Lecture 1. SYSTEMS OF ALGEBRAIC EQUATIONS

The main objects of study in algebraic geometry are systems of algebraic equations and their sets of solutions. Let k be a field and $k[T_1, \dots, T_n] = k[T]$ be the algebra of polynomials in n variables over k. A *system of algebraic equations* over k is an expression

$$\{F = 0\}_{F \in S}$$

where S is a subset of $k[T]$. We shall often identify it with the subset S.

Let K be a field extension of k. A *solution* of S in K is a vector $(x_1, \dots, x_n) \in K^n$ such that for all $F \in S$

$$F(x_1, \dots, x_n) = 0.$$

Let $\mathrm{Sol}(S; K)$ denote the set of solutions of S in K. Letting K vary, we get different sets of solutions, each a subset of K^n. For example, let

$$S = \{F(T_1, T_2) = 0\}.$$

be a system consisting of one equation in two variables. Then

$\mathrm{Sol}(S; \mathbf{Q})$ is a subset of $\mathbf{Q}^2$ and its study belongs to number theory. For example one of the most beautiful results of the theory is the Mordell Theorem (until very recently the Mordell Conjecture) which gives conditions for finiteness of the set $\mathrm{Sol}(S; \mathbf{Q})$.

$\mathrm{Sol}(S; \mathbf{R})$ is a subset of $\mathbf{R}^2$ studied in topology and analysis. It is a union of a finite set and an algebraic curve, or the whole $\mathbf{R}^2$, or empty.

$\mathrm{Sol}(S; \mathbf{C})$ is a Riemann surface or its degeneration studied in complex analysis and topology. All these sets are different incarnations of the same object, an affine algebraic variety over k studied in algebraic geometry. One can generalize the notion of a solution of a system of equations by allowing K to be any commutative k-algebra. Recall that this means that K is a commutative unitary ring equipped with a structure of vector space over k so that the multiplication law in K is a bilinear map $K \times K \to K$. The map $k \to K$ defined by sending $a \in k$ to $a \cdot 1$ is an isomorphism from k to a subfield of K isomorphic to k so we can and we will identify k with a subfield of K.

The solution sets $\mathrm{Sol}(S; K)$ are related to each other in the following way. Let $\phi : K \to L$ be a homomorphism of k-algebras, i.e a homomorphism of rings which is identical on k. We can extend it to the homomorphism of the direct products $\phi^{\oplus n} : K^n \to L^n$. Then we obtain for any $a = (a_1, \dots, a_n) \in \mathrm{Sol}(S; K)$,

$$\phi^{\oplus n}(a) := (\phi(a_1), \dots, \phi(a_n)) \in Sol(S; L).$$

This immediately follows from the definition of a homomorphism of k-algebras (check it!). Let

$$sol(S; \phi) : \mathrm{Sol}(S; K) \to \mathrm{Sol}(S; L)$$

be the corresponding map of the solution sets. The following properties are immediate:

(i) $sol(S; \mathrm{id}_K) = \mathrm{id}_{\mathrm{Sol}(S;K)}$, where id_A denotes the identity map of a set A;

(ii) $sol(S; \psi \circ \phi) = sol(S; \psi) \circ sol(S; \phi)$, where $\psi : L \to M$ is another homomorphism of k-algebras.

Remark One can rephrase the previous properties by saying that the correspondences

$$K \mapsto \mathrm{Sol}(S; K), \quad \phi \to sol(S; \phi)$$

define a functor from the category of k-algebras $\mathcal{A}lg_k$ to the category of sets $\mathcal{S}ets$.

Definition Two systems of algebraic equations $S, S' \subset k[T]$ are called equivalent if $\mathrm{Sol}(S; K) = \mathrm{Sol}(S', K)$ for any k-algebra K. An equivalence class is called an *affine algebraic variety* over k (or an affine algebraic k-variety). If X denotes an affine algebraic k-variety containing a system of algebraic equations S, then, for any k-algebra K, the set $X(K) = Sol(S; K)$ is well-defined. It is called the set of *K-points* of X.

Examples. 1. The system $S = \{0\} \subset k[T_1, \ldots, T_n]$ defines an affine algebraic variety denoted by $\mathbf{A}^n_k$. It is called the *affine n-space over k*. We have, for any k-algebra K,

$$\mathrm{Sol}(\{0\}; K) = K^n.$$

2. The system $1 = 0$ defines the *empty affine algebraic variety* over k and is denoted by $\emptyset_k$. We have, for any K-algebra K,

$$\emptyset_k(K) = \emptyset.$$

We shall often use the following interpretation of a solution $a = (a_1, \ldots, a_n) \in \mathrm{Sol}(S; K)$. Let $ev_a : k[T] \to K$ be the homomorphism defined by sending each variable T_i to a_i. Then

$$a \in \mathrm{Sol}(S; K) \Longleftrightarrow ev_a(S) = \{0\}.$$

In particular, ev_a factors through the factor ring $k[T]/(S)$, where (S) stands for the ideal generated by the set S, and defines a homomorphism of k-algebras

$$ev_{S,a} : k[T]/(S) \to K.$$

Conversely any homomorphism $k[T]/(S) \to K$ composed with the canonical surjection $k[T] \to k[T]/(S)$ defines a homomorphism $k[T] \to K$. The images a_i of the variables T_i define a solution $(a_1, \ldots, a_n)$ of S since for any $F \in S$ the image $F(a)$ of F must be equal to zero. Thus we have a natural bijection

$$\mathrm{Sol}(S; K) \longleftrightarrow \mathrm{Hom}_k(k[T]/(S), K).$$

It follows from the previous interpretations of solutions that S and (S) define the same affine algebraic variety.

The next result gives a simple criterion when two different systems of algebraic equations define the same affine algebraic variety.

Proposition 1. *Two systems of algebraic equations $S, S' \subset k[T]$ define the same affine algebraic variety if and only if the ideals (S) and (S') coincide.*

Proof. The part "if" is obvious. Indeed, if $(S) = (S')$, then for every $F \in S$ we can express $F(T)$ as a linear combination of the polynomials $G \in S'$ with coefficients in $k[T]$. This shows that $\mathrm{Sol}(S'; K) \subset \mathrm{Sol}(S; K)$. The opposite inclusion is proven similarly. To prove the part "only if" we use the bjection $\mathrm{Sol}(S; K) \longleftrightarrow \mathrm{Hom}_k(k[T]/(S), K)$. Take $K = k[T]/(S)$ and $a = (t_1, \ldots, t_n)$ where t_i is the residue of T_i mod (S). For each $F \in S$,

$$F(a) = F(t_1, \ldots, t_n) \equiv F(T, \ldots, T_n) \bmod (S) = 0.$$

This shows that $a \in \mathrm{Sol}(S; K)$. Since $\mathrm{Sol}(S; K) = \mathrm{Sol}(S'; K)$, for any $F \in (S')$ we have $F(a) = F(T_1, \ldots, T_n) \mod (S) = 0$ in K, i.e., $F \in (S)$. This gives the inclusion $(S') \subset (S)$. The opposite inclusion is proven in the same way.

Example. 3. Let $n = 1, S = T = 0, S' = T^p = 0$. It follows immediately from the Proposition 1 that S and S' define different algebraic varieties X and Y. For every k-algebra K the set $\mathrm{Sol}(S; K)$ consists of one element, the zero element 0 of K. The same is true for $\mathrm{Sol}(S'; K)$ if K does not contain elements a with $a^p = 0$ (for example, K is a field, or more general, K does not have zero divisors). Thus the difference between X and Y becomes noticeable only if we admit solutions with values in rings with zero divisors.

Corollary-Definition. Let X be an affine algebraic variety defined by a system of algebraic equations $S \subset k[T_1, \ldots, T_n]$. The ideal (S) depends only on X and is called the *defining ideal* of X. It is denoted by $I(X)$. For any ideal $I \subset k[T]$ we denote by $V(I)$ the affine algebraic k-variety corresponding to the system of algebraic equations I (or, equivalently, any set of generators of I). Clearly, the defining ideal of $V(I)$ is I.

The next theorem is of fundamental importance. It shows that one can always restrict oneself to finite systems of algebraic equations.

Theorem 1 (Hilbert's Basis Theorem). *Let I be an ideal in the polynomial ring $k[T] = k[T_1, \ldots, T_n]$. Then I is generated by finitely many elements.*

Proof. The assertion is true if $k[T]$ is the polynomial ring in one variable. In fact, we know that in this case $k[T]$ is a principal ideal ring, i.e., each ideal is generated by one element. Let us use induction on the number n of variables. Every polynomial $F(T) \in I$ can be written in the form $F(T) = b_0 T_n^r + \ldots + b_r$, where b_i are polynomials in the first $n-1$ variables and $b_0 \neq 0$. We will say that r is the degree of $F(T)$ with respect to T_n and b_0 is its highest coefficient with respect to T_n. Let J_r be the subset $k[T_1, \ldots, T_{n-1}]$ formed by 0 and the highest coefficients with respect to T_n of all polynomials from I of degree r in T_n. It is immediately checked that J_r is an ideal in $k[T_1, \ldots, T_{n-1}]$. By induction, J_r is generated by finitely many elements $a_{1,r}, \ldots, a_{m(r),r} \in k[T_1, \ldots, T_{n-1}]$. Let $F_{ir}(T), i = 1, \ldots, m(r)$, be the polynomials from I which have the highest coefficient equal to $a_{i,r}$. Next, we consider the union J of the ideals J_r. By multiplying a polynomial F by a power of T_n we see that $J_r \subset J_{r+1}$. This immediately implies that the union J is an ideal in $k[T_1, \ldots, T_{n-1}]$. Let $a_1, \ldots, a_t$ be generators of this ideal (we use the induction again). We choose some polynomials $F_i(T)$ which have the highest coefficient with respect to T_n equal to a_i. Let $d(i)$ be the degree of $F_i(T)$ with respect to T_n. Put $N = \max\{d(1), \ldots, d(t)\}$. Let us show that the polynomials

$$F_{ir}, i = 1, \ldots, m(r), r < N, \quad F_i, i = 1, \ldots, t,$$

generate I.

Let $F(T) \in I$ be of degree $r \geq N$ in T_n. We can write $F(T)$ in the form

$$F(T) = (c_1 a_1 + \dots c_t a_t) T_n^r + \dots = \sum_{1 \leq i \leq t} c_i T_n^{r-d(i)} F_i(T) + F'(T),$$

where $F'(T)$ is of lower degree in T_n. Repeating this for $F'(T)$, if needed, we obtain

$$F(T) \equiv R(T) \bmod (F_1(T), \dots, F_t(T)),$$

where $R(T)$ is of degree d strictly less than N in T_n. For such $R(T)$ we can subtract from it a linear combination of the polynomials $F_{i,d}$ and decrease its degree in T_n. Repeating this, we see that $R(T)$ belongs to the ideal generated by the polynomials $F_{i,r}$, where $r < N$. Thus F can be written as a linear combination of these polynomials and the polynomials $F_1, \dots, F_t$. This proves the assertion.

Finally, we define a subvariety of an affine algebraic variety.

Definition. An affine algebraic variety Y over k is said to be a *subvariety* of an affine algebraic variety X over k if $Y(K) \subset X(K)$ for any k-algebra K. We express this by writing $Y \subset X$.

Clearly, every affine algebraic variety over k is a subvariety of some n-dimensional affine space $\mathbf{A}_k^n$ over k. The next result follows easily from the proof of Proposition 1:

Proposition 2. *An affine algebraic variety Y is a subvariety of an affine variety X if and only if $I(X) \subset I(Y)$.*

Exercises.

1. For which fields k do the systems

$$S = \{\sigma_i(T_1, \dots, T_n) = 0\}_{i=1,\dots,n}, \text{ and } S' = \{\sum_{j=1}^{n} T_j^i = 0\}_{i=1,\dots,n}$$

define the same affine algebraic varieties? Here $\sigma_i(T_1, \dots, T_n)$ denotes the elementary symmetric polynomial of degree i in $T_1, \dots, T_n$.

2. Prove that the systems of algebraic equations over the field $\mathbf{Q}$ of rational numbers

$$\{T_1^2 + T_2 = 0, T_1 = 0\} \text{ and } \{T_2^2 T_1^2 + T_1^2 + T_2^3 + T_2 + T_1 T_2 = 0, T_2 T_1^2 + T_2^2 + T_1 = 0\}$$

define the same affine algebraic $\mathbf{Q}$-varieties.

3. Let $X \subset \mathbf{A}_k^n$ and $X' \subset \mathbf{A}_k^m$ be two affine algebraic k-varieties. Let us identify the Cartesian product $K^n \times K^m$ with K^{n+m}. Define an affine algebraic k-variety such that its set of K-solutions is equal to $X(K) \times X'(K)$ for any k-algebra K. We will denote it by $X \times Y$ and call it the Cartesian product of X and Y.

4. Let X and X' be two subvarieties of $\mathbf{A}_k^n$. Define an affine algebraic variety over k such that its set of K-solutions is equal to $X(K) \cap X'(K)$ for any k-algebra K. It is called the intersection of X and X' and is denoted by $X \cap X'$. Can you define in a similar way the union of two algebraic varieties?

5. Suppose that S and S' are two systems of linear equations over a field k. Show that $(S) = (S')$ if and only if $\mathrm{Sol}(S; k) = \mathrm{Sol}(S'; k)$.

6. A commutative ring A is called *Noetherian* if every ideal in A is finitely generated. Generalize Hilbert's Basis Theorem by proving that the ring $A[T_1, \dots, T_n]$ of polynomials with coefficients in a Noetherian ring A is Noetherian.

Lecture 2. AFFINE ALGEBRAIC SETS

Let X be an affine algebraic variety over k. For different k-algebras K the sets of K-points $X(K)$ could be quite different. For example it could be empty although $X \neq \emptyset_k$. However if we choose K to be algebraically closed, $X(K)$ is always non-empty unless $X = \emptyset_k$. This follows from the celebrated Nullstellensatz of Hilbert that we will prove in this Lecture.

Definition. Let K be an algebraically closed field containing the field k. A subset V of K^n is said to be an *affine algebraic k-set* if there exists an affine algebraic variety X over k such that $V = X(K)$.

The field k is called the *ground field* or the *field of definition* of V. Since every polynomial with coefficients in k can be considered as a polynomial with coefficients in a field extension of k, we may consider an affine algebraic k-set as an affine algebraic K-set. This is often done when we do not want to specify to which field the coefficients of the equations belong. In this case we call V simply an affine algebraic set.

First we will see when two different systems of equations define the same affine algebraic set. The answer is given in the next theorem. Before we state it, let us recall that for every ideal I in a ring A its *radical* $rad(I)$ is defined by

$$rad(I) = \{a \in A : a^n \in I \quad \text{for some } n \geq 0\}.$$

It is easy to verify that $rad(I)$ is an ideal in A. Obviously it contains I.

Theorem (Hilbert's Nullstellensatz). *Let K be an algebraically closed field and S and S' be two systems of algebraic equations in the same number of variables over a subfield k. Then*

$$\mathrm{Sol}(S; K) = \mathrm{Sol}(S'; K) \Longleftrightarrow rad((S)) = rad((S')).$$

Proof. Obviously the set of zeroes of an ideal I and its radical $rad(I)$ in K^n are the same. Here we only use the fact that K has no zero divisors so that $F^n(a) = 0 \Longleftrightarrow F(a) = 0$. This proves $\Leftarrow$. Let V be an algebraic set in K^n given by a system of algebraic equations S. Let us show that the radical of the ideal (S) can be defined in terms of V only:

$$rad((S)) = \{F \in k[T] : F(a) = 0 \ \forall a \in V\}.$$

This will obviously prove our assertion. Let us denote the right-hand side by I. This is an ideal in $k[T]$ that contains the ideal (S). We have to show that for any $G \in I$, $G^r \in (S)$ for some $r \geq 0$. Now observe that the system Z of algebraic equations

$$\{F(T) = 0\}_{F \in S}, 1 - T_{n+1}G(T) = 0$$

in variables $T_1, \ldots, T_n, T_{n+1}$ defines the empty affine algebraic set in K^{n+1}. In fact, if $a = (a_1, \ldots, a_n, a_{n+1}) \in \mathrm{Sol}(Z; K)$, then $F(a_1, \ldots, a_n, a_{n+1}) = F(a_1, \ldots, a_n) = 0$ for all $F \in S$. This implies $(a_1, \ldots, a_n) \in V$ and hence

$$G(a_1, \ldots, a_n, a_{n+1}) = G(a_1, \ldots, a_n) = 0$$

and $(1 - T_{n+1}G)(a_1, \ldots, a_n, a_{n+1}) = 1 - a_{n+1}G(a_1, \ldots, a_n, a_{n+1}) = 1 \neq 0$. We will show that this implies that the ideal (Z) contains 1. Suppose this is true. Then, we may write

$$1 = \sum_{F \in S} P_F F + Q(1 - T_{n+1}G)$$

for some polynomials P_F and Q in $T_1, \ldots, T_{n+1}$. Plugging in $1/G$ instead of T_{n+1} and reducing to the common denominator, we obtain that a certain power of G belongs to the ideal generated by the polynomials $F, F \in S$.

So, we can concentrate on proving the following assertion:

Lemma 1. *If I is a proper ideal in $k[T]$, then the set of its solutions in an algebraically closed field K is non-empty.*

We use the following simple assertion which easily follows from the Zorn Lemma: every ideal in a ring is contained in a maximal ideal unless it coincides with the whole ring. Let $\mathfrak{m}$ be a maximal ideal containing our ideal I. We have a homomorphsim of rings $\phi : k[T]/I \to A = k[T]/\mathfrak{m}$ induced by the factor map $k[T] \to k[T]/\mathfrak{m}$. Since $\mathfrak{m}$ is a maximal ideal, the ring A is a field containing k as a subfield. Note that A is finitely generated as a k-algebra (because $k[T]$ is). Suppose we show that A is an algebraic extension of k. Then we will be able to extend the inclusion $k \subset K$ to a homomorphism $A \to K$ (since K is algebraically closed), the composition $k[T]/I \to A \to K$ will give us a solution of I in K^n.

Thus Lemma 1 and hence our theorem follows from the following:

Lemma 2. *Let A be a finitely generated algebra over a field k. Assume A is a field. Then A is an algebraic extension of k.*

Before proving this lemma, we have to remind one more definition from commutative algebra. Let A be a commutative ring without zero divisors (an integral domain) and B be another ring which contains A. An element $x \in B$ is said to be *integral* over A if it satisfies a monic equation : $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ with coefficients $a_i \in A$. If A is a field this notion coincides with the notion of algebraicity of x over A. We will need the following property which will be proved later (when we will deal with the concept of dimension in algebraic geometry).

Fact: The subset of elements in B which are integral over A is a subring of B.

We will prove Lemma 2 by induction on the minimal number r of generators $t_1, \ldots, t_r$ of A. If $r = 1$, the map $k[T_1] \to A$ defined by $T_1 \mapsto t_1$ is surjective. It is not injective since otherwise $A \cong k[T_1]$ is not a field. Thus $A \cong k[T_1]/(F)$ for some $F(T_1) \neq 0$, hence A is a finite extension of k of degree equal to the degree of F. Therefore A is an algebraic extension of k. Now let $r > 1$ and suppose the assertion is not true for A. Then, one of the generators $t_1, \ldots, t_r$ of A is transcendental over k. Let it be t_1. Then A contains the field $F = k(t_1)$, the minimal field containing t_1. It consists of all rational functions in t_1, i.e. ratios of the form $P(t_1)/Q(t_1)$ where $P, Q \in k[T_1]$. Clearly A is generated over F by $r - 1$ generators $t_2, \ldots, t_r$. By induction, all $t_i, i \neq 1$, are algebraic over F. We know that each $t_i, i \neq 1$, satisfies an equation of the form $a_i t_i^{d(i)} + \ldots = 0, a_i \neq 0$, where

the coefficients belong to the field F. Reducing to the common denominator, we may assume that the coefficients are polynomial in t_1, i.e., belong to the smallest subring $k[t_1]$ of A containing t_1. Multiplying each equation by $a_i^{d(i)-1}$, we see that the elements $a_i t_i$ are integral over $k[t_1]$. At this point we can replace the generators t_i by $a_i t_i$ to assume that each t_i is integral over $k[t_1]$. Now using the Fact we obtain that every polynomial expression in $t_2, \ldots, t_r$ with coefficients in $k[t_1]$ is integral over $k[t_1]$. Since $t_1, \ldots, t_r$ are generators of A over k, every element in A can be obtained as such polynomial expression. So every element from A is integral over $k[t_1]$. This is true also for every $x \in k(t_1)$. Since t_1 is transcendental over k, $k[x_1]$ is isomorphic to the polynomial algebra $k[T_1]$. Thus we obtain that every fraction $P(T_1)/Q(T_1)$, where we may assume that P and Q are coprime, satisfies a monic equation $X^n + A_1 X^n + \ldots + A_n = 0$ with coefficients from $k[T_1]$. But this is obviously absurd. In fact if we plug in $X = P/Q$ and clear the denominators we obtain

$$P^n + A_1 Q P^{n-1} + \ldots + A_n Q^n = 0,$$

hence

$$P^n = -Q(A_1 P^{n-1} + \cdots + A_n Q^{n-1}).$$

This implies that Q divides P^n and since $k[T_1]$ is a principal ideal domain, we obtain that P divides Q contradicting the assumption on P/Q. This proves Lemma 2 and also the Nullstellensatz.

Corollary 1. *Let X be an affine algebraic variety over a field k, K is an algebraically closed extension of k. Then $X(K) = \emptyset$ if and only if $1 \in I(X)$.*

An ideal I in a ring A is called *radical* if $rad(I) = I$. Equivalently, I is radical if the factor ring A/I does not contain nilpotent elements (a nonzero element of a ring is *nilpotent* if some power of it is equal to zero).

Corollary 2. *Let K be an algebraically closed extension of k. The correspondences*

$$V \mapsto I(V) := \{F(T) \in k[T] : F(x) = 0 \ \forall x \in V\},$$

$$I \mapsto V(I) := \{x \in K^n : F(x) = 0 \ \forall F \in I\}$$

define a bijective map

$$\{\text{affine algebraic } k\text{-sets in } K^n\} \to \{\text{radical ideals in } k[T]\}.$$

Corollary 3. *Let k be an algebraically closed field. Any maximal ideal in $k[T_1, \ldots, T_n]$ is generated by the polynomials $T_1 - c_1, \ldots, T_n - c_n$ for some $c_1, \ldots, c_n \in k$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal. By Nullstellensatz, $V(\mathfrak{m}) \neq \emptyset$. Take some point $x = (c_1, \ldots, c_n) \in V(\mathfrak{m})$. Now $\mathfrak{m} \subset I(\{x\})$ but since $\mathfrak{m}$ is maximal we must have the equality. Obviously, the ideal $(T_1 - c_1, \ldots, T_n - c_n)$ is maximal and is contained in $I(\{x\}) = \mathfrak{m}$. This implies that $(T_1 - c_1, \ldots, T_n - c_n) = \mathfrak{m}$.

Next we shall show that the set of algebraic k-subsets in K^n can be used to define a unique topology in K^n for which these sets are closed subsets. This follows from the following:

Proposition 1.

(i) The intersection $\cap_{s\in S}V_s$ of any family $\{V_s\}_{s\in S}$ of affine algebraic k-sets is an affine algebraic k-set in K^n.

(ii) The union $\cup_{s\in S}V_s$ of any finite family of affine algebraic k-sets is an affine algebraic k-set in K^n.

(iii) $\emptyset$ and K^n are affine algebraic k-sets.

Proof. (i) Let $I_s = I(V_s)$ be the ideal of polynomials vanishing on V_s. Let $I = \sum_s I_s$ be the sum of the ideals I_s, i.e., the minimal ideal of $k[T]$ containing the sets I_s. Since $I_s \subset I$, we have $V(I) \subset V(I_s) = V_s$. Thus $V(I) \subset \cap_{s\in S}V_s$. Since each $f \in I$ is equal to a finite sum $\sum f_s$, where $f_s \in I_s$, we see that f vanishes at each x from the intersection. Thus $x \in V(I)$, and we have the opposite inclusion.

(ii) Let I be the ideal generated by products $\prod_s f_s$, where $f_s \in I_s$. If $x \in \cup_s V_s$, then $x \in V_s$ for some $s \in S$. Hence all $f_s \in I_s$ vanishes at x. But then all products vanishes at x, and therefore $x \in V(I)$. This shows that $\cup_s V_s \subset V(I)$. Conversely, suppose that all products vanish at x but $x \notin V_s$ for any s. Then, for any $s \in S$ there exists some $f_s \in I_s$ such that $f_s(x) \neq 0$. But then the product $\prod_s f_s \in I$ does not vanish at x. This contradiction proves the opposite inclusion.

(iii) This is obvious, $\emptyset$ is defined by the system $\{1 = 0\}, K^n$ is defined by the system $\{0 = 0\}$.

Using the previous Proposition we can define the topology on K^n by declaring that its closed subsets are affine algebraic k- subsets. The previous proposition verifies the axioms. This topology on K^n is called the *Zariski k-topology* (or *Zariski topology* if $k = K$). The corresponding topological space K^n is called the n-dimensional *affine space* over k and is denoted by $\mathbf{A}^n_k(K)$. If $k = K$, we drop the subscript k and call it the n-dimensional affine space.

Example. A proper subset in $\mathbf{A}^1(K)$ is closed if and only if it is finite. In fact every ideal I in $k[T]$ is principal, so that its set of solutions coincides with the set of solutions of one polynomial. The latter set is finite unless the polynomial is identical zero.

Remark. As the previous example easily shows the Zarisky topology in K^n is not Hausdorff (=separated), however it satisfies a weaker property of separability. This is the property

(T_1): for any two points $x \neq y$ in $\mathbf{A}^n(k)$, there exists an open subset U such that $x \in U$ but $y \notin U$ (see Problem 5).

Any point $x \in V = X(K)$ is defined by the homomorphism of k-algebras $\mathrm{ev}_x : \mathcal{O}(X) \to K$. Let $\mathfrak{p} = \mathrm{Ker}(\mathrm{ev}_x)$. Since K is a field $\mathfrak{p}$ is a prime ideal. It corresponds to a closed subset which is the closure of the set $\{x\}$. Thus a point x is closed in the Zariski topology if and only if $\mathfrak{p}_x$ is a maximal ideal. By Lemma 2, in this case the quotient ring $\mathcal{O}(X)/\mathfrak{p}_x$ is an algebraic extension of k. Conversely, a finitely generated domain contained in an algebraic extension of k is a field (we shall prove it later in Lecture 10). Thus if we assume that K is an algebraic extension of k then all points of V are closed.

Problems.

1. Let $A = k[T_1, T_2]/(T_1^2 - T_2^3)$. Find an element in the field of fractions of A which is integral over A but does not belong to A.

2. Let V and V' be two affine algebraic sets in K^n. Prove that $I(V \cup V') = I(V) \cap I(V')$. Give an example where $I(V) \cap I(V') \neq I(V)I(V')$.

3. Find the radical of the ideal in $k[T_1, T_2]$ generated by the polynomials $T_1^2T_2$ and $T_1T_2^3$.

4. Show that the Zariski topology in $\mathbf{A}^n(K), n \neq 0$, is not Hausdorff but satisfies property (T_1). Is the same true for $\mathbf{A}^n_k(K)$ when $k \neq K$?

5. Find the ideal $I(V)$ of the algebraic subset of K^n defined by the equations $T_1^3 = 0, T_2^3 = 0, T_1T_2(T_1 + T_2) = 0$. Does $T_1 + T_2$ belong to $I(V)$?
6. What is the closure of the subset $\{(z_1, z_2) \in \mathbf{C}^2 \mid |z_1|^2 + |z_2|^2 = 1\}$ in the Zariski topology?

Lecture 3. MORPHISMS OF AFFINE ALGEBRAIC VARIETIES

In Lecture 1 we defined two systems of algebraic equations to be equivalent if they have the same sets of solutions. This is very familiar from the theory of linear equations. However this notion is too strong to work with. We can succeed in solving one system of equation if we would be able to find a bijective map of its set of solutions to the set of solutions of another system of equations which can be solved explicitly. This idea is used for the following notion of a morphism between affine algebraic varieties.

Definition. A *morphism* $f : X \to Y$ of affine algebraic varieties over a field k is a set of maps $f_K : X(K) \to Y(K)$ where K runs over the set of k-algebras such that for every homomorphism of k-algebras $\phi : K \to K'$ the following diagram is commutative:

$$\begin{array}{ccc} X(K) & \stackrel{X(\phi)}{\longrightarrow} & X(K') \\ f_K \downarrow & & \downarrow f_{K'} \\ Y(K) & \stackrel{Y(\phi)}{\longrightarrow} & Y(K'). \end{array} \tag{1}$$

We denote by $Mor_{\mathbf{Aff}/k}(X, Y)$ the set of morphisms from X to Y.

Remark 1. The previous definition is a special case of the notion of a morphism (or, a natural transformation) of functors.

Let X be an affine algebraic variety. We know from Lecture 1 that for every k-algebra K there is a natural bijection

$$X(K) \to \mathrm{Hom}_k(k[T]/I(X), K). \tag{2}$$

From now on we will denote the factor algebra $k[T]/I(X)$ by $\mathcal{O}(X)$ and will call it the *coordinate algebra* of X. We can view the elements of this algebra as functions on the set of points of X. In fact given a K-point $a \in X(K)$ and an element $\varphi \in \mathcal{O}(X)$ we find a polynomial $P \in k[T]$ representing φ and put

$$\varphi(a) = P(a).$$

Clearly this definition does not depend on the choice of the representative. Another way to see this is to view the point a as a homomorphism $ev_a : \mathcal{O}(X) \to K$. Then

$$\varphi(a) = ev_a(\varphi).$$

Note that the range of the function φ depends on the argument: if a is a K-point then $\varphi(a) \in K$.

Let $\psi : A \to B$ be a homomorphism of k-algebras. For every k-algebra K we have a natural map of sets $\mathrm{Hom}_k(B, K) \to \mathrm{Hom}_k(A, K)$, which is obtained by composing a map $B \to K$ with ψ. Using the bijection (2) we see that any homomorphism of k-algebras

$$\psi : \mathcal{O}(Y) \to \mathcal{O}(X)$$

defines a morphism $f : X \to Y$ by setting, for any $\psi : \mathcal{O}(X) \to K$,

$$f_K(\alpha) = \psi \circ \alpha. \tag{3}$$

Thus we have a natural map of sets

$$\xi : \mathrm{Hom}_k(\mathcal{O}(Y), \mathcal{O}(X)) \to \mathrm{Mor}_{\mathbf{Aff}/k}(X, Y). \tag{4}$$

Recall how this correspondence works. Take a K-point $a = (a_1, \ldots, a_n) \in X(K)$ in a k-algebra K. It defines a homomorphism $ev_a : \mathcal{O}(X) = k[T_1, \ldots, T_n]/I(X) \to K$ by assigning a_i to $T_i, i = 1, \ldots, n$. Composing this homomorphism with a given homomorphism $\psi : \mathcal{O}(Y) = k[T_1, \ldots, T_m]/I(Y) \to \mathcal{O}(X)$, we get a homomorphism $ev_a \circ \phi : \mathcal{O}(Y) \to K$. Let $b = (b_1, \ldots, b_m)$ where $b_i = ev_a \circ \phi(T_i), i = 1, \ldots, m$. This defines a K-point of Y. Varying K, we obtain a morphism $X \to Y$ which corresponds to the homomorphism ψ.

Proposition 1. *The map ξ from (3) is bijective.*

Proof. Let $f : X \to Y$ be a morphism. Then $f_{\mathcal{O}(X)}$ is a map from $\mathrm{Hom}_k(\mathcal{O}(X), \mathcal{O}(X))$ to $\mathrm{Hom}_k(\mathcal{O}(Y), \mathcal{O}(X))$. The image of the identity homomorphism $id_{\mathcal{O}(X)}$ is a homomorphism $\psi : \mathcal{O}(Y) \to \mathcal{O}(X)$. Let us show that $\xi(\psi) = f$. Let $\alpha \in X(K) = \mathrm{Hom}_k(\mathcal{O}(X), K)$. By definition of a morphism of affine algebraic k-varieties we have the following commutative diagram:

$$\begin{array}{ccc} X(K) = \mathrm{Hom}_k(\mathcal{O}(X), K) & \xrightarrow{f_K} & Y(K) = \mathrm{Hom}_k(\mathcal{O}(Y), K) \\ \alpha\circ? \uparrow & & \uparrow \alpha\circ? \\ X(\mathcal{O}(X)) = \mathrm{Hom}_k(\mathcal{O}(X), \mathcal{O}(X)) & \xrightarrow{f_{\mathcal{O}(X)}} & Y(\mathcal{O}(X)) = \mathrm{Hom}_k(\mathcal{O}(Y), \mathcal{O}(X)). \end{array}$$

Take the identity map $id_{\mathcal{O}(X)}$ in the left bottom set. It goes to the element α in the left top set. The bottom horizontal arrow sends $id_{\mathcal{O}(X)}$ to ψ. The right vertical arrow sends it to $\alpha \circ \psi$. Now, because of the commutativity of the diagram, this must coincide with the image of α under the top arrow, which is $f_K(\alpha)$. This proves the surjectivity. The injectivity is obvious.

As soon as we know what is a morphism of affine algebraic k-varieties we know how to define an *isomorphism*. This will be an invertible morphism. We leave to the reader to define the composition of morphisms and the identity morphism to be able to say what is the inverse of a morphism. The following proposition is clear.

Proposition 2. *Two affine algebraic k-varieties X and Y are isomorphic if and only if their coordinate k-algebras $\mathcal{O}(X)$ and $\mathcal{O}(Y)$ are isomorphic.*

Let $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$ be a homomorphism of the coordinate algebras of two affine algebraic varieties given by a system S in unknowns $T_1, \ldots, T_n$ and a system S' in unknowns $T'_1, \ldots, T'_m$. Since $\mathcal{O}(Y)$ is a homomorphic image of the polynomial algebra $k[T]$, ϕ is defined by assigning to each T'_i an element $p_i \in \mathcal{O}(X)$. The latter is a coset of a polynomial $P_i(T) \in k[T]$. Thus ϕ is defined by a collection of m polynomials $(P_1(T), \ldots, P_m(T))$ in unknowns T_j. Since the homomorphism $k[T] \to \mathcal{O}(X), T_i \to P_i(T) + I(X)$ factors through the ideal (Y), we have

$$F(P_1(T), \ldots, P_m(T)) \in I(X), \ \forall F(T'_1, \ldots, T'_n) \in I(Y). \tag{5}$$

Note that it suffices to check the previous condition only for generators of the ideal $I(Y)$, for example for the polynomials defining the system of equations Y. In terms of the polynomials $(P_1(T), \ldots, P_m(T))$ satisfying (5), the morphism $f : X \to Y$ is given as follows:

$$f_K(a) = (P_1(a), \ldots, P_m(a)) \in Y(K), \quad \forall a \in X(K).$$

It follows from the definitions that a morphism ϕ given by polynomials $((P_1(T),\dots,P_m(T))$ satisfying (5) is an isomorphism if and only if there exist polynomials $(Q_1(T'),\dots,Q_n(T'))$ such that

$$G(Q_1(T'),\dots,Q_n(T'))\in I(Y),\ \forall G\in I(X),$$

$$P_i(Q_1(T'),\dots,Q_n(T'))\equiv T_i' \bmod I(Y), i=1,\dots,m,$$

$$Q_j(P_1(T),\dots,P_m(T))\equiv T_j \bmod I(X), j=1,\dots,n.$$

The main problem of (affine) algebraic geometry is to classify affine algebraic varieties up to isomorphism. Of course, this is a hopelessly difficult problem.

Examples. 1. Let Y be given by the equation $T_1^2-T_2^3=0$, and $X=\mathbb{A}^1_k$ with $\mathcal{O}(X)=k[T]$. A morphism $f:X\to Y$ is given by the pair of polynomials (T^3,T^2). For every k-algebra K,

$$f_K(a)=(a^3,a^2)\in Y(K), a\in X(K)=K.$$

The affine algebraic varieties X and Y are not isomorphic since their coordinate rings are not isomorphic. The quotient field of the algebra $\mathcal{O}(Y)=k[T_1,T_2]/(T_1^2-T_2^3)$ contains an element $\bar{T}_1/\bar{T}_2$ which does not belong to the ring but whose square is an element of the ring $(=\bar{T}_2)$. Here the bar denotes the corresponding coset. As we remarked earlier in Lecture 2, the ring of polynomials does not have such a property.

2. The "circle" $X=\{T_1^2+T_2^2-1=0\}$ is isomorphic to the "hyperbola" $Y=\{T_1T_2-1=0\}$ provided that the field k contains a square root of -1 and $\mathrm{char}(k)\neq 2$.

3. Let $k[T_1,\dots,T_m]\subset k[T_1,\dots,T_n],\ m\leq n$, be the natural inclusion of the polynomial algebras. It defines a morphism $\mathbb{A}^t_k o\mathbb{A}^m_k$. For any k-algebra K it defines the projection map $K^n\to K^m$, $(a_1,\dots,a_n)\mapsto(a_1,\dots,a_m)$.

Consider the special case of morphisms $f:X\to Y$, where $Y=\mathbb{A}^1_k$ (the *affine line*). Then f is defined by a homomorphism of the corresponding coordinate algebras: $\mathcal{O}(Y)=k[T_1]\to\mathcal{O}(X)$. Every such homomorphism is determined by its value at T_1, i.e. by an element of $\mathcal{O}(X)$. This gives us one more interpretation of the elements of the coordinate algebra $\mathcal{O}(X)$. This time as morphisms from X to $\mathbb{A}^1_k$ and hence again can be thought as functions on X.

Let $f:X\to Y$ be a morphism of affine algebraic varieties. We know that it arises from a homomorphism of k-algebras $f^*:\mathcal{O}(Y)\to\mathcal{O}(X)$.

Proposition 3. *For any* $\varphi\in\mathcal{O}(Y)=Mor_{\mathbf{Aff}/k}(Y,\mathbb{A}^1_k)$,

$$f^*(\varphi)=\varphi\circ f.$$

Proof. This follows immediately from the above definitions.

This justifies the notation f^* (the pull-back of a function).

By now you must feel comfortable with identifying the set $X(K)$ of K-solutions of an affine algebraic k-variety X with homomorphisms $\mathcal{O}(X)\to K$. The identification of this set with a subset of K^n is achieved by choosing a set fo generators of the k-algebra $\mathcal{O}(X)$. Forgetting about generators gives a coordinate-free definition of the set $X(K)$. The correspondence $K\to\mathrm{Hom}(\mathcal{O}(X),K)$ has the property of naturality, i.e. a homomorphism of k-algebras $K\to K'$ defines a map $\mathrm{Hom}_k(\mathcal{O}(X),K)\to\mathrm{Hom}_k(\mathcal{O}(X),K')$ such that a natural diagram, which we wrote earlier, is commutative. This leads to a generalization of the notion of an affine k-variety.

Definition An (abstract) affine algebraic k-variety is the correspondence which assigns to each k-algebra K a set $X(K)$. This assignment must satisfy the following properties:

(i) for each homomorphism of k-algebras $\phi : K \to X'$ there is a map $X(\phi) : X(K) \to X(K')$;

(iii) $X(id_K) = id_{X(K)}$;

(ii) for any $\phi_1 : K \to K'$ and $\phi_2 : K' \to K''$ we have $X(\phi_2 \circ \phi_1) = X(\phi_2) \circ X(\phi_1)$;

(iv) there exists a finitely generated k-algebra A such that for each K there is a bijection $X(K) \to \mathrm{Hom}_k(A, K)$ for which the maps $X(\phi)$ correspond to the composition maps $\mathrm{Hom}(A, K) \to \mathrm{Hom}_k(A, K')$.

We leave to the reader to define a morphism of abstract affine algebraic k-varieties and prove that they are defined by a homomorphism of the corresponding algebras defined by property (iii). A choice of n generators $f_1, \ldots, f_n)$ of A defines a bijection from $X(K)$ to a subset $\mathrm{Sol}(I; K) \subset K^n$, where I is the kernel of the homomorphism $k[T_1, \ldots, T_n] \to A$, defined by $T_i \mapsto f_i$. This bijection is natural in the sense of the commutativity of the natural diagrams.

Examples. 4. The correspondence $K \to \mathrm{Sol}(S; K)$ is an abstract affine algebraic k-variety. The corresponding algebra A is $k[T]/(S)$.

5. The correspondence $K \to K^*$ (= invertible elements in K) is an abstract affine algebraic k-variety. The corresponding algebra A is equal to $k[T_1, T_2]/(T_1T_2 - 1)$. The cosets of T_1 and T_2 define a set of generators such that the corresponding affine algebraic k-variety is a subvariety of $\mathbb{A}^2$. It is denoted by $\mathbf{G}_{m,k}$ and is called the *multiplicative algebraic group* over k. Note that the maps $X(K) \to X(K')$ are homomorphisms of groups.

6. More generally we may consider the correspondence $K \to GL(n, K)$ (=invertible $n \times n$ matrices with entries in K). It is an abstract affine k-variety defined by the quotient algebra $k[T_{11}, \ldots, T_{nn}, U]/(\det((T_{ij})U - 1)$. It is denoted by $\mathbf{GL}_k(n)$ and is called the *general linear group* of order n over k.

Remark 2. We may make one step further and get rid of the assumption in (iii) that A is a finitely generated k-algebra. The corresponding generalization is called an *affine k-scheme*. Note that, if k is algebraically closed, the algebraic set $X(k)$ defined by an affine algebraic k-variety X is in a natural bjection with the set of maximal ideals in $\mathcal{O}(X)$. This follows from Corollary 2 of the Hilbert's Nullstellensatz. Thus the analog of the set $X(k)$ for the affine scheme is the set $Spm(A)$ of maximal ideals in A. For example take an affine schele defined by the ring of integers $\mathbb{Z}$. Each maximal ideal is a principal ideal generated by a prime number p. Thus the set $X(k)$ becomes the set of prime numbers. An number $m \in \mathbb{Z}$ becomes a function on the set $X(k)$. It assigns to a prime number p the image of m in $\mathbb{Z}/(p) = \mathbb{F}_p$, i.e., the residue of m modulo p.

Now, we specialize the notion of a morphism of affine algebraic varieties to define the notion of a *regular map* of affine algebraic sets.

Recall that affine algebraic k-set is a subset V of K^n of the form $X(K)$, where X is an affine algebraic variety over k and K is an algebraically closed extension of k. We can always choose V to be equal $V(I)$,where I is a radical ideal. This ideal is determined uniquely by V and is equal to the ideal $I(V)$ of polynomials vanishing on V (with coefficients in k). Each morphism $f : X \to Y$ of algebraic varieties defines a map $f_K : X(K) = V \to Y(K) = W$ of the algebraic sets. So it is natural to take for the definition of regular maps of algebraic sets the maps arising in this way. We know that f is given by a homomorphism of k-algebras $f^* : \mathcal{O}(Y) = k[T']/I(W)) \to \mathcal{O}(X) = k[T]/I(V)$. Let $P_i(T_1, \ldots, T_n), i = 1, \ldots, m$, be the representatives in $k[T]$ of the images of T_i' mod $I(W)$ inder f^*. For any $a = (a_1, \ldots, a_n) \in V$ viewed as a homomorphism $\mathcal{O}(X) \to K$ its image $f_K(a)$ is a homomorphism $\mathcal{O}(Y) \to K$ given by sending T_i' to $P_i(a), i = 1, \ldots, m$. Thus

the map f_K is given by the formula

$$f_K(a) = (P_1(a_1, \ldots, a_n), \ldots, P_m(a_1, \ldots, a_n)).$$

Note that this map does not depend on the choice of the representatives P_i of $f^*(T_i' \bmod I(W))$ since any polynomial from $I(W)$ vanishes at a. All of this motivates the following

Definition. A *regular function* on V is a map of sets $f : V \to K$ such that there exists a polynomial $F(T_1, \ldots, T_n) \in k[T_1, \ldots, T_n]$ with the property

$$F(a_1, \ldots, a_n) = f(a_1, \ldots, a_n), \forall a = (a_1, \ldots, a_n) \in V.$$

A *regular map* of affine algebraic sets $f : V \to W \subset K^m$ is a map of sets such that its composition with each projection map $pr_i : K^m \to K, (a_1, \ldots, a_n) \mapsto a_i$, is a regular function. An invertible regular map such that its inverse is also a regular map is called a *biregular map* of algebraic sets.

Remark 3. Let $k = \mathbf{F}_p$ be a prime field. The map $K \to K$ defined by $x \to x^p$ is regular and bijective (it is surjective because K is algebraically closed and it is injective because $x^p = y^p$ implies $x = y$). However, the inverse is obviously not regular.

Sometimes, a regular map is called a polynomial map. It is easy to see that it is a continuous map of affine algebraic k-sets equipped with the induced Zariski topology. However, the converse is false (Problem 7).

It follows from the definition that a regular function $f : V \to k$ is given by a polynomial $F(T)$ which is defined uniquely modulo the ideal $I(V)$ (of all polynomials vanishing identically on V). Thus the set of all regular functions on V is isomorphic to the factor-algebra $\mathcal{O}(V) = k[T]/I(V)$. It is called the *algebra of regular functions* on V, or the *coordinate algebra* of V. Clearly it is isomorphic to the coordinate algebra of the affine algebraic variety X defined by the ideal $I(V)$. Any regular map $f : V \to W$ defines a homomorphism

$$f^* : \mathcal{O}(W) \to \mathcal{O}(V), \quad \varphi \mapsto \varphi \circ f,$$

and conversely any homomorphism $\alpha : \mathcal{O}(W) \to \mathcal{O}(V)$ defines a unique regular map $f : V \to W$ such that $f^* = \alpha$. All of this follows from the discussion above.

Problems.

1. Let X be the subvariety of $\mathbb{A}^2_k$ defined by the equation $T_2^2 - T_1^2 - T_1^3 = 0$ and let $f : \mathbb{A}^1_k \to X$ be the morphism defined by the formula $T_1 \to T^2 - 1$, $T_2 \to T(T^2 - 1)$. Show that $f^*(\mathcal{O}(X))$ is the subring of $\mathcal{O}(\mathbb{A}^1_k) = k[T]$ which consists of polynomials $G(T)$ such that $g(1) = g(-1)$ (if $\mathrm{car}(k) \neq 2$) and consists of polynomials $g(T)$ with $g(1)' = 0$ if $\mathrm{char}(k) = 2$. If $\mathrm{char}(k) = 2$ show that X is isomorphic to the variety Y from Example 1.
2. Prove that the variety defined by the equation $T_1T_2 - 1 = 0$ is not isomorphic to the affine line $\mathbb{A}^1_k$.
3. Let $f : \mathbb{A}^2_k(K) \to \mathbb{A}^2_k(K)$ be the regular map defined by the formula $(x, y) \mapsto (x, xy)$. Find its image. Will it be closed, open, dense in the Zariski topology?
4. Find all isomorphisms from $\mathbb{A}^1_k$ to $\mathbb{A}^1_k$.
5. Let X and Y be two affine algebraic varieties over a field k, and let $X \times Y$ be its Cartesian product (see Problem 4 in Lecture 1). Prove that $\mathcal{O}(X \times Y) \cong \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$.
6. Prove that the correspondence $K \to O(n, K)$ ($= n \times n$-matrices with entries in K satisfying $M^T = M^{-1}$) is an abstract affine algebraic k-variety.
7. Give an example of a continuous map in the Zariski topology which is not a regular map.

Lecture 4. IRREDUCIBLE ALGEBRAIC SETS AND RATIONAL FUNCTIONS

We know that two affine algebraic k-sets V and V' are isomorphic if and only if their coordinate algebras $\mathcal{O}(V)$ and $\mathcal{O}(V')$ are isomorphic. Assume that both of these algebras are integral domains (i.e. do not contain zero divisors). Then their fields of fractions $R(V)$ and $R(V')$ are defined. We obtain a weaker equivalence of varieties if we require that the fields $R(V)$ and $R(V')$ are isomorphic. In this lecture we will give a geometric interpretation of this equivalence relation by means of the notion of a rational function on an affine algebraic set.

First let us explain the condition that $\mathcal{O}(V)$ is an integral domain. We recall that $V \subset K^n$ is a topological space with respect to the induced Zariski k-topology of K^n. Its closed subsets are affine algebraic k-subsets of V. From now on we denote by $V(I)$ the affine algebraic k-subset of K^n defined by the ideal $I \subset k[T]$. If $I = (F)$ is the principal ideal generated by a polynomial F, we write $V((F)) = V(F)$. An algebraic subsets of this form, where $(F) \neq \{0\}, (1)$, is called a *hypersurface*.

Definition. A topological space V is said to be *reducible* if it is a union of two proper non-empty closed subsets (equivalently, there are two open disjoint proper subsets of V). Otherwise V is said to be *irreducible*. By definition the empty set is irreducible. An affine algebraic k-set V is said to be reducible (resp. irreducible) if the corresponding topological space is reducible (resp. irreducible).

Remark 1. Note that a Hausdorff topological space is always reducible unless it consists of at most one point. Thus the notion of irreducibility is relevant only for non-Hausdorff spaces. Also one should compare it with the notion of a connected space. A topological spaces X is *connected* if it is not equal to the union of two disjoint proper closed (equivalently open) subsets. Thus an irreducible space is always connected but the converse is not true in general.

For every affine algebraic set V we denote by $I(V)$ the ideal of polynomials vanishing on V. Recall that, by Nullstellensatz, $I(V(I)) = \mathrm{rad}(I)$.

Proposition 1. *An affine algebraic set V is irreducible if and only if its coordinate algebra $O(V)$ has no zero divisors.*

Proof. Suppose V is irreducible and $a, b \in \mathcal{O}(V)$ are such that $ab = 0$. Let $F, G \in k[T]$ be their representatives in $k[T]$. Then $ab = FG + I(V) = 0$ implies that the polynomial FG vanishes on V. In particular, $V \subset V(F) \cup V(G)$ and hence $V = V_1 \cup V_2$ is the union of two closed subsets $V_1 = V \cap V(F)$ and $V_2 = V \cap V(G)$. By assumption, one of them, say V_1, is equal to V. This implies that $V \subset V(F)$, i.e., F vanishes on V, hence $F \in I(V)$ and $a = 0$. This proves that $\mathcal{O}(V)$ does not have zero divisors.

Conversely, suppose that $\mathcal{O}(V)$ does not have zero divisors. Let $V = V_1 \cup V_2$ where V_1 and V_2 are closed subsets. Let $F \in I(V_1)$ and $G \in I(V_2)$. Then $FG \in I(V_1 \cup V_2)$ and $(F+I(V))(G+I(V)) =$

0 in $\mathcal{O}(V)$. Since $\mathcal{O}(V)$ has no zero divisors, one of the cosets is zero, say $F + I(V)$. This implies that $F \in I(V)$ and $I(V_1) \subset I(V)$, i.e., $V = V_1$. This proves the irreducibility of V.

Definition. A topological space V is called *Noetherian* if every strictly decreasing sequence $Z_1 \supset Z_2 \supset \ldots \supset Z_k \supset$ of closed subsets is finite.

Proposition 2. *An affine algebraic set is a Noetherian topological space.*

Proof. Every decreasing sequence of closed subsets $Z_1 \supset Z_2 \supset \ldots \supset Z_j \supset \ldots$ is defined by the increasing sequence of ideals $I(V_1) \subset I(V_2) \subset \ldots$. By Hilbert's Basis Theorem their union $I = \cup_j I(V_j)$ is an ideal generated by finetely many elements $F_1, \ldots, F_m$. All of them lie in some $I(V_N)$. Hence $I = I(V_N)$ and $I(V_j) = I = I(V_N)$ for $j \geq N$. Returning to the closed subsets we deduce that $Z_j = Z_N$ for $j \geq N$.

Theorem 1. *Let V be a Noetherian topological space. Then V is a union of finitely many irreducible closed subsets V_k of V. Furthermore, if $V_i \not\subset V_j$ for any $i \neq j$, then the subsets V_k are defined uniquely.*

Proof. Let us prove the first part. If V is irreducible, then the assertion is obvious. Otherwise, $V = V_1 \cup V_2$, where V_i are proper closed subsets of V. If both of them are irreducible, the assertion is true. Otherwise, one of them, say V_1 is reducible. Hence $V_1 = V_{11} \cup V_{12}$ as above. Continuing in this way, we either stop somewhere and get the assertion or obtain an infinite strictly decreasing sequence of closed subsets of V. The latter is impossible because V is Noetherian. To prove the second assertion, we assume that

$$V = V_1 \cup \ldots \cup V_k = W_1 \cup \ldots \cup W_t,$$

where neither V_i (resp. W_j) is contained in another $V_{i'}$ (resp. $W_{j'}$). Obviously,

$$V_1 = (V_1 \cap W_1) \cup \ldots (V_1 \cap W_t).$$

Since V_1 is irreducible, one of the subsets $V_1 \cap W_i$ is equal to V_1, i.e., $V_1 \subset W_j$. We may assume that $j = 1$. Similarly, we show that $W_1 \subset V_i$ for some i. Hence $V_1 \subset W_1 \subset V_i$. This contradicts the assumption $V_i \not\subset V_j$ for $i \neq j$ unless $V_1 = W_1$. Now we replace V by $V_2 \cup \ldots \cup V_k = W_2 \cup \ldots \cup W_t$ and repeat the argument.

An irreducible closed subset Z of a topological space X is called an *irreducible component* if it is not properly contained in any irreducible closed subset. Let V be a Noetherian topological space and $V = \cup_i V_i$, where V_i are irreducible closed subsets of V with $V_i \not\subset V_j$ for $i \neq j$, then each V_i is an irreducible component. Otherwise V_i is contained properly in some Z, and $Z = \cup_i (Z \cap V_i)$ would imply that $Z \subset V_i$ for some i hence $V_i \subset V_k$. The same argument shows that every irreducible component of X coincides with one of the V_i's.

Remark 2. Compare this proof with the proof of the theorem on factorization of integers into prime factors. Irreducible components play the role of prime factors.

In view of Proposition 2, we can apply the previous terminology to affine algebraic sets V. Thus, we can speak about irreducible affine algebraic k-sets, irreducible components of V and a decomposition of V into its irreducible components. Notice that our topology depends very much on the field k. For example, an irreducible k-subset of K is the set of zeroes of an irreducible polynomial in $k[T]$. So a point $a \in K$ is closed only if $a \in k$. We say that V is *geometrically irreducible* if it is irreducible considered as a K-algebraic set.

Recall that a polynomial $F(T) \in k[T]$ is said to be irreducible if $F(T) = G(T)P(T)$ implies that one of the factors is a constant (since $k[T]^* = k^*$, this is equivalent to saying that $F(T)$ is an irreducible or prime element of the ring $k[T]$).

Lemma. *Every polynomial $F \in k[T_1, \ldots, T_n]$ is a product of irreducible polynomials which are defined uniquely up to multiplication by a constant.*

Proof. This follows from the well-known fact that the ring of polynomials $k[T_1, \ldots, T_n]$ is a UFD (a unique factorization domain). The proof can be found in any advanced text-book of algebra.

Proposition 3. *Let $F \in k[T]$. A subset $Z \subset K^n$ is an irreducible component of the affine algebraic set $V = V(F)$ if and only if $Z = V(G)$ where G is an irreducible factor of F. In particular, V is irreducible if and only if F is an irreducible polynomial.*

Proof. Let $F = F_1^{a_1} \ldots F_r^{a_r}$ be a decomposition of F into a product of irreducible polynomials. Then

$$V(F) = V(F_1) \cup \ldots \cup V(F_r)$$

and it suffices to show that $V(F_i)$ is irreducible for every $i = 1, \ldots, r$. More generally, we will show that $V(F)$ is irreducible if F is irreducible. By Proposition 1, this follows from the fact that the ideal (F) is prime. If (F) is not prime, then there exist $P, G \in k[T] \setminus (F)$ such that $PG \in (F)$. The latter implies that $F|PG$. Since F is irreducible, $F|P$ or $F|G$ (this follows easily from the above Lemma). This contradiction proves the assertion.

Let $V \subset K^n$ be an irreducible affine algebraic k-set and $\mathcal{O}(V)$ be its coordinate algebra. By Proposition 1, $\mathcal{O}(V)$ is a domain, therefore its quotient field $Q(\mathcal{O}(V))$ is defined. We will denote it by $R(V)$ and call it the *field of rational functions* on V. Its elements are called *rational functions* on V.

Recall that for every integral domain A its quotient field $Q(A)$ is a field uniquely determined (up to isomorphisms) by the following two conditions:

(i) there is an injective homomorphism of rings $i : A \to Q(A)$;

(ii) for every injective homomorphism of rings $\phi : A \to K$, where K is a field, there exists a unique homomorphism $\bar{\phi} : Q(A) \to K$ such that $\bar{\phi} \circ i = \phi$.

The field $Q(A)$ is constructed as the factor-set $A \times (A \setminus \{0\})/R$, where R is the equivalence relation $(a, b) \sim (a', b') \Longleftrightarrow ab' = a'b$. Its elements are denoted by $\frac{a}{b}$ and added and multiplied by the rules

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$

The homomorphism $i : A \to Q(A)$ is defined by sending $a \in A$ to $\frac{a}{1}$. Any homomorphism $\phi : A \to K$ to a field K extends to a homomorphism $\bar{\phi} : Q(A) \to K$ by sending $\frac{a}{b}$ to $\frac{\phi(a)}{\phi(b)}$. We will identify the ring A with the subring $i(A)$ of $Q(A)$. Notice that, if A happens to be a k-algebra. In particular, the field $R(V)$ will be viewed as an extension $k \subset \mathcal{O}(V) \subset R(V)$. We will denote the field of fractions of the polynomial ring $k[T_1, \ldots, T_n]$ by $k(T_1, \ldots, T_n)$. It is called the field of rational functions in n variables.

Definition. A *dominant rational k-map* from an irreducible affine algebraic k-set V to an irreducible affine algebraic k-set W is a homomorphism of k-algebras $f : k(W) \to R(V)$. A *rational map* from V to W is a dominant rational map to a closed irreducible subset of W.

Let us interpret this notion geometrically. Restricting f to $\mathcal{O}(W)$ and composing with the factor map $k[T'_1, \ldots, T'_m] \to \mathcal{O}(W)$, we obtain a homomorphism $k[T'_1, \ldots, T'_m] \to R(V)$. It is given by rational functions $R_1, \ldots, R_m \in R(V)$, the images of the T_i's. Since every $G \in I(W)$ goes to zero, we have $G(R_1, \ldots, R_m) = 0$. Now each R_i can be written as

$$R_i = \frac{P_i(T_1, \ldots, T_n) + I(V)}{Q_i(T_1, \ldots, T_n) + I(V)},$$

where P_i and Q_i are elements of $k[T_1, \dots, T_n]$ defined up to addition of elements from $I(V)$. If $a \in V$ does not belong to the set $Z = V(Q_1) \cup \dots \cup V(Q_n)$, then

$$\alpha(a) = (R_1(a), \dots, R_m(a)) \in K^m$$

is uniquely defined. Since $G(R_1(a), \dots, R_m(a)) = 0$ for any $G \in I(W)$, $\alpha(a) \in W$. Thus, we see that f defines a map $\alpha : V \setminus Z \to W$ which is denoted by

$$\alpha : V \dashrightarrow W.$$

Notice the difference between the dotted and the solid arrow. A rational map is not a map in the usual sense because it is defined only on an open subset of V. Clearly a rational map is a generalization of a regular map of irreducible algebraic sets. Any homomorphism of k-algebras $\mathcal{O}(W) \to \mathcal{O}(V)$ extends uniquely to a homomorphism of their quotient fields.

Let us see that the image of α is dense in W (this explains the word dominant). Assume it is not. Then there exists a polynomial $F \notin I(W)$ such that $F(R_1(a), \dots, R_m(a)) = 0$ for any $a \in V \setminus Z$. Write

$$f(F) = F(R_1, \dots, R_m) = \frac{P(T_1, \dots, T_n)}{Q(T_1, \dots, T_n)}.$$

We have $P(T_1, \dots, T_n) \equiv 0$ on $V \setminus Z$. Since $V \setminus Z$ is dense in the Zariski topology, $P \equiv 0$ on V, i.e. , $P \in I(V)$. This shows that under the map $k(W) \to R(V)$, F goes to 0. Since the homomorphism $k(W) \to R(V)$ is injective (any homomorphism of fields is injective) this is absurd.

In particular, taking $W = \mathbb{A}^1_k(K)$, we obtain the interpretation of elements of the field $R(V)$ as non-constant rational functions $V \dashrightarrow K$ defined on an open subset of V (the complement of the set of the zeroes of the denominator). From this point of view, the homomorphism $k(W) \to R(V)$ defining a rational map $f : V \dashrightarrow W$ can be interpreted as the homomorphism f^* defined by the composition $\phi \mapsto \phi \circ f$.

Definition. A rational map $f : V \dashrightarrow W$ is called *birational* if the corresponding field homomorphism $f^* : k(W) \to R(V)$ is an isomorphism. Two irreducible affine algebraic sets V and W are said to be *birationally isomorphic* if there exists a birational map from V to W.

Clearly, the notion of birational isomorphism is an equivalence relation on the set of irreducible affine algebraic sets. If $f : V \dashrightarrow W$ is a birational map, then there exists a birational map $f : W \dashrightarrow V$ such that the compositions $f \circ f'$ and $f' \circ f$ are defined on an open subsets U and U' of V and W, respectively, with $f \circ f' = \mathrm{id}'_U$, $f' \circ f = \mathrm{id}_U$.

Remark 3. One defines naturally the category whose objects are irreducible algebraic k-sets with morphisms defined by rationa maps. A birational map is an isomorphism in this category.

Example. 1. Let $V = \mathbb{A}^1_k(K)$ and $W = V(T_1^2 + T_2^2 - 1) \subset K^2$. We assume that $\mathrm{char}(k) \neq 2$. A rational map $f : V \dashrightarrow W$ is given by a homomorphism $f^* : k(W) \to R(V)$. Restricting it to $\mathcal{O}(W)$ and composing it with $k[T_1, T_2] \to \mathcal{O}(W)$, we obtain two rational functions $R_1(T)$ and $R_2(T)$ such that $R_1(T)^2 + R_2(T)^2 = 1$ (they are the images of the unknowns T_1 and T_2. In other words, we want to find "a rational parametrization" of the circle, that is we want to express the coordinates (t_1, t_2) of a point lying on the circle as a rational function of one parameter. It is easy to do this by passing a line through this point and the fixed point on the circle, say $(1, 0)$. The slope of this line is the parameter associated to the point. Explicitly, we write $T_2 = T(T_1 - 1)$, plug into the equation $T_1^2 + T_2^2 = 1$ and find

$$T_1 = \frac{T^2 - 1}{T^2 + 1}, \quad T_2 = \frac{-2T}{T^2 + 1}.$$

Thus, our rational map is given by

$$T_1 \mapsto \frac{T^2-1}{T^2+1}, \quad T_2 \mapsto \frac{-2T}{T^2+1}.$$

Next note that the obtained map is birational. The inverse map is given by

$$T \mapsto \frac{T_2}{T_1-1}.$$

In particular, we see that

$$R(V(T_1^2+T_2^2-1)) \cong k(T_1).$$

The next theorem, although sounding as a deep result, is rather useless for concrete applications.

Theorem 2. *Assume k is of characteristic 0. Then any irreducible affine algebraic k-set is birationally isomorphic to an irreducible hypersurface.*

Proof. Since $R(V)$ is a finitely generated field over k, it can be obtained as an algebraic extension of a purely transcendental extension $L = k(t_1, \ldots, t_n)$ of k. Since $\mathrm{char}(k) = 0, R(V)$ is a separable extension of L, and the theorem on a primitive element applies (M. Artin, "Algebra", Chapter 14, Theorem 4.1): an algebraic extension K/L of characteristic zero is generated by one element $x \in K$. Let $k[T_1, \ldots, T_{n+1}] \to R(V)$ be defined by sending T_i to t_i for $i = 1, \ldots, n$, and T_{n+1} to x. Let I be the kernel, and $\phi : A = k[T_1, \ldots, T_{n+1}]/I \to R(V)$ be the corresponding injective homomorphism. Every $P(T_1, \ldots, T_{n+1}) \in I$ is mapped to $P(t_1, \ldots, t_n, x) = 0$. Considering $P(x_1, \ldots, x_n, T_{n+1})$ as an element of $L[T_{n+1}]$ it must be divisible by the minimal polynomial of x. Hence $I = (F(T_1, \ldots, T_n, T_{n+1}))$, where $F(t_1, \ldots, t_n, T_{n+1})$ is a product of the minimal polynomial of x and some polynomial in $t_1, \ldots, t_n$. Since A is isomorphic to a subring of a field it must be a domain. By definition of the quotient field ϕ can be extended to a homomorphism of fields $Q(A) \to R(V)$. Since $R(V)$ is generated as a field by elements in the image, ϕ must be an isomorphism. Thus $R(V)$ is isomorphic to $Q(k[T_1, \ldots, T_{n+1}]/(F))$ and we are done.

Remark 4. The assumption $\mathrm{char}(k) = 0$ can be replaced by the weaker assumption that k is a perfect field, for example, k is algebraically closed. In this case one can show that $R(V)$ is a separable extension of some purely transcendental extension of k.

Definition. An irreducible affine algebraic k-set V is said to be *k-rational* if $R(V) \cong k(T_1, \ldots, T_n)$ for some n. V is called rational if, viewed as algebraic K-set, it is K-rational.

Examples. 2. Assume $\mathrm{char}(k) \neq 2$. The previous example shows that the circle $V(T_1^2 + T_2^2 - 1)$ is k-rational for any k. On the other hand, $V(T_1^2 + T_2^2 + 1)$ is k-rational only if k contains $\sqrt{-1}$.
3. An affine algebraic set given by a system of linear equations is always rational (Prove it!).
4. $V(T_1^2 + T_2^3 - 1)$ is not rational. Unfortunately, we do not have yet sufficient tools to show this.
5. Let $V = V(T_1^3 + \ldots + T_n^3 - 1)$ be a "cubic hypersurface ". It is known that V is not rational for $n = 2$ and rational for $n = 3$. It was an open question for many years whether V is rational for $n = 4$. The negative answer to this problem was given by Herb Clemens and Phil Griffiths in 1972. It is known that V is rational for $n \geq 5$ however it is not known whether $V(F)$ is rational for any irreducible polynomial of degree 3 in $n \geq 5$ variables.

An irreducible algebraic set V is said to be *k-unirational* if its field of rational functions $R(V)$ is isomorphic to a subfield of $k(T_1, \ldots, T_n)$ for some n. It was an old problem (the Lüroth Problem) whether, for $k = \mathbf{C}$, there exist k-unirational sets which are not k-rational. The theory of algebraic curves easily implies that this is impossible if $\mathbf{C}(V)$ is transcendence degree 1 over $\mathbf{C}$. A purely

algebraic proof of this fact is not easy (see P. Cohn, "Algebra"). The theory of algebraic surfaces developed in the end of the last century by Italian geometers implies that this is impossible if $\mathbf{C}(V)$ of transcendence degree 2 over $\mathbf{C}$. No purely algebraic proofs of this fact is known. Only in 1972-73 a first example of a unirational non-rational set was constructed. In fact, there given independently 3 counterexamples (by Clemens-Griffiths, by Mumford-Artin and Iskovskih-Manin). The example of Clemens-Griffiths is the cubic hypersurface $V(T_1^3 + T_2^3 + T_3^3 + T_4^3 - 1)$.

Finally we note that we can extend all the previous definitions to the case of affine algebraic varieties. For example, we say that an affine algebraic variety X is irreducible if its coordinate algebra $\mathcal{O}(X)$ is an integral domain. We leave to the reader to do all these generalizations.

Problems.

1. Let k be a field of characteristic $\neq 2$. Find irreducible components of the affine algebraic k-set defined by the equations $T_1^2 + T_2^2 + T_3^2 = 0, T_1^2 - T_2^2 - T_3^2 + 1 = 0$.

2. Same for the set defined by the equations $T_2^2 - T_1T_3 = 0, T_1^2 - T_2^3 = 0$. Prove that all irreducible components of this set are birationally isomorphic to the affine line.

3. Let $f : X(K) \to Y(K)$ be the map defined by the formula from Problem 1 of Lecture 3. Show that f is a biratioanl map.

4. Let $F(T_1, \ldots, T_n) = G(T_1, \ldots, T_n) + H(T_1, \ldots, T_n)$, where G is a homogeneous polynomial of degree $d - 1$ and H is a homogeneous polynomial of degree d. Assuming that F is irreducible, prove that the algebraic set $V(F)$ is rational.

5. Prove that the affine algebraic sets given by the systems $T_1^3 + T_2^3 - 1 = 0$ and $T_1^2 - T_2^3/3 + 1/12 = 0$ are birationally isomorphic.

Lecture 5. PROJECTIVE ALGEBRAIC VARIETIES

Let A be a commutative ring and A^{n+1} $(n \geq 0)$ be the Cartesian product equipped with the natural structure of a free A-module of rank $n+1$. A free submodule M of A^{n+1} of rank 1 is said to be a *line* in A^{n+1}, if $M = Ax$ for some $x = (a_0, \ldots, a_n)$ such that the ideal generated by $a_0, \ldots, a_n$ contains 1. We denote the set of lines in A^{n+1} by $\mathbb{P}^n(A)'$. One can define $\mathbb{P}^n(A)'$ also as follows. Let

$$C(A)_n = \{x = (a_0, \ldots, a_n) \in A^{n+1} : (a_0, \ldots, a_n) = 1\}.$$

Then each line is generated by an element of $C(A)_n$. Two elements $x, y \in C(A)_n$ define the same line if and only if $x = \lambda y$ for some invertible $\lambda \in A$. Thus

$$\mathbb{P}^n(A)' = C(A)_n / A^*,$$

is the set of orbit of the group A^* of invertible elements of A acting on $C(A)_n$ by the formula $\lambda \cdot (a_0, \ldots, a_n) = (\lambda a_0, \ldots, \lambda a_n)$. Of course, in the case where A is a field,

$$C(A)_n = A^{n+1} \setminus \{0\}, \quad \mathbb{P}^n(A)' = (A^{n+1} \setminus \{0\})/A^*.$$

If $M = Ax$, where $x = (a_0, \ldots, a_n) \in C(A)_n$, then $(a_0, \ldots, a_n)$ are called the *homogeneous coordinates* of the line. In view of the above they are determined uniquely up to an invertible scalar factor $\lambda \in A^*$.

Examples. 1. Take $A = \mathbb{R}$. Then $\mathbb{P}^1(\mathbb{R})'$ is the set of lines in $\mathbb{R}^2$ passing through the origin. By taking the intersection of the line with the unit circle we establish a bijective correspondence between $\mathbb{P}^1(\mathbb{R})$ and the set of points on the unit circle with the identification of the opposite points. Or choosing a representative on the upper half circle we obtain a bijective map from $\mathbb{P}^1(\mathbb{R})'$ to the half circle with the two ends identified. This is bijective to a circle. Similarly we can identify $\mathbb{P}^2(\mathbb{R})'$ with the set of points in the upper unit hemi-sphere such that the opposite points on the equator are identified. This is homeomorphic to the unit disk where the opposite points on the boundary are identified. The obtained topological space is called the *real projective plane* and is denoted by $\mathbb{RP}^2$.
2. Take $A = \mathbb{C}$. Then $\mathbb{P}^1(\mathbb{C})'$ is the set of one-dimensional linear subspaces of $\mathbb{C}^2$. We can choose a unique basis of $x \in \mathbb{P}^1(\mathbb{C})'$ of the form $(1, z)$ unless $x = (0, z)$, $z \in \mathbb{C}\setminus\{0\}$, and $\mathbb{C}x = \mathbb{C}(0, 1)$. In this way we obtain a bijective map from $\mathbb{P}^1(\mathbb{C})'$ to $\mathbf{C} \cup \{\infty\}$, the extended complex plane. Using the stereographic projection, we can identify the latter set with a 2-dimensional sphere. The complex coordinates make it into a compact complex manifold of dimension 1, the *Riemann sphere* $\mathbf{C}\mathbb{P}^1$.

Any homomorphism of rings $\phi : A \to B$ extends naturally to the map $\tilde{\phi} = \phi^{\oplus n} : A^{n+1} \to B^{n+1}$. If $x = (a_0, \ldots, a_n) \in C(A)_n$, then one can write $1 = a_0 b_0 + \ldots + a_n b_n$ for some $b_i \in A$. Applying ϕ, we obtain $1 = \phi(a_0)\phi(b_0) + \ldots + \phi(a_n)\phi(b_n)$. This shows that $\tilde{\phi}(x) \in C(B)_n$. This

defines a map $\tilde{\phi} : C_n(A) \to C_n(B)$. Also $a = \lambda b \Longleftrightarrow \tilde{\phi}(a) = \phi(\lambda)\tilde{\phi}(b)$. Hence $\tilde{\phi}$ induces the map of equivalence classes

$$'\mathbb{P}^n(\phi) : \mathbb{P}^n(A)' \to \mathbb{P}^n(B).$$

For our future needs we would like to enlarge the set $\mathbb{P}^n(A)'$ a little further to define the set $\mathbb{P}^n(A)$. We will not be adding anything if A is a field.

Let $M = Ax \subset A^{n+1}, x = (a_0, \ldots, a_n) \in C_n(A)$, be a line in A^{n+1}. Choose $b_0, \ldots, b_n \in A$ such that $\sum_i b_i a_i = 1$. Then the homomorphism $\phi : A^{n+1} \to M$ defined by $(\alpha_0, \ldots, \alpha_n) \mapsto (\sum_i \alpha_i b_i)x$ is surjective, and its restriction to M is the identity. Since for any $m \in A^{n+1}$ we have $m - \phi(m) \in \mathrm{Ker}(\phi)$, and $M \cap \mathrm{Ker}(\phi) = \{0\}$, we see that

$$A^{n+1} \cong M \oplus \mathrm{Ker}(\phi).$$

So each line is a direct summand of A^{n+1}. Not each direct summand of A^{n+1} is necessarily free. So we can enlarge the set $\mathbb{P}^n(A)'$ by adding to it not necessarily free direct summands of A^{n+1} which become free of rank 1 after "localizing" the ring. Let us explain the latter.

Let S be a non-empty multiplicatively closed subset of A containing 1. One defines the *localization* M_S of an A-module M in the similar way as one defines the field of fractions: it is the set of equivalence classes of pairs $(m, s) \in M \times S$ with the equivalence relation: $(m, s) \equiv (m', s') \Longleftrightarrow \exists s'' \in S$ such that $s''(s'm - sm') = 0$. The equivalence class of a pair (m, s) is denoted by $\frac{m}{s}$. The equivalence classes can be added by the natural rule

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'}$$

(one verified that this definition is independent of a choice of a representative). If $M = A$, one can also multiply the fractions by the rule

$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss}.$$

Thus A_S becomes a ring such that the natural map $A \to A_S, a \mapsto \frac{a}{1}$, is a homomorphism of rings. The rule

$$\frac{a}{s} \cdot \frac{m}{s'} = \frac{am}{ss'}.$$

equips M_S with the structure of an A_S-module. Note that $M_S = \{0\}$ if $0 \in S$. Observe also that there is a natural isomorphism of A_S-modules

$$M \otimes_A A_S \to M_S, m \otimes \frac{a}{s} \mapsto \frac{am}{s},$$

where A_S is equipped with the structure of an A-module by means of the canonical homomorphism $A \to A_S$.

Examples 3. Take S to be the set of elements of A which are not zero-divisors. This is obvioulsy a multiplicatively closed subset of A. The localized ring A_S is called the *total ring of fractions*. If A is a domain, $S = A \setminus \{0\}$, and we get the field of fractions.

4. Let $\mathfrak{p}$ be a prime ideal in A. By definition of a prime ideal, the set $A \setminus \mathfrak{p}$ is multiplicatively closed. The localized ring $A_{A\setminus\mathfrak{p}}$ is denoted by $A_\mathfrak{p}$ and is called the *localization of A at a prime ideal* $\mathfrak{p}$. For example, take $A = \mathbb{Z}$ and $\mathfrak{p} = (p)$, where p is a prime number. The ring $\mathbb{Z}_{(p)}$ is isomorphic to the subring of $\mathbb{Q}$ which consists of fractions such that the denominator is not divisible by p.

As we saw earlier any line $L = Ax \in \mathbb{P}^n(A)'$ is a direct summand of the free module A^{n+1}. In general not every direct summand of a free module is free.

Definition. A *projective module* over A is a finitely generated module P over A satisfying one of the following equivalent properties:

(i) P is isomorphic to a direct summand of a free module;

(ii) For every surjective homomorphism $\phi : M \to P$ of A-modules there is a homomorphism $s : P \to M$ such that $\phi \circ s = id_P$ (a section).

Let us prove the equivalence.

(ii)$\Rightarrow$ (i) Let $A^n \to P$ be the surjective homomorphism corresponding to a choice of generators of P. By property(i) there is a homomorphism $s : P \to A^n$ such that $\phi \circ s = id_P$. Let $N = Ker(\phi)$. Consider the homomorphism $(i, s) : N \oplus P \to A^n$, where i is the identity map $N \to A^n$. It has the inverse given by $m \mapsto (m - \phi(m), \phi(m))$

(i)$\Rightarrow$ (ii) Assume $P \oplus N \cong A^n$. Without loss of generality we may assume that P, N are submodules of A^n. Let $\phi : M \to P$ be a surjective homomorphism of A-modules. We extend it to a surjective homomorphism $(\phi, id_N) : M \oplus N \to A^n$. If we prove property (ii) for free modules, we will be done since the restriction of the corresponding section to P is a section of ϕ. So let $\phi : M \to A^n$ be a surjective homomorphism. Let $m_1, \ldots, m_n$ be some pre-images of the elements of a basis $(\xi_1, \ldots, \xi_n)$ of A^n. The homomorphism $A^n \to M$ defined by $\xi \mapsto m_i$ is well-defined and is a section.

We saw in the previous proof that a free finitely generated module is projective. In general, the converse is not true. For example, let $K/\mathbb{Q}$ be a finite field extension, and A be the ring of integers of K, i.e. the subring of elements of K which satisfy a monic equation with coefficients in $\mathbb{Z}$. Then any ideal in A is a projective module but not necessarily a principal ideal.

An important class of rings A such that any projective module over A is free is the class of local rings.

A commutative ring is called *local* if it has a unique maximal ideal. For example, any field is local. The ring of power series $k[[T_1, \ldots, T_n]]$ is local (the maximal ideal is the set of infinite formal series with zero constant term).

Lemma 1. *Let A be a local ring and $\mathfrak{m}$ be its unique maximal ideal. Then $A \setminus \mathfrak{m} = A^*$ (the set of invertible elements in A).*

Proof. Let $x \in A \setminus \mathfrak{m}$. Then the principal ideal (x) is contained in some proper maximal ideal unless $(x) = A$ which is equivalent to $x \in A^*$. Since A has only one maximal ideal and it does not contain x, we see that $(x) = A$.

Proposition 1. *A projective module over a local ring is free.*

Proof. Let $\mathrm{Mat}_n(A)$ be the ring of $n \times n$ matrices with coefficients in a commutative ring A. For any ideal I in A we have a natural surjective homomorphism of rings $\mathrm{Mat}_n(A) \to \mathrm{Mat}_n(A/I), A \mapsto \bar{A}$, which obtained by replacing each entry of a matrix with its residue modulo I. Now let A be a local ring, $I = \mathfrak{m}$ be its unique maximal ideal, and $k = A/\mathfrak{m}$ (the *residue field* of A). Suppose $A \in \mathrm{Mat}_n(A)$ is such that $\bar{A}$ is an invertible matrix in $\mathrm{Mat}_n(k)$. I claim that A is invertible in A. In fact, let $\bar{B} \cdot \bar{A} = I_n$ for some $B \in \mathrm{Mat}_n(A)$. The matrix BA has diagonal elements congruent to 1 modulo $\mathfrak{m}$ and all off-diagonal elements belonging to $\mathfrak{m}$. By Lemma 1, the diagonal elements of BA are invertible in A. It is easy to see that each elementary row transformation preserve this property. This shows that there exists a matrix $S \in \mathrm{Mat}_n(A)$ such that $S(BA) = (SB)A = I_n$. Similarly we show that A has the right inverse, and hence is invertible.

Let M be a A-module and $I \subset A$ an ideal. Let IM denote the submodule of M generated by all products am, where $a \in I$. The quiotient module $M = M/IM$ is a A/I-module via the scalar multiplication $(a+I)(m+IM) = am + IM$. There is an isomorphism of A/I-modules $M/IM \cong M \otimes M \otimes_A (A/I)$, where A/I is considered as an A-algebra via the natural homomorphism $A \to A/I$. It is easy to check the following property.

$$(M \oplus N)/I(M \oplus N) \cong (M/IM) \oplus (N/IN). \tag{1}$$

Now let P be a projective module over a local ring A. Replacing P by an isomorphic module we may assume that $P \oplus N = A^n$ for some submodule N of a free A-module A^n. Let $\mathfrak{m}$ be the maximal ideal of A. Let $(m_1, \ldots, m_s)$ be elements in M such that $(m_1 + I, \ldots, m_s + I)$ is a basis of the vector space $M/\mathfrak{m}M$ over $k = A/\mathfrak{m}$. Similarly, choose $(n_1, \ldots, n_t)$ in N. By property (1) the residues of $m_1, \ldots, m_t, n_1, \ldots, n_s$ form a basis of k^n. Consider the map $f : A^n \to M \oplus N$ defined by sending the unit vector $e_i \in A^n$ to m_i if $i \leq t$ and to n_i if $i \geq t+1$. Let S be its matrix with respect to the unit bases $(e_1, \ldots, e_n)$ in A^n. Then the image of S in $\mathrm{Mat}_n(k)$ is an invertible matrix. Therefore S is an invertible matrix. Thus f is an isomorphism of A-modules. The restriction of f to the free submodule $Ae_1 + \ldots + Ae_t$ is an isomorphism $A^t \cong M$.

Corollary. *Let P be a projective module over a commutative ring A. For any maximal ideal $\mathfrak{m}$ in A the localization $P_\mathfrak{m}$ is a free module over $A_\mathfrak{m}$.*

Proof. This follows from the following lemma which we leave to the reader to prove.

Lemma 2. *Let P be a projective module over A. For any A-algebra B the tensor product $P \otimes_A B$ is a projective B-module.*

Definition. A projective module over A has rank r if for each maximal ideal $\mathfrak{m}$ the module $P_\mathfrak{m}$ is free of rank r.

Remark 1. Note that, in general, a projective module has no rank. For example, let $A = A_1 \times A_2$ be the direct sum of rings. The module $A_1^k \times A_2^n$ (with scalar multiplication $(a_1, a_2) \cdot (m_1, m_2) = (a_1 m_1, a_2 m_2)$) is projective but has no rank if $k \neq n$. If A is a domain, then the homomorphism $A \to A_\mathfrak{m}$ defines an isomorphism of the fields of fractions $Q(A) \cong Q(A_\mathfrak{m})$. This easily implies that the rank of P can be defined as the dimension of the vector space $P \otimes_A Q(A)$.

We state without proof the converse of the previous Corollary (see, for example, N. Bourbaki, "Commutative Algebra", Chapter 2, §5).

Proposition 2. *Let M be a module over A such that for each maximal ideal $\mathfrak{m}$ the module $M_\mathfrak{m}$ is free. Then M is a projective module.*

Now we are ready to give the definition of $\mathbb{P}^n(A)$.

Definition. Let A be any commutative ring. The projective n-space over A is the set $\mathbb{P}^n(A)$ of projective modules of rank 1 which are direct summands of A^{n+1}.

We have seen that

$$\mathbb{P}(A)' \subset \mathbb{P}^n(A).$$

The difference is the set of non-free projective modules of rank 1 which are direct summands of A^{n+1}.

Remark 2 A projective submodule of rank 1 of A^{n+1} may not be a direct summand. For example, a proper principal ideal $(x) \subset A$ is not a direct summand in A. A free submodule $M = A(a_0, \ldots, a_n)$

of A^{n+1} of rank 1 is a direct summand if and only if the ideal generated by $a_0, \ldots, a_n$ is equal to A, i.e. $M \in \mathbb{P}^n(A)'$.

This follows from the following charcaterization of direct summands of A^{n+1}. A submodule M of A^{n+1} is a direct summand if and only if the corresponding homomorphism of the dual modules

$$A^{n+1} \cong \mathrm{Hom}_A(A^{n+1}, A) \to M^* = \mathrm{Hom}_A(M, A)$$

is surjective. Sometimes $\mathbb{P}^n(A)$ is defined in "dual terms" as the set of projective modules of rank 1 together with a surjective homomorphism $A^{n+1} \to M$. When A is a field this is a familiar duality between lines in a vector space V and hyperplanes in the dual vector space V^*.

A set $\{f_i\}_{i \in I}$ of elements from A is called a *covering family* if it generates the unit ideal. Every covering set contains a finite covering subset. In fact if $1 = \sum_i a_i f_i$ for some $a_i \in A$, we choose those f_i which occur in this sum with non-zero coefficient. For any $f \in A$ we set $A_f = A_S$, where S consists of powers of f.

Lemma 3. *Let M be a projective module of rank r over a ring A. There exists a finite covering family $\{f_i\}_{i \in I}$ of elements in A such that for any $i \in I$ the localization M_{f_i} is a free A_{f_i}-module of rank r.*

Proof. We know that for any maximal ideal $\mathfrak{m}$ in A the localization $M_{\mathfrak{m}}$ is a free module of rank r. Let $x_1, \ldots, x_r$ be its generators. Each x_i is a "fraction" $\frac{m_i}{a_i}$, where $a_i \notin \mathfrak{m}$. Reducing to common denominator we may assume that $a_1 = \ldots = a_r = f$ for some $f \notin \mathfrak{m}$. Thus M_f is free and is generated by $x_1, \ldots, x_r$ considered as elements of M_f. Let $\{f_{\mathfrak{m}}\}_{\mathfrak{m}}$ be the set of elements $f_{\mathfrak{m}}$ chosen in this way for each maximal ideal $\mathfrak{m}$. It is a covering set. Indeed let I be the ideal generated by these elements. If $I \neq A$ then I is contained in some maximal ideal $\mathfrak{m}$, hence $f_{\mathfrak{m}} \in I$ is contained in $\mathfrak{m}$ which contradicts the choice of $f_{\mathfrak{m}}$. It remains to select a finite covering subset of the set $f_{\mathfrak{m}}$.

Using Lemma 3 we may view every projective submodule M of A^{n+1} of rank 1 as a "local line": we can find a finite covering set $\{f_i\}_{i \in I}$ such that M_{f_i} is a line in $(A_{f_i})^{n+1}$. We call such a family a *trivializing family* for M. If $\{g_j\}_{j \in J}$ is another trivializing family for M we may consider the family $\{f_i g_j\}_{(i,j) \in I \times J}$. It is a covering family as one sees by multiplying the two relations $1 = \sum_i a_i f_i, 1 = \sum_j b_j g_j$. Note that for any $f, g \in A$ there is a natural homomorphism of rings $A_f \to A_{fg}, a/f^n \to ag^n/(fg)^n$ inducing an isomomorphism of A_{fg}-modules $M_f \otimes_{A_f} A_{fg} \cong M_{fg}$. This shows that $\{f_i g_j\}_{(i,j) \in I \times J}$ is a trivializing family. Moreover, if $M_{f_i} = x_i A_{f_i}, x_i \in A_{f_i}^{n+1}$ and $M_{g_j} = y_j A_{g_j}, y_j \in A_{g_j}^{n+1}$, then

$$x_i' = \alpha_{ij} y_j' \quad \text{for some } \alpha_{ij} \in A_{f_i g_j} \tag{2}$$

where the prime indicates the image in A_{fg}.

Now let us go back to algebraic equations. Fix a field k. For any k-algebra K we have the set $\mathbb{P}^n(K)$. It can be viewed as a natural extension (in $n+1$ different ways) of the set $\mathbb{A}_k^n(K) = K^n$. In fact, for every k-algebra K we have the injective maps

$$\alpha_i : \mathbf{A}_k^n(K) = K^n \to \mathbb{P}_k^n(K), (a_1, \ldots, a_n) \to (a_1, \ldots, a_i, 1, a_{i+1}, \ldots, a_n), \quad i = 0, \ldots, n.$$

Assume that K is a local ring. Take, for example, $i = 0$. We see that

$$\mathbb{P}^n(K) \setminus K^n = \{(a_0, a_1, \ldots, a_n)A \in \mathbb{P}^n(K) : a_0 = 0\}.$$

It is naturally bijectively equivalent to $\mathbb{P}^{n-1}(K)$. Thus we have

$$\mathbb{P}^n(K) = \mathbb{A}^n_k(K) \coprod \mathbb{P}^{n-1}(K).$$

By now, I am sure you understand what do I mean when I say "naturally". The bijections we establish for different K are compatible with respect to the maps $\mathbb{P}^n(K) \to \mathbb{P}^n(K')$ and $K^n \to K'^n$ corresponding to homomorphisms $K \to K'$ of k-algebras.

Example 5. The Riemann sphere

$$\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\mathbb{P}^0(\mathbb{C}).$$

6. The real projective plane

$$\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup \mathbb{P}^1(\mathbb{R}).$$

We want to extend the notion of an affine algebraic variety by considering solutions of algebraic equations which are taken from $\mathbb{P}^n(K)$. Assume first that $L \in \mathbb{P}^n(K)$ is a global line, i.e. a free submodule of K^{n+1}. Let $(a_0, \ldots, a_n)$ be its generator. For any $F \in k[T_0, \ldots, T_n]$ it makes sense to say that $F(a_0, \ldots, a_n) = 0$. However, it does not make sense, in general, to say that $F(L) = 0$ because a different choice of a generator may give $F(a_0, \ldots, a_n) \neq 0$. However, we can solve this problem by restricting ourselves only with polynomials satisfying

$$F(\lambda T_0, \ldots, \lambda T_n) = \lambda^d F(\lambda T_0, \ldots, \lambda T_n), \quad \forall \lambda \in K^*.$$

To have this property for all possible K, we require that F be a homogeneous polynomial.

Definition. A polynomial $F(T_0, \ldots, T_n) \in k[T_0, \ldots, T_n]$ is called *homogeneous* of *degree* d if

$$F(T_0, \ldots, T_n) = \sum_{i_0, \ldots, i_n} a_{i_0 \geq 0, \ldots, i_n \geq 0} T_0^{i_0} \cdots T_n^{i_n} = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{T}^{\mathbf{i}}$$

with $|\mathbf{i}| = d$ for all $\mathbf{i}$. Here we use the vector notation for polynomials:

$$\mathbf{i} = (i_0, \ldots, i_n) \in \mathbf{N}^{n+1}, \mathbf{T}^{\mathbf{i}} = T_0^{i_0} \cdots T_n^{i_n}, |\mathbf{i}| = i_0 + \ldots + i_n.$$

By definition the constant polynomial 0 is homogeneous of any degree.

Equivalently, F is homogeneous of degree d if the following identity in the ring $k[T_0, \ldots, T_n, t]$ holds:

$$F(tT_0, \ldots, tT_n) = t^d F(T_0, \ldots, T_n).$$

Let $k[T]_d$ denote the set of all homogeneous polynomials of degree d. This is a vector subspace over k in $k[T]$ and

$$k[T] = \oplus_{d \geq 0} k[T]_d.$$

Indeed every polynomial can be written uniquely as a linear combination of monomials $\mathbf{T}^{\mathbf{i}}$ which are homogeneous of degree $|\mathbf{i}|$. We write $\deg F = d$ if F is of degree d.

Let F be homogeneous polynomial in $T_0, \ldots, T_n$. For any k-algebra K and $x \in K^{n+1}$

$$F(x) = 0 \Longleftrightarrow F(\lambda x) = 0 \quad \text{for any } \lambda \in K^*.$$

Thus if $M = Kx \subset K^{n+1}$ is a line in K^{n+1}, we may say that $F(M) = 0$ if $F(x) = 0$, and this definition is independent of the choice of a generator of M. Now if M is a local line and $M_{f_i} = x_i K_{f_i} \subset K_{f_i}^{n+1}$ for some trivializing family $\{f_i\}_{i \in I}$, we say that $F(M) = 0$ if $F(x_i) = 0$ for all $i \in I$. The fact that this definition is independent of the choice of a trivializing family follows from (2) above and the following.

Lemma 4. *Let $\{f_i\}_{i\in I}$ be a covering family in a ring A and let $a \in A$. Assume that the image of a in each A_{f_i} is equal to 0. Then $a = 0$.*

Proof. By definition of A_{f_i}, we have $a/1 = 0$ in $A_{f_i} \iff f_i^n a_i = 0$ for some $n \geq 0$. Obviously we choose n to be the same for all $i \in I$. Since $1 = \sum_{i\in I} a_i f_i$ for some $a_i \in A$, after raising the both sides in sufficient high power, we obtain $1 = \sum_{i\in I} b_i f_i^n$ for some $b_i \in A$. Then $a = \sum_{i\in I} b_i f_i^n a = 0$.

Now if $S \subset k[T_0, \ldots, T_n]$ consists of homogeneous polynomials and $\{F = 0\}_{F\in S}$ is the corresponding system of algebraic equations (we call it a *homogeneous system*), we can set for any k-algebra K

$$\mathrm{PSol}(S; K) = \{M \in \mathbb{P}^n(K) : F(M) = 0 \text{ for any } F \in S\},$$

$$\mathrm{PSol}(S; K)' = \{M \in \mathbb{P}^n(K)' : F(M) = 0 \text{ for any } F \in S\}.$$

Definition. A *projective algebraic variety* over a field k is a correspondence

$$X : K \to \mathrm{PSol}(S; K) \subset \mathbb{P}^n(K)$$

where S is a homogeneous system of algebraic equations over k. We say that X is a *subvariety* of Y if $X(K)$ is a subset of $Y(K)$ for all K.

Now we explain the process of a homogenization of an ideal in a polynomial ring which allows us to extend an affine algebraic variety to a projective one.

Let $F(Z_1, \ldots, Z_n) \in k[Z_1, \ldots, Z_n]$ (this time we have to change the notation of variables). We write $Z_i = T_i/T_0$ and plug it in F. After reducing to common denominator, we get

$$F(T_1/T_0, \ldots, T_n/T_0) = T_0^{-d} G(T_0, \ldots, T_n),$$

where $G \in k[T_0, \ldots, T_n]$ is a homogeneous polynomial of degree d equal to the highest degree of monomials entering into F.

The polynomial

$$G(T_0, \ldots, T_n) = T_0^d F(T_1/T_0, \ldots, T_n/T_0)$$

is said to be the *homogenizaton* of F. For example, the polynomial $T_2^2T_0 + T_1^3 + T_1T_0^2 + T_0^3$ is equal to the homogenization of the polynomial $Z_2^2 + Z_1^3 + Z_1 + 1$.

Let I be an ideal in $k[Z_1, \ldots, Z_n]$. We define the *homogenization* of I as the ideal I^{hom} in $k[T_0, \ldots, T_n]$ generated by homogenizations of elements of I. It is easy to see that if $I = (G)$ is principal, then $I^{hom} = (F)$, where F is the homogenization of G. However, in general it is not true that I^{hom} is generated by the homogenizations of generators of I (see Problem 6 below).

Recalling the injective map $\alpha_0 : \mathbf{A}_k^n \to \mathbb{P}_k^n$ defined in the beginning of this lecture, we see that it sends an affine algebraic subvariety X defined by an ideal I to the projective variety defined by the homogenization I^{hom}, which is said to be the *projective closure* of X.

Example. 7. Let X be given by $aT_0 + bT_1 + cT_2 = 0$, a projective subvariety of the projective plane $\mathbb{P}_k^2$. It is equal to the projective closure of the line $L \subset \mathbf{A}_k^2$ given by the equation $bZ_1 + cZ_2 + a = 0$. For every K the set $X(K)$ has a unique point P not in the image of $L(K)$. Its homogeneous coordinates are $(0, c, -b)$. Thus, X has to be viewed as $L \cup \{P\}$. Of course, there are many ways to obtain a projective variety as a projective closure of an affine variety. To see this, it is sufficient to replace the map α_0 in the above constructions by the maps $\alpha_i, i \neq 0$.

Let $\{F(T) = 0\}_{F\in S}$ be a homogeneous system. We denote by (S) the ideal in $k[T]$ generated by the polynomials $F \in S$. It is easy to see that this ideal has the following property

$$(S) = \oplus_{d\geq 0}((S) \cap k[T]_d).$$

In other words, each polynomial $F \in (S)$ can be written uniquely as a linear combination of homogeneous polynomials from (S).

Definition. An ideal $I \subset k[T]$ is said to be *homogeneous* if one of the following conditions is satisfied:
(i) I is generated by homogeneous polynomials;
(ii) $I = \oplus_{d \geq 0}(I \cap k[T]_d)$.

Let us show the equivalence of these two properties. If (i) holds, then every $F \in I$ can be written as $\sum_i Q_i F_i$, where F_i is a set of homogeneous generators. Writing each Q_i as a sum of homogeneous polynomials, we see that F is a linear combination of homogeneous polynomials from I. This proves (ii). Assume (ii) holds. Let $G_1, \ldots, G_r$ be a system of generators of I. Writing each G_i as a sum of homogeneous polynomials G_{ij} from I, we verify that the set $\{G_{ij}\}$ is a system of homogeneous generators of I. This shows (i).

We know that in the affine case the ideal $I(X)$ determines uniquely an affine algebraic variety X. This is not true anymore in the projective case.

Proposition 3. *Let $\{F(T) = 0\}_{F \in S}$ be a homogeneous system of algebraic equations over a field k. Then the following properties are equivalent:*
(i) $\mathrm{PSol}(S; K)' = \emptyset$;
(ii) $(S) \supset k[T]_{\geq r} := \sum_{d \geq r} k[T]_d$ *for some* $r \geq 0$;
(iii) $\mathrm{PSol}(S; K) = \emptyset$.

Proof. (i) $\Longrightarrow$ (ii) Let K be an algebraically closed field containing k. We can write

$$F(T_0, \ldots, T_n) = T_0^d F(1, T_1/T_0, \ldots, T_n/T_0),$$

where $d = \deg F$. Substituting $Z_i = T_i/T_0$, we see that the polynomials $G_F(Z_1, \ldots, Z_n) = F(1, Z_1, \ldots, Z_n)$ do not have common roots (otherwise, its common root $(a_1, \ldots, a_n)$ will define an element $(1, a_1, \ldots, a_n) \in \mathrm{PSol}(S; K)'$). Thus, by Nullstellensatz, $(\{G_F\}_{F \in S}) = (1)$, i.e.

$$1 = \sum_{F \in S} Q_F G_F(Z_1, \ldots, Z_n)$$

for some $Q_F \in k[Z_1, \ldots, Z_n]$. Substituting back $Z_i = T_i/T_0$ and reducing to common denominator, we find that there exists $m(0) \geq 0$ such that $T_0^{m(0)} \in (S)$. Similarly, we show that for any $i > 1$, $T_i^{m(i)} \in (S)$ for some $m(i) \geq 0$. Let $m = \max\{m(0), \ldots, m(n)\}$. Then every monomial in T_i of degree greater or equal to $r = m(n+1)$ contains some $T^{m(i)}$ as a factor. Hence it belongs to the ideal (S). This proves that $(S) \supset k[T]_{\geq r}$.

(ii) $\Longrightarrow$ (iii) If $(S) \supset k[T]_{\geq r}$ for some $r > 0$, then all T_i^r belong to (S). Thus for every $M = K(a_0, \ldots, a_n) \in \mathrm{PSol}(S; K)'$ we must have $a_i^r = 0$. Since $(a_0, \ldots, a_n) \in C_n(K)$ we can find $b_0, \ldots, b_n \in K$ such that $1 = b_0 a_0 + \ldots + b_n a_n$. This easily implies that

$$1 = (b_0 a_0 + \ldots + b_n a_n)^{r(n+1)} = 0.$$

This contradiction shows that $\mathrm{PSol}(S; K)' = \emptyset$ for any k-algebra K. From this we can deduce that $\mathrm{PSol}(S; K) = \emptyset$ for all K. In fact, every $M \in PSol(S; K)$ defines $M_f \in \mathrm{PSol}(S; K_f)'$ for some $f \in K_f$.

(iii) $\Longrightarrow$ (i) Obvious.

Note that $k[T]_{\geq r}$ is an ideal in $k[T]$ which is equal to the power $\mathfrak{m}_+^r$ where

$$\mathfrak{m}_+ = k[T]_{\geq 1} = (T_0, \ldots, T_n).$$

A homogeneous ideal $I \subset k[T]$ containing some power of $\mathfrak{m}_+$ is said to be *irrelevant*. The previous proposition explains this definition.

For every homogeneous ideal I in $k[T]$ we define the projective algebraic variety $PV(I)$ as a correspondence $K \to \mathrm{Sol}(I, K)$. We define the *saturation* of I by

$$I^{sat} = \{F \in k[T] : GF \in I \text{ for all } G \in \mathfrak{m}_+^s \text{ for some } s \geq 0\}.$$

Clearly I^{sat} is a homogeneous ideal in $k[T]$ containing the ideal I (Check it !) .

Proposition 4. *Two homogeneous systems S and S' define the same projective variety if and only if $(S)^{sat} = (S')^{sat}$.*

Proof. Let us show first that for any k-algebra K, the ideals (S) and $(S)^{sat}$ have the same set of zeroes in $\mathbb{P}_k^n(K)$. It suffices to show that they have the same set of zeroes in every $\mathbb{P}_k^n(K)'$. Clearly every zero of $(S)^{sat}$ is a zero of (S). Assume that $a = (a_0, \ldots, a_n) \in \mathbb{P}_k^n(K)'$ is a zero of (S) but not of $(S)^{sat}$. Then there exists a polynomial $F \in (S)^{sat}$ which does not vanish at a. By definition, there exists $s \geq 0$ such that $\mathbf{T}^{\mathbf{i}}F \in (S)$ for all monomials $\mathbf{T}^{\mathbf{i}}$ of degree at least s. This implies that $\mathbf{T}^{\mathbf{i}}(a)F(a) = 0$. By definition of homogeneous coordinates, one can write $1 = a_0b_0 + \ldots + b_na_n$ for some b_i. Raising this equality into the s-th power, we obtain that $\mathbf{T}^{\mathbf{i}}(a) \neq 0$ for some i. Hence $F(a) = 0$.

Thus we may assume that $(S) = (S)^{sat}, (S') = (S')^{sat}$. Take $(t_0, \ldots, t_n) \in \mathrm{Sol}(S', k[T]/(S'))$, where $t_i = T_i + (S')$. For every homogeneous generator $F = F(T_0, \ldots, T_n) \in (S')$, we consider the polynomial $F' = F(1, Z_1, \ldots, Z_n) \in k[Z_1, \ldots, Z_n]$, where $Z_i = T_i/T_0$. Let $(S')_0$ be the ideal in $k[Z]$ generated by all polynomials F' where $F \in (S')$. Then $(1, z_1, \ldots, z_n) \in \mathrm{Sol}(S'; k[Z]/(S')_0)$ where $z_i = Z_i \mod (S')_0$. By assumption, $(1, z_1, \ldots, z_n) \in \mathrm{Sol}(S; k[Z]/(S')_0)$. This shows that $G(1, Z_1, \ldots, Z_n) \in (S')_0$ for each homogeneous generator of (S), i.e.

$$G(1, Z_1, \ldots, Z_n) = \sum_i Q_i F_i(1, Z_1, \ldots, Z_n)$$

for some $Q_i \in k[Z]$ and homogeneous generators F_i of (S'). Plugging in $Z_i = T_i/T_0$ and reducing to the common denominator, we obtain

$$T_0^{d(0)}G(T_0, \ldots, T_n) \in (S')$$

for some $d(0)$. Similarly, we obtain that $T^{d(0)}G \in (S')$ for some $d(i), i = 1, \ldots, n$. This easily implies that $\mathfrak{m}_+^s G \in (S')$ for some large enough s (cf. the proof of Proposition 1) . Hence, $G \in (S')$ and $(S) \subset (S')$. Similarly, we obtain the opposite inclusion.

Definition. A homogeneous ideal $I \subset k[T]$ is said to be *saturated* if $I = I^{sat}$.

Corollary. *The map $I \to PV(I)$ is a bijection between the set of saturated homogeneous ideals in k[T] and the set of projective algebraic subvarieties of $\mathbb{P}_k^n$.*

In future we will always assume that a projective variety X is given by a system of equations S such that the ideal (S) is saturated. Then $I = (S)$ is defined uniquely and is called the homogeneous

ideal of X and is denoted by $I(X)$. The corresponding factor-algebra $k[T]/I(X)$ is denoted by $k[X]$ and is called the *projective coordinate algebra* of X.

The notion of a *projective algebraic k-set* is defined similarly to the notion of an affine algebraic k-set. We fix an algebraically closed extension K of k and consider subsets $V \subset \mathbb{P}^n(K)$ of the form $\mathrm{PSol}(S;K)$, where X is a system of homogeneous equations in n-variables with coefficients in k. We define the *Zariski k-topology* in $\mathbb{P}^n(K)$ by choosing closed sets to be projective algebraic k-sets. We leave the verification of the axioms to the reader.

Problems.

1*. Show that $\mathbb{P}^n(k[T_1,\dots,T_n]) = \mathbb{P}^n(k[T_1,\dots,T_n])'$, where k is a field.

2. Let A $= \mathbb{Z}/(6)$. Show that A has two maximal ideals $\mathfrak{m}$ with the corresponding localizations $A_{\mathfrak{m}}$ isomorphic to $\mathbb{Z}/(2)$ and $\mathbb{Z}/(3)$. Show that a projective A-modules of rank 1 is isomorphic to A.

3*. Let $A = \mathbb{C}[T_1,T_2]/(T_1^2 - T_2(T_2-1)(T_2-2)), t_1$ and t_2 be the cosets of the unknowns T_1 and T_2. Show that the ideal (t_1,t_2) is a projective A-module of rank 1 but not free.

4. Let $I \subset k[T]$ be a homogeneous ideal such that $I \supset \mathfrak{m}_+^s$ for some s. Prove that $I^{sat} = k[T]$. Deduce from this another proof of Proposition 1.

5. Find I^{sat}, where $I = (T_0^2, T_0T_1) \subset k[T_0,T_1]$.

6. Find the projective closure in $\mathbb{P}_k^3$ of an affine variety in $\mathbf{A}_k^3$ given by the equations $Z_2 - Z_1^2 = 0, Z_3 - Z_1^3 = 0$.

7. Let $F \in k[T_0,\dots,T_n]$ be a homogeneous polynomial free of multiple factors. Show that its set of solutions in $\mathbb{P}^n(K)$, where K is an algebraically closed extension of k, is irreducible in the Zariski topology if and only F is an irreducible polynomial.

Lecture 6. BÉZOUT'S THEOREM AND A GROUP LAW ON A CUBIC CURVE

We begin with an example. Consider two "concentric circles":

$$C : Z_1^2 + Z_2^2 = 1, \quad C' : Z_1^2 + Z_2^2 = 4.$$

Obviously, they have no common points in the affine plane $\mathbf{A}^2(K)$ no matter in which algebra K we consider our points. However, they do have common points "at infinity". The precise meaning of this is the following. Let

$$\bar{C} : T_1^2 + T_2^2 - T_0^2 = 0, \quad \bar{C}' : T_1^2 + T_2^2 - 4T_0^2 = 0$$

be the projective closures of these conics in the projective plane $\mathbb{P}_k^2$, obtained by the homogenization of the corresponding polynomials. Assume that $\sqrt{-1} \in K$. Then the points (one point if K is of characteristic 2) $(1, \pm\sqrt{-1}, 0)$ are the common points of $\bar{C}(K)$ and $\bar{C}(K)'$. In fact, the homogeneous ideal generated by the polynomials $T_1^2 + T_2^2 - T_0^2$ and $T_1^2 + T_2^2 - 4T_0^2$ defining the intersection is equal to the ideal generated by the polynomials $T_1^2 + T_2^2 - T_0^2$ and T_0^2. The same points are the common points of the line $L : T_0 = 0$ and the conic $\bar{C}$, but in our case, it is natural to consider the same points with multiplicity 2 (because of T_0^2 instead of T_0). Thus the two conics have in some sense 4 common points. Bézout's theorem asserts that any two projective subvarieties of $\mathbb{P}_k^2$ given by an irreducible homogeneous equation of degree m and n, respectively, have mn common points (counting with appropriate multiplicities) in $\mathbb{P}_k^2(K)$ for every algebraically closed field K containing k. The proof of this theorem which we are giving here is based on the notion of the *resultant* (or the *eliminant*) of two polynomials.

Theorem 1. *There exists a homogeneous polynomial $R_{n,m} \in \mathbf{Z}[A_0, \ldots, A_n, B_0, \ldots, B_m]$ of degree $m + n$ satisfying the following property:*

The system of algebraic equations in one unknown over a field k :

$$P(Z) = a_0 Z^n + \ldots + a_n = 0, \; Q(Z) = b_0 Z^m + \ldots + b_m = 0$$

has a solution in a field extension K of k if and only if $(a_0, \ldots, a_n, b_0, \ldots, b_m)$ is a $k-$-solution of the equation

$$R_{n,m} = 0.$$

Proof. Define $R_{m,n}$ to be equal to the following determinant of order m+n:

$$\begin{vmatrix} A_0 & \ldots & A_n & 0 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & A_0 & \ldots & A_n \\ B_0 & \ldots & B_m & 0 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & B_0 & \ldots & B_m \end{vmatrix}$$

where the first m rows are occupied with the string $(A_0, \ldots, A_n)$ and zeroes, and the remaining n rows are occupied with the string $(B_0, \ldots, B_m)$ and zeroes. Assume $\alpha \in K$ is a common solution of two polynomials $P(Z)$ and $Q(Z)$. Write

$$P(Z) = (Z - \alpha)P_1(Z), \quad Q(Z) = (Z - \alpha)Q_1(Z)$$

where $P_1(Z), Q_1(Z) \in K[Z]$ of degree $n-1$ and $m-1$, respectively. Multiplying $P_1(Z)$ by $Q_1(Z)$, and $Q(Z)$ by $P_1(Z)$, we obtain

$$P(Z)Q_1(Z) - Q(Z)P_1(Z) = 0. \tag{1}$$

This shows that the coefficients of $Q_1(Z)$ and $P_1(Z)$ (altogether we have $n+m$ of them) satisfy a system of $n+m$ linear equations. The coefficient matrix of this system can be easily computed, and we find it to be equal to the transpose of the matrix

$$\begin{pmatrix} a_0 & \ldots & a_n & 0 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & a_0 & \ldots & a_n \\ -b_0 & \ldots & -b_m & 0 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & -b_0 & \ldots & -b_m \end{pmatrix}.$$

A solution can be found if and only if its determinant is equal to zero. Obviously this determinant is equal (up to a sign) to the value of $R_{n,m}$ at $(a_0, \ldots, a_n, b_0, \ldots, b_m)$. Conversely, assume that the above determinant vanishes. Then we find a polynomial $P_1(Z)$ of degree $\leq n-1$ and a polynomial $Q_1(Z)$ of degree $\leq m-1$ satisfying (1). Both of them have coefficients in k. Let α be a root of $P(Z)$ in some extension K of k. Then α is a root of $Q(Z)P_1(Z)$. This implies that $Z - \alpha$ divides $Q(Z)$ or $P_1(Z)$. If it divides $P(Z)$, we found a common root of $P(Z)$ and $Q(Z)$. If it divides $P_1(Z)$, we replace $P_1(Z)$ with $P_1(Z)/(Z-\alpha)$ and repeat the argument. Since $P_1(Z)$ is of degree less than n, we finally find a common root of $p(Z)$ and $q(Z)$.

The polynomial $R_{n,m}$ is called the *resultant* of order (n, m). For any two polynomials $P(Z) = a_0 Z^n + \ldots + a_n$ and $Q(Z) = b_0 Z^m + \ldots + b_m$ the value of $R_{n,m}$ at $(a_0, \ldots, a_n, b_0, \ldots, b_m)$ is called the resultant of $P(Z)$ and $Q(Z)$, and is denoted by $R_{n,m}(P, Q)$.

A projective algebraic subvariety X of $\mathbb{P}^2_k$ given by an equation: $F(T_0, T_1, T_2) = 0$, where $F \neq 0$ is a homogeneous polynomial of degree d will be called a *plane projective curve of degree d*. If $d = 1$, we call it a *line*, if d = 2 , we call it a *conic* (then *cubic*, *quartic*, *quintic*, *sextic*, *septic*, *octic curve*). We say that X is irreducible if its equation is given by an irreducible polynomial.

Theorem 2 (Bézout). *Let*

$$F(T_0, T_1, T_2) = 0, G(T_0, T_1, T_2) = 0$$

be two different plane irreducible projective curves of degree n and m, respectively, over a field k. For any algebraically closed field K containing k, the system $F = 0, G = 0$ has exactly mn solutions in $\mathbb{P}^2(K)$ counted with appropriate multiplicities.

Proof. Since we are interested in solutions in an algebraically closed field K, we may replace k by its algebraic closure to assume that k is algebraically closed. In particular k is an infinite set. We shall deduce later from the theory of dimension of algebraic varieties that there are only

finitely many K-solutions of $F = G = 0$. Thus we can always find a line $T_0 + bT_1 + cT_2 = 0$ with coefficients in k that has no K-solutions of $F = G = 0$. This is where we use the assumption that k is infinite. Also choose a different line $aT_0 + T_1 + dT_2 = 0$ with $a \neq b$ such that for any $\lambda, \mu \in K$ the line $(\lambda + \mu a)T_0 + (\lambda b + \mu)T_1 + (\lambda c + \mu)T_2 = 0$ has at most one solution of $F = G = 0$ in K. The set of triples (α, β, γ) such that the line $\alpha T_0 + \beta T_1 + \gamma T_2 = 0$ contains a given point (resp. two distinct points) is a two-dimensional (resp. one-dimensional) linear subspace of k^3. Thus the set of lines $\alpha T_0 + \beta T_1 + \gamma T_2 = 0$ containing at least two solutions of $F = G = 0$ is a finite set. Thus we can always choose a line in k^3 containing $(1, b, c)$ and some other vector $(a, 1, d)$ such that it does not belong to this set. Making the invertible change of variables

$$T_0 \to T_0 + bT_1 + cT_2, T_1 \to aT_0 + T_1 + dT_2, T_2 \to T_2$$

we may assume that for every solution (a_0, a_1, a_2) of $F = G = 0$ we have $a_0 \neq 0$, and also that no line of the form $\alpha T_0 + \beta T_1 = 0$ contains more than one solution of $F = G = 0$ in K. Write

$$F = a_0 T_2^n + \ldots + a_n, G = b_0 T_2^m + \ldots + a_m,$$

where $a_i, b_i \in k[T_0, T_1]_i$. Obviously, $a_n, b_m \neq 0$, since otherwise T_2 is a factor of F or G. Let

$$R(A_0, \ldots, A_n, B_0, \ldots, B_m)$$

be the resultant of order (n, m). Plug a_i in A_i, and b_j in B_j, and let $\bar{R} = R(a_0, \ldots, a_n, b_0, \ldots, b_m)$ be the corresponding homogeneous polynomial in T_0, T_1. It is easy to see, using the definition of the determinant, that $\bar{R}$ is a homogeneous polynomial of degree mn. It is not zero, since otherwise, by the previous Lemma, for every (β_0, β_1) the polynomials $F(\beta_0, \beta_1, T_2)$ and $G(\beta_0, \beta_1, T_2)$ have a common root in K. This shows that $\mathbb{P}^2(K)$ contains infinitely many solutions of the equations $F = G = 0$, which is impossible as we have explained earlier. Thus we may assume that $\bar{R} \neq 0$. Dehomogenizing it, we obtain:

$$\bar{R} = T_0^{nm} \bar{R}'(T_1/T_0)$$

where $\bar{R}'$ is a polynomial of degree $\leq nm$ in the unknown $Z = T_1/T_0$. Assume first that the degree of $\bar{R}'$ is exactly mn. Let $\alpha_1, \ldots, \alpha_{nm}$ be its nm roots in the algebraic closure $\bar{k}$ of k (some of them may be equal). Obviously, $\bar{R}(1, \alpha) = 0$, hence

$$R(a_0(1, \alpha), \ldots, a_n(1, \alpha), b_0(1, \alpha), \ldots, b_m(1, \alpha)) = 0.$$

By Theorem 1, the polynomials in T_2 $F(1, \alpha, T_2)$ and $G(1, \alpha, T_2)$ have a common root β in $\bar{k}$. It is also unique in view of our choice of the coordinate system. Thus $(1, \alpha, \beta)$ is a solution of the homogeneous system $F = G = 0$ in $\bar{k}$. This shows that the system $F = 0, G = 0$ has nm solutions, the multiplicity of a root α of $\bar{R}' = 0$ has to be taken as the multiplicity of the corresponding common solution. Conversely, every solution $(\beta_0, \beta_1, \beta_2)$ of $F = G = 0$, where $\beta_0 \neq 0$, defines a root $\alpha = \beta_1/\beta_0$ of $\bar{R}' = 0$. To complete the proof, we have to consider the case where $\bar{R}'$ is of degree $d < nm$. This happens only if $\bar{R}(T_0, T_1) = T_0^{nm-d} P(T_0, T_1)$, where $P \in k[T_0, T_1]_d$ does not contain T_0 as its irreducible factor. Obviously, $\bar{R}(0, 1) = 0$. Thus $(0, 1, \alpha)$ is a solution of $F = G = 0$ for some $\alpha \in K$. This contradicts our assumption from the beginning of the proof.

Example 1. Fix an algebraically closed field K containing k. Assume that $m = 1$, i.e.,

$$G = \alpha_0 T_0 + \alpha_1 T_1 + \alpha_2 T_2 = 0$$

is a line. Without loss of generality, we may assume that $\alpha_2 = -1$. Computing the resultant, we find that, in the notation of the previous proof,

$$\bar{R}(T_0, T_1) = a_0(\alpha_0 T_0 + \alpha_1 T_1)^n + \ldots + a_n.$$

Thus $\bar{R}$ is obtained by "eliminating" the unknown T_2. We see that the line $L : G = 0$ "intersects" the curve $X : F = 0$ at n K-points corresponding to n solutions of the equation $\bar{R}(T_0, T_1) = 0$ in $\mathbb{P}^1(K)$. A solution is multiple, if the corresponding root of the dehomogenized equation is multiple. Thus we can speak about the multiplicity of a common K-point of L and $F = 0$ in $\mathbb{P}^2(K)$. We say that a point $x \in X(K)$ is a *nonsingular point* if there exists at most one line L over K which intersects X at x with multiplicity > 1. A curve such that all its points are nonsingular is called nonsingular. We say that L is tangent to the curve X at a nonsingular point $x \in \mathbb{P}^2(K)$ if $x \in L(K) \cap X(K)$ and its multiplicity ≥ 2. We say that a tangent line L is an *inflection line* at x if the multiplicity ≥ 3. If such a tangent line exists at a point x, we say that x is an *inflection point* (or a *flex*) of X.

Let $P(Z_1, \ldots, Z_n) \in k[Z_1, \ldots, Z_n]$ be any polynomial in n variables with coefficients in a field k. We define the partial derivatives $\frac{\partial P}{\partial Z_j}$ of Z as follows. First we assume that P is a monomial $Z_1^{i_1} \cdots Z_n^{i_n}$ and set

$$\frac{\partial P}{\partial Z_j} = \begin{cases} i_j Z_1^{i_1} \cdots Z_j^{i_j - 1} \cdots Z_n^{i_n} & \text{if } i_j > 0, \\ 0 & \text{otherwise} \end{cases}.$$

Then we extend the definition to all polynomials by linearity over k requiring that

$$\frac{\partial(aP + bQ)}{\partial Z_j} = a\frac{\partial P}{\partial Z_j} + b\frac{\partial Q}{\partial Z_j}$$

for all $a, b \in k$ and any monomials P, Q. It is easy to check that the partial derivatives enjoy the same properties as the partial derivatives of functions defined by using the limits. For example, the map $P \mapsto \frac{\partial P}{\partial Z_j}$ is a *derivation* of the k-algebra $k[Z_1, \ldots, Z_n]$, i.e. , it is a k-linear map ∂ satisfying the chain rule:

$$\partial(PQ) = P\partial(Q) + Q\partial(P).$$

The partial derivatives of higher order are defined by composing the operators of partial derivatives.

Proposition 1. *(i) $X : F(T_0, T_1, T_2) = 0$ be a plane projective curve of degree d. A point $(a_0, a_1, a_2) \in X(K)$ is nonsingular if and only if (a_0, a_1, a_2) is not a solution of the system of homogeneous equations*

$$\frac{\partial F}{\partial T_0} = \frac{\partial F}{\partial T_1} = \frac{\partial F}{\partial T_2} = 0.$$

(ii) If (a_0, a_1, a_2) is a nonsingular point, then the tangent line at this point is given by the equation

$$\sum_{i=0}^{2} \frac{\partial F}{\partial T_i}(a_0, a_1, a_2) T_i = 0.$$

(iii) Assume 2 is invertible in k (i.e. the characteristic of k is not equal to 2). A nonsingular point (a_0, a_1, a_2) is an inflection point if and only if

$$\det \begin{pmatrix} \frac{\partial^2 F}{\partial T_0^2} & \frac{\partial^2 F}{\partial T_0 \partial T_1} & \frac{\partial^2 F}{\partial T_0 \partial T_2} \\ \frac{\partial^2 F}{\partial T_1 \partial T_0} & \frac{\partial^2 F}{\partial T_1^2} & \frac{\partial^2 F}{\partial T_1 \partial T_2} \\ \frac{\partial^2 F}{\partial T_1 \partial T_0} & \frac{\partial^2 F}{\partial T_2 \partial T_1} & \frac{\partial^2 F}{\partial T_2^2} \end{pmatrix} (a_0, a_1, a_2) = 0.$$

Proof. We check these assertions only for the case $(a_0, a_1, a_2) = (1, 0, 0)$. The general case is reduced to this case by using the variable change. The usual formula for the variable change in partial derivatives are easily extended to our algebraic partial derivatives. We leave the details of this reduction to the reader. Write F as a polynomial in T_0 with coefficients polynomials in $T_1, T-2$.

$$F(T_0, T_1, T_2) = T_0^q P_{d-q}(T_1, T_2) + T_0^{q-1} P_{d-q+1}(T_1, T_2) + \cdots + P_d(T_1, T_2), \quad q \leq d.$$

Here the subscript indices coincides with the degree of the corresponding homogeneous polynomial if it is not zero and we assume that $P_{d-q} \neq 0$. We assume that $F(1, 0, 0) = 0$. This implies that $q < d$. A line through the point $(1, 0, 0)$ is defined by an equation $T_2 - \lambda T_1 = 0$ for some $\lambda \in k$. Eliminating T_2 we get

$$F(T_0, T_1, \lambda T_1) = T_0^q T_1^{d-q} P_{d-q}(1, \lambda) + T_0^{q-1} T_1^{d-q+1} P_{d-q+1}(1, \lambda) + \cdots + T_1^d P_d(1, \lambda)$$

$$= T_1^{d-q} \Big(T_0^q P_{d-q}(1, \lambda) + T_0^{q-1} T_1 P_{d-q+1}(1, \lambda) + \cdots + T_1^q P_d(1, \lambda) \Big).$$

It is clear that each line intersects the curve X at the point $(1, 0, 0)$ with multiplicity > 1 if and only if $d - q > 1$. Thus $(1, 0, 0)$ is nonsingular if and only if $q = d - 1$. Let $P(T_1, T_2) = aT_1 + bT_2$. Computing the partial derivatives of $F(T_0, T_1, T_2)$ at $(1, 0, 0)$ we easily find that

$$\frac{\partial F}{\partial T_0}(1, 0, 0) = 0, \frac{\partial F}{\partial T_1}(1, 0, 0) = a, \frac{\partial F}{\partial T_1}(1, 0, 0) = b.$$

Thus $d - q > 1$ if and only if the partial vanish. This proves assertion (i). Assume that the point is nonsingular, i.e. $d - q = 1$. The unique tangent line satisfies the linear equation

$$P_1(1, \lambda) = a + b\lambda = 0. \tag{2}$$

Obviously the lines $\lambda T_1 - T_2 = 0$ and $aT_1 + bT_2 = 0$ coincide. This proves assertion (ii).

Let $P_2(T_1, T_2) = \alpha T_1^2 + \beta T_1 T_2 + \gamma T_2^2$. Obviously, the point $(1, 0, 0)$ is an inflection point if and only if $P_2(1, \lambda) = 0$. Computing the second partial derivatives we find that

$$\det \begin{pmatrix} \frac{\partial^2 F}{\partial T_0^2} & \frac{\partial^2 F}{\partial T_0 \partial T_1} & \frac{\partial^2 F}{\partial T_0 \partial T_2} \\ \frac{\partial^2 F}{\partial T_1 \partial T_0} & \frac{\partial^2 F}{\partial T_1^2} & \frac{\partial^2 F}{\partial T_1 \partial T_2} \\ \frac{\partial^2 F}{\partial T_1 \partial T_0} & \frac{\partial^2 F}{\partial T_2 \partial T_1} & \frac{\partial^2 F}{\partial T_2^2} \end{pmatrix} (1, 0, 0) = \det \begin{pmatrix} 0 & a & b \\ a & 2\alpha & \beta \\ b & \beta & 2\gamma \end{pmatrix} = 2P_2(a, b).$$

It follows from (2) that $P_2(a, b) = 0$ if and only if $P_2(1, \lambda) = 0$. Since we assume that 2 is invertible in k we obtain that $(1, 0, 0)$ is an inflection point if and only if the determinant from assertion (3) is equal to zero.

Remark 1. The determinant

$$\det \begin{pmatrix} \frac{\partial^2 F}{\partial T_0^2} & \frac{\partial^2 F}{\partial T_0 \partial T_1} & \frac{\partial^2 F}{\partial T_0 \partial T_2} \\ \frac{\partial^2 F}{\partial T_1 \partial T_0} & \frac{\partial^2 F}{\partial T_1^2} & \frac{\partial^2 F}{\partial T_1 \partial T_2} \\ \frac{\partial^2 F}{\partial T_1 \partial T_0} & \frac{\partial^2 F}{\partial T_2 \partial T_1} & \frac{\partial^2 F}{\partial T_2^2} \end{pmatrix}$$

is a homogeneous polynomial of degree $3(d-2)$ unless it is identically zero. It is called the *Hessian polynomial* of F and is denoted by $Hess(F)$. If $Hess(F) \neq 0$, the plane projective curve of degree

$3(d-2)$ given by the equation $Hess(F) = 0$ is called the *Hessian curve* of the curve $F = 0$. Applying Proposition 1 and Bézout's Theorem, we obtain that a plane curve of degree d has $3d(d-2)$ inflection points counting with multiplicities.

Here is an example of a polynomial F defining a nonsingular plane curve with $Hess(F) = 0$:

$$F(T_0, T_1, T_2) = T_0^{p+1} + T_1^{p+1} + T_2^{p+1} = 0,$$

where k is of characteristic $p > 0$. One can show that $Hess(F) \neq 0$ if k is of characteristic 0.

Let us give an application of the Bézout Theorem. Let

$$X : F(T_0, T_1, T_2) = 0$$

be a projective plane cubic curve. Fix a field K containing k (not necessary algebraically closed). Let $\bar{k}$ be the algebraic closure of k containing K. We assume that each point of $X(\bar{k})$ is nonsingular. Later when we shall study local properties of algebraic varieties, we give some simple criterions when does it happen.

Fix a point $e \in X(K)$. Let x, y be two different points from $X(K)$. Define the sum

$$x \oplus y \in X(K)$$

as a point in $X(K)$ determined by the following construction. Find a line L_1 over K with $y, x \in L_1(K)$. This can be done by solving two linear equations with three unknowns. By Bézout's Theorem, there is a third intersection point, denote it by yx. Since this point can be found by solving a cubic equation over K with two roots in K (defined by the points x and y), the point $yx \in X(K)$. Now find another K-line L_2 which contains yx and e, and let $y \oplus x$ denote the third intersection point. If yx happens to be equal to e, take for L_2 the tangent line to X at e. If $y = x$, take for L_1 the tangent line at y. We claim that this construction defines the group law on $X(K)$.

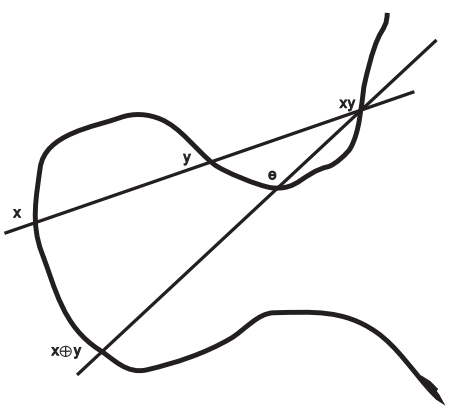

Fig.1

Clearly

$$y \oplus x = x \oplus y,$$

i.e., the binary law is commutative. The point e is the zero element of the law. If $x \in X(K)$, the opposite point $-x$ is the point of intersection of $X(K)$ with the line passing through x and the the third point x_1 at which the tangent at e intersects the curve. The only non-trivial statement is the property of associativity. We use the following picture to verify this property:

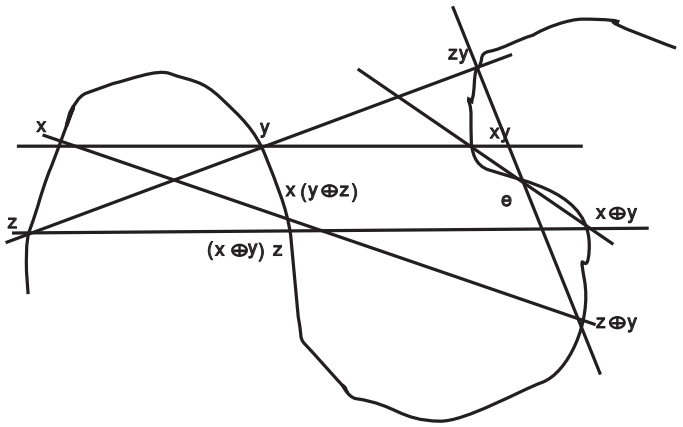

Fig.2

Consider the eight points $e, x, y, z, zy, xy, x \oplus y, y \oplus z$. They lie on three cubic curves. The first one is the original cubic X. The second one is the union of three lines

$$< x, y > \cup < yz, y \oplus z > \cup < z, x \oplus y > \tag{1}$$

where for any two distinct points $a, b \in \mathbb{P}^2(K)$ we denote by $< a, b >$ the unique K-line L with $a, b \in L(K)$. Also the "union" means that we are considering the variety given by the product of the linear polynomials defining each line. The third one is also the union of three lines

$$< y, z > \cup < xy, x \oplus y > \cup < x, y \oplus z > . \tag{20}$$

We will use the following:

Lemma 1. *Let $x_1, \ldots, x_8$ be eight distinct points in $\mathbb{P}^2(K)$. Suppose that all of them belong to $X(K)$ where X is a plane irreducible projective cubic curve. Assume also that the points x_1, x_2, x_3 lie on two different lines which do not contain points x_i with $i > 3$. There exists a unique point x_9 such that any cubic curve Y containing all eight points contains also x_9, and either $x_9 \notin \{x_1, \ldots, x_8\}$ or x_9 enters in $X(K) \cap Y(K)$ with multiplicity 2.*

Proof. Let Y be given by an equation $F = a_0 T_0^3 + a_1 T_0^2 T_1 + \ldots = 0$ the polynomial F. A point $x = (\alpha_0, \alpha_1, \alpha_2) \in X(K)$ if and only if the ten coefficients of F satisfy a linear equation whose coefficients are the values of the monomials of degree 3 at $(\alpha_0, \alpha_1, \alpha_2)$. The condition that a cubic curve passes through 8 points introduces 8 linear equations in 10 unknowns. The space of solutions of this system is of dimension ≥ 2. Suppose that the dimension is exactly 2. Then the equation of any cubic containing the points $x_1, \ldots, x_8$ can be written in the form $\lambda F_1 + \mu F_2$, where F_1 and F_2 correspond to two linearly independent solutions of the system. Let x_9 be the ninth intersection point of $F_1 = 0$ and $F_2 = 0$ (Bézout's Theorem). Obviously x_9 is a solution of $F = 0$. It remains to consider the case when the space of solutions of the system of linear equation has dimension > 2. Let L be the line with $X_1, x_2 \in L(K)$. Choose two points $x, y \in L(K) \setminus \{x_1, x_2\}$ which are not in $X(K)$. Since passing through a point imposes one linear condition, we can find a cubic curve $Y : G = 0$ with $x, y, x_1, \ldots, x_8 \in Y(K)$. But then $L(K) \cap Y(K)$ contains four points. By Bézout's Theorem this could happen only if G is the product of a linear polynomial defining L and a polynomial B of degree 2. By assumption L does not contain any other point $x_3, \ldots, x_8$. Then the conic $C : B = 0$ must contain the points $x_3, \ldots, x_8$. Repeating the argument for the points x_1, x_3, we find a conic $C' : B' = 0$ which contains the points $x_2, x_4, \ldots, x_8$. Clearly $C \neq C'$ since otherwise C contains 7 common points with an irreducible cubic. Since $C(K) \cap C'(K)$ contains 5

points in common, by Bézout's Theorem we obtain that B and B' have a common linear factor. This easily implies that 4 points among $x_4, \ldots, x_8$ must be on a line. But this line cannot intersect an irreducible cubic at four points in $\mathbb{P}^2_k(K)$.

Remark 2. Here is an example of the configuration of 8 points which do not satisfy the assumption of the Lemma. Consider the cubic curve (over $\mathbf{C}$) given by the equation:

$$T_0^3 + T_1^3 + T_2^3 + \lambda T_0 T_1 T_2 = 0.$$

It is possible to choose the parameter λ such that the curve is irreducible. Let $x_1, \ldots, x_9$ be the nine points on this curve with the coordinates:

$$(0, 1, \rho), (1, 0, \rho), (1, 1, \rho)$$

where ρ is one of three cube roots of -1. Each point x_i lies on four lines which contain two other points $x_j \neq x_i$. For example, $(0, 1, -1)$ lies on the line $T_0 = 0$ which contains the points $(0, 1, \rho), (0, 1, \rho^2)$ and on the three lines $\rho T_0 - T_1 - T_2 = 0$ which contains the points $(1, 0, \rho), (1, \rho, 0)$. The set $x_1, \ldots, x_8$ is the needed configuration. One easily checks that the nine points $x_1, \ldots, x_9$ are the inflection points of the cubic curve C (by Remark 1 we expect exactly 9 inflection points). The configuration of the 12 lines as above is called the *Hesse configuration of lines*.

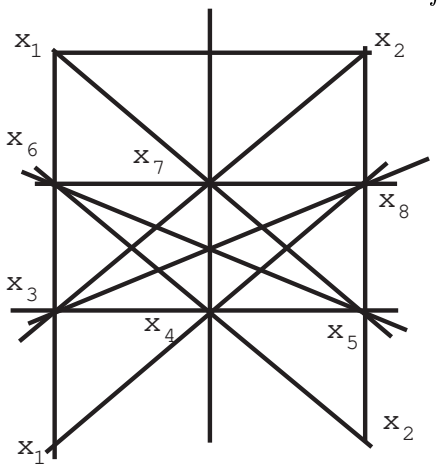

Fig. 3

Nevertheless one can prove that the assertion of Lemma 1 is true without additional assumption on the eight points.

To apply Lemma 1 we take the eight points $e, x, y, z, zy, xy, x \oplus y, y \oplus z$ in $X(K)$. Obviously they satisfy the assumptions of the lemma. Observe that $(x \oplus y)z$ lies in $X(K)$ and also in the cubic (1), and $x(y \oplus z)$ lies in $X(K)$ and in the cubic (2). By the Lemma $(x \oplus y)z = x(y \oplus z)$ is the unique ninth point. This immediately implies that $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Remark 3. Our proof is in fact not quite complete since we assumed that all the points $e, x, y, z, zy, xy, x \oplus y, y \oplus z$ are distinct. We shall complete it later but the idea is simple. We will be able to consider the product $X(K) \times X(K) \times X(K)$ as a projective algebraic set with the Zariski topology. The subset of triples (x, y, z) for which the associativity $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ holds is open (since all degenerations are described by algebraic equations). On the other hand it is also closed since the group law is defined by a polynomial map. Since $X(K) \times X(K) \times X(K)$ is an irreducible space, this open space must coincide with the whole space.

Remark 4. Depending on K the structure of the group $X(K)$ can be very different. A famous theorem of Mordell-Weil says that this group is finitely generated if K is a finite extension of $\mathbf{Q}$.

One of the most interesting problems in number theory is to compute the rank of this group. On the other hand, the group $X(\mathbf{C})$ is isomorphic to the factor group $\mathbf{C}/\mathbf{Z}^2$. Obviously it is not finitely generated.

Problems.

1. Let $P(Z) = a_0 Z^n + a_1 Z^{n-1} + \ldots + a_n$ be a polynomial with coefficients in a field k, and $P'(Z) = na_0 Z^{n-1} + (n-1)a_1 Z^{n-2} + \ldots + a_n$ be its derivative. The resultant $R_{n,n-1}(P, P')$ of P and P' is called the *discriminant* of P. Show that the discriminant is equal to zero if and only if $P(Z)$ has a multiple root in the algebraic closure $\bar{k}$ of k. Compute the discriminant of quadratic and cubic polynomials. Using computer compute the discriminant of a quartic polynomial.

2. Let $P(Z) = a_0(Z - \alpha_1)\ldots(Z - \alpha_n)$ and $Q(x) = b_0(Z - \beta_1)\ldots(Z - \beta_m)$ be the factorizations of the two polynomials into linear factors (over an algebraic closure of k). Show that

$$R_{n,m}(P, Q) = \pm a_0^m b_0^n \prod_{i=1}^{n}\prod_{i=1}^{m}(\alpha_i - \beta_j) = a_0^m \prod_{i=1}^{n} Q(\alpha_i) = b_0^n \prod_{j=1}^{m} P(\beta_j).$$

3. Find explicit formulae for the group law on $X(\mathbf{C})$, where X is a cubic curve defined by the equation $T_1^2 T_0 - T_2^3 - T_0^3 = 0$. You may take for the zero element the point $(0, 1, 0)$.

4. In the notation of the previous problem, show that elements $x \in X(\mathbf{C})$ of order 3 (i.e. $3x = 0$ in the group law) correspond to inflection points of X. Show that there are 9 of them. Show that the set of eight inflection points is an example of the configuration which does not satisfy the assumption of Lemma 1.

5. Let X be given by the equation $T_1^2 T_0 - T_2^3 = 0$. Similarly to the case of a nonsingular cubic, show that for any field K the set $X(K)' = X(K) \setminus \{(1, 0, 0)\}$ has a group structure isomorphic to the additive group K^+ of the field K.

6. Let X be given by the equation $T_1^2 T_0 - T_2^2(T_2 + T_0) = 0$. Similarly to the case of a nonsingular cubic, show that for any field K the set $X(K)' = X(K)\setminus\{(1, 0, 0)\}$ has a group structure isomorphic to the multiplicative group K^* of the field K.

Lecture 7. MORPHISMS OF PROJECTIVE ALGEBRAIC VARIETIES

Following the definition of a morphism of affine algebraic varieties we can define a morphism $f : X \to Y$ of two projective algebraic varieties as a set of maps $f_K : X(K) \to Y(K)$ defined for each k-algebra K such that, for any homomorphism $\phi : K \to L$ of k-algebras, the natural diagram

$$\begin{array}{ccc} X(K) & \stackrel{X(\phi)}{\longrightarrow} & X(L) \\ f_K \downarrow & & \downarrow f_L \\ Y(K) & \stackrel{Y(\phi)}{\longrightarrow} & Y(L). \end{array} \tag{1}$$

is commutative. Recall that a morphism of affine varieties $f : X \to Y$ is uniquely determined by the homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$. This is not true anymore for projective algebraic varieties. Indeed, let $\phi : k[Y] \to k[X]$ be a homomorphism of the projective coordinate rings. Suppose it is given by the polynomials $F_0, \ldots, F_n$. Then the restriction of the map to the set of global lines must be given by the formula

$$a = (\alpha_0, \ldots, \alpha_n) \to (F_0(a), \ldots, F_n(a)).$$

Obviously these polynomials must be homogeneous of the same degree. Otherwise, the value will depend on the choice of coordinates of the point $a \in X(K)$. This is not all. Suppose all F_i vanish at a. Since $(0, \ldots, 0) \notin C(K)_n$, the image of a is not defined. So not any homomorphism $k[Y] \to k[X]$ defines a morphism of projective algebraic varieties. In this lecture we give an explicit description for morphisms of projective algebraic varieties.

Let us first learn how to define a morphism $f : X \to Y \subset \mathbb{P}^n_k$ from an affine k-variety X to a projective algebraic k-variety Y. To define f it is enough to define $f : X \to \mathbb{P}^n_k$ and to check that $f_K(X(K)) \subset Y(K)$ for each K. We know that $X(K) = Hom_{k-alg}(\mathcal{O}(X), K)$. Take $K = \mathcal{O}(X)$ and the identity homomorphism $\mathrm{id}_{\mathcal{O}(X)} \in X(K)$. It is sent to an element $M \in \mathbb{P}^n_k(\mathcal{O}(X))$. The projective $\mathcal{O}(X)$-module M completely determines f. In fact, let $x \in X(K)$ and $ev_x : \mathcal{O}(X) \to K$ be the corresponding homomorphism of k-algebras. Using the commutative diagram (1) (where $K = \mathcal{O}(X), L = K, \phi = ev_x$), we see that

$$f_K(x) = M \otimes_{\mathcal{O}(X)} K, \tag{2}$$

where K is considered as an $\mathcal{O}(X)$-algebra by means of the homomorphism ev_x (i.e. $a \cdot z = ev_x(a)z$ for any $a \in \mathcal{O}(X), z \in K$). Conversely, any $M \in \mathbb{P}^n(\mathcal{O}(X)$ defines a map $f : X \to \mathbb{P}^n_k$ by using the formula (2). If M is a global line defined by projective coordinates $(a_0, \ldots, a_n) \in C(\mathcal{O}(X))_n$, then

$$f_K(x) = M \otimes_{\mathcal{O}(X)} K = (a_0(x), \ldots, a_n(x))K \in \mathbb{P}^n(K),$$

where as always we denote $ev_x(a)$ by $a(x)$. Since $\mathcal{O}(X) = k[Z_1, \dots, Z_n]/I$ for some ideal I, we can choose polynomial representatives of a_i's to obtain that our map is defined by a collection of $n+1$ polynomials (not necessary homogeneous of course since X is affine). They do not simulteneoulsly vanish at x since $a_0, \dots, a_n$ generate the unit ideal. However, in general M is not necessary a free module, so we have to deal with maps defined by local but not global lines over $\mathcal{O}(X)$. This explains why we had to struggle with a general notion of $\mathbb{P}^n(A)$.

Let us describe more explicitly the maps corresponding to any local line M. Let us choose a covering family $\{a_i\}_{i\in I}$ which trivializes M, i.e. $M_i = M_{a_i}$ is a global line defined by projective coordinates $(p_0^{(i)}/a_i^r, \dots, p_n^{(i)}/a_i^r) \in C(\mathcal{O}(X)_{a_i})_n$. Note that since a_i^r is invertible in $\mathcal{O}(X)_{a_i}$ we can always assume that $r = 0$. If no confusion arises we denote the elements $a/1, a \in A$ in the localization A_f of a ring A by a. Since $1 = \sum_j b_j p_j^{(i)}/a_i^r$ for some $b_0, \dots, b_n \in \mathcal{O}(X)_{a_i}$, we obtain, after clearing the denominators, that the ideal generated by $p_0^{(i)}, \dots, p_n^{(i)}$ is equal to (a_i^d) for some $d \geq 0$. So

$$(p_0^{(i)}, \dots, p_n^{(i)}) \in C(\mathcal{O}(X)_{a_i})_n \quad \text{but, in general, } (p_0^{(i)}, \dots, p_n^{(i)}) \notin C(\mathcal{O}(X))_n.$$

Assume $a_i(x) = ev_x(a_i) \neq 0$. Let x_i be the image of $x \in X(K)$ in $X(K_{a_i(x)})$ under the natural homomorphism $K \to K_{a_i(x)}$. Let us consider $K_{a_i(x)}$ as an $\mathcal{O}(X)$-algebra by means of the composition of homomorphisms $\mathcal{O}(X) \stackrel{ev_x}{\to} K \to K_{a_i(x)}$. Then

$$f_{K_{a_i(x)}}(x_i) = M \otimes_{\mathcal{O}(X)} K_{a_i(x)} \cong (M \otimes_{\mathcal{O}(X)} \mathcal{O}(X)_{a_i}) \otimes_{\mathcal{O}(X)_{a_i}} K_{a_i(x)} = M_i \otimes_{\mathcal{O}(X)_{a_i}} K_{a_i(x)},$$

where $K_{a_i(x)}$ is an $\mathcal{O}(X)_{a_i}$-algebra by means of the homomorphism $\mathcal{O}(X)_{a_i} \to K_{a_i(x)}$ defined by $\frac{a}{a_i^r} \mapsto \frac{a(x)}{a_i(x)^r}$. Since $M_i = (p_0^{(i)}, \dots, p_n^{(i)})\mathcal{O}(X)_{a_i}$ we obtain that

$$f_{K_{a_i(x)}}(x_i) = (p_0^{(i)}(x), \dots, p_n^{(i)}(x))K_{a_i(x)} \in \mathbb{P}^n(K_{a_i(x)}).$$

If K is a field, $K_{a_i(x)} = K$ (because $a_i(x) \neq 0$) and we see that, for any $x \in X(K)$ such that $a_i(x) \neq 0$ we have

$$f_K(x) = (p_0^{(i)}(x), \dots, p_n^{(i)}(x)) \in \mathbb{P}^n(K). \tag{3}$$

Thus we see that the morphism $f : X \to \mathbb{P}_k^n$ is given by not a "global" polynomial formula but by several "local" polynomial formulas (3). We take $x \in X(K)$, find $i \in I$ such that $a_i(x) \neq 0$ (we can always do it since $1 = \sum_{i\in I} b_i a_i$ for some $b_i \in \mathcal{O}(X)$) and then define $f_K(x)$ by the formula (3).

The collection

$$\{(p_0^{(i)}, \dots, p_n^{(i)})\}_{i\in I}$$

of elements $(p_0^{(i)}, \dots, p_n^{(i)}) \in \mathcal{O}(X)^{n+1}$ satisfies the following properties:

(i) $(p_0^{(i)}, \dots, p_n^{(i)}) = (a_i^{d_i})$ for some $d_i \geq 0$;

(ii) for any $i, j \in I$, $(p_0^{(i)}, \dots, p_n^{(i)}) = g_{ij}(p_0^{(j)}, \dots, p_n^{(j)})$ in $(\mathcal{O}(X)_{a_i a_j})^{n+1}$ for some invertible $g_{ij} \in \mathcal{O}(X)_{a_i a_j}$;

(iii) for any F from the homogeneous ideal defining Y, $F(p_0^{(i)}, \dots, p_n^{(i)}) = 0, i \in I$.

Note that the same map can be given by any other collection:

$$(q_0^{(j)}, \dots, q_n^{(j)})_{j\in J}$$

defining the same local line $M \in \mathbb{P}^n(\mathcal{O}(X))$ in a trivializing covering family $\{b_j\}_{j\in J}$. They agree in the folowing sense:

$$p_k^{(i)} = q_k^{(j)} g_{ij}, k = 0, \ldots, n,$$

where $g_{ij} \in \mathcal{O}(X)^*_{a_i b_j}$.

For each $i \in I$ this collection defines a projective module $M_i \in \mathbb{P}^n(\mathcal{O}(X)_{a_i})$ generated by $(p_0^{(i)}, \ldots, p_n^{(i)})$. We shall prove in the next lemma that there exists a projective module $M \in \mathbb{P}^n(\mathcal{O}(X))$ such that $M_{a_i} \cong M_i$ for each $i \in I$. This module is defined uniquely up to isomorphism. Using M we can define f by sending $id_{\mathcal{O}(X)} \in X(\mathcal{O}(X))$ to M. If $x \in X(K)$, where K is a field, the image $f_K(x)$ is defined by formulae (2).

Let us now state and prove the lemma. Recall first that for any ring A a local line $M \in \mathbb{P}^n(A)$ defines a collection $\{M_{a_i}\}_{i\in I}$ of lines in $A_{a_i}^{n+1}$ for some covering family $\{a_i\}_{i\in I}$ of elements in A. Let us see how to reconstruct M from $\{M_{a_i}\}_{i\in I}$. We know that for any $i, j \in I$ the images m_i of $m \in M$ in M_{a_i} satisfy the following condition of compatibility:

$$\rho_{ij}(m_i) = \rho_{ji}(m_j)$$

where $\rho_{ij} : M_{a_i} \to M_{a_i f_j}$ is the canonical homomorphism $m/a_i^r \to m f_j^r/(a_i f_j)^r$.

For any family $\{M_i\}_{i\in I}$ of A_{a_i}-modules let

$$\varinjlim_{i\in I} M_i = \{(m_i)_{\in I} \in \prod_{i\in I} M_i : \rho_{ij}(m_i) = \rho_{ji}(m_j) \quad \text{for any } i, j \in I\}.$$

This can be naturally considered as a submodule of the direct sum $\oplus_{i\in I} M_i$ of A-modules. There is a canonical homomorphism

$$\alpha : M \to \varinjlim_{i\in I} M_{a_i}$$

defined by $m \to (m_i = m)_{i\in I}$.

Lemma. *The homomorphism*

$$\alpha : M \to \varinjlim_{i\in I} M_{a_i}$$

is an isomorphism.

Proof. We assume that the set of indices I is finite. This is enough for our applications since we can always choose a finite covering subfamily. The proof of injectivity is similar to the proof of Lemma 4 from Lecture 5 and is left to the reader. Let us show the surjectivity. Let

$$(\frac{m_i}{a_i^{n_i}})_{i\in I} \in \varinjlim_{i\in I} M_{a_i}$$

for some $m_i \in M$ and $n_i \geq 0$. Again we may assume that all n_i are equal to some n. Since for any $i, j \in I$

$$\rho_{ij}(\frac{m_i}{a_i^n}) = \rho_{ji}(\frac{m_j}{a_j^n}),$$

we have

$$(a_i a_j)^r (a_j^n m_i - a_i^n m_j) = 0$$

for some $r \geq 0$. Let $p_i = m_i a_i^r$, $k = r + n$. Then

$$\frac{m_i}{a_i^n} = \frac{p_i}{a_i^k}, \quad f_j^k p_i = a_i^k p_j.$$

We can write $1 = \sum_i b_i a_i^k$. Set $m = \sum_i b_i p_i$. Then

$$a_j^k m = \sum_i b_i a_j^k p_i = \sum_i b_i a_i^k p_j = 1 p_j = p_j.$$

This shows that the image of m in each M_{a_i} coincides with $p_i/a_i^k = m_i/a_i^n$ for each $i \in I$. This proves the surjectivity.

In our situation, M_i is generated by $(p_0^{(i)}, \ldots, p_n^{(i)}) \in C(\mathcal{O}(X_{a_i})$ and property (ii) from above tells us that $(M_i)_{a_j} = (M_j)_{a_i}$. Thus we can apply the lemma to define M.

Let $f : X \to Y$ be a morphism of projective algebraic varieties, $X \subset \mathbb{P}_k^m, Y \subset \mathbb{P}_k^n$. For every k-algebra K and $M \in X(K)$ we have $N = f_K(M) \in Y(K)$. It follows from commutativity of diagrams (1) that for any $a \in K$, $f(K_a)(M_a) = N_a$. Let $\{a_i\}_{i \in I}$ be a covering family of elements in K. Then, applying the previous lemma, we will be able to recover N from the family $\{N_{a_i}\}_{i \in I}$. Taking a covering family which trivializes M, we see that our morphism $f : X \to Y$ is determined by its restriction to $X' : K \to \mathbb{P}^n(K)' \cap X(K)$, i.e., it suffices to describe it only on "global" lines $M \in X(K)$. Also observe that we can always choose a trivializing family $\{a_i\}_{i \in I}$ of any local line $M \in X(K)$ in such a way that M_{a_i} is given by projective coordinates $(t_0^{i(i)}, \ldots, t_m^{(i)})$ with at least one $t_j^{(i)}$ invertible in M_{a_i}. For example we can take the covering family, where each a_i is replaced by $\{a_i t_0^{(i)}, \ldots, a_i t_m^{(i)}\}$ (check that it is a covering family) then each $t_j^{(i)}$ is invertible in $K_{a_i t_j^{(i)}}$. Note that this is true even when $t_j^{(i)} = 0$ because $K_0 = \{0\}$ and in the ring $\{0\}$ one has $0 = 1$. Thus it is enough to define the maps $X(K) \to Y(K)$ on the subsets $X(K)''$ of global K-lines with at least one invertible projective coordinate.

Let X be defined by a homogeneous ideal $I \subset k[T_0, \ldots, T_m]$. We denote by I_r the ideal in the ring $k[T_0/T_r, \ldots, T_m/T_r]$ obtained by dehomogenizations of polynomials from I. Let $X_r \subset \mathbb{A}_k^m$ be the corresponding affine algebraic k-variety. We have $\mathcal{O}(X_r) \cong k[T_0/T_r, \ldots, T_m/T_r]/I_r$. We have a natural map $i_r : X_r(K) \to X(K)''$ obtained by the restriction of the natural inclusion map $i_r : K^m \to \mathbb{P}^m(K)''$ (putting 1 at the rth spot). It is clear that each $x \in X(K)''$ belongs to the image of some i_r. Now to define the morphism $X \to Y$ it suffices to define the morphisms $f_r : X_r \to Y, r = 0, \ldots, m$. This we know how to do. Each f_r is given by a collection $\{(p_0^{(s)}, \ldots, p_n^{(s)})\}_{s \in S(r)}$, where each coordinate $p_j^{(s)}$ is an element of the ring $\mathcal{O}(X)_r$), and $a_s \in \mathrm{rad}(\{p_0^{(s)}, \ldots, p_n^{(s)}\})$ for some $a_s \in \mathcal{O}(X)_r$. We can find a representative of $p_j^{(s)}$ in $k[T_0/T_r, \ldots, T_n/T_r]$ of the form $P_j^{(s)}/T_r^{d_j}$ where $P_j^{(s)}$ is a homogeneous polynomials of the same degree d_j. Reducing to the common denominator, we can assume that $d_j = d(s)$ is independent of $j = 0, \ldots, n$. Also by choosing appropriate representative F_s/T_r^l for a_s, we obtain that $T_r^\alpha F_s^\beta \in (P_0^{(s)}, \ldots, P_n^{(s)}) + I$. Collecting all these data for each $r = 0, \ldots, m$, we get that our morphism is given by a collection of

$$(P_0^{(s)}, \ldots, P_n^{(s)}) \in k[T_0, \ldots, T_m]_{d(s)}, s \in S = S(0) \coprod \ldots \coprod S(m).$$

The map is given as follows. Take $x = (x_0, \ldots, x_m) \in X(K)''$. If x_r is invertible in K, send x to a local line from $Y(K)$ defined by the global lines

$$(P_0^{(s)}(x), \ldots, P_n^{(s)}(x)) \in Y(K_{F_s(x)}), s \in S(r)$$

Since we can write for any $s \in S(r), T_r^{\alpha(r)} F_s^{\beta(r)} = \sum_j L_j P_j^{(s)} + I$, plugging x in both sides, and using that $T_r(x)^{\alpha(r)} = x_r^{\alpha(r)}$ is invertible, we obtain

$$F_s(x)^{\beta(r)} = \sum_j L_j(x) P_j^{(s)}(x).$$

This shows that $(P_0^{(s)}(x), \ldots, P_n^{(s)}(x)) \in C_n(K_{F_s(x)})$ is satisfied. Note that this definition is independent from the choice of projective coordinates of x. In fact, if we multiply x by $\lambda \in K^*$, we get $P_0^{(s)}(\lambda x) = \lambda^{k(s)} P_0^{(s)}(x)$. Also $F_s(x)$ will change to $\lambda^d F_s(x)$ for some $d \geq 0$, which gives the same localization $K_{F_s(x)}$.

Of course this representation is not defined uniquely in many ways. Also it must be some compatibility condition, the result of our map is independent from which r we take with the condition that $x_r \in K^*$. As is easy to see this is achieved by requiring:

$$P_j^{(s)} P_k^{(s')} - P_k^{(s)} P_j^{(s')} \in I$$

for any $s \in S(r), s' \in S(r')$ and any $k, j = 0, \ldots, n$. Since $F(p_0^{(s)}, \ldots, p_n^{(s)}) = 0$ for any F from the homogeneous ideal J defining Y, we must have

$$F(P_0^{(s)}, \ldots, P_n^{(s)}) \in I \quad \text{for any } s \in S.$$

The following proposition gives some conditions when a morphism $X \to Y$ can be given by one collection of homogeneous polynomials:

Proposition 1. *Let $X \subset \mathbb{P}_k^m$ and $Y \subset \mathbb{P}_k^n$ be two projective algebraic varieties defined by homogeneous ideals $I \subset k[T_0, \ldots, T_m]$ and $J \subset k[T_0', \ldots, T_n']$, respectively. Let $\phi : k[T']/J \to k[T]/I$ be a homomorphism given by polynomials $F_0, \ldots, F_n \in k[T_0, \ldots, T_m]$ (whose cosets modulo I are the images of T_i' modulo I). Assume*

(i) all $F_i \in k[T_0, \ldots, T_m]_d$ for some $d \geq 0$;

(ii) the ideal in $k[T_0, \ldots, T_m]$ generated by the ideal I and F_i's is irrelevant (i.e., contains the ideal $k[T_0, \ldots, T_m]_{\geq s}$ for some $s > 0$).

Then the formula:

$$a = (\alpha_0, \ldots, \alpha_m) \to (F_0(a), \ldots, F_n(a)), a \in X(K) \cap \mathbb{P}^m(K)'$$

defines a morphism $f : X \to Y$.

Proof. We have to check that $(F_0(a), \ldots, F_n(a)) \in C_n(K) \cap Y(K)$ for all K-algebras K. The "functoriality" (i.e. the commutativity of tyhe diagrams corresponding to homomorphisms $K \to K'$) is clear. Let $a^\sharp : k[T]/I \to K$, $T_i \bmod I \to \alpha_i$, be the homomorphisms defined by the point a. The composition $a^\sharp \circ \phi : k[T']/J \to K$ is defined by sending $T_j' \bmod J$ to $F_j(a)$. Thus for any $G \in J$ we have $G(F_0(a), \ldots, F_n(a)) = 0$. It remains to show that $(F_0(a), \ldots, F_n(a)) \in C(K)_n$. Suppose the coordinates generate a proper ideal I of K. By assumption, for some $s > 0$, we can write $T_i^s = \sum_j Q_j F_j + I$, for some $Q_j \in k[T]$. Thus $a_i^s = T_i^s(a) \in I$. Writing $1 = \sum_i b_i a_i^s$, we obtain that $1 \in I$. This contradiction shows that $(F_0(a), \ldots, F_n(a)) \in C(K)_n$. This proves the assertion.

Examples. 1. Let $\phi : k[T_0, \ldots, T_n] \to k[T_0, \ldots, T_n]$ be an automorphism of the polynomial algebra given by a linear homogeneous change of variables. More precisely:

$$\phi(T_i) = \sum_{j=0}^n a_{ij} T_j, \quad i = 0, \ldots, n$$

where (a_{ij}) is an invertible $(n+1)\times(n+1)$-matrix with entries in k. It is clear that ϕ satisfies the assumption of Proposition 1, therefore it defines an automorphism: $f:\mathbb{P}^n_k\to\mathbb{P}^n_k$. It is called a *projective automorphism.*

2. Assume $\mathrm{char}(k)\neq 2$. Let $C\subset\mathbb{A}^2_k$ be the circle $Z_1^2+Z_2^2=1$ and let $X: T_1^2+T_2^2=T_0^2$ be its projective closure in $\mathbb{P}^2_k$. Applying a projective automorphism of $\mathbb{P}^2_k, T_0\to T_2, T_1\to T_0-T_1, T_2\to T_0+T_1$ we see that X is isomorphic to the curve $T_0^2-T_1T_2=0$. Let us show that X is isomorphic to $\mathbb{P}^1_k$. The corresponding morphism $f:\mathbb{P}^1_k\to X$ is given by

$$(a_0,a_1)\to(a_0a_1,a_0^2,a_1^2).$$

The polynomials T_0T_1, T_0^2, T_1^2, obviously satisfy the assumption of the Proposition 1. The inverse morphism $f^{-1}: X\to\mathbb{P}^1_k$ is defined by the formula:

$$(a_0,a_1,a_2)\to\begin{cases}(a_1,a_0) & \text{if } a_1\in K^*,\\ (a_0,a_2) & \text{if } a_2\in K^*.\end{cases}$$

Note that $a_0\in K^*$ if and only if $a_1,a_2\in K^*$,

$$(a_1,a_0)=a_2(a_1,a_0)=(a_1a_2,a_0a_2)=(a_0^2,a_0a_2)=a_0(a_0,a_2)=(a_0,a_2)$$

if $a_1,a_2\in K^*$, and

$$(a_0,a_1,a_2)\to(a_1,a_0)\to(a_1a_0,a_1^2,a_0^2)=(a_1a_0,a_1^2,a_1a_2)=$$

$$a_1(a_0,a_1,a_2)=(a_0,a_1,a_2)\quad\text{if } a_1\in K^*,$$

$$(a_0,a_1,a_2)\to(a_0,a_2)\to(a_0a_2,a_0^2,a_2^2)=$$

$$(a_0a_2,a_1a_2,a_2^2)=a_2(a_0,a_1,a_2)=(a_0,a_1,a_2)\quad\text{if } a_2\in K^*.$$

Similarly, we check that the other composition of the functor morphisms is the identity. Recall that the affine circle X is not isomorphic to the affine line $\mathbb{A}^1_k$.

2. A projective subvariety E of $\mathbb{P}^n_k$ is said to be a projective d-subspace if it is given by a system of linear homogeneous equations with coefficients in k, whose set of solutions in k^{n+1} is a linear subspace E of k^{n+1} of dimension $d+1$. It follows from linear algebra that each such E can be given by a homogeneous system of linear equations

$$L_0=0,\dots,L_{n-d-1}=0.$$

Let $X\subset\mathbb{P}^n_k$ be such that

$$X(k)\cap E(k)=\emptyset.$$

Then the map

$$a\mapsto(L_0(a),\dots,L_{n-d-1}(a)),\quad a\in X(K),$$

defines a morphism

$$p_E: X\to\mathbb{P}^{n-d-1}_k$$

which is said to be a *linear projection* from E. Let $i:\mathbb{P}^{n-d-1}_k\to\mathbb{P}^n_k$ be the map given by $(a_0,\dots,a_{n-d-1})\mapsto(a_0,\dots,a_{n-d-1},0,\dots,0)$, then we can interpret the composition $p_E: X\to$

$\mathbb{P}_k^{n-d-1} \to \mathbb{P}_k^n$ as follows. Take a point $x \in X(K)$, find a projective subspace $E' \subset \mathbb{P}_k^n$ of dimension $d+1$ such that $E'(K)$ contains $E(K)$ and x. Then

$$p_E(x) = E'(K) \cap i(\mathbb{P}_k^{n-d-1}(K)).$$

We leave this verification to the reader (this is a linear algebra exercise).

3. We already know that $\mathbb{P}_k^1$ is isomorphic to a subvariety of $\mathbb{P}_k^2$ given by an equation of degree 2. This result can be generalized as follows. Let $N = \binom{n+m}{m} - 1$. Let us denote the projective coordinates in $\mathbb{P}_k^N$ by

$$\mathbf{T_i} = T_{i_0 \ldots i_n}, i_0 + \ldots + i_n = |\mathbf{i}| = m.$$

Choose some order in the set of multi-indices $\mathbf{i}$ with $|\mathbf{i}| = m$. Consider the morphism (the *Veronese morphism* of degree m)

$$v_{n,m} : \mathbb{P}_k^n \to \mathbb{P}_k^N,$$

defined by the collection of monomials $(\ldots, \mathbf{T^i}, \ldots)$ of degree m. Since $\mathbf{T^i}$ generate an irrelevant ideal, we can apply Proposition 1, so this is indeed a morphism. For any k-algebra K the corresponding map $v_{n,m}(K)' : \mathbb{P}_k^n(K)' \to \mathbb{P}_k^N(K)$ is defined by the formula $(a_0, \ldots, a_n) \to (\ldots, T^{\mathbf{i}}(a), \ldots)$. The image of $v_{n,m}(K)'$ is contained in the set $Ver_n^m(K)$, where Ver_n^m is the projective subvariety of $\mathbb{P}_k^N$ given by the following system of homogeneous equations

$$\{\mathbf{T_i T_j} - \mathbf{T_k T_t} = 0\}_{\mathbf{i+j=k+t}}.$$

It is called the m-fold *Veronese variety* of dimension n. We claim that $v_{n,m}(K) = Ver_n^m(K)$ for all K, so that $v_{n,m}$ defines an isomorphism of projective algebraic varieties:

$$v_{n,m} : \mathbb{P}_k^n \to Ver_n^m.$$

To verify this it suffices to check that $v_{n,m}(K)(\mathbb{P}_k^n(K)'') = Ver_n^m(K)''$ (compare with the beginning of the lecture). It is easy to see that for every $(\ldots, a_{\mathbf{i}}, \ldots) \in Ver_n^m(K)''$ at least one coordinate a_{me_i} is not zero (e_i is the i-th unit vector $(0, \ldots, 1, \ldots 0)$). After reindexing, we may assume that $a_{me_1} \neq 0$. Then the inverse map is given by the formula:

$$(x_0, x_1, \ldots, x_n) = (a_{(m,0,\ldots,0)}, a_{(m-1,1,1,\ldots,1)}, \ldots, a_{(m-1,0,\ldots,0,1)}).$$

Note that the Veronese map $v_{1,2} : \mathbb{P}_k^1 \to \mathbb{P}_k^2$ is given by the same formulas as the map from Example 2, and its image is a conic.

Next we want to define the Cartesian product $X \times Y$ of two projective varieties X and Y in such a way that the set of K-points of $X \times Y$ is naturally bijectively equivalent to $X(K) \times Y(K)$. The naturality is again defined by the commutativity of diagrams corresponding to the maps $X \times Y(K) \to X \times Y(L)$ and the product map $X(K) \times Y(K) \to X(L) \times Y(L)$. Consider first the case where $X = \mathbb{P}_k^n$ and $Y = \mathbb{P}_k^m$. For any k-algebra K and two submodules $M \subset K^{n+1}, M' \subset K^{m+1}$ we shall consider the tensor product $M \otimes N$ as a submodule of $K^{n+1} \otimes_k K^{m+1} \cong K^{(n+1)(m+1)}$. It is easy to see that this defines a map

$$s(n,m)_K : \mathbb{P}^n(K) \times \mathbb{P}^m(K) \to \mathbb{P}^N(K), \quad N = (n+1)(m+1) - 1.$$

Its restriction to $\mathbb{P}^n(K)' \times \mathbb{P}^m(K)'$ is defined by the formula

$$((a_0, \ldots, a_n), (b_0, \ldots, b_m)) = (a_0 b_0, \ldots, a_0 b_m, a_1 b_0, \ldots, a_1 b_m, \ldots, a_n b_0, \ldots, a_n b_m).$$

It is checked immediately that this map is well defined. It is easy to see that it is injective on the subsets $\mathbb{P}^n(K)'' \times \mathbb{P}^m_k(K)''$. In fact, if $a_i \in K^*$, we may assume $a_i = 1$, and reconstruct $(b_0, \ldots, b_m)$ from the right-hand side. Similarly we reconstruct $(a_0, \ldots, a_n)$. It is clear that the image of the map $s(n,m)_K$ is contained in the set $Z(K)$, where Z is a projective subvariety of $\mathbb{P}^N_k$ given by the equations:

$$T_{ij}T_{lk} - T_{ik}T_{lj} = 0, \quad i,l = 0,\ldots,n; \quad j,k = 0,\ldots,m. \tag{4}$$

in the polynomial ring $k[T_0, \ldots, T_N], T_0 = T_{00}, \ldots, T_N = T_{nm}$. Let us show that the image of $s(n,m)_K$ is equal to Z. Since we can reconstruct any $M \in \mathbb{P}^n(K)$ from its localizations, it suffices to verify that the map $s(n,m)''_K : \mathbb{P}^n(K)'' \times \mathbb{P}^m(K)'' \to Z(K)''$ is surjective. Let $z = (z_{00}, \ldots, z_{nm}) \in Z(K)''$ with some $z_{ij} \in K^*$. After reindexing we may assume that $z_{00} \in K^*$. Then $z_{ij} = z_{00}z_{ij} = z_{0j}z_{i0}$ for any $i = 0,\ldots,n, j = 0,\ldots,m$. Thus, $z = s_{n,m}(K)''(x,y)$, where

$$x = (z_{00}, z_{10}, \ldots, z_{n0}), \quad y = (z_{00}, z_{01}, \ldots, z_{0m}).$$

It remains to set

$$\mathbb{P}^n_k \times \mathbb{P}^m_k = Z \subset \mathbb{P}^N_k. \tag{5}$$

At this point it is natural to generalize the notion of a projective variety similarly as we did for an affine variety.

Definition. A *projective algebraic k-variety* is a correspondence $\mathcal{F}$ which assigns to each k-algebra K a set $\mathcal{F}(K)$ together with maps $\mathcal{F}(\phi) : \mathcal{F}(K) \to \mathcal{F}(L)$ defined for any homomorphism $\phi : K \to L$ of k-algebras such that the following properties hold:

(i) $\mathcal{F}(\phi) \circ \mathcal{F}(\psi) = \mathcal{F}(\phi \circ \psi)$ for any $\phi : K \to L$ and $\psi : L \to N$;

(ii) there exists a projective algebraic k-variety X and a set of bijections $\Phi_K : \mathcal{F}(K) \to X(K)$ such that for any $\phi : K \to L$ the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{F}(K) & \stackrel{\mathcal{F}(\phi)}{\longrightarrow} & \mathcal{F}(L) \\ \Phi_K \downarrow & & \downarrow \Phi_L \\ X(K) & \stackrel{X(\phi)}{\longrightarrow} & X(L). \end{array} \tag{5}$$

With this definition in mind we can say that the correspondence $K \to \mathbb{P}^n(K) \times \mathbb{P}^m(K)$ is a projective algebraic variety.

We leave to the reader to define the notions of a morphism and isomorphism between projective algebraic k-varieties.

For example, one defines the projection morphisms:

$$p_1 : \mathbb{P}^n_k \times \mathbb{P}^m_k \to \mathbb{P}^n_k, \quad p_2 : \mathbb{P}^n_k \times \mathbb{P}^m_k \to \mathbb{P}^m_k.$$

Now for any two projective subvarieties $X \subset \mathbb{P}^n_k$ and $Y \subset \mathbb{P}^m_k$ defined by the equations $\{F_s(T_0, \ldots, T_n) = 0\}_{s \in S}$ and $\{G_s(T'_0, \ldots, T'_m) = 0\}_{s' \in S'}$, respectively, the product $X \times Y$ is isomorphic to the projective subvariety of $\mathbb{P}^N_k, N = (n+1)(m+1) - 1$, defined by the equations:

$$T'^{r(s)}_j F_s(T) = 0, \quad j = 0,\ldots,m, \ s \in S, \ r(s) = \deg(F_s(T)),$$

$$T^{r(s')}_i F_{s'}(T') = 0, \quad i = 0,\ldots,n, \ s' \in S', \ r(s') = \deg(F'_{s'}(T)),$$

$$T_{ij}T_{lk} - T_{ik}T_{lj} = 0, \quad i,l = 0,\ldots,n; \ j,k = 0,\ldots,m,$$

where we write (uniquely) every monomial $T_j'^{r(s)}\mathbf{T}^{\mathbf{i}}$ (resp. $T_i^{r(s')}\mathbf{T}'^{\mathbf{i}}$) as the product of the variables $T_{ij} = T_iT_j', i = 0, \dots, n$ (resp. $T_{ij} = T_i'T_j, j = 0, \dots, m$).

Remark. Recall that for any two objects X and Y of a category $\mathcal{C}$, the Cartesian product is defined as an object $X \times Y$ satisfying the following properties. There are morphisms $p_1 : X \times Y \to X$ and $p_2 : X \times Y \to Y$ such that for any object Z and morphisms $f : Z \to X, g : Z \to Y$ there exists a unique morphism $\alpha : Z \to X \times Y$ such that $f = p_1 \circ \alpha, g = p_2 \circ g$. It is easy to see that the triple $(X \times Y, p_1, p_2)$ is defined uniquely, up to isomorphism, by the above properties. A category is called a *category with products* if for any two objects X and Y the Cartesian product $X \times Y$ exists. For example, if $\mathcal{C} = \mathcal{S}ets$, the Cartesian product is the usual one. If $\mathcal{C}$ is the category $\check{\mathcal{A}}$ of contravariant functors from a category $\mathcal{A}$ to $\mathcal{S}ets$, then it has products defined by the products of the values:

$$X \times Y(A) = X(A) \times Y(A).$$

The Segre construction shows that the category of projective algebraic varieties over a field k has products. As we saw earlier, the category of affine algebraic varieties also has products.

Problems.

1. Prove that any projective d-subspace in $\mathbb{P}_k^n$ is isomorphic to $\mathbb{P}_k^d$.
2. Prove that $\mathbb{P}_k^1 \times \mathbb{P}_k^1$ is isomorphic to a hypersurface $Q \subset \mathbb{P}_k^3$ given by a homogeneous equation of degree 2 (a *quadric*). Conversely, assuming that k is algebraically closed of $\mathrm{char}(k) \neq 2$, show that every hypersurface :

$$F(T_0, T_1, T_2, T_3) = \sum_{0 \leq i \leq \leq 3} a_{ij}T_i^2 + 2 \sum_{0 \leq i < j \leq 3} a_{ij}T_iT_j = 0,$$

where the symmetric matrix (a_{ij}) is nonsingular, is isomorphic to $\mathbb{P}_k^1 \times \mathbb{P}_k^1$. Give an explicit formula for the projection maps: $p_i : Q \to \mathbb{P}_k^1$.
3. Show that Ver_1^n is isomorphic to the projective closure of the affine curve given by the equations $\{Z_n - Z_1^n = 0, \dots, Z_2 - Z_1^2 = 0\}$ (a *rational normal curve* of degree n). Compare this with the problem 6 of Lecture 5.
4. Show that the image of a linear projection of the twisted cubic curve in $\mathbb{P}_k^3$ from a point not lying on this curve is isomorphic to a plane cubic curve. Find its equation and show that this curve is singular in the sense of the previous lecture.
5. Show that the symmetric m-power $S^m(M)$ of a projective module is a projective module. Using this prove that the Veronese map $v_{n,m}$ is defined by the formula $M \to Sym^m(M)$.
6. a) Show that $\mathbb{P}^n(K)'' \times \mathbb{P}_k^m(K)''$ is naturally bijectively equivalent to the set of $(n+1) \times (n+1)$ matrices of rank 1 with coefficients in K defined up to multiplication by a nonzero scalar.
b)Show $Ver_n^2(K)''$ is naturally bijectively equivalent to the set of symmetric rank 1 square matrices of size $n+1$ with coefficients in K defined up to multiplication by a nonzero scalar.
7. Construct a morphism from $\mathbb{P}_k^1$ to the curve X equal to the projective closure of the affine curve $(Z_1^2 + Z_2^2)^2 - Z_2(3Z_1^2 - Z_2^2)) \subset \mathbb{A}_k^2$. Is X isomorphic to $\mathbb{P}_k^1$?

Lecture 8. QUASI-PROJECTIVE ALGEBRAIC SETS

Let k be a field and K be an algebraically closed field containing k as a subfield.

Definition 1. A *projective algebraic set* over k (or a projective algebraic k-set) is a subset V of $\mathbb{P}^n(K)$ such that there exists a projective algebraic variety X over k with $X(K) = V$.

The variety X with $X(K) = V$ is not defined uniquely by V. However, as follows from the Nullstellensatz

$$X(K) = Y(K) \Longleftrightarrow \mathrm{rad}(I(X)) = \mathrm{rad}(I(Y)).$$

Thus, if we require that X is given by a radical homogeneous ideal, the variety X is determined uniquely by the set $X(K)$. In the following we will always assume this. Note that a radical homogeneous ideal I coincides with its saturation I^{sat}. Indeed, if $\mathfrak{m}^s F \in I$ for some s and $F \in k[T]_d$ then all monomials entering into F belong to $\mathfrak{m}^d$. In particular, $F^s \in \mathfrak{m}^{ds} \subset \mathfrak{m}^s$ and $F^s F = F^{s+1} \in I$. Since I is radical this implies that $F \in I$. In fact we have shown that, for any ideal I, we have

$$I \subset I^{sat} \subset \mathrm{rad}(I).$$

This, if $I = \mathrm{rad}(I)$, then $I = I^{sat}$. Since a projective algebraic k-variety is uniquely determined by a saturated homogeneous ideal, we see that there is a bijective correspondence between projective algebraic k-sets and projective algebraic k-varieties defined by a radical homogeneous ideal (they are called *reduced* projective algebraic k-varieties).

We can consider $\mathbb{P}^n(K)$ as a projective algebraic set over any subfield k of K. Any projective algebraic k-subset of $\mathbb{P}^n(K)$ is called a closed subset of $\mathbb{P}^n(K)$. The reason for this definition is explained by the following lemma.

Proposition 1. *There exists a unique topology on the set $\mathbb{P}^n(K)$ whose closed subsets are projective algebraic k-subsets of $\mathbb{P}^n_k(K)$.*

Proof. This is proven similarly to that in the affine case and we omit the proof.

The topology on $\mathbb{P}^n(K)$ whose closed sets are projective algebraic subsets is said to be the *Zariski k-topology*. We will denote the corresponding topological space by $\mathbb{P}^n_k(K)$. As is in the affine case we will drop k from the definitions and the notations if $k = K$. Every subset of $\mathbb{P}^n_k(K)$ will be considered as a topological subspace with respect to the induced Zariski k-topology.

Lemma-Definition 2. *A subset V of a topological space X is said to be locally closed if one the following equivalent properties holds:*

(i) $V = U \cap Z$, *where U is open and Z is closed;*

(ii) V *is an open subset of a closed subset of X;*

(iii) $V = Z_1 \setminus Z_2$, *where Z_1 and Z_2 are closed subsets of X.*

Proof. Left to the reader.

Definition 3. A locally closed subset subset of $\mathbb{P}^n_k(K)$ is called a *quasi-projective algebraic k-set.*

In other words, a quasi-projective k-subset of $\mathbb{P}^n(K)$ is obtained by taking the set of K-solutions of a homogeneous system of algebraic equations over k and throwing away a subset of the solutions satisfying some additional equations.

An example of an open quasi-projective subset is the subset

$$\mathbb{P}^n(K)_i = \{(a_0, \dots, a_n) \in \mathbb{P}^n(K) : a_i \neq 0\}.$$

Its complement is the "coordinate hyperplane":

$$H_i = \{(a_0, \dots, a_n) \in \mathbb{P}^n(K) : a_i = 0\}.$$

Every affine algebraic k-set $V \subset \mathbb{A}^n_k(K)$ can be naturally considered as a quasi-projective algebraic set. We view $\mathbb{A}^n(K) = K^n$ as the open subset $\mathbb{P}^n(K)_0$, then note that $V = \bar{V} \cap \mathbb{P}^n(K)_0$, where $\bar{V}$ is the closure of V defined by the homogenization of the ideal defining V. It is clear that, in general V is neither open nor closed subset of $\mathbb{P}^n(K)$. Also observe that $\bar{V}$ equals the closure in the sense of topology, i.e., the minimal closed subset of $\mathbb{P}^n_k(K)$ which contains V.

Next, we want to define regular maps between quasi-projective algebraic sets.

Definition 4. A map $f : V \to W \subset \mathbb{P}^m(K)$ of quasi-projective algebraic $k$sets is called *regular* if there exists a finite open cover $V = \cup_i U_i$ such that the restriction of f to each open subset U_i is given by a formula:

$$x \to (F_0^{(i)}(x), \dots, F_m^{(i)}(x)),$$

where $F_0^{(i)}(T), \dots, F_m^{(i)}(T)$ are homogeneous polynomials of some degree d_i with coefficients in k.

Proposition 2. *If $V = X(K)$ and $W = Y(K)$ for some projective algebraic k-varieties X and Y, and $f : X \to Y$ is a morphism of projective algebraic varieties, then $f_K : V \to W$ is a regular map.*

Proof. We have shown in Lecture 7 that the restriction of f_K to each open set $V \cap (\mathbb{P}^n)_i$ is given by several collections of homogeneous polynomials. Each collection is defined on an open set of points where some element of a covering family does not vanish.

Example 1. Let $V \subset \mathbb{P}^n_k(K), W = \mathbf{A}^1(K)$. A regular map $f : V \to \mathbf{A}^1(K) \subset \mathbb{P}_k(K)$ is given ("locally") by two homogeneous polynomials $F_0(T), F_1(T) \in k[T_0, \dots, T_n]_d$ such that $F_0(x) \neq 0$ for all x in some open subset U_i of V (could be the whole V but this is unlikely in general). Its value

$$f(x) = (F_0(x), F_1(x)) = (1, F_1(x)/F_0(x))$$

can be identified with the element $F_1(x)/F_0(x)$ of the field $K = \mathbf{A}^1(K)$. Thus f is given in U_i by a function of the form F/G, where F and G are homogeneous polynomials of the same degree with $G(x) \neq 0$ for all $x \in U_i$. Two such functions F/G and F'/G' are equal on U_i if and only if $(FG' - F'G)(x) = 0$ for all $x \in U_i$. If V is irreducible this implies that $(FG' - F'G)(x) = 0$ for all $x \in V$.

A regular map $f : V \to \mathbf{A}^1(K)$ is called a *regular function* on V. The set of regular functions form a k- algebra with respect to multiplication and addition of functions. We shall denote it by $\mathcal{O}(V)$. As we will prove later $\mathcal{O}(V) = k$ if V is a projective algebraic k-set. On the opposite side we have:

Proposition 3. *Let $V \subset \mathbb{A}^n$ be an affine algebraic set considered as a closed subset in $\mathbb{P}^n(K)_i$. Then $\mathcal{O}(V)$ is isomorphic to the algebra of regular function of the affine algebraic set V.*

Proof. Without loss of generality we may assume that $i = 0$. Let us, for a moment, denote the algebra of regular functions on an affine algebraic set (in the old sense) by $\mathcal{O}(V)'$. If $f \in \mathcal{O}(V)'$, we represent it by a polynomial $F(Z_1, \dots, Z_n) = P(T_0, \dots, T_n)/T_0^r$ for some homogeneous polynomial P of degree r. Then f coincides with a regular function in the new definition given by polynomials $(T_0^r, P(T_0, \dots, T_n))$. This defines a homomorphism $\mathcal{O}(V)' \to \mathcal{O}(V)$. Its injectivity is obvious. Let us show that this homomorphism is surjective. Let V be given by a system of equations $F_s(Z_1, \dots, Z_n) = 0, s \in S$, and $f \in \mathcal{O}(V)$ and $\{U_i\}_{i \in I}$ be an open cover of V such that there exist homogeneous polynomials $P_i(T_0, \dots, T_n), Q_i(T_0, \dots, T_n)$ of the same degree d_i for which

$$f_i(x) = P_i(x)/Q_i(x), Q_i(x) \neq 0 \quad \text{for all } x \in U_i.$$

Let $Q_i(Z)', P_i(Z)'$ denote the dehomogeneized polynomials. We have

$$Q_i(x)' f(x) = P_i(x)', \quad i \in I, x \in U_i.$$

If we multiply both sides by a polynomial vanishing on the closed subset $V \setminus U_i$, we will have the equality valid for all $x \in V$. We assume that this is the case. The system of equations

$$Q_i(Z)' = 0, i \in I, \quad F_s(Z) = 0, s \in S,$$

has no solutions in K^n. By Hilbert's Nullstellensatz

$$1 = \sum_i A_i Q_i' + \sum_s B_s F_s \tag{1}$$

for some polynomials $A_i, i \in I$, and $B_s, s \in S$. Thus, for any $x \in V$,

$$f(x) = \sum_i A_i(x) Q_i'(x) f(x) = \sum_i A_i(x) P_i'(x) = (\sum_i A_i Q_i')(x).$$

This shows that f is a global polynomial map, i.e. a regular function on V.

An *isomorphism* (or a *biregular map*) of quasi-projective algebraic sets is a bijective regular map such that the inverse map is regular (see Remark 3 in Lecture 3 which shows that we have to require that the inverse is a regular map). Two sets are isomorphic if there exists an isomorphism from one set to another.

It is not difficult to see (see Problem 8) that a composition of regulsr maps is a regular map. This implies that a regular map $f : V \to W$ defines the homomorphism of k-algebras $f^*(\mathcal{O}(W) \to \mathcal{O}(V)$. However, in general, this homomorphism does not determine f uniquely (as in the case of affine algebraic k-sets).

Definition 3. A quasi-projective algebraic set is said to be *affine* if it is isomorphic to an affine algebraic set.

Example 2. Let V be a closed subset of $\mathbb{P}^n(K)$ defined by an irreducible homogeneous polynomial F of degree $m > 1$. The complement set $U = \mathbb{P}^n(K) \setminus V$ does not come from any closed subset of $\mathbb{P}^n(K)_i$ since V does not contain any hyperplane $T_i = 0$. So, U is not affine in the way we consider any affine set as a quasi-projective algebraic set. However, U is affine. In fact, let $v_{n,m} : \mathbb{P}^n(K) \to \mathbb{P}^{N(n,m)}$ be the Veronese map defined by monomials of degree m. Then $v_{n,m}(U)$ is contained in the complement of a hyperplane H in $\mathbb{P}^{N(n,m)}$ defined by considering F as a linear combination of monomials. composing $v_{n,m}$ with a projective linear transformation we may assume that H is a coordinate hyperplane. Thus $v_{n,m}$ defines an isomorphism from U to the open subset of the Veronese projective algebraic set $Ver_{n,m}(K) = v_{n,m}(\mathbb{P}^n(K))$ whose complement is the closed subset $Ver_{n,m}(K) \cap H$. But this set is obviously affine, it is defined in $\mathbb{P}^{N(n,m)}(K)_i = K^{N(n,m)}$ by dehomogenizations of the polynomials defining $Ver_{n,m}$.

Lemma 2. *Let V be an affine algebraic k-set and $f \in \mathcal{O}(X)$. Then the set*

$$D(f) = \{x \in V : f(x) \neq 0\}$$

is affine and

$$\mathcal{O}(D(f)) \cong \mathcal{O}(V)_f.$$

Proof. Replacing V by an isomorphic algebraic k-set, we may assume that $V = X(K)$, where $X \subset K^n$ is an affine algebraic k-variety defined by an ideal I. Let $F \in k[Z_1, \dots, Z_n]$ be a polynomial representing f. Consider the closed subset of $K^{n+1} = K^n \times K$ defined by the equation $FZ_{n+1} - 1 = 0$ and let V' be its intersection with the closed subset $V \times K$. It is an affine algebraic k-set. We have

$$\mathcal{O}(V') = k[Z_1, \dots, Z_n, Z_{n+1}]/(I, FZ_{n+1} - 1) \cong k[Z_1, \dots, Z_n]/(I)[\frac{1}{f}] = \mathcal{O}(V)_f.$$

Let $p : K^{n+1} \to K^n$ be the projection. I claim that the restriction of p to V' defines an isomorphism $p' : V' \to D(f)$. It is obviously a regular map, since it is defined by the polynomials $(Z_1, \dots, Z_n)$. The inverse map $p^{-1} : V \to V'$ is defined by the map $x \mapsto (x, \frac{1}{f(x)})$. Let us see that it is a regular map. Let $P(T_0, \dots, T_n)$ be a homogenization of F, i.e., $F = \frac{P}{T_0^d}$ for some $d > 0$. We view V' as a closed subset of $\mathbb{P}^{n+1}(K)_0$ and $D(f)$ as a locally closed subset of $\mathbb{P}^n_k(K)_0$. Obviously the map p^{-1} coincides with the map

$$x = (1, x_1, \dots, x_n) \mapsto (PT_0(x), PT_1(x), \dots, PT_n(x), T_0^{d+1}(x)) = (1, x_1, \dots, x_n, \frac{1}{f(x)}).$$

defined by homogeneous polynomials $(PT_0, PT_1, \dots, PT_n, T_0^{d+1})$ of degree $d + 1$.

Theorem 1. *Let V be a quasi-projective k-set and $x \in V$. Then there exists an open subset $U \subset V$ containing x which is an affine quasi-projective set.*

Proof. Let $V = Z_1 \setminus Z_2$, where Z_1, Z_2 are closed subsets of $\mathbb{P}^n_k(K)$. Obviously $x \in \mathbb{P}^n(K)_i$ for some i. Thus x belongs to $(Z_1 \cap \mathbb{P}^n(K)_i) \setminus (Z_2 \cap \mathbb{P}^n(K)_i$. The subsets $Z_1 \cap \mathbb{P}^n(K)_i$ and $Z_2 \cap \mathbb{P}^n(K)_i$ are closed subsets of K^n. Let F be a regular function on K^n which vanishes on $Z_2 \cap \mathbb{P}^n(K)_i$ but does not vanish at x. Then its restriction to $V = Z_1 \cap \mathbb{P}^n(K)_i$ defines a regular function $f \in \mathcal{O}(V)$ such that $x \in D(f) \subset V \subset Z_2 \cap \mathbb{P}^n(K)_i$. By the previous lemma $D(f)$ is an affine quasi-projective k-set.

Corollary. *The set of open affine quasi-projective sets form a basis in the Zariski topology of $\mathbb{P}^n(K)$.*

Recall that a basis of a topological space X is a family $\mathcal{F}$ of open subsets such that for any $x \in X$ and any open U containing x there exists $V \in \mathcal{F}$ such that $x \in V \subset U$. We shall prove in the next lecture that the intersection of two open affine sets is an open affine set. This implies that the Zariski topology can be reconstructed from the set of affine open sets.

Remark. The reader who is familiar with the notion of a manifold (real or complex) will easily notice the importance of the previous theorem. It shows that the notion of a quasi-projective algebraic set is very similar to the notion of a manifold. A quasi-projective algebraic set is a topological space which is locally homeomorphic to a special topological space, an affine algebraic set.

Proposition 4. *Every quasi-projective algebraic k-set V is a quasi-compact topological space.*

Proof. Recall that a topological space V (not necessarily separated) is said to be *quasi-compact* if every its open covering $\{U_i\}_{i\in I}$ contains a finite subcovering, i.e.

$$V = \cup_{i\in I} U_i \Longrightarrow V = \cup_{i\in J} U_i,$$

where J is a finite subset of I.

Every Noetherian space is quasi-compact. Indeed, in the above notation we form a decreasing sequence of closed subsets

$$V \setminus U_{i_1} \supset V \setminus (U_{i_1} \cup U_{i_2}) \supset \dots$$

which must stabilize with a set $V' = V \setminus (U_{i_1} \cup \dots \cup U_{i_r})$. If it is not empty, we can subtract one more subset U_{i_j} to decrease V'. Therefore, $V' = \emptyset$ and $V = U_{i_1} \cup \dots \cup U_{i_r}$. Thus, it suffices to show that a quasi-projective set is Noetherian. But obviously it suffices to verify that its closure is Noetherian. This is checked similarly to that as in the affine case by applying Hilbert's Basis Theorem.

Corollary. *Every algebraic set can be written uniquely as the union of finitely many irreducible subspaces Z_i, such that $Z_i \not\subset Z_j$ for any $i \neq j$.*

Lemma 3. *Let V be a topological space and Z be its subspace. Then Z is irreducible if and only if its closure $\bar{Z}$ is irreducible.*

Proof. Obviously follows from the definition.

Proposition 5. *A subspace Z of $\mathbb{P}^n_k(K)$ is irreducible if and only if the radical homogeneous ideal defining the closure of Z is prime.*

Proof. By the previous lemma, we may assume that Z is closed. Then Z is a projective algebraic set defined by its radical homogeneous ideal. The assertion is proven similarly to the analogous assertion for an affine algebraic set. We leave the proof to the reader.

Problems.

1. Is the set $\{(a,b,c) \in \mathbb{P}^2(K) : a \neq 0, b \neq 0\} \cup \{(1,0,0)\}$ quasi-projective?
2. Let V be a quasi-projective algebraic set in $\mathbb{P}^n(K), W$ be a quasi-projective algebraic set in $\mathbb{P}^r(K)$. Prove that $s_{n,m}(K)(V \times W)$ is a quasi-projective algebraic subset of $Seg_{n,m}(K) = s_{n,m}(K)(\mathbb{P}^n(K) \times \mathbb{P}^r(K)) \subset \mathbb{P}^{(n+1)(m+1)-1}(K)$.
3. Let us identify the product $V \times W \subset \mathbb{P}^n(K) \times \mathbb{P}^r(K)$ of two quasi-projective algebraic k-sets with a quasi-projective algebraic k-subset of the Segre set $Seg_{n,m}(K)$. Let $f : V \to V'$ and $g : W \to W'$ be two regular maps. Show that the map $f \times g : V \times W \to V' \times W'$ is a regular map.
4. Is the union (resp. the intersection) of quasi-projective algebraic sets a quasi-projective algebraic set?
5. Find the irreducible components of the projective subset of $\mathbb{P}^3(K)$ given by the equations: $T_2T_0 - T_1^2 = 0, T_1T_3 - T_2^2 = 0$.
6. Show that every irreducible component of a projective hypersurface $V(F) = \{a \in \mathbb{P}^n(K) : F(a) = 0\}$ is a hypersurface $V(G)$, where G is an irreducible factor of the homogeneous polynomial $F(T)$.

7. Describe explicitly (by equations) a closed subset of some K^n which is isomorphic to the complement to a conic $T_0T_1 + T_2^2 = 0$ in $\mathbb{P}^2(K)$.
8. Prove that a regular map is a continuous map and that the composition of regular maps is a regular map.

Lecture 9. THE IMAGE OF A PROJECTIVE ALGEBRAIC SET

Let $f : V \to W$ be a regular map of quasi-algebraic k-sets. We are interested in its image $f(V)$. Is it a quasi-projective algebraic set? For instance, let $f : K^2 \to K^2$ be given by $(x, y) \mapsto (x, xy)$. Then its image is the union of the set $U = \{(a, b) \in K^2 : a \neq 0\}$ and the closed subset $Z = \{(0, 0)\}$. The only open subset of $\mathbb{A}^2_k(K)$ which contains the image $f(K^2)$ is K^2 and the image is not closed there. Thus $f(\mathbb{A}^2_k(K))$ is not locally closed in $\mathbb{A}^2_k(K)$. Since K^2 is an open subset of $\mathbb{P}^2_k(K)$, $f(\mathbb{A}^2_k(K))$ is not locally closed in $\mathbb{P}^2_k(K)$, i.e., it is not a quasi-projective algebraic set.

However, the situation is much better in the case where V is a projective set. We will prove the following result:

Theorem 1. *The image of a projective algebraic k-set V under a regular map $f : V \to W$ is a closed subset of W in the Zariski k-topology.*

To prove this theorem we note first that

$$f(V) = \mathrm{pr}_2(\Gamma_f)$$

where

$$\Gamma_f = \{(x, y) \in V \times W : y = f(x)\}$$

is the graph of f, and $rmpr_2 : V \times W \to W, (x, y) \mapsto y$ is the projection map. We will always consider the product $V \times W$ as a quasi-projective set by embedding it into a projective space by the Segre map. In particular, $V \times W$ is a topological space with respect to the Zariski topology.

Our theorem follows from the following two results:

Proposition 1. *The graph Γ_f of a regular map $f : V \to W$ is a closed subset of $V \times W$.*

Theorem 2 (Chevalley). *Let V be a projective algebraic k-set, W be a quasi-projective algebraic k-set and Z be a closed subset of $V \times W$. Then $\mathrm{pr}_2(Z)$ is closed in W.*

Let us first prove the proposition. The proof is based on the following simple observations:

(i) If $W \subset W'$ and $f' : V \to W'$ is the composition of f and the inclusion map, then $\Gamma_f = (V \times W) \cap \Gamma_{f'}$. Thus, the closedness of $\Gamma_{f'}$ in $V \times W'$ implies the closedness of Γ_f.

(ii) If $f : V \to W$ and $f' : V' \to W'$ are two regular maps, then the map $f \times f' : V \times W \to V' \times W', (x, x') \mapsto (f(x), f'(y))$ is a regular map (Problem 4 from Lecture 8).

(iii) If $\Delta_W = \{(y, y') \in W \times W : y = y'\}$ (the *diagonal* of W), then $\Gamma_f = (f \times \mathrm{id}_W)^{-1}(\Delta_W)$.

By (ii), $f \times \mathrm{id}_W : V \times W \to W \times W$ is continuous. Thus it suffices to check that $\Delta_W \subset W \times W$ is closed. By (i) we may assume that $W = \mathbb{P}^n_k(K)$. However, the diagonal $\Delta_{\mathbb{P}^n_k(K)} \subset \mathbb{P}^n_k(K) \times \mathbb{P}^n_k(K)$ is given by the system of equations:

$$T_{ij} - T_{ji} = 0, i, j = 0, \dots, n, \quad T_{ij}T_{rt} - T_{it}T_{rj} = 0, i, j, r, t = 0, \dots, n.$$

in coordinates T_{ij} of the space containing the image of $\mathbb{P}^n_k(K) \times \mathbb{P}^n_k(K)$ under the Segre map $s_{n,n}(K)$. This proves Proposition 1.

Remarks 1. It is known from general topology that the closedness of the diagonal of a topological space X is equivalent to the Hausdorff separatedness of X. Since we know that algebraic sets are usually not separated topological spaces, Proposition 1 seems to be contradictory. To resolve this paradox we observe that the Zariski topology of the product $V \times W$ is not the product of topologies of the factors.

2. One should also compare the assertion of Theorem 2 with the definition of a perfect map of topological spaces. According to this definition (see N. Bourbaki, General Topology, Chapter 1, §11), the assertion of the theorem implies that the constant map $X \to \{point\}$ is perfect. Corollary 1 to Theorem 1 from loc. cit. says that this is equivalent to that X is quasi-compact. Since we know that X is quasi-compact always (projective or not projective), this seems to be a contradiction again. The explanation is the same as above. The Zariski topology of the product is not the product topology. Nevertheless, we should consider the assertion of Theorem 2 as the assertion about the "compactness" of a projective algebraic set.

Before proving Theorem 2 let us prove the following:

Lemma. *Let V be a closed subset of $\mathbb{P}^n_k(K) \times \mathbb{P}^m_k(K)$ (resp. of $\mathbb{P}^n_k(K) \times \mathbb{A}^m_k(K)$). Then V is the set of zeroes of polynomials $P_s(T_0, \dots, T_n, T'_0, \dots, T'_m) \in k[T_0, \dots, T_n, T'_0, \dots, T'_m], s \in S$, which are homogeneous of degree $d(s)$ in variables $T_0, \dots, T_n$ and homogeneous of degree $d(s)'$ in the variables $T'_0, \dots, T'_m$ (resp. V is the set of zeroes of polynomials $P_s(T_0, \dots, T_n, Z'_1, \dots, Z'_m) \in k[T_0, , \dots, T_n, Z'_1, \dots, Z'_m], s \in S$, which are homogeneous of degree $d(s)$ in variables $T_0, \dots, T_n$). Conversely every subset of $\mathbb{P}^n_k(K) \times \mathbb{P}^m_k(K)$ (resp. of $\mathbb{P}^n_k(K) \times \mathbb{A}^m_k(K)$) defined in this way is a closed subset in the Zariski k-topology of the product.*

Proof. It is enough to prove the first statement. The second one will follow from the first one by taking the closure of V in $\mathbb{P}^n_k(K) \times \mathbb{P}^m_k(K)$ and then applying the dehomogenization process in the variable T'_0. Now we know that V is given by a system of homogeneous polynomials in variables T_{ij} in the space $\mathbb{P}^{(n+1)(m+1)-1}_k$ and the system of equations defining the Segre set $Seg_{n,m}(K)$. Using the substitution $T_{ij} = T_iT'_j$, we see that V can be given by a system of equations in $T_0, \dots, T_n, T'_0, \dots, T'_m$ which are homogeneous in each set of variables of the same degree. If we have a system of polynomials $P_s(T_0, \dots, T_n, T'_0, \dots, T'_m)$ which are homogeneous of degree $d(s)$ in variables $T_0, \dots, T_n$ and homogeneous of degree $d(s)'$ in variables $T'_0, \dots, T'_m$, its set of solutions in $\mathbb{P}^n_k(K) \times \mathbb{P}^m_k(K)$ is also given by the system in which we replace each P_s by $T_i'^{d(s)-d(s)'}P_s, i = 0, \dots, m$, if $d(s) > d(s)'$ and by $T_i^{d(s)'-d(s)}P_s, i = 0, \dots, n$, if $d(s) < d(s)'$. Then the enlarged system arises from a system of polynomials in T_{ij} after substitution $T_{ij} = T_iT'_j$.

Now let us prove Theorem 2. Let V be a closed subset of $\mathbb{P}^n_k(K)$. Then $Z \subset V \times W$ is a closed subset of $\mathbb{P}^n(K) \times W$ and $\mathrm{pr}_2(Z)$ equals the image of Z under the projection $\mathbb{P}^n_k(K) \times W \to W$. Thus we may assume that $V = \mathbb{P}^n_k(K)$.

Let $W = \cup_{i \in I} U_i$ be a finite affine covering of W (i.e. a covering by open affine sets). Then $V \times W = \cup_{i \in I}(V \times U_i), Z = \cup_{i \in I} Z \cap (V \times U_i)$ and $\mathrm{pr}_2(Z) = \cup_{i \in I} pr_2 Z \cap (V \times U_i)$. This shows

that it suffices to check that $\mathrm{pr}_2 Z \cap (V \times U_i)$ is closed in U_i. Thus we may assume that $W = U_i$ is affine. Then W is isomorphic to a closed subset of some $\mathbb{A}^m_k(K)$, $V \times W$ is closed in $V \times \mathbb{A}^m_k(K)$ and $\mathrm{pr}_2(Z)$ is equal to the image of Z under the second projection $V \times \mathbb{A}^m_k \to \mathbb{A}^m_k$. Thus we may assume that $W = \mathbb{A}^m_k(K)$ and $V = \mathbb{P}^n_k(K)$.

Let Z be a closed subset of $\mathbb{P}^n_k(K) \times \mathbb{A}^m_k(K)$. By the Lemma, Z can be given by a system of equations

$$F_i(T_0, \ldots, T_n, t_1, \ldots, t_m) = 0, i = 1, \ldots, N.$$

where $F_i \in k[T_0, \ldots, T_n, t_1, \ldots, t_m]$ is a homogeneous of degree $d(i)$ in variables $T_0, \ldots, T_n$. For every $a = (a_1, \ldots, a_m) \in K^m$, we denote by X_a the projective algebraic subset of $\mathbb{P}^n(K)$ defined by the system of homogeneous equations:

$$F_i(T_0, \ldots, T_n, a_1, \ldots, a_m) = 0, i = 1, \ldots, N.$$

It is clear that $X_a = \emptyset$ if and only if $(0, \ldots, 0)$ is the only solution of this system in K^{n+1}. By Nullstellensatz, this happens if only if the radical of the ideal I_a generated by the polynomials $F_i(T, a_1, \ldots, a_m)$ is equal to $(T_0, \ldots, T_n)$. This of course equivalent to the property that $(T_0, \ldots, T_n)^s \subset I_a$ for some $s \geq 0$.

Now we note that

$$\mathrm{pr}_2(Z) = \{a \in K^m : X_a \neq \emptyset\} = \{a \in K^m : (T_0, \ldots, T_n)^s \not\subset I_a \quad \text{for any } s \geq 0\}$$

$$= \cap_{s \geq 0} \{a \in K^m : (T_0, \ldots, T_n)^s \not\subset I_a\}.$$

Thus it suffices to show that each set $Y_s = \{a \in K^m : (T_0, \ldots, T_n)^s \not\subset I_a\}$ is closed in the Zariski k-topology. Note that $(T_0, \ldots, T_n)^s \subset I_a$ means that every homogeneous polynomial of degree s can be written as $\sum_i, F_i(T, a)Q_i(T))$ for some $Q_i(T) \in k[T]_{s-d(i)}$, where $d(i) = \deg F_i(T, a)$. Consider the linear map of linear k-spaces

$$\phi : \oplus_{i=1}^N k[T]_{s-d(i)}, \quad (Q_1, \ldots, Q_N) \mapsto \sum_i F_i(T, a)Q_i(T)).$$

This map is surjective if and only if $a \in K^m \backslash Y_s$. Thus, $a \in Y_s$ if and only if $\mathrm{rank}(\phi) < d = \dim k[T]_s$. The latter condition can be expressed by the equality to zero of all minors of order d in any matrix representing the linear map ϕ. However, the coefficients of such a matrix (for example, with respect to a basis formed by monomials) are polynomials in $a_1, \ldots, a_n$ with coefficients from k. Thus, every minor is also a polynomial in a. The vanishing of these polynomials define the closed subset Y_s in the Zariski k-topology. This proves Theorem 2.

Recall that a topological space X is said to be *connected* if $X \neq X_1 \cup X_2$ where V_1 and V_2 are proper open (equivalently, closed) subsets with empty intersection. One defines naturally the notion of a connected component of V and shows that V is the union of finitely many connected components. Clearly, an irreducible space is always connected, but the converse is false in general. For every quasi-projective algebraic k-set V we denote by $\pi_0(V)$ the set of its connected components. Let $\bar{\pi}_0(V)$ denote the set of connected components of the corresponding K-set. Both of these sets are finite since any irreducible component of V is obviously connected. We say that V is *geometrically connected* if $\#\bar{\pi}_0(V) = 1$. Notice the difference between connectedness and geometric connectedness. For example, the number of connected components of the affine algebraic k-subset of $\mathbb{A}^1_k$ defined by a non-constant non-zero polynomial $F(Z) \in k[Z]$ equals the number of irreducible factors of $F(Z)$. The number of connected components of the corresponding K-set equals the number of distinct roots of $F(Z)$ in K.

Corollary 1. *Assume k is a perfect field. Let V be a projective algebraic k-set, $n = \#\pi_0(V)$. Then there is an isomorphism of k-algebras $\mathcal{O}(V) \cong k_1 \oplus \ldots \oplus k_n$ where each k_i is a finite field extension of k. Moreover*

$$\sum_i^n [k_i : k] = \#\bar{\pi}_0(V).$$

In particular, if V is connected as an algebraic K-set, $\mathcal{O}(V) = K$.

Proof. Let $V_1, \ldots, V_n$ be connected components of V. It is clear that $\mathcal{O}(V) \cong \mathcal{O}(V_1) \oplus \ldots \oplus \mathcal{O}(V_n)$ so we may assume that V is connected. Let $f \in \mathcal{O}(V)$. It defines a regular map $f : V \to \mathbb{A}^1(K)$. Composing it with the inclusion $\mathbb{A}^1(K) \hookrightarrow \mathbb{P}^1_k(K)$, we obtain a regular map $f' : V \to \mathbb{P}^1_k(K)$. By Theorem 1, $f(V) = f'(V)$ is closed in $\mathbb{P}^1_k(K)$. Since $f(V) \subset \mathbb{A}^1_k(K)$, it is a proper closed subset, hence finite. Since V is connected, $f(V)$ must be connected (otherwise the pre-image of a connected component of $f(V)$ is a connected component of V). Hence $f(V) = \{a_1, \ldots, a_r\} \subset K$ is the set of roots of an irreducible polynomial with coefficients in k. It is clear that $a_i \neq 0$ unless $f(V) = \{0\}$ hence $f = 0$. This implies that $f(x) \neq 0$ for any $x \in V$. If f is given by a pair of homogeneous polynomials (P, Q) then f^{-1} is given by the pair (Q, P) and belongs to $\mathcal{O}(V)$. Therefore $\mathcal{O}(V)$ is a field. Assume $k = K$, then the previous argument shows that $r = 1$ and $f(x) = a_1$ for all $x \in V$, i.e., $\mathcal{O}(V) = k$. Thus if $\bar{V}$ denotes the set V considered as a K-set, we have shown that $\mathcal{O}(\bar{V}) \cong K^m$ where $m = \#\bar{\pi}_0(V) = \#\pi_0(\bar{V})$. But obviously $\mathcal{O}(\bar{V}) = \mathcal{O}(V) \otimes_k K \cong K^d$ where $d = [\mathcal{O}(V) : k]$. Here we again use that $\mathcal{O}(V)$ is a separable extension of k. This shows that $m = [\mathcal{O}(V) : k]$ and proves the assertion.

Corollary 2. *Let Z be a closed connected subset of $\mathbb{P}^n_k(K)$. Suppose Z is contained in an affine subset U of $\mathbb{P}^n_k(K)$. Then the ideal of $\mathcal{O}(U)$ of functions vanishing on Z is a maximal ideal. In particular, Z is one point if k is algebraically closed.*

Proof. Obviously Z is closed in U, hence is an affine algebraic k-set. We know that $\mathcal{O}(Z) = k'$ is a finite field extension of k. The kernel of the restriction homomorphism $\mathrm{res}_{U/Z} : \mathcal{O}(U) \to \mathcal{O}(Z) = k'$ is a maximal ideal in $\mathcal{O}(U)$. In fact if A is a subring of k' containing k it must be a field (every nonzero $x \in A$ satisfies an equation $x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0$ with $a_n \neq 0$, hence $x(x^{n-1} + a_1 x^{n-2} + \ldots + a_{n-1})(-a_n^{-1}) = 1$). This shows that Z does not contain proper closed subsets in the Zariski k-topology. If k is algebraically closed, all points are closed, hence Z must be a singleton.

Corollary 3. *Let $f : V \to W$ be a regular map of a connected projective algebraic set to an affine algebraic set. Then f is a constant map.*

Proof. We may assume that $k = K$ since we are talking about algebraic K-sets. Let $W \subset \mathbb{P}^n(K)_0 \subset \mathbb{P}^n(K)$ for some n, and $f' : V \to \mathbb{P}^n(K)$ be the composition of f and the natural inclusion $W \hookrightarrow \mathbb{P}^n(K)$. By Theorem 1, $f(V) = f'(V)$ is a closed connected subset of $\mathbb{P}^n(K)$ contained in an affine set (the image of a connected set under a continuous map is always connected). By Corollary 2, $f(V)$ must be a singleton.

Problems.

1. Let $K[T_0, \ldots, T_n]_d$ be the space of homogeneous polynomials of degree d with coefficients in an algebraically closed field K. Prove that the subset of reducible polynomials is a closed subset of $K[T_0, \ldots, T_n]_d$ where the latter is considered as affine space $\mathbb{A}^N(K), N = \binom{n+d}{d}$. Find its equation when $n = d = 2$.

2. Prove that $K^n \setminus \{\text{a point}\}$ or $\mathbb{P}^n(K) \setminus \{\text{point}\}$ is not an affine algebraic set if $n > 1$, also is not isomorphic to a projective algebraic set.

3. Prove that the intersection of open affine subsets of a quasi-projective algebraic set is affine [Hint: Use that for any two subsets A and B of a set S, $A \cap B = \Delta_S \cap (A \times B)$ where the diagonal Δ_S is identified with S].

4. Let $X \subset \mathbb{P}^n$ be a connected projective algebraic set other than a point and Y is a projective set defined by one homogeneous polynomial. Show that $X \cap Y \neq \emptyset$.

5. Let $f : X \to Z$ and $g : Y \to Z$ be two regular maps of quasi-projective algebraic sets. Define $X \times_Z Y$ as the subset of $X \times Y$ whose points are pairs (x, y) such that $f(x) = g(y)$. Show that $X \times_Z Y$ is a quasi-algebraic set. A map $f : X \to Z$ is called *proper* if for any map $g : Y \to Z$ and any closed subset W of $X \times_Z Y$ the image of W under the second projection $X \times Y \to Y$ is closed. Show that f is always proper if X is a projective algebraic set.

Lecture 10. FINITE REGULAR MAPS

The notion of a finite regular map of algebraic sets generalizes the notion of a finite extension of fields. Recall that an extension of fields $F \to E$ is called finite if E is a finite-dimensional vector space over F. This is easy to generalize. We say that an injective homomorphism $\phi : A \to B$ of commutative rings is finite if B considered as a module over A via of the homomorphism ϕ is finitely generated. What is the geometric meaning of this definition? Recall that a finite extension of fields is an algebraic extension. This means that any element in E satisfies an algebraic equation with coefficients in F. The converse is also true provided E is finitely generated over F as a field. We shall prove in the next lemma that a finite extension of rings has a similar property: any element in B satisfies an algebraic equation with coefficients in $\phi(A)$. Also the converse is true if we additionally require that B is a finitely generated algebra over A and every element satisfies a monic equation (i.e. with the highest coefficient equal to 1) with coefficients in $\phi(A)$.

Let us explain the geometric meaning of the additional assumption that the equations are monic. Recall that an algebraic extension E/F has the following property. Let $y : F \to K$ be a homomorphism of F to an algebraically closed field K. Then y extends to a homomorphism of fields $x : E \to K$. Moreover the number of these extensions is finite and is equal to the separable degree $[E : F]_s$ of the extension E/F. An analog of this property for ring extensions must be the following. For any algebraically closed field K which has a structure of a A-algebra via a homomorphism $y : A \to K$ (this is our analog of an extension K/F) there a non-empty finite set of homomorphisms $x_i : B \to K$ such that $x_i \circ \phi = y$. Let us interpret this geometrically in the case when ϕ is a homomorphism of finitely generated k-algebras. Let X and Y be afiine algebraic k-varieties such that $\mathcal{O}(X) \cong B$, $\mathcal{O}(Y) \cong A$. The homomorphism ϕ defines a morphism $f : X \to Y$ such that $\phi = f^*$. A homomorphism $y : A \to K$ is a K-point of Y. A homomorphism $y_i : B \to K$ such that $x_i \circ \phi = y$ is a K-point of X such that $f_K(x_i) = y$. Thus the analog of the extension property is the property that the map $X(K) \to Y(K)$ is surjective and has finite fibres. Let B is generated over A by one element b satisfying an algebraic equation

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

with coefficients in A. Assume the ideal $I = (a_0, \ldots, a_{n-1})$ is proper but a_n is invertible in A. Let $\mathfrak{m}$ be a maximal ideal in A containing I. Let K be an algebraically closed field containing the residue field $A/\mathfrak{m}$. Consider the K-point of Y corresponding to the homomorphism $y : A \to A/\mathfrak{m} \to K$. Since $B \cong A[x]/(a_0 x^n + a_1 x^{n-1} + \ldots + a_n)$, any homomorphism extending y must send a_n to zero but this is impossible since a_n is invertible. Other bad thing may happen if $a_n \in I$. Then we obtain infinitely many extensions of y, they are defined by sending x to any element in K. It turns out that requiring that a_0 is invertible will guarantee that $X(K) \to Y(K)$ is surjective with finite fibres.

We start with reviewing some facts from commutative algebra.

Definition. A commutative algebra B over a commutative ring A is said to be *integral* over A if every element $x \in B$ is integral over A (i.e. satisfies an equation $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ with $a_i \in A$).

Lemma 1. *Assume that B is a finitely generated A-algebra. Then B is integral over A if and only if B is a finitely generated module over A.*

Proof. Assume B is integral over A. Let $x_1, \ldots, x_n$ be generators of B as an A-algebra (i.e., for any $b \in B$ there exists $F \in A[Z_1, \ldots, Z_n]$ such that $b = F(x_1, \ldots, x_n)$). Since each x_i is integral over A, there exists some integer $n(i)$ such that $x_i^{n(i)}$ can be written as a linear combination of lower powers of x_i with coefficients in A. Hence every power of x_i can be expressed as a linear combination of powers of x_i of degree less than $n(i)$. Thus there exists a number $N > 0$ such that every $b \in B$ can be written as a polynomial in $x_1, \ldots, x_n$ of degree $< N$. This shows that a finite set of monomials in $x_1, \ldots, x_n$ generate B as an A-module.

Conversely, assume that B is a finitely generated A-module. Then every $b \in B$ can be written as a linear combination $b = a_1 b_1 + \ldots + a_r b_r$, where $b_1, \ldots, b_r$ is a fixed set of elements in B and $a_i \in A$. Multiplying the both sides by b_i and expressing each product $b_i bj$ as a linear combination of b_i's we get

$$bb_i = \sum_j a_{ij} b_i, \quad a_{ij} \in A. \tag{1}$$

This shows that the vector $\mathbf{b} = (b_1, \ldots, b_r)$ satisfies the linear equation $(M - bI_n)\mathbf{b} = 0$, where $M = (a_{ij})$. Let $D = \det(M - bI_n)$. Applying the Cramer rule, we obtain that $Db_i = 0, i = 1, \ldots, n$. Using (1) we see that $Dx = 0$ for all $x \in B$. In particular, $D \cdot D = D^2 = 0$. It remains to use that the equation $D^2 = 0$ is a monic equation for b with coefficients in A.

This Lemma implies the following result which we promised to prove in Lecture 2:

Corollary. *Let B be an A-algebra. The set of elements in B which are integral over A is a subring of B (it is called the integral closure of A in B).*

Proof. Let $b, b' \in B$ be integral over A. Consider the A-subalgebra $A[b, b']$ of B generated by these elements. Since b is integral over A, it satisfies an equation $b^n + a_1 b^{n-1} + \ldots + a_n, a_i \in A$, hence $A[b]$ is a finitely generated A-module generated by $1, \ldots, b^{n-1}$. Similarly, since b' is integral over A, hence over $A[b]$, we get $A[b, b'] = A[b][b']$ is a finitely generated $A[b]$-module. But then $A[b, b']$ is a finitely generated A-module. By Lemma 1, $A[b, b']$ is integral over A. This checks that $b + b', b \cdot b'$ are integral over A.

Lemma 2. *Let B be integral over its subring A. The following assertions are true:*

(i) if A is a field and B is without zero divisors, then B is a field;
(ii) if I is an ideal of B such that $I \cap A = \{0\}$ and B is without zero divisors then $I = \{0\}$;
(iii) if $\mathcal{P}_1 \subset \mathcal{P}_2$ are two ideals of B with $\mathcal{P}_1 \cap A = \mathcal{P}_2 \cap A$ and $\mathcal{P}_1$ is prime, then $\mathcal{P}_1 = \mathcal{P}_2$;
(iv) if S is a multiplicatively closed subset of A, then the natural homomorphism $A_S \to B_S$ makes B_S an integral algebra over A_S;
(v) if I is a proper ideal of A then the ideal IB of B generated by I is proper;
(vi) for every prime ideal $\mathcal{P}$ in A there exists a prime ideal $\mathcal{P}'$ of B such that $\mathcal{P}' \cap A = \mathcal{P}$.

Proof. (i) Every x satisfies an equation $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ with $a_i \in A$. Since B has no zero divisors, we may assume that $a_n \neq 0$ if $x \neq 0$. Then $x(x^{n-1} + a_1 x^{n-2} + \ldots + a_{n-1})(-a_n^{-1}) = 1$. Hence x is invertible.

(ii) As in (i), we may assume that every nonzero $x \in I$ satisfies an equation $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ with $a_i \in A$ and $a_n \neq 0$. Then $a_n = -x(x^{n-1} + a_1 x^{n-2} + \ldots + a_{n-1}) \in I \cap A$. Since $I \cap A = \{0\}$, we obtain $a_n = 0$. Thus I has no nonzero elements.

(iii) Let $\mathcal{P}_0 = \mathcal{P}_1 \cap A$. Then we may identify $\bar{A} = A/\mathcal{P}_0$ with a subring of $\bar{B} = B/\mathcal{P}_1$ with respect to the natural homomorphism $A/\mathcal{P}_0 \to B/\mathcal{P}_1$. Let $\mathcal{P}_2'$ be the image of $\mathcal{P}_2$ in $\bar{B}$. Then $\mathcal{P}_2' \cap \bar{A} = \{0\}$. Obviously, $\bar{B}$ is integral over A and has no zero divisors. Thus we may apply (ii) to obtain $\mathcal{P}_2' = \{0\}$ hence $\mathcal{P}_2 = \mathcal{P}_1$.

(iv) Obviously the map $A_S \to B_S$ is injective, so we may identify A_S with a subring of B_S. If $b/s \in B_S$ and b satisfies a monic equation $b^n + a_1 b^{n-1} + \ldots + a_n = 0, a_i \in A$, then b/s satisfies the monic equation $(b/s)^n + (a_1/s)(b/s)^{n-1} + \ldots + (a_n/s^n) = 0$ with coefficients in A_S.

(v) If $IB = B$, then we can write $1 = a_1 b_1 + \ldots + a_n b_n$ for some $b_i \in B, a_i \in I$. Let $x_1, \ldots, x_m$ be a set of generators of B considered as A-module. Multiplying both sides of the previous equality x_i and expressing $x_i b_j$ as a linear combination of the x_i's with coefficients in A we can write

$$x_i = \sum_{j=1}^{n} a_{ij} x_j, i = 1, \ldots, n \quad \text{for some } a_{ij} \in I.$$

Thus, the vector $\mathbf{x} = (x_1, \ldots, x_n) \in B^n$ is a solution of a system of linear equations $(M - I_n)\mathbf{x} = 0$ where $M = (a_{ij})$. Let $D = \det(M - I_k)$. As in the proof of Lemma 1, we get $D^2 = 0$. Clearly

$$D = \det(M - I_k) = (-1)^k + c_1(-1)^{k-1} + \ldots + c_k$$

where c_i, being polynomials in a_{ij}, belong to I. Squaring the previous equality, we express 1 as a linear combination of the products $c_i c_j$. This shows that $1 \in I$. This contradiction proves the assertion.

(vi) We know that the ideal

$$\mathcal{P}' = \mathcal{P}A_{\mathcal{P}} = \{a/b \in A_{\mathcal{P}}, a \in \mathcal{P}\}$$

is maximal in $A_{\mathcal{P}}$. In fact, any element from its complement is obviously invertible. Let $B' = B_S$, where $S = A \setminus \mathcal{P}$. Then B' is integral over $A' = A_{\mathcal{P}}$ and, by (v), the ideal $\mathcal{P}'B'$ is proper. Let m be a maximal ideal containing it. Then $m \cap A' = \mathcal{P}'$ because it contains the maximal ideal $\mathcal{P}'$. Now it is easy to see that the pre-image of m under the canonical homomorphism $B \to B_S$ is a prime ideal of B cutting out the ideal $\mathcal{P}$ in A.

Definition. A regular map $f : X \to Y$ of affine algebraic k-sets is said to be *finite* if $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective and $\mathcal{O}(X)$ is integral over $f^*(\mathcal{O}(Y))$. A regular map $f : X \to Y$ of quasi-projective algebraic k-sets is said to be finite if for every point $y \in Y$ there exists an affine open neighborhood V of y such that $f^{-1}(V)$ is affine and the restriction map $f^{-1}(V) \to V$ is finite.

Note that if $f : X \to Y$ is a map of affine sets, then $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective if and only if $f(X)$ is dense in Y. Indeed, if $f^*(\phi) = 0$ then $f(X) \subset \{y \in Y : \phi(y) = 0\}$ which is a closed subset. Conversely, if $f(X)$ is contained in a closed subset Z of Y then for every function $\phi \in I(Y)$ we have $f^*(\phi) = 0$.

Examples. 1. Let $X = \{(x, y) \in K^2 : y = x^2\} \subset A^2(K)$ and $Y = A^1(K)$. Consider the projection map $f : X \to Y,\ (x, y) \mapsto y$. Then f is finite. Indeed, $\mathcal{O}(X) \cong k[Z_1, Z_2]/(Z_2 - Z_1^2), \mathcal{O}(Y) \cong k[Z_2]$ and f^* is the composition of the natural inclusion $k[Z_2] \to k[Z_1, Z_2]$ and the natural homomorphism $k[Z_1, Z_2] \to k[Z_1, Z_2]/(Z_2 - Z_1^2)$. Obviously it is injective. Let z_1, z_2 be the images of Z_1 and Z_2 in the factor ring $k[Z_1, Z_2]/(Z_2 - Z_1^2)$. Then $\mathcal{O}(X)$ is generated over $f^*(\mathcal{O}(Y))$ by one element z_1.

The latter satisfies a monic equation: $z_1^2 - f^*(Z_2) = 0$ with coefficients in $f^*(\mathcal{O}(Y))$. As we saw in the proof of Lemma 1, this implies that $\mathcal{O}(X)$ is a finitely generated $f^*(\mathcal{O}(Y))$-module and hence $\mathcal{O}(X)$ is integral over $f^*(\mathcal{O}(Y))$. Therefore f is a finite map.
2. Let x_0 be a projective subspace of $\mathbb{P}_k^n(K)$ of dimension 0, i.e., a point $(a_0, \ldots, a_n)$ with coordinates in k. Let X be a projective algebraic k-set in $\mathbb{P}_k^n(K)$ with $x_0 \notin X$ and let $f = pr_{x_0} : X \to \mathbb{P}_k^{n-1}(K)$ be the projection map. We know that $Y = f(X)$ is a projective set. Let us see that $f : X \to Y$ is finite. First, by a variable change, we may assume that x_0 is given by a system of equations $T_0 = \ldots = T_{n-1} = 0$ where $T_0, \ldots, T_n$ are homogeneous coordinates. Then f is given by $(x_0, \ldots, x_n) \mapsto (x_0, \ldots, x_{n-1})$. We may assume that $y \in Y$ lies in the open subset $V = Y \cap \mathbb{P}_k^{n-1}(K)_0$ where $x_0 \neq 0$. Its preimage $U = f^{-1}(V) = X \cap \mathbb{P}_k^n(K)_0$. Since f is surjective $f^* : \mathcal{O}(V) \to \mathcal{O}(U)$ is injective. Let us show that $\mathcal{O}(U)$ is integral over $f^*(\mathcal{O}(V))$. Let $I_0 \subset k[Z_1, \ldots, Z_n]$ be the ideal of $X \cap \mathbb{P}_k^n(k)_0$, where $Z_i = T_i/T_0, i = 1, \ldots, n$. Then V is given by some ideal J_0 in $k[Z_1, \ldots, Z_{n-1}]$, and the homomorphism f^* is induced by the natural inclusion $k[Z_1, \ldots, Z_{n-1}] \subset k[Z_1, \ldots, Z_n]$. Since $\mathcal{O}(U)$ is generated over k by the cosets z_j of Z_j modulo the ideal I_0 we may take z_n to be a generator of $\mathcal{O}(U)$ over $f^*(\mathcal{O}(V))$. Let $\{F_s(T) = 0\}_{s \in S}$ be the equations defining X. Since $x_0 \notin X$, the ideal generated by the polynomials F_s and $T_i, i \leq n-1$, must contain $k[T]_d$ for some $d \geq 0$. Thus we can write

$$T_n^d = \sum_{s \in S} A_s F_s + \sum_{i=0}^{n-1} B_i T_i$$

for some homogeneous polynomials $A_s, B_i \in k[T_0, \ldots, T_n]$. Obviously the degree of each B_i in T_n is strictly less than d. Dividing by some power of T_0, and reducing modulo I_0 we obtain that z_n satisfies a monic equation with coefficients in $f^*(\mathcal{O}(V))$. This implies that $\mathcal{O}(V)$ is a finitely generated $f^*(\mathcal{O}(U))$-module, hence is integral over $f^*(\mathcal{O}(U))$. By definition, X is finite over Y.
3. Let $A = k[Z_1]$ and $B = A[Z_1, Z_2]/Z_1 Z_2 - 1$. Consider $\phi : A \to B$ defined by the natural inclusion $k[Z_1] \subset k[Z_1, Z_2]$. This corresponds to the projection of the "hyperbola' to the x-axis. It is clearly not surjective. Thus property (v) is not satisfied (take $I = (Z_1)$). So, the corresponding map of affine sets is not finite (although all fibres are finite sets).

Lemma 3. *Let X be a quasi-projective algebraic k-set, $\phi \in \mathcal{O}(X)$ and $D(\phi) = \{x \in X : \phi(x) \neq 0\}$. Then*

$$\mathcal{O}(D(\phi)) \cong \mathcal{O}(X)_\phi.$$

Proof. We know that this is true for an affine set X (see Lecture 9). Let X be any quasi-projective algebraic k-set. Obviously, for any open affine set U we have $D(\phi|U) = U \cap D(\phi)$. This shows that $\phi|U \cap D(\phi)$ is invertible, and by taking an affine open cover of $D(\phi)$, we conclude that $\phi|D(\phi)$ is invertible. By the universal property of localization, this defines a homomorphism $\alpha : \mathcal{O}(X)_\phi \to \mathcal{O}(D(\phi))$. The restriction homomorphism $\mathcal{O}(X) \to \mathcal{O}(U)$ induces the homomorphism $\alpha_U : \mathcal{O}(U)_{\phi|U} \to \mathcal{O}(D(\phi) \cap U)$. By taking an affine open cover of $X = \cup_i U_i$, we obtain that all α_{U_i} are isomorphisms. Since every element of $\mathcal{O}(X)$ is uniquely determined by its restrictions to each U_i, and any element of $\mathcal{O}(D(\phi))$ is determined by its restriction to each $D(\phi) \cap U_i$, we obtain that α is an isomorphism.

Lemma 4. *Let X and Y be two quasi-projective algebraic k-sets. Assume that Y is affine. Then the natural map*

$$Map_{reg}(X, Y) \to Hom_{k-alg}(\mathcal{O}(Y), \mathcal{O}(X)), \quad f \to f^*,$$

is bijective.

Proof. We know this already if X and Y are both affine. Let U be an affine open subset of X. By restriction of maps (resp. functions), we obtain a commutative diagram:

$$\begin{array}{ccc} Map_{reg}(X,Y) & \to & Hom_{k-alg}(\mathcal{O}(Y),\mathcal{O}(X)) \\ \downarrow & & \downarrow \\ Map_{reg}(U,Y) & \to & Hom_{k-alg}(\mathcal{O}(Y),\mathcal{O}(U)). \end{array}$$

Here the bottom horizontal arrow is a bijection. Thus we can inverse the upper horizontal arrow as follows. Pick up an open affine cover $\{U_i\}_{i\in I}$ of X. Take a homomorphism $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$, its image in $Hom_{k-alg}(\mathcal{O}(Y),\mathcal{O}(U_i))$ is the composition with the restriction map $\mathcal{O}(X) \to \mathcal{O}(U_i)$. It defines a regular map $U_i \to Y$. Since a regular map is defined on its open cover, we can reconstruct a "global" map $X \to Y$. It is easy to see that this is the needed inverse.

Lemma 5. *Let X be a quasi-prjective algebraic k-set. Then X is affine if and only if $\mathcal{O}(X)$ is a finitely generated k- algebra which contains a finite set of elements ϕ_i which generate the unit ideal and such that each $D(\phi_i)$ is affine.*

Proof. The part "only if" is obvious. Let $\phi_1,\dots,\phi_n \in \mathcal{O}(X)$ which generate the unit ideal. Then $X = \cup_i D(\phi_i)$. Let $k[Z_1,\dots,Z_n] \to \mathcal{O}(X)$ be a surjective homomorphism of k-algebras and I be its kernel. The set of zeroes of I in $\mathbb{A}^n(K)$ is an affine algebraic set X' with $\mathcal{O}(X') \cong \mathcal{O}(X)$. Let $f : X \to X'$ be the regular map corresponding by Lemma 4 to the previous isomorphism. Its restriction to $D(\phi_i)$ is an isomorphism for each i (here we use that $D(\phi_i)$ is affine). Hence f is an isomorphism.

Proposition 2. *Let $f : X \to Y$ be a finite regular map of quasi-projective algebraic k-sets. The following assertions are true:*

(i) for every affine open subset U of Y, $f^{-1}(U)$ is affine and $f : f^{-1}(U) \to U$ is finite;

(ii) if Z is a locally closed subset of Y, then $f : f^{-1}(Z) \to Z$ is finite;

(iii) if $f : X \to Y$ and $g : Y \to Z$ are finite regular maps, then $g \circ f : X \to Z$ is a finite regular map.

Proof. (i) Obviously we may assume that $Y = U$ is affine. For any $y \in Y$, there exists an open affine neighborhood V of y such that $f : f^{-1}(V) \to V$ is a finite map of affine k-sets. Let $\phi \in \mathcal{O}(Y)$, then $D(\phi) \subset V$ is affine and $f^{-1}(D(\phi)) = D(f^*(\phi)) \subset f^{-1}(V)$ is affine. Moreover the map $f^{-1}(D(\phi)) \to D(\phi)$ is finite (this follows from Lemma 2(iv) and Lemma 3). Thus we may assume that Y is covered by affine open sets of the form $D(\phi)$ such that $f^{-1}(D(\phi))$ is affine and the restriction of the map f to $f^{-1}(D(\phi))$ is finite.

Now let

$$Y = \cup_i V_i, V_i = D(\phi_i), \phi_i \in \mathcal{O}(Y),$$

$$X = \cup_i U_i, U_i = f^{-1}(V_i) = D(f^*(\phi_i)),$$

$$f_i = f|U_i : U_i \to V_i \quad \text{is a finite map of affine sets.}$$

By Lemma 1, $\mathcal{O}(U_i)$ is a finitely generated $\mathcal{O}(V_i)$-module. Let $\{\omega_{ij}\}_{j=1,\dots,n(i)}$ be a set of generators of this module. Since $\omega_{ij} = a/f^*(\phi_i)^n$ for some $a \in \mathcal{O}(X)$ and $n \geq 0$, and $f^*(\phi_i)$ is invertible in $\mathcal{O}(U_i)$, we may assume that $\omega_{ij} \in \mathcal{O}(X)$. For every $\phi \in \mathcal{O}(X)$ we may write

$$\phi|U_i = \sum_{i=0}^{n(i)} (b_j/f^*(\phi_i)^{n(i)})\omega_{ij}$$

for some $b_j/f^*(\phi_i)^{n(i)} \in \mathcal{O}(U_i)$. Since $\cap_i(Y \setminus D(\phi_i)) = \cap_i V(\phi_i) = \cap_i V(\phi_i^{n(i)}) = \emptyset$, the ideal in $\mathcal{O}(Y)$ generated by the ϕ_i's contains 1. Thus $1 = \sum_i h_i \phi_i^{n(i)}$ for some $h_i \in \mathcal{O}(Y)$, hence

$$1 = \sum_i f^*(h_i) f^*(\phi_i)^{n(i)}$$

and

$$\phi|U_i = \sum_i (\phi|U_i) f^*(h_i) f^*(\phi_i)^{n(i)} = (\sum_i f^*(h_i) b_j \omega_{ij})|U_i.$$

This shows that $\phi = \sum_{ij} c_{ij}\omega_{ij}$ for some $c_{ij} \in \mathcal{O}(X)$, that is, $\{\omega_{ij}\}$ is a generating set of the $f^*(\mathcal{O}(Y))$-module $\mathcal{O}(X)$. In particular, $\mathcal{O}(X)$ is integral over $f^*(\mathcal{O}(Y))$ and $\mathcal{O}(X)$ is an algebra of finite type over k. Since the elements $f^*(\phi_i)^{n(i)}$ generate the unit ideal in $\mathcal{O}(X)$, applying by Lemma 5, we obtain that X is an affine set .

(ii) Let Z be a locally closed subset of Y. Then $Z = U \cap Z'$, where U is open and Z' is closed in Y. Taking an affine open cover of U and applying (i), we may assume that $Y = U$ is affine and Z is a closed subset of Y. Then $f^{-1}(Z)$ is closed in X. Since X is affine $f^{-1}(Z)$ is affine. The restriction of f to $f^{-1}(Z)$ is a regular map $\bar{f} : f^{-1}(Z) \to Z$ of affine sets corresponding to the homomorphism of the factor-algebras $\bar{f}^* : \mathcal{O}(Y)/I(Z) \to \mathcal{O}(X)/I(f^{-1}(Z))$. Since $I(f^{-1}(Z)) = f^*(I(Z))\mathcal{O}(X)$, $\bar{f}^*$ is injective. By Lemma 2, the corresponding extension of algebras is integral. Thus $\bar{f}$ is finite.

(iii) Applying (i), we reduce the proof to the case where X, Y and Z are affine. By Lemma 1, $\mathcal{O}(X)$ is finite over $f^*(\mathcal{O}(Y))$ and $f^*(\mathcal{O}(Y))$ is finite over $f^*(g^*(\mathcal{O}(Z))) = (g \circ f)^*(\mathcal{O}(Z))$. Thus $\mathcal{O}(X)$ is finite over $(g \circ f)^*(\mathcal{O}(Z))$, hence integral over $(g \circ f)^*(\mathcal{O}(Z))$.

Proposition 3. *Let $f : X \to Y$ be a finite regular map of algebraic k-sets. Then*
(i) f is surjective;
(ii) for any $y \in Y$, the fibre $f^{-1}(y)$ is a finite set.

Proof. Clearly, we may assume that X and Y are affine, $B = \mathcal{O}(X)$ is integral over $A = \mathcal{O}(Y)$ and $\phi = f^*$ is injective. A point $y \in Y$ defines a homomorphism $ev_y : A \to K$ whose kernel is a prime ideal $\mathfrak{p}$. A point $x \in f^{-1}(y)$ corresponds to a homomorphism $ev_x : B \to K$ of k-algebras such that its composition with ϕ is equal to ev_y. By Lemma 2 (vi), there exists a prime ideal $\mathcal{P}$ in B such that $\phi^{-1}(\mathcal{P}) = \mathfrak{p}$. Let $Q(B/\mathcal{P})$ be the field of fractions of the quotient ring $B/\mathcal{P}$ and $Q(A/\mathfrak{p})$ be the field of fractions of the ring $A/\mathfrak{p}$. Since B is integral over A, the homomorphism ϕ defines an algebraic extension $Q(B/\mathcal{P})/Q(A/\mathfrak{p})$ (Lemma 2 (iv)). Since K is algebraically closed, there exists a homomorphism $Q(B/\mathcal{P}) \to K$ which extends the natural homomorphism $Q(A/\mathfrak{p}) \to K$ defined by the injective homomorphism $A/\mathfrak{p} \to K$ induced by ev_y. The composition of the restriction of the homomorphism $Q(B/\mathcal{P}) \to K$ to $B/\mathcal{P}$ and the factor map $B \to B/\mathcal{P}$ defines a point $x \in f^{-1}(y)$. This proves the surjectivity of f.

Note that the field extension $Q(B/\mathcal{P})/Q(A/\mathfrak{p})$ is finite (since it is algebraic and $Q(B/\mathcal{P})$ is a finitely generated algebra over $Q(A/\mathfrak{p})$. It is known from the theory of field extensions that the number of homomorphisms $Q(B/\mathcal{P}) \to K$ extending the homomorphism $A/\mathfrak{p} \to K$ is equal to the separable degree $[Q(B/\mathcal{P}) : Q(A/\mathfrak{p})]_s$ of the extension $Q(B/\mathcal{P})/Q(A/frakp)$. It follows from the previous arguments that the number of points in $f^{-1}(y)$ is equal to the sum

$$\sum_{\mathcal{P}:\phi^{-1}(P)=\mathfrak{p}} [Q(B/\mathcal{P}) : Q(A/\mathfrak{p})]_s.$$

So it suffices to show that the number of prime ideals $\mathcal{P} \subset B$ such that $\phi^{-1}(\mathcal{P}) = \mathfrak{p}$ is finite. It follows from Lemma 2 (iii) that the set of such prime ideals is equal to the set of irreducible components of the closed subset of X defined by the proper ideal $\mathfrak{p}B$. We know that the number of irreducible components of an affine k-set is finite. This proves the second assertion.

Theorem. *Let X be a projective (resp. affine) irreducible algebraic k-set. Then there exists a finite regular map $f : X \to \mathbb{P}^n_k(K)$ (resp. $\mathbb{A}^n_k(K)$).*

Proof. Assume first that X is projective. Let X be a closed subset of some $\mathbb{P}^r_k(K)$ for some r as a closed subset. If $X = \mathbb{P}^r_k(K)$, we take for f the identity map. Let $x \in \mathbb{P}^r_k(K) \setminus X$ and $p_x : X \to \mathbb{P}^{r-1}_k(K)$ be the linear projection from the point x. We know from the previous examples that $p_x : X \to p_x(X)$ is a finite map. If $p_x(X) = \mathbb{P}^{r-1}_k(K)$, we are done. Otherwise, we take a point outside $p_x(X)$ and project from it. Finally, we obtain a finite map (composition of finite maps) $X \to \mathbb{P}^n_k(K)$ for some n.

Assume that X is affine. Then, we replace X by an isomorphic set lying as a closed subset of $\mathbb{P}^r_k(K)_0$ of some $\mathbb{P}^r_k(K)$. Let $\bar{X}$ be the closure of X in $\mathbb{P}^r_k(K)$. Projecting from a point $x \in \mathbb{P}^r_k(K) \setminus (\bar{X} \cup \mathbb{P}^r_k(K)_0)$, we define a finite map $\bar{X} \to \mathbb{P}^{r-1}_k(K)$. Since one of the equations defining x can be taken to be $T_0 = 0$, the image of $\mathbb{P}^r_k(K)_0$ is contained in $\mathbb{P}^{r-1}_k(K)_0$. Thus the image of X is contained in $\mathbb{P}^{r-1}_k(K)_0 \cong \mathbb{A}^{r-1}_k(K)$. Continuing as in the projective case, we prove the theorem.

The next corollary is called the Noether Normalization theorem. Together with the two Hilbert's theorems (Basis and Nullstellensatz) these three theorems were known as "the three whales of algebraic geometry."

Corollary. *Let A be a finitely generated algebra over a field k. Then A is isomorphic to an integral extension of the polynomial algebra $k[Z_1, \dots, Z_n]$.*

Proof. Find an affine algebraic set X with $\mathcal{O}(X) \cong A$ and apply the previous theorem.

Problems.

1. Decide whether the following maps $f : X \to Y$ are finite:
(a) $Y = V(Z_1^2 - Z_2^3)$ be the cuspidal cubic, $X = \mathbb{A}^1$, f is defined by the formula $x \to (x^3, x^2)$;
(b) $X = Y = \mathbb{A}^2$, f is defined by the formula $(x, y) \to (xy, y)$.
2. Let $f : X \to Y$ be a finite map. Show that the image of any closed subset of X is closed in Y.
3. Let $f : X \to Y$ and $g : X' \to Y'$ be two finite regular maps. Prove that the Cartesian product map $f \times g : X \times X' \to Y \times Y'$ is a finite regular map.
4. Give an example of a surjective regular map with finite fibres which is not finite.
5. Let A be an integral domain, Q be its field of fractions. The integral closure $\bar{A}$ of A in Q is called the *normalization* of A. A *normal ring* is a ring A such that $A = \bar{A}$.
(a) Prove that $\bar{A}$ is a normal ring;
(b) Prove that the normalization of the ring $k[Z_1, Z_2]/(Z_1^2 - Z_2^2(Z_2 + 1))$ is isomorphic to $k[T]$;
(c) Show that $k[Z_1, Z_2, Z_3]/(Z_1 Z_2 - Z_3^2)$ is a normal ring.
6. Let $B = k[Z_1, Z_2]/(Z_1 Z_2^2 + Z_2 + 1)$. Find a subring A of B isomorphic to a ring of polynomials such that B is finite over A.

Lecture 11. DIMENSION

In this lecture we give a definition of the dimension of an algebraic (= quasi-projective algebraic) k-set. Recall that the dimension of a linear space L can be defined by :

$$\dim L = \sup\{r : \exists \text{ a strictly decreasing chain of linear subspaces } L_0 \supset L_1 \supset \ldots \supset L_r\}.$$

The dimension of algebraic sets is defined in a very similar way:

Definition. Let X be a non-empty topological space. Its *Krull dimension* is defined to be equal to

$$\dim X = \sup\{r : \exists \text{ a chain } Z_0 \supset Z_1 \supset \ldots \supset Z_r \neq \emptyset \text{ of closed irreducible subsets of } X\}.$$

By definition the dimension of the empty set is equal to $-\infty$.

The dimension of an algebraic k-set X is the Krull dimension of the corresponding topological space.

Example. $\dim \mathbb{A}^1_k(K) = 1$. Indeed, the only proper closed irreducible subset is a finite set defined by an irreducible polynomial with coefficients in k. It does not contain any proper closed irreducible subsets.

Propositon 1 (General properties of dimension). *Let X be a topological space. Then*

(i) $\dim X = 0$ *if X is a non-empty Hausdorff space;*

(ii) $\dim X = \sup\{\dim X_i, i \in I\}$, *where $X_i, i \in I$, are irreducible components of X;*

(iii) $\dim X \geq \dim Y$ *if $Y \subset X$, the strict inequality takes place if none of the irreducible components of the closure of Y is an irreducible component of X;*

Proof. (i) In a non-empty Hausdorff space a point is the only closed irreducible subset.

(ii) Let $Z_0 \supset Z_1 \supset \ldots \supset Z_r$ be a strictly decreasing chain of irreducible closed subsets of X. Then $Z_0 = \cup_{i \in I}(Z_0 \cap X_i)$ is the union of closed subsets $Z_0 \cap X_i$. Since Z_0 is irreducible, $Z_0 \cap X_i = Z_0$ for some X_i, i.e., $Z_0 \subset X_i$. Thus the above chain is a chain of irreducible closed subsets in X_i and $r \leq \dim X_i$.

(iii) Let $Z_0 \supset Z_1 \supset \ldots \supset Z_r$ be a strictly decreasing chain of irreducible closed subsets of Y, then the chain of the closures $\bar{Z}_i$ of Z_i in X of these sets is a strictly decreasing chain of irreducible closed subsets of X. As we saw in the proof of (ii) all $\bar{Z}_i$ are contained in some irreducible component X_i of X. If this component is a not an irreducible component of the closure of Y, then $X_i \supset \bar{Z}_0$ and we can add it to the chain to obtain that $\dim X > \dim Y$.

Proposition 2. *An algebraic k-set X is of dimension 0 if and only if it is a finite set.*

Proof. By Proposition 1(ii) we may assume that X is irreducible. Suppose $\dim X = 0$. Take a point $x \in X$ and consider its closure Z in the Zariski k-topology. It is an irreducible closed subset which does not contain proper closed subsets (if it does, we find a proper closed irreducible subset of Z). Since $\dim X = 0$, we get $Z = X$. We want to show that X is finite. By taking an affine open cover, we may assume that X is affine. Now $\mathcal{O}(X)$ is isomorphic to a quotient of polynomial algebra $k[Z_1, \ldots, Z_n]/I$. Since X does not contain proper closed subsets I must be a maximal ideal. As we saw in the proof of the Nullstellensatz this implies that $\mathcal{O}(X)$ is a finite field extension of k. Every point of X is defined by a homomorphism $\mathcal{O}(X) \to K$. Since K is algebraically closed there is only a finite number of homomorphisms $\mathcal{O}(X) \to K$. Thus X is a finite set (of cardinality equal to the separable degree of the extension $\mathcal{O}(X)/k$).

Conversely, if X is a finite irreducible set, then X is a finite union of the closures of its points. By irreduciblity it is equal to the closure of any of its points. Clearly it does not contain proper closed subsets, hence $\dim X = 0$.

Definition. For every commutative ring A its *Krull dimension* is defined by

$$\dim A = \sup\{r : \exists \text{strictly increasing chain } \mathcal{P}_0 \subset \ldots \subset \mathcal{P}_k \text{ of proper prime ideals in } A\}$$

Proposition 3. *Let X be an affine algebraic k-set and $A = \mathcal{O}(X)$ be the k-algebra of regular functions on X. Then*

$$\dim X = \dim A.$$

Proof. Obviously follows from the existence of the natural corresponence between closed irreducible subsets of X and prime ideals in $\mathcal{O}(X) \cong A$.

Recall that a finite subset $\{x_1, \ldots, x_k\}$ of a commutative algebra A over a field k is said to be algebraically dependent (resp. independent) over k if there exists (resp. does not exist) a non-zero polynomial $F(Z_1, \ldots, Z_k) \in k[Z_1, \ldots, Z_k]$ such that $F(x_1, \ldots, x_k) = 0$. The algebraic dimension of A over k is the maximal number of algebraically independent elements over k in A if it is defined and ∞ otherwise. We will denote it by $\text{alg.dim}_k(A)$.

Lemma 1. *Let A be a k-algebra without zero divisors and $Q(A)$ be the field of fractions of A. Then*

(i) $\text{alg.dim}_k Q(A) = \text{alg.dim}_k(A)$;

(ii) $\text{alg.dim}_k(A) \geq \dim A$.

Proof. (i) Obviously, $\text{alg.dim}_k(A) \leq \text{alg.dim}_k(Q(A))$. If $x_1, \ldots, x_r$ are algebraically independent elements in $Q(A)$ we can write them in the form a_i/s, where $a_i \in A, i = 1, \ldots, r$, and $b \in A$. Consider the subfield Q' of $Q(A)$ generated by $a_1, \ldots, a_r, s$. Since Q' contains $x_1, \ldots, x_r, s$, $\text{alg.dim}_k Q' \geq r$. If $a_1, \ldots, a_r$ are algebraically dependent, then Q' is an algebraic extension of the subfield Q'' generated by s and $a_1, \ldots, a_r$ with some a_i, say a_r, omitted. Since $\text{alg.dim}_k Q' = \text{alg.dim}_k Q''$, we find r algebraically independent elements $a_1, \ldots, a_{r-1}, s$ in A. This shows that $\text{alg.dim}_k Q(A) \leq \text{alg.dim}_k A$.

(ii) Let $\mathcal{P}$ be a prime ideal in A. Let $\bar{x}_1, \ldots, \bar{x}_r$ be algebraically independent elements over k in the factor ring $A/\mathcal{P}$ and let $x_1, \ldots, x_r$ be their representatives in A. We claim that for every nonzero $x \in \mathcal{P}$ the set $x_1, \ldots, x_r, x$ is algebraically independent over k. This shows that

alg.dim$_k A >$ alg.dim$_k A/\mathcal{P}$ and clearly proves the statement. Assume that $x_1, \ldots, x_r, x$ are algebraically dependent. Then $F(x_1, \ldots, x_r, x) = 0$ for some polynomial $F \in k[Z_1, \ldots, Z_{n+1}] \setminus \{0\}$. We can write F as a polynomial in Z_{n+1} with coefficients in $k[Z_1, \ldots, Z_n]$. Then

$$F(x_1, \ldots, x_r, x) = a_0(x_1, \ldots, x_r)x^n + \ldots + a_{n-1}(x_1, \ldots, x_r)x + a_n(x_1, \ldots, x_r) = 0,$$

where $a_i \in k[Z_1, \ldots, Z_n]$. Cancelling by x, if needed, we may assume that $a_n \neq 0$ (here we use that A does not have zero divisors). Passing to the factor ring $A/\mathcal{P}$, we obtain the equality

$$F(\bar{x}_1, \ldots, \bar{x}_r, \bar{x}) = a_0(\bar{x}_1, \ldots, \bar{x}_r)\bar{x}^n + \ldots + a_{n-1}(\bar{x}_1, \ldots, \bar{x}_r)\bar{x} + a_n(\bar{x}_1, \ldots, \bar{x}_r) = a_n(\bar{x}_1, \ldots, \bar{x}_r) = 0,$$

which shows that $\bar{x}_1, \ldots, \bar{x}_r$ are algebraically dependent. This contradiction proves the claim.

Proposition 4.

$$\dim \mathbb{A}_k^n(K) = n.$$

Proof. By Proposition 3, we have to check that dim $k[Z_1, \ldots, Z_n] = n$. Obviously,

$$(0) \subset (Z_1) \subset (Z_1, Z_2) \subset \ldots \subset (Z_1, \ldots, Z_n)$$

is a strictly increasing chain of proper prime ideals of $k[Z_1, \ldots, Z_n]$. This shows that

$$\dim k[Z_1, \ldots, Z_n] \geq n.$$

By Lemma 1,

$$\text{alg.dim}_k k[Z_1, \ldots, Z_n] = \text{alg.dim}_k k(Z_1, \ldots, Z_n) = n \geq \dim k[Z_1, \ldots, Z_n] \geq n.$$

This proves the assertion.

Lemma 2. *Let B a k-algebra which is integral over its subalgebra A. Then*

$$\dim A = \dim B.$$

Proof. For every strictly increasing chain of proper prime ideals $\mathcal{P}_0 \subset \ldots \subset \mathcal{P}_k$ in B, we have a strictly increasing chain $\mathcal{P}_0 \cap A \subset \ldots \subset \mathcal{P}_k \cap A$ of proper prime ideals in A (Lemma 2 (iii) from Lecture 10). This shows that dim $B \leq$ dim A.

Now let $\mathcal{P}_0 \cap A \subset \ldots \subset \mathcal{P}_k \cap A$ be a strictly increasing chain of prime ideals in A. By Lemma 2 from Lecture 10, we can find a prime ideal $\mathcal{Q}_0$ in B with $\mathcal{Q}_0 \cap A = \mathcal{P}_0$. Let $\bar{A} = A/\mathcal{P}_0, \bar{B} = B/\mathcal{Q}_0$, the canonical injective homomorphism $\bar{A} \to \bar{B}$ is an integral extension. Applying the Lemma again we find a prime ideal $\bar{\mathcal{Q}}_1$ in $\bar{B}$ which cuts out in $\bar{A}$ the image of $\mathcal{P}_1$. Lifting $\bar{\mathcal{Q}}_1$ to a prime ideal $\mathcal{Q}_1$ in B we find $\mathcal{Q}_1 \supset \mathcal{Q}_0$ and $\mathcal{Q}_1 \cap A = \mathcal{P}_1$. Continuing in this way we find a strictly increasing chain of prime ideals $\mathcal{Q}_0 \supset \mathcal{Q}_1 \supset \ldots \supset \mathcal{Q}_k$ in B. This checks that dim $B \geq$ dim A and proves the assertion.

Theorem 1. *Let A be a finitely generated k-algebra without zero divisors. Then*

$$\dim A = \text{alg.dim}_k A = \text{alg.dim}_k Q(A).$$

In particular, if X is an irreducible affine algebraic k-set and $R(X)$ is its field of rational functions, then

$$\dim X = \text{alg.dim}_k \mathcal{O}(X) = \text{alg.dim}_k R(X).$$

Proof. By Noether's Normalization Theorem from Lecture 10, A is integral over its subalgebra isomorphic to $k[Z_1, \ldots, Z_n]$. Passing to the localization with respect to the multiplicative set $S = k[Z_1, \ldots, Z_n] \setminus \{0\}$, we obtain an integral extension $k(Z_1, \ldots, Z_n) \to A_S$. Since $k(Z_1, \ldots, Z_n)$ is a field, and A is a domain, A_S must be a field equal to its field of fractions $Q(A)$. The field extension $k(Z_1, \ldots, Z_n) \to Q(A)$ is algebraic. Applying Lemmas 1 and 2 we get

$$\text{alg.dim}_k A \geq \dim A = \dim k[Z_1, \ldots, Z_n] = \text{alg.dim}_k k(Z_1, \ldots, Z_n) = \text{alg.dim}_k Q(A) = \text{alg.dim}_k A.$$

This proves the assertion.

So we see that for irreducible affine algebraic sets the following equalities hold:

$$\dim X = \dim \mathcal{O}(X) = \text{alg.dim}_k \mathcal{O}(X) = \text{alg.dim}_k R(X) = n$$

where n is defined by the existence of a finite map $X \to \mathbb{A}^n_k(K)$.

Note that, since algebraic dimension does not change under algebraic extensions, we obtain

Corollary. *Let X be an affine algebraic k-set and let X' be the same set considered as an algebraic k'-set for some algebraic extension k' of k. Then*

$$\dim X = \dim X'.$$

To extend the previous results to arbitrary algebraic sets X, we will show that for every dense open affine subset $U \subset X$

$$\dim U = \dim X.$$

This will follow from the following:

Theorem 2 (Geometric Krull's Hauptidealsatz). *Let X be an affine irreducible algebraic k-set of dimension n and let ϕ be a non-invertible and non-zero element of $\mathcal{O}(X)$. Then every irreducible component of the set $V(\phi)$ of zeroes of ϕ is of dimension $n-1$.*

To prove this theorem we shall need two lemmas.

Lemma 3. *Let B be a domain which is integral over $A = k[Z_1, \ldots, Z_r]$, and let x and y be coprime elements of A. Assume that $x|uy$ for some $u \in B$. Then $x|u^j$ for some j.*

Proof. Let $uy = xz$ for some $z \in B$. Since z is integral over $Q(A)$ its minimal monic polyomial over $Q(A)$ has coefficients from A. This follows from the Gauss Lemma (if $F(T) \in Q(A)[T]$ divides a monic polynomial $G(T) \in A[T]$ then $F(T) \in A[T]$). Let

$$F(T) = T^n + a_1 T^{n-1} + \ldots + a_n = 0, a_i \in A,$$

be a minimal monic polynomial of z. Plugging $z = uy/x$ into the equation, we obtain that u satisfies a monic equation:

$$F(T)' = T^n + (a_1 x/y)T^{n-1} + \ldots + (a_n x^n/y^n) = 0$$

with coefficients in the field $Q(A)$. If u satisfies an equation of smaller degree over $Q(A)$, after plugging in $u = xz/y$, we find that z satisfies an equation of degree smaller than n. This is impossible by the choice of $F(T)$. Thus $F(T)'$ is a minimal polynomial of u. Since u is integral over A, the coefficients of $F(T)'$ belong to A. Therefore, $y^i | a_i x^i$, and, since x and y are coprime, $y^i | a_i$. This implies that $u^n + xt = 0$ for some $t \in A$, and therefore $x|u^n$.

Lemma 4. *Assume k is infinite. Let X be an irreducible affine k-set, and let ϕ be a non-zero and not invertible element in $\mathcal{O}(X)$. There exist $\phi_1, \ldots, \phi_n \in \mathcal{O}(X)$ such that the map $X \to \mathbb{A}_k^{n+1}(K)$ defined by the formula $x \to (\phi(x), \phi_1(x), \ldots, \phi_n(x))$ is a regular finite map.*

Proof. Replacing X by an isomorphic set, we may assume that X is a closed subset of some $\mathbb{P}_k^m(K)_0$, $\phi = F(T_0, \ldots, T_m)/T_0^r$ for some homogeneous polynomial $F(T)$ of degree $r > 0$. Since ϕ is not invertible and $\mathcal{O}(X)$ is a domain, (ϕ) is a proper ideal with $\mathrm{rad}(\phi) \neq \{0\}$. Thus $V(\phi)$ is a proper closed subset of X. Let $\bar{X}$ be the closure of X in $\mathbb{P}_k^m(K)$. Obviously every irreducible component of the closure $V(F)$ of $V(\phi)$ in $\bar{X}$ is not contained in $V(T_0)$. By Proposition 1 this implies that $\dim \bar{X} \cap V(F) \cap V(T_0) < \dim \bar{X} \cap V(F) < \dim X = n$. Let $F_1(T)$ be a homogeneous polynomial of degree d which does not vanish identically on any irreducible component of $\bar{X} \cap V(T_0)$. One constructs $F_1(T)$ by choosing a point in each component and a linear homogeneous form L not vanishing at each point (here where we use the assumption that k is infinite) and then taking $F_1 = L^d$. Then

$$\dim \bar{X} \cap V(T_0) \cap V(F) \cap V(F_1) < \dim \bar{X} \cap V(F) \cap V(T_0)$$

Continuing in this way we find n homogeneous polynomials $F_1(T), \ldots, F_n(T)$ of degree d such that

$$\bar{X} \cap V(T_0) \cap V(F) \cap V(F_1) \cap \ldots \cap V(F_n) = \emptyset.$$

Let $f : \bar{X} \to \mathbb{P}_k^{n+1}(K)$ be the regular map given by the polynomials $(T_0^d, F, F_1, \ldots, F_n)$. We claim that it is finite. Indeed, replacing $\bar{X}$ by its image $v_d(\bar{X})$ under the Veronese map $v_d : \mathbb{P}_k^m(K) \to \mathbb{P}_k^N(k)$, we see that f is equal to the restriction of the linear projection map

$$pr_E : v_d(\bar{X}) \to \mathbb{P}_k^n(K)$$

where E is the linear subspace defined by the linear forms in $N+1$ unknowns corresponding to the homogeneneous forms $T_0^d, F, F_1, \ldots, F_n$. We know that the linear projection map is finite. Obviously, $f(X) \subset \mathbb{P}_k^{n+1}(K)_0$, and the restriction map $f|X : X \to \mathbb{P}_k^{n+1}(K)_0 \cong \mathbb{A}_k^{n+1}(K)$, defined by the formula

$$x \to (\frac{F}{T_0^d}(x), \frac{F_1}{T_0^d}(x), \ldots, \frac{F_n}{T_0^d}(x)) = (\phi(x), \phi_1(x), \ldots, \phi_n(x))$$

is finite.

Proof of Krull's Hauptidealsatz:

Let $f : X \to A^{n+1}(K)$ be the finite map constructed in the previous lemma. It suffices to show that the restrictions $\bar{\phi}_i$ of the functions $\phi_i (i = 1, \ldots, n)$ to any irreducible component Y of $V(\phi)$ are algebraically independent elements of the ring $\mathcal{O}(Y)$ (since $\dim Y = \mathrm{alg.dim}_k \mathcal{O}(Y)$). Let $F \in k[Z_1, \ldots, Z_n] \setminus \{0\}$ be such that $F(\phi_1, \ldots, \phi_n) \in I(Y)$. Choosing a function $g \notin I(Y)$ vanishing on the remaining irreducible components of $V(\phi)$, we obtain that

$$V(F(\phi_1, \ldots, \phi_n)g) \supset V(\phi).$$

By the Nullstellensatz, $\phi | (F(\phi_1, \ldots, \phi_n)g)^N$ for some $N > 0$. Now, we can apply Lemma 3. Identifying $k[Z_1, \ldots, Z_n, Z_{n+1}]$ with the subring of $\mathcal{O}(X)$ by means of f^*, we see that $\phi = Z_{n+1}, F(\phi_1, \ldots, \phi_n) = F(Z_1, \ldots, Z_n)$, and $Z_{n+1} | F(Z_1, \ldots, Z_n)^N g^N$ in $\mathcal{O}(X)$. From Lemma 4 we deduce that $Z_{n+1} | g^{jN}$ for some $j \geq 0$, i.e., $g \equiv 0$ on $V(\phi)$ contradicting the choice of g. This proves the assertion.

Theorem 3. *Let X be an algebraic set and U be a dense open subset of X. Then*

$$\dim X = \dim U.$$

Proof. Obviously we may assume that X is irreducible and U is its open subset. First let us show that all affine open subsets of X have the same dimension. For this it is enough to show that $\dim U = \dim V$ if $V \subset U$ are affine open subsets. Indeed, we know that for every pair U and U' of open affine subsets of X we can find an affine non-empty subset $W \subset U \cap U'$. Then the above will prove that $\dim W = \dim U, \dim W = \dim U'$. Assume U is affine, we can find an open subset $D(\phi) \subset V \subset U$, where $\phi \in \mathcal{O}(U) \setminus \mathcal{O}(U)^*$. Then

$$\dim D(\phi) = \dim \mathcal{O}(D(\phi)) = \dim \mathcal{O}(U)[Z]/(Z\phi - 1) = (\dim \mathcal{O}(U) + 1) - 1 = \dim \mathcal{O}(U) = \dim U.$$

Here we have used that

$$\dim A[Z] = \text{alg.dim}_k A[Z] = \text{alg.dim}_k Q(A[Z]) + 1 =$$

$$\text{alg.dim}_k Q(A)(Z) = \text{alg.dim}_k Q(A) + 1 = \dim A + 1$$

for every finitely generated k-algebra A, and, of course the Krull Hauptidealsatz. This shows that all open non-empty affine subsets of X have the same dimension. Let $Z_0 \supset Z_1 \supset \ldots \supset Z_n$ be a maximal decreasing chain of closed irreducible subsets of X, i.e., $n = \dim X$. Take $x \in Z_n$ and let U be any open affine neighborhood of x. Then

$$Z_0 \cap U \supset Z_1 \cap U \supset \ldots \supset Z_n \cap U \neq \emptyset$$

is a decreasing chain of closed irreducible subsets of U (note that $Z_i \cap U \neq Z_j \cap U$ for $i \geq j$ since otherwise $Z_j = Z_i \cup (Z_j \cap (X - U))$ is the union of two closed subsets). Thus $\dim U \geq \dim X$, and Proposition 1 implies that $\dim U = \dim X$. This proves that for every affine open subset U of X we have $\dim U = \dim X$. Finally, if U is any open subset, we find an affine subset $V \subset U$ and observe that

$$n = \dim V \leq \dim U \leq \dim X = n$$

which implies that $\dim U = \dim X$.

Corollary 1.

$$\dim \mathbb{P}^n(k) = n.$$

Proof. Apply Proposition 4.

Corollary 2. *Let $f : X \to Y$ be a finite map of algebraic k-sets. Then*

$$\dim X = \dim Y.$$

Proof. Let Y_i be an irreducible component of Y. By Proposition 2 of Lecture 10, the restriction of the map f to $f^{-1}(Y_i)$ is a finite regular map $f_i : f^{-1}(Y_i) \to Y_i$. Take any open affine subset U of Y_i. Then $V = f^{-1}(U)$ is affine and the restriction map $V \to U$ is finite. By Lemma 2, $\dim U = \dim V$. Hence $\dim f^{-1}(Y_i) = \dim V = \dim U = \dim Y_i$. Since any irreducible component of X is contained in $f^{-1}(V_j)$ for some irreducible component V_j of Y, the assertion follows from Proposition 1.

Theorem 4. *Let F be a homogeneous polynomial not vanishing identically on an irreducible quasi- projective set X in $\mathbb{P}^n_k(K)$ and Y be an irreducible component of $X \cap V(F)$, then, either Y is empty, or*

$$\dim Y = \dim X - 1.$$

Proof. Assume $Y \neq \emptyset$. Let $y \in Y$ and U be an open affine subset of X containing y. Then $Y \cap U$ is an open subset of Y, hence $\dim Y \cap U = \dim Y$. Replacing U with a smaller subset, we may assume that $U \subset \mathbb{P}^n(k)_i$ for some i. Then F defines a regular function $\phi = F/T_i^r, r = \deg(F)$, on U, and $Y \cap U = D(\phi) \subset U$. By Krull's Hauptidealsatz, $\dim Y \cap U = \dim U - 1$. Hence

$$\dim Y = \dim Y \cap U = \dim U - 1 = \dim X - 1.$$

Corollary 1. *Let X be a quasi-projective algebraic k-set in $\mathbb{P}^n_k(K), F_1, \ldots, F_r \in k[T_0, \ldots, T_n]$ be homogeneous polynomials, $Y = X \cap V((F_1, \ldots, F_r)) = X \cap V(F_1) \cap \ldots \cap V(F_r)$ be the set of its common zeroes and Z be an irreducible component of this set. Then, either Z is empty, or*

$$\dim Z \geq \dim X - r.$$

The equality takes place if and only if for every $i = 1, \ldots, r$ the polynomial F_i does not vanish identically on any irreducible component of $X \cap V(F_1) \cap \ldots \cap V(F_{i-1})$.

Corollary 2. *Every $r \leq n$ homogeneous equations in $n+1$ unknowns have a common solution over an algebraically closed field. Moreover, if $r < n$, then the number of solutions is infinite.*

Proof. Apply the previous Corollary to $X = \mathbb{P}^n_k$ and use that an algebraic set is finite if and only if it is of dimension 0 (Proposition 2).

Example. Let $C = v_3(\mathbb{P}^1(K))$ be a twisted cubic in $\mathbb{P}^3(K)$. We know that C is given by three equations:

$$F_1 = T_0T_2 - T_1^2 = 0, F_2 = T_0T_3 - T_1T_2 = 0, F_3 = T_1T_3 - T_2^2 = 0.$$

We have $V(F_1) \cap V(F_2) = C \cup L$, where L is the line $T_0 = T_1 = 0$. At this point, we see that each irreducible component of $V(F_1) \cap V(F_2)$ has exactly dimension $1 = 3 - 2$. However, $V(F_3)$ contains C and cuts out L in a subset of C. Hence, every irreducible component of $V(F_1) \cap V(F_2) \cap V(F_3)$ is of the same dimension 1.

Theorem 5 (On dimension of fibres). *Let $f : X \to Y$ be a regular surjective map of irreducible algebraic sets, $m = \dim X, n = \dim Y$. Then*

(i) $\dim f^{-1}(y) \geq m - n$ *for any $y \in Y$;*

(ii) there exists a nonempty open subset V of Y such that $\dim f^{-1}(y) = m - n$ *for any $y \in V$.*

Proof. Let $x \in f^{-1}(y)$. Replacing X with an open affine neighborhood of x, and same for y, we assume that X and Y are affine. Let $\phi : Y \to \mathbb{A}^n(K)$ be a finite map and $f' = \phi \circ f$. Applying Proposition 3 from Lecture 10 we obtain that, for any $z \in \mathbb{A}^n(K)$, the fibre $f'^{-1}(z)$ is equal to a finite disjoint union of the fibres $f^{-1}(y)$ where $y \in \phi^{-1}(z)$. Thus we may assume that $Y = \mathbb{A}^n(K)$.

(i) Each point $y = (a_1, \ldots, a_n) \in \mathbb{A}^n(K)$ is given by n equations $Z_i - a_i = 0$. The fibre $f^{-1}(y)$ is given by n equations $f^*(Z_i - a_i) = 0$. Applying Hauptidealsatz, we obtain (i).

(ii) Since f is surjective, $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective, hence defines an extension of fields of rational functions $f^* : R(Y) \to R(X)$. By the theory of finitely generated field extensions,

$L = R(X)$ is an algebraic extension of a purely transcendental extension $K' = R(Y)(z_1, \ldots, z_r)$ of $K = R(Y)$. Clearly,

$$m = \text{alg.dim} R(X) = \text{alg.dim} R(Y) + r = n + r.$$

Let $\phi : X \dashrightarrow Y \times \mathbb{A}^r(K)$ be a rational map of affine sets corresponding to the extension L/K'. We may replace again X and Y by open affine subsets to assume that ϕ is regular. Let $\mathcal{O}(X)$ be generated by $u_1, \ldots, u_N$ as a k-algebra. We know that every u_i satisfies an algebraic equation $a_0 u_i^d + \ldots + a_d = 0$ with coefficients in $K' = R(Y \times \mathbb{A}^r(K))$. Replacing $Y \times \mathbb{A}^r(K)$ by an open subset U_i we may assume that all $a_i \in \mathcal{O}(U)$ and a_0 is invertible (throwing away the closed subset of zeroes of a_0). Taking the intersection U of all U_i's, we may assume that all u_i satisfy monic equations with coefficients in $\mathcal{O}(U)$. Thus $\mathcal{O}(X)$ is integral over $\mathcal{O}(U)$ hence $\phi : X \to U$ is a finite map. Let $p : Y \times \mathbb{A}^r(K) \to Y$ be the first projection. The corresponding extension of fields K'/K is defined by p^*. Since p is surjective, $p(U)$ is a dense subset of Y. Let us show that $p(U)$ contains an open subset of Y. We may replace U by a subset of the form $D(F)$ where $F = F(Y_1, \ldots, Y_n, Z_1, \ldots, Z_r) \in \mathcal{O}(Y \times \mathbb{A}^r(K))$. Write $F = \sum_i F_i Z^i$ as a sum of monomials in $Z_1, \ldots, Z_r$. For every $y \in Y$ such that not all $F_i(y) = 0$, we obtain non-zero polynomial in Z, hence we can find a point $z \in \mathbb{A}^r(K)$ such that $F(y, z) \neq 0$. This shows that $p(D(F)) \supset \cup D(F_i)$, hence the assertion follows. Let V be an open subset contained in $p(U)$. Replacing U by an open subset contained in $p^{-1}(V)$, we obtain a regular map $p : U \to V$ and the commutative triangle:

$$\begin{array}{ccc} \phi^{-1}(U) & \xrightarrow{\phi} & U \\ f \searrow & & \swarrow p \\ & V & \end{array}$$

The fibres of p are open subsets of fibres of the projection $Y \times \mathbb{A}^r(K) \to \mathbb{A}^r(K)$ which are affine n-spaces. The map $\phi : \phi^{-1}(U) \to U$ is finite as a restriction of a finite map over an open subset. Its restriction over the closed subset $p^{-1}(y)$ is a finite map too. Hence ϕ defines a finite map $f^{-1}(y) \to p^{-1}(y)$ and

$$\dim f^{-1}(y) = \dim p^{-1}(y) = r = m - n.$$

The theorem is proven.

Corollary. *Let X and Y be irreducible algebraic sets. Then*

$$\dim X \times Y = \dim X + \dim Y.$$

Proof. Consider the projection $X \times Y \to Y$ and apply the Theorem.

Theorem 6. *Let X and Y be irreducible quasi-projective subsets of $\mathbb{P}^n(K)$. For every irreducible component Z of $X \cap Y$*

$$\dim Z \geq \dim X + \dim Y - n.$$

Proof. Replacing X and Y by its open affine subsets, we may assume that X and Y are closed subsets of $\mathbb{A}^n(K)$. Let $\Delta : \mathbb{A}^n(K) \to \mathbb{A}^n(K) \times \mathbb{A}^n(K)$ be the diagonal map. Then Δ maps $X \cap Y$ isomorphically onto $(X \times Y) \cap \Delta_{\mathbb{A}^n(K)}$, where $\Delta_{\mathbb{A}^n(K)}$ is the diagonal of $\mathbb{A}^n(K)$. However, $\Delta_{\mathbb{A}^n(K)}$ is the set of common zeroes of n polynomials $Z_i - Z_i'$ where $Z_1, \ldots, Z_n$ are coordinates in the first

factor and $Z'_1, \ldots, Z'_n$ are the same for the second factor. Thus we may apply Theorem 2 n times to obtain

$$\dim Z \geq \dim X \times Y - n.$$

It remains to apply the previous corollary.

We define the *codimension* codim Y (or codim (Y, X) to be precise) of a subspace Y of a topological space X as $\dim X - \dim Y$. The previous theorem can be stated in these terms as

$$\text{codim } (X \cap Y, \mathbb{P}^n(K)) \leq \text{codim } (X, \mathbb{P}^n(K)) + \text{codim } (Y, \mathbb{P}^n(K)).$$

In this way it can be stated for the intersection of any number of subsets.

Exercises.

1. Give an example of
(a) a topological space X and its dense open subset U such that $\dim U < \dim X$;
(b) a surjective continuous map $f : X \to Y$ of topological spaces with $\dim X < \dim Y$;
(c) a Noetherian topological space of infinite dimension.

2. Prove that every closed irreducible subset of $\mathbb{P}^n(K)$ or $\mathbb{A}^n(K)$ of codimension 1 is the set of zeroes of one irreducible polynomial.

3. Let us identify the space K^{nm} with the space of matrices of size $m \times n$ with entries in K. Let X' be the subset of matrices of rank $\leq m - 1$ where $m \leq n$. Show that the image of $X' \setminus \{0\}$ in the projective space $\mathbb{P}^{nm-1}(K)$ is an irreducible projective set of codimension $n - m + 1$.

4. Show that for every irreducible closed subset Z of an irreducible algebraic set X there exists a chain of $n = \dim X + 1$ strictly decreasing closed irreducible subsets containg Z as its member. Define codimension of an irreducible closed subset Z of an irreducible algebraic set X as

$$\text{codim } (Y, X) = \max\{k : \exists \text{ a chain of closed irreducible subsets } Z = Z_0 \subset Z_1 \subset \ldots \subset Z_k\}.$$

Prove that $\dim Y + \text{codim } (Y, X) = \dim X$. In particular, our definition agrees with the one given at the end of this lecture.

5. A subset V of a topological space X is called *constructible* if it is equal to a disjoint union of finitely many locally closed subsets. Using the proof of Theorem 5 show that the image $f(V)$ of a constructible subset $V \subset X$ under a regular map $f : X \to Y$ of quasi-projective sets contains a non-empty open subset of its closure in Y. Using this show that $f(V)$ is constructible (Chevalley's theorem).

6*. Let X be an irreducible projective curve in $\mathbb{P}^n(K)$, where $k = K$, and $E = V(a_0T_0 + \ldots + a_nT_n)$ be a linear hyperplane. Show that E intersects X at the same number of distinct points if the coefficients $(a_0, \ldots, a_n)$ belong to a certain Zariski open subset of the space of the coefficients. This number is called the *degree* of X.

7*. Show that the degree of the Veronese curve $v_r(\mathbb{P}^1(K)) \subset \mathbb{P}^n(K)$ is equal to r.

8*. Generalize Bezout's theorem by proving that the set of solution of n homogeneous equations of degree $d_1, \ldots, d_n$ is either infinite or consists of $d_1 \cdots d_n$ points taken with appropriate multiplicities.

Lecture 12. LINES ON HYPERSURFACES

In this lecture we shall give an application of the theory of dimension. Consider the following problem. Let $X = V(F)$ be a projective hypersurface of degree $d = \deg F$ in $\mathbf{P}^n(K)$. Does it contain a linear subspace of given dimension, and if it does, how many? Consider the simplest case when $d = 2$ (the case $d = 1$ is obviously trivial). Then F is a quadratic form in $n+1$ variables. Let us assume for simplicity that $\mathrm{char}(K) \neq 2$. Then a linear m-dimensional subspace of dimension in $V(F)$ corresponds to a vector subspace L of dimension $m+1$ in K^{n+1} contained in the set of zeroes of F in K^{n+1}. This is an isotropic subspace of the quadratic form F. From the theory of quadratic forms we know that each isotropic subspace is contained in a maximal isotropic subspace of dimension $n+1-r+[r/2]$, where r is the rank of F. Thus $V(F)$ contains linear subspaces of dimension $\leq n-r+[r/2]$ but does not contain linear subspaces of larger dimension . For example, if $n = 3$, and $r = 4$, F is isomorphic to $V(G)$, where G is given by the equations

$$T_0T_1 - T_2T_3 = 0.$$

For every $\lambda, \mu \in K$, we have a line $L(\lambda, \mu)$ given by the equations

$$\lambda T_0 + \mu T_2 = 0, \mu T_1 + \lambda T_3 = 0,$$

or a line $M(\lambda, \mu)$ given by the equation

$$M(\lambda, \mu) : \lambda T_0 + \mu T_3 = 0, \mu T_1 + \lambda T_2 = 0.$$

It is clear that $L(\lambda, \mu) \cap L(\lambda', \mu') = \emptyset$ (resp. $M(\lambda, \mu) \cap M(\lambda', \mu') \neq \emptyset$) if and only if $(\lambda, \mu) \neq (\lambda', \mu')$ as points in $\mathbf{P}^1(K)$. On the hand $L(\lambda, \mu) \cap M(\lambda', \mu')$ is one point always. Under an isomorphism $V(F) \cong \mathbf{P}^1(K) \times \mathbf{P}^1(K)$, the two families of lines $L(\lambda, \mu)$ and $M(\lambda, \mu)$ correspond to the fibres of the two projections $\mathbf{P}^1(K) \times \mathbf{P}^1(K) \to \mathbf{P}^1(K)$.

Another example is the *Fermat hypersurface* of $V(F) \subset \mathbf{P}^3(K)$ of degree d, where

$$F = T_0^d + T_1^d + T_2^d + T_3^d.$$

Since

$$T_i^d + T_j^d = \prod_{s=1}^{d} (T_i + \rho^s T_j))$$

where ρ is a primitive d-th root of -1, we see that $V(F)$ contains $3d^2$ lines. Each one is defined by the equations of the type:

$$T_i + \rho^s T_j = 0, T_k + \rho^t T_l = 0,$$

where $\{i,j,k,l\} = \{0,1,2,3\}$. In particular, when $d = 3$, we obtain 27 lines. As we shall see in this Lecture, "almost every" cubic surface contains exactly 27 lines. On the other hand if $d \geq 4$, "almost no" surface contains a line.

To solve our problems, we first parametrize the set of linear r-dimension al subspaces of of $\mathbf{P}^n(K)$ by some projective algebraic set. This is based on the classic construction of the Grassmann variety.

Let V be a vector space of dimension $n+1$ over a field K and let L be its linear subspace of dimension $r+1$. Then the exterior product $\bigwedge^{r+1}(L)$ can be identified with a one-dimensional subspace of $\bigwedge^{r+1}(V)$, i.e., with a point $[L]$ of the projective space $\mathbf{P}(\bigwedge^{r+1}(V)) = \bigwedge^{r+1}(V)\backslash\{0\}/K^*$. In coordinates, if $e_1,\dots,e_{n+1}$ is a basis of V, and $f_1,\dots,f_{r+1}$ is a basis of L, then $\bigwedge^{r+1}(L)$ is spanned by one vector

$$f_1 \wedge \dots \wedge f_{r+1} = \sum_{1 \leq i_1 < \dots < i_{r+1} \leq n+1} p[i_1,\dots,i_{r+1}] e_{i_1} \wedge \dots e_{i_{r+1}}.$$

If we order the vectors $e_{i_1} \wedge \dots e_{i_{r+1}}$ we may identify $\bigwedge^{r+1}(V)$ with $K^{\binom{n+1}{r+1}}$, then the coordinate vector of the point $[L]$ in $\mathbf{P}(\bigwedge^{r+1}(V)) \cong \mathbf{P}^{\binom{n+1}{r+1}-1}(K)$ is the vector $(\dots, p[i_1,\dots,i_{r+1}],\dots)$. The coordinates $p[i_1,\dots,i_{r+1}]$ are called the *Plücker coordinates* of L. If we denote by $M(L)$ the matrix of size $(r+1)\times(n+1)$ with the j-th row formed by the coordinates of f_j with respect to the basis $(e_0,\dots,e_{n+1})$, then $p[i_1,\dots,i_{r+1}]$ is equal to the maximal size minor of $M(L)$ composed of the columns $A_{i_1},\dots,A_{i_{r+1}}$.

The next theorem shows that the correspondence $L \to [L]$ is a bijective map from the set of linear subspaces of dimension $r+1$ in V to the set of K-points of a certain projective subset $G(r+1,n+1)$ in $\mathbf{P}^{\binom{n+1}{r+1}-1}(K)$.

Theorem 1. *The subset $G(r+1,n+1)$ of lines in $\bigwedge^{r+1}(V)$ spanned by decomposable $(r+1)$-vectors $f_1 \wedge \dots \wedge f_{r+1}$ is a projective algebraic set in $\mathbf{P}(\bigwedge^{r+1}(V)) \cong \mathbf{P}^{\binom{n+1}{r+1}-1}(K)$. The map $L \to [L] = \bigwedge^{r+1}(L)$ is a bijective map from the set of linear subspaces of V of dimension $r+1$ to the set $G(r+1,n+1)$.*

Proof. We use the following fact from linear algebra. For every $t \in \bigwedge^{r+1}(V)$ let $L(t) = \{x \in V : t \wedge x = 0\}$. This is a linear subspace of V. Then $\dim L(t) \geq r+1$ if and only if t is decomposable and equal to $f_1 \wedge \dots \wedge f_{r+1}$ for some linear independent vectors $f_1,\dots,f_{r+1}$ which have to form a basis of $L(t)$. This assertion shows that the subspace L can be reconstructed uniquely from $[L]$ as the subspace $L(t)$, where t is any basis of $[L]$. Let us prove the assertion. The sufficiency is easy. If $t = f_1 \wedge \dots \wedge f_{r+1}$ for some basis $\{f_1,\dots,f_{r+1}\}$ of a linear subspace of dimension $r+1$, then, obviously, $f_1 \wedge \dots \wedge f_{r+1} \wedge x = 0$ for any $x \in L = Kf_1 + \dots + Kf_{r+1}$ so that $L \subset L(t)$. Since $f_1 \wedge \dots \wedge f_{r+1} \wedge x = 0$ implies that $\bigwedge^{r+2}(Kf_1 + \dots + Kf_{r+1} + Kx) = 0$, we obtain that $\dim(Kf_1 + \dots + Kf_{r+1} + Kx) = r+1$, hence $x \in Kf_1 + \dots + f_{r+1}$. This shows that $L = L(t)$. Conversely assume $\dim L(t) = r+1$. Let $f_1,\dots f_{r+1}$ be a set of linear independent vectors in $L(t)$, and let $\{f_1,\dots,f_{r+1},f_{r+1},\dots,f_{n+1}\}$ be an extension of $\{f_1,\dots,f_{r+1}\}$ to a basis of V. We can write

$$t = \sum_{i_1 < \dots < i_{r+1}} a_{i_1 \dots i_{r+1}} f_{i_1} \wedge \dots \wedge f_{i_{r+1}}.$$

It is easy to see that $t \wedge f_i = 0, i = 1,\dots,r+1$, implies $a_{i_1\dots i_{r+1}} = 0$ for $\{i_1,\dots i_{r+1}\} \neq \{1,\dots,r+1\}$. Hence t is proportional to $f_1 \wedge \dots \wedge f_{r+1}$.

To see why decomposable non-zero $(r+1)$-vectors define a closed subset $G(r+1,n+1)$ of $\mathbf{P}(\bigwedge^{r+1}(V))$ it suffices to observe that $\dim L(t) \geq r+1$ if and only if $rk(T_t) \leq n-r$, where T_t is the linear map $V \to \bigwedge^{r+2}(V)$ defined by the formula $x \mapsto t \wedge x$. The latter condition is equivalent to vanishing of $(n-r+1)$-minors of the matrix of T_t with respect to some basis. By taking a basis $e_1, \ldots, e_{n+1}$ of V, it is easy to see that the entries of the matrix of T_t are the Plücker coordinates of the space $L(t)$. Thus we obtain that $G(r+1,n+1)$ is the set of zeroes of a set of homogeneous polynomials of degree $n-r+1$. Observe that these polynomials have integer coefficients, so $G(r+1,n+1)$ is a projective k-set for any $k \subset K$.

More generally, we can define a projective algebraic variety $G_k(r+1,n+1)$ defined by:

$$G_k(r+1,n+1)(K) = \{\text{direct summands of } K^{n+1} \text{ of rank } r+1\}.$$

Note that a direct summand of a free module is a projective module. The operation of exterior power, $M \to \bigwedge^{r+1}(M)$ defines a morphism of projective algebraic varieties

$$p : G_k(r+1,n+1) \to \mathbf{P}_k^{\binom{n+1}{r+1}-1}.$$

If $r=0$ this morphism is an isomorphism.

Definition. The projective variety $G_k(r+1,n+1)$ is called the *Grassmann variety* over the field k. The morphism p is called the *Plücker embedding* of $G_k(r+1,n+1)$. For every algebraically closed field K containing k, we shall identify the set $G_k(r+1,n+1)(K)$ with the projective algebraic subset $G(r+1,n+1)$ of $\mathbf{P}_k^{\binom{n+1}{r+1}-1}$.

Proposition 1. *The projective algebraic set $G(r+1,n+1)$ is an irreducible projective set of dimension $(n-r)(r+1)$.*

Proof. We shall give two different proofs of this result. Each one carries some additional information about $G(r+1,n+1)$. In the first one we use the following obvious fact: the general linear group $GL(n+1,K)$ acts transitively on the set of $(r+1)$-dimension al linear subspaces of K^{n+1}. Moreover the stabilizer of each such subspace L is isomorphic to the subgroup P of $GL(n+1,K)$ that consists of matrices of the form:

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

where A, B, C are matrices of size $(r+1)\times(r+1)$, $(r+1)\times(n-r)$, $(n-r)\times(n-r)$, respectively. Let us consider $GL(n+1,K)$ as a closed subset of K^{n^2+1} defined by the equation $T_0 det((T_{ij}))-1=0$. then it is clear that P is a closed subset of $GL(n+1,K)$ defined by the additional equations $T_{ij}=0, i=n+2-r,\ldots,n+1, j=1,\ldots,r+1$. The dimension of P is equal to $(n+1)^2-(n-r)(r+1)$. Next we define a surjective regular map of algebraic k-sets $f : GL(n+1,K) \to G(r+1,n+1)$ by the formula $M \to M(L_0)$, where $L_0 = Ke_1 + \ldots + Ke_{r+1}$. If $M=(a_{ij})$, then

$$M(L_0) = \text{span}\{a_{11}e_1 + \ldots + a_{n+11}e_{n+1}, \ldots, a_{1r+1}e_1 + \ldots + a_{n+1r+1}\}$$

so that the Plücker coordinates $p[i_1,\ldots,i_{r+1}]$ of $M(L_0)$ are equal to the minor of the matrix (a_{ij}) formed by the first $r+1$ columns and the rows indexed by the set $\{i_1,\ldots,i_{r+1}\}$. This shows that f is a regular map from the affine k-set $GL(n+1,K)$ to the projective algebraic k-set $G(r+1,n+1)$.

Its fibres are isomorphic to P. By the theorem on the dimension of fibres from Lecture 11, we obtain that

$$\dim G(r+1,n+1) = \dim GL(n+1,K) - \dim P = (n+1)^2 - ((n+1)^2 - (n-r)(r+1)) = (n-r)(r+1).$$

Since $GL(n+1,K)$ is irreducible, $G(r+1,n+1)$ is irreducible.

Now let us give another proof of this result. Choose the Plücker coordinates $p[j_1,\dots,j_{r+1}]$ and consider the open subsets $D(p[j_1,\dots,j_{r+1}]) \subset \mathbf{P}_k^{\binom{n+1}{r+1}-1}(K)$. The intersection $D(p[j_1,\dots,j_{r+1}]) \cap G(r+1,n+1)$ is equal to the set of linear subspaces L which admit a basis

$$f_1 = a_{11}e_1 + \ldots + a_{1n+1}e_n, \ldots, \ f_{r+1} = a_{r+11}e_1 + \ldots + a_{r+1n+1}e_n,$$

such that $p[j_1,\dots,j_{r+1}] = \det(A_{j_1 j_2 \dots j_{r+1}}) \neq 0$, where

$$A_{i_1 i_2 \dots i_{r+1}} = \begin{pmatrix} a_{1j_1} & a_{1j_2} & \dots & a_{1j_{r+1}} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{r+1j_1} & a_{1j_2} & \dots & a_{r+1j_{r+1}} \end{pmatrix}$$

After we replace $f_1,\dots,f_{r+1}$ with $f'_1,\dots,f'_{r+1}$ such that

$$f'_1 = b_{11}f_1 + \ldots + b_{1r+1}f_{r+1}, \ldots, f'_{r+1} = b_{r+11}f_1 + \ldots + b_{r+1r+1}f_{r+1},$$

where (b_{ij}) is the inverse of the matrix $A_{j_1 j_2 \dots j_{r+1}}$, we may assume that $A_{i_1 i_2 \dots i_{r+1}}$ is the identity matrix I_{r+1}. Then we may take all $(n-r)(r+1)$ other entries $a_{ij}, j \neq j_k$ arbitrary, and obtain that $D(p[i_1,\dots,i_{r+1}]) \cap G(r+1,n+1)$ is isomorphic to the affine space $\mathbf{A}_k^{(n-r)(r+1)}(K)$. Thus $G(r+1,n+1)$ is covered by $\binom{n+1}{r+1}$ open subsets isomorphic to the affine space of dimension $(n-r)(r+1)$. This obviously proves the assertion.

Example 1. Let us consider the case $r=1, n=3$. Then $G(2,4) \subset \mathbf{P}^5$ parametrizes lines in $\mathbf{P}^3(K)$. We have six Plücker coordinates $p[ij], i,j = 1,2,3,4$. An element $\omega \in \bigwedge^2(V)$ can be identified with a skew-symmetric bilinear form $V^* \to V^* \to K$. The matrix M of this bilinear form with respect to the dual basis $e_1^*,\dots,e_4^*$ has entries above the diagonals equal to a_{ij}, where $\omega = \sum_{1 \leq i < j \leq 4} a_{ij} e_i \wedge e_j$. The element $\omega = f_1 \wedge f_2$ if and only if the matrix is of rank < 4. In fact, take $\phi \in V^*$ such that $\phi(f_1) = \phi(f_2) = 0$. For any $x \in V^*$ we have $f_1 \wedge f_2(x,\phi) = x(f_1)\phi(f_2) - x(f_2)\phi(f_1) = 0$. Thus the bilinear form has the kernel and the matrix has zero determinant. The determinant of a skew-symmetric matrix is equal to the square of the Pffafian. Thus we get that all decomposables vectors ω satisfy the condition $Pf(M) = 0$. The equation of the Pffafian of a 4×4 skew symmetric matrix is

$$a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23} = 0.$$

Since we know already that $G(2,4)$ is an irreducible projective set of dimension 4, we obtain that it coincides with the quadric $V(Q)$ where

$$Q = p[12]p[34] - p[13]p[24] + p[14]p[23].$$

Evidently Q is a non-degenerate quadratic form.

Remark 1. Let us take $K = \mathbb{C}$. Consider the anti-holomorphic involution of $G(2,4)$ defined by

$$(p[12],p[13],p[14],p[23],p[24],p[34]) \mapsto (\bar{p}[12],-\bar{p}[24],\bar{p}[23],\bar{p}[14],-\bar{p}[13],\bar{p}[34]).$$

Then the set of fixed points consists of points $(z_1, z_2, z_3, z_4, z_5, z_6) \in \mathbb{P}^5(\mathbb{C})$ such that $z_1, z_2 \in \mathbb{R}$, $\bar{z}_3 = z_4, \bar{z}_5 = z_6$. They satisfy the equation equation

$$z_1 z_2 + |z_3|^2 + |z_4|^2 = 0.$$

Changing the variables z_1, z_2 to $x_1 - x_2, x_1 + x_2$, and dividing by x_2 (it is easy to see that x_1, x_2 cannot be equal to zero), we obtain the equation of a unit sphere in $\mathbb{R}^5$. Thus $G(2,4)$ admits a real structure (not the standard one) such that the set of real points is S^4. The 4-dimensional sphere is a natural compactification of $\mathbb{R}^4$, the space-time. In the twistor theory of Penrose, $G(2,4)$ is viewed as a complexification of the real space-time.

Remark 2. The equation for $G(2,4)$ given in the proof of Theorem 1 differs from the equation $Q = 0$ by a factor. Any Grassmannian $G(r+1, n+1)$ can be given by a system of equations of degree 2, so called the *Plücker equations*. They look as follows:

$$\sum_{s=1}^{r+2} (-1)^s p[i_1, \ldots, i_r, j_s] p[j_1 \ldots, j_{s-1}, j_{s+1}, \ldots, j_{r+2}] = 0,$$

where $\{i_1, \ldots, i_r\}$ and $\{j_1, \ldots, j_{r+2}\}$ are any two strictly increasing sequences of the set $\{1, \ldots, n+1\}$.

We denote by $\mathrm{Hyp}(d; n)$ the projective space $\mathbf{P}^{\binom{n+d}{d}-1}$. If we use $\Upsilon_{i_0,\ldots,i_n}, 0 \leq i_j, i_0 + \ldots + i_n = d$ to denote projective coordinates in this space then each K-point $(\ldots, a_{i_0,\ldots,i_n}, \ldots)$ of this space defines the projective K-subvariety $F = 0$ of $\mathbf{P}^n_K$ where

$$F = \sum_{i_0,\ldots,i_n} a_{i_0,\ldots,i_n} T_0^{i_0} \cdots T_n^{i_n} = 0.$$

Thus we can view K-points of the projective space $\mathbf{P}^{\binom{n+d}{d}-1}$ as projective hypersurfaces of degree d. This explains the notation. In the special case when $d = 1$, the space $\mathrm{Hyp}(1, n)$ is called the *dual space* of $\mathbf{P}^n_k$ and is denoted by $\check{\mathbf{P}}^n_k$. Its K-points are in a bijective correspondence with linear subspaces of $\mathbf{P}^n_k(K)$ of dimension $n-1$ (*hyperplanes*) .

Now, everything is ready to solve our problem. Fix any algebraically closed field K. Let $H = \mathrm{Hyp}(d; n)(K)$ and $G = G(r+1, n+1)(K)$. Define

$$I(r, d, n)(K) = \{(X, E) \in H(K) \times G(K) : E \subset X\}.$$

Lemma 1. *$I(r,d,n)$ is a closed irreducible subset of $H \times G$ of dimension equal to $(r+1)(n-r) + \binom{n+d}{d} - \binom{r+d}{d} - 1$.*

Proof. Let E' denote the linear subspace of K^{n+1} corresponding to E. Let $f_1, \ldots, f_{r+1}$ be a basis of E', extended to a basis $(f_1, \ldots, f_{n+1})$ of K^{n+1}. Any $x \in E'$ defines a linear form ϕ_x on $\bigwedge^r(K^{n+1})$ given by the formula

$$x \wedge \omega \wedge f_{r+2} \wedge \ldots \wedge f_{n+1} = \phi_x(\omega) f_1 \wedge \ldots \wedge f_{n+1}.$$

In particular, if $x = \lambda_1 f_1 + \ldots + \lambda_{r+1} f_{r+1}$, then taking the wedge product of both sides with each $f_1 \wedge \ldots \wedge f_{i-1} \wedge f_{i+1} \wedge \ldots f_{n+1}$, we obtain

$$x = \phi_x(f_2 \wedge \ldots \wedge f_{r+1}) f_1 - \phi_x(f_1 \wedge f_3 \wedge \ldots \wedge f_{r+1}) f_2 + \ldots + (-1)^r \phi_x(f_1 \wedge \ldots \wedge f_r) f_{r+1}.$$

Let $(e_1^*, \ldots, e_{n+1}^*)$ be the dual basis of the canonical basis of K^{n+1}. Writing $\phi_x = \sum \alpha_{i_1 \ldots i_r} e_{i_1}^* \wedge \ldots \wedge e_{i_r}^*$, we get that λ_i are equal to some linear combinations of the Plücker coordinates of E'. Now plugging in $(\lambda_0, \ldots, \lambda_n)$ into the equation of X , we see that $I(r,d,n)$ is given by bi-homogeneous polynomials in the coefficients of F and in the Plücker coordinates of E. This proves that $I(r,d,n)$ is a closed subset of the product $H \times G$. Now consider the projection $p : I(r,d,n) \to G$. For each $E \in G$, the fibre $p^{-1}(E)$ consists of all hypersurfaces $V(F)$ containing E. Choose a coordinate system such that E is given by the equations $T_{r+1} = \ldots = T_n = 0$. Then $E \subset V(F)$ if and only if each monomial entering into F with non-zero coefficient contains some positive power of T_i with $i \geq r+1$. In other words F is defined by vanishing of all coefficients at the monomials of degree d in the variables $T_0, \ldots, T_r$. This gives $\binom{r+d}{r}$ linear conditions on the coefficients of F, hence $\dim p^{-1}(E) = \binom{n+d}{d} - 1 - \binom{r+d}{r}$. Let us assume that $I(r,d,n)$ is irreducible. By the Theorem on dimension of fibres,

$$\dim I(r,d,n) = \dim p^{-1}(E) + \dim G = (n-r)(r+1) + \binom{n+d}{d} - 1 - \binom{r+d}{r}.$$

It remains to prove the irreducibility of $I(r,d,n)$. Considering the projection $p : I(r,d,n) \to G$, the assertion follows from the following:

Lemma 2. *Let $f : X \to Y$ be a surjective regular map of projective algebraic sets. Assume that Y is irreducible and all fibres of f are irreducible and of the same dimension n. Then X is irreducible.*

Proof. Let $X = X_1 \cup \ldots \cup X_n$ be the union of irreducible closed sets. Since f is a map of projective sets, the images $f(X_i)$ are closed and irreducible. By assumption, Y is irreducible, hence the set $I = \{i : f(X_i) = Y\}$ is not empty. For every $y \in Y \setminus (\cup_{i \notin I} f(X_i))$, we have $f^{-1}(y) = \cup_{i \in I}(X_i \cap f^{-1}(y))$. Since $f^{-1}(y)$ is irreducible, there exists $X_i, i \in I$, such that $f^{-1}(y) \subset X_i$. Since the set I is finite, we can find an open subset $U \subset Y$ such that $f^{-1}(y) \subset X_i$ for all $y \in U$. Let $f_i : X_i \to Y$ be the restriction of f to X_i. By the Theorem on dimension of fibres, any fibre of f_i is of dimension $\geq n$. By assumption, $\dim f_i^{-1}(y) \geq n = \dim f^{-1}(y)$. This implies that $f_i^{-1}(y) = f^{-1}(y)$ for any $y \in Y$. This certainly implies that $X_i = X$ proving the assertion.

Theorem 2. *Assume that*

$$(n-r)(r+1) < \binom{r+d}{r}.$$

Then the subset of $\mathrm{Hyp}(d;n)(K)$ which consists of hypersurfaces containing a linear subspace of dimension r is a proper closed subset.

Proof. Consider the other projection $q : I(r,d,n) \to H = \mathrm{Hyp}(d;n)(K)$. Since $I(r,d,n)$ is a projective set, its image is a closed subset of H. Suppose q is surjective. Then

$$(n-r)(r+1) + \binom{n+d}{d} - 1 - \binom{r+d}{r} = \dim I(r,d,n) \geq \dim H = \binom{n+d}{d} - 1.$$

This is impossible in view of the assumption of the theorem.

Remark 3. One expects that each $V(F) \in \mathrm{Hyp}(d;n)$ contains a linear subspace of dimension r when $(n-r)(r+1) \geq \binom{r+d}{r}$. This is true if $d > 2$ but false if $d = 2$. For example let $d = 2, n = 4$. A nonsingular quadratic form in 5 variables does not contain isotropic subspaces of dimension 3. Hence the corresponding quadric does not contain planes. However, $(n-r)(r+1) = 6 \geq \binom{r+d}{r} = 6$.

From now on we restrict ourselves with the case $n = 3$ and $d = 3$, i.e. cubic surfaces in $\mathbf{P}^3(K)$. We shall be looking for lines on cubic surfaces. In this case $(n-r)(r+1) = 6 > \binom{r+d}{d} = 4$, so we expect that every cubic surface has a line. As we saw in the previous remark it needs to be proven.

Theorem 3.
(i) Every cubic surface X contains a line.
(ii) There exists an open subset $U \subset \mathrm{Hyp}(3;3)(K)$ such that any $X \in U$ contains exactly 27 lines.

Proof. (i) In the notation of the proof of Theorem 2, it suffices to show that the projection map $q : I(1,3,3) \to \mathrm{Hyp}(3;3)(K)$ is surjective. Suppose the image of q is a proper closed subset Y of $\mathrm{Hyp}(3;3)(K)$. Then $\dim Y < \dim \mathrm{Hyp}(3;3)(K) = 19$ and $\dim I(1,3,3) = 19$. By the theorem on dimension of fibres, we obtain that all fibres of q are of dimension at least one. In particular, every cubic surface containing a line contains infinitely many of them. But let us consider the surface X given by the equation

$$T_1T_2T_3 - T_0^3 = 0.$$

Suppose a line ℓ lies on X. Let $(a_0, a_1, a_2, a_3) \in \ell$. If $a_0 \neq 0$, then $a_i \neq 0, i \neq 0$. On the other hand, every line hits the planes $T_i = 0$. This shows that ℓ is contained in the plane $T_0 = 0$. But there are only three lines on X contained in this plane: $T_i = T_0 = 0, i = 1, 2$ and 3. Therefore X contains only 3 lines. This proves the first assertion.

(ii) We already know that every cubic surface $X = V(F)$ has at least one line. Pick up such a line ℓ. Without loss of generality we may assume that it is given by the equation:

$$T_2 = T_3 = 0.$$

As we saw in the proof of Lemma 1:

$$F = T_2Q_0(T_0, T_1, T_2, T_3) + T_3Q_1(T_0, T_1, T_2, T_3) = 0,$$

where Q_0 and Q_1 are quadratic homogeneous polynomials. Each plane π containing the line ℓ is given by the equation

$$\lambda T_2 - \mu T_3 = 0$$

for some scalars $\lambda, \mu \in K$. The intersection $\pi \cap V(F)$ contains the line λ and a curve of degree 2 in π. More explicitly, choose coordinates t_0, t_1, t_2 in the plane, related to our coordinates T_0, T_1, T_2, T_3 by the formulas:

$$T_0 = t_0, T_1 = t_1, T_2 = \mu t_2, T_3 = \lambda t_2.$$

Plugging these expression into F, we obtain:

$$\mu t_2 Q_0(t_0, t_1, \mu t_2, \lambda t_2) + \lambda t_2 Q_1(t_0, t_1, \mu t_2, \lambda t_3) = 0.$$

This shows that $\pi \cap X \subset \pi$ consists of the line ℓ with the equation $t_2 = 0$ and the conic $C(\lambda, \mu)$ with the equation:

$$\mu Q_0(t_0, t_1, \mu t_2, \lambda t_2) + \lambda Q_1(t_0, t_1, \mu t_2, \lambda t_2) = 0.$$

We may also assume that the line enters with multiplicity one (since we take "general " coeficients of F). Let

$$Q_0 = \sum_{0 \leq i < j \leq 3} a_{ij}T_iT_j, \quad Q_1 = \sum_{0 \leq i < j \leq 3} b_{ij}T_iT_j.$$

Then $C(\lambda, \mu)$ is given by the equation:

$$(\mu a_{00} + \lambda b_{00})t_0^2 + (\mu a_{11} + \lambda b_{11})t_1^2 + (\mu^2(\mu a_{22} + \lambda b_{22}) + \lambda^2(\mu a_{33} + \lambda b_{33}))t_2^2 + (\mu a_{01} + \lambda b_{01})t_0t_1$$

$$+(\mu(\mu a_{02} + \lambda b_{02}) + \lambda(\mu a_{03} + \lambda b_{03}))t_0t_2 + (\mu^2 a_{12} + \lambda\mu b_{12}) + ((\mu\lambda a_{13} + \lambda^2 b_{13}))t_1t_2 = 0.$$

Now, let us start vary the parameters λ and μ and see how many reducible conics $C(\lambda, \mu)$ we obtain. The conic $C(\lambda, \mu)$ is reducible if and only if the quadratic form defining it is degenerate. The condition for the latter is the vanishing of the discriminant D of the quadratic form $C(\lambda, \mu)$. Observe that D is a homogeneous polynomial of degree 5 in λ, μ. Thus there exists a Zariski open subset of Hyp(3; 3) for which this determinant has 5 distinct roots (λ_i, μ_i). Each such solution defines a plane π_i which cut out on X the line ℓ and a reducible conic. The latter is the union of two lines or a double line. Again, for some open subset of Hyp(3; 3) we expect that the double line case does not occur. Thus we found 11 lines on X: the line ℓ and 5 pairs of lines ℓ_i, ℓ_i' lying each lying in the plane π_i. Pick up some plane, say π_1. We have 3 lines ℓ, ℓ', and ℓ'' in π_1. Replacing ℓ by ℓ', and then by ℓ'', and repeating the construction, we obtain 4 planes through ℓ, ℓ' and 4 planes through ℓ'', each containing a pair of lines. Altogether we found $3 + 8 + 8 + 8 = 27$ lines on X. To see that all lines are accounted for, we observe that any line intersecting either ℓ, or ℓ', or ℓ'' lies in one of the planes we have considered before. So it has been accounted for. Now let L be any line. We find a plane π through L that contains three lines L, L' and L'' on X. This plane intersects the lines ℓ, ℓ', and ℓ'' at some points p, p' and p'' respectively. We may assume that these points are distinct. Otherwise we find three nocoplanar lines in X passing through one point. As we shall see later this implies that X is singular at this point. Since neither L' nor L'' can pass through two of these points, one of these points lie on L. Hence L is coplanar with one of the lines ℓ, ℓ', ℓ''. Therefore L has been accounted for.

Remark 4. Using more techniques one can show that every "nonsingular" (in the sense of the next lectures) cubic surface contains exactly 27 lines. Let us define the graph whose vertices are the lines and two vertices are joined by an edge if the lines intersect. This graph is independent on the choice of a nonsingular cubic surface and its group of symmetries is isomorphic to the group $W(E_6)$ of order 51840 (the Weyl group of the root system of a simple Lie algebra of type E_6).

Exercises.

1. Show that the set π_x of lines in $\mathbf{P}^3(K)$ passing through a point $x \in \mathbf{P}^3(K)$ is a closed subset of $G(2, 4)$ isomorphic to $\mathbf{P}^2(K)$. Also show that the set π_P of lines in $\mathbf{P}^3(K)$ contained in a plane $P \subset \mathbf{P}^3(K)$ is a closed subset of $G(2, 4)$ isomorphic to $\mathbf{P}^2(K)$.

2. Prove that the subset of quartic surfaces in Hyp(4; 3) which contain a line is an irreducible closed subset of Hyp(4; 3) of codimension 1.

3. Prove that every hypersurface of degree $d \leq 5$ in $\mathbf{P}^4(K)$ contains a line, and, if $d \leq 4$, then it contains infinitely many lines.

4. Let X be a general cubic hypersurface in $\mathbb{P}^4(K)$ (general means that X belongs to an open subset U of Hyp(3; 4)). Show that there exists an open subset $V \subset X$ such that any $x \in V$ lies on exactly six lines contained in X.

5*. Let $1 \leq m_1 < m_2 < \ldots < m_r \leq n + 1$, a flag in K^{n+1} of type $(m_1, \ldots, m_r)$ is a chain of linear subspaces $L_1 \subset \ldots \subset L_r$ with $\dim L_i = m_i$.

(a) Show that the set of flags is a closed subset in the product of the Grassmannians $G(m_1, n+1) \times \ldots \times G(m_r, n+1)$. This projective algebraic set is called the *flag variety* of type $(m_1, \ldots, m_r)$ and is denoted by $F_k(m_1, \ldots, m_r; n + 1)$.

(b) Find the dimension of $F_k(m_1, \ldots, m_r; n + 1)$.

6. By analizing the proof of Theorem 3 show the following:

(a) The set of 27 lines on a cubic surface X contains 45 triples of lines which lie in a plane (called a *tritangent plane*).

(b) There exist 12 lines $l_1, \dots, l_6, l'_1, \dots, l'_6$ such that $l'_i \cap l_i = \emptyset, i = 1, \dots, 6, l_i \cap l'_j \neq \emptyset$ if $i \neq j$. Such a set is called a *double-sixer*.

(c)* Show that there are 36 different double sixers.

(d) Check all the previous assertions for the Fermat cubic.

7*. Prove that

(a) A general cubic surface $V(F)$ contains 9 lines $\ell_{ij}, i, j = 1, 2, 3$ such that $\ell_{ij} \cap \ell_{km} \neq \emptyset$ if and only if $i = k$ or $j = m$.

(b) Using (a) show that $V(F)$ can be given by the equation

$$\det \begin{pmatrix} L_1 & 0 & M_1 \\ M_2 & L_2 & 0 \\ 0 & M_3 & L_3 \end{pmatrix} = 0,$$

where L_i, M_i are linear forms.

(c) Show that the map $T : V(F) \to \mathbb{P}^2$ which assigns to a point $x \in V(F)$ the set of solutions of the equation $(t_0, t_1, t_2) \cdot A = 0$ is a birational map. Here A is the matrix of linear from from (b).

(d) Find an explicit formulas for the inverse birational map T^{-1}.

8. Using Problem 5 (b),(c) show that the group W of symmetries of 27 lines consists of 51840 elements.

9*. Let C be a twisted cubic in $\mathbb{P}^3$ (the image of $\mathbb{P}^1$ under a Veronese map given by monomials of degree 3). For any two distinct point $x, y \in C$ consider the line $l_{x,y}$ joining these points. Show that the set of such lines is a locally closed subset of $G(2, 4)$. Find the equations defining its closure.

10*. Let $k = k_0(t)$, where k_0 is an algebraically closed field and $F(T_0, \dots, T_n) \in k[T_1, \dots, T_n]$ be a homogeneous polynomial of degree $d < n$. Show that $V(F)(k) \neq \emptyset$ (Tsen's Theorem).

Lecture 13. TANGENT SPACE

The notion of the tangent space is familiar from analytic geometry. For example, let $F(x, y) = 0$ be a curve in $\mathbb{R}^2$ and let $a = (x_0, y_0)$ be a point lying on this surface. The tangent line of X at the point a is defined by the equation:

$$\frac{\partial F}{\partial x}(a)(x - x_0) + \frac{\partial F}{\partial y}(a)(y - y_0) = 0.$$

It is defined only if at least one partial derivative of F at a is not equal to zero. In this case the point is called nonsingular. Otherwise it is said to be singular.

Another notion of the tangent space is familiar from the theory of differentiable manifolds. Let X be a differentiable manifold and a be its point. By definition, a tangent vector t_a of X at a is a derivation (or differentiation) of the ring $\mathcal{O}(X)$ of differentiable functions on X, that is, a $\mathbb{R}$-linear map $\delta : \mathcal{O}(X) \to \mathbb{R}$ such that

$$\delta(fg) = f(a)\delta(g) + g(a)\delta(f) \quad \text{for any } f, g \in \mathcal{O}(X).$$

It is defined by derivation of a function f along t_a given by the formula

$$< f, t_a >= \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a) t_i$$

where $(t_1, \ldots, t_n)$ are the coordinates of t_a and $(x_1, \ldots, x_n)$ are the local coordinates of X at the point a.

In this lecture we introduce and study the notion of a tangent space and a nonsingular point for arbitrary algebraic sets or varieties.

For every k-algebra K let $K[\varepsilon] = K[t]/(t^2)$ be the K-algebra of dual numbers. If ε is taken to be $t \bmod(t^2)$, then $K[\varepsilon]$ consists of linear combinations $a + b\varepsilon, a, b \in K$, which are added coordinate wise and multiplied by the rule

$$(a + b\varepsilon)(a' + b'\varepsilon) = aa' + (ab' + a'b)\varepsilon.$$

We denote by

$$\alpha_1 : K[\varepsilon] \to K$$

the natural homomorphism $a + b\varepsilon \to a$. Its kernel is the ideal $(\varepsilon) = \{b\varepsilon, b \in K\}$.

Definition. Let X be an affine or a projective algebraic variety over a field k and $x \in X(K)$ be its K-point. A *tangent vector* t_x of F at x is a $K[\varepsilon]$-point $t_x \in X(K[\varepsilon])$ such that $X(\alpha_1)(t_x) = x$. The set of tangent vectors of X at x is denoted by $T(X)_x$ and is called the *tangent space* of F at x.

Example 1. Assume X is an affine algebraic variety given by a system of equations

$$F_1(Z_1, \dots, Z_n) = 0, \dots, F_r(Z_1, \dots, Z_n) = 0.$$

A point $x \in X(K)$ is a solution $(a_1, \dots, a_n) \in K^n$ of this system. A tangent vector t_x is a solution $(a_1 + b_1\varepsilon, \dots, a_n + b_n\varepsilon) \in X(K[\varepsilon])$ of the same system. Write down the polynomials $F_i(Z)$ in the form :

$$F_i(Z_1, \dots, Z_n) = G_i(Z_1 - a_1, \dots, Z_n - a_n) = \sum_{j=1}^{n} \alpha_j^{(i)}(Z_i - a_i) + \sum_{j,k=1}^{n} \alpha_{jk}^{(i)}(Z_j - a_i)(Z_k - a_j) + \dots.$$

(Taylor's expansion). Note that the G_i's do not contain the constant term because $(a_1, \dots, a_n) \in X(K)$. By definition, the coefficient $\alpha_j^{(i)}$ is the partial derivative of F_i with respect to Z_j at the point $x = (a_1, \dots, a_n)$. It is denoted by $\frac{\partial F_i}{\partial Z_j}(x)$. Obviously it is an element of K. Now we plug the point $(a_1 + b_1\varepsilon, \dots, a_n + b_n\varepsilon)$ into the previous equations to obtain

$$F_i(a_1 + b_1\varepsilon, \dots, a_n + b_n\varepsilon) = \sum_{j=1}^{n} \alpha_j^{(i)} b_i \varepsilon + \sum_{j,k=1}^{n} \alpha_{jk}^{(i)} b_i b_j \varepsilon^2 + (\dots.)\varepsilon^3 + \dots = \sum_{j=1}^{n} \alpha_j^{(i)} b_i \varepsilon = 0.$$

From this we deduce that $(b_1, \dots, b_n)$ satisfies the system of linear homogeneous equations:

$$\sum_{j=1}^{n} \frac{\partial F_i}{\partial Z_j}(x) b_j = 0, \quad i = 1, \dots, r. \tag{1}$$

Thus the set of tangent vectors $T(X)_x$ is bijective to the submodule of K^n which consists of solutions of a homogeneous system of linear equations. In particular, we have introduced the structure of a K-module on $T(X)_x$.

Example 2. Assume $X = \mathbb{P}_k^n$ is projective space over k. Let $x = (a_0, \dots, a_n) \in \mathbb{P}_k^n(K)$, where K is a field. A tangent vector at x is a local line M over $K[\varepsilon]$ such that $M/\varepsilon M = (a_0, \dots, a_n)K$. Since the ring $K[\epsilon]$ is obviously local, M is a global line given by coordinates $(a_0 + b_0\varepsilon, \dots, a_n + b_n\varepsilon)$. Note that $1 = \sum_i b_i a_i$ for some $b_i \in K$, and therefore $\sum_i b_i(a_i + \varepsilon t_i) = 1 + \varepsilon(\sum_i b_i t_i) \in K[\varepsilon]^*$. This shows that $K[\varepsilon](a_0 + \varepsilon t_0, \dots, a_n + \varepsilon t_n)$ is a global line for any $(t_0, \dots, t_n)$. This shows that $M \in T(\mathbb{P}_k^n)_x$ is determined by $(t_0, \dots, t_n)$ up to the equivalence relation defined by

$$(t_0, \dots, t_n) \sim (t_0', \dots, t_n') \quad \text{if } (a_0 + \varepsilon t_0, \dots, a_n + \varepsilon t_n) = (a_0 + \varepsilon t_0', \dots, a_n + \varepsilon t_n') \text{ in } \mathbb{P}_k^n(K[\varepsilon]).$$

The latter means that

$$(a_0' + \varepsilon t_0', \dots, a_n' + \varepsilon t_n') = (\lambda + \mu\varepsilon)(a_0 + \varepsilon t_0, \dots, a_n + \varepsilon t_n)$$

for some $\lambda + \mu\varepsilon \in K[\varepsilon]^*$ (i.e. $\lambda \in K^*, \mu \in K$). This implies that

$$(a_0', \dots, a_n') = \lambda(a_0, \dots, a_n), \quad (t_0', \dots, t_n') = \lambda(t_0, \dots, t_n) + \mu(a_0, \dots, a_n).$$

Let L_x be the line in K^{n+1} corresponding to x. We see that a tangent vector t_x defines a homomorphism $L_x \to K^{n+1}/L_x$ by assigning to $(a_0, \ldots, a_n) \in L$ the coset of $(t_0, \ldots, t_n)$ modulo L_x. Thus there is a natural bijection

$$T(\mathbb{P}^n_k)_x \to \mathrm{Hom}_k(L_x, K^{n+1}/L_x).$$

Since the right-hand side has a natural structure of a rank n free module over K, we can transfer this structure to $T(\mathbb{P}^n_k)_x$.

Example 3. Let $X = \mathrm{GL}_{n,k}$ be the affine algebraic variety with $\mathrm{GL}_{n,k}(K) = \mathrm{GL}(n, K)$. A point of $\mathrm{GL}_{n,k}(K[\varepsilon])$ is a matrix $A + \varepsilon B$, where $A \in \mathrm{GL}(n, K), B \in \mathrm{Mat}_n(K)$.

If we take $x \in X(K)$ to be the identity matrix I_n, we obtain that $T(X)_{I_n}$ can be identified with $\mathrm{Mat}_n(K)$. Now, take $X = \mathrm{SL}_{n,k}$ with $X(K) = \mathrm{SL}(n, k)$. Then

$$T(X)_{I_n} = \{I_n + \varepsilon B \in \mathrm{GL}(n, K[\varepsilon]) : \det(I_n + \varepsilon B) = 1\} =$$

$$\{I_n + \varepsilon B \in \mathrm{GL}(n, K[\varepsilon]) : \mathrm{Trace}(B) = 0\}.$$

Thus we can identify $T(\mathrm{SL}_{n,k})_{I_n}$ with the vector space of matrices with entries in K with trace equal to zero.

Now let us take $X = \mathrm{O}_{n,k}$ with $\mathrm{O}_{n,k} = \{A \in \mathrm{Mat}_n(K) : A \cdot {}^tA = I_n\}$. We get

$$T(X)_{I_n} = \{I_n + \varepsilon B \in \mathrm{Mat}(n, K[\varepsilon]) : (I_n + \varepsilon B)(I_n + \varepsilon {}^tB) = I_n\} =$$

$$\{I_n + \varepsilon B \in \mathrm{GL}(n, K[\varepsilon]) : B + {}^tB = 0\}.$$

Thus we can identify $T(\mathrm{O}_{n,k})_{I_n}$ with the vector space of skew-symmetric matrices with entries in K. Note that the choice of K depends on identification of I_n with a K-point.

The tangent space of an algebraic group at the identity point has a structure of a *Lie algebra* defined by the Lie bracket.

Remark 1. For any functor F from the category of k-algebras to the category of sets one can define the tangent space of F at a "point" $x \in F(K)$ as the set of elements t of the set $F(K[\varepsilon])(t) = x$.

Now, if we have a projective variety X given by a system of homogeneous equations $F_1 = \cdots = F_k = 0$, we obtain that

$$T(X)_x = \{\mathbf{a} + \mathbf{b}\varepsilon \in T(\mathbb{P}^n_k)_x : F_1(\mathbf{a} + \mathbf{b}\varepsilon) = \cdots = F_k(\mathbf{a} + \mathbf{b}\varepsilon) = 0.\}$$

By using the Taylor exapnsion, as in the previous example, we obtain that $\mathbf{b} = (b_0, \ldots, b_n)$ satisfies a system of homogeneous linear equations:

$$\sum_{j=0}^{n} \frac{\partial F_i}{\partial T_j}(\mathbf{a}) b_j = 0, \quad i = 1, \ldots, k. \tag{2}$$

Recall that a tangent vector is determined by $\mathbf{b} = (b_0, \ldots, b_n)$ only up to adding a vector proportional to $\mathbf{a} = (a_0, \ldots, a_n)$. Thus $\mathbf{a}$ must satisfy the previous system of linear equations. But this is clear. For any homogeneous polynomial $F(T_0, \ldots, T_n)$ of degree d we have (easily verified) *Euler's identity*

$$dF(t_0, \ldots, T_n) = \sum_{j=0}^{n} T_i \frac{\partial F}{\partial T_j}. \tag{3}$$

This gives

$$0 = d_i F_i(a_0, \dots, a_n) = \sum_{j=0}^{n} a_i \frac{\partial F}{\partial T_j}(\mathbf{a}), \quad i = 1, \dots, k,$$

where d_i is the degree of F_i.

As we saw the tangent space of an affine or a projective variety has a structure of a linear space. However, it is not clear that this structure is independent of a choice of the system of equations defining X. To overcome this difficulty, we shall give another, more invariant, definition of $T(X)_x$.

Let A be a commutative k-algebra and let M be A-module. A M-derivation of A is a linear map of the corresponding k-linear spaces $\delta : A \to M$ such that for all $a, b \in A$

$$\delta(ab) = a\delta(b) + b\delta(a).$$

The set of M-derivations is denoted by $\mathrm{Der}_k(A, M)$. It has a natural structure of a A-module via

$$(a\delta)(b) = a\delta(b) \quad \text{for all } a, b \in A.$$

We will be interested in a special case of this definition.

Lemma 1. *If $f : A \to B$ is a homomorphism of k-algebras, and $\delta : B \to M$ is a M-derivation of B, then the composition $\delta \circ f : A \to B \to M$ is a $M_{[f]}$-derivation of A, where $M_{[f]}$ is the A-module obtained from M by the operation of restriction of scalars (i.e., $a \cdot m = f(a)m$ for any $a \in A, m \in M$).*

Proof. Trivial verification of the definition.

Let us apply this to our situation. Note that the k-linear map:

$$\alpha_2 : K[\varepsilon] \to K, a + b\varepsilon \to b$$

is a K-derivation of $K[\varepsilon]$ considered as a K-algebra. Here K is considered as a $K[\varepsilon]$-module by means of the homomorphism $\phi_1 : K[\varepsilon] \to K, a + b\varepsilon \mapsto a$. We identify a K-point $x \in X(K)$ with a homomorphism of k-algebras $ev_x : \mathcal{O}(X) \to K$, $\phi \mapsto \phi(x)$. A tangent vector $t_x \in T(X)_x$ is identified with a homomorphism $ev_{t_x} : \mathcal{O}(X) \to K[\varepsilon]$. Its composition with the derivation $\alpha_2 : K[\varepsilon] \to K, a + b\varepsilon \mapsto b$, is a K-derivation of $k[X]$. Here K is considered as a $\mathcal{O}(X)$-module via the homomorphism ev_x. This defines a map:

$$T(X)_x \to \mathrm{Der}_k(\mathcal{O}(X), K)_x$$

where the subscript x stands to remind us about the structure of a $\mathcal{O}(X)$-module on K. By definition,

$$\mathrm{Der}_k(\mathcal{O}(X), K)_x = \{\delta \in \mathrm{Hom}_k(\mathcal{O}(X), K) : \delta(pq) = p(x)\delta(q) + q(x)\delta(p) \quad \text{for any } p, q \in \mathcal{O}(X)\}.$$

Lemma 2. *The map*

$$T(X)_x \to \mathrm{Der}_k(\mathcal{O}(X), K)_x$$

is a bijection.

Proof. Let $\delta \in \mathrm{Der}_k(k[X], K)_x$. We define a map $f_\delta : \mathcal{O}(X) \to K[\varepsilon]$ by the formula:

$$f_\delta(p) = p(x) + \varepsilon\delta(p).$$

It is easy to verify that f_δ is a homomorphism, and its composition with $\alpha_1 : K[\varepsilon] \to K$ is equal to ev_x. Thus f_δ defines a tangent vector at x and the formula $\delta \mapsto f_\delta$ makes the inverse of our map.

Now $\mathrm{Der}_k(\mathcal{O}(X), K)_x$ has a structure of a K-module, defined by the formula $(a\delta)(p) = a\delta(p)$ for any $a \in K, p \in \mathcal{O}(X)$. We transfer this structure to $T(X)_x$ by means of the bijection from Lemma 2. This structure of a K-module on $T(X)_x$ is obviously independent (up to isomorphism) on the choice of equations defining X. We leave to the reader to verify that this structure agrees with the one defined in the beginning of the lecture.

Let us specialize our definition to the case when $x \in X(k)$ (a *rational point* of X). Then the kernel of the homomorphism $x : \mathcal{O}(X) \to k$ is a maximal ideal $\mathfrak{m}_x$ of $\mathcal{O}(X)$ and $\mathcal{O}(X)/\mathfrak{m}_x \cong k$. Let $\delta \in \mathrm{Der}_k(\mathcal{O}(X), k)$ be a k-derivation of $\mathcal{O}(X)$. For any $p, q \in m_x$, we have

$$\delta(p \cdot q) = p(x)\delta(q) + q(x)\delta(p) = 0.$$

Thus the restriction of δ to m_x^2 is identical zero.

Lemma 3. *Assume $x \in X(k)$. The restriction map $\delta \to \delta|\mathfrak{m}_x$, defines an isomorphism of k-linear spaces*

$$T(X)_x \to \mathrm{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k).$$

Proof. Since $\mathcal{O}(X)/m_x^2$ has a natural structure of a k-algebra there is a canonical homomorphism $k \to \mathcal{O}(X)/m_x^2$ such that its composition with the factor map $\mathcal{O}(X)/m_x^2 \to \mathcal{O}(X)/m_x = k$ is the identity. We shall identify k with the subring of $\mathcal{O}(X)/m_x^2$ by means of this map so that the restriction of the factor map $\mathcal{O}(X)/m_x^2 \to \mathcal{O}(X)/m_x$ to k is the identity. For any $p \in \mathcal{O}(X)$ we denote by p_x the residue of p mod m_x^2. Obviously, $p_x - p(x) \in m_x/m_x^2$, so that for every linear function $f \in \mathrm{Hom}_k(m_x/m_x^2, k)$ we can define the map $\delta : m_x/m_x^2 \to K$ by setting for any $p \in \mathcal{O}(X)$

$$\delta(p) = f(p_x - p(x)).$$

Since for any $p, q \in \mathcal{O}(X), (p_x - p(x))(q_x - q(x)) \in m_x^2$, we have

$$\delta(pq) = f(p_x q_x - p(x)q(x)) = f((p_x - p(x))(q_x - q(x)) + p(x)(q_x - q(x)) + q(x)(p_x - p(x))) =$$
$$= f(p(x)(q_x - q(x)) + q(x)(p_x - p(x))) = p(x)f(q_x - q(x)) + q(x)f(p_x - p(x))) = p(x)\delta(q) + q(x)\delta(p).$$

We leave to the reader to verify that the constructed map $f \mapsto \delta$ is the needed inverse.

Let $f : X \to Y$ be a morphism of algebraic k-varieties (affine or projective). Let $x \in X(K)$, and $y = f_K(x) \in Y(K)$. By definition of a morphism, the map $f_{K[\varepsilon]} : X(K[\varepsilon]) \to Y(K[\varepsilon])$ induces a natural map

$$(df)_x : T(X)_x \to T(Y)_y.$$

It is called the *differential* of f at the point x. If $f : X \to Y$ is a morphism of affine k-varieties corresponding to a homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ of k-algebras, $x \in X(K), y = f_K(x) \in Y(K)$, then, after we use the bijection from Lemma 2, it is immediately verified that the differential $(df)_x$ coincides with the map

$$\mathrm{Der}_k(\mathcal{O}(X), K)_x \to \mathrm{Der}_k(\mathcal{O}(Y), K)_y$$

defined in Lemma 1, where f is the homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$. This is obviously a K-linear map.

Proposition 1 (Chain Rule). *Let $f : X \to Y, g : Y \to Z$ be morphisms of algebraic k-varieties, $x \in X(K), y = f_(x) \in Y(K)$. Then*

$$d(g \circ f)_x = (dg)_y \circ (df)_x.$$

Proof. Immediately follows from the definition of a morphism.

Now we can define the tangent space for any quasi-projective algebraic set $V \subset \mathbb{P}^n(K)$. Here K, as usual, is a fixed algebraically closed field containing k. First, we assume that V is affine. Choose the unique affine algebraic K-variety X such that $I(X)$ is radical and $X(K) = V$. Then we define the the tangent space $T(V)_x$ of V at x by setting

$$T(V)_x = T(X)_x.$$

By Lemma 3, for every $x \in V$ we have an isomorphism of K-linear spaces.

$$T(X)_x \cong \mathrm{Der}_k(\mathcal{O}(X), K).$$

Since an isomorphism of affine varieties is defined by an isomorphism of their coordinate algebras, we see that this definition is independent (up to isomorphism of linear spaces) of a choice of equations defining X.

Lemma 4. *Let A be a commutative K-algebra, M an A-module, and S a multiplicatively close subset of A. There is an isomorphism of A_S-modules*

$$\mathrm{Der}_k(A, M)_S \cong \mathrm{Der}_k(A_S, M_S)$$

Proof. Let $\delta : A \to M$ be a derivation of A. We assign to it the derivation of A_S defined by the familiar rule:

$$\delta\big(\frac{a}{s}\big) = \frac{\delta(a)s - \delta(s)a}{s^2}.$$

This definition does not depend on the choice of a representative of the fraction $\frac{a}{s}$. In fact, assume $s''(s'a - sa') = 0$. Then

$$0 = s''\delta(s'a - sa') - (s'a - sa')\delta(s'') = s''[\delta(s'a) - \delta(sa')] + (as' - a's)\delta(s'').$$

Multiplying both sides by s'', we obtain

$$s''^2[\delta(s'a) - \delta(sa')] = 0. \tag{4}$$

Let us show that this implies that

$$s''^2[s^2(s'\delta(a') - a'\delta(s'))] = s''^2[s'^2(s\delta(a) - a\delta(s))].$$

This will proves our assertion. The previous identity is equivalent to the following one

$$s''^2[s^2s'\delta(a') - s'^2s\delta(a)] = s''^2[s^2a'\delta(s') - s'^2a\delta(s)],$$

or

$$s's s''^2[s\delta(a') - s'\delta(a)] = ss's''^2[a\delta(s') - a'\delta(s)].$$

Now this follows from equality (4) after we multiply it by ss'.

So we have defined a homomorphism of A-modules $\mathrm{Der}_k(A,M) \to \mathrm{Der}_k(A_S, M_S)$. It induces a map of A_S-modules $\mathrm{Der}_k(A,M)_S \to \mathrm{Der}_k(A_S, M_S)$. The inverse of this map is defined by using Lemma 1 applied to the homomorphism $A \to A_S$.

Let us apply the previous lemma to our situation. Let X be an affine k-variety, $x \in X(K)$, $\mathfrak{p} = \mathrm{Ker}(ev_x)$. Assume that K is a field. Then the ideal $\mathfrak{p}$ is prime since $\mathcal{O}(X)/\mathfrak{p}$ is isomorphic to a subring of K. Consider K as a module over $\mathcal{O}(X)$ by means of the homomorphism ev_x. Let $S = A \setminus \mathfrak{p}$. Then $K_S = K$ since the image of S under ev_x does not contain 0. It is easy to see that the linear K-spaces $\mathrm{Der}(A,K)_\mathfrak{p}$ and $\mathrm{Der}(A,K)$ are isomorphic (the map $\frac{\partial}{s} \mapsto ev(s)^{-1}\partial$ is the isomorphism). Applying lemma 4, we obtain an isomorphism of vector K-spaces

$$T(X)_x = \mathrm{Der}_k(A,K)_x \cong \mathrm{Der}_k(A_\mathfrak{p}, K). \tag{5}$$

The previous isomorphism suggests a definition of the tangent space of any quasi-projective algebraic k-set X.

Definition. The *local ring* of X at $x \in X$ is the factor set

$$\mathcal{O}_{X,x} = \bigcup_{x \in U} \mathcal{O}(U)/R$$

where U runs through the set of all open affine neighbourhoods of x and the equivalence relation R is defined as follows:

Let $f \in \mathcal{O}(U), g \in \mathcal{O}(V)$, then

$$f \equiv g \Longleftrightarrow f\big|W = g\big|W \quad \text{for some open affine neighborhood of } x \text{ contained in } U \cap V.$$

We shall call the equivalence class of $f \in \mathcal{O}(U)$, the *germ* of f at x. The structure of a ring in $\mathcal{O}_{X,x}$ is induced by the ring structure of any $\mathcal{O}(U)$. We take two elements of $\mathcal{O}_{X.x}$, represent them by regular functions on a common open affine subset, multiply or add them, and take the germ of the result. Let $\mathfrak{m}_{X,x}$ be the ideal of germs of functions $f \in \mathcal{O}(U)$ which vanish at x.

It follows from the definition that, for any open affine neighborhood U of x, the natural map $\mathcal{O}(U) \to \mathcal{O}_{X,x}, \phi \mapsto \phi_x$ defines an isomorphism

$$\mathcal{O}_{U,x} \cong \mathcal{O}_{X,x}.$$

Lemma 5. *(i) $m_{X,x}$ is the unique maximal ideal of $\mathcal{O}_{X,x}$.*

(ii) If X is affine and irreducible, the canonical homomorphism $\mathcal{O}(X) \to \mathcal{O}_{X,x}$ induces an isomorphism $\mathcal{O}(X)_\mathfrak{p} \cong \mathcal{O}_{X,x}$, where $\mathfrak{p}_x = \mathrm{Ker}(ev_x)$.

(iii) If X is affine, the canonical homomorphism $\mathcal{O}(X) \to \mathcal{O}_{X,x}$ induces an isomorphism of fields $k(x) := Q(\mathcal{O}(X)/\mathfrak{p}_x) \to \mathcal{O}_{X,x}/\mathfrak{m}_{X,x}$.

Proof. (i) It suffices to show that every element $\alpha \in \mathcal{O}_{X,x} \setminus m_{X,x}$ is invertible. Let $\alpha = f_x$, where f is regular on a some open affine set U containing x. Since $f(x) \neq 0, x$ is contained in the open principal affine subset $V = D(f)$ of U. Hence the restriction g of f to V is invertible in $\mathcal{O}(V)$. The germ $g_x = f_x$ is now invertible.

(ii) For any $\phi \in \mathcal{O}(X) \setminus \mathfrak{p}_x$ its germ in $\mathcal{O}_{X,x}$ is invertible. By the universal property of localizations, this defines a homomorphism $\mathcal{O}(X)_{\mathfrak{p}_x} \to \mathcal{O}_{X,x}$. An element of the kernel of this

homomorphism is a function whose restriction to some open neighborhood of x is identically zero. Since X is irreducible, this implies that the function is zero. Let $f_x \in \mathcal{O}_{X,x}$ be the germ of a function $f \in \mathcal{O}(U)$, where U is an open affine neighborhood of x. Replacing U by a principal open subset $D(\phi) \subset U$, we may assume that $U = D(\phi)$ and $f = F/\phi^n$, where $F, \phi \in \mathcal{O}(X)$. Since $\phi(x) \neq 0$, we get that ϕ does not belong to $\mathfrak{p}_x$, and hence $f \in \mathcal{O}(X)_{\mathfrak{p}_x}$ and its germ at x equals f_x. This proves the surjectivity.

(iii) This follows easily from the definition of the localization ring $A_\mathfrak{p}$ for any ring A and a prime ideal $\mathfrak{p}$. The homomorphism $A \to A_\mathfrak{p}, a \mapsto \frac{a}{1}$ defines a homomorphism $A/\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. The target space is a field. By the universal property of fields of fractions, we get a homomorphism of fields $g : Q(A/\mathfrak{p}) \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Let $\frac{a}{s} + \mathfrak{p}A_\mathfrak{p} \in A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Then it is the image of the fraction $\frac{a+\mathfrak{p}}{s+\mathfrak{p}} \in Q(A/\mathfrak{p})$. This shows that g is bijective.

The previous isomorphism allows us to define the tangent space for any quasi-projective k-set X by

$$T(X)_x = \mathrm{Der}_k(\mathcal{O}_{X,x}, K). \tag{6}$$

In the case when $x \in X(k)$, choosing an open affine neighborhood of x and applying Proposition 2, we obtain

$$T(X)_x = \mathrm{Hom}_k(\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2, k). \tag{7}$$

For any rational point $x \in X(k)$, the right-hand side of (7) is called the *Zariski tangent space* of X at x.

Let $f : X \to Y$ be a regular map of algebraic k-sets, $x \in X$ and $y = f(x)$. Let V be an open affine neighborhood of y and U bean open affine neighborhood of x contained in $f^{-1}(V)$. The restriction of f to U defines a regular map $f : U \to V$. For any $\phi \in \mathcal{O}(V)$, the composition with f defines a regular function $f^*(\phi)$ on U. Let $f^*(\phi)_x \in \mathcal{O}_{U,x}$ be its germ at x. The homomorphism $f^* : \mathcal{O}(V) \to \mathcal{O}_{U,x}$ extends to a homomorphism $f^* : \mathcal{O}_{V,y} \to \mathcal{O}_{U,x}$ of the local rings. It is clear that $f^*(\mathfrak{m}_{V,y}) \subset \mathfrak{m}_{U,x}$. Composing this homomorphism with the isomorphisms $\mathcal{O}_{X,x} \cong \mathcal{O}_{U,x}$ and $\mathcal{O}_{Y,y} \cong \mathcal{O}_{V,y}$ we get a homomorphism of local rings

$$f_{x,y}^* : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}. \tag{8}$$

Applying Lemma 1, we get a K-linear map

$$T_{X,x} = \mathrm{Der}_k(\mathcal{O}_{X,x}, K) \to T_{Y,y} = \mathrm{Der}_k(\mathcal{O}_{Y,y}, K),$$

which we call the *differential* of f at the point x and denote by df_x.

Let $X \subset \mathbb{P}_k^n(K)$ be an quasi-projective algebraic k-set and $T(X)_x$ be the tangent space at its point $x \in X(K)$. It is a vector space over K of finite dimension. In fact, it is a subspace of $T(\mathbb{P}^n(K))_x \cong K^n$ and hence

$$\dim_K T(X)_x \leq n. \tag{9}$$

If x is contained in an affine open subset U which is isomorphic to a closed subset of some $\mathbf{A}^n(K)$, then $T(X)_x$ is a subspace of $T(\mathbf{A}^n(K))_x \cong K^n$ and

$$\dim_K T(X)_x \leq n.$$

It follows from (9) that X is not isomorphic to a quasi-projective subset of $\mathbb{P}_k^n(K)$ for any $n < \dim_K T(X)_x$.

Example 4. Let X be the union of the three coordinate axes in $\mathbf{A}^3(K)$. It is given by the system

$$Z_1Z_2 = Z_1Z_3 = Z_2Z_3 = 0.$$

The tangent space at the origin $x = (0,0,0)$ is the whole tangent space $T(\mathbb{A}^3(K))_x \cong K^3$. Thus $\dim_K T(X)_x = 3$. This shows that X is not isomorphic to the union of three lines in $\mathbb{A}^2(K)$.

Let us now show that $\dim_K T(X)_x \geq \dim X$ for any irreducible algebraic set X and the equality takes place for almost all points x (i.e., for all points belonging to a Zariski open subset of X). For this, we may obviously assume that X is affine.

Let $V = X(K)$ for some affine variety defined by a radical ideal in $k[Z_1, \ldots, Z_n]$. The set $T(V) = X(K[\varepsilon])$ is a subset of $K[\varepsilon]^n$ which can be thought as the vector space K^{2n}. It is easy to see that $T(X)$ is a closed algebraic subset of K^{2n} and the map $p = X(\phi) : T(X) \to X$, is a regular map (check it !). Note that the fibre $p^{-1}(x)$ is equal to the tangent space $T(X)_x$. Applying the theorem about the dimension of fibres of a regular map, we obtain

Proposition 3. *There exists a number d such that*

$$\dim_K T(X)_x \geq d$$

and the equality takes place for all points x belonging to an open subset of X.

We will show that the number d from above is equal to $\dim X$.

Lemma 6. *Let K be an algebraically closed field of characteristic p. Let $F \in K[Z_1, \ldots, Z_n]$ with all the partial derivatives $\partial F/\partial Z_i$ equal to zero. If $p = 0$, then F is a constant polynomial. If $p > 0$, then $F = G^p$ for some polynomial G.*

Proof. Write $F = \sum_{\mathbf{r}} a_{\mathbf{r}} Z^{\mathbf{r}}$. Then

$$\frac{\partial F}{\partial Z_i} = \sum_{\mathbf{r}} a_{\mathbf{r}}(\mathbf{r} \bullet \mathbf{e}_i) Z^{\mathbf{r}-\mathbf{e}_i}$$

where $\bullet$ denotes the dot product of vectors and $\mathbf{e}_i$ is the i-th unit vector. If this polynomial is equal to zero, then $a_{\mathbf{r}}(\mathbf{r} \bullet \mathbf{e}_i) = 0$ for all r. Assume that $a_{\mathbf{r}} \neq 0$. If $\mathrm{char}(k) = 0$ this implies that $\mathbf{r} \bullet \mathbf{e}_i = 0$. In particular, if all $\frac{\partial F}{\partial Z_i} = 0$, we get $\mathbf{r} = 0$, i.e., F is a constant polynomial. If $\mathrm{char}(k) = p > 0$, we obtain that p divides $\mathbf{r} \bullet \mathbf{e}_i$, i.e., $\mathbf{r} = p\mathbf{r}'$ for some vector r'. Thus

$$F = \sum_{\mathbf{r}} a_{\mathbf{r}} Z^{\mathbf{r}} = \sum_{\mathbf{r}} a_{\mathbf{r}} (Z^{\mathbf{r}'})^p = (\sum_{\mathbf{r}} a_{\mathbf{r}}^{1/p} Z^{\mathbf{r}'})^p = G^p,$$

where $G = \sum_{\mathbf{r}} a_{\mathbf{r}}^{1/p} Z^{\mathbf{r}'}$.

Theorem 1. *Let X be an irreducible algebraic set and $d = \min\{T(X)_x\}$. Then*

$$d = \dim X.$$

Proof. Obviously, it suffices to find an open subset U of X where $\dim_K T(X)_x = \dim X$ for all $x \in U$. Replacing X by an open affine set, we may assume that X is isomorphic to an open subset of a hypersurface $V(F) \subset \mathbb{A}^n(K)$ for some irreducible polynomial F (Theorem 2 of Lecture

4). This shows that we may assume that $X = V(F)$. For any $x \in X$, the tangent space $T(X)_x$ is given by one equation

$$\frac{\partial F}{\partial Z_1}(x)b_1 + \ldots + \frac{\partial F}{\partial Z_n}(x)b_n = 0.$$

Clearly, its dimension is equal to $n-1 = \dim X$ unless all the coefficients are zeroes. The set of common zeroes of the polynomials $\frac{\partial F}{\partial Z_i}$ is a closed subset of $\mathbb{A}^n(K)$ contained in each hypersurface $V(\frac{\partial F}{\partial Z_i})$. Obviously $\frac{\partial F}{\partial Z_i} \notin (F)$ unless it is equal to zero (compare the degrees). Now the assertion follows from Lemma 6.

Obviously, the assertion of the previous theorem is not true for a reducible set. To see this it is sufficient to consider the union of two sets of different dimension. It is easy to modify the statement to extend it to the case of reducible sets.

Definition. The dimension of X at a point x is the maximum $\dim_x X$ of the dimensions of irreducible components of X containing x.

Corollary. *Let X be an algebraic set and $x \in X$. Then*

$$\dim_K T(X)_x \geq \dim_x X.$$

Proof. Let Y be an irreducible component of X containing x. Obviously $T(Y)_x \subset T(X)_x$. Hence

$$\dim_x Y \leq \dim_K T(Y)_x \leq \dim_K T(X)_x.$$

This proves the assertion.

Definition. A point x of an algebraic set X is said to be *nonsingular* (or *simple*, or *smooth*) if $\dim_K T(X)_x = \dim_x X$. Otherwise, it is said to be *singular*. An algebraic set X is said to be nonsingular (or smooth) if all its points are nonsingular. Otherwise X is said to be singular.

We already know how to recognize whether a point is nonsingular.

Theorem 2. *(The Jacobian criterion of a nonsingular point). Assume that X is an affine algebraic k-set given by a system of equations $F_1(Z) = \ldots = F_r(Z) = 0$ in $\mathbb{A}^n(K)$. Then $x \in X$ is nonsingular if and only if $\mathrm{rk}\ J(x) = n - \dim_x X$, where*

$$J(x) = \begin{pmatrix} \frac{\partial F_1}{\partial Z_1}(x) & \ldots & \frac{\partial F_1}{\partial Z_n}(x) \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \frac{\partial F_r}{\partial Z_1}(x) & \ldots & \frac{\partial F_r}{\partial Z_n}(x) \end{pmatrix}.$$

Problems.

1. Assume $k = K$ is algebraically closed field of characteristic 0. Show that, up to a projective automorphism of $\mathbb{P}^2(K)$, there are only two irreducible singular plane cubic curves.
2. Prove that $T(X \times Y)(x, y) \cong T(X)_x \oplus T(Y)_y$. Using this show that if x is a nonsingular point of X and y is a nonsingular point of Y, then (x, y) is a nonsingular point of $X \times Y$.
3. Let X be a closed subset of $\mathbf{A}^n(K), x = (a_1, \ldots, a_n) \in X$ and $f : \mathbb{A}^1(K) \to \mathbb{A}^n(K)$ given by $t \mapsto (b_1 t + a_1, \ldots, b_n t + a_n)$. Let (Z^r) be the ideal of $\mathcal{O}(\mathbb{A}^1(K)) \cong k[Z]$ generated by the functions $f^*(\phi), \phi \in I(X)$. Show that $(a_1 + b_1\varepsilon, \ldots, a_n + b_n\varepsilon) \in K[\varepsilon]^n$ is a tangent vector of X if and only if $r > 1$. Note that r can be interpreted as the intersection multiplicity of X and the line $f(\mathbb{A}^1(K))$ at x.
4. Suppose a hypersurface $X = V(F)$ of degree > 1 in $\mathbb{P}^n(K)$ contains a linear subspace E of dimension $r \geq n/2$. Show that X has singular points contained in E.
5. Find singular points of the Steiner quartic $V(T_0^2T_1^2 + T_1^2T_2^2 + T_0^2T_2^2 - T_0T_1T_2T_3)$ in $\mathbb{P}^3(K)$.
6. Let X be a surface in $\mathbb{P}^3(K)$. Assume that X contains three nocoplanar lines passing through a point $x \in X$. Show that this point is singular.
7. Let $G_k(r + 1, n + 1)$ be the Grassmann variety over k. For every $M \in G_k(r + 1, n + 1)(K)$ show that the tangent space of $G_k(r + 1, n + 1)$ at M is naturally identified with $\mathrm{Hom}_K(M, K^{n+1}/M)$.

Lecture 14. LOCAL PARAMETERS

In this lecture we will give some other properties of nonsingular points. As usual we fix an algebraically closed field K containing k and consider quasi-projective algebraic k-sets, i.e. locally closed subsets of projective spaces $\mathbb{P}^n_k(K)$.

Recall that a point $x \in X$ is called nonsingular if $\dim_K T(X)_x = \dim_x X$. When $x \in X(k)$ is a rational point, we know that $T(X)_x \cong \mathrm{Hom}_k(m_{X,x}/m^2_{X,x}, K)$. Thus a rational point is nonsingular if and only if

$$\dim_k m_{X,x}/m^2_{X,x} = \dim_x X.$$

Let us see first that $\dim_x X = \dim \mathcal{O}_{X,x}$.

The number $\dim \mathcal{O}_{X,x}$ is denoted often by $\mathrm{codim}_x X$ and is called the codimension of the point x in X. The reason is simple. If X is affine and $\mathfrak{p}_x = \mathrm{Ker}(\mathrm{ev}_x)$, then we have

$$\dim \mathcal{O}(X)_{\mathfrak{p}} = \sup\{r : \exists \text{strictly decreasing chain } \mathfrak{p}_x = \mathfrak{p}_0 \supset \ldots \supset \mathfrak{p}_r \text{ of prime ideals in } \mathcal{O}(X)\}.$$

This follows from the following.

Lemma 1. *Let $\mathfrak{p}$ be a prime ideal in a ring A. Then*

$$\dim A_{\mathfrak{p}} = \sup\{r : \exists \textit{strictly decreasing chain } \mathfrak{p} = \mathfrak{p}_0 \supset \ldots \supset \mathfrak{p}_r \textit{ of prime ideals in } A\}.$$

Proof. Let $\mathfrak{q}_r \subset \ldots \subset \mathfrak{q}_0$ be the largest increasing chain of prime ideals in $A_{\mathfrak{p}}$. We may assume that $\mathfrak{q}_0$ is the maximal ideal $\mathfrak{m}$ of A. Let $\mathfrak{p}_i$ be the pre-image of $\mathfrak{q}_i$ in A under the natural homomorphism $A \to A_{\mathfrak{p}}$. Since $\mathfrak{p}_0 = \mathfrak{p}$, we get a chain of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \supset \ldots \supset \mathfrak{p}_r$. Conversely, any chain of such ideals in A generates an increasing chain of prime ideals in $A_{\mathfrak{p}}$. It is easy to see that $\mathfrak{p}_i A_{\mathfrak{q}} = \mathfrak{p}_{i+1} A_{\mathfrak{p}}$ implies $\mathfrak{p}_i = \mathfrak{p}_{i+1}$. This proves the assertion.

In commutative algebra the dimension of $A_{\mathfrak{p}}$ is called the *height* of the prime ideal $\mathfrak{p}$.

Proposition 1.

$$\mathrm{codim}_x X + \mathrm{algdim}_k\ k(x) = \dim_x X.$$

Proof. We use induction on $\dim_x X$. Let $\mathfrak{p} = \mathrm{Ker}(\mathrm{ev}_x)$. If $\dim_x X = 0$, X consists of finitely many points, $\mathfrak{p}$ is a maximal ideal, $k(x)$ is algebraic over k, and $\mathrm{codim}_x X = 0$. This checks the assertion in this case. Assume the assertion is true for all pairs (Y, y) with $\dim_y Y < \dim_x X$. If

$\mathfrak{p} = \{0\}$, then $k(x) = Q(\mathcal{O}(X))$ and $\text{algdim}_k\ k(x) = \dim X$. Obviously, $\text{codim}_x X = 0$. This checks the assertion in this case. Assume that $\mathfrak{p} \neq \{0\}$. Let X' be an irreducible component of X of dimension $\dim_x X$ which contains x. Take an nonzero element $\phi \in \mathfrak{p}$ which does not vanish on X' and consiser the closed subset $V(\phi)$ of X' containing x. By Krull's Theorem, the dimension of each irreducible component of $V(\phi)$ is equal to $\dim X' - 1 = \dim_x X - 1$. Let Y be an irreducible component of $V(\phi)$ containing x and let $\mathfrak{q}$ be the prime ideal in $\mathcal{O}(X)$ of functions vanishing on Y. There exists a strictly decreasing chain of length $\text{codim}_x Y$ of prime ideals in $\mathcal{O}(Y)$ descending from the image of $\mathfrak{p}$ in $\mathcal{O}(Y) = \mathcal{O}(X)/\mathfrak{q}$. Lifting these ideals to prime ideals in $\mathcal{O}(X)$ and adding $\mathfrak{q}$ as the last ideal we get a chain of lenghth $1 + \text{codim}_x Y$ of prime ideals in $\mathcal{O}(X)$ descending from $\mathfrak{p}$. By induction,

$$\text{codim}_x Y + \text{algdim}_k\ k(x) = \dim_x Y = \dim\ X - 1.$$

Under the natural homomorphism $\mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$, the maximal ideal $\mathfrak{m}_{X,x}$ generates the maximal ideal $\mathfrak{m}_{Y,x}$. This easily implies that the residue field of x in X and in Y are isomorphic. This gives

$$\text{codim}_x X + \text{algdim}_k\ k(x) \geq 1 + \text{codim}_x Y + \text{algdim}_k\ k(x) = 1 + \dim_x X - 1 = \dim_x X. \qquad (1)$$

Recall that $\text{algdim}_k\ k(x) = \dim \mathcal{O}(X)/\mathfrak{p}$. Any increasing chain of prime ideals in $\mathcal{O}(X)/\mathfrak{p}$ can be lifted to an increasing chain of prime ideals in $\mathcal{O}(X)$ beginning at $\mathfrak{p}$, and after adding a chain of prime ideals descending from $\mathfrak{p}$ gives an increasing chain of prime ideals in $\mathcal{O}(X)$. This shows that $\text{codim}_x X + \text{algdim}_k\ k(x) \leq \dim_x X$. Together with the inequality (1), we obtain the assertion.

Corollary. *Assume that $k(x)$ is an algebraic extension of k. Then*

$$\dim \mathcal{O}_{X,x} = \dim_x X.$$

Now we see that a rational point is nonsingular if and only if

$$\dim_k \mathfrak{m}_{X,x}/m_{X,x}^2 = \dim \mathcal{O}_{X,x}.$$

Proposition 2. *Let $(A, \mathfrak{m})$ be a Noetherian local ring. Then*

$$\dim_\kappa \mathfrak{m}/\mathfrak{m}^2 \geq \dim A.$$

Proof. We shall prove it only for geometric local rings, i.e., when $A \cong B_\mathfrak{p}$, where B is a finitely generated k-algebra B and $\mathfrak{p}$ is a prime ideal in B. This will be enough for our applications. Thus we may assume that $B = \mathcal{O}(X)$ for some affine algebraic k-variety X and $\mathfrak{p}$ corresponds to some irreducible subvariety Y of X. Let K be some algebraically closed field containing the field of fractions $Q(\mathcal{O}(X)/\mathfrak{p})$. The canonical homomorphism $\mathcal{O}(X) \to \mathcal{O}(X)/\mathfrak{p} \to Q(\mathcal{O}(X)/\mathfrak{p}) \to K$ defines a point x of the algebraic k-set $X(K)$ with $k(x) = Q(\mathcal{O}(X)/\mathfrak{p})$. Thus we see that any geometric local ring is isomorphic to the local ring $\mathcal{O}_{X,x}$ of some affine algebraic k-set and its point x.

Let X_1 be an irreducible component of $X(K)$ of dimension equal to $\dim X$ which contains x. Since $\text{alg.dim}_k \mathcal{O}(X)/\mathfrak{p} = \dim \mathcal{O}(X)/\mathfrak{p} = \dim Y$, we see that

$$\dim \mathcal{O}_{X,x} = \dim_x X - \dim Y = \dim X_1 - \dim Y.$$

Suppose $a_1, \ldots, a_n$ generate the maximal ideal of $\mathcal{O}_{X,x}$. Let U be an open affine neighborhood of x such that $a_1, \ldots, a_n$ are represented by regular functions $\phi_1, \ldots, \phi_n$ on U. Clearly, $Y \cap$

$U = V(\phi_1, \ldots, \phi_n)$. Applying Krull's Hauptsatz, we obtain that $\dim Y = \dim V(\phi_1, \ldots, \phi_n) \geq \dim X_1 - n$. This implies $\dim \mathcal{O}_{X,x} = \dim X_1 - \dim Y \leq n$ which proves the assertion. In fact, this proof gives more. By choosing elements from $\phi_1, \ldots, \phi_n$ such that each ϕ does not vanish on any irreducible component of $V(\phi_1, \ldots, \phi_{i-1})$ containing x, we obtain that $V(\phi_1, \ldots, \phi_n) = \dim Y$, where $n = \operatorname{codim}_x X$. Thus, Y is an irreducible component of $V(\phi_1, \ldots, \phi_n)$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be prime ideals corresponding to other irreducible components of $V(\phi_1, \ldots, \phi_n)$. Let U be an open subset of X obtained by deleting the irreducible components of $V(\phi_1, \ldots, \phi_n)$ different from Y. Then, replacing X with U, we may assume that $V(\phi_1, \ldots, \phi_n) = Y$. Thus $\mathfrak{p} = \operatorname{rad}(\phi_1, \ldots, \phi_n)$ and replacing ϕ_i's with their germs a_i in $\mathcal{O}_{X,x}$ we obtain that $\mathfrak{m} = \operatorname{rad}(a_1, \ldots, a_n)$.

Definition A Noetherian local ring (A with maximal ideal $\mathfrak{m}$) and residue field $\kappa = A/\mathfrak{m}$ is called *regular* if $\dim_\kappa(\mathfrak{m}/\mathfrak{m}^2) = \dim A$.

Thus a rational point x is nonsingular if and only if the local ring $\mathcal{O}_{X,x}$ is regular.

For any point $x \in X$ (not necessary rational) we define the Zariski tangent space to be

$$\Theta(X)_x = \operatorname{Hom}_{k(x)}(\mathfrak{m}_{X,x}/m_{X,x}^2, k(x))$$

considered as a vector space over the residue field $k(x) = \mathcal{O}_{X,x}/\mathfrak{m}_{X,x}$.

We define the embedding dimension of X at x by setting

$$\operatorname{embdim}_x X = \dim_{k(x)} \Theta(X)_x.$$

Note that for a rational point we have

$$T(X)_x = \Theta(X)_x \otimes_k K. \tag{2}$$

In particular, for a rational point x we have

$$\dim_K T(X)_x = \operatorname{embdim}_x X. \tag{3}$$

Definition. A point $x \in X$ is called *regular* if $\mathcal{O}_{X,x}$ is a regular local ring, i.e.

$$\operatorname{embdim}_x X = \operatorname{codim}_x X.$$

Remark 1. We know that a rational point is regular if and only if it is regular. In fact, any nonsingular point is regular (see next Remark) but the converse is not true. Here is an example. Let k be a field of characteristic 2 and $a \in k$ which is not a square. Let X be defined in $\mathbb{A}_k^2(K)$ by the equation $Z_1^2 + Z_2^3 + a = 0$. Taking the partial derivatives we see that $(\sqrt{a}, 0) \in K^2$ is a singular point. On the other hand, the ring $\mathcal{O}_{X,x}$ is regular of dimension 1. In fact, the ideal $\mathfrak{p} = \operatorname{Ker}(\operatorname{ev}_x)$ is a maximal ideal generated by the cosets of $Z_1^2 + a$ and Z_2. But the first coset is equal to the coset of Z_2^3, hence $\mathfrak{p}$ is a principal ideal generated by Z_2. Thus $m_{X,x}$ is generated by one element and $\mathcal{O}_{X,x}$ is a regular ring of dimension 1.

Remark 2. If x is not a rational point, the equality (3) may not be true. For example, let $k = \mathbb{C}$, K be the algebraic closure of the field $k(t)$ and consider $X = \mathbb{A}_k(K)$. A point $x = t$ defines the prime ideal $\mathfrak{p} = \{0\} = \operatorname{Ker}(\operatorname{ev}_x)$ (because t is not algebraic over k). The local ring $\mathcal{O}_{X,x}$ is isomorphic to the field of fractions of $k[Z_1]$. Hence its maximal ideal is the zero ideal and the Zariski tangent space is 0-dimensional. However, $\dim_K T(X)_x = 1$ since X is nonsingular of dimension 1. Thus $\Theta(X)_x \neq T(X)_x$.

However, it is true that a nonsingular point is regular if we assume that $k(x)$ is a separable extension of k (see Remark 6 later).

Let us give another characterization of a regular local ring in terms of generators of its maximal ideal.

Lemma 2 (of Nakayama). *Let A be a local ring with maximal ideal m, and let M be a finitely generated A-module. Assume that $M = N + mM$ for some submodule N of M. Then $M = N$.*

Proof. Replacing M by the factor module M/N, we may assume that $N = 0$. Let $f_1, \ldots, f_r$ be a set of generators of M. Since $mM = M$, we may write

$$f_i = \sum_{j=1}^{r} a_{ij} f_j, \quad i = 1, \ldots, r,$$

for some a_{ij} in m. Let $R = (a_{ij})$ be the matrix of coefficients. Since $(f_1, \ldots, f_r)$ is a solution of the homogeneous system of equations $R \cdot x = 0$, by Cramer's rule,

$$\det(R) f_i = 0, i = 1, \ldots, r.$$

However, $\det(R) = (-1)^r + a$ for some $a \in m$ (being the value of the characteristic polynomial of R at 1). In particular $\det(R)$ is invertible in A. This implies that $f_i = 0$ for all i, i.e., $M = \{0\}$.

Corollary 1. *Let A be a local Noetherian ring and m be its maximal ideal. Elements $a_1, \ldots, a_r$ generate m if and only if their residues modulo m^2 span m/m^2 as a vector space over $k = A/m$. In particular, the minimal number of generators of the maximal ideal m is equal to the dimension of the vector space m/m^2.*

Proof. Let $M = m, N = (a_1, \ldots, a_r)$. Since A is Noetherian, M is a finitely generated A-module and N its submodule. By the assumption, $M = mM + N$. By the Nakayama lemma, $M = N$.

Corollary 2. *The maximal ideal of a Noetherian local ring of dimension n cannot be generated by less than n elements.*

Proof. This follows from Proposition 2.

Definition A *system of parameters* in a local ring A is a set of $n = \dim A$ elements $(a_1, \ldots, a_n)$ generating an ideal whose radical is the maximal ideal, i.e.,

$$\mathfrak{m}^s \subset (a_1, \ldots, a_n) \subset \mathfrak{m}$$

for some $s > 0$).

It follows from the proof of Proposition 2 that local rings $\mathcal{O}_{X,x}$ always contain a system of parameters. A local ring is regular, if and only if it admits a system of parameters generating the maximal ideal. Such system of parameters is called a *regular system of parameters.*

Let $a_1, \ldots, a_n$ be a system of parameters in $\mathcal{O}_{X,x}$, Choose an U be an open affine neighborhhod of x such that $a_1, \ldots, a_n$ are represented by some regular functions $\phi_1, \ldots, \phi_n$ on U. Then $V(\phi_1, \ldots, \phi_n) \cap U$ is equal to the closure of x in U corresponding to the prime ideal $\mathfrak{p} \subset \mathcal{O}(U)$ such that $\mathcal{O}_{X,x} \cong \mathcal{O}(U)_{\mathfrak{p}}$). In fact, the radical of $(\phi_1, \ldots, \phi_n)$ must be equal to $\mathfrak{p}$.

Examples. 1. Let X be given by the equation $Y^2 + X^3 = 0$ and $x = (0, 0)$. The maximal ideal $m_{X,x}$ is generated by the residues of the two unknowns. It is easy to see that this ideal is not principal. The reason is clear: x is a singular point of X and $\mathrm{embdim}_x X = 2 > \dim_x X = 1$. On

the other hand, if we replace X by the set given by the equation $Y^2 + X^3 + X = 0$, then $m_{X,x}$ is principal. It is generated by the germ of the function Y. Indeed, $Y^2 = -X(X^2+1)$ and the germ of X^2+1 at the origin is obviously invertible. Note that the maximal ideal $m(X)_x$ of $\mathcal{O}(X)$ is not principal.

2. Let $x = (a_1, \dots, a_n) \in k^n \subset X = \mathbb{A}^n_k(K)$. The germs of the polynomials $Z_i - a_i, i = 1, \dots, n$, form a system of parameters at the point x. For any polynomial $F(Z_1, \dots, Z_n)$ we can write

$$F(Z_1, \dots, Z_n) = F(x) + \sum_{i=1}^{n} \frac{\partial F}{\partial Z_i}(x)(Z_i - a_i) + G(Z_1, \dots, Z_n),$$

where $G(Z_1, \dots, Z_n) \in m_x^2$. Thus the cosets dZ_i of $Z_i - a_i \bmod m_{X,x}^2$ form a basis of the linear space $m_{X,x}/m_{X,x}^2$ and the germ $F_x - F(x) = F(Z_1, \dots, Z_n) - F(x) \bmod m_{X,x}^2$ is a linear combination of $dZ_1, \dots, dZ_n$ with the coefficients equal to the partial derivatives evaluated at x. Let $\frac{\partial}{\partial Z_i}$ denote the basis of $T(X)_x$ dual to the basis $dZ_1, \dots, dZ_n$. Then the value of the tangent vector $\sum_i \alpha_i \frac{\partial}{\partial Z_i}$ at $F_x - F(x)$ is equal to

$$\sum_{i=1}^{n} \alpha_i \frac{\partial F}{\partial Z_i}(x).$$

This is also the value at F of the derivation of $k[Z_1, \dots, Z_n]$ defined by the tangent vector $\sum_i \alpha_i \frac{\partial}{\partial Z_i}$.

Let $f : X = \mathbb{A}^n(K) \to Y = \mathbb{A}^m(K)$ be a regular map given by a homomorphism

$$k[T_1, \dots, T_m] \to k[Z_1, \dots, Z_n], T_i \to P_i(Z_1, \dots, Z_n).$$

Let $\partial_x = \sum_i \alpha_i \frac{\partial}{\partial Z_i} \in T(X)_x$, then

$$(df)_x(\partial_x)(T_i) = \partial_x(f^*(T_i)) = \partial_x(P_i(Z_1, \dots, Z_n)) =$$

$$= \sum_{j=1}^{n} \alpha_j \frac{\partial P_i}{\partial Z_j}(x) = \sum_{k=1}^{m} \sum_{j=1}^{n} \alpha_j \frac{\partial P_i}{\partial Z_j}(x) \frac{\partial}{\partial T_k}(T_i).$$

From this we infer that the matrix of the differential $(df)_x$ with respect to the bases $\frac{\partial}{\partial Z_1}, \dots, \frac{\partial}{\partial Z_n}$ and $\frac{\partial}{\partial T_1}, \dots, \frac{\partial}{\partial T_m}$ of $T(X)_x$ and $T(Y)_{f(x)}$, respectively, is equal to

$$\begin{pmatrix} \frac{\partial P_1}{\partial Z_1} & \dots & \frac{\partial P_1}{\partial Z_n} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \frac{\partial P_m}{\partial Z_1} & \dots & \frac{\partial P_m}{\partial Z_n} \end{pmatrix}.$$

Let $f : X \to Y$ be a regular map of algebraic sets. Recall that for every $x \in X$ with $y = f(x)$ we have a homomorphism of local rings

$$f^*_{x,y} : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}.$$

Since $f_x^*(m_{Y,y}) \subset m_{X,x}$, we can define a homomorphism $\mathcal{O}_{Y,y}/\mathfrak{m}_{Y,y} \to \mathcal{O}_{X,x}/\mathfrak{m}_{X,x}$ and passing to the fields of quotienst we obtain an extension of fields $k(x)/k(y)$. Also, $f^*_{x,y}$ induces a linear map $m_{Y,y}/m_{Y,y}^2 \to m_{X,x}/m_{X,x}^2$, where the target space is considered as a vector space over the subfield

$k(y)$ of $k(x)$, or equivalently a linear map of $k(x)$-spaces $\left(m_{Y,y}/m_{Y,y}^2\right) \otimes_k (y)k(x) \to m_{X,x}/m_{X,x}^2$ The transpose map defines a linear map of the Zariski tangent spaces

$$df_x^{\mathrm{zar}} : \Theta(X)_x \to \Theta(Y)_y \otimes_{k(y)} k(x). \tag{5}$$

It is called the (Zariski) *differential* of f at the point x.

Let Y be a closed subset of X and $f : Y \to X$ be the inclusion map. Let $U \subset X$ be an affine open neighborhood of a point $x \in X$ and let $\phi_1, \ldots, \phi_r$ be equations defining Y in U. The natural projection $\mathcal{O}(X \cap U) \to \mathcal{O}(Y \cap U) = \mathcal{O}(U \cap X)/(\phi_1, \ldots, \phi_r)$ defines a surjective homomorphism $\mathcal{O}_{X,x} \to \mathcal{O}_{Y,x}$ whose kernel is generated by the germes a_i of the functions ϕ_i. Let $\bar{a}_i$ be the residue of a_i modulo $m_{X,x}^2$. Then $f_{x,y}^*$ defines a surjective map $m_{X,x}/m_{X,x}^2 \to m_{Y,x}/m_{Y,x}^2$ whose kernel is the subspace E spanned by $\bar{a}_1, \ldots, \bar{a}_r$. The differential map is the inclusion map

$$\Theta(Y)_x \cong E^\perp = \{l \in \Theta(X)_x : l(E) = \{0\}\} \to T(X)_x. \tag{6}$$

This shows that we can identify $\Theta(Y)_x$ with a linear subspace of $\Theta(X)_x$. Let

$$\mathrm{codim}(\Theta(Y)_x, \Theta(X)_x) = \mathrm{dim}\Theta(X)_x - \mathrm{dim}\Theta(Y)_x,$$

$$\mathrm{codim}_x(Y, X) = \mathrm{codim}_x X - \mathrm{codim}_x Y,$$

$$\delta_x(Y, X) = \mathrm{codim}_x(Y, X) - \mathrm{codim}(\Theta(Y)_x, \Theta(X)_x). \tag{7}$$

Then

$$\mathrm{dim}\Theta(Y)_x - \mathrm{codim}_x Y = \mathrm{dim}\Theta(X)_x - \mathrm{codim}_x X + \delta_x(Y, X).$$

Thus we obtain

Proposition 3. *Let Y be a closed subset of X and $x \in Y$. Assume x is a regular point of X, then $\delta_x(Y, X) \geq 0$ and x is a regular point of Y if and only if $\delta_x(Y, X) = 0$.*

In particular, x is a regular point of Y if and only if the cosets of the germs of the functions defining X in an neighborhood of x modulo $m_{X,y}^2$ span a linear subspace of codimension equal to $\mathrm{codim}_x X - \mathrm{codim}_x X$. Applying Nakayama's Lemma, we see that this is the same as saying that X can be locally defined by $\mathrm{codim}_x X - \mathrm{codim}_x X$ equations in an open neighborhood of x whose germs are linearly independent modulo $\mathfrak{m}_{X,x}^2$.

For example, if Y is a *hypersurface* in X in a neighborhood of x, i.e. $\mathrm{codim}_x Y = \mathrm{codim}_x X - 1$, then x is a regular point of Y if and only if Y is defined by one equation in an open neighborhood of x whose germ does not belong to $\mathfrak{m}_{X,x}^2$.

Definition. Let Y, Z be closed subsets of an algebraic set $X, x \in Y \cap Z$. We say that Y and Z intersect transversally at the point x if X is nonsingular at x and

$$\mathrm{codim}(\Theta(Y \cap Z)_x, \Theta(X)_x) = \mathrm{codim}_x(Y, X) + \mathrm{codim}_x(Z, X). \tag{8}$$

Since for any linear subpaces E_1, E_2 of a linear space V we have

$$(E_1 + E_2)^\perp = E_1^\perp \cap E_2^\perp,$$

using (6) we see that (8) is equivalent to

$$\mathrm{codim}(\Theta(Y)_x \cap \Theta(Z)_x) = \mathrm{codim}_x(Y, X) + \mathrm{codim}_x(Z, X). \tag{9}$$

Corollary. *Let Y and Z be closed subsets of an algebraic set X which intersect transversally at $x \in X$. Then*

(i) the linear subspaces $\Theta(Y)_x, \Theta(Z)_x$ intersect transversally in $\Theta(X)_x$ (i.e., $\operatorname{codim}(\Theta(Y)_x \cap \Theta(Z)_x, \Theta(X)_x) = \operatorname{codim}(\Theta(Y)_x, \Theta(X)_x) + \operatorname{codim}(\Theta(Y)_x, \Theta(X)_x)$);

(ii) x is a nonsingular point of $Y \cap Z$;

(iii) Y and Z are nonsingular at x.

Proof. We have

$$\delta_x(Y, X) = \operatorname{codim}_x(Y, X) - \operatorname{codim}(\Theta(Y)_x, \Theta(X)_x) \geq 0,$$

$$\delta_x(Z, X) = \operatorname{codim}_x(Z, X) - \operatorname{codim}(\Theta(Z)_x, \Theta(X)_x) \geq 0.$$

Since Y and Z intersect transversally at x, we obtain from (9)

$$\operatorname{codim}_x(Y, X) + \operatorname{codim}_x(Z, X) = \operatorname{codim}(\Theta(Y)_x \cap \Theta(Z)_x, \Theta(X)_x) \leq$$

$$\operatorname{codim}(\Theta(Y)_x, \Theta(X)_x) + \operatorname{codim}(\Theta(Z)_x, \Theta(X)_x) \leq \operatorname{codim}_x(Y, X) + \operatorname{codim}_x(Z, X). \qquad (10)$$

This shows that all the inequalities must be equalities. This gives

$$\operatorname{codim}(\Theta(Y)_x \cap \Theta(Z)_x, \Theta(X)_x) = \operatorname{codim}(\Theta(Y)_x, \Theta(X)_x) + \operatorname{codim}(\Theta(Z)_x, \Theta(X)_x)$$

proving (i), and $\delta_x(Y, X) = \delta_x(Z, X) = 0$ proving (iii). By Theorem 6 of Lecture 11, we have $\dim_x(Y \cap Z) \geq \dim_x X - \dim_x(Y) - \dim_x(Z)$. Applying Proposition 1, we get $\operatorname{codim}_x(Y \cap Z) \geq \operatorname{codim}_x Y + \operatorname{codim}_x Z$. Together with inequality (10) we obtain $\delta_x(Y \cap Z, X) = 0$ proving assertion (ii).

Next we will show that every function from $\mathcal{O}_{X,x}$ can be expanded into a formal power series in a set of local parameters at x.

Recall that the k-algebra of formal power series in n variables $k[[Z]] = k[[Z_1, \ldots, Z_n]]$ consists of all formal (infinite) expressions

$$P = \sum_{\mathbf{r}} a_{\mathbf{r}} Z^{\mathbf{r}},$$

where $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbf{N}^n, a_{\mathbf{r}} \in k, Z^{\mathbf{r}} = Z_1^{r_1} \ldots Z_n^{r_n}$. The rules of addition and multiplicaton are defined naturally (as for polynomals). Equivalently, $k[[Z]]$ is the set of functions $P : \mathbf{N}^n \to k, \mathbf{r} \to a_{\mathbf{r}}$, with the usual addition operation and the operation of multiplication defined by the convolution of functions:

$$(P * Q)(\mathbf{r}) = \sum_{\mathbf{i}+\mathbf{j}=\mathbf{r}} P(\mathbf{i})Q(\mathbf{j}).$$

The polynomial k-algebra $k[Z_1, \ldots, Z_n]$ can be considered as a subalgebra of $k[[Z_1, \ldots, Z_n]]$. It consists of functions with finite support. Clearly every formal power series $P \in k[[Z]]$ can be written as a formal sum $P = \sum_j P_j$, where $P_j \in k[Z_1, \ldots, Z_n]_j$ is a homogeneous polynomal of degree j.

We set

$$P_{[r]} = P_0 + P_1 + \ldots + P_r.$$

This is called the *r-truncation* of P.

Theorem 1 (Taylor expansion). *Let x be a regular point of an algebraic set X of dimension n, and $\{f_1, \ldots, f_n\}$ be a regular system of parameters at x. There exists a unique injective homomorphism $\phi : \mathcal{O}_{X,x} \hookrightarrow k[[Z_1, \ldots, Z_n]]$ such that for every $i \geq 0$*

$$f - \phi(f)_{[i]}(f_1, \ldots, f_n) \in m_{X,x}^{i+1}.$$

Proof. Take any $f \in \mathcal{O}_{X,x}$, we denote by $f(x)$ the image of f in $k = \mathcal{O}_{X,x}/m_{X,x}$ then $f - f(x) \in m_{X,x}$. Since the local parameters $f_1, \ldots, f_n$ generate $m_{X,x}$, we can find elements $g_1, \ldots, g_n \in \mathcal{O}_{X,x}$ such that

$$f = f(x) + g_1 f_1 + \ldots + g_n f_n.$$

Replacing f by g_i, we can write similar expressions for the $g_i's$. Plugging them into the above expresson for f, we obtain

$$f = f(x) + \sum_i g_i(x) f_i + \sum_{ij} h_{ij} f_i f_j,$$

where $h_{ij} \in \mathcal{O}_{X,x}$. Continuing in this way, we will find a formal power series $P = \sum_j P_j$ such that

$$(*) \qquad f - P_{[r]}(f_1, \ldots, f_n) \in m_{X,x}^{r+1} \quad \text{for any } r \geq 0.$$

Let us show that $f \mapsto P$ defines an injective homomorphism $\mathcal{O}_{X,x} \to k[[Z]]$ satisfying the assertion of the theorem. First of all, we have to verify that this map is well defined, i.e. property $(*)$ determines P uniquely. Suppose there exists another formal power series $Q(Z) = \sum_j Q_j$ such that

$$f - Q_{[r]}(f_1, \ldots, f_n) \in m_{X,x}^{r+1} \quad \text{for any } r \geq 0.$$

Let $r = \min\{j : Q_j \neq P_j\}$ and $F = Q_j - P_j \in k[Z_1, \ldots, Z_n]_r \setminus \{0\}$. Taking into account $(*)$, we obtain that $F(f_1, \ldots, f_n) \in m_{X,x}^{r+1}$. Making an invertible change of variables, we may assume that $F(0, \ldots, 0, 1) \neq 0$, i.e.,

$$F(f_1, \ldots, f_n) = G_0 f_n^r + G_1(f_1, \ldots, f_{n-1}) f_n^{r-1} + \ldots + G_r(f_1, \ldots, f_{n-1})$$

where $G_i(Z_1, \ldots, Z_{n-1}) \in k[Z_1, \ldots, Z_{n-1}]_i, G_0 \neq 0$. Since $f_1, \ldots, f_n$ generate $m_{X,x}$, we can write

$$F(f_1, \ldots, f_n) = H_1(f_1, \ldots, f_n) f_n^r + H_2(f_1, \ldots, f_{n-1}) f_n^{r-1} + \ldots + H_{r+1}(f_1, \ldots, f_{n-1}),$$

where $H_i \in k[Z_1, \ldots, Z_{n-1}]_i$. After subtracting the two expressions, we get

$$(G_0 - H_1(f_1, \ldots, f_n)) f_n^r \in (f_1, \ldots, f_{n-1}).$$

Since $H_1(f_1, \ldots, f_n) \in m_{X,x}, G_0 - H_1(f_1, \ldots, f_n)$ is invertible and $f_n^r \in (f_1, \ldots, f_{n-1})$. Passing to the germs, we find that $m_{X,x} = (f_1, \ldots, f_n) \subset \mathrm{rad}(f_1, \ldots, f_{n-1})$, and hence $(f_1, \ldots, f_n) = (f_1, \ldots, f_{n-1})$ because $m_{X,x}$ is a maximal ideal. But this contradicts Corollary 2 of Nakayama's Lemma.

We leave to the reader to verify that the constructed map $\phi : \mathcal{O}_{X,x} \to k[[Z]]$ is a ring homomorphism. Let us check now that it is injective. It follows from the definition of this map that $\phi(f) = 0$ implies $f \in (m_{X,x})^r$ for all $r \geq 0$. Let $I = \cap_r m_{X,x}^r \neq \{0\}$. Since $m_{X,x} I = I$ Nakayama's lemma implies that $I = 0$.

Definition. Let $\phi : \mathcal{O}_{X,x} \to k[[Z_1, \ldots, Z_n]]$ be the injective homomorphism constructed in Theorem 1. The image $\phi(f)$ of an element $f \in \mathcal{O}_{X,x}$ is called the Taylor expansion of f at x with respect to the local parameters $f_1, \ldots, f_n$.

Corollary 1. *The local ring $\mathcal{O}_{X,x}$ of a nonsingular point does not have zero divisors.*

Proof. $\mathcal{O}_{X,x}$ is isomorphic to a subring of the ring $k[[Z]]$ which, as is easy to see, does not have zero divisors .

Corollary 2. *A nonsingular point of an algebraic set X is contained in a unique irreducible component of X.*

Proof. This immediately follows from Corollary 1. Indeed, assume $x \in Y_1 \cap Y_2$ where Y_1 and Y_2 are irreducible components of X containing the point x. Replacing X by a small open affine neighborhood, we may find a regular function f_1 vanishing on Y_1 but not vanishing on the whole Y_2. Similarly, we can find a function f_2 vanishing on $X \setminus Y_1$ and not vanishing on the whole Y_1. The product $f = f_1 f_2$ vanishes on the whole X. Thus the germs of f_1 and f_2 are the zero divisors in $\mathcal{O}_{X,x}$. This contradicts the previous corollary.

Remarks. 3. Note the analogy with the usual Taylor expansion which we learn in Calculus. The local parameters are analogous to the differences $\Delta x_i = x_i - a_i$. The condition $f - [P]_r(f_1, \ldots, f_n) \in m_{X,x}^{r+1}$ is the analog of the convergence: the difference between the function and its truncated Taylor expansion vanishes at the point $x = (a_1, \ldots, a_n)$ with larger and larger order. The previous theorem shows that a regular function on a nonsingular algebraic set is like an analytic function: tits Taylor expansion converges to the function.

4. For every commutative ring A and its proper ideal I, one can define the I-adic formal completion of A as follows. Let $p_{n,k} : A/I^{n+1} \to A/I^{k+1}$ be the canonical homomorphism of factor rings $(n \geq k)$. Set

$$\hat{A}_I = \{(\ldots, a_k, \ldots, a_n \ldots) \in \prod_{r \geq 0} (A/I^{r+1}) : p_{n,k}(a_n) = a_k \quad \text{for all } n \geq k\}.$$

It is easy to see that $\hat{A}_I$ is a commutative ring with respect to the addition and multiplication defined coordinatewise. We have a canonical homomorphism:

$$i : A \to \hat{A}_I, a \mapsto (a_0, a_1, \ldots, a_n, \ldots)$$

where a_n = residue of a modulo I^{n+1}. Note the analogy with the ring of p-adic numbers which is nothing else as the formal completion of the local ring $\mathbf{Z}_{(p)}$ of rational numbers $a/b, p \not| b$.

The formal I-adic completion $\hat{A}$ is a completion in the sense of topology. One makes A a topological ring (i.e. a topological space for which addition and multiplication are continuous maps) by taking for a basis of topology the cosets $a + I^n$. This topology is called the *I-adic topology* in A. One defines a Cauchy sequence as a sequence of elements a_n in A such that for any $N \geq 0$ there exists $n_0(N)$ such that $a_n - a_m \in I^N$ for all $n, m \geq n_0(N)$. Two Cauchy sequences $\{a_n\}$ and $\{b_n\}$ are called equivalent if $\lim_{n \to \infty}(a_n - b_n) = 0$, that is, for any $N > 0$ there exists $n_0(N)$ such that $a_n - b_n \in I^N$ for all $n \geq 0$. An equivalence class of a Cauchy sequence $\{a_n\}$ defines an element of $\hat{A}$ as follows. For every $N \geq 0$ let α_N be the image of a_n in A/I^{N+1} for $n \geq n_0(N)$. Obvioulsy, the image of α_{N+1} in A/I^{N+1} is equal to α_N. Thus $(\alpha_0, \alpha_1, \ldots, \alpha_N, \ldots)$ is an element from $\hat{A}$. Conversely, any element $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ in $\hat{A}$ defines an equivalence class of a Cauchy sequence, namely the equivalence class of $\{a_n\}$. Thus we see that $\hat{A}$ is the usual completion of A equipped with the I-adic topology.

If A is a local ring with maximal ideal $\mathfrak{m}$, then $\hat{A}$ denotes the formal completion of A with respect to the $\mathfrak{m}$-adic topology. Note that this topology is Hausdorff. To see this we have to show that for any $a, b \in A, a \neq b$, there exists $n > 0$ such that $a + \mathfrak{m}^n \cap b + \mathfrak{m}^n = \emptyset$. this is equivalent to

the existence of $n > 0$ such that $a - b \notin \mathfrak{m}^n$. This will follow if we show that $\cap_{n \geq 0} \mathfrak{m}^n = \{0\}$. But this follows immediately from Nakayama's Lemma as we saw in the proof of Theorem 1. Since the topology is Hausdorff, the canonical map from the space to its completion is injective. Thus we get

$$A \hookrightarrow \hat{A}.$$

Note that the ring $\hat{A}$ is local. Its unique maximal ideal $\hat{\mathfrak{m}}$ is equal to the closure of $\mathfrak{m}$ in $\hat{A}$. It consists of elements $(0, a_1, \ldots, a_n, \ldots)$. The quotient $\hat{A}/\hat{\mathfrak{m}}$ is isomorphic to $A/\mathfrak{m} = \kappa$. The canonical homomorphism $\hat{(}A) \to \hat{A}/\hat{\mathfrak{m}}$ is of course $(a_0, a_1, \ldots, a_n, \ldots) \to a_0$.

5. The local ring $\hat{A}$ is complete with respect to its $\hat{\mathfrak{m}}$-topology. A fundamental result in commutative algebra is the *Cohen Structure Theorem* which says that any complete Noetherian local ring $(A, \mathfrak{m})$ which contains a field is isomorphic to the quotient ring $\kappa[[T_1, \ldots, T_n]]$, where κ is the residue field and $n = \dim_\kappa \mathfrak{m}/\mathfrak{m}^2$. This of course applies to our situation when $A = \hat{\mathcal{O}}_{X,x}$, where x is not necessary a rational point of X. In particular, when x is a regular point, we obtain

$$\hat{\mathcal{O}}_{X,x} \cong k(x)[[T_1, \ldots, T_n]] \tag{11}$$

which generalizes our Theorem 1.

6. Let us use the isomorphism (11) to show that a nonsingular point is regular if assume that the extension $k(x)/k$ is separable (i.e. can be obtained as a separable finite extension of a purely transcendental extension of k). We only sketch a proof. We have a canonical linear map $\alpha : \mathrm{Der}_k(\hat{\mathcal{O}}_{X,x}, K) \to \mathrm{Der}_k(\mathcal{O}_{X,x}, K)$ corresponding to the inclusion map of the ring into its completion. Note that for any local ring $(A, \mathfrak{m})$ which contains k, the canonical homomorphism of A-modules

$$\rho_A : \mathrm{Der}_k(A, K) \to \mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, K)$$

is injective. In fact, if M is its kernel, then, for any $\delta \in M$ we have $\delta(\mathfrak{m}) = 0$. This implies that for any $a \in \mathfrak{m}$ and any $x \in A$, we have $0 = \delta(ax) = a\delta(x) + x\delta(a) = a\delta(x)$. Thus $a\delta = 0$. This shows that $\mathfrak{m}M = 0$, and by Nakayama's lemma we get $M = 0$. Composing α with $\rho_{\mathcal{O}_{X,x}}$ we obviously get $\rho_{\hat{\mathcal{O}}_{X,x}}$. Since the latter is injective, α is injective. Now we show that it is surjective. Let $\delta \in \mathrm{Der}_k(\mathcal{O}_{X,x}, K)$. Since its restriction to $\mathfrak{m}^2_{X,x}$ is zero, we can define $\delta(a + \mathfrak{m}^2_{X,x})$ for any $a \in \mathcal{O}_{X,x}$. For any $x = (x_0, x_1, \ldots) \in \hat{\mathcal{O}}_{X,x}$ we set $\tilde{\delta}(x) = \delta(x_1)$. It is easy to see that this defines a derivation of $\hat{\mathcal{O}}_{X,x}/\hat{\mathfrak{m}}^2$ such that $\rho(\tilde{\delta}) = \delta$.

So, we obtain an isomorphism of K-vector spaces:

$$\mathrm{Der}_k(\hat{\mathcal{O}}_{X,x}, K) \cong \mathrm{Der}_k(\mathcal{O}_{X,x}, K).$$

By Cohen's Theorem, $\hat{\mathcal{O}}_{X,x} \cong k(x)[[T_1, \ldots, T_n]]$, where the pre-image of the field of constant formal series is a subfield L of $\hat{\mathcal{O}}_{X,x}$ isomorphic to $k(x)$ under the projection to the residue field. It is clear that the pre-image of the maximal ideal $(T_1, \ldots, T_n)$ is the maximal ideal of $\mathcal{O}_{X,x}$. Let $\mathrm{Der}_L(\hat{\mathcal{O}}_{X,x}, K)$ be the subspace of $\mathrm{Der}_k(\hat{\mathcal{O}}_{X,x}, K)$ of derivation trivial on L. Using the same proof as in Lemma 3 of Lecture 13, we show that $\mathrm{Der}_L(\hat{\mathcal{O}}_{X,x}, K) \cong \Theta(X)_x$. Now we have an exact sequence, obtained by restrictions of derivations to the subfield L:

$$0 \to \mathrm{Der}_L(\hat{\mathcal{O}}_{X,x}, K) \to \mathrm{Der}_k(\hat{\mathcal{O}}_{X,x}, K) \to \mathrm{Der}_k(L, K). \tag{12}$$

It is easy to see that $\dim_K \mathrm{Der}_k(L, K) = \mathrm{algdim}_k L = \mathrm{algdim}_k k(x)$. In fact, $\mathrm{Der}_k(k(t_1, \ldots, t_r), K) \cong K^r$ (each derivation is determined by its value on each t_i). Also each derivation can be uniquely extended to a separable extension. Thus exact sequence (12) gives

$$\dim_K \mathrm{Der}_k(\hat{\mathcal{O}}_{X,x}, K) = \dim_K \mathrm{Der}_k(\hat{\mathcal{O}}_{X,x}, K) \leq \mathrm{embdim}_x X + \mathrm{algdim}_k k(x).$$

This implies that $\text{embdim}_x(X) = \dim \mathcal{O}_{X,x}$ and hence $\mathcal{O}_{X,x}$ is regular.

Let (X, x) be a pair that consists of an algebraic set X and its point $x \in X$. Two such pairs are called *locally isomorphic* if the local rings $\mathcal{O}_{X,x}$ and $\mathcal{O}_{Y,y}$ are isomorphic. They are called *formally isomorphic* if the completions of the local rings are isomorphic. Thus any pair (X, x) where x is a nonsingular point of X is isomorphic to a pair $(\mathbb{A}^n(K), 0)$ where $n = \dim_x X$. Compare this with the definion of a smooth (or complex manifold).

Theorem 2. *A regular local ring is a UFD (= factorial ring).*

The proof of this non-trivial result can be found in Zariski-Samuel's Commutative Agebra, vol. II. See the sketch of this proof in Shafarevich's book, Chapter II, §3. It uses an embedding of a regular ring into the ring of formal power series.

Corollary. *Let X be an algebraic set, $x \in X$ be its regular point, and Y be a closed subset of codimension 1 which contains x. Then there exists an open subset U containing x such that $Y \cap U = V(f)$ for some regular function on U.*

Proof. Let V be an opne affine open neighborhood of x, $g \in I(Y \cap V)$, and let g_x be the germ of g at x and f_x be a prime factor of g_x which has a representative $f \in \mathcal{O}(U)$ vanishing on $Y \cap U$ for some smaller affine neighborhood U of x. At this point we may assume that $X = U$. Since $V(f) \supset Y$ and $\dim V(f) = \dim Y$, Y is equal to some irreducible component of $V(f)$, i.e., $V(f) = Y \cup Z$ for some closed subset of U. If $x \in Z$, then there exist regular functions h and h' on X such that $hh' \equiv 0$ on $V(f)$ but $h \not\equiv 0$ on Y and $h' \not\equiv 0$ on Z. By Hilbert's Nullstellensatz, $(hh')^r \in (f)$. Passing to the germs, we obtain that $f_x | (h_x h'_x)^r$. Since $\mathcal{O}_{X,x}$ is factorial, we obtain that $f_x | h_x$ or $f_x | h'_x$. Therefore for some open neighborhood $U' \subset U$, either $h|U'$ or $h'|U'$ vanishes identically on $(Y \cup Z) \cap U'$. This contradicts the choice of h and h'. This shows that $x \notin Z$, and replacing U by a smaller open subset, the proof is complete.

Here is the promised application.

Recall that a rational map $f : X \dashrightarrow Y$ from an irreducible algebraic set X to an algebraic set Y is a regular map of an open subset of X. Two rational maps are said to be equal if they coincide on an open subset of X. Replacing X and Y by open affine subsets, we find ourselves in the affine situation of Lecture 4. We say that a rational map $f : X \dashrightarrow Y$ is defined at a point $x \in X$ if it can be represented by a regular map defined on an open subset containing the point x. A point x where f is not defined is called a *point of indeterminacy* of f.

Theorem 3. *Let $f : X \dashrightarrow Y$ be a rational map of a nonsingular algebraic set X to a projective set Y. Then the set of indeterminacy points of f is a closed subset of X each irreducible component of which is of codimension ≥ 2.*

Proof. Since $Y \subset \mathbb{P}^n(K)$ for some n, we may assume that $Y = \mathbb{P}^n(K)$. Let U be the maximal open subset where f is represented by a regular map $f : U \to \mathbb{P}^n(K)$, and $Z = X \setminus U$. Assume Z contains an irreducible component of codimension 1. By Corollary to Theorem 2, for any $x \in Z$ there exists an open neighborhood V of x such that $Z \cap V = V(\phi)$ for some regular function ϕ on V. Restricting f to some smaller subset of $D(\phi) = V \setminus V(\phi)$ we may assume that $f|D(\phi)$ is given by $n+1$ regular functions $\phi_1, \ldots, \phi_{n+1}$ on $D(\phi)$. Since $\mathcal{O}_{X,x}$ is factorial, we may cancel the germs $(\phi_i)_x$ by their common divisor to assume that not all of them are divisible by the germ ϕ_x of ϕ. The resulting functions define the same map to $\mathbb{P}^n(K)$. It is not defined at the set of common zeroes of the functions ϕ_i. Its intersection with Z cannot contain any open neighborhood of x, hence is a proper closed subset of Z. This shows that we can extend f to a larger open subset contradicting the maximality of U.

Corollary. *Any rational map of a nonsingular curve to a projective set is a regular map. In particular, two nonsingular projective curves are birationally isomorphic if and only if they are isomorphic.*

This corollary is of fundamental importance. Together with a theorem on resolution of singularities of a projective curve it implies that the set of isomorphism classes of field extensions of k of transcedence degree 1 is in a bijective correspondence with the set of isomorphism classes of nonsingular projective algebraic curves over k.

Problems.

1. Using Nakayama's Lemma prove that a finitely generated projective module over a local ring is free.

2. Problem 6 from Shafarevich, Chap. II, §3.

3. Let A be a ring with a decreasing sequence of ideals $A = I_0 \supset I_1 \supset \cdots \supset I_n \supset \cdots$ such that $I_i \cdot I_j \subset I_{i+j}$ for all i, j. Let $\mathrm{Gr}_F(A) = \oplus_{i=0}^{\infty} I_i/I_{i+1}$ with the obvious ring structure making $Gr_F(A)$ a graded ring. Show that a local ring $(A, \mathfrak{m})$ of dimension n is regular if and only $\mathrm{Gr}_F(A) \cong \kappa[T_1, \ldots, T_n]$, where $I_i = \mathfrak{m}^i$.

4. Let $X = V(F) \subset \mathbb{A}^2(K)$ where $F = Z_1^3 - Z_2(Z_2 + 1)$. Find the Taylor expansion at $(0, 0)$ of the function $Z_2 \bmod (F)$ with respect to the local parameter $Z_1 \bmod (F)$.

5. Give an example of a singular point $x \in X$ such that there exists an injective homomorphism $\mathcal{O}_{X,x} \to k[[Z_1]]$. Give an example of a curve X and a point $x \in X$ for which such homomorphism does not exist.

6. Let $X = V(Z_1 Z_2 + Z_3^2) \subset K^4$. Show that the line $V(Z_1, Z_3) \subset X$ cannot be defined by one equation in any neighborhood of the origin.

7. Show that Theorem 3 is not true for singular projective algebraic curves.

8*. Let $X = V(Z_1 Z_2 + F(Z_1, Z_2)) \subset \mathbf{A}^2(K)$ where F is a homogeneous polynomial of degree ≥ 3. Show that $\hat{\mathcal{O}}_{X,x} \cong K[[T_1, T_2]]/(T_1 T_2)$ and hence the singulaity $(X, 0)$ and $(V(Z_1 Z_2), 0)$ are formally isomorphic.

Lecture 15. PROJECTIVE EMBEDDINGS

In this Lecture we shall address the following question: Given a projective algebraic k-set X, what is the minimal N such that X is isomorphic to a closed subset of $\mathbb{P}^N_k(K)$? We shall prove that $N \leq 2\dim X + 1$. For simplicity we shall assume here that $k = K$. Thus all points are rational, the kernel of the evaluation maps is a maximal ideal, the tangent space is equal to the Zariski tangent space, a regular point is the same as a nonsingular point.

Definition. A regular map of projective algebraic sets $f : X \to \mathbb{P}^r(K)$ is called an *embedding* if it is equal to the composition of an isomorphism $f' : X \to Y$ and the identity map $i : Y \to \mathbb{P}^r(K)$, where Y is a closed subset of $\mathbb{P}^r(K)$.

Theorem 1. *A finite regular map $f : X \to Y$ of algebraic sets is an isomorphism if and only if it is bijective and for every point $x \in X$ the differential map $(df)_x : T(X)_x \to T(Y)_{f(x)}$ is injective.*

Proof. To show that f is an isomorphism it suffices to find an open affine covering of Y such that for any open affine subset V from this covering the homomorphism of rings $f^* : \mathcal{O}(V) \to \mathcal{O}(f^{-1}(V))$ is an isomorphism. The inverse map will be defined by the maps of affine sets $V \to f^{-1}(V)$ corresponding to the inverse homomorphisms $(f^*)^{-1} : \mathcal{O}(f^{-1}(V)) \to \mathcal{O}(V)$. So we may assume that X and Y are affine and also irreducible.

Let $x \in X$ and $y = f(x)$. Since f is bijective, $f^{-1}(y) = \{x\}$. The homomorphism f^* induces the homomorphism of local rings $f^*_y : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$. Let us show that it makes $\mathcal{O}_{X,x}$ a finite $\mathcal{O}_{Y,y}$-module. Let $m \subset \mathcal{O}(Y)$ be the maximal ideal corresponding to the point y and let $S = \mathcal{O}(Y) \setminus m$. We know that $\mathcal{O}_{Y,y} = \mathcal{O}(Y)_S$, and, since finiteness is preserved under localizations, $\mathcal{O}(X)_{f^*(S)}$ is a finite $\mathcal{O}_{Y,y}$-module. I claim that $\mathcal{O}(X)_{f^*(S)} = \mathcal{O}_{X,x}$. Any element in $\mathcal{O}_{X,x}$ is represented by a fraction $\alpha/\beta \in Q(\mathcal{O}(X))$ where $\beta(x) \neq 0$. Since the map f is finite and bijective it induces a bijection from the set $(V(\beta))$ of zeroes of β to the closed subset $f(V(\beta))$ of Y. Since $y \notin f(V(\beta))$ we can find a function $g \in S$ vanishing on $f(V(\beta))$. By Nullstellensatz, $f^*(g)^r = \beta\gamma$ for some $r > 0$ and some $\gamma \in \mathcal{O}(X)$. Therefore we can rewrite the fraction α/β in the form $\alpha\gamma/f^*(g)^r$ showing that it comes from $\mathcal{O}(X)_{f^*(S)}$. This proves the claim.

By assumption $f^*_y : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ induces a linear surjective map:

$$^t(df)_x : m_{Y,y}/m^2_{Y,y} \to m_{X,x}/m^2_{X,x}$$

where "t" stands for the transpose map of the dual vector spaces. Let $h_1, \ldots, h_k$ be a set of local parameters of Y at the point y. Their images $f^*_y(h_1), \ldots, f^*_y(h_k)$ in $m_{X,x}$ span $m_{X,x}/m^2_{X,x}$. As

follows from Lecture 14, this implies that $f_y^*(h_1), \ldots, f_y^*(h_k)$ generate $m_{X,x}$. Therefore,

$$f_y^*(m_{Y,y})\mathcal{O}_{X,x} = m_{X,x}.$$

Since $f_y^*(\mathcal{O}_{Y,y})$ contains constant functions, and $\mathcal{O}_{X,x} = k + m_{X,x}$, we get

$$\mathcal{O}_{X,x} = f_y^*(\mathcal{O}_{Y,y}) + m_{Y,y}\mathcal{O}_{X,x}.$$

Having proved that $\mathcal{O}_{X,x}$ is a finitely generated $\mathcal{O}_{Y,y}$-module we may apply Nakayama's lemma to obtain that

$$\mathcal{O}_{X,x} = f_y^*(\mathcal{O}_{Y,y}).$$

Therefore the map $f_y^* : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is surjective. It is obviously injective. Let $\phi_1, \ldots, \phi_m$ be generators of the $\mathcal{O}(Y)$-module $\mathcal{O}(X)$. The germs $(\phi_i)_x$ belong to $\mathcal{O}_{X,x} = f^*(\mathcal{O}_{Y,y})$ allowing us to write $(\phi_i)_x = f^*((\psi_i)_y)$, where ψ_i are regular functions on some affine open neighborhood V of $f(x)$. This shows that the germs of ϕ_i and $f^*(\psi_i)$ at the point x are equal. Hence, after replacing V by a smaller set V' if needed, we can assume that $\phi_i = f^*(\psi_i)$ for some open subset U of $f^{-1}(V)$. Since X is irreducible we can further assume that $U = f^{-1}(V)$. If we replace again V by a principal open subset $D(h) \subset Y$, we get $U = D(f^*(h)), \mathcal{O}(V) = \mathcal{O}(Y)_h, \mathcal{O}(U) = \mathcal{O}(X)_{f^*(h)}$, and the functions $\phi_i|U$ generate $\mathcal{O}(U)$ as a module over $\mathcal{O}(V)$. This implies that $f^* : \mathcal{O}(V) \to \mathcal{O}(f^{-1}(V))$ is surjective, hence an isomorphism. This proves the assertion.

Remark 1. The assumption of finiteness is essential. To see this let us take X to be the union of two disjoint copies of affine line with the origin in the second copy deleted, and let $Y = V(Z_1 Z_2)$ be the union of two coordinate lines in $\mathbf{A}^2(K)$. We map the first copy isomorphically onto the lines $Z_1 = 0$ and map the second component of X isomorphically onto the line $Z_2 = 0$ with the origin deleted. It is easy to see that all the assumptions of Theorem 1 are satisfied except the finiteness. Obviously the map is not an isomorphism.

Definition. We say that a line ℓ in $\mathbb{P}^n(K)$ is *tangent* to an algebraic set X at a point $x \in X$ if $T(\ell)_x$ is contained in $T(X)_x$ (both are considered as linear subspaces of $T(\mathbb{P}^n(K))_x$).

Let E be a linear subspace in $\mathbb{P}^n(K)$ defined by a linear subspace $\bar{E}$ of K^{n+1}. For any point $x = (a_0, \ldots, a_n) \in E$ defined by the line $L_x = K(a_0, \ldots, a_n)$ in $\bar{E}$, the tangent space $T(E)_x$ can be identified with the factor space $\mathrm{Hom}_K(L_x, \bar{E}/K(a_0, \ldots, a_n)$ (see Example 2 of Lecture 13). The inclusion $\bar{E} \subset K^{n+1}$ identifies it naturally with the subspace of $T(\mathbb{P}^n(K))_x = \mathrm{Hom}_K(L_x, K^{n+1}/L_x)$. Now let X be a projective subset of $\mathbb{P}^n(K)$ defined by a system of homogeneous equations $F_1(T_0, \ldots, T_n) = \ldots = F_m(T_0, \ldots, T_n) = 0$ and let $x \in X$. Then the tangent space $T(X)_x$ can be identified with the subspace of $T(\mathbb{P}^n(K))_x$ defined by the equations

$$\sum_{j=0}^{n} \frac{\partial F_i}{\partial T_j}(x) b_j = 0, \quad i = 1, \ldots m. \tag{1}$$

Now we see that a line E is tangent to X at the point x if and only if $\bar{E}$ is contained in the space of solutions of (1). In particular we obtain that the union of lines tangent to X at the point x is the linear subspace of $\mathbb{P}^n(K)$ defined by the system of linear homogeneous equations

$$\sum_{j=0}^{n} \frac{\partial F_i}{\partial T_j}(x) T_j = 0, \quad i = 1, \ldots m. \tag{2}$$

It is called the *embedded tangent space* and is denoted by $\mathrm{ET}(X)_x$.

Lemma 1. *Let X be a projective algebraic set in $\mathbb{P}^n(K), a \in \mathbb{P}^n(K) \subset X$, the linear projection map $p_a : X \to \mathbb{P}^{n-1}(K)$ is an embedding if and only if every line ℓ in $\mathbb{P}^n(K)$ passing through the point a intersects X in at most one point and is not tangent to X at any point.*

Proof. The induced map of projective sets $f : X \to Y = p_a(X)$ is finite and bijective. By Theorem 1, it suffices to show that the tangent map $(df)_x$ is injective. Without loss of generality we may assume that $a = (0, \dots, 0, 1)$ and the map p_a is given by restriction to X of the projection $p : \mathbb{P}^n(K) \setminus \{a\} \to \mathbb{P}^{n-1}(K)$ is given by the formula:

$$(T_0, \dots, T_n) \to (T_0, \dots, T_{n-1}).$$

For any point $x = (x_0, \dots, x_n) \neq a$, we can identify the tangent space $T(\mathbb{P}^n(K))_x$ with the quotient space $K^{n+1}/K(x_1, \dots, x_n)$, the tangent space $T(\mathbb{P}^{n-1}(K))_{p_a(x)}$ with $K^n/K(x_1, \dots, x_{n-1})$, and the differential $(dp_a)_x$ with the map $K^{n+1}/K(x_1, \dots, x_n) \to K^n/K(x_1, \dots, x_{n-1})$ induced by the projection $K^{n+1} \to K^n$. It is clear that its kernel is spanned by $Kx + K(0, \dots, 0, 1)/Kx$. But this is exactly the tangent space of the line ℓ spanned by the points $x = (x_0, \dots, x_n)$ and $a = (0, \dots, 0, 1)$. Thus the differential of the restriction of p_a to X is injective if and only if the tangent space of the line ℓ is not contained in the tangent space $T(X)_x$. This proves the assertion.

Lemma 2. *Let X be a quasi-projective algebraic subset of $\mathbb{P}^n(K)$ and $x \in X$ be its nonsingular point. Then $\mathrm{ET}(X)_x$ is a projective subspace in $\mathbb{P}^n(K)$ of dimension equal to $d = \dim_x X$.*

Proof. We know that $\mathrm{ET}(X)_x$ is the subspace of $\mathbb{P}^n(K)$ defined by the equations (2). So it remains only to compute the dimension of this subspace. Since x is a nonsingular point of X, the dimension of $T(X)_x$ is equal to d. Now the result follows from comparing the equations (1) and (2). The first one defines the tangent space $T(X)_x$ and the second $\mathrm{ET}(X)_x$. The (linear) dimension of solutions of both is equal to

$$d + 1 = n + 1 - \mathrm{rank}(\frac{\partial F_i}{\partial T_j})(x) = dim_K T(X)_x + 1 = \mathrm{dim ET}(X)_x + 1.$$

Note that the previous lemma shows that one can check whether a point of a projective set X is nonsingular by looking at the Jacobian matrix of homogeneous equations defining X.

Let

$$Z = \{(x, y, z) \in \mathbb{P}^n(K) \times \mathbb{P}^n(K) \times \mathbb{P}^n(K) : x, y, z \in \ell \quad \text{for some line } \ell\}.$$

This is a closed subset of $\mathbb{P}^n(K) \times \mathbb{P}^n(K) \times \mathbb{P}^n(K)$ defined by the equations expressing the condition that three lines $x = (x_0, \dots, x_n), y = (y_0, \dots, y_n), z = (z_0, \dots, z_n)$ are linearly dependent. The tri-homogeneous polynomials defining Z are the 3×3-minors of the matrix

$$\begin{pmatrix} T_0 & \dots & T_n \\ T_0' & \dots & T_n' \\ T_0'' & \dots & T_n'' \end{pmatrix}.$$

Let $p_{12} : Z \to \mathbf{P}^n(K) \times \mathbf{P}^n(K)$ be the projection map to the product of the first two factors. For any $(x, y) \in \mathbf{P}^n(K) \times \mathbf{P}^n(K)$

$$p_3(p_{12}^{-1}((x, y))) = \begin{cases} < x, y > & \text{if } x \neq y, \\ \mathbf{P}^n(K) & \text{if } x = y \end{cases}$$

where $< x, y >$ denotes the line spanned by the points x, y.

Let X be a closed subset of $\mathbf{P}^n(K)$. We set

$$\mathrm{Sec}_X^h = p_{12}^{-1}(X \times X \setminus \Delta_X),$$
$$\mathrm{Sec}_X = \text{ closure of } \mathrm{Sec}_X^h \text{ in } Z.$$

The projection p_{12} and the projection $p_3 : Z \to \mathbf{P}^n(K)$ to the third factor define the regular maps

$$p : \mathrm{Sec}_X \to X \times X, \quad q : \mathrm{Sec}_X \to \mathbf{P}^n(K).$$

For any $(x, y) \in X \times X \setminus \Delta_X$ the image of the fibre $p^{-1}(x, y)$ under the map q is equal to the line $< x, y >$. Any such lines is called a *honest secant* of X. The union of all honest secants of X is equal to the image of Sec_X^h under the map q. The closure of this union is equal to $q(\mathrm{Sec}_X)$. It is denoted by $\mathrm{Sec}(X)$ and is called the *secant variety* of X.

Lemma 3. *Let X be an irreducible closed subset of $\mathbb{P}^n(K)$. The secant variety $Sec(X)$ is an irreducible projective algebraic set of dimension $\leq 2\dim X + 1$.*

Proof. It is enough to show that Sec_X^h is irreducible. This would imply that Sec_X and $\mathrm{Sec}(X)$ are irreducible, and by the theorem on dimension of fibres

$$\dim\, \mathrm{Sec}_X^h = \dim(X \times X) + 1 = 2\dim X + 1.$$

This gives

$$\dim\, \mathrm{Sec}(X) \leq \dim\, \mathrm{Sec}(X) = \dim\, \mathrm{Sec}_X^h = 2\dim X + 1.$$

To prove the irreduciblity of Sec_X^h we modify a little the proof of Lemma 2 of Lecture 12. We cannot apply it directly since Sec_X^h is not projective set. However, the map $p^h : \mathrm{Sec}_X^h \to X \times X \setminus \Delta_X$ is the restriction of the projection sets $(X \times X \setminus \Delta_X) \times \mathbf{P}^n(K) \to X \times X \setminus \Delta_X$. By Chevalley's Theorem from Lecture 9, the image of a closed subset of Sec_X^h is closed in $X \times X \setminus \Delta_X$. Only this additional property of the map $f : X \to Y$ was used in the proof of Lemma 2 of Lecture 12.

Lemma 4. *The tangential variety $Tan(X)$ of an irreducible projective algebraic set of $\mathbb{P}^n(K)$ is an irreducible projective set of dimension $\leq 2\dim X$.*

Proof. Let $Z \subset X \subset \mathbb{P}^n(K) \subset \mathbb{P}^n(K) \times \mathbb{P}^n(K)$ be a closed subset defined by equations (1), where x is considered as a variable point in X. Consider the projection of Z to the first factor. Its fibres are the embedded tangent spaces. Since X is nonsingular, all fibres are of dimension $\dim X$. As in the case of the secant variety we conclude that Z is irreducible and its dimension is equal to $2\dim X$. Now the projection of Z to $\mathbb{P}^n$ is a closed subset of dimension $\leq 2\dim X$. It is equal to the tangential variety $\mathrm{Tan}(X)$.

Now everything is ready to prove the following main result of this Lecture:

Theorem 2. *Every nonsingular projective d-dimensional algebraic set X can be embedded into $\mathbb{P}^{2d+1}$.*

Proof. The idea is very simple. Let $X \subset \mathbb{P}^n(K)$, we shall try to project X into a lower-dimensional projective space. Assume $n > 2d + 1$. Let $a \in \mathbf{P}^n(K) \setminus X$. By Lemma 1, the projection map

$$p_a : X \to Y \subset \mathbb{P}^{n-1}(K)$$

is an isomorphism unless either x lies on a honest secant of X or in the tangential variety of X. Since all honest secants are contained in the secant variety $\mathrm{Sec}(X)$ of X, and

$$\dim \mathrm{Sec}(X) \leq 2\dim X + 1 < n, \quad \dim \mathrm{Tan}(X) \leq 2\dim X < n,$$

we can always find a point $a \notin X$ for which the map p_a is an isomorphism. Continuing in this way, we prove the theorem.

Corollary. *Every projective algebraic curve (resp. surface) is isomorphic to a curve (resp. a surface) in* $\mathbb{P}^3(K)$ *(resp.* $\mathbb{P}^5(K)$*).*

Remark 2. The result stated in the Theorem is the best possible for projective sets. For example, the affine algebraic curve: $V(T_1^2 + F_n(T_2)) = 0$, where F_n is a polynomial of degree $n > 4$ without multiple roots, is not birationally isomorphic to any nonsingular plane projective algebraic curve. Unfortunately, we have no sufficient tools to prove this claim. Let me give one more unproven fact. To each nonsingular projective curve X one may attach an integer $g \geq 0$, called the *genus* of X. If $K = \mathbb{C}$ is the field of complex numbers, the genus is equal to the genus of the Riemann surface associated to X. Each compact Riemann surface is obtained in this way. Now for any plane curve $V(F) \subset \mathbb{P}^2(K)$ of degree n one computes the genus by the formula

$$g = \frac{(n-1)(n-2)}{2}.$$

Since some values of g cannot be realized by this formula (for example $g = 2, 4, 5$) we obtain that not every nonsingular projective algebraic curve is isomorphic to a plane curve.

Let $\mathrm{Sec}(X)$ be the secant variety of X. We know that it is equal to the closure of the union $\mathrm{Sec}(X)^h$ of honest secant lines of X. A natural guess is that the complementary set $\mathrm{Sec}(X) \setminus \mathrm{Sec}(X)^h$ consists of the union of tangent lines to X, or in other words to the tangential variety $\mathrm{Tan}(X)$ of X. This is true.

Theorem 3. *Let* $X \subset \mathbf{P}^n(K)$ *be a nonsingular irreducible closed subset of* $\mathbf{P}^n(K)$*. Then*

$$\mathrm{Sec}(X) = \mathrm{Sec}(X)^h \cup \mathrm{Tan}(X).$$

Proof. Since $\mathrm{Sec}(X)$ is equal to the closure of an irreducible variety $\mathrm{Sec}(X)^h$ and $\mathrm{Tan}(X)$ is closed, it is enough to prove that $\mathrm{Sec}(X)^h \cup \mathrm{Tan}(X)$ is a closed set.

Let Z ne the closed subset of $X \times \mathbb{P}^n(K)$ considered in the proof of Lemma 4. Its image under the projection to X is X, and its fibre over a point x is isomorphic to the embedded tangent space $\mathrm{ET}(X)_x$. Its image under the projection to $\mathbb{P}^n$ is the variety $\mathrm{Tan}(X)$. We can view any point $(x, y) = ((x_0, \ldots, x_n), (y_0, \ldots, y_n)) \in \mathrm{ET}(X)$ as a pair $x + y\epsilon \in K[\epsilon]^{n+1}$ satisfying the equations $F_i(T) = 0$. Note that for $X = \mathbb{P}^n$ we have $\mathrm{ET}(X) = \mathbb{P}^n \times \mathbb{P}^n$. Consider a closed subset Z of $\mathrm{ET}(X) \times ET(X) \times \mathrm{ET}\mathbb{P}^n(K)$ defined by the equations

$$\mathrm{rank}[x + \epsilon y, x' + \epsilon y', x'' + \epsilon y''] < 3, \tag{3}$$

where the matrix is of size $3 \times (n+1)$ with entries in $K[\epsilon]$. The equations are of course the 3×3-minors of the matrix. By Chevaley's Theorem, the projection Z' of Z to $\mathrm{ET}(X) \times \mathrm{ET}(X)$ is closed. Applying again this theorem, we obtain that the projection of Z' to $\mathbb{P}^n$ is closed. Let us show that it is equal to $\mathrm{Sec}^h(X) \cup \mathrm{Tan}(X)$.

It is clear that the image (x, x', x'') of $z = (x + \epsilon y, x' + \epsilon y', x'' + \epsilon y')$ in $X \times X \times X$ satisfies $\mathrm{rank}[x, x', x''] < 3$. This condition is equivalent to the following. For any subset I of three elements from the set $\{0, \ldots, n\}$ let $|x_I + \epsilon y_I, x'_I + \epsilon y'_I, x''_I + \epsilon y''_I|$ be the corresponding minor. Then equation (3) is equivalent to the equations

$$|x_I + \epsilon y_I, x'_I + \epsilon y'_I, x''_I + \epsilon y''_I| = 0.$$

Or, equivalently,

$$|x_I, x'_I, x''_I| = 0, \tag{4}$$

$$|x_I, y'_I, x''_I| + |x_I, x'_I, y''_I| + |y_I, x'_I, x''_I| = 0. \quad (5)$$

Suppose equations (4) and (5) are satisfied. Then (4) means that the point $x'' \in \mathbb{P}^n$ lies in the line spanned by the points x, x' or $\mathrm{rank}[x, x'] = 1$. In the first case we obtain that $x'' \in \mathrm{Sec}^h(X)$. Assume $x = x'$ as points in $\mathbb{P}^n$. Then (5) gives $|x_I, x''_I, y'_I - y_I| = 0$. Since (x, y) and (x, y') lie in $\mathrm{ET}(X)_x$, we obtain that x'' lies on the line spanned by a point x and a point in $\mathrm{ET}(X)_x$. Hence $x'' \in \mathrm{ET}(X)_x$. This proves the assertion.

Remark 3. If X is singular, the right analog of the embedded tangent space $\mathrm{ET}(X)$ is the tangent cone $CT(X)_x$. It is defined as the the union of limits of the lines $< x, y >$ where $y \in X$. See details in Shafarevich's book, Chapter II, §1, section 5.

Definition A closed subset $X \subset \mathbf{P}^n(K)$ is called *non-degenerate* if it is not contained in a hyperplane in $\mathbf{P}^n(K)$. A nondegenerate subset is called *linearly normal* if it cannot be obtained as an isomorphic projection of some $X' \subset \mathbb{P}^{n+1}(K)$.

Theorem 4. *Let X be a nonsingular irreducible non-degenerate projective curve in $\mathbb{P}^3(K)$. Then X cannot be isomorphically projected into $\mathbb{P}^2(K)$ from a point outside X. In particular any plane nonsingular projective curve of degre > 1 is linearly normal.*

Proof. Applying Theorem 3 and Lemma 1, we have to show that $\mathrm{Sec}(X) = \mathbb{P}^3(K)$. Assume the contrary. Then $\mathrm{Sec}(X)$ is an irreducible surface. For any $x \in X, \mathrm{Sec}(X)$ contains the union of lines joining x with some point $y \neq x$ in X. Since X is not a line, the union of lines $< x, y >, y \in Y, y \neq x$, is of dimension > 1 hence equal to $\mathrm{Sec}(X)$. Pick up three non-collinear points $x, y, z \in X$. Then $\mathrm{Sec}(X)$ contains the line $< x, y >$. Since each point of $\mathrm{Sec}(X)$ is on the line passing through z, we obtain that each line $< z, t >, t \in < x, y >$ belongs to $\mathrm{Sec}(X)$. But the union of these lines is the plane spanned by x, y, z. Thus $\mathrm{Sec}(X)$ coincides with this plane. Since X is obviously contained in $\mathrm{Sec}(X)$ this is absurd.

The next two important results of F. Zak are given without proof.

Theorem 5. *Let X be a nonsingular nondegenerate closed irreducible subset of $\mathbf{P}^n(K)$ of dimension d. Assume $\mathrm{Sec}(X) \neq \mathbf{P}^n(K)$. Then*

$$n \geq 2 + \frac{3d}{2}.$$

In particular, any nonsingular nondegenerate d-dimensional closed subset of $\mathbf{P}^n(K)$ is linearly normal if $n \leq \frac{3d}{2}$.

If $d = 2$, this gives that any surface of degre > 1 in $\mathbb{P}^3(K)$ is linearly normal. This bound is sharp. To show this let us consider the Veronese surface $X = v_2(\mathbb{P}^2(K)$ in $\mathbb{P}^5(K)$. Then we know that it is isomorphic to the set of symmetric 3×3-matrices of rank 1 up to proportionality. It is easy to see, by using linear algebra, that $\mathrm{Sec}(X)$ is equal to the set of symmetric matrices of rank ≤ 2 up to proportionality. This is a cubic hypersurface in $\mathbb{P}^3(K)$ defined by the equation expresing the determinant of symmetric matrix. Thus we can isomorphically project X in $\mathbb{P}^4(K)$.

Remark 4. According to a conjecture of R. Hartshorne, any non-degenerate nonsingular closed subset $X \subset \mathbb{P}^n(K)$ of dimension $d > 2n/3$ is a complete intersection (i.e. can be given by $n - d$ homogeneous equations).

Definition. A *Severi variety* is a nonsingular irreducible algebraic set X in $\mathbf{P}^n(K)$ of dimension $d = 2(n-2)/3$ which is not contained in a hyperplane and with $\mathrm{Sec}(X) \neq \mathbf{P}^n(K)$.

The following result of F. Zak classifies Severi varieties in characteristic 0:

Theorem 6. *Assume char$(K) = 0$. Each Severi variety is isomorphic to one of the following four varieties:*

($n = 2$) the Veronese surface $v_2(\mathbb{P}^2(K)) \subset \mathbb{P}^5(K)$;
($n = 4$) the Segre variety $s_{2,2}(\mathbb{P}^2(K) \times \mathbb{P}^2(K)) \subset \mathbb{P}^8(K)$;
($n = 8$) the Grassmann variety $G(2,6) \subset \mathbb{P}^{14}(K)$ of lines in $\mathbb{P}^5(K)$;
($n = 16$) the E_6-variety X in $\mathbb{P}^2(K)$.

The last variety (it was initially missing in Zak's classification and was added to the list by R. Lazarsfeld) is defined as follows. Choose a bijection between the set of 27 lines on a nonsingular cubic surface and variables $T_0, \ldots, T_{26}$. For each triple of lines which span a tri-tangent plane form the corresponding monomial $T_iT_jT_k$. Let F be the sum of such 45 monomials. Its set of zeroes in $\mathbb{P}^{26}(K)$ is a cubic hypersurface $Y = V(F)$. It is called the *Cartan cubic*. Then X is equal to the set of singularities of Y (it is the set of zeroes of 27 partial derivatives of F) and Y equals $\mathrm{Sec}(X)$. From the point of view of algebraic group theory, $X = G/P$, where G is a simply connected simple algebraic linear group of exceptional type E_6, and P its maximal parabolic subgroup corresponding to the dominant weight ω defined by the extreme vertex of one of the long arms of the Dynkin diagram of the root system of G. The space $\mathbb{P}^{26}(K)$ is the projectivization of the representation of G with highest weight ω.

We only check that all the four varieties from Theorem 6 are in fact Severi varieties. Recall that the Veronese surface can be described as the space of 3×3 symmetric matrices of rank 1 (up to proportionality). Since a linear combination of two rank 1 matrices is a matrix of rank ≤ 2, we obtain that the secant variety is contained in the cubic hypersurface in $\mathbb{P}^5$ defining matrices of rank ≤ 2. Its equation is the symmetric matrix determinant. It is easy to see that the determinant equation defines an irreducible variety. Thus the dimension count gives that it coincides with the determinant variety. Similarly, we see that the secant variety of the Segre variety coinicides with the determinant hypersurface of a general 3×3 matrix. The third variety can be similarly described as the variety of skew-symmetrix 6×6 matrices of rank 2. Its secant varity is equal to the Pffafian cubic hypersurface defining skew-symmetric matrices of rank < 6. Finally, the secant variety of the E_6-variety is equal to the Cartan cubic. Since each point of the Severi variety is a singular point of the cubic, the restriction of the cubic equation to a secant line has two multiple roots. This easily implies that the line is contained in the cubic. To show that the secant variety coincides with the cartan cubic is more involved, One looks at the projective linear representation of the exceptional algebraic group G of type E_6 in $\mathbb{P}^{26}$ defining the group G. One analyzes its orbits and shows that there are only three orbits: the E_6-variety X, the Cartan cubic with X deleted and $\mathbb{P}^{26}$ with Cartan cubic deleted. Since the secant variety is obvioulsy invariant under the action of G, it must coincide with the Cartan cubic.

Note that in all four cases the secant variety is a cubic hypersurface and its set of singular points is equal to the Severy variety. In fact, the previous argument shows that the secant variety of the set of singular points of any cubic hypersurface is contained in the cubic. Thus Theorem 6 gives a classification of cubic hypersurfaces in $\mathbb{P}^n$ whose set of singular points is a smooth variety of dimension $2(n-2)/3$.

There is a beautiful uniform description of the four Severi varieties. Recall that a composition algebra is a finite-dimensional algebra A over a field K (not necessary commutative or associative) such that there exists a non-degenerate quadratic form $\Phi : A \to K$ such that for any $x, y \in A$

$$\Phi(x \cdot y) = \Phi(x)\Phi(y).$$

According to a classical theorem of A. Hurwitz there are four isomorphism classes of composition algebras over a field K of characteristic 0: K, Co, Ha and Oc of dimension 1, 2, 4 and 8, respectively.

Here

$$Co = K \oplus K, (a,b)\cdot(a',b') = (aa' - bb', ab' + a'b),$$

$$Ha = Co \oplus Co, (x,y)\cdot(x',y') = (x\cdot x' - \bar{y}\cdot y', x\cdot y' + y\cdot \bar{x}'),$$

$$Oc = Ha \oplus Ha, (h,g)\cdot(h',g') = (h\cdot h' - \bar{g}\cdot g', h\cdot g' + g\cdot \bar{h}'),$$

where for any $x = (a,b) \in Co$ we set $\bar{x} = (a,-b)$, and for any $h = (x,y) \in Ha$ we set $\bar{h} = (\bar{x},-y)$. The quadratic form Φ is given by

$$\Phi(x) = x\cdot\bar{x},$$

where $\bar{x}$ is defined as above for $A = Ca$ and H, $\bar{x} = x$ for $A = K$, and $\bar{x} = (\bar{h},-h')$ for any $x = (h,h') \in Oc$.

For example, if $K = \mathbb{R}$, then $Co \cong \mathbb{C}$ (complex numbers), $Ha \cong \mathbb{H}$ (quaternions), $Oc = \mathbb{O}$ (octonians or Cayley numbers).

For every composition algebra A we can consider the set $\mathcal{H}_3(A)$ of Hermitian 3×3-matrices (a_{ij}) with coefficients in A, where Hermitian means $a_{ij} = \bar{a}_{ji}$. Its dimension as a vector space over K equals $3+3r$, where $r = \dim_K A$. There is a natural definition of the rank of a matrix from $\mathcal{H}_3(A)$. Now Theorem 6 says that the four Severi varieties are closed subsets of $\mathbb{P}^{3r+2}$ defined by rank 1 matrices in $\mathcal{H}_3(A)$. The corresponding secant variety is defined by the homogeneous cubic form representing the "determinant" of the matrix.

Let us define $\mathbb{P}^n(A)$ for any composition algebra as $A^{n+1}\setminus\{0\}/A^*$. Then one view the four Severi varieties as the "Veronese surfaces" corresponding to the projective planes over the four composition algebra.

As though it is not enough of these mysterious coincidences of the classifications, we add one more. Using the stereographic projection one can show that

$$\mathbb{P}^1(\mathbb{R}) = S^1, \quad \mathbb{P}^1(\mathbb{C}) = S^2, \quad \mathbb{P}^1(\mathbb{H}) = S^4, \quad \mathbb{P}^1(\mathbb{O}) = S^8,$$

where S^k denote the unit sphere of dimension k. The canonical projection

$$\mathbb{A}^2\setminus\{0\} \to \mathbb{P}^1(A) = S^k$$

restricted to the subset $\{(x,y)\in\mathbb{R}^2 : x\cdot\bar{x} + y\cdot\bar{y} = 1\} = S^{2r-1}$ defines a map

$$\pi : S^{2r-1} \to S^r$$

which has a structure of a smooth bundle with fibres diffeomorphic to the sphere $S^{r-1} = \{x\in A^* : x\cdot\bar{x} = 1\}$. In this way we obtain 4 examples of a Hopf bundle: a smooth map of a sphere to a sphere which is a fibre bundle with fibres diffeomorphic to a sphere. According to a famous result of F. Adams, each Hopf bundle is diffeomorphic to one of the four examples coming from the composition algebras.

Is there any direct relationship between Hopf bundles and Severi varieties?

Problems.

1. Let X be a nonsingular closed subset of $\mathbb{P}^n(K)$. Show that the set $J(X)$ of secant or tangent lines of X is a closed subset of the Grassmann variety $G(2,n+1)$. Let $X = v_3(\mathbb{P}^1(K))$ be a twisted cubic in $\mathbb{P}^3(K)$. Show that $J(X)$ is isomorphic to $\mathbb{P}^2(K)$.

2. Find the equation of the tangential surface $\mathrm{Tan}(X)$ of the twisted cubic curve in $\mathbb{P}^3(K)$.
3. Show that each Severi variety is equal to the set of singular points of its secant variety. Find the equations of the tangential variety $\mathrm{Tan}(X)$.
4. Assume that the secant variety $\mathrm{Sec}(X)$ is not the whole space. Show that any X is contained in the set of singular points of $\mathrm{Sec}(X)$.
5. Show that a line ℓ is tangent to an algebraic set X at a point $x \in X$ if and only if the restriction to ℓ of any polynomial vanishing on X has the point x as its multiple root.
6*. Let X be a nonsingular irreducible projective curve in $\mathbf{P}^n(K)$. Show that the image of the Gauss map $g : X \to G(2, n+1)$ is birationally isomorphic to X unless X is a line.

Lecture 16. BLOWING UP AND RESOLUTION OF SINGULARITIES

Let us consider the projection map $p_a : \mathbf{P}^n(K) \setminus \{a\} \to \mathbb{P}^{n-1}(K)$. If $n > 1$ it is impossible to extend it to the point a. However, we may try to find another projective set X which contains an open subset isomorphic to $\mathbf{P}^n(K) \setminus \{a\}$ such that the map p_a extends to a regular map $\bar{p}_a : X \to \mathbb{P}^{n-1}(K)$. The easiest way to do it is to consider the graph $\Gamma \subset \mathbf{P}^n(K) \setminus \{a\} \times \mathbb{P}^{n-1}(K)$ of the map p_a and take for X its closure in $\mathbf{P}^n(K) \times \mathbb{P}^{n-1}(K)$. The second projection map $X \to \mathbb{P}^{n-1}(K)$ will solve our problem. It is easy to find the bi-homogeneous equations defining X. For simplicity we may assume that $a = (1, 0, \dots, 0)$ so that the map p_a is given by the formula $(x_0, x_, \dots, x_n) \to (x_1, \dots, x_n)$. Let $Z_0, \dots, Z_n$ be projective coordinates in $\mathbf{P}^n(K)$ and let $T_1, \dots, T_n$ be projective coordinates in $\mathbb{P}^{n-1}(K)$. Obviously the graph Γ is contained in the closed set X defined by the equations

$$(*) \qquad Z_i T_j - Z_j T_i = 0, i, j = 1, \dots, n.$$

The projection $q : X \to \mathbb{P}^{n-1}(K)$ has the fibre over a point $t = (t_1, \dots, t_n)$ equal to the linear subspace of $\mathbf{P}^n(K)$ defined by the equations

$$(**) \qquad Z_i t_j - Z_j t_i = 0, i, j = 1, \dots, n.$$

Assume that $t_i = 1$. Then the matrix of coefficients of the system of linear equations $(**)$ contains $n - 1$ unit columns so that its rank is equal to $n - 1$. This shows that the fibre $q^{-1}(t)$ is isomorphic, under the first projection $X \to \mathbf{P}^n(K)$, to the line spanned by the points $(0, t_1, \dots, t_n)$ and $(1, 0, \dots, 0)$. On the other hand the first projection is an isomorphism over $\mathbf{P}^n(K) \setminus \{0\}$. Since X is irreducible (all fibres of q are of the same dimension), we obtain that X is equal to the closure of Γ. By plugging $z_1 = \dots z_n$ in equations $(**)$ we see that the fibre of p over the point $a = (1, 0, \dots, 0)$ is isomorphic to the projective space $\mathbb{P}^{n-1}(K)$. Under the map q this fibre is mapped isomorphically to $\mathbb{P}^{n-1}(K)$.

The pre-image of the subset $\mathbf{P}^n(K) \setminus V(Z_0) \cong \mathbf{A}^n(K)$ under the map p is isomorphic to the closed subvariety B of $\mathbf{A}^n(K) \times \mathbb{P}^{n-1}(K)$ given by the equations $(*)$ where we consider $Z_1, \dots, Z_n$ as inhomogeneous coordinates in affine space. The restriction of the map p to B is a regular map $\sigma : B \to \mathbf{A}^n(K)$ satisfying the following properties

(i) $\sigma | \sigma^{-1}(\mathbf{A}^n(K) \setminus \{(0, \dots, 0)\}) \to \mathbf{A}^n(K) \setminus \{(0, \dots, 0)\}$ is an isomorphism;

(ii) $\sigma^{-1}(0, \dots, 0) \cong \mathbb{P}^{n-1}(K)$.

We express this by saying that σ " blows up" the origin. Of course if we take $n = 1$ nothing happens. The algebraic set B is isomorphic to $\mathbf{A}^n(K)$. But if take $n = 2$, then B is equal to the closed subset of $\mathbf{A}^2(K) \times \mathbb{P}^1(K)$ defined by the equation

$$Z_2 T_0 - T_1 Z_1 = 0.$$

It is equal to the union of two affine algebraic sets V_0 and V_1 defined by the condition $T_0 \neq 0$ and $T_1 \neq 0$, respectively. We have

$$V_0 = V(Z_2 - XZ_1) \subset \mathbf{A}^2(K) \times \mathbb{P}^1(K)_0, \quad X = T_1/T_0,$$

$$V_1 = V(Z_2Y - Z_1) \subset \mathbf{A}^2(K) \times \mathbb{P}^1(K)_1, \quad Y = T_0/T_1.$$

If $L : Z_2 - tZ_1 = 0$ is the line in $\mathbf{A}^2(K)$ through the origin "with slope" t, then the pre-image of this line under the projection $\sigma : B \to \mathbf{A}^2(K)$ consists of the union of two curves, the fibre $E \cong \mathbb{P}^1(K)$ over the origin, and the curve $\bar{L}$ isomorphic to L under σ. The curve $\bar{L}$ intersects E at the point $((0,0),(1,t)) \in V_0$. The pre-image of each line L with the equation $tZ_2 - Z_1$ consists of E and the curve intersecting E at the point $((0,0),(t,1)) \in V_1$. Thus the points of E can be thought as the set of slopes of the lines through $(0,0)$. The "infinite slope" corresponding to the line $Z_1 = 0$ is the point $(0,1) \in V_1 \cap E$.

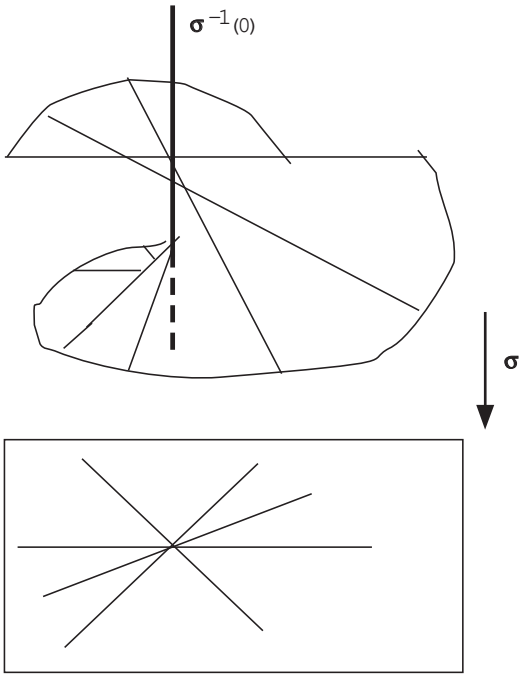

Fig.1

Let I be an ideal in a commutative ring A. Each power I^n of I is a A-module and $I^n I^r \subset I^{n+r}$ for every $n, r \geq 0$. This shows that the multipication maps $I^n \times I^r \to I^{n+r}$ define a ring structure on the direct sum of A-modules

$$A(I) = \oplus_{n \geq 0} I^n.$$

Moreover, it makes this ring a graded algebra over $A = A(I)_0 = I^0$. Its homogeneous elements of degree n are elements of I^n.

Assume now that I is generated by a finite set $f_0, \ldots, f_n$ of elements of A. Consider the surjective homomorphism of graded A-algebras

$$\phi : A[T_0, \ldots, T_n] \to A(I)$$

defined by sending T_i to f_i. The kernel $Ker(\phi)$ is a homogeneous ideal in $A[T_0, \ldots, T_n]$. If we additionally assume that A is a finitely generated algebra over a field k, we can interpret $Ker(\phi)$

as the ideal defining a closed subset in the product $X \times \mathbb{P}^n_k$ where X is an affine algebraic variety with $\mathcal{O}(X) \cong A$. Let Y be the subvariety of X defined by the ideal I.

Definition The subvariety of $X \times \mathbb{P}^n_k$ defined by the ideal $\mathrm{Ker}(\phi)$ is denoted by $B_Y(X)$ and is called the blow-up of X along Y. The morphism $\sigma : B_Y(X) \to X$ defined by the projection $X \times \mathbb{P}^n_k \to X$ is called the *monoidal transformation* or the *σ-process* or the *blowing up morphism* along Y.

Let us fix an algebraically closed field K containing k and describe the algebraic set $B_Y(X)(K)$ as a subset of $X(K) \times \mathbf{P}^n(K)$. Let $U_i = X \times (\mathbf{P}^n(K))_i$ and $B_Y(X)_i = B_Y(X) \cap U_i$. This is an affine algebraic k-set with

$$\mathcal{O}(B_Y(X)_i) \cong \mathcal{O}(X)[T_0/T_i \ldots, T_n/T_i]/Ker(\phi)_i$$

where $Ker(\phi)_i$ is obtained from the ideal $Ker(\phi)$ by dehomogenization with respect to the variable T_i. The fact that the isomorphism class of $B_Y(X)$ is independent of the choice of generators $f_0, \ldots, f_n$ follows from the following

Lemma 1. *Let $Y \subset X \times \mathbb{P}^n_k(K)$ and $Y' \subset X \times \mathbb{P}^r_k(K)$ be two closed subsets defined by homogeneous ideals $I \subset \mathcal{O}(X)[T_0, \ldots, T_n]$ and $J \subset \mathcal{O}(X)[T'_0, \ldots, T'_r]$, respectively. Let $p : Y \to X$ and $p' : Y' \to X$ be the regular maps induced by the first projections $X \times \mathbb{P}^n_k(K) \to X$ and $X \times \mathbb{P}^r_k(K) \to X$. Assume that there is an isomorphism of graded $\mathcal{O}(X)$-algebras $\psi : \mathcal{O}(X)[T'_0, \ldots, T'_r]/I' \to \mathcal{O}(X)[T_0, \ldots, T_n]/I$. Then there exists an isomorphism $f : Y \to Y'$ such that $p = p' \circ f$.*

Proof. Let $t'_i = T'_i \bmod I', t_i = T_i \bmod I$, and let

$$\psi(t'_i) = F_i(t_1, \ldots, t_n), i = 0, \ldots, r,$$

for some polynomial $F_i[T_0, \ldots, T_n]$. Since f is an isomorphism of graded $\mathcal{O}(X)$-algebras the polynomials $F_i(T)$ are linear and its coefficients are regular functions on X. The value of F_i at a point $(x, t) = (x, (t_0, \ldots, t_n))$ in $X \times \mathbb{P}^n_k(K)$ is defined by plugging x into the coefficients and plugging t into the unknowns T_j. Define $f : X \to Y$ by the formula:

$$f(x, t) = (x, (F_0(x, t), \ldots, F_n(x, t))).$$

Since ψ is invertible, there exist linear polynomials $G_j(T) \in \mathcal{O}(X)[T'_0, \ldots, T'_r], j = 0, \ldots, n$, such that

$$F_i(G_0(t'_0, \ldots, t'_n), \ldots, G_n(t_0, \ldots, t'_n)) = t'_i, i = 0, \ldots, r,$$

$$G_j(F_0(t_0, \ldots, t_n), \ldots, F_n(t_0, \ldots, t_n)) = t_j, j = 0, \ldots, n.$$

This easily implies that f is defined everywhere and is invertible. The property $p = p' \circ f$ follows from the definition of f.

Example 1. We take $X = \mathbf{A}^2_k(K), \mathcal{O}(X) = k[Z_1, Z_2], I = (Z_1, Z_2), Y = V(I) = \{(0, 0)\}$. Then $\phi : k[Z_1, Z_2][T_0, T_1] \to k[Z_1, Z_2](I)$ is defined by sending T_0 to Z_1, and T_1 to Z_2. Obviously $\mathrm{Ker}(\phi)$ contains $Z_2T_0 - Z_1T_1$. We will prove later in Proposition 2 that $\mathrm{Ker}(\phi) = (Z_2T_0 - Z_1T_1)$. Thus $B_Y(X)$ coincides with the example considered in the beginning of the Lecture.

Lemma 2. *Let $U = D(f) \subset X$ be a principal affine open subset of an affine set X, then*

$$B_{Y\cap U} \cong \sigma^{-1}(U).$$

Proof. We have $\mathcal{O}(U) \cong \mathcal{O}(X)_f, I(Y \cap U) = I(Y)_f$. If $I(Y)$ is generated by $f_0, \dots, f_n$ then $I(Y \cap U)$ is generated by $f_0/1, \dots, f_n/1$, hence $B_{Y\cap U}$ is defined by the kernel of the homomorphism

$$\phi_f : \mathcal{O}(X)_f[T_0, \dots, T_n] \to \mathcal{O}(X)(I(Y)_f), T_i \to f_i/1.$$

Obviously the latter is obtained by localizing the homomorphism of $\mathcal{O}(X)$-algebras

$$\phi : \mathcal{O}(X)[T_0, \dots, T_n] \to \mathcal{O}(X)(I(Y)), T_i \to f_i.$$

Therefore the kernel of ϕ_f is isomorphic to $(\mathrm{Ker}(\phi))_f$. The set of zeroes of this ideal is equal to $\sigma^{-1}(D(f))$.

Proposition 1. *The blow-up $\sigma : B_Y(X) \to X$ induces an isomorphism*

$$\sigma^{-1}(X \setminus Y) \cong X \setminus Y.$$

Proof. It is enough to show that for any prinicpal open subset that $U = D(f) \subset X \setminus Y$ the induced map $\sigma^{-1}(U) \to U$ is an isomorphism. Since $Y \subset X \setminus U$ and $I(Y)$ is radical ideal, f must belong to $I(Y)$. Thus $I(Y)_f = \mathcal{O}(X)_f$ and, taking 1 as a generator of $I(Y)_f$ we get $\mathcal{O}(X)_f((1) = \mathcal{O}(X)_f$, and the map $\phi_f : \mathcal{O}(X)_f[T_0] \to \mathcal{O}(X)_f, T_0 \to 1$ has the kernel equal to $(T_0 - 1)$. Applying the previous Lemma, we get $B_\emptyset(X) \cong D(f) \cong \sigma^{-1}(D(f))$. This proves the assertion.

To find explicitly the equations of the blow-up $B_Y(X)$, we need to make some assumptions on X and Y.

Definition. Let A be a commutative ring. A sequence of elements $a_1, \dots, a_n \in A$ is called a *regular sequence* if the ideal generated by $a_1, \dots, a_n$ is a proper ideal of A and, for any $i = 1, \dots, n$, the image of a_i in $A/(a_1, \dots, a_{i-1})$ is a non-zero divisor (we set $a_0 = 0$).

Lemma 3. *Let M be a module overa commutative ring A. Assume that for any maximal ideal m of A, the localization $M_m = \{0\}$. Then $M = \{0\}$.*

Proof. Let $x \in M$. For any maximal ideal $m \subset A$, there exists $a_m \notin m$ such that $a_m x = 0$. The ideal of A generated by the elements a_m is the unit ideal. Hence $1 = \sum_m b_m a_m$ for some $b_m \in A$ and

$$x = 1 \cdot x = \sum_m b_m a_m x = 0.$$

This proves the assertion.

Proposition 2. *Let $a_0, \dots, a_n$ be a regular sequence of elements in an integral domain A and let I be the ideal generated by $a_1, \dots, a_n$. Then the kernel J of the homomorphism*

$$\phi : A[T_0, \dots, T_n] \to A(I), T_i \mapsto a_i,$$

is generated by the polynomials $P_{ij} = a_i T_j - a_j T_i, i, j = 0, \dots, n$.

Proof. Let J' be the ideal in $A[T_0, \dots, T_n]$ generated by the polynomials P_{ij}. Let $A_0 = A[a_0^{-1}] \cong A_{a_0}$ be the subring of the quotient field $Q(A)$ of A, $I_0 = (a_1/a_0, \dots, a_n/a_0) \subset A_0$.

Define a homomorphism $\phi_0 : A[Z_1, \ldots, Z_n] \to A_0[I_0]$ via sending each Z_i to a_i/a_0. We claim that $J_0 = \mathrm{Ker}(\phi_0)$ is equal to the ideal J_0' generated by the polynomials $L_i = a_0 Z_i - a_i$. Assume this is so. Then for any $F(T_0, \ldots, T_n) \in Ker(\phi)$, after dehomogenizing with respect to T_0, we obtain that $F(1, Z_1, \ldots, Z_n)$ belongs to J_0'. This would immediately imply that $T_0^N F \in J'$ for some $N \geq 0$. Replacing T_0 with T_i, and f_0 with f_i, we will similarly prove that $T_i^N F \in J'$ for any $i = 0, \ldots, n$. Now consider the A-submodule M of $A[T_0, \ldots, T_n]/J'$ generated by F. Since $T_i^N F = 0, i = 0, \ldots, n$, it is a finitely generated A-module. For any maximal ideal $m \subset A$ let $\bar{P}_{ij} = (a_i \bmod m)T_j - (a_j \bmod m)T_i$. The ideal in $(A/m)[T_0, \ldots, T_n]$ generated by the linear polynomials $\bar{P}_{ij}$ is obviously prime. Thus $T_i^N F = 0$ implies $M \otimes A/m = \{0\}$. Applying Nakayama's Lemma we infer that, for any maximal ideal $m \subset A$, the localization M_m is equal to zero. By the previous lemma this gives $M = 0$ so that $F \in J'$.

It remains to show that $\mathrm{Ker}(\phi_0)$ is generated by by the polynomials $L_i = a_0 Z_i - a_i$. We use induction on n. Assume $n = 1$. Let $F \in \mathrm{Ker}(\phi_0)$, i.e., $\phi_0(F(Z_1)) = F(a_1/a_0) = 0$. Dividing by $L_1 = a_0 Z_1 - a_1$, we obtain for some $G(Z_1) \in A[Z_1]$ and $r \geq 0$

$$a_0^r F(Z_1) = G(Z_1)(a_0 Z_1 - a_1) = a_0 G(Z_1) Z_1 - a_1 G(Z_1).$$

Since (a_0, a_1) is a regular sequence, this implies that $G(a) \in (a_0)$ for any $a \in A$. From this we deduce that all coefficients of $G(Z_1)$ are divisible by a_0 so that we can cancel a_0 in the previous equation. Proceeding in this way we find, by induction on r, that F is divisible by L_1.

Now assume $n > 1$ and consider the map ϕ_0 as the composition map

$$A[Z_1, \ldots, Z_n] \to A'[Z_2, \ldots, Z_n] \to A_0[I_0] = A'[I'],$$

where $A' = A[a_1/a_0]$ is the subalgebra of A_0 generated by a_1/a_0, and $I' = (a_2/a_0, \ldots, a_n/a_0)$. It is easy to see that $a_0, \ldots, a_n$ is a regular sequence in A'. By induction, $L_2, \ldots, L_n$ generate the kernel of the second map $A'[Z_2, \ldots, Z_n] \to A_0[I_0]$. Thus $F(Z_1, \ldots, Z_n) \in Ker(\phi_0)$ implies

$$F(a_1/a_0, Z_2, \ldots, Z_n) = \sum_{i=2}^{n} Q_i(a_1/a_0, Z_2, \ldots, Z_n) L_i,$$

for some polynomials $Q_i(Z_1, \ldots, Z_n) \in A[Z_1, \ldots, Z_n]$. Thus by the case $n = 1$

$$F(Z_1, \ldots, Z_n) - \sum_{i=2}^{n} Q_i(a_1/a_0, Z_2, \ldots, Z_n) L_i \in (L_1),$$

and we are done.

Example 2. Take $A = k[Z_1, \ldots, Z_N], I = (a_0, \ldots, a_n) = (Z_1, \ldots, Z_{n+1})$ to obtain that the blow-up $B_{V(I)}(\mathbf{A}_k^N)(K))$ is a subvariety of $\mathbf{A}_k^N \times \mathbb{P}_k^n$ given by the equations

$$T_0 Z_i - T_{i-1} Z_1 = 0, i = 1, \ldots, n+1.$$

This agrees with Example 1.

Remark 1. The assertion of Proposition 2 can be generalized as follows. Let $a_1, \ldots, a_n$ be a regular sequence in A. Consider the free module A^n with basis $e_1, \ldots, e_n$ and let $\bigwedge^r A^n$ be its r-th exterior power. It is a free A-module with basis formed by the wedge products $e_{i_1} \wedge \ldots \wedge e_{i_r}$ where $1 \leq i_1 < \ldots, i_r \leq n$. For each $r = 1, \ldots, n$. Define the map

$$\delta_r : \bigwedge^r A^n \to \bigwedge^{r-1} A^n$$

by the formula

$$\delta_r(e_{i_1} \wedge \ldots \wedge e_{i_r}) = \sum_i (-1)^j a_{i_j} e_{i_1} \wedge \ldots \wedge e_{i_{j-1}} \wedge e_{i_{j+1}} \ldots \wedge e_{i_r}.$$

Now the claim is that the complex of A-modules (called the *Koszul complex*)

$$\{0\} \to \bigwedge^n A^n \to \bigwedge^{n-1} A^n \to \ldots \to \bigwedge^2 A^n \to \bigwedge^1 A^n \to A \to A/(a_1, \ldots, a_n) \to \{0\}$$

is exact. The previous proposition asserts only that this complex is exact at the term $\bigwedge^1 A^n$.

Proposition 3. *Let X be an affine irreducible algebraic k-set, I be an ideal in $\mathcal{O}(X)$ generated by a regular sequence $(f_0, \ldots, f_n)$, and let $Y = V(I)$ be the set of zeroes of this ideal. Let $\sigma : B_Y(X) \to X$ be the blow-up of X along Y. Then for any $x \in Y$,*

$$\sigma^{-1}(x) \cong \mathbf{P}^n(K).$$

The pre-image of every irreducible component of Y is an irreducible subset of $B_Y(X)$ of codimension 1.

Proof. By Proposition 2, $Z = B_Y(X)$ is a closed subset of $X \times \mathbf{P}^n(K)$ defined by the equations

$$T_0 f_i - T_i f_0 = 0, i = 1, \ldots, n.$$

For any point $y \in Y$ we have $f_0(y) = \ldots = f_n(y) = 0$. Hence for any $t \in \mathbf{P}^n(K)$, the point (y, t) is a zero of the above equations. This shows that $\sigma^{-1}(y)$ is equal to the fibre of the projection $X \times \mathbf{P}^n(K) \to X$ over y which is obviously equal to $\mathbf{P}^n(K)$. For each irreducible component Y_i of Y the restriction map $\sigma : \sigma^{-1}(Y_i) \to Y_i$ has fibres isomorphic to n-dimensional projective spaces. By Lemma 2 of Lecture 12 (plus the remark made in the proof of Lemma 3 in Lecture 15) we find that $\sigma^{-1}(Y_i)$ is irreducible of dimension equal to $n + \dim Y_i$. By Krull's Hauptidealsatz, $\dim Y_i = \dim X - n - 1$ (here we use again that $(f_0, \ldots, f_n)$ is a regular sequence).

Lemma 4. *Let X be a nonsingular irreducible affine algebraic k-set, Y be a nonsingular closed subset of X. For any $x \in Y$ with $\dim_x Y = \dim_x X - n$ there exists an affine open neighborhood U of x in X such that $Y \cap U = V(f_1, \ldots, f_n)$ for some regular sequence $(f_1, \ldots, f_n)$ of elements in $\mathcal{O}(U)$.*

Proof. Induction on n. The case $n = 1$ has been proven in Lecture 13. Let $f_0 \in I(Y)$ such that its germ $(f_0)_x$ in $m_{X,x}$ does not belong to $m^2_{X,x}$. Let $Y' = V(f_0)$. By Lemma 2 from lecture 14, $T(Y')_x$ is of codimension 1 in $T(X)_x$. By Krull's Hauptidealsatz, $\dim_x Y' = \dim X - 1$, hence Y' is nonsingular at x. Replacing X with a smaller open affine set U, we may assume that $Y' \cap U$ is nonsingular everywhere. By induction, for some $V \subset Y', Y \cap V$ is given in V by an ideal $(f_1, \ldots, f_n)$ so that Y is given locally by the ideal $(f_0, \ldots, f_n)$. Now the assertion follows from the following statement from Commutative Algebra (see Matsumura, pg.105): A sequence $(a_1, \ldots, a_n)$ of elements from the maximal ideal of a regular local ring A is a regular sequence if and only if $\dim A/(a_1, \ldots, a_n) = \dim A - n$. By this result, the germs of $f_0, \ldots, f_n$ in $\mathcal{O}_{X,x}$ form a regular sequence. Then it is easy to see that their representatives in some $\mathcal{O}(U)$ form a regular sequence.

Theorem 1. *Let $\sigma : B_Y(X) \to X$ be the blow-up of a nonsingular irreducible affine algebraic k-set X along a nonsingular closed subset Y. Then the following is true*
(i) σ is an isomorphism outside Y;
(ii) $B_Y(X)$ is nonsingular;
(iii) for any $y \in Y, \sigma^{-1}(y) \cong \mathbb{P}^n(K)$, where $n = \mathrm{codim}_y(Y, X) - 1 = \dim X - \dim_y Y - 1$;
(iv) for any irreducible component Y_i of Y, $\sigma^{-1}(Y_i)$ is an irreducible subset of codimension one.

Proof. Properties (i) and (iv) have been already verified. Propertry (iii) follows from Proposition 3 and lemma 4. We include them only for completeness sake. Using (i), we have to verify the nonsingularity of $B_Y(X)$ only at points x' with $\sigma(x') = y \in Y$. Replacing X by an open affine neighborhood U of y, we may assume that $Y = V(I)$ where I is an ideal generated by a regular sequence $f_0, \ldots, f_n$. By Lemma 2, $\sigma^{-1}(U) \cong B_{Y \cap U}(U)$ so that we may assume $X = U$. By Proposition 2, $B_Y(X) \subset X \times \mathbb{P}^n_k(K)$ is given by the equations: $f_i T_j - f_j T_i = 0, i, j = 0, \ldots, n$. Let $p = (y, t) \in B_Y(X)$ where $y \in Y, t = (t_0, \ldots, t_n) \in \mathbb{P}^{\mathbf{n}}(\mathbf{K})$. We want to verify that it is a nonsingular point of $B_Y(X)$. Without loss of generality we may assume that the point p lies in the open subset $W = B_Y(X)_0$ where $t_0 \neq 0$. Since

$$T_0(f_i T_j - f_j T_i) = T_i(f_0 T_j - f_j T_0) - T_j(f_0 T_i - f_i T_0)$$

we may assume that $B_Y(X)$ is given by the equations

$$f_0 T_i - f_i T_0 = 0, i = 0, \ldots, n$$

in an affine neighborhood of the point p. Let $G_1(T_1, \ldots, T_N) = \ldots = G_m(T_1, \ldots, T_N)$ be the system of equations defining X in $\mathbf{A}^N(K)$ and let $F_i(T_1, \ldots, T_N)$ represent the function f_i. Then W is given by the following equations in $\mathbf{A}^N(K) \times \mathbf{A}^n(K)$:

$$G_s(T_1, \ldots, T_N) = 0, s = 1, \ldots, m,$$

$$Z_i F_0(T_1, \ldots, T_N) - F_i(T_1, \ldots, T_N) = 0, i = 1, \ldots, n.$$

It is easy to compute the Jacobian matrix. We get

$$\begin{pmatrix}
\frac{\partial G_1}{\partial T_1}(y,z) & \ldots & \frac{\partial G_1}{\partial T_N}(y,z) & 0 & \ldots & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\frac{\partial G_m}{\partial T_1}(y,z) & \ldots & \frac{\partial G_m}{\partial T_N}(y,z) & 0 & \ldots & \ldots & 0 \\
z_1 \frac{\partial F_0}{\partial T_1}(y) - \frac{\partial F_1}{\partial T_1}(y) & \ldots & z_1 \frac{\partial F_0}{\partial T_N}(y) - \frac{\partial F_1}{\partial T_N}(y) & -\frac{\partial F_0}{\partial T_1}(y) & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
z_1 \frac{\partial F_0}{\partial T_1}(y) - \frac{\partial F_n}{\partial T_1}(y) & \ldots & z_1 \frac{\partial F_0}{\partial T_N}(y) - \frac{\partial F_n}{\partial T_N}(y) & -\frac{\partial F_n}{\partial T_N}(y) & 0 & \ldots & 0
\end{pmatrix}$$

We see that the submatrix J_1 of J formed by the first N columns is obtained from the Jacobian matrix of Y computed at the point y by applying elementary row transformations and when deleting the row corresponding to the polynomial F_0. Since Y is nonsingular at y, the rank of J_1 is greater or equal than $N - \dim_x Y - 1 = N - \dim X + n$. So rank $J \geq N + n - \dim X = N + n - \dim B_Y(X)$. This implies that $B_Y(X)$ is nonsingular at the point (y, z).

Remarks. 2. The pre-image $E = \sigma^{-1}(Y)$ of Y is called the *exceptional divisor* of the blowing up $\sigma : B_Y(X) \to X$. The map σ "blows down" E of $B_Y(X)$ to the closed subset Y of X of codimension $n + 1$.

3. Lemma 2 allows us to "globalize" the definition of the blow-up. Let X be any quasi-projective algebraic set and Y be its closed subset. For every affine open set $U \subset X, Y \cap U$ is a closed subset of U and the blow-up $B_{Y \cap U}(U)$ is defined. It can be shown that for any open affine cover $\{U_i\}_{i \in I}$ of X, the blowing-ups $\sigma_i : B_{U_i \cap Y}(U_i) \to U_i$ and $\sigma_j : B_{U_j \cap Y}(U_j) \to U_j$ can be "glued together" along their isomorphic open subsets $\sigma_i^{-1}(U_i \cap U_j) \cong \sigma_j^{-1}(U_j \cap U_j)$. Using more techniques one can show that there exists a quasi-projective algebraic set $B_Y(X)$ and a regular map $\sigma : B_Y(X) \to X$ such that $\sigma^{-1}(U_i) \cong B_{U_i \cap Y}(U_i)$ and, under this isomorphism, the restriction of σ to $\sigma^{-1}(U_i)$ coincides with σ_i.

The next fundamental results about blow-ups are stated without proof.

Theorem 2. *Let $f : X - \to Y$ be a rational map between two quasi-projective algebraic sets. There exists a closed subset Z of X and a regular map $f' : B_Z(X) \to Y$ such that f' is equal to the composition of the rational map $\sigma : B_Z(X) \to X$ and f.*

Although it sounds nice, the theorem gives very little. The structure of the blowing-up along an arbitrary closed subset is very complicated and hence this theorem gives little insight into the structure of any birational map. It is conjectured that every birational map between two nonsingular algebraic sets is the composition of blow-ups along nonsingular subsets and of their inverses. It is known for surfaces and, under some restriction, for threefolds.

Definition. A birational regular map $\sigma : \bar{X} \to X$ of algebraic sets is said to be a *resolution of singularities* of X if $\bar{X}$ is nonsingular and σ is an isomorphism over any open set of X consisting of nonsingular points.

The next fundamental result of Heisuki Hironaka brought him the Fields Medal in 1966:

Theorem 3. *Let X be an irreducible algebraic set over an algebraically closed field k of characteristic 0. There exists a sequence of monoidal transformations $\sigma_i : X_i \to X_{i-1}, i = 1, \ldots, n$, along nonsingular closed subsets of X_{i-1} contained in the set of singular points of X_{i-1}, and such that the composition $X_n \to X_0 = X$ is a resolution of singularities.*

A most common method for define a resolution of singularities is to embed a variety into a nonsingular one, blow up the latter and see what happens with the proper inverse transform of the subvariety (embedded resolution of singularities).

Definition. Let $\sigma : X \to Y$ be a birational regular map of irreducible algebraic sets, Z be a closed subset of X. Assume that σ is an isomorphism over an open subset U of X. The proper inverse transform of Z under σ is the closure of $\sigma^{-1}(U \cap Z)$ in X.

Clearly, the restriction of σ to the proper inverse transform Z' of Z is a birational regular map and $Z' = \sigma^{-1}(Z \cap U) \cup (Z' \cap \sigma^{-1}(X \setminus U)$.

Example 3. Let $\sigma : B = B_{\{0\}}(\mathbb{A}^2(K)) \to \mathbb{A}^2(K)$ be the blowing up of the origin $0 = V(Z_1, Z_2)$ in the affine plane. Let

$$Y = V(Z_2^2 - Z_1^2(Z_1 + 1)).$$

The pre-image $\sigma^{-1}(Y)$ is the union of the proper inverse transform $\bar{\sigma}^{-1}(Y)$ of Y and the fibre $\sigma^{-1}(0) \cong \mathbb{P}^1(K)$. Let us find $\bar{\sigma}^{-1}(Y)$. Recall that B is the union of two affine pieces:

$$U = V(Z_2 - Z_1 t) \subset X \times \mathbb{P}^1(K)_0, t = T_1/T_0,$$

$$V = V(Z_2 t' - Z_1) \subset X \times \mathbb{P}^1(K)_1, t' = T_0/T_1.$$

The restriction σ_1 of σ to U is the regular map $U \to \mathbb{A}^2(K)$ given by the homomorphism of rings:

$$\sigma_1^* : k[Z_1, Z_2] \to \mathcal{O}(U) = k[Z_1, Z_2, t]/(Z_2 - Z_1 t) \cong k[Z_1, t].$$

The pre-image of Y in U is the set of zeroes of the function

$$\sigma_1^*(Z_2^2 - Z_1^2(Z_1 + 1)) = Z_1^2(t^2 - Z_1 - 1)).$$

Similarly, the restriction σ_2 of σ to V is a regular map $V \to \mathbf{A}^2(K)$ given by the homomorphism of rings:

$$\sigma_2^* : k[Z_1, Z_2] \to \mathcal{O}(U) = k[Z_1, Z_2, t]/(Z_2 t' - Z_1) \cong k[Z_2, t'].$$

The pre-image of Y in V is the set of zeroes of the function

$$\sigma_2^*(Z_2^2 - Z_1^2(Z_1 + 1)) = Z_2^2(1 - t'^2(Z_2 t' + 1)).$$

Thus

$$\sigma^{-1}(Y) \cap U = E_1 \cup C_1, \sigma^{-1}(Y) \cap V = E_2 \cup C_2,$$

where

$$E_1 = V(Z_1), C_1 = V(t^2 - Z_1 - 1) \subset U \cong \mathbb{A}^2(K),$$
$$E_2 = V(Z_2), C_2 = V(1 - t'^2(Z_2 t' + 1)) \subset V \cong \mathbb{A}^2(K).$$

It is clear that

$$E_1 = \sigma^{-1}(0) \cap U \cong \mathbb{A}^1(K), E_2 = \sigma^{-1}(0) \cap V \cong \mathbb{A}^1(K),$$

i.e.,$\sigma^{-1}(0) = E_1 \cup E_2 \cong \mathbb{P}^1(K)$. Thus the proper inverse transform of Y is equal to the union $C = C_1 \cup C_2$. By differentiating we find that both C_1 and C_2 are nonsingular curves, hence C is nonsingular. Moreover,

$$C_1 \cap \sigma^{-1}(0) = V(Z_1, t^2 - 1) = \{(0, 1), (0, -1)\},$$

$$C_2 \cap \sigma^{-1}(0) = V(Z_2, t'^2 - 1) = \{(0, 1), (0, -1)\}.$$

Note that since $t = t'^{-1}$ at $U \cap V$, we obtain $C_1 \cap \sigma^{-1}(0) = C_2 \cap \sigma^{-1}(0)$. Hence $\sigma^{-1}(0) \cap C$ consists of two points. Moreover, it is easy to see that the curve C intersects the exceptional divisor $E = \sigma^{-1}(0)$ transversally at the two points. So the picture is as follows:

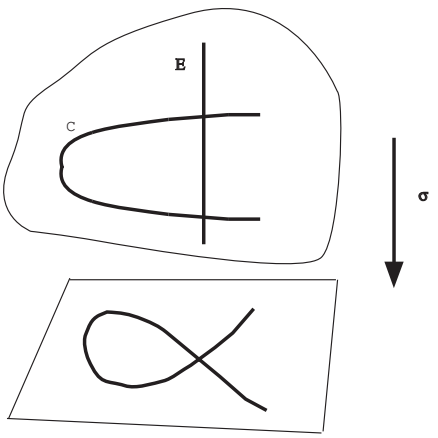

Fig.2

The restriction $\sigma : C \to Y$ is a resolution of singularities of Y.

Example 4. This time we take $Y = V(Z_1^2 - Z_2^3)$. We leave to the reader to repeat everything we have done in Example 1 to verify that the proper transform $\bar{\sigma}^{-1}(Y)$ is nonsingular and is tangent to the exceptional divisor E at one point. So, the picture is like this

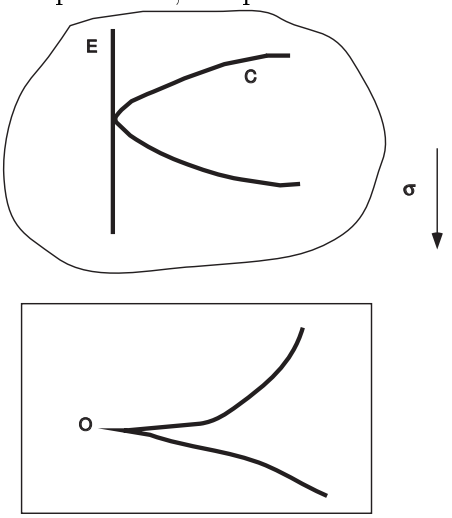

Fig.3

Example 5. Let $Y = V(F(Z_1, \ldots, Z_n)) \subset \mathbb{A}^n(K)$, where F is a homogeneous polynomial of degree d. We say that Y is a cone over $\bar{Y} = V(F(Z_1, \ldots, Z_n)$ in $\mathbb{P}^{n-1}(K)$. If identify $\mathbb{A}^n(K)$ with $\mathbb{P}^n(K)_0$, and $\bar{Y}$ with the closed subset $V(Z_0, F) \subset V(Z_0) \cong \mathbb{P}^{n-1}(K)$, we find that Y is the union of the lines joining the point $(1, 0, \ldots, 0)$ with points in $\bar{Y}$. Let $\sigma : B = B_{\{0\}}(\mathbb{A}^n(K)) \to \mathbb{A}^n(K)$ be the blowing up of the origin in $\mathbb{A}^n(K)$. Then

$$B = \cup_i U_i, U_i = B \cap \mathbb{A}^n(K) \times \mathbb{P}^{n-1}(K)_i,$$

and

$$\sigma^{-1}(Y) \cap U_i = V(F(Z_1, \ldots Z_n)) \cap V(\{Z_j - t_j Z_i\}_{j \neq i}) \cong V(Z_i^d G(t_1, \ldots, t_{n-1})),$$

where $t_j = T_j/T_0$, and G is obtained from F via dehomogenization with respect to T_i. This easily implies that

$$\sigma^{-1}(Y) = \bar{\sigma}^{-1}(Y) \cup \sigma^{-1}(0), \quad \bar{\sigma}^{-1}(Y) \cap \sigma^{-1}(0) \cong \bar{Y}.$$

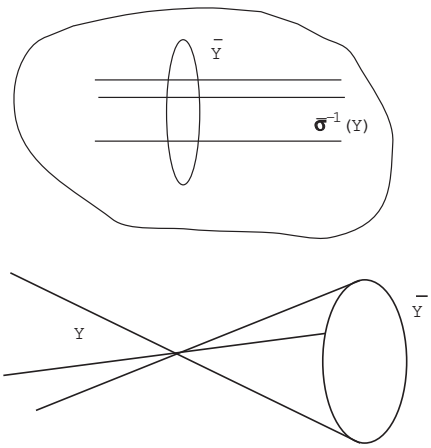

Fig.4

Example 6. Let $X = V(Z_1^2 + Z_2^3 + Z_3^4) \subset \mathbb{A}^3(K)$ and let $Y_1 = B_{\{0\}}(\mathbb{A}^3(K))$ be the blow-up. The full inverse transform of X in Y_1 is the union of three affine open subsets each isomorphic to a closed subset of $\mathbb{A}^3(K)$:

$$V_1 : Z_1^2(1 + U^3 Z_1 + V^4 Z_1^2) = 0,$$

$$V_2 : Z_2^2(U^2 + Z_2 + V^4 Z_2^2) = 0,$$

$$V_3 : Z_3^2(U^2 + V^3 Z_3 + Z_3^2) = 0.$$

The equations of the proper inverse transform X_1 are obtained by dropping the first factors. In each piece V_i the equations $Z_i = 0$ define the intersection of the proper inverse transform X_1 of X with the exceptional divisor $E_1 \cong \mathbb{P}^2(K)$. It is empty set in V_1, the affine line $U = 0$ in V_2 and V_3. The fibre of the map $X_1 \to X$ over the origin is $R_1 \cong \mathbb{P}^1(K)$. It is easy to see (by differentiation) that V_1 and V_2 are nonsingular but V_3 is singular at the point $(U, V, Z_3) = (0, 0, 0)$. Now let us start again. Replace X by $V_3 \cong V(Z_1^2 + Z_2^3 Z_3 + Z_3^2) \subset \mathbb{P}^3(K)$ and blow-up the origin. Then glue the blow-up with V_1 and V_2 along $V_3 \cap (V_1 \cup V_2)$. We obtain that the proper inverse transform X_2 of X_1 is covered by V_1, V_2 as above and three more pieces

$$V_4 : 1 + U^3 V Z_1^2 + V^3 Z_1 = 0$$

$$V_5 : U^2 + Z_2^2 V + V^2 = 0,$$

$$V_6 : U^2 + V^3 Z_3^2 + 1 = 0.$$

The fibre over the origin is the union of two curves R_2, R_3 each isomorphic to $\mathbb{P}^1(K)$. The equation of $R_2 \cup R_3$ in V_5 is $U^2 + V^2 = 0$. The equation of $R_2 \cup R_3$ in V_3 is $U^2 + 1 = 0$. Since $R_1 \cap V_3$ was given by the equation $Z_3 = 0$ and we used the substitution $Z_3 = V Z_2$ in V_5, we see that the pre-image of R_1 intersects R_1 and R_2 at their common point $(U, V, Z_2) = (0, 0, 0)$ in V_5. This point is the unique singular point of X_2. Let us blow-up the origin in V_5. We obtain X_3 which is covered by open sets isomorphic to V_1, V_2, V_4, V_6 and three more pieces:

$$V_7 : 1 + V U^2 Z_1 + V^2 = 0,$$

$$V_8 : U^2 + V^2 Z_3 + 1.$$

$$V_9 : U^2 + V Z_2 + V^2 = 0,$$

The pre-image of the origin in the proper inverse transform X_3 of X_2 consists of two curves R_4, R_5 each isomorphic to $\mathbb{P}^1(K)$. In the open set V_9 they are given by the equations $V = 0, U = \pm\sqrt{-1}V$. The inverse image of the curve R_1 intersects R_4, R_5 at their intersection point. The inverse images of R_2 intersects R_4 at the point $(U, V, Z_2) = (1, \sqrt{-1}, 0)$, the inverse image of R_3 intersects R_5 at the point $(1, -\sqrt{-1}, 0)$. Finally we blow up the origin at V_9 and obtain that the proper-inverse transform X_4 is nonsingular. It is covered by opne affine subsets isomorphic to $V_1, \ldots, V_8$ and three more open sets

$$V_{10} : 1 + UV + V^2 = 0,$$

$$V_{11} : U^2 + V + V^2 = 0,$$

$$V_{12} : U^2 + V + 1 = 0.$$

The pre-image of the origin in X_4 is a curve $R_6 \cong \mathbb{P}^1(K)$. It is given by the homogeneous equation $T_0^2 + T_1 T_2 + T_2^2$ in homogeneous coordinates of the exceptional divisor of the blow-up (compare it with Example 5). The image of the curve R_1 intersects R_6 at one point. So we get a resoluton

of singularities $\sigma : \bar{X} = X_4 \to X$ with σ^{-1} equal to the union of six curves each isomorphic to projective line. They intersect each other according to the picture:

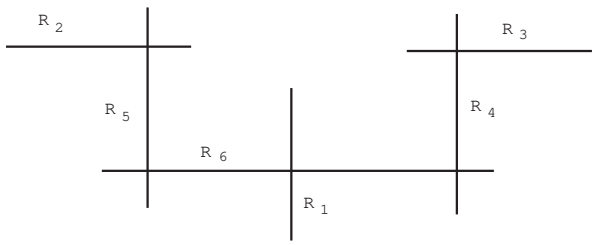

Fig.5

Let Γ be the graph whose vertices correspond to irreducible components of $\sigma^{-1}(0)$ and edges to intersection points of components. In this way we obtain the graph

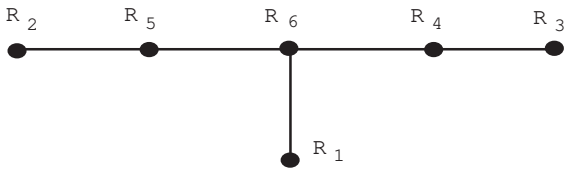

Fig.6

It is the Dynkin diagram of simple Lie algebra of type E_6.

Exercises.

1. Prove that $B_{V(I)}(X)$ is not affine unless I is (locally) a principal ideal.
2. Resolve the singularities of the curve $x^n + y^r = 0, (n, r) = 1$, by a sequence of blow-ups in the ambient space. How many blow-ups do you need to resolve the singularity?
3. Resolve the singularity of the affine surface $X : Z_1^2 + Z_2^3 + Z_3^3 = 0$ by a sequence of blow-ups in the ambient space. Describe the exceptional curve of the resolution $f : \bar{X} \to X$.
4. Describe $A(I)$, where $A = k[Z_1, Z_2,], I = (Z_1, Z_2^2)$. Find the closed subset $B_I(A)$ of $\mathbb{A}^2(K) \times \mathbb{P}^1(K)$ defined by the kernel of the homomorphism $\phi : A[T_0, T_1] \to A(I), T_0 \to Z_1, T_2 \to Z_2^2$. Is it nonsingular?
5*. Resolve the singularities of the affine surface $X : Z_1^2 + Z_2^3 + Z_3^5 = 0$ by a sequence of blow-ups in the ambient space. Show that one can find a resolution of singularities $f : \bar{X} \to X$ such that the graph of irreducible components of $f^{-1}(0)$ is the Dynkin diagram of the root system of a simple Lie algebra of type E_8.
6*. Resolve the singularities of the affine surface $X : Z_1 Z_2^3 + Z_1^3 + Z_3^2 = 0$ by a sequence of blow-ups in the ambient space. Show that one can find a resolution of singularities $f : \bar{X} \to X$ such that the graph of irreducible components of $f^{-1}(0)$ is the Dynkin diagram of the root system of a simple Lie algebra of type E_7.
7*. Resolve the singularities of the affine surface $X : Z_1(Z_2^2 + Z_1^n) + Z_3^2 = 0$ by a sequence of blow-ups in the ambient space. Show that one can find a resolution of singularities $f : \bar{X} \to X$ such that the graph of irreducible components of $f^{-1}(0)$ is the Dynkin diagram of the root system of a simple Lie algebra of type D_n.

8*. Resolve the singularities of the affine surface $X : Z_1 Z_2^2 + Z_3^{n+1} = 0$ by a sequence of blow-ups in the ambient space. Show that one can find a resolution of singularities $f : \bar{X} \to X$ such that the graph of irreducible components of $f^{-1}(0)$ is the Dynkin diagram of the root system of a simple Lie algebra of type A_n.

9*. Let $f : \mathbb{P}^2(K) - \to \mathbb{P}^2(K)$ be the rational map given by the formula $T_0 \to T_1 T_2, T_1 \to T_2 T_3, T_2 \to T_0 T_1$. Show that there exist two birational regular maps $\sigma_1, \sigma_2 : X \to \mathbb{P}^2(K)$ with $f \circ \sigma_1 = \sigma_2$ such that the restriction of each σ_i over $\mathbb{P}^2(K)_j, j = 0, 1, 2$ is isomorphic to the blow-up along one point.

Lecture 17. RIEMANN-ROCH THEOREM FOR CURVES

Let k be an arbitrary field and K be its algebraic closure. Let X be a projective variety over k such that $X(K)$ is a connected nonsingular curve.

A *divisor* on X is an element of the free abelian group $\mathbb{Z}^X$ generated by the set $X(K)$ (i.e. a set of maps $X(K) \to \mathbb{Z}$ with finite support). We can view a divisor as a formal sum

$$D = \sum_{x \in X(K)} n(x)x,$$

where $x \in X$, $n(x) \in \mathbb{Z}$ and $n(x) = 0$ for all x except finitely many. The group law is of course defined coefficientwisely. We denote the group of divisors by $\mathrm{Div}(X)$.

A divisor D is called *effective* if all its coefficients are non-negative. Let $\mathrm{Div}(X)^+$ be the semi-group of effective divisors. It defines a partial order on the group $\mathrm{Div}(X)$:

$$D \geq D' \iff D - D' \geq 0.$$

Any divisor D can be written in a unique way as the difference of effective divisors

$$D = D_+ - D_-.$$

We define the *degree* of a divisor $D = \sum n(x)x$ by

$$\deg(D) = \sum_{x \in X(K)} n(x)[k(x) : k].$$

Recall that $k(x)$ is the residue field of the local ring $\mathcal{O}_{X,x}$. If $k = K$, then $k(x) = k$.

The local ring $\mathcal{O}_{X,x}$ is a regular local ring of dimension 1. Its maximal ideal is generated by one element t. We call it a *local parameter*. For any nonzero $a \in \mathcal{O}_{X,x}$, let $\nu_x(a)$ be the the smallest r such that $a \in \mathfrak{m}_{X,x}^r$.

Lemma 1. *Let $a, b \in \mathcal{O}_{X,x} \setminus \{0\}$. The following properties hold:*

(i) $\nu_x(ab) = \nu_x(f) + \nu_x(g)$;
(ii) $\nu_x(a + b) \geq \min\{\nu_x(a), \nu_x(b)\}$ if $a + b \neq 0$.

Proof. If $\nu_x(a) = r$, then $a = t^r a_0$, where $a_0 \notin \mathfrak{m}_{X,x}$. Similarly we can write $b = t^{\nu_x} b_0$. Assume $\nu_x(a) \leq \nu_x(b)$ Then

$$ab = t^{\nu_x(a)+\nu_x(b)} a_0 b_0, \quad a + b = t^{\nu_x(a)}(a_0 + t^{\nu_x(b)-\nu_x(b)} b_0)$$

This proves (i),(ii). Note that we have the equality in (ii) when $\nu_x(a) \neq \nu_x(b)$.

Let $f \in R(X)$ be a nonzero rational function on X. Since $R(X) = Q(\mathcal{O}_{X,x})$, we can write f as a fraction a/b, where $a, b \in \mathcal{O}_{X,x}$. We set

$$\nu_x(f) = \nu_x(a) - \nu_x(b).$$

It follows from Lemma 1 (i), that this definition does not depend on the way we write f as a fraction a/b.

Lemma 2. *Let $f, g \in R(X) \setminus \{0\}$. The following properties hold:*

(i) $\nu_x(fg) = \nu_x(f) + \nu_x(g)$;
(ii) $\nu_x(f+g) \geq \min\{\nu_x(f), \nu_x(g)\}$ if $f + g \neq 0$;
(iii) $\nu_x(f) \geq 0 \Leftrightarrow f \in \mathcal{O}_{X,x}$;
(iv) $\nu_x(f) \neq 0$ only for finitely many points $x \in X(K)$.

Proof. (i), (ii) follow immediately from Lemma 1. Assertion (iii) is immediate. Let U be an open Zariski set such that $f, f^{-1} \in \mathcal{O}(U)$. Then, for any $x \in U$, $\nu_x(f) = -\nu_x(f^{-1}) \geq 0$ implies that $\nu_x(f) = 0$. Since $X(K) \setminus U$ is a finite set, we get (iv).

Now we can define the *divisor of a rational function* f by setting

$$\operatorname{div}(f) = \sum_{x \in X(K)} \nu_x(f)x.$$

The following Proposition follows immediately from Lemma 2.

Proposition 1. *For any nonzero $f, g \in R(X)$,*

$$\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g).$$

In particular, the map $f \mapsto \operatorname{div}(f)$ defines a homomorphism of groups

$$\operatorname{div} : R(X)^* \to \operatorname{Div}(X).$$

If $D = \operatorname{div}(f)$, we write $D_+ = \operatorname{div}(f)_0, D_- = \operatorname{div}(f)_\infty$. We call $\operatorname{div}(f)_0$ the *divisor of zeroes* of f and $\operatorname{div}(f)_\infty$ the *divisor of poles* of f. We say that $\nu_x(f)$ is the order of pole (or zero) if $x \in \operatorname{div}(f)_\infty$ (or $\operatorname{div}(f)_0$).

We define the divisor class group of X by

$$\operatorname{Cl}(X) = \operatorname{Div}(X)/\operatorname{div}(R(X)^*).$$

Two divisors in the same coset are called *linearly equivalent*. We write this $D \sim D'$.

For any divisor $D = \sum n(x)x$ let

$$L(D) = \{f \in R(X) : \operatorname{div}(f) + D \geq 0\} = \{f \in R(X) : \nu_x(f) \geq -n(x), \forall x \in X(K)\}.$$

It follows from Lemma 2 that $L(D)$ is a vector space over k. The Riemann-Roch formula is a formula for the dimension of the vector space $L(D)$.

Proposition 2.

(i) $L(D)$ is a finite-dimensional vector space over k;
(ii) $L(D) \cong L(D + \mathrm{div}(f))$ for any $f \in R(X)$;
(iii) $L(0) = k$.

Proof. (i) Let $D = D_+ - D_-$. then $D_+ = D + D_-$ and for any $f \in L(D)$, we have

$$(f) + D \geq 0 \Rightarrow \mathrm{div}(f) + D + D_- = (f) + D_+ \geq 0.$$

This shows that $f \in L(D_+)$. Thus it suffices to show that $L(D)$ is finite-dimensional for an effective divisor D. For each $x \in X(K)$, $\nu_x(f) \geq -n(x)$ is non-positive. Let t be a local parameter at x. Then $\nu_x(t^{n(x)}f) \geq 0$ and hence $\nu_x(t^{n(x)}f) \in \mathcal{O}_{X,x}$. Consider the inclusion $\mathcal{O}_{X,x} \subset K[[T]]$ given by the Taylor expansion. Then we can write

$$f = T^{-n(x)}(\sum_{i=0}^{\infty} a_i T^i),$$

where the equality is taken in the field of fractions $K((T))$ of $K[[T]]$. We call the right-hans side, the *Laurent series* of f at x. Consider the linear map

$$L(D) \to \oplus_{x \in X(K)} T^{-n(x)} K[[T]]/K[[T]] \cong \oplus_{x \in X(K)} K^{n(x)},$$

which assigns to f the collection of cosets of the Laurent series of f modulo $k[[T]]$. The kernel of this homomorphism consists of functions f such that $\nu_x(f) \geq 0$ for all $x \in X(K)$, i.e., regular function on X. Since $X(K)$ is a connected projective set, any regular function on X is a constant. This shows that $L(D) \otimes_k K$ is a finite-dimensional vector space over K. This easily implies that $L(D)$ is a finite-dimensional vector space over k.

(ii) Let $g \in L(D + \mathrm{div}(f))$, then

$$\mathrm{div}(g) + \mathrm{div}(f) + D = \mathrm{div}(fg) + D \geq 0.$$

This shows that the injective homomorphsim of the additive groups $R(D) \to R(D), g \mapsto fg$, restricting to the space $L(D + \mathrm{div}(f))$ defines an an injective linear map $L(D + \mathrm{div}(f)) \cong L(D)$. The inverse map is defined by the multiplication by f^{-1}.

(iii) Clearly $L(0) = \mathcal{O}(X) = k$.

It follows from the previous Proposition that $\dim_k L(D)$ depends only on the divisor class of D. Thus the function $\dim : \mathrm{Div}(X) \to \mathbb{Z}, D \mapsto \dim_k L(D)$ factors through a function on $\mathrm{Cl}(X)$ which we will continue to denote by dim.

Theorem (Riemann-Roch). *There exists a unique divisor class K_X on X such that for any divisor class D*

$$\dim_k L(D) = \deg(D) + \dim_k L(K_X - D) + 1 - g,$$

where $g = \dim_k L(K_X)$ (called the genus of X),

Before we start proving this theorem, let us deduce some immediate corollaries.

Taking D from K_X, we obtain

$$\deg(D) = 2g - 2.$$

Taking $D = \mathrm{div}(f)$, we get

$$\deg(\mathrm{div}(f)) = 0.$$

This implies that the degrees of linearly equivalent divisors are equal. In particlular, we can define the degree of a divisor class.

Also observe that, for any divisor D of negative degree we have $L(D) = \{0\}$. In fact, if $\mathrm{div}(f) + D \geq 0$ for some $f \in R(X)^*$, then $\deg(\mathrm{div}(f) + D) = \deg(D) \geq 0$. Thus if take a divisor D of degree $> 2g - 2$, we obtain $\dim L(K_X - D) = 0$. Thus the Riemann-Roch Theorem implies the following

Corollary 1. *Assume* $\deg(D) > 2g - 2$, *then*

$$\dim L(D) = \deg(D) + 1 - g.$$

Example 1. Assume $X = \mathbb{P}^1_k$. Let $U = \mathbb{P}^1(K)_0 = \mathbb{A}^1(K) = K$. Take $D = x_1 + \ldots + x_n$, where $x_i \in k$. Then $L(D)$ consists of rational functions $f = P(Z)/Q(Z)$, where $P(Z), Q(Z)$ are polynomials with coefficients in k and $Q(T)$ has zeroes among the points x_i's. This easily implies that $L(D)$ consists of functions

$$P(T_0, T_1)/(T_1 - a_0 T_0) \cdots (T_1 - x_i T_0),$$

where $\deg P(T_0, T_1) = n$. The dimension of $L(D)$ is equal to $n + 1$. Taking n sufficiently large, and applying the Corollary, we find that $g = 0$.

The fact that $\deg(\mathrm{div}(f)) = 0$ is used for the proof of the Riemann-Roch formula. We begin with proving this result which we will need for the proof. Another proof of the formula, using the sheaf theory, does not depend on this result.

Lemma 3. *(Approximation lemma). Let* $x_1, \ldots, x_n \in X, \phi_1, \ldots, \phi_n \in R(X)$, *and* N *be a positive integer. There exists a rational function* $f \in R(X)$ *such that*

$$\nu_x(f - \phi_i) > N, \quad i = 1, \ldots, n.$$

Proof. We may assume that X is a closed subset of $\mathbb{P}^n$. Choose a hyperplane H which does not contain any of the points x_i. Then $\mathbb{P}^n \setminus H$ is affine, and $U = X \cap (\mathbb{P}^n \setminus H)$ is a closed subset of $\mathbb{P}^n \setminus H$. Thus U is an affine open subset of X containing the points x_i. This allows us to assume that X is afiine. Note that we can find a function g_i which vanishes at a point x_i and has poles at the other points $x_j, j \neq i$. One get such a function as the ratio of a function vanishing at x_i but not at any x_j and the function which vanishes at all x_j but not at x_i. Let $f_i = 1/(1 + g_i^m)$. Then $f_i - 1 = -g_i^m/(1 + g_i^m)$ has zeroes at the points x_j and has zero at x_i. By taking m large enough, we may assume that $\nu_{x_i}(f_i - 1), \nu_{x_j}(f_i - 1)$ are sufficiently large. Now let

$$f = f_1\phi_1 + \cdots + f_n\phi_n.$$

It satisfies the assertion of the lemma. Indeed, we have

$$\nu_{x_i}(f - \phi_i) = \nu_{x_i}(f_1\phi_1 + \ldots + f_{i-1}\phi_{i-1} + (f_i - 1)\phi_i + f_{i+1}\phi_{i+1} + \ldots + f_n\phi_n).$$

This can be made arbitrary large.

Corollary 1. *Let $x_1, \dots, x_n \in X$ and $m_1, \dots, m_n$ be integers. There exists a rational function $f \in R(X)$ such that*

$$\nu_{x_i}(f) = m_i, \quad i = 1, \dots, n.$$

Proof. Let $t_1, \dots, t_n$ be local parameters at $x_1, \dots, x_n$, respectively. This means that $\nu_{x_i}(t_i) = 1, i = 1, \dots, n$. Take N larger than each m_i. By the previous lemma, there exists $f \in R(X)$ such that $\nu_{x_i}(f - t_i^{m_i}) > m_i, i = 1, \dots, n$. Thus, by Lemma 2,

$$\nu_{x_i}(f) = \min\{\nu_{x_i}(t_i^{m_i}), \nu_{x_i}(f - t_i^{m_i})\} = m_i, \quad i = 1, \dots, n.$$

Let $f : X \to Y$ be a regular map of projective algebraic curves and let $y \in Y, x \in f^{-1}(y)$. Let t be a local parameter at y. We set

$$e_x(f) = \nu_x(f^*(t)).$$

It is easy to see that this definition does not depend on the choice of a local parameter. The number $e_x(f)$ is called the *ramification index* of f at x.

Lemma 4. *For any rational function $\phi \in R(Y)$ we have*

$$\nu_x(\phi^*(\phi)) = e_x \nu_y(\phi).$$

Proof. This follows immediately from the definition of the ramification index and Lemma 2.

Corollary 2. *Let $f^{-1}(y) = \{x_1, \dots, x_r\}$ and $e_i = e_{x_i}$. Then*

$$\sum_{i=1}^{r} e_i \le [R(X) : f^*(R(Y))].$$

Proof. Applying Corollary 1, we can find some rational functions $\phi_1^{(i)}, \dots, \phi_{e_i}^{(i)}$, $i = 1, \dots, r$ such that

$$\nu_{x_i}(\phi_s^{(i)}) = s, \quad \nu_{x_j}(\phi_s^{(i)}) >> 0, \ j \neq i, \ s = 1, \dots, e_i.$$

Let us show that $\sum_{i=1}^{r} e_i$ functions obtained in this way are linearly independent over $f^*(R(Y))$. Assume

$$\sum_{i=1}^{r} \sum_{s=1}^{e_i} a_{is} \phi_s^{(i)} = 0$$

for some $a_{is} \in f^*(R(Y))$ which we will identify with functions on Y. Without loss of generality we may assume that

$$\nu_y(a_{1s}) = \min\{\nu_y(a_{is}) : a_{is} \neq 0\}.$$

Dividing by by a_{1s}, we get $\sum_{is} c_{is} \phi_s^{(i)} = 0$, where

$$c_{1s} = 1, \quad \nu_y(c_{is}) \ge 0,$$

We have

$$\sum_{s=1}^{e_1} \phi_s^{(1)} = -\big(\sum_{i=2}^{r}\sum_{s=1}^{e_s} c_{is}\phi_s^{(i)}\big).$$

By Lemma 4,

$$\nu_{x_1}(c_{1s}\phi_s^{(1)}) = \nu_{x_1}(c_{1s}) + \nu_{x_1}(\phi_s^{(1)}) \equiv s \bmod e_1.$$

This easily implies that no subset of summands in the left-hand side L.H.S. add up to zero. Therefore,

$$\nu_{x_1}(L.H.S) = \min_s\{\nu_{x_1}(c_{1s}\phi_s^{(1)}\} \leq e_1.$$

On the other hand, $\nu_{x_1}(R.H.S.)$ can be made arbitrary large. This contradiction proves the assertion.

Let Λ be the direct product of the fraction fields $R(X)_x$ of the local rings $\mathcal{O}_{X,x}$, where $x \in X$. By using the Taylor expansion we can embed each $R(X)_x$ in the fraction field $K((T))$ of $K[[T]]$. Thus we may view Λ as the subring of the ring of functions

$$K((T))^X = \mathrm{Maps}(X, K((T)).$$

The elements of Λ will be denoted by $(\xi_x)_x$. We consider the subring $\mathbf{A}_X$ of Λ formed by $(\xi_x)_x$ such that $\xi_x \in \mathcal{O}_{X,x}$ except for finitely many x's. Such elements are called *adeles*. For each divisor $D = \sum n(x)x$, we define the vector space over the field k:

$$\Lambda(D) = \{(\xi_x)_x \in \Lambda : \nu_x(\xi_x) \geq -n(x)\}.$$

Clearly,

$$\Lambda(D) \cap R(X) = L(D), \quad \Lambda(D) \subset \mathbf{A}_X.$$

For each $\phi \in R(X)$, let us consider the adele

$$\phi = (\phi_x)_x,$$

where ϕ_x is the element of $R(X)_x$ represented by ϕ. Recall that the field of fractions of $\mathcal{O}_{X,x}$ is equal to the field $R(X)$. Such adeles are called *principal adeles*. We will identify the subring of principal adeles with $R(X)$.

Lemma 5. *Assume $D' \geq D$. Then*

(i) $\Lambda(D) \subset \Lambda(D')$;
(ii) $\dim(\Lambda(D')/\Lambda(D)) = \deg(D') - \deg(D)$;
(iii)

$$\dim_k L(D') - \dim_k L(D) = \deg(D') - \deg(D) - \dim_k(\Lambda(D') + R(X)/(\Lambda(D) + R(X)),$$

where the sums are taken in the ring of adeles.

Proof. (i) Obvious
(ii) Let $D = \sum n(x)x$, $D' = \sum n(x)'x$. If $\xi = (\xi_x)_x \in L(D')$, the Laurent expansion of ξ_x looks like

$$\xi_x = T^{-n(x)}(a_0 + a_1T + \ldots).$$

This shows that

$$\Lambda(D')/\Lambda(D) \cong \bigoplus_{x\in X}(T^{-n(x)'}K[[T]]/T^{-n(x)}K[[T]]) \cong \bigoplus_{x\in X} K^{n(x)'-n(x)},$$

which proves (ii).

(iii) Use the following isomorphisms of vector spaces

$$\Lambda(D') + R(X)/\Lambda(D') \cap R(X) \cong \Lambda(D') \oplus R(X),$$

$$\Lambda(D) + R(X)/\Lambda(D) \cap R(X) \cong \Lambda(D) \oplus R(X),$$

$$\Lambda(D') \oplus R(X)/\Lambda(D) \oplus R(X) \cong \Lambda(D')/\Lambda(D).$$

Then the canonical surjection

$$\Lambda(D') + R(X) \to \Lambda(D') \oplus \Lambda(D') \oplus R(X)$$

induces a surjection

$$\big(\Lambda(D') + R(X)\big)/\big(\Lambda(D) + R(X)\big) \to \big(\Lambda(D') \oplus R(X)\big)/\big(\Lambda(D) \oplus R(X)\big)$$

with kernel $\Lambda(D') \cap R(X)/\Lambda(D) \cap R(X) \cong L(D')/L(D)$. This implies that

$$\deg(D') - \deg(D) = \dim_k \Lambda(D')/\Lambda(D)$$

$$= \dim_k bigl(\Lambda(D') + R(X)\big)/\big(\Lambda(D) + R(X)\big) + \dim_k L(D')/L(D).$$

Proposition 3. *In the notation of Corollary 2,*

$$e_1 + \ldots + e_r = [R(X) : f^*(R(Y))].$$

Proof. Let $f : X \to Y$, $g : Y \to Z$ be two regular maps. Let $z \in Z$ and

$$g^{-1}(z) = \{y_1, \ldots, y_r\}, \quad f^{-1}(y_j) = \{x_{1j}, \ldots, x_{r_j j}\}.$$

Denote by e_i the ramification index of g at y_i and by e_{ij} the ramification index of f at x_{ij}. By Corollary 2,

$$\sum e_j e_{ij} = e_1(\sum e_{i1}) + \ldots + e_r(\sum e_{ir}) \leq (\sum e_j)[R(X) : f^*(R(Y))].$$

If we prove the theorem for the maps g and $g \circ f$, we get

$$[R(X) : R(Z)] = \sum e_i e_{ij} \leq [R(Y) : R(Z)][R(X) : R(Y)] = [R(X) : R(Z)]$$

which proves the assertion.

Let $\phi \in R(Y)$ considered as a rational (and hence regular) map $g : Y \to \mathbb{P}^1$ of nonsingular projective curves. The composed map $g \circ f : X \to \mathbb{P}^1$ is defined by the rational function $f^*(\phi) \in R(X)$. By the previous argument, it is enough to prove the proposition in the case when f is a regular map from X to $\mathbb{P}^1$ defined by a rational function ϕ. If $t = T_1/T_0 \in R(\mathbb{P}^1)$, then $\phi = f^*(t)$.

Without loss of generality we may assume that $y = \infty = (0,1) \in \mathbb{P}^1$. Let $f^{-1}(y) = \{x_1, \ldots, x_r\}$. It is clear that

$$\nu_{x_i}(\phi) = \nu_{x_i}(f^*(t)) = -\nu_{x_i}(f^*(t^{-1})).$$

Since t is a local parameter at y, we have that the divisor $D = \mathrm{div}(\phi)_\infty$ of poles of f is equal to the sum $\sum e_i x_i$. Let $(\phi_1, \ldots, \phi_n)$ be a basis of $R(X)$ over $R(\mathbb{P}^1)$. Each ϕ_i satisfies an equation

$$a_0(\phi)X^d + a_1(\phi)X^{d-1} + \ldots + a_d(\phi) = 0,$$

where $a_i(Z)$ some rational function in a variable Z. After reducing to common denominator and multiplying the equation by the $(d-1)$th power of the first coefficient, we may assume that the equation is monic, and hence each ϕ_i is integral over the ring $K[t]$, but $1 + a_1(\phi)\phi_i^{-1} + \ldots + a_d(\phi)\phi_i^{-d} = 0$ shows that this is impossible. Thus we see that every pole of ϕ_i belongs to the set $f^{-1}(\infty)$ of poles of ϕ. Choose an integer m_0 such that

$$\mathrm{div}(\phi_i) + m_0 D \geq 0, \quad i = 1, \ldots, n.$$

Let m be sufficiently large integer. For each integer s satisfying $0 \leq s \leq m - m_0$, we have $\phi^s \phi_i \in L(mD)$. Since the set of functions

$$\phi^s \phi_i, \quad i = 1, \ldots, n, \quad s = 0, \ldots, m - m_0$$

is linearly independent over k, we obtain $\dim_k L(D) \geq (m - m_0 + 1)n$. Now we apply Lemma 5 (iii), taking $D' = mD, D = 0$. Let

$$N_m = \dim_k(\Lambda(mD) + R(X)/\Lambda(0) + R(X)).$$

Then

$$m\deg(D) = m(\sum e_i) = N_m + \dim L(mD) - 1 \geq N_m + (m - m_0 + 1)n - 1.$$

Dividing by m and letting m go to infinity, we obtain $\sum e_i \geq n = [R(X) : R(Y)]$. Together with Corollary 2, this proves the assertion.

Corollary 1. *For any rational function $\phi \in R(X)$,*

$$\deg(\mathrm{div}(f)) = 0.$$

Proof. Let $f : X \to \mathbb{P}^1$ be the regular map defined by ϕ. Then, as we saw in the previous proof, $\deg(\mathrm{div}(f)_\infty) = [R(X) : k(\phi)]$. Similarly, we have $\deg(\mathrm{div}(\phi^{-1})_\infty) = [R(X) : k(\phi)]$. Since $\mathrm{div}(\phi) = \mathrm{div}(f)_0 - \mathrm{div}(f)_\infty$, we are done.

Corollary 2. *Assume $\deg(D) < 0$. Then $L(D) = \{0\}$.*

Set

$$r(D) = \deg(D) - \dim L(D).$$

By Corollary 1, this number depends only on the linear equivalence class of D. Note that, assuming the Riemann-Roch Theorem, we have $r(D) = g - 1 - \dim L(K - D) \leq g - 1$. This shows that the function $D \mapsto r(D)$ is bounded on the set of divisors. Let us prove it.

Lemma 6. *The function $D \mapsto r(D)$ is bounded on the set* $\mathrm{Div}(X)$.

Proof. As we have already observed, it suffices to prove the boundness of this function on $\mathrm{Cl}(X)$. By Proposition 3(iii), for any two divisors D', D with $D' \geq D$,

$$r(D') - r(D) = \dim(\Lambda(D') + R(X))/(\Lambda(D) + R(X)) \geq 0.$$

Take a non-zero rational function $\phi \in R(X)$. Let $D = \mathrm{div}(\phi)_\infty, n = \mathrm{deg}D$. As we saw in the proof of Proposition 3,

$$mn \geq r(mD) - r(0) + m(m - m_0 - n) - 1 = r(MD) + mn - m_0 n.$$

This implies $r(mD) \leq m_0 n - n$, hence $r(mD)$ is bounded as a function of n. Let $D' = \sum n(x_i)x_i$ be a divisor, $y_i = f(x_i) \in \mathbb{P}^1$, where $f : X \to \mathbb{P}^1$ is the regular map defined by ϕ. Let $P(t)$ be a polynomial vanishing at the points y_i which belong to the affine part $(\mathbb{P}^1)_0$. Replacing $P(t)$ by some power, if needed, we have $f^*(P(t)) = P(\phi) \in R(X)$ and $\mathrm{div}(P(\phi)) + mD \geq D'$ for sufficiently large m. This implies that

$$r(D') \leq r(mD + \mathrm{div}(P(\phi))) = r(mD)).$$

This proves the assertion.

Corollary. *For any divisor D*

$$\dim \mathbf{A}/(\Lambda(D) + R(X)) < \infty.$$

Proof. We know that

$$r(D') - r(D) = \dim(\Lambda(D') + R(X)/\Lambda(D) + R(X))$$

is bounded on the set of pairs (D, D') with $D' \geq D$. Since every adele ξ belongs to some space $\Lambda(D)$, the falsity of our assertion implies that we can make the spaces $(\Lambda(D') + R(X)/\Lambda(D) + R(X))$ of arbitrary dimension. This contradicts the boundness of $r(D') - r(D)$.

Let

$$H(D) = \mathbf{A}/(\Lambda(D) + R(X)).$$

We have $r(D') - r(D) = \dim_k H(D) - \dim_k H(D')$ if $D' \geq D$. In particular, setting

$$g = \dim_k H(0),$$

we obtain

$$r(D) = g - 1 - \dim_k H(D),$$

or, equvalently

$$\dim_k L(D) = \deg(D) + \dim_k H(D) - g + 1. \tag{1}$$

To prove the Riemann-Roch Theorem, it suffices to show that

$$\dim_k H(D) = \dim_k L(K - D).$$

To do this we need the notion of a *differential* of the field X.

A differential ω of $R(X)$ is a linear function on $\mathbf{A}$ which vanish on some subspace $\Lambda(D)+R(X)$. A differential can be viewed as an element of the dual space $H(D)^*$ for some divisor D.

Note that the set $\Omega(X)$ of differentials is a vector space over the field $R(X)$. Indeed, for any $\phi \in R(X)$ and $\omega \in \Omega(X)$, we can define

$$\phi\omega(\xi) = \omega(\phi\xi).$$

This makes $\Omega(X)$ a vector space over $R(X)$. If $\omega \in H(D)^*$, then $\phi\omega \in H(D - \mathrm{div}(\phi))^*$.

Let us prove that

$$\dim_{R(X)}\Omega(X) = 1.$$

Lemma 7. *Let $\omega \in \Omega(X)$. There exists a maximal divisor D (with respect to the natural order on $\mathrm{Div}(X)$) such that $\omega \in H(D)^*$.*

Proof. If $\omega \in H(D_1) \cup H(D_2)$, then $\omega \in H(D_3)$, where $D_3 = \sup(D_1, D_2)$. This shows that it suffices to verify that the degrees of D such that $\omega \in H(D)^*$ is bounded. Let D' be any divisor, $\phi \in L(D')$. Since $D + \mathrm{div}(\phi) \geq D - D'$, we have

$$\Lambda(D - D') \subset \Lambda(D + \mathrm{div}(\phi)).$$

Let $\phi_1, \ldots, \phi_n$ be linearly independent elements from $L(D')$. Since ω vanishes on $\Lambda(D)$, the functions $\phi_1\omega, \ldots, \phi_n\omega$ vanish on $\Lambda(D - D') \subset \Lambda(D + \mathrm{div}(\phi_i))$ and linearly independent over K. Thus

$$\dim_k H(D - D') \geq \dim_k L(D').$$

Applying equality (1) from above, we find

$$\dim_k L(D - D') = \deg(D) + \deg(D') - 1 + g \geq \dim_k L(D') \geq$$
$$\deg(D') + 1 - g + \dim_k H(D').$$

Taking D' with $\deg(D') > \deg(D)$ to get $L(D - D') = \{0\}$, we obtain

$$\deg(D) \leq 2g - 2.$$

Proposition 4.

$$\dim_{R(X)}\Omega(X) = 1.$$

Proof. Let ω, ω' be two linearly independent differentials. For any linearly independent (over K) sets of functions $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_n\}$ in $R(X)$, the differentials

$$a_1\omega, \ldots, a_n\omega, b_1\omega, \ldots, b_n\omega \tag{2}$$

are linearly independent over K. Let D be such that $\omega, \omega' \in \Omega(D)$. It is easy to see that such D always exists. For any divisor D', we have

$$\Lambda(D - D') \subset \Lambda(D + \mathrm{div}(\phi)), \ \forall \phi \in L(D').$$

Thus the $2n$ differentials from equation (2), where $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are two bases of $L(D')$, vanish on $\Lambda(D - D')$. Therefore,

$$\dim_k H(D - D') \geq 2\dim_k L(D').$$

Again, as in the proof of the previous lemma, we find

$$\dim_k L(D - D') \geq 2\deg(D') + 2 - 2g.$$

taking D' with $\deg(D') > \deg(D) + 2 - 2g$, we obtain

$$0 \geq 2\deg(D') + 2 - 2g > 0.$$

This contradiction proves the assertion.

For any $\omega \in \Omega(X)$ we define the divisor of ω as the largest divisor D such that $\omega \in H(D)$. We denote it by $\mathrm{div}(\omega)$.

Corollary. *Let $\omega, \omega' \in \Omega(X)$. Then* $\mathrm{div}(\omega)$ *is linearly equivalent to* $\mathrm{div}(\omega')$.

Proof. We know that $\omega \in H(D)$ implies $\phi\omega \in H(D + \mathrm{div}(\phi))$. Thus the divisor of $\phi\omega$ is equal to $\mathrm{div}(\omega) + \mathrm{div}(\phi)$. But each $\omega' \in \Omega(X)$ is equal to $\phi\omega$ for some $\phi \in R(X)$.

The linear equivalence class of the divisor of any differential is denoted by K_X. It is called the *canonical class* of X. Any divisor from K_X is called a *canonical divisor* on X.

Theorem (Riemann-Roch). *Let D be any divisor on X, and K any canonical divisor. Then*

$$\dim_k L(D) = \deg(D) + \dim_k L(K - D) + 1 - g,$$

where $g = \dim_k L(K)$.

Proof. Using formula (2), it suffices to show that

$$\dim_k H(D) = \dim_k L(K - D),$$

or, equivalently, $\dim_k H(K - D) = \dim_k L(D)$. We will construct a natural isomorphism of vector spaces

$$c : L(D) \to H(K - D)^*.$$

Let $\phi \in L(D), K = \mathrm{div}(\omega)$. Then

$$\mathrm{div}(\phi\omega) = \mathrm{div}(\omega) + \mathrm{div}(\phi) \geq K - D.$$

Thus $\phi\omega$ vanishes on $\Lambda(K - D)$, and therefore $\phi\omega \in H(K - D)^*$. This defines a linear map $c : L(D) \to H(K_D)^*$. Let $\alpha \in H(K - D)^*$ and $K' = \mathrm{div}(\alpha)$. Since K' is the maximal divisor D' such that α vanishes on $\Lambda(D')$, we have $K' \geq K - D$. By Proposition 4, $\alpha = \phi\omega$ for some $\phi \in R(X)$. Hence

$$K' - K = \mathrm{div}(\alpha) - \mathrm{div}(\omega) = \mathrm{div}(\phi) \geq -D.$$

showing that $\phi \in L(D)$. This defines a linear map

$$H(K - D)^* \to L(D),\ \alpha \to \phi.$$

Obviously this map is the inverse of the map c.

The number $g = \dim_k L(K)$ is called the *genus* of X. It is easy to see by going through the definitions that two isomorphic curves have the same genus.

Now we will give some nice applications of the Riemann-Roch Theorem. We have already deduced some corollaries from the RRT. We repeat them.

Corollary.

$$\deg(K_X) = 2g - 2,$$

$$\dim_k L(D) = \deg(D) + 1 - g,$$

if $\deg(D) \geq 2g - 2$ and $D \notin K_X$.

Theorem 1. *Assume $g = 0$ and $X(k) \neq \emptyset$ (e.g. $k = K$). Then $X \cong \mathbb{P}^1$.*

Proof. By Riemann-Roch, for any divisor $D \geq 0$,

$$\dim_k L(D) = \deg(D) + 1.$$

Dake $D = 1 \cdot x$ for some point $x \in X(k)$. Then $\deg(D) = 1$ and $\dim L(D) = 2$. Thus there exists a nonconstant function $\phi \in R(X)$ such that $\mathrm{div}(\phi) + D \geq 0$. Since ϕ cannot be regular everywhere, this means that ϕ has a pole of order 1 at x and regular in $X \setminus \{x\}$. Consider the regular map $f : X \to \mathbb{P}^1$ defined by ϕ. The fibre $f^{-1}(\infty)$ consists of one point x and $\nu_x(\phi) = -1$. Applying Proposition 3, we find that $[R(X) : R(\mathbb{P}^1)] = 1$, i.e. X is birationally (and hence biregularly) isomorphic to $\mathbb{P}^1$.

Theorem 2. *Let $X = V(F) \subset \mathbb{P}^2$ be a nonsingular plane curve of degree d. Then*

$$g = (d-1)(d-2)/2.$$

Proof. Let H be a general line intersecting X at d points $x_1, \ldots, x_d$. By changing coordinates, we may assume that this line is the line at infinity $V(T_0)$. Let $D = \sum_{i=1}^{d}$. It is clear that every rational function ϕ from the space $L(nD), n \geq 0$, is regular on the affine part $U = X \cap (\mathbb{P}^2 \setminus V(T_0))$. A regular function on U is a n element of the ring $k[Z_1, Z_2]/(f(Z_1, Z_2))$, where $f(Z_1, Z_2) = 0$ is the affine equation of X. We may represent it by a polynomial $P(Z_1, Z_2)$. Now it is easy to compute the dimension of the space of polynomials $P(X_1, X_2)$ modulo (f) which belong to the linear space $L(nD)$. We can write

$$P(Z_1, Z_2) = \sum_{i=1}^{n} G_i(Z_1, Z_2),$$

where $G_i(Z_1, Z_2)$ is a homogeneous polynomial of degree i. The dimension of the space of such P's is equal to $(n+2)(n+1)/2$. The dimension of P's which belong to (f) is equal to the dimension of the space of polynomials of degree $d-n$ which is equal to $(n-d+2)(n-d+1)/2$. Thus we get

$$\dim L(nD) = \frac{1}{2}(n+2)(n+1)/2 - \frac{1}{2}(n-d+2)(n-d+1) = \frac{1}{2}(d-1)(d-2) + 1 + nd.$$

When $n > 2g - 2$, the RRT gives

$$\dim_k L(nD) = nd + 1 - g.$$

comparing the two answers for $\dim L(D)$ we obtain the formula for g.

Theorem 3. *Assume that $g = 1$ and $X(k) \neq \emptyset$. Then X is isomorphic to a plane curve of degree 3.*

Proof. Note thyat by the previous theorem, the genus of a plane cubic is equal to 1. Assume $g = 1$. Then $\deg(K_X) = 2g - 2 = 0$. Since $L(K_X - D) = \{0\}$ for any divisor $D > 0$, the RRT gives

$$\dim L(D) = \deg(D).$$

Take $D = 2 \cdot x$ for some point $x \in X(k)$. Then $\dim L(D) = \deg(D) = 2$, hence there exists a nonconstant function ϕ_1 such that $\nu_x(\phi_1) \geq -2, \phi_1 \in \mathcal{O}(X \setminus \{x\})$. If $\nu_x(\phi_1) = -1$, then the argument from Theorem 1, shows that $X \cong \mathbb{P}^1$ and hence $g = 0$. Thus $\nu_x(\phi_1) = -2$. Now take $D = 3 \cdot x$. We have $\dim L(D) = 3$. Obviously $L(2 \cdot x) \subset L(3x)$. Hence there exists a function

$\phi_2 \notin L(D)$ such that $\nu_x(\phi_2) = -3$, $\phi_2 \in \mathcal{O}(X\setminus\{x\})$. Next we take $D = 6\cdot x$. We have $\dim L(D) = 6$. Obviously, we have the following functions in $L(D)$:

$$1, \phi_1,\ \phi_1^2,\ \phi_1^3,\ \phi_2,\ \phi_2^2,\ \phi_1\phi_2.$$

The number of them is 7, hence they must be linearly dependent in $L(6\cdot x)$. Let

$$a_0 + a_1\phi_1 + a_2\phi_1^2 + a_3\phi_1^3 + a_4\phi_2 + a_5\phi_2^2 + a_6\phi_1\phi_2.$$

with not all coefficients $a_i \in k$ equal to zero. I claim that $a_5 \neq 0$. Indeed, assume that $a_5 = 0$. Since ϕ_1^2 and ϕ_2^3 are the only functions among the seven ones which has pole of order 6 at x, the coefficient a_3 must be also zero. Then $\phi_1\phi_2$ is the only function with pole of order 5 at x. This implies that $a_6 = 0$. Now ϕ_1^2 is the only function with pole of order 4, so we must have $a_2 = 0$. If $a_4 \neq 0$, then ϕ_2 is a linear combination of 1 and ϕ_1, and hence belongs to $L(2\cdot x)$. This contradicts the choice ϕ_2. So, we get $a_0 + a_1\phi_1 = 0$. This implies that $a_0 = a_1 = 0$.

Consider the map $f : X \to \mathbb{P}^1$ given by the function ϕ_1. Since ϕ_2 satisfies an equation of degree 2 with coefficients from the field $f^*(R(\mathbb{P}^1))$, we see that $[R(X) : R(\mathbb{P}^1)] = 2$. Thus, adding ϕ_2 to $f^*(R(\mathbb{P}^1))$ we get $R(X)$. Let

$$\Phi : X \setminus \{x\} \to \mathbb{A}^2$$

be the regular map defined by $\Phi^*(Z_1) = \phi_1, \Phi^*(Z_2) = \phi_2$. Its image is the affine curve defined by the equation

$$a_0 + a_1 Z_1 + a_2 Z_1^2 + a_3 Z_1^3 + a_4 Z_2 + a_5 Z_2^2 + a_6 Z_1 Z_2 = 0.$$

Since $k(X) = k(\Phi^*(Z_1), \Phi^*(Z_2))$ we see that X is birationally isomorphic to the affine curve $V(F)$. Note that $a_3 \neq 0$, since otherwise, after homogenizing, we get a conic which is isomorhic to $\mathbb{P}^1$. So, homogenizing F we get a plane cubic curve with equation

$$F(T_0, T_1, T_2) = a_0T_0^3 + a_1T_0^2T_1 + a_2T_0T_1^2 + a_3T_1^3 + a_4T_0^2T_2 + a_5T_0T_2^2 + a_6T_0T_1T_2 = 0. \quad (3)$$

It must be nonsingular, since a singular cubic is obviously rational (consider the pencil of lines through the singular point to get a rational parametrization). Since a birational isomorphism of nonsingular projective curves extends to an isomorophism we get the assertion.

Remark. Note that we can simplify the equation of the plane cubic as follows. First we may assume that $a_6 = a_3 = 1$. Suppose that $\mathrm{char}(k) \neq 2$. Replacing Z_2 with $Z_2' = Z_2 + \frac{1}{2}(a_6Z_1 + a_4Z_0)$, we may assume that $a_4 = a_5 = 0$. If $\mathrm{char}(k) \neq 2, 3$, then replacing Z_1 with $Z_1 + \frac{1}{3}a_2Z_0$, we may assume that $a_2 = 0$. Thus, the equation is reduced to the form

$$F(T_0, T_1, T_2) = T_0T_2^2 + T_1^3 + a_1T_0^2T_1 + a_0T_0^3,$$

or, after dehomogenizing,

$$Z_2^2 + Z_1^3 + a_1Z_1 + a_0 = 0.$$

It is called the *Weierstrass equation.* Since the curve is nonsingular, the cibic polynomial $Z_1^3 + a_1Z_1 + a_0$ does not have multiple roots. This occurs if and only if its discriminant

$$\Delta = 4a_1^3 + 27a_0^2 \neq 0.$$

Problems

1. Show that a regular map of nonsingular projective curves is always finite.

2. Prove that for any nonsingular projective curve X of genus g there exists a regular map $f : X \to \mathbb{P}^1$ of degree $(= [R(X) : f^*(R(\mathbb{P}^1))])$ equal to $g = 1$.

3. Show that any nonsingular projective curve X of genus 0 with $X(k) = \emptyset$ is isomorphic to a nonsingular conic on $\mathbb{P}^2_k$ [Hint: Use that $\dim L(-K_X) > 0$ to find a point x with $\deg(1 \cdot x) = 2$].

4. Let X be a nonsingular plane cubic with $X(k) \neq \emptyset$. Fix a point $x_0 \in X(k)$. For any $x, y \in X$ let $x \oplus y$ be the unique simple pole of a nonconstant function $\phi \in L(x + y - x_0)$. show that $x \oplus y$ defines a group law on X. Let $x_0 = (0, 0, 1)$, where we assume that X is given by equation (3). Show that x_0 is the inflection point of X and the group law coincides with the group law on X considered in Lecture 6.

5. Prove that two elliptic curves given by Weierstrass equations $Z_2^2 + Z_3^2 + a_1 Z_1 + a_0 = 0$ and $Z_2^2 + Z_3^2 + b_1 Z_1 + b_0 = 0$ are isomorhic if and only if $a_1^3/a_0^2 = b_1^3/b_0^2$.

6. Let X be a nonsingular curve in $\mathbb{P}^1 \times \mathbb{P}^1$ given by a bihomogeneous equation of degree (d_1, d_2). Prove that its genus is equal to

$$g = (d_1 - 1)(d_2 - 1).$$

7. Let $D = \sum_{i=1}^r n_i x_i$ be a positive divisor on a nonsingular projective curve X. For any $x \in X \setminus \{x_1, \ldots, x_r\}$ denote, let $l_x \in L(D)^*$ be defined by evaluating $\phi \in L(D)$ at the point x. Show that this defines a rational map from X to $\mathbb{P}(L(D)^*)$. Let $\phi_D : X \to \mathbb{P}(L(D)^*)$ be its unique extension to a regular map of projective varieties. Assume $X = \mathbb{P}^1$ and $\deg(D) = d$. Show that $\phi_D(\mathbb{P}^1)$ is isomorphic to the Veronese curve $\nu_d(\mathbb{P}^1) \subset \mathbb{P}^d$.

8. Show the map ϕ_D is one-to-one on its image if $\deg(D) \geq 2g - 1$.