H$ in $G$.

We finish this short trip to the land of profinite groups with our most interesting example. For an arbitrary Galois extension $N$ of a field $K$, let $I$ be the set of all intermediate finite Galois extensions $K \subseteq F \subseteq N$. The set $I$ is a directed set when ordered by inclusion. For each $F \in I$ denote by $G_F$ the Galois group $G(F/K)$ of $F$ over $K$. For $E \subseteq F \in I$ write $\psi_{F,E}$ for the natural surjective homomorphism $G_F \twoheadrightarrow G_E$ defined by restricting a $K$-automorphism of $F$ to the subfield $E$. Then $\{\, (G_E, G_F, \psi_{F,E}) \mid E, F \in I \,\}$ is an inverse system of finite groups. Set $G = \varprojlim G_F$ for short.

Now let $G(N/K)$ be the Galois group of all $K$-automorphisms of $N$ endowed with the topology which has the set of all $G(N/F)$, $F \in I$, as a fundamental system of neighborhoods of the identical map. From

$$N = \bigcup_{F \in I} F \qquad \text{one gets} \qquad \bigcap_{F \in I} G(N/F) = \{\mathrm{id}\} \,.$$

Hence this topology has the Hausdorff property. We shall see that $G(N/K)$ is also compact and totally disconnected, i.e., it is a profinite group. Moreover, $G$ and $G(N/K)$ are topologically isomorphic. To show these facts, define

$$\Phi : G(N/K) \longrightarrow \prod_{F \in I} G_F \qquad \text{by} \qquad \Phi(\sigma) = (\sigma|_F)_{F \in I} \,.$$

Clearly $\Phi$ is an injective group homomorphism, and by proving that $\Phi$ is continuous with a closed image, we shall get the other two desired properties for $G(N/K)$. Every basic open neighborhood of the $1 \in \prod_{F \in I} G_F$ is a finite intersection of subsets of the type

$$V_E = \{\, (\rho_F)_{F \in I} \mid \rho_E = \mathrm{id} \,\} \subseteq \prod_{F \in I} G_F \,,$$

with $E \in I$. Hence $\Phi$ is continuous, since $\Phi^{-1}(V_E) = G(N/E)$.

Next take $(\rho_F)_{F \in I} \notin \Phi(G(N/K))$ in order to show that $\Phi(G(N/K))$ is closed. If for every $E \subseteq F$ one finds that $\rho_E = \rho_F|_E$, then we saw in the very beginning of this discussion that $\rho : N \longrightarrow N$, constructed as

$$\rho(x) = \rho_F(x) \text{ for all } x \in F \,,$$

would be a $K$-automorphism of $N$ such that $\Phi(\rho) = (\rho_F)_{F\in I}$, a contradiction. Thus there exist $E, F \in I$ such that $\rho_E \neq \rho_F|_E$, and the open set

$$V = \{\, (\sigma_F)_{F\in I} \mid \sigma_E = \rho_E \text{ and } \sigma_F = \rho_F \,\}$$

contains $(\rho_F)_{F\in I}$ and satisfies $V \cap \Phi(G(N/K)) = \emptyset$. Thus $\Phi(G(N/K))$ is closed as required and thus $G(N/K)$ is a profinite group.

Additionally, composing $\Phi$ with the projections $\prod_{F\in I} G_F \longrightarrow\!\!\!\!\!\rightarrow G_F$, one gets continuous maps $\varphi_F : G(N/K) \longrightarrow G_F$ satisfying $\psi_{F,E} \circ \varphi_F = \varphi_E$ whenever $E \subseteq F$. Therefore the universal property of $G$ (cf. Lemma 5.1.1) gives a continuous group homomorphism $\varphi : G(N/K) \longrightarrow G$ satisfying $\psi_F \circ \varphi = \varphi_F$ for every $F \in I$.

Clearly $\varphi$ is injective. We shall prove next that each $\varphi_F$ is a surjective map. Thus Lemma 5.1.1 also implies that $\varphi$ is surjective. From compactness it follows that $\varphi$ is a topological isomorphism.

In order to prove that $\varphi_F$ is surjective, take $\sigma \in G_F$, and consider the set of ordered pairs $(E, \sigma_E)$, where $E$ is a normal extension of $F$ contained in $N$, $\sigma_E \in G(E/F)$, and $\sigma = \sigma_E|_F$. This set contains $(F, \sigma)$, and can be partially ordered as follows:

$$(E, \sigma_E) \leq (E', \sigma_{E'}) \Leftrightarrow E \subseteq E' \text{ and } \sigma_E = \sigma_{E'}|_E \,.$$

By Zorn's lemma there exists a maximal such pair $(E_0, \sigma_0)$. By proving that $E_0 = N$, we show the surjectivity of $\varphi_F$. If there were $x \in N \smallsetminus E_0$ there would be a Galois extension $E_1$ of $F$ with $x \in E_1$ and $E_1$ finite over $E_0$. Hence $\sigma_0$ would have an extension $\sigma_1$ to $E_1$. Thus $(E_0, \sigma_0) < (E_1, \sigma_1)$, contradicting the maximality of $(E_0, \sigma_0)$.

Consequently $G(N/K) = \varprojlim G_F$, where $F$ ranges over the set of all finite intermediate Galois extensions.

Next we quote the Galois correspondence for arbitrary Galois extensions, finite or infinite.

**Theorem 5.1.2.** *Let $N$ be a Galois extension of a field $K$ with Galois group $G$. Then the assignments*

$$E \longmapsto G(N/E) \quad \textit{and} \quad H \longmapsto \operatorname{Fix} H$$

*yield an inclusion-reversing, bijective correspondence between the set of all intermediate extensions $K \subseteq E \subseteq N$ and the set of all closed subgroups $H$ of $G$.*

## 5.2 Unramified Extensions – First Exact Sequence

For a valued field $(K, \mathcal{O})$, let $\mathcal{O}^s$ be an extension of $\mathcal{O}$ to the separable closure $K^s$ of $K$. Set

$$G^h(\mathcal{O}^s) = \{\, \sigma \in G(K^s/K) \mid \sigma(\mathcal{O}^s) = \mathcal{O}^s \,\} ,$$

or just $G^h$ if the valuation ring $\mathcal{O}^s$ is clear in the context. Obviously, $G^h(\mathcal{O}^s)$ is a subgroup of $G(K^s/K)$; it is called the *decomposition group* of $\mathcal{O}^s$ over $K$.

Note that by Lemma 3.2.8, $\sigma \in G(K^s/K)$ belongs to $G^h(\mathcal{O}^s)$ if and only if $\mathcal{O}^s \subseteq \sigma(\mathcal{O}^s)$.

**Lemma 5.2.1.** *$G^h(\mathcal{O}^s)$ is a closed subgroup of $G(K^s/K)$. Moreover, if $\mathcal{O}_1^s$ is another prolongation of $\mathcal{O}$ to $K^s$, then $G^h(\mathcal{O}_1^s)$ is conjugate to $G^h(\mathcal{O}^s)$ in $G(K^s/K)$.*

*Proof.* Given $\sigma \notin G^h(\mathcal{O}^s)$, take $\alpha \in \mathcal{O}^s$ with $\alpha \notin \sigma(\mathcal{O}^s)$. Let $N \subseteq K^s$ be a finite Galois extension of $K$ such that $\alpha \in N$. We see that $\mathcal{O}^s \cap N \neq \sigma(\mathcal{O}^s) \cap N$. Since for every $\rho \in G(K^s/N)$ we have $\rho(\mathcal{O}^s) \cap N = \mathcal{O}^s \cap N$, it follows that $\sigma \circ \rho(\mathcal{O}^s) \neq \mathcal{O}^s$. Hence $\sigma G(K^s/N) \cap G^h(\mathcal{O}^s) = \emptyset$, proving the first statement.

By the Conjugation Theorem 3.2.15, $\mathcal{O}_1^s = \sigma(\mathcal{O}^s)$ for some $\sigma \in G(K^s/K)$. Thus $G^h(\mathcal{O}_1^s) = \sigma G^h(\mathcal{O}^s)\sigma^{-1}$, proving the second statement. □

Set $K^h(\mathcal{O}^s)$ for the fixed field of $G^h(\mathcal{O}^s)$. This field is called the *decomposition field* of $\mathcal{O}^s$ over $K$. From Galois theory we obtain $G(K^s/K^h(\mathcal{O}^s)) = G^h(\mathcal{O}^s)$. Therefore the Conjugation Theorem 3.2.15 implies that $\mathcal{O}^s$ is the unique extension of $\mathcal{O}^s \cap K^h(\mathcal{O}^s)$ to $K^s$. According to Lemma 4.1.1, $\mathcal{O}^h := \mathcal{O}^s \cap K^h(\mathcal{O}^s)$ is thus a henselian valuation ring.

The valued field $(K^h, \mathcal{O}^h)$ is called a *henselization* of $(K, \mathcal{O})$. Lemma 5.2.1 now shows that any two henselizations of $(K, \mathcal{O})$ are $K$-conjugate. Observe that $(K, \mathcal{O})$ is henselian if and only if $K = K^h$.

**Theorem 5.2.2.** *The henselization $(K^h, \mathcal{O}^h)$ of $(K, \mathcal{O})$ has the following characterization:*

*(1) $(K^h, \mathcal{O}^h)$ is henselian, and*
*(2) if $(K_1, \mathcal{O}_1)$ is a henselian valued extension of $(K, \mathcal{O})$, then there exists a uniquely determined $K$-embedding $\iota : (K^h, \mathcal{O}^h) \longrightarrow (K_1, \mathcal{O}_1)$, i.e., $\iota(\mathcal{O}^h) = \mathcal{O}_1 \cap \iota(K^h)$ and $\iota|_K = \mathrm{id}$.*

*Proof.* We will first show that $(K^h, \mathcal{O}^h)$ satisfies (2).

We know from Corollary 4.1.5 that a relatively separably closed subfield $(L, \mathcal{O}') \subseteq (K_1, \mathcal{O}_1)$ is also henselian. Hence it suffices to consider the case in which $K_1/K$ in (2) is separable.

Let $\mathcal{O}_1^s$ be the uniquely determined extension of $\mathcal{O}_1$ to $K^s$. Then $G(K^s/K_1) \subseteq G^h(\mathcal{O}_1^s)$; equivalently $K^h(\mathcal{O}_1^s) \subseteq K_1$. Moreover, $\mathcal{O}_1^s$ is also an extension of $\mathcal{O}$ to $K^s$. Thus there exists $\iota \in G(K^s/K)$ such that $\iota(\mathcal{O}^s) = \mathcal{O}_1^s$ and, according to Lemma 5.2.1, $\iota(K^h) = K^h(\mathcal{O}_1^s)$.

Moreover, $\iota$ is uniquely determined: suppose that $\rho : K^h \longrightarrow K_1$ is a homomorphism such that $\rho|_K = \mathrm{id}$ and $\rho(\mathcal{O}^h) = \mathcal{O}_1^s \cap \rho(K^h)$. Extend $\rho$ to a $K$-automorphism of $K^s$, also called $\rho$. Then

$$\rho(\mathcal{O}^s) \cap \rho(K^h) = \rho(\mathcal{O}^s \cap K^h) = \rho(\mathcal{O}^h) = \mathcal{O}_1^s \cap \rho(K^h) .$$

But $\rho(\mathcal{O}^h)$ is also henselian. Hence $\rho(\mathcal{O}^s) = \mathcal{O}_1^s$. Consequently $\rho^{-1}\iota(\mathcal{O}^s) = \mathcal{O}^s$, and so $\rho^{-1}\iota \in G^h$. Whence the restrictions of $\rho$ and $\iota$ to $K^h$ must be equal.

Conversely, suppose that $(K_0, \mathcal{O}_0)$ is a valued extension of $(K, \mathcal{O})$ satisfying conditions (1) and (2) above. From (2) and Corollary 4.1.5 it follows that $K_0$ is a separable extension of $K$. Now, from (1) one gets $G(K^s/K_0) \subseteq G^h(\mathcal{O}_0^s)$, where $\mathcal{O}_0^s$ is the unique extension of $\mathcal{O}_0$ to $K^s$. Hence $K^h(\mathcal{O}_0^s) \subseteq K_0$, and $(K^h(\mathcal{O}_0^s), \mathcal{O}_0^s \cap K^h(\mathcal{O}_0^s))$ is a henselian valued extension of $(K, \mathcal{O})$. Again (2) yields a unique $K$-embedding $\iota : (K_0, \mathcal{O}_0) \longrightarrow (K^h(\mathcal{O}_0^s), \mathcal{O}_0^s \cap K^h(\mathcal{O}_0^s))$.

Since the identity is a $K$-embedding $(K_0, \mathcal{O}_0) \longrightarrow (K_0, \mathcal{O}_0)$, it follows that $\iota = \mathrm{id}$ and $K_0 = K^h(\mathcal{O}_0^s)$. □

**Corollary 5.2.3.** *For any intermediate extension $K \subseteq L \subseteq K^s$, we have that $K^h(\mathcal{O}^s) \subseteq L$ if and only if $\mathcal{O}^s \cap L$ is henselian.*

For any separable extension $E$ of $K$ we see that

$$G^h(\mathcal{O}^s) \cap G(K^s/E) = \{\, \sigma \in G(K^s/E) \mid \sigma(\mathcal{O}^s) = \mathcal{O}^s \,\}$$

is the decomposition group of $\mathcal{O}^s$ over $E$. Therefore, taking $\mathcal{O}' = \mathcal{O}^s \cap E$, it follows from Galois theory that $(EK^h(\mathcal{O}^s), \mathcal{O}^s \cap EK^h(\mathcal{O}^s))$ is a henselization of $(E, \mathcal{O}')$. In particular, let us remark for further reference:

*Remark 5.2.4.* If $K \subseteq L \subseteq K^s$, it follows from the definition of the decomposition group that $(K^h L, \mathcal{O}^s \cap K^h L)$ is a henselization of $(L, \mathcal{O}^s \cap L)$. Hence for a finite separable extension $K(z)$ we obtain that $(K^h(z), \mathcal{O}^s \cap K^h(z))$ is a henselization of $(K(z), \mathcal{O}^s \cap K(z))$.

We next state one of the most important properties of the henselization.

**Theorem 5.2.5.** $(K^h, \mathcal{O}^h)$ *is an immediate extension of* $(K, \mathcal{O})$.

*Proof.* Let us write $\Gamma^h$ and $\Gamma$ for the value group of $\mathcal{O}^h$ and $\mathcal{O}$, respectively. As usual, $\overline{K^h}$ and $\overline{K}$ are the residue class fields of these valuation rings. Clearly

$$\Gamma^h = \bigcup_L \Gamma_L \quad \text{and} \quad \overline{K^h} = \bigcup_L \overline{L}\,,$$

where $L$ runs over all finite intermediate extensions $K \subseteq L \subseteq K^h$. It suffices to show that $(L, \mathcal{O}^h \cap L)$ is an immediate extension of $(K, \mathcal{O})$.

Let $N$ be the Galois closure of $L/K$. Then $L \subseteq N \cap K^h$. Clearly $N \cap K^h$ is the fixed field of the group of restrictions $\sigma|_N$ with $\sigma \in G^h(\mathcal{O}^s)$. This group clearly is contained in the group

$$H = \{\, \tau \in G(N/K) \mid \tau(\mathcal{O}^h \cap N) = \mathcal{O}^h \cap N \,\}\,.$$

Conversely, every $\tau \in H$ extends to some $\sigma \in G^h(\mathcal{O}^s)$. In fact, let $\sigma'$ be any extension of $\tau$ to $K^s$. Then the valuation rings $\mathcal{O}^s$ and $\sigma'(\mathcal{O}^s)$ both extend $\mathcal{O}^s \cap N$. Thus by the Conjugation Theorem 3.2.15 there exists $\varrho \in G(K^s/N)$

such that $\varrho(\sigma'(\mathcal{O}^s)) = \mathcal{O}^s$. Hence $\sigma = \varrho \circ \sigma'$ lies in $G^h(\mathcal{O}^s)$ and restricts to $\tau$ on $N$.

Now by Lemma 3.3.1 the fixed field $N \cap K^h$ of $H$ is an immediate extension of $(K, \mathcal{O})$. □

Keeping notations as above, we know from Theorem 3.2.11 that the residue class field $\overline{K^s}$ of $\mathcal{O}^s$ is the algebraic closure of the residue class field $\overline{K}$ of $\mathcal{O}^h$. (Observe that in general $\overline{K^s} \neq \overline{K}^s$.) Moreover, every $\sigma \in G^h$ (the Galois group of $K^h$) induces $\overline{\sigma} \in G\big(\overline{K^s}/\overline{K}\big)$ by Proposition 3.2.16 (3). Let us write $\phi : G^h \longrightarrow G\big(\overline{K^s}/\overline{K}\big)$ for the map $\sigma \mapsto \overline{\sigma}$. Note that $G\big(\overline{K^s}/\overline{K}\big) = G\big(\overline{K}^s/\overline{K}\big)$, as $\overline{K^s}$ is purely inseparable over $\overline{K}^s$.

**Lemma 5.2.6.** *$\phi$ is a continuous homomorphism, and thus its kernel $G^t(\mathcal{O}^s)$ is a closed subgroup of $G^h$. Moreover,*

*(1) $\phi$ is surjective;*
*(2) if $\mathcal{O}_1^s$ is another prolongation of $\mathcal{O}$ to $K^s$, then $G^t(\mathcal{O}_1^s)$ is $K$-conjugate to $G^t(\mathcal{O}^s)$.*

*Proof.* It clearly follows from the construction that $\overline{\sigma\tau} = \overline{\sigma}\,\overline{\tau}$ for all $\sigma, \tau \in G^h$. Thus $\phi$ is a group homomorphism.

To prove the continuity of $\phi$ it suffices to show that for every finite Galois extension $\overline{K} \subseteq \kappa \subseteq \overline{K}^s$, there exists a finite normal extension $K \subseteq N \subseteq K^s$ such that $\mathcal{O}^s \cap N$ has a residue class field $\overline{N}$ satisfying $\kappa \subseteq \overline{N}$. In fact, translating these conditions to the profinite group language, we have that

$$\phi(G(K^s/N) \cap G^h) \subseteq G\big(\overline{K}^s/\overline{N}\big) \subseteq G\big(\overline{K}^s/\kappa\big) \ .$$

This expresses continuity of $\phi$ at the identity id, from which the continuity of the map follows.

Now $N$ can simply be taken as the Galois closure of the extension $K(x)/K$, where $x$ is chosen from $\mathcal{O}^s$ such that $\kappa = \overline{K}(\overline{x})$. Then clearly the residue class field $\overline{N}$ contains $\kappa$.

In order to prove (1), let us write

$$G\big(\overline{K}^s/\overline{K}\big) = \varprojlim G\big(\kappa_i/\overline{K}\big) \ ,$$

with $\kappa_i$ running through all finite intermediate Galois extensions $\overline{K} \subseteq \kappa_i \subseteq \overline{K}^s$. Denote by $\Theta_i : G\big(\overline{K}^s/\overline{K}\big) \longrightarrow G\big(\kappa_i/\overline{K}\big)$ the canonical map of the inverse limit (cf. Lemma 5.1.1). Observe that $\Theta_i$ is surjective for every $i$. Actually, $\Theta_i(\rho)$ is the restriction of $\rho$ to $\kappa_i$.

According to Lemma 5.1.1, in order to show that $\phi$ is surjective, we have to prove that the composition $\Theta_i \circ \phi : G^h \longrightarrow G\big(\kappa_i/\overline{K}\big)$ is surjective, for every $i$. To this end, take any $\rho \in G\big(\kappa_i/\overline{K}\big)$, where $\kappa_i$ is a finite Galois extension of $\overline{K}$. Write $\kappa_i = \overline{K}(\overline{x})$ for some $x \in \mathcal{O}^s$. Take the set $x_1, \ldots, x_n \in K^s$ of all elements conjugate to $x$ over $K^h$. There exists $j$ such that $1 \leq j \leq n$ and $\overline{x_j} = \rho(\overline{x})$.

Moreover, $x_j = \sigma(x)$ for some $\sigma \in G^h$. Thus $\overline{\sigma}(\overline{x}) = \rho(\overline{x})$. Consequently, $\overline{\sigma}$ and $\rho$ coincides on $\kappa_i$, which already means that $\Theta_i \circ \phi(\sigma) = \rho$. Thus $\Theta_i \circ \phi$ is surjective for every $i$, as contended.

The proof of statement (2) is a direct consequence of the Conjugation Theorem 3.2.15. □

The subgroup $G^t(\mathcal{O}^s)$ of $G(K^s/K)$ (or just $G^t$ if the valuation ring $\mathcal{O}^s$ is clear in the context) is called the *inertia group*[1] of $\mathcal{O}^s$ over $K$. Set $K^t(\mathcal{O}^s)$ for the fixed field of $G^t(\mathcal{O}^s)$. Then by Galois theory we have $G(K^s/K^t(\mathcal{O}^s)) = G^t(\mathcal{O}^s)$. The field $K^t(\mathcal{O}^s)$ (or just $K^t$) is called the *inertia field* of $\mathcal{O}^s$ over $K$. Since $G^t$ is a normal subgroup (recall that $G^t$ is the kernel of the group homomorphism $\phi$) of $G^h$ it follows that $K^t$ is a Galois extension of $K^h$. Lemma 5.2.6 in particular expresses the exactness of the sequence

$$1 \longrightarrow G^t \longrightarrow G^h \longrightarrow G\big(\overline{K}^s/\overline{K}\big) \longrightarrow 1 \,,$$

called earlier the *first exact sequence*.

Next we shall prove the main properties of inertia fields, as promised in the introduction of the chapter.

**Theorem 5.2.7.** *Let $(K, \mathcal{O})$ be a henselian valued field, and denote by $\mathcal{O}^s$ the unique extension of $\mathcal{O}$ to $K^s$. Let $G^t$ and $K^t$ be respectively the inertia group and the inertia field of $\mathcal{O}^s$ over $K$. As usual, $\Gamma$ and $\overline{K}$ stand for the value group and the residue class field of $\mathcal{O}$, respectively.*

(1) *The extension $\mathcal{O}^t = \mathcal{O}^s \cap K^t$ of $\mathcal{O}$ to $K^t$ has value group $\Gamma$ and residue class field $\overline{K}^s$, the separable closure of $\overline{K}$.*
(2) *$K^t$ is a Galois extension of $K$ and the Galois group $G(K^t/K)$ is topologically isomorphic to $G\big(\overline{K}^s/\overline{K}\big)$. Consequently, there exists an inclusion-preserving bijective correspondence between the set of all intermediate extensions $K \subseteq L \subseteq K^t$ and the set of all separable extensions $\kappa$ of $\overline{K}$ (inside $\overline{K}^s$). $\kappa/\overline{K}$ is a Galois extension if and only if $L/K$ is Galois. Moreover, $\kappa$ is the residue class field of $\mathcal{O}^s \cap L$.*
(3) *If $K \subseteq L \subseteq N \subseteq K^t$ are extensions of $K$ with $[N : L]$ finite, then $f(\mathcal{O}^s \cap N/\mathcal{O}^s \cap L) = [N : L]$ and $e(\mathcal{O}^s \cap N/\mathcal{O}^s \cap L) = 1$.*
(4) *Let $\mathcal{M}^s$ denote the maximal ideal of $\mathcal{O}^s$. Then*

$$G^t = \{\, \sigma \in G(K^s/K) \mid \sigma(x) - x \in \mathcal{M}^s \text{ for every } x \in \mathcal{O}^s \,\} \,.$$

*Proof.* (2) follows from Lemma 5.2.6. In fact, the continuity of $\phi$ implies that its kernel $G^t$ is a closed subgroup of $G(K^s/K)$. Hence $G^t$ is the Galois group of $K^t$. So $K^t$ is a Galois extension of $K$ and $G(K^t/K)$ is topologically isomorphic to $G(K^s/K)/G^t$. Let us denote by $\overline{K^t}$ the residue class field of $\mathcal{O}^t$. By Proposition 3.2.16 (2), $\overline{K^t}$ is a normal extension of $\overline{K}$, and Lemma 5.2.6 implies that $G(K^t/K)$ is topologically isomorphic to $G\big(\overline{K^t}/\overline{K}\big)$. Hence the

[1] The letter $t$ stands for the German word "träge".

correspondence between the sets of intermediate fields $K \subseteq L \subseteq K^t$ and $\overline{K} \subseteq \kappa \subseteq \overline{K^t}$ with $\kappa/\overline{K}$ separable follows from Galois theory as well as the statement concerning normality. To see the last statement observe that $K^t$ is also the inertia field of $\mathcal{O}^s$ over any intermediate extension $K \subseteq L \subseteq K^t$. Therefore, if $\mathcal{O}^s \cap L$ has residue class field $\kappa$, then $G(K^t/L) \cong G\big(\overline{K^t}/\kappa\big)$, by what we have just seen.

(1) Now let $\kappa$ be the separable closure of $\overline{K}$ inside $\overline{K^t}$. By the last item there exists an intermediate field $L$ such that $\kappa$ is the residue class field of $\mathcal{O}^s \cap L$ and $G(K^t/L) \cong G\big(\overline{K^t}/\kappa\big)$. Therefore, since the choice of $\kappa$ implies that $G\big(\overline{K^t}/\kappa\big)$ is trivial, it follows that $L = K^t$ and so $\kappa = \overline{K^t}$. Hence $\overline{K^t}$ is a separable extension of $\overline{K}$ (In fact a Galois extension since we already know that it is a normal extension.) On the other hand, the restriction of $\phi : G(K^s/K) \longrightarrow G\big(\overline{K^s}/\overline{K}\big)$ to $G(K^s/K^t)$ corresponds to the map $G(K^s/K^t) \longrightarrow G\big(\overline{K^s}/\overline{K^t}\big)$ described in the previous Lemma 5.2.6, which is surjective. Therefore, since $G^t$ is the kernel of $\phi$ it follows that $G\big(\overline{K^s}/\overline{K^t}\big)$ is trivial. Thus $\overline{K^s}$ is a purely inseparable extension of $\overline{K^t}$. Since $\overline{K^s}$ is algebraically closed, it follows that $\overline{K^t}$ is separably closed, more precisely, the separable closure of $\overline{K}$, as required.

The fact that $\mathcal{O}^t$ has value group $\Gamma$ will follow from (3).

We now prove item (3). For any pair of extensions $L$ and $N$ of $K$ contained in $K^t$ such that $N$ is finite over $L$, the isomorphism of the last item shows that $(G(K^t/L) : G(K^t/N)) = \big(G\big(\overline{K}^s/\overline{L}\big) : G\big(\overline{K}^s/\overline{N}\big)\big)$, where $\overline{L}$ and $\overline{N}$ are the residue class fields of $\mathcal{O}^t \cap L$ and $\mathcal{O}^t \cap N$, respectively. Hence $[N : L] = \big[\overline{N} : \overline{L}\big]$, i.e., $f(\mathcal{O}^s \cap N/\mathcal{O}^s \cap L) = [N : L]$, as desired. The inequality $ef \leq [N : L]$ in Corollary 3.2.3 implies then $e(\mathcal{O}^s \cap N/\mathcal{O}^s \cap L) = 1$.

Now let $v^t$ be a valuation corresponding to $\mathcal{O}^t$. For the sake of obtaining a contradiction, suppose there exists $x \in K^t$ such that $v^t(x) \notin \Gamma$. For $N = K(x)$ we then cannot have $e(\mathcal{O}^s \cap N/\mathcal{O}) = 1$, a contradiction.

(4) Let $\sigma \in G(K^s/K)$, and assume $\sigma(x) - x \in \mathcal{M}^s$ for all $x \in \mathcal{O}^s$. Then clearly $\sigma(\mathcal{O}^s) \subseteq \mathcal{O}^s$. Hence $\sigma \in G^h$. Now, for any $\tau \in G^h$ we have $\tau \in G^t$ if and only if $\overline{\tau(x)} = \overline{\tau}(\overline{x}) = \overline{x}$, i.e.,$\overline{\tau(x) - x} = \overline{0}$, for every $x \in \mathcal{O}^s$. This proves (4). □

*Remark 5.2.8.* From the last condition (4) of the above Theorem 5.2.7 we see that if $K \subseteq L \subseteq K^s$, then $G^t \cap G(K^s/L)$ is the inertia group of $\mathcal{O}^s$ over $L$. It then follows from Galois theory that $K^t L$ is the inertia field of $\mathcal{O}^s$ over $L$. As was true for decomposition fields, we also have:

For a finite separable extension $K(z)$ of $K$, the inertia field of $\mathcal{O}^s$ over $K(z)$ is $K^t(z)$.

Let $(K_2, \mathcal{O}_2)$ be a valued extension of $(K_1, \mathcal{O}_1)$. The equation $[K_2 : K_1] = f(\mathcal{O}_2/\mathcal{O}_1)$ means that for any pair $E, L$ with $K_1 \subseteq E \subseteq L \subseteq K_2$ and $L/E$ finite, the equation $[L : E] = \big[\overline{L} : \overline{E}\big]$ holds, where $\overline{L}$ and $\overline{E}$ are the residue class fields of $\mathcal{O}_2 \cap L$ and $\mathcal{O}_2 \cap E$, respectively.

**Theorem 5.2.9.** *For a valued field $(K, \mathcal{O})$, let $\mathcal{O}^s$ be an extension of $\mathcal{O}$ to $K^s$. Denote respectively by $K^h$ and $K^t$ the henselization and the inertia field*

*of $\mathcal{O}^s$ over $K$. For an intermediate extension $K^h \subseteq L \subseteq K^s$, let $\overline{L}$ be the residue class field of $\mathcal{O}^s \cap L$.*

*(1) If $\overline{L}$ is a separable extension of $\overline{K}$ and $[L : K^h] = \big[\overline{L} : \overline{K}\big]$, then $L \subseteq K^t$.*
*(2) $K^t \subseteq L$ if and only if the residue class field $\overline{K^s}$ of $\mathcal{O}^s$ is a purely inseparable extension of $\overline{L}$.*

*Proof.* (1) Set $\mathcal{O}^h = \mathcal{O}^s \cap K^h$. For any finite intermediate extension $K^h \subseteq E \subseteq L$, let $\mathcal{O}' = \mathcal{O}^s \cap E$, with residue class field $\overline{E}$. There exists $\alpha \in \overline{L}$ such that $\overline{E} = \overline{K}(\alpha)$. Let $f(X) \in \mathcal{O}^h[X]$ be a monic polynomial such that $\overline{f}$ is the minimal polynomial of $\alpha$ over $\overline{K}$. Since $\overline{f}$ has a simple root in $\overline{E}$ and $\mathcal{O}^s \cap E$ is henselian, $f$ has a root $u$ in $E$. The irreducibility of $\overline{f}$ implies that $f$ is irreducible, too. Consequently $[E : K^h] \geq [K^h(u) : K^h] = \deg f = \big[\overline{E} : \overline{K}\big]$. Since by assumption $\big[\overline{E} : \overline{K}\big] = [E : K^h]$, it follows that $E = K^h(u)$.

On the other hand, if $\kappa \subseteq \overline{K}^s$ is a Galois extension of $\overline{K}$ such that $\alpha \in \kappa$, then (2) of Theorem 5.2.7 implies that there exists $F \subseteq K^t$, a Galois extension of $K^h$, such that $\mathcal{O}^s \cap F$ has residue class field $\kappa$. Since $\mathcal{O}^s \cap F$ is henselian and $\overline{f}$ has a simple root in $\kappa$, it follows that $f$ has a root in $F$. As $f$ is irreducible and $F/K$ is a normal extension, we have that $f$ has all its roots in $F$. In particular, $u \in F$ and so $E = K^h(u) \subseteq K^t$. We therefore conclude that any finite extension $E/K^h$ contained in $L$ is also contained in $K^t$. Thus $L \subseteq K^t$ as contended.

(2) One side of the equivalence follows immediately from Theorem 5.2.7 (1). Let then $L$ be an extension of $K^h$ such that $\overline{K^s}$ is purely inseparable over $\overline{L}$. Observe that $\mathcal{O}^s \cap L$ is henselian because $K^h \subseteq L$. The hypothesis on the residue class fields implies that $G(K^s/L)$ is the inertia group of $\mathcal{O}^s$ over $L$, since the map $G(K^s/L) \longrightarrow G\big(\overline{K^s}/\overline{L}\big) = \{\mathrm{id}\}$ is constant. Therefore, by (4) of Theorem 5.2.7, we have

$$G(K^s/L) = \{\, \sigma \in G(K^s/L) \mid \sigma(x) - x \in \mathcal{M}^s \text{ for every } x \in \mathcal{O}^s \,\} \subseteq G^t$$

and the statement follows from Galois theory. □

## 5.3 Ramified Extensions – Second Exact Sequence

In the next step we shall enlarge $K^t$ towards $K^s$ by adding finite extensions $L$ of $K^t$ for which $[L : K^t]$ equals the ramification index. This will be done by the following construction: if $\sigma(\mathcal{O}^s) = \mathcal{O}^s$, it follows for all $x \in (K^s)^\times$ that $x$ and $\sigma(x)$ have the same value (Lemma 3.2.16 (1)). Hence

$$\frac{\sigma(x)}{x} \in (\mathcal{O}^s)^\times \text{ and the map } x \mapsto \overline{\frac{\sigma(x)}{x}}$$

from $(K^s)^\times$ into $(\overline{K^s})^\times$ is a group homomorphism.

As we shall see below, the map above induces a homomorphism $\psi : G^t \longrightarrow \mathrm{Hom}\big(\Delta/\Gamma, \big(\overline{K}^s\big)^\times\big)$, where $\Delta$ and $\Gamma$ are respectively the value groups of $\mathcal{O}^s$

and $\mathcal{O}^t = \mathcal{O}^s \cap K^t$. In fact, if $v^s : K^s \longrightarrow\!\!\!\!\!\rightarrow \Delta \cup \{\infty\}$ and $v^t : K^t \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ are the corresponding valuations, then for $\sigma \in G^t$ and $\delta \in \Delta$ we may define

$$\psi(\sigma)(\delta + \Gamma) = \overline{\frac{\sigma(x)}{x}} \ ,$$

where $x \in (K^s)^\times$ satisfies $v^s(x) = \delta$.

**Lemma 5.3.1.** *For every $\sigma \in G^t$, $\psi(\sigma)$ is a well defined group homomorphism. Moreover, $\psi$ is also a group homomorphism and for every $\delta \in \Delta$, $\psi(\sigma)(\delta + \Gamma)$ is a root of unity which has order not divisible by the characteristic of $\overline{K^s}$.*

*Proof.* To see that $\psi(\sigma)$ is well defined, observe that if $x, y \in (K^s)^\times$ satisfy $v^s(x) = v^s(y) + v^s(z)$ for some $z \in (K^t)^\times$, then $x = yzu$ for some $u \in (\mathcal{O}^s)^\times$. From $\sigma(z) = z$ and (4) of Theorem 5.2.7 we obtain

$$\overline{\frac{\sigma(u)}{u}} = 1, \text{ and hence } \overline{\frac{\sigma(x)}{x}} = \overline{\frac{\sigma(y)}{y}} \ ,$$

which shows that $\psi(\sigma)(\delta + \Gamma)$ does not depend on the representative of the class $\delta + \Gamma$. Clearly, $\psi(\sigma)$ is a group homomorphism.

We next show that $\psi$ is a group homomorphism. For $\sigma, \tau \in G^t$ and $x \in (K^s)^\times$, one has

$$\frac{\sigma\tau(x)}{x} = \frac{\sigma(\tau(x))}{\sigma(x)} \frac{\sigma(x)}{x} \ ,$$

and by Theorem 5.2.7 (4),

$$\sigma\left(\frac{\tau(x)}{x}\right) - \frac{\tau(x)}{x} \in \mathcal{M}^s \ .$$

Hence

$$\overline{\frac{\sigma\tau(x)}{x}} = \overline{\frac{\tau(x)}{x}}\,\overline{\frac{\sigma(x)}{x}} \ ,$$

for every $x \in (K^s)^\times$. It follows from this that $\psi$ is a group homomorphism, as desired.

Finally, let $\Omega$ be the group of all roots of unity lying in $\overline{K^s}$. Since $\Omega$ consists of the set of all elements of $(\overline{K^s})^\times$ having finite order and $\Delta/\Gamma$ is a torsion group, its homomorphic images in $(\overline{K^s})^\times$ are always contained in $\Omega$. Moreover, the order of each element of $\Omega$ is not divisible by the characteristic of $\overline{K^s}$. □

Observe that every element of $\Delta/\Gamma$ of $p$-power order lies in the kernel of each element of $\mathrm{Hom}\big(\Delta/\Gamma, \big(\overline{K^s}\big)^\times\big)$ in case $\mathrm{char}\,\overline{K} = p$. On the other hand, the above lemma shows that we actually have $\psi : G^t \longrightarrow \mathrm{Hom}(\Delta/\Gamma, \Omega)$, where $\Omega$ is isomorphic to the subgroup of the additive group $\mathbb{Q}/\mathbb{Z}$ consisting

of those elements having order not divisible by $p$. The group $\mathrm{Hom}(\Delta/\Gamma, \Omega)$ is usually called the *$p$-character group* of $\Delta/\Gamma$.

It is well known that $\mathrm{Hom}(-, \Omega)$ is a *left-exact contravariant functor* in the category of abelian groups. I.e., for a short exact sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

of abelian groups, we get the exact sequence

$$0 \longrightarrow \mathrm{Hom}(C, \Omega) \xrightarrow{g^*} \mathrm{Hom}(B, \Omega) \xrightarrow{f^*} \mathrm{Hom}(A, \Omega) \ ,$$

where $g^*$ is given by $g^*(\chi) = \chi \circ g$, and analogously for $f^*$ [26, Theorem 10.3]. Moreover, since $\Omega$ is a divisible abelian group, $f^*$ is also surjective [26, Theorem 10.6]; $\mathrm{Hom}(-, \Omega)$ is then called an *exact functor*. The strong property of $\mathrm{Hom}(-, \Omega)$ being an exact functor will be very useful. In particular, it implies that $\mathrm{Hom}(A, \Omega)$ is a profinite group for every abelian torsion group $A$. Let us see this for our group $\Delta/\Gamma$.

For any pair of finite subgroups $\Lambda_1/\Gamma$, $\Lambda_2/\Gamma \subseteq \Delta/\Gamma$, there exists a third finite subgroup $\Lambda_3/\Gamma$ which contains both, $\Lambda_1/\Gamma$ and $\Lambda_2/\Gamma$. Hence the union of all finite subgroups of $\Delta/\Gamma$ is also a subgroup of $\Delta/\Gamma$. Moreover, as $\Delta/\Gamma$ is a torsion group, every $a \in \Delta/\Gamma$ is contained in some finite subgroup of $\Delta/\Gamma$. Hence $\Delta/\Gamma$ is in fact the union of all its finite subgroups. We express this fact by writing

$$\Delta/\Gamma = \varinjlim \Delta'/\Gamma \quad \text{and saying that } \Delta/\Gamma \text{ is a "direct limit"} \ ,$$

where $\Delta'$ is a subgroup of $\Delta$ containing $\Gamma$, and such that $\Delta'/\Gamma$ is finite. From the categorical properties of the functor $\mathrm{Hom}(-, \Omega)$ (it inverts arrows and it interchanges surjectivity and injectivity) we get an isomorphism of groups

$$\mathrm{Hom}(\Delta/\Gamma, \Omega) = \mathrm{Hom}\left(\varinjlim \Delta'/\Gamma, \Omega\right) \cong \varprojlim \mathrm{Hom}(\Delta'/\Gamma, \Omega) \ .$$

Since for each finite $\Delta'/\Gamma$ we have that $\mathrm{Hom}(\Delta'/\Gamma, \Omega)$ is also a finite group, $\mathrm{Hom}(\Delta/\Gamma, \Omega)$ is a profinite group as claimed above.

**Lemma 5.3.2.** *$\psi$ is a continuous homomorphism, and its kernel $G^v(\mathcal{O}^s)$ is a closed normal subgroup of $G^t(\mathcal{O}^s)$ which can be characterized as follows:*

$$G^v(\mathcal{O}^s) = \left\{ \sigma \in G(K^s/K) \;\middle|\; \frac{\sigma(x)}{x} - 1 \in \mathcal{M}^s \ \textit{for all } x \in (K^s)^\times \right\} \ ,$$

*where $\mathcal{M}^s$ is the maximal ideal of $\mathcal{O}^s$.*

*Proof.* To prove continuity of $\psi$ we have to show that if $\Delta'/\Gamma$ is a finite subgroup of $\Delta/\Gamma$, then there exists a finite intermediate extension $K^t \subseteq L \subseteq K^s$ such that $\Delta' \subseteq v^s(L^\times)$ and $\psi(\sigma)(v^s(L^\times)/\Gamma) = \{1\}$. In order to construct

$L$, pick $x_1, \ldots, x_m \in K^s$ such that $\Delta'/\Gamma = \{v^s(x_1)+\Gamma, \ldots, v^s(x_m)+\Gamma\}$, and let $L$ be a finite Galois extension of $K^t$ containing $K^t(x_1, \ldots, x_m)$. Observe that

$$\overline{\frac{\sigma(x)}{x}} = 1$$

for any $x \in L^\times$ and any $\sigma \in G(K^s/L)$, because $\sigma(x) = x$. Hence $\psi(\sigma)(\delta+\Gamma) = 1$ for $\delta \in v^s(L^\times)$ and $\sigma \in G(K^s/L)$. Since $\Delta' \subseteq v^s(L^\times)$ by construction, the continuity is proved.

To prove the second statement of the lemma, take $\sigma \in G(K^s/K)$ such that for every $x \in (K^s)^\times$ there exists some $y_x \in \mathcal{M}^s$ satisfying

$$\frac{\sigma(x)}{x} - 1 = y_x \ .$$

Then for $x \in \mathcal{O}^s$ it follows that $\sigma(x) = x + xy_x \in \mathcal{O}^s$. Consequently $\sigma \in G^h(\mathcal{O}^s)$. Moreover, for $x \in \mathcal{O}^s$ we also have $\sigma(x) - x \in \mathcal{M}^s$. Thus, according to Theorem 5.2.7 (4), $\sigma \in G^t(\mathcal{O}^s)$. Finally, the condition

$$\frac{\sigma(x)}{x} - 1 \in \mathcal{M}^s$$

for all $x \in (K^s)^\times$ implies that $\sigma \in \ker(\psi)$, as desired.

Conversely, $\sigma \in \ker(\psi)$ implies that

$$\overline{\frac{\sigma(x)}{x}} = 1 \ ,$$

for every $x \in (K^s)^\times$, completing the proof. □

The subgroup $G^v(\mathcal{O}^s)$ (or $G^v$ for short) is called the *ramification group*[2] of $\mathcal{O}^s$ over $K$. Set $K^v(\mathcal{O}^s)$ for the fixed field of $G^v(\mathcal{O}^s)$. From Galois theory we have $G(K^s/K^t(\mathcal{O}^s)) = G^v(\mathcal{O}^s)$. The field $K^v(\mathcal{O}^s)$ (or just $K^v$) is called the *ramification field* of $\mathcal{O}^s$ over $K$. Since $G^v$ is a normal subgroup of $G^t$, it follows that $K^v$ is a Galois extension of $K^t$.

Lemma 5.3.2 together with the surjectivity of $\psi$, proved in Theorem 3.3.3 (3) below, expresses the exactness of the *second exact sequence*

$$1 \longrightarrow G^v \longrightarrow G^t \xrightarrow{\psi} \mathrm{Hom}(\Delta/\Gamma, \Omega) \longrightarrow 1 \ .$$

Before we state the main properties of the ramification field let us introduce one more notation. Denote by $(\Delta/\Gamma)_p$ the subgroup consisting of those elements of $\Delta/\Gamma$ having order prime to $p$, the characteristic of $\overline{K}$. If we write $\Delta'$ for the *p-component* of $\Delta/\Gamma$ (i.e., the group of all elements of $\Delta/\Gamma$ having order a power of $p$), then $\Delta/\Gamma = (\Delta/\Gamma)_p \oplus \Delta'$ and every character $\chi \in \mathrm{Hom}(\Delta/\Gamma, \Omega)$ is trivial on $\Delta'$. Hence we may consider $\chi$ as a homomorphism on $(\Delta/\Gamma)_p$.

[2] The letter $v$ stands for the German word "verzweigt".

On the other hand, one also concludes that $K^v/K^t$ is an abelian extension since $G^t/G^v$ is isomorphic to a closed subgroup of $\mathrm{Hom}(\Delta/\Gamma, \Omega)$. In order to prepare for stating the main properties of $G^v$ and $K^v$, let us describe $G^t/G^v$ more precisely. For any prime $q$ let $\Delta(q)$ be the subgroup of those elements $\delta \in \Delta$ such that $\delta + \Gamma \in \Delta/\Gamma$ has order a power of $q$. Let also $\Omega(q)$ be the $q$-component of $\Omega$, $q \neq p$. The decomposition of abelian groups in a direct sum of their $q$-components gives (note that $\Delta(q)/\Gamma$ is the $q$-component of $\Delta/\Gamma$)

$$\Delta/\Gamma = \bigoplus_q \Delta(q)/\Gamma, \quad \text{and} \quad \Omega = \bigoplus_{q \neq p} \Omega(q) \ .$$

The functor $\mathrm{Hom}(-, \Omega)$ has one more important property which we shall use now. $\mathrm{Hom}(-, \Omega)$ is an "additive" functor ([26, Theorems 10.7 and 10.8]):

$$\mathrm{Hom}(\Delta/\Gamma, \Omega) = \prod_{q \neq p} \mathrm{Hom}(\Delta(q)/\Gamma, \Omega(q)) \ .$$

For any $q \neq p$, let $r_q$ be the $\mathbb{F}_q$-dimension of $\Gamma/q\Gamma$. Since $\Delta$ is the divisible hull of $\Gamma$ (by Theorem 3.2.4 (1) and Theorem 3.2.11), it follows that

$$\Delta(q)/\Gamma \cong \bigoplus_{i=1}^{r_q} (\mathbb{Q}/\mathbb{Z})(q)\gamma_i \ ,$$

choosing $\gamma_i \in \Delta(q)$ suitably. Using again that $\mathrm{Hom}(-, \Omega)$ is additive, we get

$$\mathrm{Hom}(\Delta(q)/\Gamma, \Omega(q)) \cong \prod_{i=1}^{r_q} \mathbb{Z}_q \chi_i \cong \mathbb{Z}_q^{r_q} \ ,$$

where $\chi_i$ is taken as the dual $\mathbb{F}_q$-basis of $\gamma_i$. Thus $G^v/G^t$ is isomorphic to a subgroup of

$$\prod_{q \neq p} \mathbb{Z}_q^{r_q} \ .$$

Consequently the index $(G^t : G^v)$ is not divisible by $p$ (as a supernatural number).

**Theorem 5.3.3.** *Let $(K, \mathcal{O})$ be a valued field and fix an extension $\mathcal{O}^s$ of $\mathcal{O}$ to $K^s$. Let $G^h$, $G^t$, and $G^v$ be the decomposition group, the inertia group, and the ramification group of $\mathcal{O}^s$ over $K$. Set $K^h$, $K^t$ and $K^v$ for their fixed fields. As usual, $\Gamma$ and $\overline{K}$ stand for the value group and the residue class field of $\mathcal{O}$, respectively. With the above notations it follows that:*

*(1) $G^v$ is the (unique) $p$-Sylow subgroup of $G^t$, where $p = \mathrm{char}\ \overline{K}$ ($G^v$ is trivial when $p = 0$).*
*(2) $G^v$ is a normal subgroup of $G^h$. Consequently $K^v$ is a Galois extension of $K^h$.*

*(3) $\psi$ is surjective and*

$$G^t/G^v \cong \prod_{q \neq p} \mathbb{Z}_q^{r_q}$$

*as profinite groups, where for each prime $q \neq p$, $r_q$ is the $\mathbb{F}_q$-dimension of $\Gamma/q\Gamma$; $r_q$ is called the q-rank of $\Gamma$.*

*(4) The residue class field of $\mathcal{O}^s \cap K^v$ equals the residue class field of $\mathcal{O}^s \cap K^t$, and the value group $\Gamma^v$ satisfies $\Gamma^v/\Gamma = (\Delta/\Gamma)_p$.*

*(5) If $K^t \subseteq L \subseteq N \subseteq K^v$ are extensions of $K^t$ with $[N : L]$ finite, then $e(\mathcal{O}^s \cap N/\mathcal{O}^s \cap L) = [N : L]$ and $f(\mathcal{O}^s \cap N/\mathcal{O}^s \cap L) = 1$.*

*(6) Given an intermediate extension $K^t \subseteq L \subseteq K^v$, let $\Gamma_L$ be the value group of $\mathcal{O}^s \cap L$. The map $L \longmapsto \Gamma_L$ is a bijective inclusion-preserving correspondence between the set of all subextensions of $K^v/K^t$ and the set of totally ordered groups between $\Gamma$ and $\Gamma^v$.*

*Proof.* (1) As we remarked just before Theorem 5.3.3, the index $(G^t : G^v)$ is not divisible by $p$. Consequently, it remains to show that $G^v$ is a pro-$p$ group. For further use we shall prove this in a more general form.

**Lemma 5.3.4.** *Let $(N, \mathcal{O}_2)$ be an extension of $(L, \mathcal{O}_1)$ with $N$ Galois over $L$. Suppose that for every $\sigma \in G(N/L)$ and any $x \in N^\times$ we have that*

$$\frac{\sigma(x)}{x} - 1 \in \mathcal{M}_2 \ ,$$

*where $\mathcal{M}_2$ is the maximal ideal of $\mathcal{O}_2$. Let $\overline{L}$ be the residue class field of $\mathcal{O}_1$ and $p = \operatorname{char} \overline{L}$. Then $G(N/L)$ is a pro-p group ($G(N/L)$ is trivial in case $\operatorname{char} \overline{L} = 0$).*

*Proof.* Suppose $G(N/L)$ is not a pro-$p$ group, and take $q \neq p$, a prime divisor of the order of $G(N/L)$. Thus there exist extensions $L \subseteq E \subseteq F \subseteq N$ such that $F$ is a Galois extension of $E$ of degree $q$. Let $F = E(x)$ for some $x \in N$. Replacing $x$ by $y = qx - T(x)$ if necessary, we may assume that $T(x) = 0$. Here $T : F \to E$ denotes the trace map.

Next take $\sigma \in G(N/L)$ whose restriction to $F$ generates the group $G(F/E)$. Then

$$\overline{\frac{\sigma(x)}{x}} = 1, \ \overline{\frac{\sigma^2(x)}{x}} = 1, \ \ldots, \ \overline{\frac{\sigma^{q-1}(x)}{x}} = 1 \ .$$

Thus

$$0 = \overline{\frac{T(x)}{x}} = \overline{\frac{\sigma^0(x) + \sigma(x) + \cdots + \sigma^{q-1}(x)}{x}} = \overline{\frac{\sigma^0(x)}{x}} + \overline{\frac{\sigma(x)}{x}} + \cdots + \overline{\frac{\sigma^{q-1}(x)}{x}} = \overline{q},$$

contradicting $q \neq p = \operatorname{char} \overline{K}$, (or $\overline{q} \neq 0$ in case $\operatorname{char} \overline{L} = 0$). □

Back to Theorem 5.3.3, we see that (1) follows from Lemma 5.3.4.
(2) For any $\sigma \in G^v$, $\tau \in G^h$ and $x \in (K^s)^\times$,

$$\frac{\tau^{-1}\sigma\tau(x)}{x} = \tau^{-1}\left(\frac{\sigma\tau(x)}{\tau(x)}\right) .$$

Now, from

$$\overline{\frac{\sigma(\tau(x))}{\tau(x)}} = 1 \text{ and } \overline{\tau^{-1}\left(\frac{\sigma(\tau(x))}{\tau(x)}\right)} = \overline{\tau^{-1}}\left(\overline{\frac{\sigma(\tau(x))}{\tau(x)}}\right)$$

it follows that

$$\overline{\frac{\tau^{-1}\sigma\tau(x)}{x}} = 1 .$$

Hence $\tau^{-1}\sigma\tau \in G^v$ by Lemma 5.3.2 and so $G^v$ is a normal subgroup of $G^h$, as desired.

We continue the proof with the following construction: Let $\Gamma \subseteq \Delta' \subseteq \Delta$ be a subgroup such that $\Delta'/\Gamma = \{\, \delta_1 + \Gamma, \ldots, \delta_n + \Gamma \,\}$ is finite. Pick $x_1, \ldots, x_n \in K^s$ satisfying $v^s(x_i) = \delta_i$ for every $1 \le i \le n$ and set $N$ for a finite Galois extension of $K^t$ containing $K^t(x_1, \ldots, x_n)$. For $L = N \cap K^v$ we write $\mathcal{O}' = \mathcal{O}^s \cap L$ and $v' = v^s|_L$. Let $\Gamma' = v'(L^\times)$ be the value group of $\mathcal{O}'$. Then $\Gamma'/\Gamma$ is finite subgroup of $\Delta/\Gamma$. Since the absolute Galois group of $L$, $G_L = G(K^s/L)$, is a subgroup of $G^t$, Theorem 5.2.7 (4) implies that $G_L$ is the inertia group of $\mathcal{O}^s$ over $L$. Let $\psi_L$ be the map corresponding to $L$, as described in Lemma 5.3.1, and consider the following diagram,

$$\begin{array}{ccc}
1 & & 0 \\
\downarrow & & \downarrow \\
G_L & \xrightarrow{\psi_L} & \mathrm{Hom}(\Delta/\Gamma', \Omega) \\
\downarrow & & \downarrow \Theta \\
G^t & \xrightarrow{\psi} & \mathrm{Hom}(\Delta/\Gamma, \Omega) \\
\pi \downarrow & & \downarrow \Theta' \\
G^t/G_L & \xrightarrow{\psi'} & \mathrm{Hom}(\Gamma'/\Gamma, \Omega) \\
\downarrow & & \downarrow \\
1 & & 0
\end{array} \tag{5.3.1}$$

where the upper map in the left column is the inclusion and $\pi$ is the canonical quotient map. The maps in the right column are induced by the maps which correspond to the inclusion and the quotient map in the following exact sequence

$$0 \longrightarrow \Gamma'/\Gamma \longrightarrow \Delta/\Gamma \longrightarrow \Delta/\Gamma' \longrightarrow 0 \,.$$

Moreover, all maps in the above diagram (5.3.1) are continuous, columns are exact sequences, and the upper square is commutative. Thus, $\psi$ induces $\psi'$ defined as:

$$\psi'(\pi(\sigma)) = \Theta'(\psi(\sigma))$$

for every $\pi(\sigma) \in G^t$. We shall prove first that $\psi'$ is an isomorphism in order to be able to deduce almost all the remaining statements in the theorem.

$\psi'$ is injective. Indeed, let $H$ be the kernel of $\psi'$. Since any $\pi(\sigma) \in H$ satisfies $\psi'(\pi(\sigma)) = 1$, the very definition of $\psi'$ implies that $\psi(\sigma)(\Gamma'/\Gamma) = 1$. Therefore, for any $x \in L^\times$ and $\gamma' = v'(x)$,

$$1 = \psi(\sigma)(\gamma' + \Gamma) = \frac{\overline{\sigma(x)}}{x} \,.$$

Whence, by Lemma 5.3.4, $H$ is a pro-$p$ group. Thus $H$ is trivial, since from $K^t \subseteq L \subseteq K^v$ it follows that $p$ does not divide $[L : K^t]$.

The injectivity of $\psi'$ implies that $|G^t/G_L| \leq |\operatorname{Hom}(\Gamma'/\Gamma, \Omega)|$. Next, since $\Gamma'/\Gamma$ is a finite group, it follows that $\Gamma'/\Gamma$ and $\operatorname{Hom}(\Gamma'/\Gamma, \Omega)$ have the same order. Thus $[L : K^t] = |G^t/G_L| \leq |\Gamma'/\Gamma| = e$. Since by Corollary 3.2.3, $e \leq [L : K^t]$, it follows that $|G^t/G_L| = |\operatorname{Hom}(\Gamma'/\Gamma, \Omega)|$ and so $\psi'$ has to be bijective, as desired.

Let us label what we have obtained so far.

*Remark 5.3.5.* Observe that $e(L/K^t) = [L : K^t]$ and $f(L/K^t) = 1$ for every finite intermediate extension $K^t \subseteq L \subseteq K^v$. Moreover, $p$ does not divide $|\Gamma'/\Gamma|$, where $\Gamma'$ is the value group of $L$.

We now prove (4) and (5). (4): Let $\overline{K}^s$ be the residue class field of $\mathcal{O}^s \cap K^t$. If $\overline{x} \notin \overline{K}^s$ for some $x \in K^v$, then $L = K^t(x)$ would be an intermediate extension for which $f \neq 1$, contradicting Remark 5.3.5 above. Similarly, if there exists $x \in K^v$ for which $v^s(x) + \Gamma$ has order properly divisible by $p$ in $\Delta/\Gamma$, $L = K^t(x)$ is an intermediate extension of $K^v/K^t$ for which the value group $\Gamma'$ of $\mathcal{O}^s \cap L$ satisfies: $|\Gamma'/\Gamma|$ is properly divisible by $p$. Since this cannot occur, we may conclude that every element in $\Gamma^v/\Gamma$ has order prime to $p$. Consequently $\Gamma^v/\Gamma \subseteq (\Delta/\Gamma)_p$.

To show that the inverse inclusion also holds, let $\delta \in \Delta$ such that $\delta + \Gamma$ has order $r$, relatively prime to $p$. Take $x \in K^s$ satisfying $v^s(x) = \delta$ and let $M/K^v$ be a finite Galois extension containing $K^v(x)$. According to (1), $G(M/K^v)$ is a $p$-group. Therefore, if $X^m + \cdots + a_m$ is the minimal polynomial of $x$ over $K^v$, then $m = p^\nu$ for some positive integer $\nu$. Remark 3.2.17 now implies that $p^\nu v^s(x) = v^s(a_m) \in \Gamma^v$. Now take $a, b \in \mathbb{Z}$ such that $1 = ar + bp^\nu$. Hence $\delta = (ar + bp^\nu)\delta \in \Gamma^v$ and so $\delta + \Gamma \in \Gamma^v/\Gamma$, as required.

(5): Consider $K^t \subseteq L \subseteq N \subseteq K^v$ with $[N : L]$ finite. By Remark 5.2.8, $L$ is already the inertia field of $\mathcal{O}^s$ over $L$. Thus, by Remark 5.3.5, $[N : L] = e$ and $f = 1$.

We now prove (3). As we remarked during the preparation for Theorem 5.3.3, $\mathrm{Hom}(\Delta/\Gamma, \Omega) = \mathrm{Hom}(\Gamma^v/\Gamma, \Omega)$, since by (4), $\Gamma^v/\Gamma = (\Delta/\Gamma)_p$. Let us next write

$$\mathrm{Hom}(\Gamma^v/\Gamma, \Omega) = \varprojlim \mathrm{Hom}(\Delta_i/\Gamma, \Omega) \ ,$$

with $\Gamma \subseteq \Delta_i \subseteq \Gamma^v$ and $\Delta_i/\Gamma$ finite. Denote by $\Theta_i : \mathrm{Hom}(\Gamma^v/\Gamma, \Omega) \longrightarrow \mathrm{Hom}(\Delta_i/\Gamma, \Omega)$ the canonical map of the inverse limit (cf. Lemma 5.1.1). Observe that $\Theta_i$ is surjective since it is induced by the inclusion $\Delta_i/\Gamma \hookrightarrow \Gamma^v/\Gamma$. From Lemma 5.1.1, it is enough to prove that the composition $\Theta_i \circ \psi$ is surjective for every $i$ in order to get that $\psi$ is surjective. To this end, recall our construction corresponding to the diagram (5.3.1) where now $\Delta_i \subseteq \Gamma^v$ plays the role of $\Delta'$. Keeping the notation used in this construction, we now have $L = N$ and so $\Delta_i/\Gamma \subseteq \Gamma'/\Gamma$. Consider next the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma'/\Gamma, \Omega) & \xrightarrow{\ \theta\ } & \mathrm{Hom}(\Delta_i/\Gamma, \Omega) \\ & {\scriptstyle \Theta'} \searrow \quad \nearrow {\scriptstyle \Theta_i} & \\ & \mathrm{Hom}(\Gamma^v/\Gamma, \Omega) & \end{array}$$

where $\Theta'$ is the map from diagram (5.3.1) and $\theta$ corresponds to the inclusion $\Delta_i/\Gamma \hookrightarrow \Gamma'/\Gamma$. All these maps are surjective. Since we have proved the surjectivity of $\psi'$ in diagram (5.3.1), it follows that $\Theta' \circ \psi$ is also surjective. Thus, for $\chi \in \mathrm{Hom}(\Delta_i/\Gamma, \Omega)$ there exists $\sigma \in G^t$ such that

$$\chi = \theta(\Theta' \circ \psi(\sigma)) = \Theta_i \circ \psi(\sigma) \ .$$

Hence $\Theta_i \circ \psi$ is surjective for every $i$, implying the surjectivity of $\psi$. □

We end this section by two remarks and a corollary, already used in the proof of Theorem 3.3.3.

*Remark 5.3.6.* Let us point out that

$$\Gamma^v = \{\, \gamma \in \Delta \mid \gamma + \Gamma \text{ has order not divisible by } p \,\}$$

if $\mathrm{char}\, \overline{K} = p$. If $\mathrm{char}\, \overline{K} = 0$, then $\Gamma^v = \Delta$.

*Remark 5.3.7.* As for the henselization and the inertia field, for an extension field $L \subseteq K^s$ of $K$, the ramification field of $\mathcal{O}^s$ over $L$ is $LK^v$.

**Corollary 5.3.8.** *Let $(K, \mathcal{O})$ be a valued field and $\mathcal{O}^s$ an extension of $\mathcal{O}$ to $K^s$. Define the fields $K^h, K^t$ and $K^v$ as in Theorem 5.3.3 and assume that $N/K$ is a finite Galois extenion. Considering the inclusion sequence*

$$K \subseteq K_h \subseteq K_t \subseteq K_v \subseteq N$$

*defined by* $K_h = K^h \cap N, K_t = K^t \cap N$, *and* $K_v = K^v \cap N$ *with respect to the corresponding valuations induced by* $\mathcal{O}^s$, *we obtain the following consequences:*

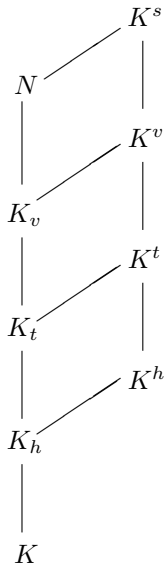
(0) $e(K_h/K) = 1$ *and* $f(K_h/K) = 1$

(1) $e(K_t/K_h) = 1$ *and* $f(K_t/K_h) = [K_t : K_h]$

(2) $f(K_v/K_t) = 1$ *and* $e(K_v/K_t) = [K_v : K_t]$

(3) $[N : K_v], e(N/K_v), f(N/K_v)$ *are powers of* $p$, *where* $p = 1$ *if* $\operatorname{char} \overline{K} = 0$ *and* $p = \operatorname{char} \overline{K}$, *otherwise.*

*Proof.* Let us consider the following diagram:




Since the henselization $K^h$ is immediate over $K$ by Theorem 5.2.5, also $K_h$ is immediate over $K$. This yields (0).

To see that $[K_t : K_h] = f(K_t/K_h)$ and hence $e(K_t/K_h) = 1$, let us consider the composition $L_h = K_t K^h$. From Galois theory and Theorem 5.2.7 (3) we know that $[K_t : K_h] = [L_h : K^h] = f(L_h/K^h)$. Moreover from Remark 5.2.4 we see that $K^h$ is the henselization of $K_h$ and $L_h$ is the henselization of $K_t$. Thus both extensions, $K^h/K_h$ and $L_h/K_t$ are immediate. Going now from $K_h$ to $L_h$ via $K_t$ and also via $K^h$ and using the multiplicativity of $f$, we obtain

$$f(K_t/K_h) \cdot 1 = f(L_h/K_h) = 1 \cdot f(L_h/K^h) \, .$$

Thus we obtain $[K_t : K_h] = f(K_t/K_h)$, and hence (1).

In order to find $[K_v : K_t] = e(K_v/K_t)$, we proceed similarly: First consider the composition $L_t = K_v K^t$, apply Theorem 5.3.3 (5) to the extension $L_t/K^t$,

and observe that by Remark 5.2.8, $K^t$ is the inertia field of $K_t$ and $L_t$ is the inertia field of $K_v$. By Theorem 5.2.7 (3) we obtain from the latter facts that $e(K^t/K_t) = 1$ and $e(L_t/K_v) = 1$. Now the multiplicativity of $e$ yields the result (as in (1) for $f$). This proves (2).

It remains the prove (3). In case $\operatorname{char} \overline{K} = 0$, by Theorem 5.3.3 (1) we have $K^s = K^v$ and hence $N = K_v$. Thus assume that $p = \operatorname{char} \overline{K}$. Now Theorem 5.3.3 (1) tells us that $G^v = G(K^s/K^v)$ is a pro-$p$ group. Since $N \cap K^v = K_v$, the restriction map from $G^v$ to $G(N/K_v)$ is surjective. Thus also $G(N/K_v)$ is a pro-$p$ group, showing that $[N : K_v]$ is a power of p. This together with Remark 3.2.17 yields that also $e(N/K_v)$ is a power of $p$. In fact, as we saw in the proof of Theorem 5.2.5, the valuation $\mathcal{O}^s \cap K_h = \mathcal{O}^s \cap (N \cap K^h)$ has a unique extension to $N$. Thus also $\mathcal{O}^s \cap K_v$ has a unique extension to $N$. Now let $x \in N$ and $X^m + \cdots + a_0 \in K_v[X]$ its irreducible polynomial over $K_v$. Then $m$ is a power of $p$, and (by Remark 3.2.17) $mw(x) = w(a_0)$, where $w$ denotes the valuation corresponding to $\mathcal{O}^s$.

Finally we show that the residue class field $\overline{K_v}$ does only allow purely inseparable extensions inside $\overline{N}$. Assume on the contrary that $\overline{x} \in \overline{N} \setminus \overline{K_v}$ is separable over $\overline{K_v}$. Let $\overline{x_1} \neq \overline{x}$ be conjugate to $\overline{x}$ in $\overline{N}$ over $\overline{K_v}$. (By Proposition 3.2.16, $\overline{N}$ is normal over $\overline{K_v}$.) Choose $x_2 \in N$ conjugate to $x$ in $N$ over $K_v$ such that $\overline{x_2} = \overline{x_1}$. Let $\sigma \in G(N/K_v)$ be such that $x_2 = \sigma(x)$. Since the restriction map from $G^v$ to $G(N/K_v)$ is surjective, we may take $\sigma \in G^v$. Thus $\overline{\sigma}$ is defined (as in Proposition 3.2.16) and yields $\overline{\sigma}(\overline{x}) = \overline{x}_1$. This, however, is impossible since $\sigma \in G^v$ even implies $\overline{\sigma} = \mathrm{id}$. □

## 5.4 Galois Characterization of Henselian Fields

In this section we shall see how to recognize in the absolute Galois group $G(K^s/K)$ of a given field $K$ the existence of certain non-trivial henselian valuations in $K$. Although this cannot be done for all types of henselian valuations, the class for which it is possible turns out to be quite comprehensive.

Let us start by investigating situations in which a certain profinite group $G$ occurs at the same time as the absolute Galois group of a field $K$ carrying a non-trivial henselian valuation $v$ and of a field $L$ that does not carry any non-trivial henselian valuation. First observe that if $\operatorname{char} L = 0$ and $G = G(L^s/L)$ then also $G = G(K^s/K)$ where we let $K$ be the formal power series field $L((\mathbb{Q}))$. This follows from the structure theory in Sects. 5.2 and 5.3 observing that $K$ is henselian with respect to its canonical valuation $v$ (see Exercise 3.5.6 and Remark 4.1.8) having divisible value group $\mathbb{Q}$. Thus the henselianity of the valuation $v$ cannot be recognized from the group $G$, as the field $L$ may be without any non-trivial henselian valuation. This suggests that we restrict ourselves to valuations $v$ where the value group is not divisible by at least one prime number $p$.

The next example shows that this $p$ should not be the characteristic of the residue class field of $v$. In fact, the construction of Mináč and Ware in [18]

yields a field $L$ without non-trivial henselian valuation having the same absolute Galois group as the fixed field $K$ of a $p$-Sylow subgroup of the absolute Galois group of the $p$-adic number field $\mathbb{Q}_p$. The value group of $K$ is divisible by all primes except $p$.

This together with the observations below leads us to the following class of valuations. We call a valuation $v$ of $K$ *tamely branching at* $p$, if the value group $v(K)$ is not divisible by $p$ and $p$ is different from the characteristic of the residue class field $\overline{K}$. Moreover, we require that $p^\infty$ divides the order of $G(\overline{K}^s/\overline{K})$ in case we have $(v(K) : pv(K)) = p$. This last condition is motivated by the observation that the henselian field $K = \mathbb{C}((\mathbb{Z}))$ has absolute Galois group $\widehat{\mathbb{Z}}$, which also occurs as absolute Galois group of the finite field $\mathbb{F}_p$. Clearly $\mathbb{F}_p$ does not allow any non-trivial (henselian) valuation. One should note that the requirement $G(\overline{K}^s/\overline{K}) \neq \{1\}$ would not be sufficient, as the next example shows. The henselian field $K = \mathbb{R}((\mathbb{Z}))$ also has value group $\mathbb{Z}$, and hence $(\mathbb{Z} : p\mathbb{Z}) = p$ for every $p$. Here we have $G(\overline{K}^s/\overline{K}) \neq \{1\}$, but the absolute Galois group $G = \widehat{\mathbb{Z}} \rtimes \mathbb{Z}/2\mathbb{Z}$ of $K$ also occurs as $G = G(L^s/L)$ where $L = R \cap \sigma(R)$, $R$ is the relative algebraic closure of $\mathbb{Q}$ in $\mathbb{R}$ and $\sigma \in G(\mathbb{Q}^s/\mathbb{Q})$ is such that $\langle\sigma\rangle \cong \widehat{\mathbb{Z}}$. Since $L$ does not have any non-archimedean ordering, it cannot carry a non-trivial henselian valuation by Lemma 4.3.6 and Corollary 2.2.6.

*Remark 5.4.1.* If $L/K$ is algebraic, and $v$ is a valuation on $L$, tamely branching at $p$, then $v|K$ is also tamely branching at $p$. This follows from the fact that the $p$-rank of $v(L)$ is less or equal to that of $K$ (see Exercise 5.5.2).

We shall now come to the main result of this section stating that the existence of a tamely branching henselian valuation can be recognized in the absolute Galois group. The main lemma we are then going to prove below is

**Lemma 5.4.2.** *Let $p$ be a fixed prime number and let $K$ be a field for which a $p$-Sylow subgroup $P$ of $G(K^s/K)$ satisfies the following conditions.*

*(1) $P \ncong \mathbb{Z}_p$ and in the case $p = 2$ assume also $P \ncong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$.*
*(2) $P$ has a non-trivial abelian normal closed subgroup.*

*Then $K$ admits a henselian valuation, tamely branching at $p$.*

With the use of this lemma and some basic facts about pro-$p$ groups collected in Exercises 5.5 we obtain the following characterization:

**Theorem 5.4.3.** (Koenigsmann) *A field $K$ admits a henselian valuation, tamely branching at some prime $p$ if and only if $G(K^s/K)$ has a non-procyclic Sylow subgroup $P \ncong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$ with a non-trivial abelian normal closed subgroup $N$ of $P$.*

*Proof.* Assume first that $(K, \mathcal{O})$ is henselian and tamely branching at $p$. Let $P$ be a $p$-Sylow subgroup of $G_K = G(K^s/K)$, and denote by $L$ its fixed field

in $K^s$. Let $\mathcal{O}' = \mathcal{O}^s \cap L$, where $\mathcal{O}^s$ is the unique extension of $\mathcal{O}$ to $K^s$. Then $(L, \mathcal{O}')$ is a henselian field with absolute Galois group $G(L^s/L) = P$, a pro-$p$ group. As $\mathcal{O}$ was tamely branching at $p$, the characteristic of $\overline{L}$ is different from $p$, and thus the ramification group $P^v$ is trivial (Theorem 5.3.3 (1)). Hence the inertia group $P^t$ is abelian by the second exact sequence. More precisely, we get

$$P^t \cong \mathrm{Hom}\big(\Delta/\Gamma', (\overline{L}^s)^\times\big) \ ,$$

where $\Gamma'$ is the value group of $\mathcal{O}'$ and $\Delta$ the value group of $\mathcal{O}^s$. Since $p$ does not divide the degree $[L : K]$, it follows that $p$ does not divide $\big[\overline{L} : \overline{K}\big]$ either, and $(\Gamma' : p\Gamma') = (\Gamma : p\Gamma)$, where $\Gamma$ is the value group of $\mathcal{O}$. In particular, $\mathcal{O}'$ is tamely branching at $p$.

By Theorem 5.3.3 (3), $P^t$ is isomorphic to $\mathbb{Z}_p^{r_p}$ where $r_p$ is the $p$-rank of $\Gamma'$, i.e., the $\mathbb{F}_p$-dimension of $\Gamma'/p\Gamma'$. Since $\mathcal{O}'$ is tamely branching at $p$, we have $r_p \geq 2$, or $r_p = 1$ and $p^\infty$ divides $\big|G\big(\overline{L}^s/\overline{L}\big)\big|$. At this point, recall the first exact sequence,

$$1 \longrightarrow P^t \longrightarrow P \longrightarrow G(\overline{L}^s/\overline{L}) \longrightarrow 1 \ .$$

From what we have obtained so far, we see first that $P^t$ is a non-trivial abelian normal and closed subgroup of $P$. Secondly we see that $P$ is neither isomorphic to $\mathbb{Z}_p$ nor to $\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$, as for $r_p = 1$ the group $G(\overline{L}^s/\overline{L})$ is not finite (cf Exercise 5.5.3). The case $P \cong \mathbb{Z}/2\mathbb{Z}$ clearly cannot occur.

In order to prove the converse of the theorem, assume that $P$ is a non-procyclic $p$-Sylow subgroup of $G_K$ with $P \ncong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$ and having a non-trivial abelian normal subgroup $N$. Then by Lemma 5.4.2, $K$ admits a henselian valuation ring $\mathcal{O}$, tamely branching at $p$. □

Before we come to the proof of the crucial Lemma 5.4.2, we shall need two technical lemmas that enable us to treat first the 'classical case' where $G(K^s/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$. In this case, the $p$-Sylow subgroup obviously is the group $G(K^s/K)$ itself and $\mathbb{Z}_p$ is the abelian normal subgroup. With the help of rigid elements (see Sect. 2.2.3) we shall then define a henselian valuation on $K$. In the general case we shall first find a suitable henselian valuation on the fixed field $L$ of the $p$-Sylow subgroup $P$, and then use 'going down' to find the required henselian valuation on $K$.

Let us now start with

**Lemma 5.4.4.** *Let $K$ be a field with $G(K^s/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$. Then*

*(1) For every finite extension $L$ of $K$ we have that $G(K^s/L) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$.*
*(2) $\mathrm{char}\, K \neq p$ and $K$ has a primitive $p$-th root of unity.*
*(3) $K^\times/(K^\times)^p$ has order $p^2$ for every finite extension $L$ of $K$.*
*(4) For every $a \in K^\times \smallsetminus \pm(K^\times)^p$, the image $\mathrm{Im}(N)$ of the norm map $N : K(\sqrt[p]{a})^\times \longrightarrow K^\times$ satisfies*

$$\mathrm{Im}(N) = \begin{cases} \bigcup_{i=0}^{p-1} a^i (K^\times)^p & \text{if } p \neq 2 \\ (K^\times)^2 \cup (-a)(K^\times)^2 & \text{if } p = 2 \ . \end{cases}$$

*Proof.* (1) Consider the split exact sequence associated with the semi-direct product description of $G = G(K^s/K)$,

$$1 \longrightarrow \mathbb{Z}_p \xrightarrow{\iota} G \xrightarrow{\pi} \mathbb{Z}_p \longrightarrow 1 \ .$$

Let $H = G(K^s/L)$. Then $H$ is of finite index in $G$ and thus open. Hence also $\pi(H)$ and $\iota^{-1}(H)$ are of finite index in $\mathbb{Z}_p$. Since subgroups of finite index of $\mathbb{Z}_p$ are open and again isomorphic to $\mathbb{Z}_p$, $H \cong \iota^{-1}(H) \rtimes \pi(H)$ is a decomposition of $H$ of the same shape as $G$.

(2) The first part of this item follows from Galois cohomology: if $\operatorname{char} K = p$, we have $\operatorname{cd}_p\ G(K^s/K) \leq 1$ [28, Ch. II, Prop. 3]. On the other hand $\operatorname{cd}_p\ \mathbb{Z}_p \rtimes \mathbb{Z}_p = 2$ [28, Ch. I, Prop. 22]. In order to avoid the use of Galois cohomology, we also give the following elementary proof for $\operatorname{char} K \neq p$.

In case $\operatorname{char} K = p$, the Artin-Schreier operator $\wp(x) = x^p - x$ maps the additive group $K^+$ of $K$ to a subgroup of $K^+$. By the Artin-Schreier theory, the Galois extensions $M$ of $K$ of exponent $p$ (i.e., $\sigma^p = 1$ for every $\sigma \in G(M/K)$) correspond bijectively to the subgroups of the quotient group $K^+/\wp(K)$ viewed as an $\mathbb{F}_p$-vector space [15, Ch. VIII, Theorem 15].

As we saw in part (1), every finite extension $L$ of $K$ has an absolute Galois group $G(K^s/L) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$. Thus the $\mathbb{F}_p$-dimension of $L^+/\wp(L)$ is 2 for every such $L$. Let $a, b \in K$ be such that $a + \wp(K)$ and $b + \wp(K)$ form an $\mathbb{F}_p$-basis of $K^+/\wp(K)$. We shall obtain a contradiction to the assumption $\operatorname{char} K = p$ by constructing a finite extension $L$ of $K$ such that for a certain element $\alpha \in L$ we find that $b, b\alpha$, and $a\alpha$ are $\mathbb{F}_p$-linearly independent modulo $\wp(L)$.

Choose $x \in K^s$ such that $x^p - x - a = 0$. Thus $L = K(x)$ is a cyclic Galois extension of $K$ of degree $p$. From $(x^{-1})^p + a^{-1}(x^{-1})^{p-1} - a^{-1} = 0$ we see that the trace $T(x)$ of $L/K$ is $-a^{-1}$. Hence $x^{p-1} = 1 + ax^{-1}$ shows that $\alpha = -x^{p-1}$ has trace 1. Now assume that $ib + jb\alpha + ka\alpha = u^p - u$ for some $0 \leq i, j, k \leq p-1$ and some $u \in L$. Taking traces on both sides of the equality gives

$$jb + ka = T(u)^p - T(u) \in \wp(K) \ .$$

The choice of $a$ and $b$ then implies $j = 0 = k$. Thus $ib = u^p - u$. If $i \neq 0$, then $u$ is a zero of $X^p - X - ib$ such that $K(u) = L$. Now $K(u) = K(x)$ implies $ib \in \mathbb{F}_p a + \wp(K)$, contradicting the choice of $a$ and $b$. Hence also $i = 0$, showing that $b, b\alpha$, and $a\alpha$ are $\mathbb{F}_p$-linearly independent modulo $\wp(L)$.

Next, as all finite extensions of $K$ within $K^s$ have degree a power of $p$, it follows that $K$ contains a primitive $p$-th root of unity.

(3) The absolute Galois group $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ of $L$ has exactly $p + 1$ closed subgroup of index $p$. Thus $L$ has exactly $p + 1$ extensions of degree $p$. Since $L$ contains a primitive $p$-th root of unity it follows from Kummer theory that $L^\times/(L^\times)^p$ has order $p^2$ ([15, Theorem 14, p. 220]).

To prove (4), observe first that $K^\times/(K^\times)^p$ has order $p^2$ by (3). Moreover, Kummer theory also implies for $L = K(\sqrt[p]{a})$, with $a \notin (K^\times)^p$, that $(L^\times)^p \cap K = \langle a \rangle (K^\times)^p$.

Computing the norm $N$ relative to this extension we have that

$$N(\sqrt[p]{a}) = \begin{cases} a \text{ for } p \neq 2 \\ -a \text{ for } p = 2 \, . \end{cases}$$

Hence $N(\sqrt[p]{a}) \notin (K^\times)^p$, if we assume $a \notin \pm(K^\times)^p$ (if $p \neq 2$ this already means $\notin (K^\times)^p$). Thus $\sqrt[p]{a} \notin (L^\times)^p$.

Next take any $b \in K^\times \setminus \langle a \rangle (K^\times)^p$. Then $b \notin (L^\times)^p$. Moreover, $N(b) = b^p$ implies $b \notin \langle \sqrt[p]{a} \rangle (L^\times)^p$. Consequently

$$L^\times = \bigcup_{i,j=0}^{p-1} b^i (\sqrt[p]{a})^j (L^\times)^p \, ,$$

which for $p \neq 2$ implies that

$$\mathrm{Im}(N) = \bigcup_{k=0}^{p-1} a^k (K^\times)^p \, .$$

Finally, for $p = 2$,

$$N(b^i(\sqrt{a})^j) = \begin{cases} (b^i)^2 \in \quad (K^\times)^2 & \text{if } j = 0 \, , \\ -(b^i)^2 a \in -a(K^\times)^2 & \text{if } j = 1 \, . \end{cases}$$ □

From the last lemma we shall now deduce the existence of many rigid elements in $K$. This will enable us to use Theorem 2.2.7 in order to find a suitable valuation ring on $K$. Recall that for a subgroup $T$ of $K^\times$ an element $x \in K^\times \setminus T$ is called $T$-rigid if

$$T + xT \subseteq T \cup xT \, .$$

**Lemma 5.4.5.** *Fix a prime number $p$. Let $K$ be a field and let $S$ be a subgroup of $K^\times$, containing $(K^\times)^p$, and for which each $x \in K^\times \setminus S$ satisfies*

$$S + xS \subseteq \bigcup_{i=0}^{p-1} x^i S \, . \tag{5.4.1}$$

*Assume also that $K^\times \neq S$ and if $p \neq 2$ that $(K^\times : S) \geq p^2$. Under these conditions there exists a subgroup $T \subseteq K^\times$ containing $S$ such that $(T : S) \leq p$ and all $x \in K^\times \setminus T$ are $S$-rigid and moreover also $T$-rigid. Furthermore, if $p = 2$, then $T = S$.*

*Proof.* If $p = 2$ condition (5.4.1) just means $S + xS \subseteq S \cup xS$. Thus $T = S$ will do the job.

Assume now $p > 2$. We first show that if there exists $T$ containing $S$, $(T : S) \leq p$, for which all $x \in K^\times \setminus T$ are $S$-rigid, then also any $x \in K^\times \setminus T$ is $T$-rigid. We may assume $(T : S) = p$ since otherwise the statement is trivially true. Then $T = \bigcup_{i=0}^{p-1} t^i S$ for some $t \in T \setminus S$. Let $x \in K^\times \setminus T$, $0 \leq \nu, \mu < p$ and $a, b \in S$. Then $xt^{\mu-\nu} \notin T$ and so

$$(t^\nu a) + x(t^\mu b) = t^\nu(a + (xt^{\mu-\nu})b) \in t^\nu(S \cup xt^{\mu-\nu}S) \subseteq T \cup xT \ .$$

Thus $x$ is $T$-rigid. It therefore suffices to prove $S$-rigidity for $x \in K^\times \smallsetminus T$.

Let us assume the lemma is false. Then there exist $a,\ b \in K^\times$ such that $(\langle a, b\rangle S : S) = p^2$, and elements $x, y \in S$ such that for some $k, l \in \{2, 3, \ldots, p-1\}$ we have that

$$x + a \in a^k S \qquad \text{and} \qquad y + b \in b^l S \ .$$

In fact, since $(S : S) = 1 \leq p$, by our assumption there has to be some $a \in K^\times \smallsetminus S$ and some $x \in S$ such that $x + a \notin S \cup aS$. Moreover, since $(\langle a\rangle S : S) \leq p$, again by our assumption there has to be some $c \in K^\times \smallsetminus \langle a\rangle S$ and some $z \in \langle a\rangle S$ such that $z + c \notin \langle a\rangle S \cup c\langle a\rangle S$. Let $z = a^\nu y$ with $0 \leq \nu \leq p-1$ and $y \in S$, and let $b = ca^{-\nu}$. Then $y + b \notin S \cup bS$. As $(K^\times)^p \subseteq S$, we may consider $K^\times/S$ as a $\mathbb{F}_p$-vector space and take exponents modulo $p$. In this vector space $aS$ and $bS$ are linearly independent.

*Claim*: $2l - 1 \neq 0$ in $\mathbb{F}_p$ and $y - b \in b^{\frac{l}{2l-1}} S$.

From the hypothesis (5.4.1) there exist $j, r, s, t \in \mathbb{F}_p$ such that $bx + ay = a(y + a^{-1}bx) \in a^{1-j}b^j S$ and

$$xy + bx + ay = \begin{cases} xy + (bx + ay) & \in (a^{1-j}b^j)^r S \\ b(x + b^{-1}(x + a)y) & \in b(a^k b^{-1})^s S \\ a(y + a^{-1}(y + b)x) & \in a(a^{-1}b^l)^t S \ . \end{cases}$$

So comparing the exponents of $aS$ and $bS$ one gets

$$\begin{array}{ll} (I) & r(1-j) = ks = 1 - t \\ (II) & rj = 1 - s = tl \ . \end{array}$$

As $l \neq 0$ this implies $r \neq 0$. Thus

$$\begin{array}{ll} (I) + (II) & \Rightarrow r = (l-1)t + 1 \\ (I) + k(II) & \Rightarrow k = (kl-1)t + 1 \ . \end{array}$$

Since $k \neq 1$, we have that $kl - 1 \neq 0$. Thus

$$t = \frac{k-1}{kl-1} \quad \text{and} \quad r = \frac{2kl - k - l}{kl - 1}$$

and so $2kl - k - l \neq 0$. From (II) we then obtain

$$j = \frac{lt}{r} = \frac{l(k-1)}{2kl - k - l} \neq 0 \ .$$

Now let $y - b \in b^i S$ for some $0 \leq i \leq p-1$. We have to compute $i$. We recall that $bx + ay \in a^{1-j}b^j S$. On the other hand

$$bx + ay = (b - y)x + (a + x)y \in a^k(a^{-k}b^i)^q S \ ,$$

for some $q$. Comparing again the exponents of $aS$ and $bS$ we have that $1-j = k(1-q)$ and $j = iq = i(j+k-1)k^{-1}$. As $j \neq 0$, also $j+k-1 \neq 0$. Therefore

$$j+k-1 = \frac{l(k-1)}{2kl-k-l} + k - 1 = \frac{(k-1)k(2l-1)}{2kl-k-l}$$

implies $2l-1 \neq 0$. Now,

$$i = \frac{jk}{j+k-1} \quad \text{and} \quad jk = \frac{l(k-1)k}{2kl-k-l} .$$

Hence

$$i = \frac{l}{2l-1} ,$$

which proves the claim. Since $l \neq 0, 1$ we also have that $i \neq 0, 1$.

Consider next the set

$$I = \{\, i \in \mathbb{F}_p \setminus \{0, 1\} \mid \exists b_1 \in \langle b \rangle S \setminus S \text{ and } y \in S \text{ such that } y + b_1 \in b_1^i S \,\} .$$

Then $I \neq \emptyset$, since $l \in I$. Also, $I$ is closed under the operation $i \mapsto i^{-1}$. In fact, if $y + b_1 = b_1^i z$ for some $z \in S$, then $y - b_1^i z = -b_1$. Putting $b_2 = -b_1^i z$ it follows that $y + b_2 \in b_2^{i^{-1}} S$. Moreover, the claim shows also that $I$ is closed under the operation $i \mapsto \frac{i}{2i-1}$. (Note that $-1 = (-1)^p \in S$.) The proof of the claim also shows for $i \in I$ that $2i - 1 \neq 0$ in $\mathbb{F}_p$, i.e., $2^{-1} \notin I$.

Observe now that if for some $m$ with $2 \leq m < p$ we have that $m(m+1)^{-1} \in I$, then

$$\frac{m-1}{m} = \left(\frac{m}{m-1}\right)^{-1} = \left(\frac{\frac{m}{m+1}}{2\frac{m}{m+1} - 1}\right)^{-1} \in I .$$

Repeating this process we get after some steps $\frac{1}{1+1} \in I$, contradicting $\frac{1}{2} \notin I$. Consequently $I$ contains no element of the form $\frac{m}{m+1}$, with $2 \leq m < p$. On the other hand, each element $i \in \mathbb{F}_p$ can be written in this form:

$$i = \frac{\frac{i}{1-i}}{\frac{i}{1-i} + 1} ,$$

a contradiction. □

We finally come to the proof of Lemma 5.4.2. This proof will be divided into three parts:

*classical case:* $G(K^s/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$, and $\sqrt{-1} \in K$ in case $p = 2$.

*pro-p case:* $G(K^s/K)$ is a non-procyclic pro-$p$ group without elements of finite order,[3] having a non-trivial normal abelian subgroup $H$

*general case:* $G(K^s/K)$ satifies the assumptions of Lemma 5.4.2.

*Proof of Lemma 5.4.2. Classical Case*: Note that by our assumption $K$ automatically contains a primitive $p$-th root of unity. For the case $p = 2$ we assume in addition that $\sqrt{-1} \in K$. We shall first show that $S = (K^\times)^p$ satisfies the assumptions of Lemma 5.4.5.

Take $x \in K^\times \setminus (K^\times)^p$, set $L = K(\sqrt[p]{x})$, and let $N : L \longrightarrow K$ be the norm map. Next take two elements $a, b \in K^\times$. For $p \neq 2$, we have $a^p + xb^p = N(a + b\sqrt[p]{x})$. In case $p = 2$, let $\zeta \in K^\times$ satisfy $-1 = \zeta^2$. Then $a^2 + xb^2 = a^2 - x(\zeta b)^2 = N(a + \zeta b\sqrt{x})$. Setting $\alpha = a + b\sqrt[p]{x}$ for $p \neq 2$ and $\alpha = a + \zeta b\sqrt{x}$ for $p = 2$ we get for every $p$ that $a^p + xb^p = N(\alpha)$. Since we are assuming $-1 \in (K^\times)^2$ if $p = 2$, it follows from Lemma 5.4.4 that

$$N(\alpha) \in \bigcup_{i=0}^{p-1} x^i (K^\times)^p$$

(no matter if $p = 2$ or $p \neq 2$). Hence the condition (5.4.1) of Lemma 5.4.5 holds for $S = (K^\times)^p$. Moreover, $(K^\times : S) \geq p^2$ by Lemma 5.4.4. Consequently, there exists a subgroup $T$ of $K^\times$ satisfying:

- $(K^\times)^p \subseteq T$ and $T \neq K^\times$. If $p = 2$, then $T = (K^\times)^2$.
- Every $x \in K^\times \setminus T$ is $T$-rigid.

We are now ready to apply Theorem 2.2.7. Thus there exists a subgroup $T_1$ of $K^\times$ such that $\mathcal{O}(T_1)$ is a valuation ring of $K$ with $\mathcal{O}(T_1)^\times \subseteq T_1$. Furthermore, for $p \neq 2$, $T_1 = T \neq K^\times$, and for $p = 2$, as $(T_1 : (K^\times)^2) \leq 2$, also $T_1 \neq K^\times$. Since we have $(K^\times)^p \subseteq T_1$, it follows that the value group of $\mathcal{O}(T_1)$ is not $p$-divisible. Therefore, $\mathcal{O}(T_1)$ is a proper valuation ring of $K$.

We shall next construct from $\mathcal{O}(T_1)$ a valuation ring of $K$, tamely branching at $p$. Let $\Gamma_1$ be the value group of $\mathcal{O}(T_1)$. Let $\Delta$ be the maximal convex $p$-divisible subgroup of $\Gamma_1$. As $\Gamma_1$ is not $p$-divisible, the same is true for $\Gamma = \Gamma_1/\Delta$. Moreover, $\Gamma$ contains no non-trivial convex $p$-divisible subgroup. According to Lemma 2.3.1 there exists a valuation ring $\mathcal{O}$ containing $\mathcal{O}(T_1)$ that has $\Gamma$ as its value group. We shall prove that $\mathcal{O}$ is the desired valuation ring. Let $v : K \longrightarrow\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ be a valuation corresponding to $\mathcal{O}$ and $\Gamma$.

Assume first, for the sake of obtaining a contradiction, that the residue class field $\overline{K}$ of $\mathcal{O}$ has characteristic $p$. Then $v(p) > 0$ and there exists $\pi \in K^\times$, satisfying $0 < v(\pi) \leq v(p)$ and $v(\pi) \notin p\Gamma$. Indeed, if all positive values $\leq v(p)$ were $p$-divisible, the convex hull of the group generated by $v(p)$ would be a $p$-divisible convex subgroup, a contradiction. Now consider the extension $E = K(\sqrt[p]{\pi})$ and the norm map $N : E^\times \longrightarrow K^\times$. By Lemma 5.4.4 (4), $(N(E^\times) : (K^\times)^p) = p$. As $\pi$ and $1 + \pi$ are norms, they have to be $\mathbb{F}_p$-linearly dependent, i.e., there exist $i, j \in \{0, 1, \ldots, p-1\}$, not both zero, such that $\pi^i(1 + \pi)^j \in (K^\times)^p$. Actually we must have $i = 0$, as $v(\pi) \notin p\Gamma$. Hence $(1 + \pi)^j \in (K^\times)^p$, and as $\operatorname{char} \overline{K} = p$ (our assumption!) and $\pi \in \mathcal{M}$, there must exist $y \in \mathcal{M}$ such that $(1 + \pi)^j = (1 + y)^p$.

[3] Recall that $G(K^s/K)$ can have only elements of finite order $m$, if $p = 2$ and $m = 2$ (Theorem 4.3.5).

It follows from this that

$$\pi\left(\sum_{t=1}^{j}\binom{j}{t}\pi^{t-1}\right)=\sum_{t=1}^{p-1}\binom{p}{t}y^t+y^p. \qquad (*)$$

Moreover, $p$ divides $\binom{p}{t}$ for all $t=1,\dots,p-1$. So $v(\binom{p}{t}y^t) > v(p)$ for all $t=1,\dots,p-1$. On the other hand,

$$v\left(\pi\left(\sum_{t=1}^{j}\binom{j}{t}\pi^{t-1}\right)\right)=v(\pi)\le v(p)\ .$$

Thus the equation $(*)$ above implies $v(\pi)=v(y^p)\in p\Gamma$, a contradiction.

We have thus proved $\operatorname{char}\overline{K}\neq p$. It remains to show that $\mathcal{O}$ is henselian, and that $p^\infty$ divides $|G(\overline{K}^s/\overline{K})|$ in case $\Gamma/p\Gamma$ has order $p$.

We shall prove first that if $\mathcal{O}$ is not henselian, there exists a Galois extension $L$ of $K$ with $[L:K]=p$ for which the norm map $N: L^\times \longrightarrow K^\times$ contradicts Lemma 5.4.4 (4).

If $\mathcal{O}$ is not henselian, it can also not be $p$-henselian, since in our situation $K^s=K(p)$. Thus by Theorem 4.2.2 there exists a Galois extension $L/K$ of degree $p$ to which $\mathcal{O}$ has more than one prolongation. But then by the formula "$p=ref$" of Theorem 3.3.3 (note that $\operatorname{char}\overline{K}\neq p$, hence $d=1$), $\mathcal{O}$ has exactly $p$ immediate prolongations, say $\mathcal{O}_1,\dots,\mathcal{O}_p$. Let $v: L\longrightarrow \Gamma\cup\{\infty\}$ be a valuation corresponding to $\mathcal{O}_1$. As $K$ contains all $p$-th roots of unity, we find $a\in K\setminus K^p$ such that $L=K(\sqrt[p]{a})$. Moreover, we may assume that $a\in\mathcal{O}^\times$. In fact, $v(a)$ has to be $p$-divisible, since otherwise $e=p$ and thus $r=1$. Modifying $a$ by a $p$-th power then yields $a\in\mathcal{O}^\times$.

Let $G(L/K)=\{\sigma_1,\dots,\sigma_p\}$, where we choose $\sigma_i$ such that $\mathcal{O}_i=\sigma_i^{-1}(\mathcal{O}_1)$ ($\sigma_1=\mathrm{id}$). Using week approximation, Theorem 3.2.7 (3), we find $x\in L$ satisfying $x\in\mathcal{M}_1$, and $x\in\mathcal{O}_i^\times$ for every $i=2,\dots,p$. We then have $x\in\mathcal{M}_1$, and $\sigma(x)\in\mathcal{O}_1^\times$ for every $\sigma\in G(L/K)$, $\sigma\neq\mathrm{id}$. Observe that if $v(x)\in p\Gamma$, there exists $y\in K^\times$ with $0<v(y)<v(x)$ and $v(y)\notin p\Gamma$. (As in the proof of $\operatorname{char}\overline{K}\neq p$.) Replacing $x$ by $x+y$, if necessary, we get $v(x+y)=v(y)\notin p\Gamma$, and still $\sigma(x)+y\in\mathcal{O}_1^\times$ for every $\sigma\neq\mathrm{id}$. Hence we may assume that $v(x)\notin p\Gamma$.

For the value of $N(x)$ we get

$$v(N(x))=\sum_{i=1}^{p}v(\sigma_i(x))=v(x)\notin p\Gamma\ .$$

Thus the norms $a$ and $N(x)$ are $\mathbb{F}_p$-linearly independent. Indeed, if $a^iN(x)^j\in(K^\times)^p$ for some $i,j\in\{0,1,\dots,p-1\}$, not both zero, then $j=0$ as $v(N(x))\notin p\Gamma$. This however would imply $a\in(K^\times)^p$, contrary to our assumption on $a$. Hence we obtain $(N(L^\times):(K^\times)^p)\ge p^2$, contradicting Lemma 5.4.4 (4).

Summarizing, $\mathcal{O}$ is a henselian valuation ring with non-$p$-divisible value group and residue class field $\overline{K}$ of characteristic different from $p$. We then apply the results of the previous Sects. 5.2 and 5.3 to the unique extension $\mathcal{O}^s$

of $\mathcal{O}$ to $K^s$ in order to finish the proof. Observe first that $\operatorname{char}\overline{K} \neq p$ together with $G(K^s/K)$ being a $p$-group implies that $G^v(\mathcal{O}^s)$ is trivial by Theorem 5.3.3 (1). Write $\Gamma^s$ for the value group of $\mathcal{O}^s$. Recall that $\Gamma^s$ is the divisible closure of $\Gamma$, and since $G^v(\mathcal{O}^s)$ is trivial and $G^t(\mathcal{O}^s)$ is a $p$-group, it follows from Theorem 5.3.3 (3) that

$$G^t(\mathcal{O}^s) \cong \mathbb{Z}_p^{r_p} \ ,$$

where $r_p$ is the $\mathbb{F}_p$-dimension of $\Gamma/p\Gamma$. Consequently, if $\Gamma/p\Gamma$ has order $p$ then $r_p = 1$ and $G^t(\mathcal{O}^s) \cong \mathbb{Z}_p$ is procyclic. It then follows from $G(K^s/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$ and the first exact sequence that $p^\infty$ divides $|G(\overline{K}^s/\overline{K})|$. This concludes the proof of the classical case.

Before we continue with the proof of Lemma 5.4.2, let us prove a little lemma that will be used several times.

**Lemma 5.4.6.** *Let $K$ be a field having a henselian valuation ring $\mathcal{O}$ with maximal ideal $\mathcal{M}$ and value group $\Gamma$. Assume that $\mathcal{O}$ is strictly finer than the canonical henselian valuation ring $\mathcal{O}_c$ (cf. Sect. 4.4). Let $\mathcal{M}_c$ be the maximal ideal of $\mathcal{O}_c$ and $\Gamma_c$ the corresponding value group. If $\mathcal{O}$ is tamely branching at $p$, also $\mathcal{O}_c$ is tamely branching at $p$. Moreover, $(\Gamma_c : p\Gamma_c) = (\Gamma : p\Gamma)$.*

*Proof.* Since $\mathcal{O} \subsetneqq \mathcal{O}_c, H_2(K)$ is non-empty, and thus both residue class fields, $\mathcal{O}/\mathcal{M}$ as well as $\mathcal{O}_c/\mathcal{M}_c$ are separably closed. As $\mathcal{O}/\mathcal{M}$ is a homomorphic image of the subring $\mathcal{O}/\mathcal{M}_c$ of $\mathcal{O}_c/\mathcal{M}_c, \operatorname{char}(\mathcal{O}/\mathcal{M}) = p$ would be inherited from $\operatorname{char}(\mathcal{O}_c/\mathcal{M}_c) = p$. Thus it remains to show that $\Gamma_c$ is not $p$-divisible. By the explanations after Corollary 2.3.2, $\Gamma_c$ is obtained from $\Gamma$ by dividing $\Gamma$ by a convex subgroup $\Gamma_0$ that is the value group of the valuation ring $\mathcal{O}/\mathcal{M}_c$ of the field $\mathcal{O}_c/\mathcal{M}_c$. As the latter is separably closed (and $\mathcal{O} \neq \mathcal{O}_c$), Theorem 3.2.11 tells us that $\Gamma_0$ is divisible. Therefore $\Gamma_c/p\Gamma_c \cong \Gamma/p\Gamma$ and hence $(\Gamma_c : p\Gamma_c) = (\Gamma : p\Gamma)$. In particular, if $\Gamma$ was not $p$-divisible, so is $\Gamma_c$. Note that the case $(\Gamma : p\Gamma) = p$ cannot occur, as the residue class field $\mathcal{O}/\mathcal{M}$ is separably closed. □

We now continue with the proof of the

*pro-p case*: Let $H$ be a non-trivial normal abelian subgroup of $G(K^s/K)$, and denote by $L$ its fixed field. Since by assumption $H$ is torsionfree, it is a free $\mathbb{Z}_p$-module.

If $H$ is not procyclic, $H$ contains a subgroup $H' \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Let $L'$ be the fixed field of $H'$. According to the classical case, $L'$ has a henselian valuation ring $\mathcal{O}'$, tamely branching at $p$. Replacing $\mathcal{O}'$ by the canonical henselian valuation of $L'$, if necessary (Lemma 5.4.6), we may assume that $\mathcal{O}'$ is coarser than the canonical henselian valuation ring of $L'$. From the abelian property of $H$ we get that $L'/L$ is a Galois extension. Hence by Theorem 4.4.3, $\mathcal{O}' \cap L$ is a henselian valuation of $L$. Moreover, since $L'/L$ is an algebraic extension, $\mathcal{O}' \cap L$ is also tamely branching at $p$ (Remark 5.4.1). Since $L/K$ is a Galois extension, we can repeat the argument and obtain a tamely branching henselian valuation ring on $K$.

In the case $H \cong \mathbb{Z}_p$, since $G(K^s/K) \ncong \mathbb{Z}_p$, there exists $\sigma \in G(K^s/K) \setminus H$ such that $H' = \langle H, \sigma \rangle = H \rtimes \langle \sigma \rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$ (recall that $G(K^s/K)$ has no element of finite order). Let $L'$ be the fixed field of $H'$. By the classical case, $L'$ has the desired henselian valuation ring $\mathcal{O}'$. By Lemma 5.4.6, we may assume that $\mathcal{O}'$ is coarser than the canonical valuation ring of $L'$. Next, the unique prolongation $\mathcal{O}$ of $\mathcal{O}'$ to $L$ is a proper henselian valuation ring of $L$. Thus the canonical valuation ring $\mathcal{O}_c$ of $L$ is also non-trivial. If $\mathcal{O}$ is coarser than $\mathcal{O}_c$, then $\mathcal{O} \cap K = \mathcal{O}' \cap K$ is henselian and inherits[4] from $\mathcal{O}'$ that it is tamely branching at $p$. If $\mathcal{O}$ is strictly finer than $\mathcal{O}_c$, then the residue class field $k$ of $\mathcal{O}_c$ is separably closed. Clearly $\operatorname{char} k \neq p$, since $\mathcal{O} \subseteq \mathcal{O}_c$ and the residue class field of $\mathcal{O}'$ has characteristic $\neq p$. Hence, by Theorem 3.3.3, the value group $\Gamma_c$ of $\mathcal{O}_c$ is not $p$-divisible ($L \neq K^s$). Next, as $\mathcal{O}'$ by assumption is coarser than the canonical valuation of $L'$ and $\mathcal{O}_c \cap L'$ properly contains $\mathcal{O}'$, we conclude that $\mathcal{O}_c \cap L'$ cannot have residue class field separably closed. Furthermore, as $G(K^s/L')$ is a $p$-group, this means that $p^\infty$ divides the order of the absolute Galois group of the residue class field $k'$ of $\mathcal{O}_c \cap L'$, unless $p = 2$ and $k'$ is real closed. But then the field $L'$ is real, and hence the absolute Galois group of $L'$ (which is a subgroup of $G(K^s/K)$) would contain an element of order 2, contradicting our assumption in the pro-$p$ case. Moreover, as $\Gamma_c \neq p\Gamma_c$ and $L/L'$ is algebraic, the value group of $\mathcal{O}_c \cap L'$ is also not $p$-divisible[4]. Whence $\mathcal{O}_c \cap L'$ is tamely branching at $p$. Finally, $\mathcal{O}_c \cap K$ is henselian by Theorem 4.4.3, as $L/K$ is a Galois extension. Thus also $\mathcal{O}_c \cap K = \mathcal{O}_c \cap L' \cap K$ is tamely branching at $p$.

Finally we come to the proof of the

*General case*: We now let $P$ be a $p$-Sylow subgroup of $G(K^s/K)$ satisfying (1) and (2) of Lemma 5.4.2. Let $L$ be the fixed field of $P$. We then discuss the two cases $p \neq 2$ and $p = 2$.

Let first $p \neq 2$. In this case $P$ satisfies the conditions of the 'pro-$p$ case', and thus we find a valuation $\mathcal{O}$ on $L$, tamely branching at $p$. By Lemma 5.4.6 we may assume that $\mathcal{O}$ is coarser than the canonical henselian valuation ring of $L$. Then $\mathcal{O} \cap K$ is tamely branching[4] at $p$, and by Theorem 4.4.5 also henselian.

Now let $p = 2$. In this case let $L_1 = L(\sqrt{-1})$. Then $G(L_1^s/L_1)$ satisfies the assumption of the 'pro-2 case': Note that $H \cap G(L_1^s/L_1)$ is a non-trivial normal abelian subgroup of $G(L_1^s/L_1)$, if $H$ is a non-trivial abelian normal subgroup of $G(L^s/L)$. Thus as above we find a henselian valuation ring $\mathcal{O}_1$ on $L_1$, tamely branching at 2. Again we may assume that $\mathcal{O}_1$ is coarser than the canonical henselian valuation ring of $L_1$. Then by Remark 5.4.1, $\mathcal{O} = \mathcal{O}_1 \cap L$ in tamely branching at 2. By Theorem 4.4.4, $\mathcal{O}$ is also henselian and still coarser than the canonical henselian valuation ring of $L$. In order to be able to apply Theorem 4.4.5 now (as in the case $p \neq 2$), we need to know in addition that $\mathcal{O}$ is coarser than the valuation ring $\mathcal{O}^+$ introduced in Theorem 4.4.5. This, however, can be done as in Lemma 5.4.6:

[4] Recall Remark 5.4.1

Assume that $\mathcal{O}$ is strictly finer than $\mathcal{O}^+$, and denote by $\mathcal{M}$ and $\Gamma$ the maximal ideal and the value group of $\mathcal{O}$. For $\mathcal{O}^+$ we use correspondingly $\mathcal{M}^+$ and $\Gamma^+$. As both residue class fields $\mathcal{O}^+/\mathcal{M}^+$ as well as $\mathcal{O}/\mathcal{M}$ now are real closed, we need to know that $(\Gamma^+ : 2\Gamma^+) \geq 2^2$. This follows from the facts that $(\Gamma : 2\Gamma) \geq 2^2$ (recall that $\mathcal{O}$ is tamely branching at 2), and that $\Gamma^+$ is obtained from $\Gamma$ by dividing by a convex subgroup $\Gamma'$ that is the value group of the valuation ring $\mathcal{O}/\mathcal{M}^+$. Since $\mathcal{O}^+/\mathcal{M}^+$ is real closed and $\mathcal{O}/\mathcal{M}^+$ is henselian (Corollary 4.1.4), $\Gamma'$ must be divisible by Lemma 4.3.6 and Theorem 4.3.7. Thus $(\Gamma^+ : 2\Gamma^+) = (\Gamma : 2\Gamma) \geq 2^2$.

This finishes the proof of the general case and hence the proof of Lemma 5.4.2. □

## 5.5 Exercises

**Exercise 5.5.1.**
Let $(K^h, \mathcal{O}^h)$ be a henselization of a valued field $(K, \mathcal{O})$. For a finite separable extension $K(z)$ of $K$, let $f$ be the minimal polynomial of $z$ over $K$. Suppose that $f = g_1 \cdots g_m$ is the decomposition of $f$ in irreducible factors in $K^h[X]$. Show that $\mathcal{O}$ has exactly $m$ prolongations to $K(z)$. Try to describe these prolongaions by choosing roots $z_1, \ldots, z_m \in K^s$ of the factors $g_1, \ldots, g_m$, respectively.

**Exercise 5.5.2.**
Let $\Gamma \subseteq \Delta$ be torsionfree abelian groups such that $\Delta/\Gamma$ is a torsion group.

(a) If $p \nmid (\Delta : \Gamma)$, show that $\Delta/p\Delta \cong \Gamma/p\Gamma$.
(b) Verify the exactness of the sequences

$$0 \to (p\Delta \cap \Gamma)/p\Gamma \to \Gamma/p\Gamma \to \Gamma/(p\Delta \cap \Gamma) \to 0$$

$$0 \to (\Gamma + p\Delta)/p\Delta \to \Delta/p\Delta \to \Delta/(\Gamma + p\Delta) \to 0\ ,$$

and conclude that $\dim_{\mathbb{F}_p} \Delta/p\Delta \leq \dim_{\mathbb{F}_p} \Gamma/p\Gamma$.

*Hint:* It suffices to show that $\dim_{\mathbb{F}_p}(\Delta/(\Gamma + p\Delta)) \leq \dim_{\mathbb{F}_p}((p\Delta \cap \Gamma)/p\Gamma)$. Take a family $\delta_1, \ldots, \delta_n$ such that each residue $\delta_j + \Gamma$ generates a single cyclic component of $\Delta/\Gamma$ of (finite) $p$-power order. Show that the family $\delta_1 + (\Gamma + p\Delta), \ldots, \delta_n + (\Gamma + p\Delta)$ is linearly independent in $\Delta/(\Gamma + p\Delta)$, viewed as $\mathbb{F}_p$-vector space. Let $p^{\nu_j}$ be the order of $\delta_j + \Gamma$ and set $\lambda_j = p^{\nu_j}\delta_j$, for every $j$. Show next that $\lambda_1 + p\Gamma, \ldots, \lambda_n + p\Gamma$ are $\mathbb{F}_p$-linearly independent in $(p\Delta \cap \Gamma)/p\Gamma$.

**Exercise 5.5.3.**

(a) Show that every non-trivial closed subgroup of the procyclic pro-$p$ group $\mathbb{Z}_p$ is open and hence isomorphic to $\mathbb{Z}_p$.
(b) Show that a closed normal subgroup of $\mathbb{Z}_p \rtimes \mathbb{Z}/p\mathbb{Z}$, isomorphic to $\mathbb{Z}_p$, is always open.
(c) Show that a closed normal subgroup of $\mathbb{Z}_p \rtimes \mathbb{Z}_p$, isomorphic to $\mathbb{Z}_p$, is never open.
(d) Let $\mathbb{Z}_p$ be a closed normal subgroup of the torsionfree pro-$p$ group $H$. If $H/\mathbb{Z}_p$ is a torsion group, then $H \cong \mathbb{Z}_p$.

**Exercise 5.5.4.**

Let $G$ be an abelian pro-$p$ group and set $G^* = \bigcap U$, were $U$ ranges over the set of all open normal subgroups of $G$ such that $(G : U) = p$.

(a) $G/G^*$ is an abelian pro-$p$-group.
(b) $\mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Hom}(G/G^*, \mathbb{Z}/p\mathbb{Z})$, where "Hom" refers to continuous homomorphisms.
(c) Let $\varphi : G \to G_1$ be a continuous homomorphism to another pro-$p$ group $G_1$. Show that $\varphi$ induces homomorphisms $\varphi^* : G/G^* \to G_1/G_1^*$ and $\varphi_* : \mathrm{Hom}(G_1, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$ such that the following conditions are equivalent:
  (i) $\varphi$ is surjective.
  (ii) $\varphi^*$ is surjective.
  (iii) $\varphi_*$ is injective.

**Exercise 5.5.5.**

(a) Assume that $K$ is a field for which $G = G(K^s/K)$ is abelian and not procyclic. Then $K$ admits a henselian valuation ring tamely branching at some prime $p$ (Hint: if every Sylow subgroup of $H$ is cyclic, then $H$ is cyclic).
(b) Assume that for every non-trivial valuation ring $\mathcal{O}$ of $K$ there exists a prime $p$ different from the characteristic of the residue class field of $(K, \mathcal{O})$, such that in every $p$-Sylow extension $L$ of the henselization of $(K, \mathcal{O})$ all closed abelian subgroups of $G(K^s/L)$ are procyclic. Show that every closed abelian subgroup of $G(K^s/K)$ is procyclic.
(c) Use (b) and the structure theory of Chapter 5 in order to deduce that every closed abelian subgroup of $G(\mathbb{Q}^s/\mathbb{Q})$ has to be procyclic.
(d) Try to generalize (b) such that it becomes applicable to $\mathbb{Q}(X)$.

# 6

# Applications of Valuation Theory

In this chapter we shall give applications of the theory of general valuations and their henselizations developed so far. In the first application, we treat Artin's conjecture about the $p$-adic number fields $\mathbb{Q}_p$. In the second application we characterize those valued fields that share with $\mathbb{Q}_p$ all its 'algebraic' properties (as the real closed fields do with $\mathbb{R}$). The third application provides a local-global principle for isotropy of iterated quadratic forms over a real field $K$. The local objects are just certain henselizations of the given field $K$.

In all three cases, the use of general (higher rank) valuations and their henselizations is essential – the use of absolute values alone would not be sufficient.

## 6.1 Artin's Conjecture

This conjecture concerns the solvability of certain diophantine equations over the field $\mathbb{Q}_p$ of $p$-adic numbers. Its formulation does not refer to any valuation. Nevertheless the only proof known makes use of abstract valuation theory. In particular, it uses valuations of arbitrarily high rank, and it is clear from the proof that absolute values would not suffice.

Now, what is Artin's Conjecture?

Let $K$ be any field, and let $i$ and $d$ be positive integers. $K$ is said to be a $C_i(d)$-*field* if every homogeneous polynomial of (total) degree $d$ in more than $d^i$ variables, with coefficients from $K$, has a non-trivial zero in $K$. All finite fields $k$ are $C_1(d)$ for every $d$ (see [5]). If a field $k$ is $C_i(d)$ for every $d$, then the field $k((X))$ of formal Laurent-series over $k$ is $C_{i+1}(d)$ for all $d$ (see [16]). In particular, all fields $\mathbb{F}_p((X))$ are $C_2(d)$ for all $d$.

By an easy application of Hensel's Lemma, one sees that every quadratic form (= homogeneous polynomial of degree 2) in more than $4 = 2^2$ variables has a non-trivial zero over each $p$-adic field $\mathbb{Q}_p$. Hence each $\mathbb{Q}_p$ is $C_2(2)$. A classical proof of Lewis (see [17]) shows that each $\mathbb{Q}_p$ is also $C_2(3)$. It was then conjectured by E. Artin that, because of its great similarity to $\mathbb{F}_p((X))$, the

field $\mathbb{Q}_p$ should actually be $C_2(d)$ for all $d$. In 1965 Ax and Kochen showed (see [2]) that this is "almost" true. More precisely, they showed that for each fixed degree $d$, for almost all primes $p$, $\mathbb{Q}_p$ is $C_2(d)$. Based on an example of Terjanian (see [30]) it was later shown that this result is somehow best possible: For every $p$ there exist degrees $d \geq 4$ such that $\mathbb{Q}_p$ is not $C_2(d)$.

We are now going to prove this "almost" solution. Let us fix a degree $d$ and assume that the set

$$A_d = \{\, p \in \mathbb{P} \mid \mathbb{Q}_p \text{ is not } C_2(d) \,\}$$

is infinite, where $\mathbb{P}$ denotes the set of all rational primes. It will be shown that this assumption leads to a contradiction. This will be done as follows.

As explained in the Appendix A, because $A_d$ is infinite, there exists a non-principal ultrafilter $\mathcal{F}$ on the collection of all subsets of $\mathbb{P}$, with $A_d \in \mathcal{F}$ (Corollary A.2). Moreover it is shown there that the ultraproducts

$$K^* = \prod_{p\in\mathbb{P}} \mathbb{Q}_p/\mathcal{F} \qquad \text{and} \qquad L^* = \prod_{p\in\mathbb{P}} \mathbb{F}_p((X))/\mathcal{F}$$

are both henselian fields with respect to their canonical valuations $v^*$ and $w^*$, resp. (Theorem A.4). They actually have the same residue class field,

$$k = \prod_{p\in\mathbb{P}} \mathbb{F}_p/\mathcal{F}\,,$$

which has characteristic zero (Corollary A.5), and they both have the same value group,

$$\Gamma = \prod_{p\in\mathbb{P}} \mathbb{Z}/\mathcal{F}\,,$$

which has infinite rank (a fact that follows from Theorem A.6, but is not needed here).

Since $A_d \in \mathcal{F}$ and, for every $p \in A_d$, $\mathbb{Q}_p$ is not $C_2(d)$, we find that $K^*$ is not $C_2(d)$ (Theorem A.4). On the other hand, since $\mathbb{P} \in \mathcal{F}$ and, for every $p \in \mathbb{P}$, $\mathbb{F}_p((X))$ is $C_2(d)$, we have that $L^*$ is $C_2(d)$ (Theorem A.4). Thus obviously $K^*$ and $L^*$ cannot be isomorphic. On the other hand, assuming the Continuum Hypothesis $2^{\aleph_0} = \aleph_1$, we could actually prove that $K^*$ is isomorphic to $L^*$. So we would have the desired contradiction. It is, however, possible to obtain the contradiction even by proving less than isomorphism. Without the Continuum Hypothesis we shall proceed as follows:

Since $K^*$ and $L^*$ have residue characteristic 0, the identity isomorphism

$$\delta : \mathbb{Q} \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Q}$$

of the prime fields of $K^*$ and $L^*$ is clearly value-preserving, as $v^*$ and $w^*$ restricted to $\mathbb{Q}$ are trivial. Moreover, $\mathbb{Q}$ with this restriction is a henselian subfield of both $K^*$ and $L^*$. Now let $h_1 \in K^*[X_1, \ldots, X_{d^2+1}]$ be homogeneous

of degree $d$ but with no non-trivial zero in $K^*$. Denote by $c_1, \ldots, c_N$ the coefficients of $h_1$ in some fixed order. We shall show in Theorem 6.1.1 below that the isomorphism $\delta$ can be extended to a subfield

$$F_1 \supseteq \mathbb{Q}(c_1, \ldots, c_N)$$

of $K^*$, say to $\delta_1 : F_1 \longrightarrow\!\!\!\!\!\rightarrow F_2 \subseteq L^*$ such that $\delta_1$ is still value-preserving (i.e., $w^*(\delta_1(x)) = v^*(x)$ for all $x \in F_1$). Since $L^*$ is $C_2(d)$, the image polynomial $\delta_1(h_1) \in F_2[X_1, \ldots, X_{d^2+1}]$ has a non-trivial zero in $L^*$, say $x_1, \ldots, x_{d^2+1}$. Once again, by Theorem 6.1.1 we can extend the isomorphism $\delta_1^{-1} : F_2 \longrightarrow\!\!\!\!\!\rightarrow F_1$ to an embedding

$$\delta_2 : F_2(x_1, \ldots, x_{d^2+1}) \longrightarrow K^* \ .$$

But then $(\delta_2(x_1), \ldots, \delta_2(x_{d^2+1}))$ is a non-trivial zero of $h_1$ in $K^*$, giving the desired contradiction.

Before we state Theorem 6.1.1, let us repeat the assumptions, and at the same time make the situation symmetric. Thus for $i = 1, 2$, let

(1) $(K_i, v_i)$ *be henselian fields,*
(2) *both fields have the same residue class field* $k$ *of characteristic zero,*
(3) *both fields have the same value group* $\Gamma$*,*
(4) *both fields are* $\aleph_1$*-saturated* (Theorem A.6).

The structure of $k$ and of $\Gamma$ does actually not matter for the following arguments. When $\aleph_1$-saturatedness is needed, we shall refer to the Appendix A.

Under these assumptions we shall prove

**Theorem 6.1.1.** *Let $F$ be a subfield of $K_1$ and let $\sigma : F \longrightarrow K_2$ be a value-preserving embedding, meaning here: $v_2(\sigma(x)) = v_1(x)$ for all $x \in F$, and $\overline{\sigma(x)} = \overline{x}$ for all $x \in \mathcal{O}_{v_1} \cap F$. Assume that*

*(i) $F$ is countable and henselian with respect to $v_1|_F$,*
*(ii) $v_1(F)$ is pure in $\Gamma$, i.e., $\Gamma / v_1(F)$ is torsion free.*

*Then to $a_1, \ldots, a_m \in K_1$ there exists a value-preserving extension $\sigma' : F' \longrightarrow K_2$ of $\sigma$ such that $F(a_1, \ldots, a_m) \subseteq F'$ and $F'$ again satisfies (i) and (ii).*

In order to prove this theorem, we shall need

**Lemma 6.1.2.** *Let $F_0$ be a countable subfield of $K_1$. Then there exists a countable extension $F'$ of $F_0$ in $K_1$ such that $v_1(F')$ is pure in $\Gamma = v_1(K_1)$.*

*Proof.* Let $\Gamma_0 = v_1(F_0)$, and denote by $\widehat{\Gamma}_0$ its relative divisible hull in $\Gamma$, i.e.,

$$\widehat{\Gamma}_0 = \{\, \gamma \in \Gamma \mid m\gamma \in \Gamma_0 \text{ for some } m \geq 1 \,\} \ .$$

As $\Gamma_0$ is countable, so is $\widehat{\Gamma}_0$. Thus let $(\gamma_n)_{n \in \mathbb{N}}$ be an enumeration of all elements of $\widehat{\Gamma}_0$. We shall define an increasing sequence $F_n$ of countable subfields of $K_1$ with

$$\gamma_n \in v_1(F_{n+1}) \subseteq \widehat{\Gamma}_0 \ .$$

Thus $F' := \bigcup_n F_n$ is a countable subfield of $K_1$ with $v_1(F') = \widehat{\Gamma}_0$. Hence $v_1(F')$ is pure in $\Gamma$.

Assume we have already constructed $F_n$. We then construct $F_{n+1}$ such that $\gamma_n \in v_1(F_{n+1})$ and $v_1(F_{n+1}) \subseteq \widehat{\Gamma}_0$.

By the definition of $\widehat{\Gamma}_0$, $m\gamma_n \in \Gamma_0$ for some $m \geq 1$. Choose $x \in K_1$ such that $v_1(x) = \gamma_n$. Then

$$v_1(x^m) = m\gamma_n = v_1(a) \ ,$$

for some $a \in F_0^\times$. Hence $\overline{x^m/a} = \overline{c}$ for some $c \in K_1^\times$. Note that $c$ is not uniquely determined. This fact will be used later. Thus by Hensel's Lemma (observe that char $\overline{K}_1 = 0$), the polynomial

$$Z^m - \frac{x^m}{ac} \in K_1[Z]$$

has a zero in $K_1$, say $z$. Then define

$$F_{n+1} = F_n\left(c, \frac{x}{z}\right) = F_n(c, \sqrt[m]{ac}) \ ,$$

and observe that for the right choice of $c$ (see below) we get

$$\overline{F}_{n+1} = \overline{F}_n(\overline{c}) \qquad \text{and} \qquad \gamma_n \in v_1(F_{n+1}) \subseteq \widehat{\Gamma}_0 \ .$$

Indeed, let us first adjoin $c$ to $F_n$. If $\overline{c}$ is algebraic over $\overline{F}_n$, let $\overline{f}(X)$ be the minimal polynomial of $\overline{c}$ over $\overline{F}_n$. Then $f(X)$ remains irreducible over $F_n$, and by Hensel's Lemma it also has a zero in $K_1$ with residue $\overline{c}$. Thus let us choose $c$ to be this zero. Then $[F_n(c) : F_n] = \deg f$. Hence by Corollary 3.2.3 we find $\overline{F_n(c)} = \overline{F}_n(\overline{c})$ and $v_1(F_n(c)) = v_1(F_n)$. If, however, $\overline{c}$ is transcendental over $\overline{F}_n$, then also $c$ is transcendental over $F_n$, and by Corollary 2.2.2 we get

$$\overline{F_n(c)} = \overline{F}_n(\overline{c}) \qquad \text{and} \qquad v_1(F_n(c)) = v_1(F_n) \ .$$

The extension $F_{n+1}/F_n(c)$ is algebraic. Hence by Theorem 3.2.4, $v_1(F_{n+1})$ is torsion over $v_1(F_n)$, and thus $v_1(F_{n+1}) \subseteq \widehat{\Gamma}_0$. Clearly

$$\gamma_n = v_1(x) = v_1\left(\frac{x}{z}\right) \in v_1(F_{n+1}) \ . \qquad \square$$

*Proof of Theorem 6.1.1.* We first apply Lemma 6.1.2 to the subfield $F_0 = F(a_1, \ldots, a_m)$ of $K_1$ in order to obtain an extension $F' \subseteq K_1$ of $F_0$ such that $\Gamma' := v_1(F')$ is pure in $\Gamma = v_1(K_1)$. Since the henselization of a field is an immediate extension, we may even have that $F'$ is henselian with respect to $v_1|_{F'}$ (note that $(K_1, v_1)$ is henselian). Clearly $F'$ is countable. It remains to extend $\sigma : F \longrightarrow K_2$ to a value-preserving embedding $\sigma' : F' \longrightarrow K_2$. By Zorn's Lemma we know that there exists a maximal value-preserving extension

$$\sigma'' : M \longrightarrow K_2 \,,$$

with $M \subseteq F'$ and $v_1(M)$ pure in $\Gamma'$. Note that $v_1(F)$ is pure in $\Gamma'$. From the maximality of $\sigma''$ and the uniqueness of the henselian closure it follows that $M$ is henselian with respect to $v_1|_M$. We assume that $M \neq F'$ and distinguish three cases, each of which will lead to a contradiction. This will then prove our claim.

*Case 1:* There exists $x \in F'$ such that $\overline{x} \in \overline{F'} \setminus \overline{M}$.

As in the proof of Lemma 6.1.2, we first assume that $\overline{x}$ is algebraic over $\overline{M}$ with minimal polynomial $\overline{f}(X)$. By Hensel's Lemma, $f(X)$ has a zero in $F'$ lying over $\overline{x}$. Thus we may assume that $x$ is this zero. By the same argument, the image polynomial $\sigma''(f)(X)$ has a zero in $K_2$, say $y$, lying also over $\overline{x}$. Note that the image polynomial also yields the residue polynomial $\overline{f}$. The embedding $\sigma''$ therefore extends to an embedding $\sigma'''$ of $M(x)$ into $K_2$ by sending $x$ to $y$. As $M$ is henselian with respect to $v_1|_M$, the valuation $v_1|_{M(x)}$ is its only possible extension to $M(x)$. Thus the embedding is value-preserving, and we have $v_1(M(x)) = v_1(M)$.

If $\overline{x}$ is transcendental over $\overline{M}$, then $x$ is also transcendental over $M$, and, if we choose $y \in K_2$ such that $\overline{y} = \overline{x}$, $y$ is transcendental over $\sigma''(M)$. Thus sending $x$ to $y$ extends $\sigma''$ to $M(x)$, and by Corollary 2.2.2 this extension is value-preserving, with $v_1(M(x)) = v_1(M)$. In both cases, the existence of the extension $\sigma''' : M(x) \longrightarrow K_2$ contradicts the maximality of $\sigma''$.

*Case 2:* $\overline{F'} = \overline{M}$, and there exists $x \in F'$ with $v_1(x) \notin v_1(M)$.

As $v_1(M)$ is pure in $\Gamma'$, the sum $v_1(M) + \mathbb{Z}v_1(x)$ is direct. In this case $x$ must be transcendental over $M$ and the valuation $v_1|_{M(x)}$ is uniquely determined by

$$v_1(c_0 + c_1 x + \cdots + c_d x^d) = \min \{\, v_1(c_i) + i\gamma \mid 0 \leq i \leq d \,\} \,,$$

with $\gamma := v_1(x)$ and $c_0, \ldots, c_d \in M$ (cf. Corollary 2.2.3). Thus if we choose $y \in K_2$ with $v_2(y) = v_1(x)$, the extension of $\sigma''$ to $M(x)$ defined by sending $x$ to $y$ is again value-preserving. In order to obtain also in this case a contradiction to the maximality of $\sigma''$, we have to extend

$$\sigma''' : M(x) \longrightarrow K_2$$

still further, to a subfield $M^*$ of $F'$ such that $v_1(M^*)$ is pure in $\Gamma'$.

Here we can just take for $M^*$ the relative algebraic closure of $M(x)$ in $F'$. To see this, let $\gamma = v_1(\alpha) \in v_1(F') = \Gamma'$, and assume that $m\gamma = v_1(a)$ for some $m \geq 1$ and some $a \in M(x)$. Then $\alpha^m a^{-1}$ has value zero in $F'$, and thus

$$\overline{\alpha^m a^{-1}} = \overline{c} \,,$$

for some $c \in M(x)$, as $\overline{M(x)} = \overline{F'}$. Thus by Hensel's Lemma the polynomial $Z^m - \alpha^m/ac$ has a zero, say $z$, in $F'$. But then

$$\left(\frac{\alpha}{z}\right)^m = ac \in M(x) \,.$$

Thus $\alpha/z \in M^*$ and $\gamma = v_1(\alpha) = v_1(\alpha/z) \in v_1(M^*)$. Therefore $v_1(M^*)$ is pure in $\Gamma'$.

Now that we have $M^*$, we still have to extend $\sigma'''$ to $M^*$. Actually, we shall not do exactly this. Instead we show that $\sigma'' : M \longrightarrow K_2$ has a value-preserving extension to every finitely generated subfield of $M^*$. Then by the Saturation Theorem A.6 applied to $K_2$ we shall find[1] a value-preserving extension of $\sigma''$ to $M^*$.

By the choice of $M^*$, every subfield of $M^*$, finitely generated over $M$, is contained in some field

$$M(x, \alpha) \ ,$$

where $x$ is the transcendental element fixed at the beginning of 'Case 2', and $\alpha \in M^*$ is algebraic over $M(x)$. From the fact that

$$v_1(M(x)) = \mathbb{Z}v_1(x) \oplus v_1(M) \ ,$$

one deduces that also

$$v_1(M(x, \alpha)) = \mathbb{Z}v_1(z) \oplus v_1(M) \ ,$$

for some $z \in M^*$. Since $z$ has to be transcendental over $M$, we also find

$$v_1(M(z)) = \mathbb{Z}v_1(z) \oplus v_1(M) \ .$$

Hence $M(x, \alpha)$ is an immediate extension of $M(z)$ (recall that $\overline{M} = \overline{F'}$). Thus by Theorem 4.1.10, $M(x, \alpha)$ is contained in the henselization of $M(z)$. Therefore it suffices to find a value-preserving extension of $\sigma''$ to $M(z)$ (which then automatically extends to the henselization of $M(z)$). This, however, was already done at the beginning of 'Case 2' (replacing $x$ by $z$).

*Case 3:* $\overline{F'} = \overline{M}$, $v_1(M) = v_1(F')$, and $x \in F' \setminus M$.

Since the henselian field $M$ has no immediate extension by Theorem 4.1.10, $x$ must be transcendental over $M$. By our assumption, for every $a \in M$ there exists $b \in M$ such that

$$v_1(x - a) = v_1(b) \ .$$

We shall now proceed in two steps. In step 1 we find $y \in K_2$ such that

$$v_1(x - a) = v_2(y - \sigma''(a)) \ ,$$

for all $a \in M$. In step 2 we show that even

$$v_1(f(x)) = v_2(\sigma''(f)(y))$$

holds for all $f \in M[X]$. Then the extension of $\sigma''$ to $M(x)$ by sending $x$ to $y$ clearly is a value-preserving isomorphism. (Note that $\sigma''(f)(y) = 0$ would imply $v_1(f(x)) = \infty$, hence $f \equiv 0$.)

[1] This is explained just before stating Theorem A.6 in Appendix A.

*Step 1:* By the saturation property of $K_2$ it suffices to find, for every finite set $a_1, \ldots, a_m \in M$ with

$$v_1(x - a_i) = v_1(b_i)$$

(for suitably chosen $b_i \in M^\times$), an element $y \in K_2$ such that

$$v_2(y - \sigma''(a_i)) = v_2(\sigma''(b_i)) \; .$$

Then by Theorem A.6 there exists $y \in K_2$ with

$$v_2(y - \sigma''(a)) = v_2(\sigma''(b_a)) = v_1(b_a) = v_1(x - a)$$

for all $a \in M$.

Now let $v_1(x - a_1) = v_1(b_1)$ be maximal among the values $v_1(x - a_i)$, $1 \leq i \leq m$. Since $\frac{x-a_1}{b_1}$ is a unit, by our assumptions there exists $c \in M$ such that

$$\overline{\left(\frac{x - a_1}{b_1}\right)} = \overline{c} \; .$$

Hence

$$v_1(x - a_1 - b_1 c) > v_1(b_1) = v_1(x - a_1) \geq v_1(x - a_i) \; .$$

Taking $d = a_1 + b_1 c$ we find

$$v_1(d - a_i) = v_1((x - d) - (x - a_i)) = v_1(x - a_i) = v_1(b_i) \; ,$$

and hence

$$v_2(\sigma''(d) - \sigma''(a_i)) = v_2(\sigma''(b_i)) \; .$$

Thus $y = \sigma''(d)$ does the job for $a_1, \ldots, a_m$.

*Step 2:* By induction on $\deg f = d$ we prove

$$v_1(f(x)) = v_2(\sigma''(f)(y)) \; . \qquad (*)$$

The case $d = 1$ is just step 1. Let $d > 1$, and assume we have the identity $(*)$ for all polynomials of degree less than $d$. We then consider the $d$-dimensional $M$-vector space

$$V = M + Mx + \cdots + Mx^{d-1}$$

of polynomials over $M$ of degree $< d$. For each polynomial $f(x) \in V$ we have $(*)$, by the induction hypothesis. Thus it remains to consider irreducible polynomials $f$ of degree $d$.

The restriction of $v_1$ to $V$ yields a "valuation"

$$v_1 : V \longrightarrow\!\!\!\!\!\rightarrow \Gamma' \cup \{\infty\}$$

of the $M$-vector space $V$. Computing modulo $f$ introduces a multiplication on $V$ such that $V$ becomes isomorphic to the field $M[x]/(f) =: M_1$.

More precisely, for $g, h \in V$ their product is defined to be the uniquely determined $r \in V$ such that

$$gh = r + sf \ ,$$

for some $s \in V$.

If we now had

$$v_1(r) = v_1(g) + v_1(h) = v_1(gh) \ ,$$

for all $g, h \in V$, then clearly $v_1$ would define a valuation on $M_1$ such that $v_1(M_1) = \Gamma'$ and $\overline{M_1} = \overline{M}$. Thus we would obtain an immediate extension of $v_1|_M$ to the algebraic extension $M_1$ of $M$. By Theorem 4.1.10 this is impossible. Hence there must exist $g, h \in V$ such that

$$v_1(r) \neq v_1(gh) \ . \qquad (**)$$

This, however, implies $v_1(gh - r) = \min\{v_1(gh), v_1(r)\}$. Hence

$$v_1(f) = -v_1(s) + \min\{v_1(g) + v_1(h),\ v_1(r)\} \ . \qquad (+)$$

Substituting $y$ in the images of polynomials from $M[x]$ yields

$$\sigma''(gh)(y) = \sigma''(r)(y) + \sigma''(s)(y)\sigma''(f)(y) \ .$$

The induction hypothesis $(*)$ applied to $(**)$ yields

$$v_2(\sigma''(r)) \neq v_2(\sigma''(g)) + v_2(\sigma''(h)) = v_2(\sigma''(gh)) \ .$$

Hence

$$\begin{aligned} v_2(\sigma''(f)) &= -v_2(\sigma''(s)) + \min\{v_2(\sigma''(gh)), v_2(\sigma''(r))\} \\ &= -v_2(\sigma''(s)) + \min\{v_2(\sigma''(g)) + v_2(\sigma''(h)), v_2(\sigma''(r))\}. \qquad (++) \end{aligned}$$

Thus again by the induction hypothesis $(*)$, we can conclude from $(+)$ and $(++)$ that

$$v_2(\sigma''(f)) = v_1(f). \qquad \square$$

## 6.2 *p*-Adically Closed Fields

The notion of $p$-adically closed fields was introduced in 1965 by Ax and Kochen in connection with their "almost" solution of Artin's Conjecture (see Sect. 6.1 and [3]). Among other accomplishments in [3], they showed that $p$-adically closed fields are those fields that share all the 'algebraic' properties of the field $\mathbb{Q}_p$ of $p$-adic numbers, $p$ a fixed rational prime; this was analogous to

Artin and Schreier's introduction in 1926 of the class of real closed fields, which share all the 'algebraic' properties of $\mathbb{R}$. Independently of Ax-Kochen, also Y. Ershov (see [7]) introduced the $p$-adically closed fields in 1965. A more general approach to $p$-adically closed fields can be found in [21].

In order to make precise what we mean by 'algebraic' properties, we would have to introduce notions from Model Theory. Since, however, we want to keep this book as self-contained as possible, we shall prove only the basic algebraic theorems about $p$-adically closed fields. For the reader more advanced in model theory it then will be clear that we have actually proved that every $p$-adically closed field $K$ is 'elementarily equivalent' to $\mathbb{Q}_p$. The basic theorem to be shown below is the Embedding Theorem 6.2.3. It very much parallels the basic Theorem 6.1.1 from the last section. As an application of 6.2.3 we shall see, e.g., that for a fixed prime $p$ and a fixed positive integer $d$, the field $\mathbb{Q}_p$ is $C_2(d)$ if and only if every $p$-adically closed field $K$ is $C_2(d)$. Solvability of systems of equations (including also valuation conditions) transfers from one $p$-adically closed field to any other.

This transfer property in particular implies that the absolute Galois group $G(K^s/K)$ of a $p$-adically closed field is (as a profinite group) isomorphic to that of the field $\mathbb{Q}_p$. Actually, also the converse can be shown: the $p$-adically closed fields are exactly those fields having the same absolute Galois group as $\mathbb{Q}_p$. For the long history of this impressing theorem we refer the reader to [12].

Now, what is a *$p$-adically closed field*?

It is a henselian valued field $(K, v)$ such that

(i) the residue class field $\overline{K}$ is the finite prime field $\mathbb{F}_p$,
(ii) the value group $v(K)$ is discrete[2] with $v(p)$ as minimal positive element (hence $\operatorname{char} K = 0$), and
(iii) to every $m \geq 2$ and every $a \in K^\times$ there exists $\nu$ such that $0 \leq \nu \leq m-1$ and $v(ap^{-\nu})$ is divisible by $m$ in $v(K)$.

The last condition means that we can find $b \in K^\times$ such that $v(a) = v(p^\nu) + mv(b)$. Hence

$$a = ep^\nu b^m \ ,$$

for some unit $e \in O_v^\times$. If the value group $v(K)$ happens to be $\mathbb{Z}$ (with $v(p) = 1$), then we may clearly take $b = p^l$ and $\nu = v(a) - lm$, where we let

$$v(a) = lm + \nu$$

with $l \in \mathbb{Z}$ and $0 \leq \nu \leq m-1$.

Examples of $p$-adically closed fields are

(a) the field $\mathbb{Q}_p$ of $p$-adic numbers,

[2] Not necessarily of rank one! Recall that by "discrete" we only mean that there exists a minimal positive element.

(b) the field $\mathbb{Q}_p^a = \mathbb{Q}_p \cap \widetilde{\mathbb{Q}}$ of $p$-adic numbers algebraic over $\mathbb{Q}$,
(c) the field of Puiseux series over the $p$-adic numbers $\mathbb{Q}_p$, and
(d) the ultrapower $\mathbb{Q}_p^{\mathbb{N}}/\mathcal{F}$ with $\mathcal{F}$ an ultrafilter on $\mathbb{N}$.

Returning to the value group $v(K)$ of a $p$-adically closed field, we see from (ii) that $\mathbb{Z} \cong v(p)\mathbb{Z}$ is a convex subgroup of $v(K)$, and from (iii) that the (ordered) quotient

$$v(K)/\mathbb{Z}$$

is divisible. In fact, given $\gamma + \mathbb{Z} \in v(K)/\mathbb{Z}$, we choose $a \in K^\times$ with $v(a) = \gamma$. Then for each $m \geq 2$ we can find $b \in K^\times$ and $\nu \in \mathbb{Z}$ such that

$$\gamma - \nu = v(ap^{-\nu}) = mv(b) \ .$$

We leave it as an easy exercise to check that the converse also holds, i.e., if $v(K)$ satisfies (ii) and $v(K)/\mathbb{Z}$ is divisible, then (iii) holds.

The next lemma is very useful for finding more examples, and for what we are planning to prove.

**Lemma 6.2.1.** *Let $(K^*, v^*)$ be a $p$-adically closed field. For any subfield $K$ with induced valuation $v$, the following are equivalent:*

(1) *$(K, v)$ is $p$-adically closed,*
(2) *$K$ is relatively algebraically closed in $K^*$, and*
(3) *$v(K)$ is pure in $v^*(K^*)$ and $(K, v)$ is henselian.*

*Proof.* (3) $\Rightarrow$ (2): Is clear by Theorem 4.1.10. In fact, assume that $K$ had a proper finite extension $L$ inside $K^*$. Then by condition (3) and Theorem 3.2.4 (1), this extension would be immediate. This, however, contradicts Theorem 4.1.10, as $v^*|K$ is finitely ramified.

(2) $\Rightarrow$ (1): By (2), $K$ is henselian, since $K^*$ is so. It remains to prove condition (iii) of the definition of $p$-adically closed fields. Thus let $a \in K^\times$ and $m \geq 2$ be given. As $K^*$ is $p$-adically closed, there is $\nu$ such that $0 \leq \nu \leq m-1$ and $ap^{-\nu}$ has an $m$-divisible value in $v^*(K^*)$. Hence

$$v^*(\alpha^m) = v(ap^{-\nu}) \ ,$$

for some $\alpha \in K^*$. Thus $\beta := \alpha^m p^\nu / a$ has value zero in $K^*$. As $v(p) = 1$ is minimal positive in $v^*(K^*)$ and $\overline{K^*} = \mathbb{F}_p$, we can "develop" $\beta$ as

$$\beta = c_0 + c_1 p + \cdots + c_{2s} p^{2s} + \varrho \ ,$$

with $s \in \mathbb{N}$, $c_i \in \{0, \ldots, p-1\}$, $c_0 \neq 0$, and $v^*(\varrho) \geq 2s+1$. Let $d := c_0 + c_1 p + \cdots + c_{2s} p^{2s}$. Then $d \in K$ and $v(d) = 0$. From $v^*(\beta - d) \geq 2s+1$ we therefore get

$$v^*\left(1 - \frac{\beta}{d}\right) \geq 2s+1 \ .$$

Now we apply Hensel's Lemma (version (5) of Theorem 4.1.3) to the polynomial

$$f(X) = X^m - \frac{\beta}{d}$$

over the field $K^*$. If we choose $s = v(m)$ and substitute 1 for $X$, we find

$$2v(f'(1)) = 2v(m) = 2s < v\left(1 - \frac{\beta}{d}\right) = v(f(1)) \ .$$

Thus there exists $\varepsilon \in K^*$ such that $\varepsilon^m = \beta/d$. Hence

$$\left(\frac{\varepsilon}{\alpha}\right)^m = \frac{p^\nu}{ad} \in K \ .$$

By (2), this implies $\varepsilon/\alpha \in K$. Thus

$$v(ap^{-\nu}) = v(adp^{-\nu}) = mv\left(\frac{\alpha}{\varepsilon}\right) \in mv(K) \ .$$

(1) $\Rightarrow$ (3): Let $\gamma \in v^*(K^*)$, and assume $m\gamma = \delta \in v(K)$. Since $(K, v)$ is assumed to be $p$-adically closed, there exists $\nu$ such that $0 \leq \nu < m$ and

$$\delta - \nu = m\varepsilon \ ,$$

for some $\varepsilon \in v(K)$. Hence we have

$$\nu = m(\gamma - \varepsilon) \ .$$

This is possible only for $\nu = 0$, since $1 = v(p)$ is minimal positive also in $v^*(K^*)$. Thus we find $\delta = m\varepsilon$, and therefore $\gamma = \varepsilon \in v(K)$. □

The value groups of $p$-adically closed fields are sometimes called $\mathbb{Z}$-groups. To be more precise, an ordered abelian group $\Gamma$ is called a *$\mathbb{Z}$-group* if $\Gamma$ has a minimal positive element 1, and the quotient group $\Gamma/(1 \cdot \mathbb{Z})$ is divisible. The subgroup $1 \cdot \mathbb{Z}$ generated by 1 clearly is convex in $\Gamma$. Thus the ordering of $\Gamma$ canonically induces an ordering on $\Gamma/(1 \cdot \mathbb{Z})$. In the following we identify $1 \cdot \mathbb{Z}$ with $\mathbb{Z}$.

Divisibility of $\Gamma/\mathbb{Z}$ just means that, given $m \geq 2$, to every $\gamma \in \Gamma$ there exists $\nu \in \mathbb{Z}$ such that

$$\gamma - \nu = m\delta$$

for some $\delta \in \Gamma$. Clearly it suffices to choose $\nu$ from the set $\{0, 1, \ldots, m-1\}$. The next lemma is basic.

**Lemma 6.2.2.** *Let $\Delta$ be a subgroup of the $\mathbb{Z}$-group $\Gamma$. Assume $1 \in \Delta$. Then $\Delta$ is pure in $\Gamma$ if and only if $\Delta$ is a $\mathbb{Z}$-group.*

*Proof.* The proof of (1) $\Rightarrow$ (3) in Lemma 6.2.1 shows that $\Delta$ is pure in $\Gamma$ in case $\Delta$ is a $\mathbb{Z}$-group. Conversely, let $\Delta$ be pure in $\Gamma$. Fixing $m \geq 2$ and $\delta \in \Delta$, we find $\nu \in \mathbb{Z}$ and $\gamma \in \Gamma$ such that

$$\delta + \nu = m\gamma \ .$$

Since $\nu \in \Delta$, also $\delta + \nu \in \Delta$. Since $\Delta$ is pure in $\Gamma$, this implies $\gamma \in \Delta$. □

We are now able to prove the

**Embedding Theorem 6.2.3.** *Let $(K, v, \Gamma)$ and $(K_i, v_i, \Gamma_i)$ $(i = 1, 2)$ be p-adically closed fields. Assume that $(K, v, \Gamma) \subseteq (K_i, v_i, \Gamma_i)$ for $i = 1, 2$. Assume, moreover, that*

*(i) $K_1$ is countable, and*
*(ii) $(K_2, v_2, \Gamma_2)$ is an ultraproduct of p-adically closed fields, with respect to a non-principal ultrafilter.*

*Then there exists an embedding $\varrho : \Gamma_1 \longrightarrow \Gamma_2$ as ordered abelian groups with $\varrho|_\Gamma = \mathrm{id}$, and there exists a value-preserving embedding $\sigma : K_1 \longrightarrow K_2$ (i.e., $v_2(\sigma(x)) = \varrho(v_1(x))$ for all $x \in K_1$) with $\sigma|_K = \mathrm{id}$.*

*Proof.* We first assume that we already have obtained the embedding $\varrho : \Gamma_1 \longrightarrow \Gamma_2$, and thus identify $\Gamma_1$ with its image. Then we are in a similar position as in the proof of Theorem 6.1.1. Our $K_1$ here is the field $F'$ there, and the embedding $\sigma : F \longrightarrow K_2$ there is the identity on $K$ here. By Lemma 6.2.1, $v_1(K)$ is pure in $\Gamma_1$. As in the proof of 6.1.1 we then maximize the embedding $\mathrm{id} : K \longrightarrow K_2$ to an embedding of $K_1$ into $K_2$. The arguments are just the same. The most important reminder is that Theorem 4.1.10 also holds for valued fields with $v(p)$ minimal positive in the value groups.

Thus let us return to the embedding of $\Gamma_1$ into $\Gamma_2$ over $\Gamma$. All three groups are $\mathbb{Z}$-groups by assumption. Thus $\Gamma$ is pure in $\Gamma_1$. By Zorn's Lemma there exists a maximal order-preserving group-embedding

$$\tau : \Delta \longrightarrow \Gamma_2$$

of a pure subgroup $\Delta$ of $\Gamma_1$ with $\tau|_\Gamma = \mathrm{id}$. Assume that $\Delta \neq \Gamma_2$, say $\gamma \in \Gamma_2 \setminus \Delta$. Then the group $\Delta_\gamma$ generated from $\Delta$ and $\gamma$ is a direct sum

$$\Delta_\gamma = \mathbb{Z}\gamma \oplus \Delta \ .$$

We shall extend $\tau$ to $\Delta_\gamma$ in an order-preserving way by the saturatedness of $\Gamma_2$.

What is needed is some $\eta \in \Gamma_2$ such that

$$m\gamma + \delta > 0 \quad \text{iff} \quad m\eta + \tau(\delta) > 0, \tag{$*$}$$

for all $m \in \mathbb{Z}$ and all $\delta \in \Delta$.

If we have such an $\eta$, it cannot be torsion over $\tau(\Delta)$. Thus sending $\gamma$ to $\eta$ then yields an order-preserving group isomorphism

$$\tau_\gamma : \mathbb{Z}\gamma \oplus \Delta \longrightarrow \mathbb{Z}\eta \oplus \tau(\Delta) \subseteq \Gamma_2 \ .$$

In order to be able to apply the saturation property of Remark A.7, we need to realize finitely many conditions $(*)$ by some $\eta \in \Gamma_2$, i.e., we have to find some $\eta$ such that

$$m_i\gamma + \delta_i > 0 \quad \text{iff} \quad m_i\eta + \tau(\delta_i) > 0 \qquad (**)$$

for all $i$ such that $1 \leq i \leq n$. Passing to the divisible hull of $\Delta_\gamma$, the left hand side of $(**)$ becomes

$$\tfrac{1}{m'_1}\delta'_1, \ldots, \tfrac{1}{m'_s}\delta'_s < \gamma < \tfrac{1}{m''_1}\delta''_1, \ldots, \tfrac{1}{m''_r}\delta''_r, \qquad (+)$$

for certain elements $m'_i, m''_j \in \mathbb{N} \setminus \{0\}$ and $\delta'_i, \delta''_j \in \Delta$. It remains to find $\eta \in \Gamma_2$ satisfying the corresponding conditions on the right hand side of $(**)$.

By our assumption, $\tau$ is order-preserving. Thus the "position" of the elements $\delta'_i$ and $\delta''_j$ does not change by applying $\tau$. Therefore, assuming that $\frac{1}{m'_s}\delta'_s$ is maximal on the left hand side of $(+)$ (unless it is empty), and that $\frac{1}{m''_1}\delta''_1$ is minimal on the right hand side (unless it is empty), it follows that

$$\frac{1}{m'_s}\tau(\delta'_s) < \frac{1}{m''_1}\tau(\delta''_1)\ ,$$

and it suffices to find $\eta \in \Gamma_2$ between those two elements.

Let us assume that the left hand side of $(+)$ is nonempty. Then we have $\frac{1}{m}\delta < \gamma$ where we simply write $m$ for $m'_s$ and $\delta$ for $\delta'_s$. Since $\Delta$ is a $\mathbb{Z}$-group by Lemma 6.2.2, there exists $\nu \in \mathbb{N}$ such that $\delta = \nu + m\delta'$ for some $\delta' \in \Delta$. Choose $\mu \in \mathbb{N}$ such that $\frac{\nu}{m} < \mu$. Then we get

$$\frac{1}{m}\delta = \frac{\nu}{m} + \delta' < \mu + \delta' \leq \gamma\ .$$

The last inequality holds, since otherwise we would have

$$\frac{\nu}{m} + \delta' < \gamma < \mu + \delta'$$

or, equivalently,

$$\nu < m(\gamma - \delta') < m\mu\ .$$

This, however, implies that $m(\gamma - \delta') = t \in \mathbb{N}$, as $\mathbb{Z}$ is convex in $\Delta$. Hence $m\gamma = m\delta' + t \in \Delta$, contradicting the purity of $\Delta$ in $\Gamma_1$.

Thus we obtained

$$\frac{1}{m}\delta < \mu + \delta' \leq \gamma\ ,$$

and we may take $\eta := \mu + \tau(\delta')$ as realizing element on the right hand side of $(**)$. Thus we have extended $\tau$ to $\Delta_\gamma$.

In order to get a contradiction to the maximality of $\tau$, we still have to pass to the relative divisible hull of $\Delta_\gamma$ in $\Gamma_1$, i.e., to

$$\widehat{\Delta}_\gamma = \{\, \varepsilon \in \Gamma_1 \mid m\varepsilon \in \Delta_\gamma \text{ for some } m \in \mathbb{N} \,\}\ .$$

Here we use the same method as in the proof of Theorem 6.1.1, case 2. By the saturation of $\Gamma_2$ it suffices (Remark A.7) to prove that $\tau$ extends to every finitely generated subextension $\Delta'$ of $\widehat{\Delta}_\gamma/\Delta$. Adding $\gamma$ to $\Delta'$ if necessary, we have that $\Delta'/\Delta_\gamma$ is finite. Thus $\Delta' = \mathbb{Z}\gamma' \oplus \Delta$ for some $\gamma' \in \Gamma_2$ (same exercise as in the proof of Theorem 6.1.1, case 2). By what we just proved, $\tau$ extends to an order-preserving embedding of $\Delta'$ into $\Gamma_2$. Thus by saturatedness $\tau$ extends to $\widehat{\Delta}_\gamma$, contradicting the maximality of $\tau$. Hence $\Delta = \Gamma_1$ and we are done. □

As an application of the Embedding Theorem we shall now prove that the algebraic property $C_2(d)$ of a field carries over from one $p$-adically closed field to any other. In particular, for each $d \geq 1$, $\mathbb{Q}_p$ is $C_2(d)$ if and only if all $p$-adically closed fields are $C_2(d)$.

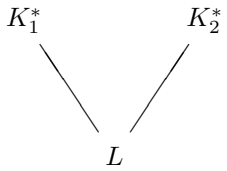
**Theorem 6.2.4.** *Let $(K_i, v_i)$ $(i = 1, 2)$ be $p$-adically closed fields, and let $d$ be a positive integer. Then $K_1$ is $C_2(d)$ if and only if $K_2$ is $C_2(d)$.*

*Proof.* In Appendix A we choose $S = \mathbb{N}$ and $\mathcal{F}$ a non-principal ultrafilter on $\mathbb{N}$. We then consider the ultrapowers

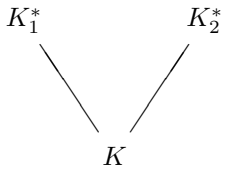
$$K_i^* := \prod_{s \in S} K_i^{(s)}/\mathcal{F} \qquad (i = 1, 2) \,,$$

where all the factors are the same, i.e., $K_i^{(s)} = K_i$. Then by Theorem A.4, $K_i^*$ is $C_2(d)$ if and only if $K_i$ is $C_2(d)$. Indeed, since all factors are equal, the set $\left\{ s \in \mathbb{N} \;\middle|\; K_i^{(s)} \text{ is } C_2(d) \right\}$ is either empty or equal to $\mathbb{N}$. Moreover, the valued fields $(K_i^*, v_i^*)$ are $p$-adically closed (Theorem A.4). Thus we may replace the valued fields $(K_i, v_i)$ by $(K_i^*, v_i^*)$. What we gain by this is the $\aleph_1$-saturatedness of $(K_i^*, v_i^*)$ (Theorem A.6). As in Sect. 6.1, we now assume that $K_1^*$ is not $C_2(d)$, while $K_2^*$ is $C_2(d)$. This will then lead to a contradiction.

In order to be able to apply the Embedding Theorem, we look for a common $p$-adically closed subfield of $K_1^*$ and $K_2^*$. This is obtained as follows. First observe that $\mathbb{Q}$ is a common subfield. The valuations $v_1^*$ and $v_2^*$ coincide on $\mathbb{Q}$ with the $p$-adic valuation $v_p$. The relative algebraic closures $L_i$ of $\mathbb{Q}$ in $K_i^*$ are $p$-adically closed by Lemma 6.2.1. Clearly, the valuations $v_i^*$ restricted to $L_i$ have value group $\mathbb{Z}$. Hence each $L_i$ with this valuation is a henselian immediate extension of $(\mathbb{Q}, v_p)$. Thus the $L_i$ are henselizations of $(\mathbb{Q}, v_p)$ (Theorem 4.1.10), therefore are value-preserving isomorphic (Theorem 5.2.2). Identifying $L_1$ with $L_2$ and simply writing $L$ for this field, we obtain the following diagram of $p$-adically closed fields



Now let $h \in K_1^*[X_1, \ldots, X_{d^2+1}]$ be a homogeneous polynomial of degree $d$ that has no non-trivial zero in $K_1^*$. Let $c_1, \ldots, c_N$ be the coefficients of $h$ in some fixed order. Next let $K$ be the relative algebraic closure of $L(c_1, \ldots, c_N)$ in $K_1^*$. Clearly, $K$ is countable, and by Lemma 6.2.1, $K$ is also $p$-adically closed. Thus by the Embedding Theorem we may embed $K$, in a value-preserving way, into $K_2^*$ over $L$. Let us identify $K$ with its image. Thus we have the new situation




i.e. $h$ is also a polynomial from $K_2^*[X_1, \ldots, X_{d^2+1}]$. By assumption, $h$ has a non-trivial zero in $K_2^*$, say $x_1, \ldots, x_{d^2+1}$. Now we interchange the role of $K_1^*$ and $K_2^*$, take the relative algebraic closure of $K(x_1, \ldots, x_{d^2+1})$ in $K_2^*$, and find an embedding $\sigma$ of this field into $K_1^*$ over $K$. But then $(\sigma(x_1), \ldots, \sigma(x_{d^2+1}))$ would be a non-trivial zero of $h$ in $K_1^*$. This is the desired contradiction. □

## 6.3 A Local-Global Principle for Quadratic Forms

In this section we shall first prove a general local-global principle for quadratic forms over arbitrary real fields and then specialize it to function fields over $\mathbb{R}$. In order to do so we begin with a brief introduction to quadratic forms and the so-called "semiorderings"[3].

Let $K$ be a field with $\operatorname{char} K \neq 2$. As usual we understand by a *quadratic form of dimension* $n$ over $K$ a homogeneous polynomial

$$\sum_{1 \leq i,j \leq n} a_{ij} X_i X_j$$

with symmetric coefficients $a_{ij} = a_{ji}$ from $K$. Two quadratic forms of dimension $n$ are called *isometric* if one is obtained from the other by an invertible homogeneous linear substitution. As one learns in linear algebra, every quadratic form of dimension $n$ over the field $K$ is isometric to a *diagonal* quadratic form

$$\varrho = \sum_{i=1}^{n} a_i X_i^2 \ .$$

Such a form is usually abbreviated by $\varrho = \langle a_1, \ldots, a_n \rangle$. If $\varrho$ represents 0 non-trivially, i.e., $0 = \sum_{i=1}^{n} a_i x_i^2$ for some $x_i \in K$, not all $x_i = 0$, then $\varrho$ is called *isotropic* in $K$. This notion is, of course, only interesting if $\varrho$ is regular, by

[3] See also [19].

what we mean that $a_i \neq 0$ for all $i \leq n$. By an ($m$-fold) multiple of $\varrho$ we mean the quadratic form

$$m\varrho := \langle a_1, \ldots, a_n, a_1, \ldots, a_n, \ldots, a_1, \ldots, a_n \rangle \ ,$$

where each entry is repeated $m$ times. $\varrho$ is called *weakly isotropic* if $m\varrho$ is isotropic for some $m \geq 1$. This just means that

$$0 = \sum_{i=1}^{n} \sigma_i a_i$$

where each $\sigma_i$ is a sum of $m$ squares from $K$ and at least one of these $nm$ squares is different from zero. This notion clearly is only interesting, if the field $K$ is real, i.e., if $\sum_{j=1}^{m} x_j^2 = 0$ always implies that all $x_i$ are 0. These are exactly the fields that admit at least one ordering (cf. [9], [15] and [20]). Thus let us assume that

*$K$ is a real field in this section .*

We are then going to present a general local-global principle, similar to the classical Hasse-Minkowski Principle, saying that a quadratic form $\varrho$ over $\mathbb{Q}$ is isotropic in $\mathbb{Q}$ if it is isotropic in all completions of $\mathbb{Q}$ with respect to its absolute values, i.e., $\varrho$ should be isotropic in $\mathbb{R}$ and in all $p$-adic number fields $\mathbb{Q}_p$. As we have seen that henselizations are a good substitution for completions in case of higher rank valuations, the following theorem in fact generalises the classical situation. It should be mentioned, however, that local-global principles for true isotropy (instead of weak isotropy) do hold only in very restricted situations, like e.g. for number fields or function fields in one variable over $\mathbb{R}$ (see [20], Theorem 3.4.12). Thus weak isotropy is the best we can hope for.

**Theorem 6.3.1.** *(Local-Global Principle for Weak Isotropy [4]). Let $K$ be a real field and $\varrho = \langle a_1, \ldots, a_n \rangle$ a regular quadratic form over $K$. Then $\varrho$ is weakly isotropic in $K$ if and only if $\varrho$ is (weakly) isotropic in $\mathbb{R}$ for every embedding of $K$ into $\mathbb{R}$ and $\varrho$ is weakly isotropic in every henselization $(K^h, v^h)$ of $(K, v)$ where $v$ is a non-trivial valuation on $K$ with real residue class field $\overline{K}$.*

For the proof we need two preparatory lemmas. The first one connects weak isotropy with so-called semiorderings. The second one connects semiorderings with valuations. Thus let us start by introducing semiorderings.

A subset $M$ of a field $K$ is called a *quadratic module* of $K$ if

(1) $M + M \subseteq M$
(2) $K^2 M \subseteq M$
(3) $1 \in M$ and $-1 \notin M$ .

[4] The principle is also known as the "Bröcker-Prestel Local-Global Principle"

For instance, if we let $M$ be the set $\Sigma K^2$ of finite sums of squares from the field $K$, we see at once that $M$ is a quadratic module of $K$ if and only if $-1$ is not a sum of squares in $K$, or equivalently if $K$ is real, i.e., admits an ordering. Another more general example is obtained when we consider the set of values of arbitrary multiples $m\varrho$ of a quadratic form $\varrho = \langle 1, a_1, \ldots, a_n \rangle$ with $a_1, \ldots, a_n \in K^\times$, i.e., the set

$$M = \{\sigma_0 + \sigma_1 a_1 + \cdots + \sigma_n a_n \mid \sigma_0, \ldots, \sigma_n \in \Sigma K^2\} .$$

This set is a quadratic module if $\varrho$ is not weakly isotropic in $K$. In fact, if $-1 \in M$, we would then have $-1 = \sigma_0 + \sigma_1 a_1 + \cdots + \sigma_n a_n$ or equivalently

$$0 = (1^2 + \sigma_0) + \sigma_1 a_1 + \cdots + \sigma_n a_n .$$

Hence $\varrho$ would be weakly isotropic.

A quadratic module $S$ of $K$ is called a *semiordering* of $K$, if $S$ satisfies in addition

$$(4) \quad S \cup -S = K$$
$$(5) \quad S \cap -S = \{0\} .$$

By Zorn's Lemma every quadratic module $M$ of $K$ is contained in a maximal such module $S$. This maximal quadratic module $S$ then has to be a semiordering. Indeed, if there existed some $a \in K$ such that neither $a$ nor $-a$ belonged to $S$, the two sets

$$S + a\Sigma K^2 \quad \text{and} \quad S - a\Sigma K^2$$

both contain $-1$. Otherwise at least one of them would be a quadratic module, properly containing $S$, which by the maximality of $S$ is impossible. Thus we find $s_1, s_2 \in S$ and $\sigma_1, \sigma_2 \in \Sigma K^2$ such that

$$-1 = s_1 + a\sigma_1 \quad \text{and} \quad -1 = s_2 - a\sigma_2 .$$

From these two equations we get

$$0 = \sigma_1(a\sigma_2) + \sigma_2(-a\sigma_1) = \sigma_1 + \sigma_1 s_2 + \sigma_2 + \sigma_2 s_1 ,$$

and hence $-\sigma_1 = \sigma_1 s_2 + \sigma_2 + \sigma_2 s_1 \in S$. But then

$$-1 = \sigma_1^{-1}(-\sigma_1) \in S ,$$

a contradiction. Note that we used here the elementary fact that the inverse of a sum of squares is again a sum of squares. In fact, if $\sigma_1 = \Sigma c_i^2$ then

$$\sigma_1^{-1} = \frac{\Sigma c_i^2}{\sigma_1^2} = \Sigma \left(\frac{c_i}{\sigma_1}\right)^2 .$$

This proves axiom (4) for $S$. In order to show (5), assume that $a \neq 0$ and $a, -a \in S$. Then also

$$-1 = a\left(\frac{a^{-1}-1}{2}\right)^2 - a\left(\frac{a^{-1}+1}{2}\right)^2 \in S\ ,$$

a contradiction.

Adding up what we have shown so far, we get

**Lemma 6.3.2.** *Let $\varrho = \langle 1, a_1, \ldots, a_n\rangle$ be a regular quadratic form over $K$. Then $\varrho$ is weakly isotropic in $K$ if and only if $\varrho$ is 'indefinite' with respect to every semiordering $S$ of $K$, i.e., $-a_i \in S$ for at least one $i \leq n$.*

*Proof.* If $\varrho$ is not weakly isotropic, then we just constructed a semiordering $S$ of $K$ with $a_1, \ldots a_n \in S$.

Conversely, if $\varrho$ is weakly isotropic in $K$, there are $\sigma_0, \ldots, \sigma_n \in \Sigma K^2$, not all $\sigma_i = 0$, such that

$$0 = \sigma_0 + a_1\sigma_1 + \cdots + a_n\sigma_n\ .$$

If then all $a_1, \ldots, a_n$ belonged to some semiordering $S$ of $K$ and say $\sigma_n \neq 0$, we would get

$$-a_n\sigma_n = \sigma_0 + \cdots + a_{n-1}\sigma_{n-1} \in S\ .$$

But then $a_n\sigma_n \in S \cap -S = \{0\}$, a contradiction. □

This lemma already gives a criterion for weak isotropy of $\varrho$. It is, however, not very informative as the totality of semiorderings of a field is in general much bigger than the collection of orderings, and even this set is very difficult to control.

As for orderings, we shall now see that semiorderings are intimately connected with valuations. To draw the parallel to orderings, let us first define

$$a \leq_S b \quad \text{iff } b - a \in S$$

where $S$ is a given semiordering of $K$. If it is clear to which semiordering we refer, we shall drop the index $S$ and simply write $a \leq b$. From the properties of $S$ we see immediately that $\leq$ defines a linear order on $K$ such that in addition we have for all $a, b, c \in K$:

$$\begin{aligned} &(i) \quad a \leq b \Longrightarrow a + c \leq b + c \\ &(ii) \quad 0 \leq a \Longrightarrow 0 \leq ac^2\ . \end{aligned}$$

Clearly every ordering as defined in Sect. 2.2.2 satisfies these conditions. The stronger property

$$(ii^*) \quad 0 \leq a, b \Longrightarrow 0 \leq ab$$

satisfied by all orderings need not be true for semiorderings. We shall call a linear order of $K$ satisfying (i) and (ii) as well a semiordering, since the set $S = \{x \in K \mid 0 \leq x\}$ then actually is a semiordering for our purpose.

**Lemma 6.3.3.** *Let $\leq$ be a semiordering on $K$. We then define*

$$\mathcal{O}(S) = \{x \in K \mid n - x, n + x \geq 0 \text{ for some } n \in \mathbb{N}\} .$$

*(a) If $\mathcal{O}(S) = K$, then $\leq$ is an archimedean ordering of $K$.*
*(b) If $\mathcal{O}(S) \neq K$, then $\mathcal{O}(S)$ is a non-trivial valuation ring of $K$; its maximal ideal is $\mathcal{M}(S) = \{x \in K \mid \frac{1}{n} - x, \frac{1}{n} + x \geq 0 \text{ for all } n \geq 1\}$.*

*Proof.* Before we can prove (a) and (b) we need to know more about how to work with semiorderings. We shall prove a sequence of elementary claims. First note that $0 < a$ implies $0 < aa^{-2} = a^{-1}$. Iterated use of this will show

$$0 < a < b \Longrightarrow ba^2 < ab^2 . \tag{6.3.1}$$

In fact, from $0 < b - a$ and $0 < a$ we get

$$0 < \frac{1}{\frac{1}{b-a} + \frac{1}{a}} \cdot b^2 = ab^2 - ba^2 . \tag{6.3.2}$$

From the conclusion of (6.3.2) we find

$$\frac{1}{b} = ba^2 \left(\frac{1}{ab}\right)^2 < ab^2 \left(\frac{1}{ab}\right)^2 = \frac{1}{a} .$$

Thus we have proved

$$0 < a < b \Longrightarrow 0 < b^{-1} < a^{-1} . \tag{6.3.3}$$

Observing that $n, n^{-1} \in \Sigma K^2$ for all natural numbers, we shall obtain

$$n < a < m \Longrightarrow n^2 < a^2 < m^2 . \tag{6.3.4}$$

In fact, from $a < m$ we obtain $ma^2 < am^2$ by (6.3.2), and thus $a^2 < am$ (dividing by the sum of squares $m$). In addition, multiplying $a < m$ by $m$ gives $am < m^2$. Together this yields $a^2 < m^2$. Similarly we conclude $n^2 < a^2$ from $n < a$.

(a) As for orderings one concludes from $\mathcal{O}(S) = K$ that the rational numbers are dense in $K$ with respect to $\leq$. What remains to be shown is $(ii^*)$.

Thus let $0 \leq a, b$ and assume that $a < b$. Setting $x = b - a$ and $y = b + a$, we get $0 < x < y$. Choose $n, m \in \mathbb{N}$ such that $x < \frac{n}{m} < y$. This then gives

$$mx < n < my .$$

Applying (6.3.4) yields $m^2x^2 < n^2 < m^2y^2$, and thus in particular

$$x^2 < y^2 .$$

Hence $(b - a)^2 < (b + a)^2$, which gives $0 \leq 4ab$. Therefore $0 \leq ab$.

(b) Clearly $\mathcal{O}(S)$ is closed under addition. By the equation

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

it suffices to show that $\mathcal{O}(S)$ is closed by squaring in order to find that $\mathcal{O}(S)$ is closed under multiplication. Thus if $x \in \mathcal{O}(S)$, we have $x, -x < n$ for some $n \in \mathbb{N}$. But then (6.3.4) implies $x^2 < n^2$. Hence $x^2 \in \mathcal{O}(S)$. Now (6.3.3) implies that $\mathcal{O}(S)$ is a valuation ring. Indeed, if $0 < x \notin \mathcal{O}(S)$, then $n < x$, and hence $0 < x^{-1} < \frac{1}{n}$ for all $n \geq 1$. Thus $x \in \mathcal{M}(S)$. Moreover, this gives the desired description of the maximal ideal $\mathcal{M}(S)$ of $\mathcal{O}(S)$. □

We are now ready for the

*Proof of Theorem 6.3.1.* For the non-trivial implication of the theorem assume that the regular quadratic form $\varrho = \langle 1, a_1, \ldots, a_n \rangle$ is not weakly isotropic in $K$. Then by Lemma 6.3.2 there exists a semiordering $S$ of $K$ such that $a_1, \ldots, a_n \in S$. Let $\leq$ be the linear order defined by $S$, i.e., $a \leq b$ iff $b - a \in S$. We then distinguish three cases.

*Case 1:* $\leq$ is archimedean:

Then by Lemma 6.3.3 (a), $(K, \leq)$ is order isomorphic to a subfield of $\mathbb{R}$ with the ordering induced from $\mathbb{R}$. Thus $\varrho$ cannot be (weakly) isotropic in $\mathbb{R}$, contrary to the assumption of the theorem.

*Case 2:* The valuation ring $\mathcal{O}(S)$ defined in Lemma 6.3.3 is non-trivial and has a rank 1 coarsening $\mathcal{O}$:

We then first observe that the maximal ideal $\mathcal{M}$ of $\mathcal{O}$ is convex with respect to $\leq$. Indeed, let $0 < x < y \in \mathcal{M}$ with $x \in K$. Then by (6.3.3) above, $0 < y^{-1} < x^{-1}$. Since $\mathcal{O}(S) \subseteq \mathcal{O}$, we have $\mathcal{M} \subseteq \mathcal{M}(S)$. Thus $y^{-1} \notin \mathcal{O}(S)$, and as $\mathcal{O}(S)$ is convex, $x^{-1} \notin \mathcal{O}(S)$. Therefore $1 < x^{-1}$, and thus $x^2 < x < y$. Hence we get $1 < \frac{y}{x^2}$.

On the other hand $x \notin \mathcal{M}$ would imply $x^{-1} \in \mathcal{O}$. This together with $y \in \mathcal{M}$ gives $\frac{y}{x^2} \in \mathcal{M} \subseteq \mathcal{M}(S)$. The convexity of $\mathcal{M}(S)$ thus gives $\frac{y}{x^2} < 1$, a contradiction.

Knowing that $\mathcal{M}$ is convex gives us the possibility to push the semiordering $S$ down to the residue class field $\overline{K} = \mathcal{O}/\mathcal{M}$: Let $S' = \overline{S \cap \mathcal{O}}$. We then immediately see all properties of a semiordering to be true for $S'$, except perhaps $-1 \in S'$. This however is impossible, because it would imply $1+s \in \mathcal{M}$ for some $s \in S$. Now $1 \leq 1 + s$ and the convexity of $\mathcal{M}$ imply $1 \in \mathcal{M}$, a contradiction.

Let $v$ be a rank 1 valuation with valuation ring $\mathcal{O}$, and let $(\widehat{K}, \widehat{v})$ be the completion of $(K, v)$. By Theorem 1.3.1 the completion is a henselian field. Thus by Corollary 4.1.5 and Corollary 5.2.3 the henselization $(K^h, v^h)$ is contained in $(\widehat{K}, \widehat{v})$. Thus if we can show that there is a semiordering $\widehat{S}$ on $\widehat{K}$ with $a_1, \ldots, a_n \in \widehat{S}$, the form $\varrho$ cannot be weakly isotropic in $K^h$. This then would contradict our assumption, since $(K, v)$ also has a real residue class field $\overline{K}$. (Note that $\overline{K}$ carries the semiordering $S'$.)

Let now $\widehat{S}$ be the topological closure of $S$ in $\widehat{K}$. In order to see that $\widehat{S}$ is a semiordering, the only non-obvious property is $\widehat{S} \cap -\widehat{S} = \{0\}$. As we have seen before Lemma 6.3.2, $0 \neq a \in \widehat{S} \cap -\widehat{S}$ would imply $-1 \in \widehat{S}$. But then there exists a sequence $a_n \in S$ such that $\lim_{n\to\infty} a_n = -1$. This, however, is impossible, since as we saw above, $1 + \mathcal{M} \subseteq S$ and thus $-1 + \mathcal{M} \subseteq -S$. Thus no $a_n \in S$ can ever enter into $-1 + \mathcal{M}$.

*Case 3:* The valuation ring $\mathcal{O}(S)$ has no rank 1 coarsening:

Then by Proposition 2.3.5 there is a neighbourhood system of 0 consisting of the maximal ideals $\mathcal{M}$ of non-trivial valuation rings $\mathcal{O}$, coarsening $\mathcal{O}(S)$. Since $a_1, \ldots, a_n \neq 0$ we may choose $\mathcal{O}$ such that

$$a_1, \ldots, a_n \in \mathcal{O} \setminus \mathcal{M} \ ,$$

i.e., they are all units in $\mathcal{O}$. Thus the quadratic form

$$\overline{\varrho} = \langle \overline{1}, \overline{a_1}, \ldots, \overline{a_n} \rangle$$

is a regular quadratic form over the residue class field $\overline{K} = \mathcal{O}/\mathcal{M}$.

As already seen in case 2, $S$ induces a semiordering $S' = \overline{S \cap \mathcal{O}}$ on $\overline{K}$. Thus $\overline{K}$ is real and all $\overline{a_1}, \ldots, \overline{a_n}$ lie in $S'$. Thus $\overline{\varrho}$ cannot be weakly isotropic in $\overline{K}$. But then $\varrho$ cannot be weakly isotropic in the henselization $K^h$ of $(K, \mathcal{O})$. In fact, assume that (taking $a_0 = 1$)

$$0 = \sum_{i=0}^{n} a_i \sum_{j=1}^{m_i} x_{ij}^2$$

with not all $x_{ij} \in K^h$ being zero. Let then $x_{i_0 j_0}$ have minimal value in the valuation corresponding to $\mathcal{O}^h$. After dividing by $x_{i_0 j_0}^2$ we obtain

$$0 = \sum_{i=0}^{n} a_i \sum_{j=1}^{m_i} y_{ij}^2$$

with $y_{ij} \in \mathcal{O}^h$ and $y_{i_0 j_0} = 1$. From the fact that $\overline{K^h} = \overline{K}$ and

$$\overline{0} = \sum_{i=0}^{n} \overline{a_i} \sum_{j=1}^{m_i} \overline{y}_{ij}^2$$

we conclude that $\overline{\varrho}$ is weakly isotropic in $\overline{K}$, a contradiction. □

By the above local-global principle the weak isotropy of the quadratic form $\varrho = \langle 1, a_1, \ldots, a_n \rangle$ in $K$ was reduced to the weak isotropy on henselian fields. The advantage of this reduction is that weak isotropy over a henselian valued field $(K, v)$ can be checked in the residue class field $\overline{K}$ of $(K, v)$. Such residue class fields are in general much simpler than the field $K$ itself. For instance the residue class field of the $p$-adic number field $\mathbb{Q}_p$ is the finite field $\mathbb{F}_p$. In

order to be more precise let us introduce the so-called "residue class forms" of a regular quadratic form $\varrho = \langle a_0, a_1, \ldots, a_n \rangle$ over $K$.

Let $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ be a non-trivial valuation of $K$. We first choose elements $c_i$ $(1 \le i \le s)$ such that the values $v(c_i)$ yield a set of representatives of the subset

$$\{v(a_\nu) + 2\Gamma \mid 0 \le \nu \le n\}$$

of $\Gamma/2\Gamma$. As a representative of $0 + 2\Gamma$ we always choose 1. We then group the elements $a_\nu$ $(0 \le \nu \le n)$ into blocks $a_{ij}$ $(1 \le i \le s,\ 1 \le j \le r_i)$ such that for fixed $i$ and all $j$

$$v(a_{ij}) \equiv v(c_i) \bmod 2\Gamma \ .$$

Next we choose elements $b_{ij} \in K^\times$ such that

$$a_{ij} c_i^{-1} b_{ij}^2 =: u_{ij}$$

is a unit in $(K, v)$, i.e., $v(u_{ij}) = 0$. Finally we see that the quadratic form $\varrho = \langle a_0, \ldots, a_n \rangle$ is isometric to the orthogonal sum

$$c_1 \varrho^{(1)} \perp \ldots \perp c_s \varrho^{(s)}$$

with $\varrho^{(i)} = \langle u_{i1}, \ldots, u_{ir_i} \rangle$. The regular quadratic forms

$$\overline{\varrho}^{(i)} := \langle \overline{u}_{i1}, \ldots, \overline{u}_{ir_i} \rangle$$

over $\overline{K}$ are called the *residue forms* of $\varrho$. Note that these forms are not uniquely determined, as the element $b_{ij}$ can only be chosen up to a unit. Thus $u_{ij}$ is determined only up to a unit square in $K^\times$. Concerning isotropy, this, however, is irrelevant. The form corresponding to $c = 1$ is called the *first residue form* of $\varrho$.

**Lemma 6.3.4.** *Let $(K, v)$ be a henselian field with non-trivial valuation $v$ and* $\operatorname{char} \overline{K} \ne 2$. *Then $\varrho$ is isotropic in $K$ if and only if at least one of the residue forms of $\varrho$ is isotropic in $\overline{K}$.*

*If $\overline{K}$ is real, the same holds for weak isotropy.*

*Proof.* Assume first that $\varrho$ is isotropic. Thus there exist $x_{ij} \in K$, not all zero, such that

$$\sum_{i=1}^{s} c_i \sum_{j=1}^{r_i} u_{ij} x_{ij}^2 = 0 \ .$$

One of the terms $c_i u_{ij} x_{ij}^2$ has minimal value in $(K, v)$, say $c_1 u_{11} x_{11}^2$. We then divide by $c_1 x_{11}^2$, and obtain

$$\sum_{i=1}^{r_1} u_{ij} \Big(\frac{x_{ij}}{x_{11}}\Big)^2 + \sum_{i=2}^{s} \sum_{j=1}^{r_i} \frac{c_i}{c_1} u_{ij} \Big(\frac{x_{ij}}{x_{11}}\Big)^2 = 0 \ .$$

Passing to the residue class field, gives

$$\sum_{j=1}^{r_1} \overline{u}_{1j} \overline{\left(\frac{x_{ij}}{x_{11}}\right)}^2 = 0 \ ,$$

as the terms in $\sum_{i=2}^{s} \dots$ all have positive values. Thus we have shown that the residue class form $\overline{\varrho}^{(1)}$ is isotropic in $\overline{K}$.

Conversely, let some residue class form $\overline{\varrho}^{(i)}$ of $\varrho$ be isotropic in $\overline{K}$, say $\overline{\varrho}^{(1)}$. Thus we get

$$\sum_{j=1}^{r_1} \overline{u}_{1j} \overline{z}_{1j}^2 = 0$$

for some $z_{1j} \in \mathcal{O}_v$, not all lying in $\mathcal{M}_v$. Say $z_{11} \in \mathcal{O}_v^\times$. Hence the quadratic polynomial

$$f(Z) = u_{11} Z^2 + \sum_{j=2}^{r_1} u_{1j} z_{1j}^2$$

has a simple zero in $\overline{K}$ (note that $\operatorname{char} \overline{K} \neq 2$). Thus by Hensel's Lemma 4.1.3 (4), we find $z \in K^\times$ such that

$$0 = f(z) = u_{11} z^2 + \sum_{j=2}^{r_1} u_{1j} z_{1j}^2 \ .$$

This clearly implies that $\varrho$ is isotropic.

Concerning weak isotropy, we just deal with a suitable multiple $m\varrho$ of $\varrho$ and apply what we just proved. In order that a sum of squares only vanishes in $\overline{K}$ if all squares are zero, we need, however, the stronger assumption that $\overline{K}$ should be real. □

Let us now consider the case of a function field $F$ over $\mathbb{R}$, i.e., $F$ is finitely generated over $\mathbb{R}$. In this case every valuation $v$ of $F$ having a real residue class field must be trivial on $\mathbb{R}$ by Corollary 2.2.6. Thus the Dimension Inequality 3.4.3 applies. Hence the transcendence degree over $\mathbb{R}$ of the residue class field $\overline{F}$ must be strictly smaller than that of $F$. Hence the Local-Global Principle 6.3.1 together with Lemma 6.3.4 reduces the problem of weak isotropy in $F$ to fields of smaller transcendence degree over $\mathbb{R}$. It should be observed, however, that $\overline{F}$ need no longer be a function field over $\mathbb{R}$, i.e., in general we cannot guarantee that $\overline{F}$ is finitely generated over $\mathbb{R}$, even if $F/\mathbb{R}$ was. In case we have equality in the Dimension Inequality (3.4.2), i.e.,

$$\operatorname{tr.deg}(\overline{F}/\mathbb{R}) + \operatorname{rr}(v(F)) = \operatorname{tr.deg}(F/\mathbb{R}) \ ,$$

we know from Theorem 3.4.3 that $v(F)$ is a finitely generated $\mathbb{Z}$-module and $\overline{F}/\mathbb{R}$ is finitely generated.

In any case we can conclude from Corollary 3.4.6 that the valuation ring $\mathcal{O}_v$ admits a rank 1 coarsening $\mathcal{O}$. With this last information we can prove another version of the local-global principle above, which parallels even more the classical one from Hasse-Minkowski for number fields.

**Theorem 6.3.5.** *Let $K/\mathbb{R}$ be a proper field extension of finite transcendence degree, and let $\varrho = \langle 1, a_1, \ldots, a_n \rangle$ be a regular quadratic form over $K$. Then $\varrho$ is weakly isotropic in $K$ if and only if $\varrho$ is weakly isotropic in the completion of $K$ with respect to any non-archimedean absolute value of $K$.*

*Proof.* Let us check the conditions of Theorem 6.3.1. Since $K/\mathbb{R}$ is proper, $K$ contains transcendental elements over $\mathbb{R}$. Thus every ordering of $K$ has to be non-archimedean, or in other words, an embedding of $K$ into $\mathbb{R}$ is impossible. Thus it remains to show that $\varrho$ is weakly isotropic in the henselization $K^h$ of every valuation ring $\mathcal{O}$ of $K$ that has a real residue class field. As remarked above, there exists a rank 1 valuation $v$ of $K$ such that $\mathcal{O} \subseteq \mathcal{O}_v$. By assumption $\varrho$ is weakly isotropic in the completion $(\widehat{K}, \widehat{v})$ of $(K, v)$, say

$$0 = \sum_i a_i \sum_j x_{ij}^2 \quad (a_0 = 1)$$

with $x_{ij} \in \widehat{K}$, not all zero. Assume that $a_{i_0} x_{i_0 j_0}$ has minimal value in $(\widehat{K}, \widehat{v})$. Dividing by this term gives the equation

$$0 = 1 + \sum_{(i,j) \neq (i_0, j_0)} \frac{a_i}{a_{i_0}} y_{ij}^2, \quad \text{with } y_{ij} = \frac{x_{ij}}{x_{i_0 j_0}} \ .$$

As $K$ is dense in $\widehat{K}$, we may replace $y_{ij} \in \widehat{K}$ by some $z_{ij} \in K$ which are so close to $y_{ij}$ that

$$1 + b \quad \text{with } b = \sum_{(i,j) \neq (i_0, j_0)} \frac{a_i}{a_{i_0}} z_{ij}^2$$

lies in the maximal ideal of $\mathcal{O}_{\widehat{v}}$. Hence the polynomial $f(Z) = Z^2 + b$ has a simple zero in the residue class field of $\mathcal{O}_{\widehat{v}}$ which actually is $\overline{K}$.

By Corollary 4.1.5 and Corollary 5.2.3 the henselization $K^h$ of $(K, v)$ is contained in $\widehat{K}$ and also has residue class field $\overline{K}$. Thus $f$ has a zero $z \in K^h$. This gives $0 = z^2 + b$ and thus

$$0 = a_{i_0} z^2 + \sum_{(i,j) \neq (i_0, j_0)} a_i z_{ij}^2 \ ,$$

showing that $\varrho$ is weakly isotropic in $K^h$. By showing now that the henselization of $(K, \mathcal{O})$ contains $K^h$, we shall finish the proof.

Let us extend $\mathcal{O}$ and $\mathcal{O}_v$ in such a way to $K^s$ that $\mathcal{O}^s$ is contained in $\mathcal{O}_v^s$ (see Lemma 3.1.5), and denote by $Z$ and $Z_v$ the decomposition groups of $\mathcal{O}$ and $\mathcal{O}_v$, respectively. By Galois theory it suffices to show that $Z \subseteq Z_v$. Let $\sigma \in Z$. As $\sigma(\mathcal{O}^s) = \mathcal{O}^s$, we get $v^s(x) = v^s(\sigma(x))$ for all $x \in K^s$ (cf. Proposition 3.2.16). Thus $\sigma$ fixes all prime ideals of $\mathcal{O}^s$ (as they are determined by their values, according to Lemma 2.3.1). Since $\mathcal{O}_v^s$ is a localization of $\mathcal{O}^s$ with respect to some prime ideal of $\mathcal{O}^s$, also the ring $\mathcal{O}_v^s$ remains fixed by $\sigma$, i.e., $\sigma \in Z_v$. □

# A

# Ultraproducts of Valued Fields

In this appendix we shall present a very useful but less known general construction in algebra – the ultraproduct of given algebraic structures. This method allows to form a kind of 'product'

$$A^* = \prod_{s \in S} A^{(s)}/\mathcal{F}$$

of given structures (all of the same type) indexed by elements $s$ from an infinite set $S$, 'modulo' an ultrafilter $\mathcal{F}$ on the collection of all subsets of $S$. The main properties of such a product are:

(I) an 'algebraic' statement $\mathcal{P}$ holds in $A^*$ if and only if it holds in $\mathcal{F}$-many factors, i.e., if the set $\{ s \in S \mid \mathcal{P} \text{ holds in } A^{(s)} \}$ belongs to $\mathcal{F}$;

(II) given a countable sequence of 'definable' subsets $M_i$ $(i \in \mathbb{N})$ of $A^*$; then the intersection $\bigcap_{i \in \mathbb{N}} M_i$ is non-empty if every finite subsequence $M_{i_1}, \ldots, M_{i_m}$ has a non-empty intersection ($\aleph_1$-*saturatedness*).

The precise meaning of 'algebraic' and 'definable' actually depends on the type of structures we consider.

The notion of ultraproduct was first introduced in Model Theory. There the meaning of 'structures', 'type', 'algebraic' and 'definable' gets a general definition in the framework of first-order logic. Since we shall need only special cases in our applications, we shall avoid these general notions and, instead, concentrate on the cases that interest us. Here we are working with valued fields. Thus it is not surprising that the structures of interest are

- fields
- ordered abelian groups
- valued fields.

In the following we introduce ultraproducts of valued fields. By restriction, it will then be clear to the reader how to introduce ultraproducts of fields and ordered abelian groups.

In this section we understand by a valued field a triple

$$(K, v, \Gamma) \ ,$$

where $K$ is a field, $\Gamma$ an ordered abelian group, and $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ is a valuation.

Let $S$ be an infinite set of indices (e.g., $S = \mathbb{N}$ or $S = \mathbb{P}$ = the set of all prime numbers). Assume that for any $s \in S$ we are given a valued field

$$\big(K^{(s)}, v^{(s)}, \Gamma^{(s)}\big) \ .$$

We then consider the direct products

$$K = \prod_{s\in S} K^{(s)} \quad \text{and} \quad \Gamma' = \prod_{s\in S} \big(\Gamma^{(s)} \cup \{\infty^{(s)}\}\big),$$

with operations defined componentwise on sequences

$$\big(a^{(s)}\big)_{s\in S} \in K \quad \text{and} \qquad \big(\gamma^{(s)}\big)_{s\in S} \in \Gamma' \ ,$$

respectively. We also consider the map $v : K \longrightarrow \Gamma'$ defined by

$$v\big(\big(a^{(s)}\big)_{s\in S}\big) := \big(v^{(s)}\big(a^{(s)}\big)\big)_{s\in S} \ .$$

Clearly $K$ is a commutative ring, but no field. We shall, however, obtain a field once we identify certain sequences $\big(a^{(s)}\big)_{s\in S}$ and $\big(b^{(s)}\big)_{s\in S}$ from $K$. Actually we shall introduce an equivalence relation on $K$ and "divide" through this relation. The equivalence classes then will form a field. In order to do so, we first need to introduce the notion of an ultrafilter on $S$.

A *filter* $\mathcal{F}$ on $S$ is a system of subsets of $S$ satisfying

$$\begin{aligned}
&\text{(F1)} \quad \emptyset \notin \mathcal{F}, \ S \in \mathcal{F} \\
&\text{(F2)} \quad U \in \mathcal{F}, \ V \in \mathcal{F} \quad \Longrightarrow \quad U \cap V \in \mathcal{F} \\
&\text{(F3)} \quad U \in \mathcal{F}, \ U \subseteq V \subseteq S \quad \Longrightarrow \quad V \in \mathcal{F}.
\end{aligned}$$

A filter $\mathcal{F}$ is called an *ultrafilter* if it satisfies in addition

$$\text{(F4)} \quad U \subseteq S, \ U \notin \mathcal{F} \quad \Longrightarrow \quad S \setminus U \in \mathcal{F}.$$

There are two important examples for a filter on $S$:

$$\begin{aligned}
&(1) \quad \mathcal{F}_a = \{\, U \subseteq S \mid a \in U \,\}, a \in S \text{ fixed} \\
&(2) \quad \mathcal{F}_{\mathrm{cf}} = \{\, U \subseteq S \mid S \setminus U \text{ is finite} \,\} \ .
\end{aligned}$$

The filter $\mathcal{F}_a$ above is actually an ultrafilter; it is called a *principal* ultrafilter. One easily sees that an ultrafilter $\mathcal{F}$ containing $\mathcal{F}_{\mathrm{cf}}$, the filter of *cofinite* sets, cannot be principal; conversely, an ultrafilter containing a finite subset of $S$ is principal. We shall be mainly interested in non-principal ultrafilters.

By Zorn's Lemma, every filter may be extended to a maximal one (with respect to inclusion).

**Lemma A.1.** *Every maximal filter $\mathcal{F}$ on $S$ is an ultrafilter. If $\mathcal{F}$ is a maximal filter containing $\mathcal{F}_{cf}$, then $\mathcal{F}$ is a non-principal ultrafilter.*

*Proof.* Let $\mathcal{F}$ be a maximal filter on $S$, and assume that $U \subseteq S$ is not a member of $\mathcal{F}$. What we will then do is to construct a new filter $\mathcal{F}'$ containing $\mathcal{F} \cup \{U'\}$, where $U' = S \setminus U$. Since $\mathcal{F}$ by assumption is maximal, it follows that $U' \in \mathcal{F}' = \mathcal{F}$.

In order to construct the extension filter $\mathcal{F}'$, consider first the set

$$\mathcal{U} = \mathcal{F} \cup \{\, U' \cap V \mid V \in \mathcal{F} \,\} .$$

This set satisfies (F1) and (F2), and contains $U'$. What is missing is (F3). Thus we simply add all bigger sets, i.e., we define

$$\mathcal{F}' = \{\, W \subseteq S \mid V \subseteq W \text{ for some } V \in \mathcal{U} \,\} .$$

Clearly, $\mathcal{F}'$ is a filter. □

Let us note two easy consequences of the ultrafilter axioms:

(F5) $U \notin \mathcal{F}$ iff $S \setminus U \in \mathcal{F}$

(F6) $U_1 \cup \cdots \cup U_n \in \mathcal{F} \implies U_i \in \mathcal{F}$ for some $1 \leq i \leq n$ .

Let us also note an important corollary to the proof of Lemma A.1.

**Corollary A.2.** *To every infinite subset $U'$ of $S$ there exists a non-principal ultrafilter $\mathcal{F}$ on $S$ such that $U' \in \mathcal{F}$.*

*Proof.* As above let $\mathcal{F}_{\mathrm{cf}}$ be the filter of cofinite subsets of $S$. If $U' \notin \mathcal{F}_{\mathrm{cf}}$, then we pass to the filter $\mathcal{F}'$ of the last proof and take a maximal extension $\mathcal{F}$ of $\mathcal{F}'$. By Lemma A.1, $\mathcal{F}$ is an ultrafilter containing $\mathcal{F}_{\mathrm{cf}} \cup \{U'\}$. □

Let us return to the ultraproduct of the valued fields

$$(K^{(s)}, v^{(s)}, \Gamma^{(s)}) \quad (s \in S)$$

with respect to a fixed ultrafilter $\mathcal{F}$ on $S$. At a later stage we shall also require that $\mathcal{F}$ be non-principal.

We define a binary relation $\sim$ on the product $K$ as follows: for two sequences $\big(a^{(s)}\big)_{s\in S}$ and $\big(b^{(s)}\big)_{s\in S}$ from the fields $K^{(s)}$, we declare that

$$\big(a^{(s)}\big)_{s\in S} \sim \big(b^{(s)}\big)_{s\in S} \quad \text{iff} \quad \big\{\, s \mid a^{(s)} = b^{(s)} \,\big\} \in \mathcal{F} .$$

We also define the relation $\sim$ on the product $\Gamma'$ in an analogous way. The relation $\sim$ (whether the one on $K$ or the one on $\Gamma'$) is actually an equivalence relation. Transitivity of this relation is obtained as follows: if also $\big(b^{(s)}\big)_{s\in S} \sim \big(c^{(s)}\big)_{s\in S}$, then $\big\{\, s \bigm| b^{(s)} = c^{(s)} \,\big\} \in \mathcal{F}$. But then by (F2) and (F3), and

$$\left\{\, s \;\middle|\; a^{(s)} = b^{(s)} \,\right\} \cap \left\{\, s \;\middle|\; b^{(s)} = c^{(s)} \,\right\} \subseteq \left\{\, s \;\middle|\; a^{(s)} = c^{(s)} \,\right\},$$

we find $\left(a^{(s)}\right)_{s\in S} \sim \left(c^{(s)}\right)_{s\in S}$. Many of the proofs below use the same scheme of arguments. Therefore we shall sometimes not be as explicit as we were here.

In order to ease notations let us write from now on $\left(a^{(s)}\right)$ for a sequence $\left(a^{(s)}\right)_{s\in S}$. By $\left[\left(a^{(s)}\right)\right]$ we denote the equivalence class of the sequence $\left(a^{(s)}\right)$. Hence

$$\left[\left(a^{(s)}\right)\right] = \left[\left(b^{(s)}\right)\right] \quad \text{iff} \quad \left(a^{(s)}\right) \sim \left(b^{(s)}\right).$$

On the set of equivalence classes of $K$ we define the field operations by referring to representatives; e.g.,

$$\left[\left(a^{(s)}\right)\right] + \left[\left(b^{(s)}\right)\right] := \left[\left(a^{(s)} + b^{(s)}\right)\right].$$

As above, (F2) and (F3) imply that these definitions do not depend on the choice of the representatives from the equivalence classes. With these operations the set

$$K^* = \left\{\, \left[\left(a^{(s)}\right)\right] \;\middle|\; \left(a^{(s)}\right) \in K \,\right\}$$

inherits from $K$ the properties of a commutative ring.

Similarly we proceed with $\Gamma' = \prod_{s\in S}\left(\Gamma^{(s)} \cup \left\{\infty^{(s)}\right\}\right)$, and obtain that

$$\left\{\, \left[\left(\gamma^{(s)}\right)\right] \;\middle|\; \left(\gamma^{(s)}\right) \in \Gamma' \,\right\} = \Gamma^* \cup \{\infty^*\}, \tag{$*$}$$

with $\Gamma^* = \left\{\left[\left(\gamma^{(s)}\right)\right] \;\middle|\; \left(\gamma^{(s)}\right) \in \prod_{s\in S}\Gamma^{(s)}\right\}$ and $\infty^* = \left[\left(\infty^{(s)}\right)\right]$. Here $\Gamma^*$ inherits from $\prod_{s\in S}\Gamma^{(s)}$ the properties of an abelian group.

In order to see $(*)$, one should observe that for an arbitrary sequence $\left(\gamma^{(s)}\right)$ from $\Gamma'$, we have

$$\left\{\, s \;\middle|\; \gamma^{(s)} \in \Gamma^{(s)} \,\right\} \cup \left\{\, s \;\middle|\; \gamma^{(s)} = \infty^{(s)} \,\right\} = S,$$

and the union is disjoint. Thus by (F6) we have that either $\left[\left(\gamma^{(s)}\right)\right] \in \Gamma^*$, or $\left[\left(\gamma^{(s)}\right)\right] = \infty^*$. This is the first time that we use the assumption that $\mathcal{F}$ is an ultrafilter.

We still need an ordering on $\Gamma^* \cup \{\infty^*\}$. This is obtained by defining

$$\left[\left(\gamma^{(s)}\right)\right] \le \left[\left(\delta^{(s)}\right)\right] \quad \text{iff} \quad \left\{\, s \;\middle|\; \gamma^{(s)} \le \delta^{(s)} \,\right\} \in \mathcal{F}.$$

Again it is easy to check that this definition is independent of the choice of representatives. Clearly $\le$ is a partial ordering, i.e.,

$$\begin{aligned} &\gamma \le \gamma \\ &\gamma \le \delta, \quad \delta \le \gamma \quad \Longrightarrow \quad \gamma = \delta \\ &\gamma \le \delta, \quad \delta \le \varepsilon \quad \Longrightarrow \quad \gamma \le \varepsilon, \end{aligned}$$

for all $\gamma, \delta, \varepsilon \in \Gamma^* \cup \{\infty^*\}$. Moreover, we have

$$\gamma \le \delta \quad \Longrightarrow \quad \gamma + \varepsilon \le \delta + \varepsilon.$$

In order to see that this ordering is total we shall need again (F4).

**Lemma A.3.** *Let $\mathcal{F}$ be an ultrafilter on $S$. Then we get*

*(i) $K^*$ is a field, i.e., to every $a^* \in K^* \setminus \{0\}$ there exists $b^* \in K^*$ such that $a^*b^* = 1^*$.*

*(ii) $\leq$ is a total ordering on $\Gamma^* \cup \{\infty^*\}$, i.e., $\gamma^* \leq \delta^*$ or $\delta^* \leq \gamma^*$ for all $\gamma^*, \delta^* \in \Gamma^* \cup \{\infty^*\}$. In particular, $(\Gamma^*, \leq)$ is an ordered abelian group.*

By $1^*$ we mean the equivalence class of the constant sequence $(1)_{s\in S}$. Similarly, $0^* = [(0)_{s\in S}]$.

*Proof.* (i) Let $a^* = [(a^{(s)})] \neq 0^*$. Then $\{s \mid a^{(s)} = 0\}$ is not in $\mathcal{F}$. Hence by (F5), we get $\{ s \mid a^{(s)} \neq 0 \} \in \mathcal{F}$. If we define the sequence $(b^{(s)})$ by

$$b^{(s)} = \begin{cases} 1/a^{(s)} & \text{if } a^{(s)} \neq 0 \\ 0 & \text{otherwise} , \end{cases}$$

we see that

$$\{ s \mid a^{(s)}b^{(s)} = 1 \} = \{ s \mid a^{(s)} \neq 0 \} \in \mathcal{F} .$$

Hence $\big[\big(a^{(s)}\big)\big]\big[\big(b^{(s)}\big)\big] = 1^*$.

(ii) Since $\Gamma^{(s)} \cup \{\infty^{(s)}\}$ is totally ordered for each $s \in S$, we get

$$\{ s \mid \gamma^{(s)} \leq \delta^{(s)} \} \cup \{ s \mid \delta^{(s)} \leq \gamma^{(s)} \} = S \in \mathcal{F} .$$

Thus by (F6), at least one of those sets is in $\mathcal{F}$. Hence $\gamma^* \leq \delta^*$ or $\delta^* \leq \gamma^*$. □

Finally, it is easy to see that the map $v^* : K^* \longrightarrow \Gamma^* \cup \{\infty^*\}$ defined by

$$v^*([(a^{(s)})]) = [(v^{(s)}(a^{(s)}))]$$

is actually well-defined and yields a valuation on $K^*$ with values in $\Gamma^* \cup \{\infty^*\}$. As an example, let us check the third axiom:

$$v^*(a^*) \leq v^*(b^*) \quad \Longrightarrow \quad v^*(a^* + b^*) \geq v^*(a^*) .$$

Indeed, from the assumption we get that the set $\{ s \mid v^{(s)}\big(a^{(s)}\big) \leq v^{(s)}\big(b^{(s)}\big) \}$ belongs to $\mathcal{F}$. Hence also the possibly bigger set

$$\{ s \mid v^{(s)}\big(a^{(s)} + b^{(s)}\big) \geq v^{(s)}\big(a^{(s)}\big) \}$$

belongs to $\mathcal{F}$, showing that $v^*(a^* + b^*) \geq v^*(a^*)$. Thus we end up with our valued field

$$(K^*, v^*, \Gamma^*) .$$

This field is called the *ultraproduct* of the valued fields $\big(K^{(s)}, v^{(s)}, \Gamma^{(s)}\big)$ $(s \in S)$. The value group $\Gamma^*$ is clearly the ultraproduct of the value groups $\Gamma^{(s)}$ $(s \in S)$. In order to indicate that $K^*$ and $\Gamma^*$ are products of fields and groups,

respectively, "modulo" the equivalence relation $\sim$ corresponding to $\mathcal{F}$, we also write

$$K^* = \prod_{s\in S} K^{(s)}/\mathcal{F} \quad \text{and} \quad \Gamma^* = \prod_{s\in S} \Gamma^{(s)}/\mathcal{F}\,.$$

Next we show that the ultraproduct $\prod_{s\in S} \overline{K^{(s)}}/\mathcal{F}$ of the residue class fields is actually the residue class field of the ultraproduct $K^*$. Recall that the valuation ring corresponding to $v^*$ is given by

$$\mathcal{O}^* = \{\, a^* \in K^* \mid v^*(a^*) \geq 0^* \,\}\,.$$

Let us define the map

$$^- : \mathcal{O}^* \longrightarrow \prod_{s\in S} \overline{K^{(s)}}/\mathcal{F}$$

by $\overline{a^*} := \big[\big(\overline{a^{(s)}}\big)\big]$. Clearly, this map is well-defined,[1] and is a homomorphism from the ring $\mathcal{O}^*$ to the field $\prod_{s\in S} \overline{K^{(s)}}/\mathcal{F}$. Its kernel consists of those equivalence classes $\big[\big(a^{(s)}\big)\big]$ for which $\big\{\, s \;\big|\; \overline{a^{(s)}} = 0 \,\big\} \in \mathcal{F}$; i.e., it consists of the maximal ideal $\mathcal{M}^*$ of $\mathcal{O}^*$. Hence the residue class field $\overline{K}^*$ of $(K^*, v^*, \Gamma^*)$ is the ultraproduct $\prod_{s\in S} \overline{K^{(s)}}/\mathcal{F}$.

We now come to property (I) of the beginning of the section. As already mentioned above, we shall not try to define what is meant by an 'algebraic' property. Instead we just prove (I) for those properties used in Sects. 6.1 and 6.2.

**Theorem A.4.** *Let $(K^*, v^*, \Gamma^*)$ be the ultraproduct defined above. Then*

*(i)* $\operatorname{char} K^* = p$ *iff* $\big\{\, s \;\big|\; \operatorname{char} K^{(s)} = p \,\big\} \in \mathcal{F}$ *(with $p \in \mathbb{P}$ fixed); similarly for $\overline{K^*}$;*

*(ii)* $K^*$ *is $C_2(d)$ iff* $\big\{\, s \;\big|\; K^{(s)}$ *is $C_2(d)$* $\big\} \in \mathcal{F}$*;*

*(iii)* $K^*$ *is not $C_2(d)$ iff* $\big\{\, s \;\big|\; K^{(s)}$ *is not $C_2(d)$* $\big\} \in \mathcal{F}$*;*

*(iv) if all $K^{(s)}$ are henselian, then so is $K^*$;*

*(v) if all $K^{(s)}$ are p-adically closed, then so is $K^*$ (with $p \in \mathbb{P}$ fixed).*

*Proof.* (i) follows at once from the equivalence

$$\underbrace{1^* + \cdots + 1^*}_{p \text{ times}} = 0^* \quad \text{iff} \quad \Big\{\, s \;\Big|\; \underbrace{1 + \cdots + 1}_{p \text{ times}} = 0 \text{ in } K^{(s)} \,\Big\} \in \mathcal{F}\,.$$

(ii): We first assume that $\big\{\, s \;\big|\; K^{(s)}$ is $C_2(d)$ $\big\} \in \mathcal{F}$, and show that $K^*$ is also $C_2(d)$. Thus let $m = d^2 + 1$ and $h \in K^*[X_1, \ldots, X_m]$ be homogeneous of degree $d$. Let $c_1^*, \ldots, c_N^*$ be the coefficients of $h$ (in some order). Fixing

[1] If the sequence $\big(a^{(s)}\big)$ represents $a^* \in \mathcal{O}^*$, then the set $A = \big\{\, s \;\big|\; v^*\big(a^{(s)}\big) \geq 0 \,\big\}$ belongs to $\mathcal{F}$. Thus only for $s \in A$ is the residue class $\overline{a^{(s)}}$ defined. This, however, creates no problem, as we may simply replace $a^{(s)}$ by 0 for $s \notin A$, and thus obtain another sequence also representing $a^*$.

a representing sequence $\big(c_i^{(s)}\big)$ for each $c_i^*$ and replacing the coefficients $c_i^*$ in $h$ by $c_i^{(s)}$, we obtain for each $s \in S$ a homogeneous polynomial $h^{(s)} \in K^{(s)}[X_1, \ldots, X_m]$. The set $A = \big\{ s \bigm| h^{(s)} \text{ has a non-trivial zero in } K^{(s)} \big\}$ contains the set $\big\{ s \bigm| K^{(s)} \text{ is } C_2(d) \big\}$, and hence belongs to $\mathcal{F}$. For each $s \in A$ we choose a non-trivial zero $\big(a_1^{(s)}, \ldots, a_m^{(s)}\big) \in \big(K^{(s)}\big)^m$ of $h^{(s)}$, and define the equivalence classes $a_i^* := \big[\big(a_i^{(s)}\big)\big]$, for $1 \le i \le m$ (cf. footnote 1). Then $(a_1^*, \ldots, a_m^*)$ is a non-trivial zero of $h$. In fact,

$$\big\{ s \bigm| h^{(s)}\big(a_1^{(s)}, \ldots, a_m^{(s)}\big) = 0 \big\} \in \mathcal{F}$$

shows that $(a_1^*, \ldots, a_m^*)$ is a zero of $h$. It remains to see that at least one $a_i^*$ is different from 0. This, however, follows from

$$\big\{ s \bigm| a_1^{(s)} \neq 0 \big\} \cup \cdots \cup \big\{ s \bigm| a_m^{(s)} \neq 0 \big\} \supseteq A$$

and $(F6)$.

Next, we assume that $\big\{ s \bigm| K^{(s)} \text{ is } C_2(d) \big\}$ is not in $\mathcal{F}$. Then by $(F5)$, $B = \big\{ s \bigm| K^{(s)} \text{ is not } C_2(d) \big\} \in \mathcal{F}$. We consider the general homogeneous polynomial $h_{m,d}$ of degree $d$ in the variables $X_1, \ldots, X_m$ (recall $m = d^2 + 1$), with general coefficients $C_1, \ldots, C_N$ (in some fixed order). For every $s \in B$ we choose a set of coefficients $c_1^{(s)}, \ldots, c_N^{(s)} \in K^{(s)}$ such that the homogeneous polynomial

$$h^{(s)} = h_{m,d}\big(c_1^{(s)}, \ldots, c_N^{(s)}; X_1, \ldots, X_m\big)$$

has only the trivial zero in $K^{(s)}$.

Now we form the equivalence classes $c_i^* = \big[\big(c_i^{(s)}\big)\big]$ for $1 \le i \le N$ (cf. footnote 1), and define

$$h = h_{m,d}(c_1^*, \ldots, c_N^*; X_1, \ldots, X_m) \; .$$

This homogeneous polynomial over $K^*$ is of degree $d$ and has no non-trivial zero in $K^*$. Indeed, since

$$\big\{ s \bigm| c_1^{(s)} \neq 0 \big\} \cup \cdots \cup \big\{ s \bigm| c_N^{(s)} \neq 0 \big\} \supseteq B \; ,$$

it follows from (F6) that at least one $c_i^*$ is non-zero. Thus $h$ has degree $d$. Assume that $a_1^*, \ldots, a_m^* \in K^*$ is a non-trivial zero of $h$, i.e., $h(a_1^*, \ldots, a_m^*) = 0^*$ and $a_1^* \neq 0^*$ or $\ldots$ or $a_m^* \neq 0^*$. From this it follows that

$$C = \big\{ s \bigm| h^{(s)}\big(a_1^{(s)}, \ldots, a_m^{(s)}\big) = 0 \big\} \cap \big( \big\{ s \bigm| a_1^{(s)} \neq 0 \big\} \cup \cdots \cup \big\{ s \bigm| a_m^{(s)} \neq 0 \big\} \big) \in \mathcal{F} \; .$$

Then also $C \cap B \in \mathcal{F}$. Hence $C \cap B \neq \emptyset$, which contradicts the choice of the $h^{(s)}$ for $s \in B$.

(iii) follows from (ii) by (F5).

(iv): Let $\big(K^{(s)}, v^{(s)}, \Gamma^{(s)}\big)$ be henselian. In order to show that $(K^*, v^*, \Gamma^*)$ is henselian, we use (7) of Theorem 4.1.3. Thus let

$$f(X) = X^{n+1} + X^n + c^*_{n-1}X^{n-1} + \cdots + c^*_0 \,,$$

with $c^*_i = \big[\big(c^{(s)}_i\big)\big] \in K^*$ and $v^*(c^*_i) > 0^*$. We want to find a zero $a^* \in K^*$ of $f$. By our assumption

$$A = \big\{\, s \;\big|\; v^{(s)}\big(c^{(s)}_0\big) > 0 \,\big\} \cap \cdots \cap \big\{\, s \;\big|\; v^{(s)}\big(c^{(s)}_{n-1}\big) > 0 \,\big\} \in \mathcal{F} \,.$$

By Theorem 4.1.3, for every $s \in A$ there exists a zero $b^{(s)} \in K^{(s)}$ of

$$f^{(s)}(X) = X^{n+1} + X^n + c^{(s)}_{n-1}X^{n-1} + \cdots + c^{(s)}_0 \,.$$

Defining

$$a^{(s)} = \begin{cases} b^{(s)} & \text{if } s \in A \\ 0 & \text{otherwise,} \end{cases}$$

it follows that

$$A \subseteq \big\{\, s \;\big|\; f^{(s)}\big(a^{(s)}\big) = 0 \,\big\} \,.$$

Thus the latter set belongs to $\mathcal{F}$ too, proving that $f(a^*) = 0^*$.

(v): By (iv), $K^*$ is henselian. Let $p^*$ be the equivalence class of the constant sequence $(p)_{s\in S}$. Then clearly $\underbrace{1^* + \cdots + 1^*}_{p \text{ times}} = p^*$, and $v^*(p^*) > 0$ since

$$\big\{\, s \;\big|\; v^{(s)}(p) > 0 \,\big\} = S \in \mathcal{F} \,.$$

Next we show that $v^*(p^*)$ is minimal positive in $\Gamma^*$, and that to every $m \geq 2$ and every $a^* \in K^*$ there exists a $\nu$ such that $0 \leq \nu < m$ and

$$v^*(a^*(p^*)^{-\nu}) = mv^*(b^*) \,,$$

for some $b^* \in K^*$. Assume that $\gamma^* = \big[\big(\gamma^{(s)}\big)\big] \in \Gamma^*$ is positive; i.e., $\big\{\, s \;\big|\; \gamma^{(s)} > 0 \,\big\} \in \mathcal{F}$. Then from

$$\big\{\, s \;\big|\; \gamma^{(s)} > 0 \,\big\} = \big\{\, s \;\big|\; \gamma^{(s)} \geq v^{(s)}(p) \,\big\}$$

we find $\gamma^* \geq v^*(p^*)$.

Next let $a^* = \big[\big(a^{(s)}\big)\big] \in K^* \smallsetminus \{0\}$, and fix $m \geq 2$. Then

$$\big\{\, s \;\big|\; v^{(s)}\big(a^{(s)}p^{-0}\big) \in m\Gamma^{(s)} \,\big\} \cup \cdots \cup \big\{\, s \;\big|\; v^{(s)}\big(a^{(s)}p^{-(m-1)}\big) \in m\Gamma^{(s)} \,\big\} = \big\{\, s \;\big|\; a^{(s)} \neq 0 \,\big\} \in \mathcal{F}.$$

By (F6) we see that one of these sets belongs to $\mathcal{F}$, say

$$B = \big\{\, s \;\big|\; v^{(s)}\big(a^{(s)}p^{-\nu}\big) \in m\Gamma^{(s)} \,\big\} \in \mathcal{F} \,.$$

If we choose

$$b^{(s)} = \begin{cases} \text{some } c^{(s)} & \text{with } v^{(s)}\big(a^{(s)}p^{-\nu}\big) = mv^{(s)}\big(c^{(s)}\big) \\ 0 & \text{otherwise,} \end{cases}$$

it follows that $B \subseteq \big\{\, s \;\big|\; v^{(s)}\big(a^{(s)}p^{-\nu}\big) = mv^{(s)}\big(b^{(s)}\big) \,\big\}$. Hence

$$v^*(a^*p^{-\nu}) = mv^*(b^*)\ .$$

It remains to prove that the residue class field of $K^*$ is $\mathbb{F}_p$. Thus let $a^* \in K^*$ have value $v^*(a^*) \geq 0$, and let $a^*$ be represented by the sequence $\big(a^{(s)}\big)$. Then $A = \big\{\, s \;\big|\; v^{(s)}(a^{(s)}) \geq 0 \,\big\} \in \mathcal{F}$. As all fields $K^{(s)}$ are supposed to be $p$-adically closed, we get

$$A = \big\{\, s \;\big|\; v^{(s)}\big(a^{(s)} - 0\big) > 0 \,\big\} \cup \cdots \cup \big\{\, s \;\big|\; v^{(s)}\big(a^{(s)} - (p-1)\big) > 0 \,\big\}\ .$$

Hence by (F6), $\big\{\, s \;\big|\; v^{(s)}\big(a^{(s)} - i\big) > 0 \,\big\} \in \mathcal{F}$, for some $i \in \{0, 1, \ldots, p-1\}$. Therefore $v^*(a^* - i) > 0$. This finishes the proof. □

The reader may wonder why we did not prove equivalences in (iv) and (v) above, and why we did not include $\operatorname{char} K^* = 0$ in (i). In particular, he may wonder whether these properties are not 'algebraic'. And the reader is actually right. Let us try to explain this.

The class of statements $\mathcal{P}$ for which (I) (p. 173) holds is quite narrow. It very much depends on the structures under consideration. The algebraic properties that work can be expressed by a single formula in a formal language suitably chosen for the given structures. For example, "$\operatorname{char} K = p$" is such a property. Also "$\operatorname{char} K \neq p$" works. Many other properties that every algebraist would immediately accept as an 'algebraic' property cannot be expressed by a single formula, but perhaps by infinitely many. Such a property is "$\operatorname{char} K = 0$". In fact, this can be expressed by an infinite collection of formulas, namely by "$\operatorname{char} K \neq p$," for all $p \in \mathbb{P}$. For such an infinite collection, (I) need not hold any longer. Other instances for such collections are "henselian" and "$p$-adically closed".

Returning to "$\operatorname{char} K = 0$", we actually have the following

**Corollary A.5.** *If $\mathcal{F}$ is a non-principal ultrafilter on $S = \mathbb{P}$, then the ultraproduct*

$$F^* = \prod_{p \in \mathbb{P}} \mathbb{F}_p / \mathcal{F}$$

*has characteristic zero.*

*Proof.* For a fixed prime $q$, the set $\{\, p \mid \operatorname{char} \mathbb{F}_p = q \,\}$ contains just one element. Hence it does not belong to $\mathcal{F}$. Therefore (F5) and (i) of Theorem A.4 imply $\operatorname{char} F^* \neq q$ for all primes $q$. Thus $\operatorname{char} F^* = 0$. □

The reader should note that in Corollary A.5, we restricted for the first time to a non-principal ultrafilter $\mathcal{F}$ on $S$. As we shall soon see, these filters

are responsible for the intersection property (II) mentioned at the beginning of this section.

Just as we did not give the most general version of (I), so also we shall not give the most general version for (II). We shall use only those 'definable' sets we need for the applications in Sects. 6.1 and 6.2. Moreover, it turns out that for our purpose it will be more convenient to work with 'definable' relations between countably many objects. Before giving the precise definitions, let us look at the application in Theorem 6.1.1, Case 2. There we considered an ultraproduct $(K_2, v_2, \Gamma_2)$ with respect to a non-principal ultrafilter. We already had a value-preserving embedding $\sigma''$ of a countable field $M$ into $K_2$. (Recall that $M$ was contained in the valued field $(K_1, v_1, \Gamma_1)$ having the same value group as $(K_2, v_2, \Gamma_2)$.) Moreover, we were given another countable subextension $M^*$ of $K_2/M$, and we wanted to extend $\sigma''$ to a value-preserving embedding of $M^*$ into $K_2$. We had already proved that $\sigma''$ is extendible to every finitely generated subextension of $M^*/M$ in a value-preserving way. Since these extensions may in general be incompatible, we have to look for a way to paste them together. This can be done by the $\aleph_1$-saturatedness of $(K_2, v_2, \Gamma_2)$, as proved in Theorem A.6 below.

Now what do we want? We want to assign to each element $a$ of $M^*$ an image $y^{(a)}$ in $K_2$ in such a way that we obtain a value-preserving embedding that coincides on $M$ with $\sigma''$. Thus the element $y^{(a)}$ is not yet determined. Therefore we treat it as an "indeterminate" corresponding to $a$. Since $M^*$ is countable, we may choose an injective enumeration $a_\nu \ \ (\nu \in \mathbb{N})$ of $M^*$.

Thus we have countably many indeterminates $Y_\nu$, one for each $a_\nu \in M^*$. Moreover, let

$$\gamma_\nu = v_1(a_\nu) \in \Gamma_1 = \Gamma_2 \ .$$

The basic "relations" we want to be respected are now chosen so that possible realizations $y_\nu$ of $Y_\nu$ in $K_2$ yield, via the assignment

$$a_\nu \overset{\tau}{\longmapsto} y_\nu \ ,$$

a value-preserving extension of $\sigma''$. These relations are

(1) $Y_\nu + Y_\mu = Y_\lambda$ if $a_\nu + a_\mu = a_\lambda$,
(2) $Y_\nu \cdot Y_\mu = Y_\lambda$ if $a_\nu \cdot a_\mu = a_\lambda$,
(3) $Y_\nu = \sigma''(a_\nu)$ if $a_\nu \in M$, and
(4) $v_2(Y_\nu) = \gamma_\nu$,

for all $\nu, \mu, \lambda \in \mathbb{N}$. If we are given realizations $y_\nu \in K_2$ for $Y_\nu (\nu \in \mathbb{N})$, then defining $\tau(a_\nu) = y_\nu$ yields a homomorphism from $M^*$ to $K_2$ by (1) and (2), extending $\sigma''$ by (3), and preserving values by (4). Clearly this homomorphism is injective, as $M^*$ is a field.

Theorem A.6 below will state that such a simultaneous realization $y_\nu$ for $Y_\nu$, for all $\nu \in \mathbb{N}$, can be found in $K_2$ if every finite subset $\mathcal{R}$ of the countably many relations (1)–(4) has a realization in $K_2$. This, however, is true, since $\mathcal{R}$ can only involve finitely many $Y_\nu$'s, say $Y_{\nu_1}, \ldots, Y_{\nu_t}$. We then consider the

finitely generated subfield $M(a_{\nu_1}, \dots a_{\nu_t})$ of $M^*$. By what we already proved, there exists a value-preserving embedding

$$\varrho : M(a_{\nu_1} \dots a_{\nu_t}) \longrightarrow K_2$$

extending $\sigma''$. Now the realization

$$y_{\nu_i} := \varrho(a_{\nu_i})$$

of $Y_{\nu_i}$ $(1 \le i \le t)$ respects the finite set $\mathcal{R}$ of relations.

What we just explained settles the application of $\aleph_1$-saturatedness in Theorem 6.1.1, Case 2. The application in Case 3 is even simpler. There we are only looking for a realization $y \in K_2$ of the relations

$$(4') \quad v_2(Y - \sigma''(a_\nu)) = v_2(\sigma''(b_\nu)) \ ,$$

where $a_\nu (\nu \in \mathbb{N})$ runs through an enumeration of all elements of $M$, and $b_\nu \in M^\times$ was chosen such that $v_1(x - a_\nu) = v_1(b_\nu)$. Thus here we have just one indeterminate $Y$, but still countably many relations. As we showed in the proof of Case 3, finitely many such relations are always realizable by some element of $K_2$. Thus by the saturation theorem A.6 below, there is a realization $y \in K_2$ for all relations $(4')$ simultaneously.

**Saturation Theorem A.6.** *Let $(K^*, v^*, \Gamma^*)$ be an ultraproduct of valued fields $\big(K^{(s)}, v^{(s)}, \Gamma^{(s)}\big)$, $s \in S$, with respect to a non-principal ultrafilter on $S$, and assume $S \subseteq \mathbb{N}$ (e.g., $S = \mathbb{P}$ or $S = \mathbb{N}$). Let $R_n$ $(n \in \mathbb{N})$ be a sequence of relations in the indeterminates $Y_\nu$ $(\nu \in \mathbb{N})$ with parameters from $K^*$ and $\Gamma^*$. If every finite set $R_0, \dots, R_m$ of relations has a realization for the $Y_\nu$ in $K^*$, then there is a realization $y_\nu \in K^*$ working simultaneously for all relations $R_n, n \in \mathbb{N}$.*

Recall that every relation $R_n$ involves only finitely many indeterminates and only finitely many parameters. For our purpose the type of relations (1)–(4), $(4')$ mentioned above actually suffice. In order to keep the proof below readable, let us write the $n$-th relation as

$$R_n((Y_\nu), a) \ .$$

By $(Y_\nu)$ we indicate the sequence of all indeterminates $Y_\nu$, $\nu \in \mathbb{N}$. The element $a$ stands as a representative of all possible parameters. Choosing a representing sequence $\big(a^{(s)}\big)$ for $a$, i.e., $a = \big[\big(a^{(s)}\big)\big]$, we may define

$$R_n^{(s)}\big((Y_\nu), a^{(s)}\big)$$

as the corresponding relation on the factor $\big(K^{(s)}, v^{(s)}, \Gamma^{(s)}\big)$. For example, (4) then reads

$$v_2^{(s)}(Y_\nu) = \gamma_\nu^{(s)} \ .$$

With these conventions let us start the proof.

*Proof.* For each $m \in \mathbb{N}$ let $(y_{\nu,m})_{\nu\in\mathbb{N}}$ be a sequence of elements from $K^*$ realizing the relations $R_0((Y_\nu), a), \ldots, R_m((Y_\nu), a)$ simultaneously. By assumption, such elements exist. Actually, in our assumption we meant elements that realize the finitely many indeterminates occurring in $R_0, \ldots, R_m$. For the non-occurring indeterminates, we may choose anything (e.g., $0^*$).

From the nature of our relations and from the definition of equality in $K^*$ and inequality in $\Gamma^*$, it follows that

$$V_m := \left\{ s \;\middle|\; R_0^{(s)}\big(\big(y_{\nu,m}^{(s)}\big), a^{(s)}\big), \ldots, R_m^{(s)}\big(\big(y_{\nu,m}^{(s)}\big), a^{(s)}\big) \right\} \in \mathcal{F} \; .$$

Clearly $V_{m+1} \subseteq V_m$. We want the $V_m$ to have empty intersection. This is achieved by defining

$$U_m = V_m \cap \{ s \mid s \geq m \} \; .$$

Since $\{ s \mid s \geq m \}$ is cofinite and $\mathcal{F}$ is non-principal, we get $U_m \in \mathcal{F}$. Now clearly $U_m \subseteq V_m$, $U_{m+1} \subseteq U_m$, and $\bigcap_m U_m = \emptyset$. Thus in particular,

$$U_m = \bigcup_{k\geq m} (U_k \smallsetminus U_{k+1}) \; .$$

We are now ready to define the sequence $y_\nu \in K^*$ ($\nu \in \mathbb{N}$) that satisfies all $R_n$ simultaneously. We use a "diagonal" argument:

$$y_\nu^{(s)} = \begin{cases} y_{\nu,m}^{(s)} & \text{if } s \in U_m \smallsetminus U_{m+1} \\ 0 & \text{otherwise} \; . \end{cases}$$

Let us look at the set

$$W_m = \left\{ s \;\middle|\; R_m\big(\big(y_\nu^{(s)}\big), a^{(s)}\big) \right\} \; .$$

By the very definition, we find $U_m \smallsetminus U_{m+1} \subseteq W_m$, since $U_m \smallsetminus U_{m+1} \subseteq V_m$. If $k \geq m$, then

$$U_k \smallsetminus U_{k+1} \subseteq V_k \subseteq V_m \; .$$

Thus $R_m^{(s)}\big(\big(y_\nu^{(s)}\big), a^{(s)}\big)$ holds as well for $s \in U_k \smallsetminus U_{k+1}$. Therefore

$$U_m = \bigcup_{k\geq m} (U_k \smallsetminus U_{k+1}) \subseteq W_m \; ,$$

implying that $W_m \in \mathcal{F}$. This, however, just means that the sequence $(y_\nu)_{\nu\in\mathbb{N}}$ realizes $R_m$. Since our argument is independent of $m$, it realizes all $R_m$ simultaneously. □

*Remark A.7.* The same saturation property just proved for valued fields applies also to ordered abelian groups:

In the proof of Theorem 6.2.3, we had an order-preserving embedding $\tau : \Delta \longrightarrow \Gamma_2$ of a countable subgroup $\Delta$ of $\Gamma_1$ into $\Gamma_2$, where $\Gamma_2$ was a non-principal ultraproduct of ordered abelian groups. We wanted to extend $\tau$ to an

order-preserving embedding of $\widehat{\Delta}_\gamma$, and showed that such an extension existed to every finitely generated subextension $\Delta'$ of $\widehat{\Delta}_\gamma/\Delta$. In this situation we can apply Theorem A.6 as follows:

We choose an enumeration $(\gamma_\nu)_{\nu\in\mathbb{N}}$ of $\widehat{\Delta}_\gamma$, and look for a simultaneous realization $\delta_\nu$ of the indeterminates $Y_\nu$, $\nu \in \mathbb{N}$, in $\Gamma_2$, satisfying the relations

(1) $Y_\nu + Y_\mu = Y_\lambda$, if $\gamma_\nu + \gamma_\mu = \gamma_\lambda$
(2) $Y_\nu < Y_\mu$, if $\gamma_\nu < \gamma_\mu$
(3) $Y_\nu = \tau(\gamma_\nu)$, if $\gamma_\nu \in \Delta$

for all $\nu, \mu, \lambda \in \mathbb{N}$. Then the assignment

$$\gamma_\nu \longmapsto \delta_\nu$$

clearly defines an order-preserving embedding of $\widehat{\Delta}_\gamma$ into $\Gamma_2$ that extends $\tau$.

# B

# Classification of $V$-Topologies

Absolute values as well as (general) valuations canonically induce a topology on their field of definition for which all field operations are continuous with the extra property that a product of two elements can only be small if at least one of the factors is already small. Such field topologies are called $V$-topologies. In this appendix we show that, conversely, every $V$-topology on a field $K$ must be induced by an absolute value or a valuation of $K$.

Recall that a topological field is a field $K$ endowed with a Hausdorff topology that makes addition, multiplication, and non-zero division ($x \mapsto x^{-1}$, $x \neq 0$) continuous. In view of the continuity of addition, such a topology may be specified merely by giving a fundamental system $\mathsf{T}$ of neighbourhoods of $0 \in K$. In fact, from $\mathsf{T}$ one gets, via the translation $x \mapsto a + x$, a system of neighbourhoods of each element $a \in K$. Therefore, for a field $K$, we shall refer to a fundamental system $\mathsf{T}$ of neighbourhoods of $0 \in K$ as a topology on $K$, and to the pair $(K, \mathsf{T})$ as a *topological field*.

Given a topological field $(K, \mathsf{T})$, the *complete* system of neighbourhoods of 0 consists of all subsets $U \subseteq K$ that contain some $\mathcal{W} \in \mathsf{T}$. We shall not distinguish between a fundamental system and a complete system of neighbourhoods of 0, and just refer to either of them as a topology $\mathsf{T}$ on $K$.

Recall that for two subsets $R$, $S$ of $K$ we use the notations:

$$\begin{aligned} R \pm S &= \{\, x \pm y \mid x \in R,\ y \in S \,\}\,, \\ RS &= \{\, xy \mid x \in R,\ y \in S \,\}\,, \\ R^{-1} &= \{x^{-1} \mid x \in R\} \text{ if } 0 \notin R\,. \end{aligned}$$

Moreover, for $R = \{x\}$ we simply write $x \pm S$ and $xS$, respectively.

A (non-discrete) topology $\mathsf{T}$ on a field $K$ is called a *$V$-topology* if the following axioms hold:

$$
\begin{aligned}
&(1)\ \bigcap \mathsf{T} := \bigcap_{\mathcal{U}\in\mathsf{T}} \mathcal{U} = \{0\};\ \{0\} \notin \mathsf{T}.\\
&(2)\ \text{For any pair } \mathcal{U},\mathcal{V} \in \mathsf{T},\ \text{there is } \mathcal{W} \in \mathsf{T} \text{ such that } \mathcal{W} \subseteq \mathcal{U} \cap \mathcal{V}.\\
&(3)\ \text{For every } \mathcal{U} \in \mathsf{T} \text{ there is } \mathcal{W} \in \mathsf{T} \text{ for which } \mathcal{W} - \mathcal{W} \subseteq \mathcal{U}.\\
&(4)\ \text{For all } \mathcal{U} \in \mathsf{T} \text{ and every pair } x, y \in K \text{ there is } \mathcal{W} \in \mathsf{T}\\
&\quad\ \text{satisfying } (x+\mathcal{W})(y+\mathcal{W}) \subseteq xy + \mathcal{U}.\\
&(5)\ \text{For } \mathcal{U} \in \mathsf{T} \text{ and } x \in K^\times,\ \text{there exists } \mathcal{W} \in \mathsf{T}\\
&\quad\ \text{such that } (x+\mathcal{W})^{-1} \subseteq x^{-1} + \mathcal{U}.\\
&(6)\ \text{For all } \mathcal{W} \in \mathsf{T} \text{ there exists } \mathcal{U} \in \mathsf{T} \text{ such that}\\
&\quad\ x, y \in K \text{ and } xy \in \mathcal{U} \text{ implies } x \in \mathcal{W} \text{ or } y \in \mathcal{W}\ .
\end{aligned}
\tag{B.1}
$$

It follows from axioms (1) to (4) that $\mathsf{T}$ is a Hausdorff topology and, taking $K \times K$ with the product topology, that addition and multiplication are continuous maps. The fifth axiom means that the map $x \mapsto x^{-1},\ K^\times \to K^\times$ is continuous. The last axiom will be responsible for the "valued" origin of the topology.

To avoid repeating arguments let us fix the following consequences from the axioms (1) to (4) above.

$$
\begin{aligned}
&(3a)\ \text{For every } \mathcal{U} \in \mathsf{T} \text{ there is } \mathcal{W} \in \mathsf{T} \text{ for which } \mathcal{W}, -\mathcal{W} \subseteq \mathcal{U}.\\
&(3b)\ \text{For all } \mathcal{U} \in \mathsf{T},\ \text{there is } \mathcal{W} \in \mathsf{T} \text{ such that } \mathcal{W} + \mathcal{W} \subseteq \mathcal{U}.\\
&(4a)\ \text{For all } \mathcal{U} \in \mathsf{T} \text{ there is } \mathcal{W} \in \mathsf{T} \text{ satisfying } \mathcal{W}\mathcal{W} \subseteq \mathcal{U}.\\
&(4b)\ \text{For } \mathcal{U} \in \mathsf{T} \text{ and } x \in K^\times,\ \text{there exists } \mathcal{W} \in \mathsf{T} \text{ such that } x\mathcal{W} \subseteq \mathcal{U}.
\end{aligned}
\tag{B.2}
$$

In fact, (3a) follows from $\mathcal{W}, -\mathcal{W} \subseteq \mathcal{W} - \mathcal{W}$. To get (3b), let $\mathcal{U}$ be given. From (3) follows the existence of $\mathcal{V}$ satisfying $\mathcal{V} - \mathcal{V} \subseteq \mathcal{U}$. From (3a) there is $\mathcal{W}$ such that $\mathcal{W}, -\mathcal{W} \subseteq \mathcal{V}$. Thus $\mathcal{W} + \mathcal{W} = \mathcal{W} - (-\mathcal{W}) \subseteq \mathcal{V} - \mathcal{V} \subseteq \mathcal{U}$, as desired.

Next, taking $x = 0 = y$ in (4) one gets (4a), while taking $y = 0$, for given $\mathcal{U}$ and $x$, it follows that $x\mathcal{W} \subseteq (x + \mathcal{W})\mathcal{W} \subseteq \mathcal{U}$.

Actually (4b) says that, for a fixed $x \in K^\times$, the set $\{\, x\mathcal{W} \mid \mathcal{W} \in \mathsf{T} \,\}$ is also a fundamental system of neighbourhoods of 0 for the topology $\mathsf{T}$.

It may be convenient to observe that axiom (5) can be formulated in the following simpler way, which sometimes is easier to use.

$$
\text{For } \mathcal{U} \in \mathsf{T} \text{ there exists } \mathcal{W} \in \mathsf{T} \text{ such that } (1+\mathcal{W})^{-1} \subseteq 1 + \mathcal{U}\ . \tag{B.3}
$$

Clearly (5) implies (B.3). However, (B.3) together with (4a) and (4b) implies (5). Indeed, let $x \in K^\times$ and $\mathcal{U} \in \mathsf{T}$ be given. From (B.2) (4b) there exists $\mathcal{V}$ such that $x^{-1}\mathcal{V} \subseteq \mathcal{U}$. By (5a) there is $\mathcal{V}'$ such that $(1 + \mathcal{V}')^{-1} \subseteq 1 + \mathcal{V}$. Again (B.2) (4b) implies the existence of $\mathcal{W}$ such that $x^{-1}\mathcal{W} \subseteq \mathcal{V}'$. Putting everything together one gets

$$(1 + x^{-1}\mathcal{W})^{-1} \subseteq (1 + \mathcal{V}')^{-1} \subseteq 1 + \mathcal{V} \subseteq 1 + x\mathcal{U} \,.$$

Multiplying by $x^{-1}$, (5) follows as required.

A typical example of a $V$-topology is the topology given by an absolute value $|\ |$. The open balls $\{\, x \in K \mid |x| < r \,\}$, with $r > 0$ are the elements of $\mathsf{T}$.

Another example of a $V$-topology is the topology generated by a valuation. Take the neighborhoods $\mathcal{U}_\gamma(0)$ in the place of $\mathcal{W} \in \mathsf{T}$, as discussed in Sect. 2.3. In Remark 2.3.3 it was already stated that this topology satisfies the axioms in (B.1). We shall prove next that, conversely, a $V$-topology derives from a valuation or an absolute value. Our main goal in this section is Theorem B.1, due to Kowaslky and Dürbaum [13], which gives the promised classification of $V$-topologies.

**Theorem B.1.** *Let $K$ be a field and $\mathsf{T}$ a topology on $K$. Then $\mathsf{T}$ is a $V$-topology if and only if there exists either an archimedean absolute value or a valuation on $K$ whose induced topology coincides with $\mathsf{T}$.*

In order to prove this result we shall introduce the concepts of bounded sets, almost valuations, and nilpotent elements. Then we prove some properties of these elements that will be needed for the proof. The first result concerns the system $\mathsf{T}$ of neighborhoods of 0.

**Lemma B.2.** *Let $\mathsf{T}$ be a $V$-topology on a field $K$. Then there exists $\mathcal{U} \in \mathsf{T}$ such that*

$$K^\times = (K \smallsetminus \mathcal{U}) \cup (K \smallsetminus \mathcal{U})^{-1} \,.$$

*Proof.* Assume, on the contrary, that for every $\mathcal{W} \in \mathsf{T}$ there is $x_{\mathcal{W}} \in K^\times$ such that $x_{\mathcal{W}} \in \mathcal{W}$ and $x_{\mathcal{W}}^{-1} \in \mathcal{W}$. According to (B.2) (4a), for every $\mathcal{U}$ there exists $\mathcal{W}$ such that $\mathcal{W}\mathcal{W} \in \mathcal{U}$. Consequently, $1 = x_{\mathcal{W}}\, x_{\mathcal{W}}^{-1} \in \mathcal{U}$, for every $\mathcal{U} \in \mathsf{T}$. Since this contradicts (B.1) (1), the statement is proved. □

We say that a subset $S$ of a topological field $(K, \mathsf{T})$ is *bounded* if for every $\mathcal{W} \in \mathsf{T}$ there exists $\mathcal{U} \in \mathsf{T}$ such that

$$\mathcal{U}S \subseteq \mathcal{W} \,.$$

Using bounded sets we can give a new and useful reformulation of axiom (6).

$$\text{For every } \mathcal{W} \in \mathsf{T}, \text{ the set } (K \smallsetminus \mathcal{W})^{-1} \text{ is bounded.} \tag{B.4}$$

Note that $(K \smallsetminus \mathcal{W})^{-1}$ is bounded for all $\mathcal{W} \in \mathsf{T}$ if and only if for all $\mathcal{W} \in \mathsf{T}$ there is $\mathcal{U} \in \mathsf{T}$ such that $\mathcal{U}(K \smallsetminus \mathcal{W})^{-1} \subseteq \mathcal{W}$. Thus, for all $x, y \in K$, if $xy \in \mathcal{U}$ and $x \in (K \smallsetminus \mathcal{W})$, then $y = xyx^{-1} \in \mathcal{U}(K \smallsetminus \mathcal{W})^{-1} \subseteq \mathcal{W}$. This proves (6). Conversely, for $\mathcal{W} \in \mathsf{T}$, pick $\mathcal{U} \in \mathsf{T}$ satisfying (6). Then $\mathcal{U}(K \smallsetminus \mathcal{W})^{-1} \subseteq \mathcal{W}$. In fact, if $x \notin \mathcal{W}$ and $u = x(ux^{-1}) \in \mathcal{U}$, then $ux^{-1} \in \mathcal{W}$.

Bounded subsets have the following properties:

**Lemma B.3.** *Let $M$ and $N$ be subsets of a topological field $(K, \mathsf{T})$.*

*(1) $M$ is bounded if and only if for every $\mathcal{U} \in \mathsf{T}$ there exists $x \in K^\times$ such that $xM \subseteq \mathcal{U}$.*
*(2) If $M$ is a finite set, then $M$ is bounded.*
*(3) If $N \subseteq M$ and $M$ is bounded, then so is $N$.*
*(4) If $M$ and $N$ are bounded, then so are $M \pm N$ and $MN$.*

*Proof.* (1) The implication "$\Longrightarrow$" is clearly true. For the other implication, given $\mathcal{U} \in \mathsf{T}$, it follows from (B.2) (4a) that there exists $\mathcal{V} \in \mathsf{T}$ such that $\mathcal{V}\mathcal{V} \subseteq U$. For $\mathcal{V}$, the assumption implies that there is $x \in K^\times$ such that $xM \subseteq \mathcal{V}$. Thus $\mathcal{V}xM \subseteq \mathcal{U}$. Now, according to (B.2) (4b), $x^{-1}\mathcal{W} \subseteq \mathcal{V}$ for some $\mathcal{W}$. Putting the two inclusions together it follows that $\mathcal{W}M \subseteq \mathcal{V}xM \subseteq \mathcal{U}$, as required.

(2) and (3) are clearly true.

(4) Let $\mathcal{U} \in \mathsf{T}$. Now (B.1) (3) implies that $\mathcal{V}_1 - \mathcal{V}_1 \subseteq \mathcal{U}$ for some $\mathcal{V}_1$, while (B.2) (3b) yields $\mathcal{V}_2 + \mathcal{V}_2 \subseteq \mathcal{U}$ for some $\mathcal{V}_2$. By (B.1) (2) there exists $\mathcal{V} \subseteq \mathcal{V}_1 \cap \mathcal{V}_2$. Thus $\mathcal{V} \pm \mathcal{V} \subseteq \mathcal{U}$.

Since $M$ and $N$ are bounded, there are $\mathcal{W}_1$ and $\mathcal{W}_2$ such that $\mathcal{W}_1 M \subseteq \mathcal{V}$ and $\mathcal{W}_2 M \subseteq \mathcal{V}$. For $\mathcal{W}$ satisfying $\mathcal{W} \subseteq \mathcal{W}_1 \cap \mathcal{W}_2$ it follows that

$$\mathcal{W}(M \pm N) \subseteq \mathcal{W}_1 M \pm \mathcal{W}_2 N \subseteq \mathcal{V} \pm \mathcal{V} \subseteq \mathcal{U} \,,$$

and so $M \pm N$ is bounded.

For the multiplication, take $\mathcal{V}$ and $\mathcal{W}$ such that $\mathcal{W}M \subseteq \mathcal{V}$ and $\mathcal{V}N \subseteq \mathcal{U}$. Then $\mathcal{W}(MN) \subseteq \mathcal{U}$. □

**Corollary B.4.** *$K$ is not bounded.*

*Proof.* The corollary follows from (1) of the previous lemma and (B.1) (1). □

The next property is a crucial aspect of $V$-topologies.

**Lemma B.5.** *If $\mathsf{T}$ is a $V$-topology, then there exists a bounded neighbourhood $\mathcal{W} \in \mathsf{T}$.*

*Moreover, for any bounded $\mathcal{W} \in \mathsf{T}$, the set*

$$\mathsf{O} := \{\, x \in K \mid x\mathcal{W} \subseteq \mathcal{W} \,\}$$

*has the following properties:*

*(1) $\mathsf{O}$ is a bounded neighbourhood,*
*(2) $1 \in \mathsf{O} \neq K$ and $\mathsf{O}\mathsf{O} \subseteq \mathsf{O}$,*
*(3) $K^\times \subseteq \dot{\mathsf{O}}(\dot{\mathsf{O}})^{-1}$, where we set $\dot{\mathsf{O}} = \mathsf{O} \setminus \{0\}$,*
*(4) there exists $d \in \dot{\mathsf{O}}$ such that for every $x \in K$ either $x \in \mathsf{O}$ or $x^{-1} \in d^{-1}\mathsf{O}$.*

*Proof.* According to Lemma B.2 there exists $\mathcal{W} \in \mathsf{T}$ such that

$$K^\times = (K \setminus \mathcal{W}) \cup (K \setminus \mathcal{W})^{-1} \,.$$

Consequently, $\mathcal{W} \smallsetminus \{0\} \subseteq (K \smallsetminus \mathcal{W})^{-1}$. Hence $\mathcal{W} = (\mathcal{W} \smallsetminus \{0\}) \cup \{0\}$ is a bounded set, by (B.4) and Lemma B.3.

Define next $\mathsf{O} := \{\, x \in K \mid x\mathcal{W} \subseteq \mathcal{W} \,\}$ for any bounded neighbourhood $\mathcal{W} \in \mathsf{T}$.

By the very definition of bounded subsets, there is $\mathcal{U} \in \mathsf{T}$ such that $\mathcal{U}\mathcal{W} \subseteq \mathcal{W}$. Thus $\mathcal{U} \subseteq \mathsf{O}$ and hence $\mathsf{O}$ is a neighbourhood. Moreover since $\mathsf{O}\mathcal{W} \subseteq \mathcal{W}$, for $0 \neq x \in \mathcal{W}$ it follows that $\mathsf{O} \subseteq \mathcal{W}x^{-1}$. Hence $\mathsf{O}$ is bounded, by Lemma B.3.

By Corollary B.4, $\mathsf{O} \neq K$. Furthermore, the construction of $\mathsf{O}$ implies that $1 \in \mathsf{O}$ and $\mathsf{O}\mathsf{O} \subseteq \mathsf{O}$, showing the first two properties.

Let $x \in K^\times$. By (B.2) (4b) there is $\mathcal{V} \in \mathsf{T}$ such that $x\mathcal{V} \subseteq \mathsf{O}$. Let $\mathcal{V}' \in \mathsf{T}$ such that $\mathcal{V}' \subseteq \mathcal{V} \cap \mathsf{O}$. Then for $0 \neq y \in \mathcal{V}'$ and $z := xy \in \mathsf{O}$ one gets $x = zy^{-1} \in \dot{\mathsf{O}}(\dot{\mathsf{O}})^{-1}$. Therefore (3) is true.

Returning to the neighbourhood $\mathcal{U} \subseteq \mathsf{O}$ from above, one sees that

$$(K \smallsetminus \mathsf{O})^{-1} \subseteq (K \smallsetminus \mathcal{U})^{-1} \,.$$

Hence $(K \smallsetminus \mathsf{O})^{-1}$ is bounded by Lemma B.3 (3). Thus, (1) of Lemma B.3 implies that $d(K \smallsetminus \mathsf{O})^{-1} \subseteq \mathsf{O}$, for some $d \in K^\times$. Consequently $(K \smallsetminus \mathsf{O})^{-1} \subseteq d^{-1}\mathsf{O}$. □

One sees that $\mathsf{O}$ is "almost" a valuation subring of $K$. In the next lemma we shall see that $\mathsf{O}$ is also almost closed under addition. For further references we shall call a subset $\mathsf{O}$ of a field $K$ with the above properties (1) to (4) an *almost valuation* of $K$.

**Lemma B.6.** *If $\mathsf{O}$ is an almost valuation, then there exists $c \in \dot{\mathsf{O}}$ such that*

$$c(\mathsf{O} \pm \mathsf{O}) \subseteq \mathsf{O} \,.$$

*Proof.* By (B.1) (3) and (B.2) (3b) there is $\mathcal{V} \in \mathsf{T}$ such that $\mathcal{V} \pm \mathcal{V} \subseteq \mathsf{O}$. On the other hand, as $\mathsf{O}$ is bounded, by Lemma B.3 (1) there is $c \in K^\times$ such that $c\mathsf{O} \subseteq \mathcal{V}$. Consequently

$$c(\mathsf{O} \pm \mathsf{O}) \subseteq c\mathsf{O} \pm c\mathsf{O} \subseteq \mathcal{V} \pm \mathcal{V} \subseteq \mathsf{O} \,.$$

Since $0, 1 \in \mathsf{O}$, it follows that $c \in \mathsf{O}$. □

*Remark B.7.* Let $K$ be a field admitting an almost valuation $\mathsf{O}$. Define $\mathsf{T}_\mathsf{O} = \{\, x\mathsf{O} \mid x \in K^\times \,\}$. One can prove that $\mathsf{T}$ has the properties (B.1) and so defines a $V$-topology on $K$.

Furthermore, for an almost valuation $\mathsf{O}$, constructed as above from a bounded neighbourhood of a topology $\mathsf{T}$, the fundamental system $\mathsf{T}_\mathsf{O}$ induces the same topology as $\mathsf{T}$. Therefore we may say that $\mathsf{O}$ "generates" $\mathsf{T}$.

*Example B.8.* For a field $K$ with an archimedean absolute value $|\ |$, the closed ball $\mathsf{O} := \{\, x \in K \mid |x| \leq 1 \,\}$ is an almost valuation of $K$.

Next, given a topological field $(K, \mathsf{T})$, we call an element $x \in K$ (*analytically*) *nilpotent* if either $x = 0$ or the sequence $(x^n)_{n\in\mathbb{N}}$ converges to 0 in the topology $\mathsf{T}$, i.e., for every $\mathcal{W} \in \mathsf{T}$ there is $n_0 \in \mathbb{N}$ such that $x_n \in \mathcal{W}$ for all $n \geq n_0$. An element $x \in K^\times$ is said to be *neutral* if $x$ and $x^{-1}$ are not nilpotent.

*Example B.9.* Let $\mathcal{O}$ be a rank one valuation ring. Every non-zero element of the maximal ideal $\mathcal{M}$ of $\mathcal{O}$ is nilpotent, since the value group $\Gamma$ of $\mathcal{O}$ is archimedean. The elements from $\mathcal{O} \smallsetminus \mathcal{M}$ are neutral.

Another example is given by an archimedean absolute value $|\ |$. In fact, if $x \in K^\times$ satisfies $|x| < 1$, then $x$ is nilpotent. Observe that $x$ is a neutral element if and only if $|x| = 1$.

**Lemma B.10.** *Let $(K, \mathsf{T})$ be a $V$-topological field.*

*(1) If there exists any nilpotent element $t \neq 0$ in $K$, then there exists a neighborhood $\mathcal{W}$ such that all $x \in \mathcal{W}$ are nilpotent.*
*(2) Let $\mathsf{O}$ be an almost valuation of $K$. If $x \in \dot{\mathsf{O}}$ is not nilpotent, then the set $\{\, x^{-n} \mid n \in \mathbb{N} \,\}$ is bounded.*

*Proof.* (1) Take a neighbourhood $\mathsf{O}$ which is an almost valuation of $K$ and set $\mathcal{U} := t\mathsf{O}$.

As $\mathsf{O}$ is bounded, given $\mathcal{W} \in \mathsf{T}$ there exists $\mathcal{V}$ such that $\mathsf{O}\mathcal{V} \subseteq \mathcal{W}$. Next, as $t$ is nilpotent, there exists $n_0 \in \mathbb{N}$ such that $t^n \in \mathcal{V}$ for all $n \geq n_0$. Since $\mathsf{O}\mathsf{O} \subseteq \mathsf{O}$ for every $u \in \mathcal{U}$ and all $n \geq n_0$, we have $u^n \in t^n\mathsf{O} \subseteq \mathcal{V}\mathsf{O} \subseteq \mathcal{W}$. Therefore $u$ is nilpotent, as required.

(2) According to (B.4) and Lemma B.3, it is enough to show that there exists $\mathcal{W} \in \mathsf{T}$ such that $\{\, x^n \mid n \in \mathbb{N} \,\} \subseteq (K \smallsetminus \mathcal{W})^{-1}$. Observe now that if $u \in K^\times$ and $x^r \in u\mathsf{O}$ for some $r \in \mathbb{N}$, then $x^{r+1} \in u\mathsf{O}\mathsf{O} \subseteq u\mathsf{O}$. Thus, recursively $x^n \in u\mathsf{O}$ for every $n \geq r$. Since by (B.2) (4b) the set $\{\, u\mathsf{O} \mid u \in K^\times \,\}$ is also a fundamental system of neighbourhoods of 0 for the topology $\mathsf{T}$, it follows that $x$ is nilpotent, a contradiction. Thus, there exists $u \in K^\times$ such that no power $x^r$ lies in $u\mathsf{O}$, i.e., $\{x^n \mid n \in \mathbb{N}\} \subseteq (K \smallsetminus u\mathsf{O})^{-1}$, as desired. □

We list some properties of nilpotent and neutral elements which will be used in the proof of Theorem B.1.

**Lemma B.11.** *Let $(K, \mathsf{T})$ be a topological field and $x, y \in K^\times$.*

*(1) If $x$ and $y$ are nilpotent, then so is $xy$.*
*(2) Suppose there exists a nilpotent element $x \neq 0$. Then the set $N_0$ consisting of all nilpotent elements is a bounded neighbourhood in $\mathsf{T}$.*
*(3) Suppose there exists a nilpotent element $x \neq 0$. Then the set $N$ consisting of all nilpotent and neutral elements is a bounded neighbourhood in $\mathsf{T}$.*
*(4) If $x$ is nilpotent and $y$ is neutral, then $xy$ is nilpotent.*
*(5) If $x, y$ are neutral, then $xy$ is neutral.*

*(6) The set $N^* = N \setminus N_0$ of all neutral elements is a subgroup of the multiplicative group $K^\times$.*

*(7) If $x \neq 0$ is nilpotent, then to every $y \neq 0$ there is $m \in \mathbb{N}$ such that $x^m y^{-1}$ is nilpotent.*

*Proof.* (1) Given $\mathcal{W}$, by (B.2) (4a), there is $\mathcal{V}$ such that $\mathcal{V}\mathcal{V} \subseteq \mathcal{W}$. For this $\mathcal{V}$ there are $n_0, n_1 \in \mathbb{N}$ such that $x^n, y^n \in \mathcal{V}$ for every $n \geq \max\{n_0, n_1\}$. Thus $xy$ is nilpotent as desired.

(2) By Lemma B.10 (1) there exists a neighbourhood $\mathcal{W}$ of nilpotent elements. Thus $\mathcal{W} \subseteq N_0$ and $N_0$ is a neighbourhood for $\mathsf{T}$. On the other hand, every $z \in (\mathcal{W}^\times)^{-1}$ cannot be nilpotent by (1). Hence $N_0^\times \subseteq (K \setminus \mathcal{W})^{-1}$, which is bounded by (B.4). Thus $N_0$ is bounded, by Lemma B.3.

(3) The neighbourhood $\mathcal{W}$ from item 2 even gives $\mathcal{W} \subseteq N$ and $N \subseteq (K \setminus \mathcal{W})^{-1}$.

(4) Clearly $y^n$ is neutral for every $n \in \mathbb{Z}$. Otherwise, if for some $m$, $y^m$ or $y^{-m}$ is nilpotent, then $y$ or $y^{-1}$ would be nilpotent, too. Thus $y^n \in N$ for every $n \in \mathbb{N}$.

On the other hand, as $N$ is bounded, for every $\mathcal{W} \in \mathsf{T}$ there is $\mathcal{V}$ such that $N\mathcal{V} \subseteq \mathcal{W}$. There exists some $n_0 \in \mathbb{N}$ such that $x^n \in \mathcal{V}$ for every $n \geq n_0$. Thus

$$x^n y^n \in \mathcal{V}N \subseteq \mathcal{W}$$

for all $n \geq n_0$. Hence $xy$ is also nilpotent.

(5) We assume that $xy$ is not neutral. Then either $xy$ is nilpotent, or $(xy)^{-1}$ is nilpotent. Neither case can occur. For if $(xy)^{-1}$ were nilpotent, then by the previous item, $x^{-1} = y(xy)^{-1}$ would be nilpotent, a contradiction; and if $xy$ were nilpotent, then $x = y^{-1}(xy)$ would be nilpotent, a contradiction as well. Consequently, $xy$ is neutral.

(6) Clearly 1 is neutral, and $z^{-1}$ has to be neutral, if $z$ is neutral. Thus, the last item completes the proof that $N^*$ is a subgroup of $K^\times$.

(7) By item (2), $N_0$ is a neighbourhood. Since $yN_0$ is also a neighbourhood for $\mathsf{T}$, there is $n \in \mathbb{N}$ such that $x^n \in yN_0$. Thus $x^n y^{-1} \in N_0$ is a nilpotent element. □

We are now ready to prove Theorem B.1. Actually, we shall prove slightly more. In fact, Proposition 2.3.5 implies that we have to distinguish two cases.

**Theorem B.12.** *Let $K$ be a field and let $\mathsf{T}$ be any Hausdorff topology on $K$ making the field operations continuous. Then*

*(1) $\mathsf{T}$ is a $V$-topology without non-zero nilpotent elements if and only if the topology is induced by a valuation ring $\mathcal{O}$ of $K$ whose chain of prime ideals is a fundamental system of neighborhoods of 0 for this topology.*

*(2) $\mathsf{T}$ is a $V$-topology with at least one non-zero nilpotent element if and only if there exists either an archimedean absolute value or a rank-one valuation on $K$ whose induced topology coincides with $\mathsf{T}$.*

*Proof.* (1) Let $(K, \mathsf{T})$ be a $V$-topological field without non-zero nilpotent elements, and take an almost valuation $\mathsf{O}$ that generates this topology (Remark B.7). Let $d \in \dot{\mathsf{O}}$ satisfy the condition (4) of Lemma B.5, i.e., $(K \smallsetminus \mathsf{O})^{-1} \subseteq d^{-1}\mathsf{O}$. Next, take

$$\widetilde{\mathsf{O}} := \{\, x \in K \mid x\mathsf{O} \subseteq d^{-n}\mathsf{O} \text{ for some } n \geq 0 \,\} .$$

From $\mathsf{OO} \subseteq \mathsf{O}$, it follows that $\mathsf{O} \subseteq \widetilde{\mathsf{O}}$. Therefore $\widetilde{\mathsf{O}}$ is a neighbourhood in $\mathsf{T}$. Since $1 \in \mathsf{O}$, one gets

$$\widetilde{\mathsf{O}} \subseteq \bigcup_{n \geq 0} d^{-n}\mathsf{O} .$$

By Lemma B.5, $\mathsf{O}$ is bounded. Assuming that there is no non-zero nilpotent element for $\mathsf{T}$, Lemma B.10 implies that $\{\, d^{-n} \mid n \in \mathbb{N} \,\}$ is bounded. Consequently, $\widetilde{\mathsf{O}}$, being a subset of $\mathsf{O}\{\, d^{-n} \mid n \in \mathbb{N} \,\}$, is bounded, by Lemma B.3. Moreover, $\widetilde{\mathsf{O}}\widetilde{\mathsf{O}} \subseteq \widetilde{\mathsf{O}}$. We may therefore conclude that $\widetilde{\mathsf{O}}$ has the properties (1) and (2) of Lemma B.5. To show that it also satisfies properties (3) and (4), we use that $(K \smallsetminus \widetilde{\mathsf{O}})^{-1} \subseteq \widetilde{\mathsf{O}}$. In fact,

$$\mathsf{O} \subseteq \widetilde{\mathsf{O}} \text{ implies } (K \smallsetminus \widetilde{\mathsf{O}})^{-1} \subseteq (K \smallsetminus \mathsf{O})^{-1} \subseteq d^{-1}\mathsf{O} \subseteq \widetilde{\mathsf{O}} .$$

Consequently, $x \in \widetilde{\mathsf{O}}$ or $x^{-1} \in \widetilde{\mathsf{O}}$ for every $x \in K$.

Now, by Lemma B.6 there is $c \in \widetilde{\mathsf{O}}^{\times}$ such that

$$c(\widetilde{\mathsf{O}} \pm \widetilde{\mathsf{O}}) \subseteq \widetilde{\mathsf{O}} .$$

Hence,

$$\widetilde{\mathsf{O}} \pm \widetilde{\mathsf{O}} \subseteq c^{-1}\widetilde{\mathsf{O}} ,$$
$$\widetilde{\mathsf{O}} \pm \widetilde{\mathsf{O}} \pm \widetilde{\mathsf{O}} \pm \widetilde{\mathsf{O}} \subseteq c^{-1}(\widetilde{\mathsf{O}} \pm \widetilde{\mathsf{O}}) \subseteq c^{-2}\widetilde{\mathsf{O}},$$

and in general

$$\underbrace{\widetilde{\mathsf{O}} \pm \cdots \pm \widetilde{\mathsf{O}}}_{2^n \text{ times}} \subseteq c^{-n}\widetilde{\mathsf{O}} .$$

Finally we let $\mathcal{O}$ be the subring of $K$ generated by $\widetilde{\mathsf{O}}$. Clearly

$$\mathcal{O} = \{\, x_1 + \cdots + x_m \mid m \geq 1, \quad x_1, \ldots, x_m \in \widetilde{\mathsf{O}} \cup -\widetilde{\mathsf{O}} \,\} .$$

Thus $\mathcal{O} \subseteq \widetilde{\mathsf{O}}\{\, c^{-n} \mid n \in \mathbb{N} \,\}$. As $\widetilde{\mathsf{O}}$ is bounded and $c$ is not nilpotent, by Lemma B.10 and Lemma B.3 also $\mathcal{O}$ is bounded. Since $\widetilde{\mathsf{O}} \subseteq \mathcal{O}$, this subring is also a neighborhood in $\mathsf{T}$. Hence, like $\widetilde{\mathsf{O}}$, the subring $\mathcal{O}$ generates $\mathsf{T}$. Moreover, for every $x \in K$ we have $x \in \widetilde{\mathsf{O}} \subseteq \mathcal{O}$ or $x^{-1} \in \widetilde{\mathsf{O}} \subseteq \mathcal{O}$; i.e., $\mathcal{O}$ is a valuation ring of $K$. To finish the proof, recall that, according to Example B.9, the topology

generated by a rank 1 valuation ring or an archimedean absolute value has nilpotent elements.

(2) We shall first prove that the set $N$ consisting of all nilpotent and neutral elements, is an almost valuation of $K$.

According to Lemma B.11, (1) to (5), $N$ is a multiplicatively closed bounded neighborhood, i.e, $N$ has the properties (1) and (2) of Lemma B.5.

Next, let $x \in K^\times$. If $x$ is not neutral, then either $x$ or $x^{-1}$ is nilpotent. Consequently, if $x \notin N$, then $x^{-1} \in N$. Hence $N$ also satisfies the properties (3) and (4) of Lemma B.5, and so $N$ is an almost valuation of $K$, as desired.

Now consider the following relation:

$$y \preceq x \text{ iff } x \in yN \ ,$$

for all $x, y \in K^\times$. This relation is reflexive, and since we have proved $NN \subseteq N$, it is also transitive. Moreover, if $x \preceq y$ and $x_1 \preceq y_1$, then $xx_1 \preceq yy_1$.

Next, note that $x \preceq y$ and $y \preceq x$ if and only $xy^{-1} \in N^*$. Hence

$$x \equiv y \text{ iff } x \preceq y \text{ and } y \preceq x$$

defines $\equiv$ as an equivalence relation. Hence the quotient

$$\Gamma := K^\times/N^* = K^\times/\equiv$$

is an ordered abelian group with the ordering $\leq$ induced by $\preceq$. Actually, $\Gamma$ is even an archimedean ordered group: if $x \neq 0$ is nilpotent and $y \in K^\times$, then by (7) of Lemma B.11 there is $m \in \mathbb{N}$ such that $yN^* \leq (xN^*)^m$. Consequently, there is an injective homomorphism $\Gamma \longrightarrow \mathbb{R}$ into the additive group of real numbers, by Proposition 2.1.1. Let us denote the composition

$$K^\times \longrightarrow \Gamma \longrightarrow \mathbb{R}$$

by $\varphi$.

In order to treat archimedean and non-archimedean absolute values simultaneously, we define

$$|x| = \begin{cases} 0 & \text{if } x = 0 \\ e^{-\varphi(x)} & \text{otherwise.} \end{cases}$$

It is now clear that $|x| \geq 0$ for every $x \in K$, and $|x| = 0$ iff $x = 0$. Moreover, $|xy| = |x||y|$ for all $x, y \in K$. It remains to prove the triangle inequality. The proof of this inequality needs some preparation.

The function $|\ |$ naturally induces a topology on $K$ by taking the balls $S(\varepsilon) = \{\, x \in K \mid |x| < \varepsilon \,\}$, with $0 < \varepsilon \in \mathbb{R}$, as the neighbourhoods of 0 in $K$. We prove that this topology coincides with the original topology $\mathsf{T}$.

Every $S(\varepsilon)$ contains some $\mathcal{W} \in \mathsf{T}$: Take $a$ such that $|a| > \varepsilon^{-1}$. Since $N_0$ is a neighbourhood in $\mathsf{T}$, there is $\mathcal{W} \in \mathsf{T}$ such that $a\mathcal{W} \subseteq N_0$, by (B.2) (4b). Hence $|x| < |a|^{-1} < \varepsilon$ for every $x \in \mathcal{W}$, and so $\mathcal{W} \subseteq S(\varepsilon)$.

Every $\mathcal{W}$ contains some $S(\varepsilon)$: As $N_0$ is bounded, for every $\mathcal{W}$ there is $b \in K^\times$ such that $bN_0 \subseteq \mathcal{W}$, by Lemma B.3 (1). Put $\varepsilon = |b|$ and observe that $S(\varepsilon) = bN_0$. Thus $S(\varepsilon) \subseteq \mathcal{W}$, as desired.

Consequently, the set of balls $S(\varepsilon)$ satisfies axioms (1) to (6) of (B.1). In particular, the field operations are continuous. We shall use this to show that for some real $\nu > 0$, $|\ |^\nu$ is an absolute value.

Now it is time to use Lemma B.6. Let $c \in N^\times$ be such that $c(N \pm N) \subseteq N$.

We claim that $|x+y| \le |c^{-1}| \max\{\,|x|, |y|\,\}$, for all $x, y \in K$.

For $x, y \in K$ assume, without loss of generality, that $|x| \le |y|$. Then $y \preceq x$, and thus there is $z \in N$ such that $x = yz$. Therefore

$$x + y = y(z+1) \in yc^{-1}N\ .$$

Hence $yc^{-1} \preceq (x+y)$ and so

$$|x+y| \le |c^{-1}||y|\ ,$$

proving our claim.

On the other hand, as $c \in N$, it follows that $|c| \le 1$. Thus $|c^{-1}| \ge 1$. Hence we can choose a real $\nu > 0$, so small that $|c^{-1}|^\nu \le 2$. Replacing $|\ |$ by $|\ |^\nu$, we get

$$|x+y| \le 2\max\{|x|, |y|\}\ .$$

Iterating the above inequality, for $n = 2^m$ and $x_1, \ldots, x_n \in K$ we find

$$|x_1 + \cdots + x_n| \le n \max_i |x_i|\ . \tag{B.5}$$

Now let $n$ be arbitrary, and add $x_i = 0$ for $i = n+1$ to the next power of 2. Then (B.5) gives

$$|x_1 + \cdots + x_n| \le 2n \max_i |x_i|\ . \tag{B.6}$$

In particular, we obtain $|x| \le 2x$ for every positive integer $x$. From (B.6) we then obtain

$$\begin{aligned}
|x+y|^n = |(x+y)^n| &\le 2(n+1) \max_i \left\{ \left| \binom{n}{i} x^i y^{n-i} \right| \right\} \\
&\le 4(n+1) \max_i \{|x|^i |y|^{n-i}\} \\
&\le 4(n+1) \sum_{i=0}^{n} \binom{n}{i} |x|^i |y|^{n-i} \\
&= 4(n+1)(|x| + |y|)^n\ .
\end{aligned}$$

Taking $n$-th roots, this yields

$$|x+y| \le \sqrt[n]{4(n+1)}\,(|x| + |y|)\ .$$

As $n$ tends to infinity, this gives

$$|x + y| \leq |x| + |y|$$

for all $x, y \in K$.

Thus $|\ |$ is an absolute value. □

It may be interesting to point out the particular nature of the almost valuation $N$ in the proof of (2) of the last theorem. If $\mathsf{O}$ is any other almost valuation of $K$, then $\mathsf{O} \subseteq N$. In fact, otherwise we would have an $x \in K$ such that $x \in \mathsf{O}$ and $x \notin N$. From $x \notin N$ it follows that $x^{-1}$ is nilpotent. Take now any $\mathcal{U} \in \mathsf{T}$. Since $\mathsf{O}$ is bounded, there is $\mathcal{V}$ such that $\mathsf{O}\mathcal{V} \subseteq \mathcal{U}$. As $x^{-1}$ is nilpotent, there is $n_0$ such that $x^{-n} \in \mathcal{V}$ for every $n \geq n_0$. Since $\mathsf{O}$ is multiplicatively closed, $x^n \in \mathsf{O}$ for every $n$. Thus $1 = x^n x^{-n} \in \mathsf{O}\mathcal{V} \subseteq \mathcal{U}$ for every $\mathcal{U}$, contradicting (B.1) (1).

# References


1. M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1969.
2. J. Ax, S. Kochen, Diophantine problems over local fields, I + II, Am. J. Math. **87** (1965), 605–648.
3. J. Ax, S. Kochen, Diophantine problems over local fields III, Annals of Math. **83** (1966), 437–456.
4. E. Becker, Euklidische Körper und euklidische Hüllen von Körpern, J. reine angew. Math. **268/269** (1974), 41–52.
5. C. Chevalley, Démonstration d'une hypothèse de M. Artin, Abh. Math. Sem. Univ. Hamburg **11** (1936), 73–75.
6. O. Endler, Valuation Theory, Springer-Verlag, 1972.
7. Y. L. Ershov, On the elementary theory of maximal valued field (in Russian) I, II, III, Algebra i Logika **4** (1965), **5** (1966), **6** (1967).
8. Y. L. Ershov, Multi-Valued Fields, Kluwer Academic, 2001.
9. N. Jacobson, Basic Algebraic I, Freeman and Company, 1974.
10. C. Jensen, A. Ledet, N. Yui, Generic Polynomials. Constructive Aspect of the Inverse Galois Problem, Cambridge University Press, 2002.
11. I. Kaplansky, Topological Methods in Valuation Theory, Duke Math. J. **14** (1947), 527–541.
12. J. Koenigsmann, Encoding valuations in absolute Galois groups, Fields Institute Communications **33** (2003), 107–132.
13. H.-J. Kowalsky, H. Dürbaum, Arithmetische Kennzeichnung von Körpertopologien, J. reine angew. Math. **191** (1953), 135–152.
14. S. Lang, Analysis I. Addison-Wesley, 1969.
15. S. Lang, Algebra. Addison-Wesley, 1972.
16. S. Lang, On quasi algebraic closure, Annals of Math. **55** (1952), 373–390.
17. D. J. Lewis, Cubic homogeneous polynomials over p-adic fields, Annals of Math. **56** (1952), 473–478.
18. J. Mináč, R. Ware, Demuškin groups of rank $\aleph_o$ as absolute Galois groups, manuscripta math. **73** (1991), 411–421.

19. A. Prestel, Lectures on formally real fields, Springer Lecture Notes in Mathematics, **1093** (1984).
20. A. Prestel, C. N. Delzell, Positive Polynomials, Springer Monographs in Mathematics, 2001.
21. A. Prestel, P. Roquette, Formally $p$-adic fields, Springer Lecture Notes in Mathematics, **1050** (1984).
22. A. Prestel, M. Ziegler, Model theoretic methods in the theory of topological fields, J. reine angew. Math. **299/300** (1978), 318–341.
23. P. Ribenboim, Théorie des Valuations, Université de Montréal, 1965.
24. L. Ribes, P. Zalesskii, Profinite Goups. Springer-Verlag, 2000.
25. P. Roquette, History of Valuation Theory I, Fields Institute Communications **32** (2002), 291-355.
26. J. J. Rotman, The Theory of Groups: An Introduction, Allyn and Bacon, Inc., 1965.
27. O. F. G. Schilling, The Theory of Valuations, A. M. S., 1950.
28. J.-P. Serre, Galois Cohomology, Springer Monographs in Mathematics, 2002.
29. A. L. Stone, Nonstandard analysis in topological algebra, Applications of model theory to algebra, analysis, and probability, W. A. J. Luxembourg, ed., Holt, Reinhart and Winston, Inc. New York, 1969, pp. 285–299.
30. G. Terjanian, Un contre-exemple à une conjecture d'Artin, C.R. Acad. Sci. Paris **262** (1966), 612.
31. J. S. Wilson, Profinite Groups. Clarendon Press – Oxford, 1998.
32. O. Zariski, P. Samuel, Commutative Algebra, Volume I, van Nostrand Company, 1958.
33. O. Zariski, P. Samuel, Commutative Algebra, Volume II, van Nostrand Company, 1960.

# Standard Notations

| | |
|---|---|
| $\mathbb{N}$ | : natural numbers including 0 |
| $\mathbb{Z}$ | : integers |
| $\mathbb{Q}$ | : rational number field |
| $\mathbb{R}$ | : real number field |
| $\mathbb{C}$ | : complex number field |
| $\mathbb{F}_p$ | : finite field with $p$ elements |
| $K[X]$ | : polynomial ring over $K$ |
| $K(X)$ | : rational function field over $K$ |
| $K((X))$ | : formal power series field over $K$ |
| $\mathbb{Q}_p$ | : $p$-adic number field |
| $\mathbb{Z}_p$ | : $p$-adic integers |
| $K^n$ | : set of $n$-th powers in $K$ |
| $L/K$ | : field extension |
| $\mathrm{Aut}(L/K)$ | : group of automorphisms of $L$ over $K$ |
| $G(L/K)$ | : Galois group of $L/K$ |
| $[L:K]$ | : degree of $L/K$ |
| tr.deg. $L/K$ | : transcendence degree of $L/K$ |
| $N_{L/K}$ | : norm of $L/K$ |
| $T_{L/K}$ | : trace of $L/K$ |
| $\widetilde{K}$ | : algebraic closure of $K$ |
| $K^s$ | : separable closure of $K$ |
| $(\Gamma:\Delta)$ | : group index of $\Delta$ in $\Gamma$ |
| $rk(G)$ | : rank of $G$ |
| $rr(G)$ | : rational rank of $G$ |
| $\widehat{\mathbb{Z}}$ | : Prüfer group |
| $v$ | : valuation |
| $\mathcal{O}$ | : valuation ring |
| $\mathcal{M}$ | : maximal ideal of $\mathcal{O}$ |
| $\overline{K}$ | : residue class field of $K$ |
| $v\|F$ | : restriction of $v$ to $F$ |

$(\widehat{K}, \widehat{v})$ : completion of $(K, v)$
$e(\mathcal{O}_2/\mathcal{O}_1)$ : ramification index of $\mathcal{O}_2/\mathcal{O}_1$
$f(\mathcal{O}_2/\mathcal{O}_1)$ : residue degree of $\mathcal{O}_2/\mathcal{O}_1$
$K^h$ : henselization of $(K, v)$
$K^t$ : inertia field of $(K, v)$
$K^v$ : ramification field of $(K, v)$

# Index