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 $k[T_1, \ldots, T_n] = k[T]$ 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 $(x_1, \ldots, x_n) \in K^n$ such that for all $F \in S$

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

Let $Sol(S; K)$ 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

$Sol(S; \mathbf{Q})$ 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 $Sol(S; \mathbf{Q})$.

$Sol(S; \mathbf{R})$ 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.

$Sol(S; \mathbf{C})$ 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 $Sol(S; K)$ 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 $a = (a_1, \ldots, a_n) \in Sol(S; K)$,

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

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

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

be the corresponding map of the solution sets. The following properties are immediate:
(i) $sol(S; \mathrm{id}_K) = \mathrm{id}_{Sol(S;K)}$, 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.

In other words, the correspondences

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

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

Recall that a *category* $\mathcal{C}$ consists of a set $Ob(\mathcal{C})$ of *objects*, and sets $Mor_{\mathcal{C}}(A, B)$ of *morphisms* $A \to B$ from an object A to an object B. Moreover, for each ordered triple of objects A, B, and C there is a map

$$Mor_{\mathcal{C}}(A, B) \times Mor_{\mathcal{C}}(B, C) \to Mor_{\mathcal{C}}(A, C),$$

whose value at a pair $\phi : A \to B$ and $\psi : B \to C$ is denoted by $\psi \circ \phi$ and is called the *composition* of ϕ and ψ. It is also required that for any object A of $\mathcal{C}$ the set $Mor_{\mathcal{C}}(A, A)$ contains a unique element id_X, called the *identity morphism*, satisfying

$$\mathrm{id}_A \circ \psi = \phi, \quad \phi \circ \mathrm{id}_A = \psi$$

for any morphism $\psi : B \to A$ or $\phi : A \to B$. If we let

$$Mor(\mathcal{C}) = \bigcup_{A,B \in Ob(\mathcal{C})} Mor_{\mathcal{C}}(A, B),$$

then the set $Ob(\mathcal{C})$ identifies naturally with a subset of $Mor(\mathcal{C})$ by assigning A to id_A. The morphsims f of the form id_A are characterized by the property that whenever the compositions $\phi \circ f$ and $f \circ \psi$ are defined they must be equal to ϕ or ψ, respectively.

This "naive" definition abuses logic since the set $Mor(\mathcal{C})$ may be too big to exist. The correct definition requires that $Mor(\mathcal{C})$ is a subset of a certain set (the universum). However, we are not going to be bothered with such problems and refer to the standard text-books on category theory for further details. A simplest example of a category is the category of sets $\mathcal{S}ets$ whose objects are sets (belonging to a certain universum to be precise) and whose morphisms are maps of set. Another example is the category *Rings* whose objects are rings and morphisms are homomorphisms of rings. This as well as some many other similar examples like the category of topological spaces *Top* or the category Vec_k of vector spaces over a field k are examples of a subcategory of $\mathcal{S}ets$.

A *subcategory* $\mathcal{C}'$ of a category $\mathcal{C}$ is defined naturally by requiring that $Mor(\mathcal{C})$ is a subset of $Mor(\mathcal{C}')$ and the law of composition in $\mathcal{C}$ restricts to the law of composition in $\mathcal{C}'$. It is called a *full subcategory* if $Mor_{\mathcal{C}'}(A, B) = Mor_{\mathcal{C}}(A, B)$ for any $A, B \in Ob(\mathcal{C}') \subset Ob(\mathcal{C})$. Thus we can speak about the category of k-algebras $\mathcal{A}lg_k$ as a subcategory of $\mathcal{R}ings$, whose morphisms are homomorphisms of rings identical on k, or its full subcategory of field extensions $\mathcal{F}ields_k$. For simplicity of the notation we put

$$Hom_k(A, B) = Mor_{\mathcal{A}lg/k}(A, B).$$

Next we recall that a *covariant functor* $F : \mathcal{C} \to \mathcal{C}'$ from a category $\mathcal{C}$ to a category $\mathcal{C}'$ is a map $F : Mor(\mathcal{C}) \to Mor(\mathcal{C}')$ which is compatible with compositions and sends $Ob(\mathcal{C})$ into $Ob(\mathcal{C}')$. The latter condition implies that

$$F(Mor_{\mathcal{C}}(A, B)) \subset Mor_{\mathcal{C}'}(F(A), F(B)).$$

A *contravariant functor* is defined similarly but we require that $F(\phi \circ \psi) = F(\psi) \circ F(\phi)$ instead of $F(\phi \circ \psi) = F(\phi) \circ F(\psi)$.

One can reduce the notion of a contravariant functor to the notion of a covariant functor by using the concept of the *dual category* $\mathcal{C}^\circ$ of a category $\mathcal{C}$. It is defined by setting $Ob_{\mathcal{C}^\circ} = Ob(\mathcal{C})$ and $Mor_{\mathcal{C}^\circ}(A, B) = Mor_{\mathcal{C}}(B, A)$ with the obvious definition of compositions. It is clear that any contravariant functor $F : \mathcal{C} \to \mathcal{C}'$ can be considered as a covariant functor from $\mathcal{C}^\circ$ to $\mathcal{C}'$. In the future a functor will always mean a covariant functor. Usually we will define a functor on the set of objects and leave to the reader to define its natural extension to the set of all morphisms.

Definition. An *affine algebraic variety* over a field k is a functor $X : \mathcal{A}lg_k \to \mathcal{S}ets$ such that

$$X(K) = Sol(S; K), \quad X(\phi) = sol(S; \phi)$$

for some system of algebraic equations S over the field k.

Examples. 1. The functor $K \to K^n$ is an affine algebraic variety. It corresponds to the system $0 = 0$. Here 0 in the left hand side is the zero of the polynomial ring $k[T_1, \ldots, T_n]$. The zero from the right-hand side is the zero element of the k-algebra K. This affine algebraic variety is called the *n-dimensional affine space* over k and is denoted by $\mathbf{A}^n_k$.
2. The functor $K \to \emptyset \subset K^n$ is an affine algebraic variety. It corresponds to the system $1 = 0$. It is called the empty affine algebraic variety over k and is denoted by $\emptyset_k$.

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

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

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

$$Sol(S; K) \longleftrightarrow Hom_k(k[T]/(S), K).$$

Two different systems of algebraic equations $S, S' \subset k[T]$ may define the same affine algebraic variety. The next result gives a simple criterion when does it happen.

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 $Sol(S'; K) \subset Sol(S; K)$. The opposite inclusion is proven similarly. To prove the part "only if" we use the bjection $Sol(S; K) \longleftrightarrow Hom_k(k[T]/(S), K)$. 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 $a \in Sol(S;K)$. Since $Sol(S;K) = Sol(S';K)$, for any $F \in (S')$ we have $F(a) = F(T_1, \ldots, T_n) \bmod(S) = 0$ 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 $Sol(S;K)$ consists of one element, the zero element 0 of K. The same is true for $Sol(S';K)$ 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 the affine algebraic variety defined by a system of algebraic equations S over k. The ideal (S) depends only on X and is called the *defining ideal* of X. It is denoted by $I(X)$.

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 $F(T) = b_0T_n^r + \ldots + b_r$, 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

$$F(T) = (c_1a_1 + \ldots c_ta_t)T_n^r + \ldots = \sum_{1 \leq i \leq k} c_i T_n^{r-d(i)} F_i(T) + F'(T),$$

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

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

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 $F_1, \ldots, F_t$. This proves the assertion.

For any ideal I in $k[T]$ let us define the functor $\underline{I} : \mathcal{A}lg_k \to \mathcal{S}ets$ by

$$\underline{I}(K) = \{x \in K^n : F(x) = 0, \ \forall F \in I\}.$$

Obviously, it is an affine algebraic variety defined by any set of generators of I. Conversely every X is equal to $\underline{I(X)}$. The Hilbert Theorem together with Proposition 1 show that any affine algebraic variety X can be defined by a finite system of algebraic equations. It follows from Proposition 1 that the correspondence $I \mapsto \underline{I}$ defines a one-to-one correspondence

$$\{\text{polynomial ideals }\} \longleftrightarrow \{\text{affine algebraic varieties }\}$$

Finally, we define a subvariety of an affine algebraic variety. Again, we use the language of functors.

Let $\mathcal{C}$ be a category and $F, G : \mathcal{C} \to \mathcal{S}ets$ be two functors from $\mathcal{C}$ to the category of sets. Then G is said to be a *subfunctor* of F (denoted by $G \subset F$) if the following two properties are satisfied:
(i) $G(A) \subset F(A)$ for any $A \in Ob(\mathcal{C})$;
(ii) for any $\phi : A \to B \in Mor_{\mathcal{C}}(A, B)$, the map $G(\phi) : G(A) \to G(B)$ is equal to the restriction of the map $F(\phi) : F(A) \to F(B)$ to the subset $G(A)$.

Definition. An affine algebraic variety Y over k is said to be a *subvariety* of an affine algebraic variety X over k if Y is a subfunctor of 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. Give two examples of subfunctors of $\mathbf{A}_k^n$ which are not affine algebraic varieties.
2. For which fields k do the systems

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

define the same affine algebraic varieties? Here $\sigma_i(T_1, \ldots, T_n)$ denotes the elementary symmetric polynomial of degree i in $T_1, \ldots, T_n$.
3. Prove that the systems of algebraic equations over the field $\mathbf{Q}$

$$\{T_1^2 + T_2 = 0, T_1 = 0\} \text{ and } \{T_2^2T_1^2 + T_1^2 + T_2^3 + T_2 + T_1T_2 = 0, T_2T_1^2 + T_2^2 + T_1 = 0\}$$

define the same affine algebraic varieties.
4. Let $X \subset \mathbf{A}_k^n$ and $X' \subset \mathbf{A}_k^m$ be two affine algebraic varieties. Prove that the functor $K \to X(K) \times X'(K) \subset K^n \times K^m = K^{n+m}$ is an affine algebraic variety.
5. Prove that if X and X' are two subvarieties of $\mathbf{A}_k^n$, then the functor $K \to X(K) \cap X'(K)$ is a subvariety of $\mathbf{A}_k^n$. It is called the intersection of X and X' and is denoted by $X \cap X'$. Is the functor $K \to X(K) \cup X'(K)$ a subvariety of $\mathbf{A}_k^n$?
6. Suppose that S and S' are two systems of linear equations over a field k. Show that $(S) = (S')$ if and only if $Sol(S; k) = Sol(S'; k)$.

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*

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

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

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

and $(1-T_{n+1}G)(a_1,\dots,a_n,a_{n+1}) = 1 - a_{n+1}G(a_1,\dots,a_n,a_{n+1}) = 1 \neq 0$. 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 $T_1,\dots,T_{n+1}$. 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 m be a maximal ideal containing our ideal I. We have a homomorphsim of rings $\phi : k[T]/I \to A = k[T]/m$ induced by the factor map $k[T] \to k[T]/m$. Since 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 : $x^n + a_1x^{n-1} + \ldots + a_n = 0$ 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 $t_1,\dots,t_r$ 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 $t_1,\dots,t_r$ 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 $t_2,\dots,t_r$. 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 $a_it_i^{d(i)} + \ldots = 0, a_i \neq 0$, 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_it_i are integral over $k[t_1]$. At this point we can replace the generators t_i by a_it_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 $X^n + A_1X^n + \ldots + A_n = 0$ 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

$$P^n + A_1QP^{n-1} + \ldots + A_nQ^n = 0.$$

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

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

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 $\cap_j V_j$ of any family of affine algebraic k-sets and the union $\cup_j V_j$ of any finite family of affine algebraic k-sets is a affine algebraic k-set in K^n.

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

Proof. (i) Let $I_j = I(V_j)$ be the ideal of polynomials vanishing on V_j. Let $I = \sum_j I_j$ be the sum of the ideals I_j, i.e., the minimal ideal of $k[T]$ containing the sets I_j. Its set of zeroes in K is equal to $\cap_j V_j$. Similarly, the union $\cup_j V_j$ is the set of zeroes of the ideal J equal to the product $\prod_j I_j$ of the ideals I_j.

(ii) 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 $\mathbf{A}_k^n(K)$. If $k = K$, we drop the subscript k and call it the n-dimensional affine space.

Example. A proper subset in $\mathbf{A}^n(K)$ 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).

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 $I(V) \cap I(V') \neq I(V)I(V')$. Recall that the product IJ of two ideals I and J is the ideal generated by products $FG, F \in I, G \in J$.
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 $\mathbf{A}_k^n(K)$ when $k \neq K$?
5. Find the ideal $I(V)$ of the algebraic subset of K^n defined by the equations $\{T_1^3 = 0, T_2^3 = 0, T_1T_2(T_1 + T_2) = 0$. Is $T_1 + T_2 \in I(V)$?
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 $\phi : K \to L$ the following diagram is commutative:

$$\begin{array}{rcl} X(K) & \xrightarrow{X(\phi)} & X(K') \\ f(K)\downarrow & & \downarrow f(L) \\ Y(K) & \xrightarrow{Y(\phi)} & Y(L). \end{array}$$

It is easily checked that this definition allows us to introduce the category of affine algebraic varieties over a field k. We denote this category by $\mathbf{Aff}/k$.

The previous definition is a special case of the notion of a morphism between functors.

A *morphism* (or a *natural transformation*) $f : F \to F'$ between two functors $F : \mathcal{C} \to \mathcal{C}'$ and $F' : \mathcal{C} \to \mathcal{C}'$ is a collection of morphisms $f(A) : F(A) \to F'(A), A \in Ob(\mathcal{C})$, in $\mathcal{C}'$ such that for every $(\phi : A \to B) \in Mor_{\mathcal{C}}(A, B)$ the following diagram is commutative:

$$\begin{array}{rcl} F(A) & \xrightarrow{F(\phi)} & F(B) \\ f(A)\downarrow & & \downarrow f(B) \\ F'(A) & \xrightarrow{F'(\phi)} & F'(B). \end{array}$$

One defines naturally the composition of functor morphisms and even the category of functors $FCT(\mathcal{C}, \mathcal{C}')$. Two functors F and F' are called isomorphic (or equivalent) if there exist two morphisms $f : F \to F'$ and $f' : F' \to F$ such that for every $A \in Ob(\mathcal{C})$ the maps $f(A)$ and $f'(A)$ are inverse to each other.

Using the language of categories, we can restate our definition as follows. A morphism from an affine variety X to an affine variety Y is a morphism of the corresponding functors $\mathcal{A}lg_k \to \mathcal{S}ets$. Two varieties are isomorphic if the corresponding functors are isomorphic. The category $\mathbf{Aff}/k$ is a subcategory of the category $FCT(\mathcal{A}lg_k, \mathcal{S}ets)$ of functors $\mathcal{A}lg_k \to \mathcal{S}ets$.

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

$$X(K) \to Hom_k(k[T]/(X), K).$$

It is immediately checked that for any homomorphism of k-algebras $f : K \to K'$ we have a commutative diagram

$$\begin{array}{ccc} X(K) & \to & Hom_k(k[T]/(X), K) \\ X(f)\downarrow & & f\circ\downarrow \\ X(K') & \to & Hom_k(k[T]/(X), K') \end{array}$$

where the right vertical arrow is defined by composing a homomorphism $k[T]/(X) \to K$ with f. Thus we see that the functor X is isomorphic to the functor

$$Hom_k(k[T]/(X), ?) : \mathcal{A}lg_k \to \mathcal{S}ets$$

which assigns to a k-algebra K the set of homomorphisms $Hom_k(k[T]/(X), K)$.

From now on we will denote the factor algebra $k[T]/(X)$ 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 $ev_{X,a} : \mathcal{O}(X) \to K$. Then

$$\varphi(a) = ev_{X,a}(\varphi).$$

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

Let $\phi : A \to B$ be a homomorphism of k-algebras. For every k-algebra K we have a natural map of sets $Hom_k(B, K) \to Hom_k(A, K)$, which is obtained by composing a map $B \to K$ with ϕ. It is easily checked that this defines a morphism of functors

$$Hom_k(B, ?) \to Hom_k(A, ?).$$

Thus we have a natural map

$$Hom_k(\mathcal{O}(Y), \mathcal{O}(X)) \to Mor_{\mathbf{Aff}/k}(X, Y).$$

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 $ev_{X,a} : \mathcal{O}(X) = k[T_1, \ldots, T_n]/(X) \to K$ by assigning a_i to $T_i, i = 1, \ldots, n$. Composing this homomorphism with a given homomorphism $\phi : \mathcal{O}(Y) = k[T_1, \ldots, T_m]/(Y) \to \mathcal{O}(X)$, we get a homomorphism $ev_{X,a} \circ \phi : \mathcal{O}(Y) \to K$. Let $b = (b_1, \ldots, b_m)$ where $b_i = ev_{X,a} \circ \phi(T_i), i = 1, \ldots, m$. This defines a K-point of Y. Varying K, we obtain a morphism $X \to Y$ which corresponds to the homomorphism ϕ.

Let us prove that the correspondence is bijective. This is a special case of the following general fact.

Let $\mathcal{C}$ be a category. For every $X \in Ob(\mathcal{C})$ denote by h_X the functor $\mathcal{C} \to \mathcal{S}ets$ defined by $h_X(Z) = Mor_{\mathcal{C}}(Z, X), h_X(\alpha : Y \to Z) : h_X(Z) \to h_X(Y)$ is the map $\phi \mapsto \alpha \circ \phi$. Now if $\phi : X \to Y$ is a morphism in $\mathcal{C}$, we can define a natural transformation $h(\phi) : h_X \to h_Y$ by setting for any $Z \in Ob(\mathcal{C})$

$$h_X(Z) \to h_Y(Z), \quad (\alpha : Z \to X) \mapsto (\phi \circ \alpha : Z \to Y).$$

In this way we obtain a functor:

$$h : \mathcal{C} \to \check{\mathcal{C}} := FCT(\mathcal{C}^\circ, \mathcal{S}ets).$$

Lemma (Yoneda). *For any two objects X, Y in $\mathcal{C}$ the map*

$$h : Mor_{\mathcal{C}}(X, Y) \to Mor_{\check{\mathcal{C}}}(h_X, h_Y), \phi \mapsto h(\phi)$$

is bijective.

Proof. We need to invert the map h. Take $f : h_X \to h_Y$. For any $Z \in Ob(\mathcal{C})$, h defines a map $f(Z) : h_X(Z) \to h_Y(Z)$. Put $Z = X$, then $f(X)(id_X)$ is a map $\phi : X \to Y$ from the set $h_Y(X)$. We define a map $u : Mor_{\check{\mathcal{C}}}(h_X, h_Y) \to Mor_{\mathcal{C}}(X, Y)$ by sending f to $\phi = f(X)(id_X)$. Let us check that $u = h^{-1}$. Obviously for any $\phi : X \to Y$,

$$u \circ h(\phi) = u(h(\phi)) = h(\phi)(X)(\mathrm{id}_X) = \mathrm{id}_X \circ \phi = \phi.$$

So u is the left inverse of s. Let us show that it is the right inverse. For any $f : h_X \to h_Y$ and $(\alpha : Z \to X) \in h_X(Z)$ we have the following commutative diagram arising from the definition of morphisms of functors:

$$\begin{array}{ccc} h_X(X) & \stackrel{f(X)}{\longrightarrow} & h_Y(X) \\ h_X(\alpha) \downarrow & & \downarrow h_Y(\alpha) \\ h_X(Z) & \stackrel{f(Z)}{\longrightarrow} & h_Y(Z). \end{array}$$

The upper horizontal arrow sends id_X to $u(f) : X \to Y$. The right vertical arrow sends the latter to $u(f) \circ \alpha$. Now the left vertical arrow sends id_X to $\mathrm{id}_X \circ \alpha = \alpha$. Hence $f(Z)(\alpha) = u(f) \circ \alpha$ and, by definition of s, we get $f = s(u(f))$. So u is the right inverse of s.

Recall that two objects A, B of a category are called *isomorphic* if there exists a morphism $f : A \to B$ and a morphism $g : B \to A$ with $g \circ f = \mathrm{id}_A, f \circ g = \mathrm{id}_B$.

Corollary. *Let $A, B \in Ob(\mathcal{C})$. Then*

$$A \cong B \text{ in } \mathcal{C} \Longleftrightarrow h_X \cong h_Y \text{ in } \check{\mathcal{C}}.$$

To apply this lemma, we take $\mathcal{C}$ equal to the dual category of the category of k-algebras. For any k-algebra K, we have $h_{\mathcal{O}(X)}(K) = Hom_k(\mathcal{O}(X), K)$. Thus the Yoneda Lemma implies that there is a one-to-one correspondence between the set of morphisms from an affine algebraic variety X to another such variety Y and homomorphisms of their coordinate algebras $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$. Its corollary tells us that X and Y are isomorphic if and only if their coordinate algebras 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 $k[T], \phi$ 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 $k[T] \to \mathcal{O}(X), T_i \to P_i(T) + (X)$ factors through the ideal (Y), we have

$$(*) F(P_1(T), \ldots, P_m(T)) \in (X),\ \forall F(T'_1, \ldots, T'_n) \in (Y).$$

Note that it suffices to check the previous condition only for generators of the ideal (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 (*), 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 (*) is an isomorphism if and only if there exist polynomials $(Q_1(T'),\dots,Q_n(T'))$ such that

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

$$P_i(Q_1(T'),\dots,Q_n(T')) \equiv T'_i \text{ mod } (Y), i = 1,\dots,m,$$

$$Q_j(P_1(T),\dots,P_m(T)) \equiv T_j \text{ mod}(X), j = 1,\dots,n.$$

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 $X = \mathbf{A}_k^1$ 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 T_1/T_2 which does not belong to the ring but whose square is an element of the ring (= coset of T'_2). 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 $\text{char}(k) \neq 2$.

Consider the special case of morphisms $f : X \to Y$, where $Y = \mathbf{A}_k^1$ (*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 $\mathbf{A}_k^1$ 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. *For any* $\varphi \in \mathcal{O}(Y) = Mor_{\mathbf{Aff}/k}(Y, \mathbf{A}_k^1)$,

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

Proof. This follows immediately from the above definitions.

After we (hopefully) get used to the functorial point of view it will be natural to generalize the notion of an affine algebraic variety.

Definition. A functor $F : \mathcal{A}lg_k \to \mathcal{S}ets$ is said to be an *affine algebraic functor* over a field k if it is isomorphic to an affine algebraic variety over k.

We can define the coordinate algebra of an affine algebraic functor F by setting

$$\mathcal{O}(F) = \mathcal{O}(X),$$

where X is an affine algebraic variety isomorphic to F. It is clear that there is a bijection

$$\mathcal{O}(F) \longleftrightarrow Mor(F, \mathbf{A}_k^1)$$

where the morphisms are taken from the category $FCT(\mathcal{A}lg_k, \mathcal{S}ets)$.

Examples. 3. Let A be a finitely generated k-algebra. Choose a surjective homomorphism $k[T] \to A$ and let I be its kernel. Let I be the affine algebraic variety corresponding to the ideal I (i.e. defined by any set of generators of I). We have already seen that there is an isomorphism of functors: $I \cong h_A$. Thus, the functor h_A is an affine algebraic functor.
4. The functor $\mathbf{G}_{\mathbf{m},k} : K \to K^*$ (= invertible elements in K) is an affine algebraic functor. It is isomorphic to the functor $K \to \{(a,b) \in K^2 : ab = 1\}$ which is given by a system of algebraic equations $T_1T_2 - 1 = 0$. The natural inclusions $K^* \subset K$ allow us to identify $\mathbf{G}_{\mathbf{m},k}$ with a subvariety of $\mathbf{A}_k^1$. This functor is called the *multiplicative group* over k.

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 X to be equal $\underline{I}$ 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 $P_i(T_1, \dots, T_n), i = 1, \dots, m$, be the representatives in $k[T]$ of the images of T_i' mod $I(W)$ inder f^*. For any $a = (a_1, \dots, a_n) \in V$ 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 $P_i(a), i = 1, \dots, m$. Thus the map $f(K)$ is given by the formula

$$f(K)(a) = (P_1(a_1, \dots, a_n), \dots, P_m(a_1, \dots, a_n)).$$

Note that this map does not depend on the choice of the representatives P_i of $f^*(T_i'$ mod $I(W))$ 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 $F(T_1, \dots, T_n) \in k[T_1, \dots, T_n]$ with the property

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

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 $pr_i : K^m \to K, (a_1, \dots, a_n) \mapsto a_i$, is a regular function. An invertible regular map is called a *biregular map* of algebraic sets.

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 obviously false.

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 $\underline{I}(V)$. Every 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 $\mathbf{A}_k^2$ defined by the equation $T_2^2 - T_1^2 - T_1^3 = 0$ and let $f : \mathbf{A}_k^1 \to X$ 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 $\mathcal{O}(\mathbf{A}_k^1) = k[T]$ 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 $\mathrm{char}(k) = 2$. In the latter case show that 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 $\mathbf{A}_k^1$.
3. Let $f : \mathbf{A}_k^2(K) \to \mathbf{A}_k^2(K)$ 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 $\mathbf{A}_k^1$ to $\mathbf{A}_k^1$.
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 functor $K \to GL(n, K)$ (= invertible $n \times n$-matrices with entries in K) is an affine algebraic functor over k. It is denoted by $\mathbf{GL}_k(n)$ and is called the *general linear group* of order n over k.

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 $k(V)$ and $k(V')$ are defined. We obtain a weaker equivalence of varieties if we require that the fields $k(V)$ and $k(V')$ 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^n 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 $F \in k[T]$ 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 $k[T]$ 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 $k(V)$ 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, $Q(A)$ has a unique structure of a k-algebra and plays the univerdal role as above in the category of k-algebras. In particular, the field $k(V)$ will be viewed as an extension $k \subset \mathcal{O}(V) \subset k(V)$. 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 $f : k(W) \to k(V)$. 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 $k[T_1', \ldots, T_m'] \to k(V)$. It is given by rational functions $R_1, \ldots, R_m \in k(V)$, 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 $k[T_1, \ldots, T_n]$ defined up to addition of elements from $I(V)$. If $a \in V$ does not belong to the set $Z = V(Q_1) \cup \ldots \cup V(Q_n)$, then

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

is uniquely defined. Since $G(R_1(a), \ldots, R_m(a)) = 0$ 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

$$\alpha : V - \to W.$$

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 $F(R_1(a), \ldots, R_m(a)) = 0$ for any $a \in V \setminus Z$. Write

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

We have $P(T_1, \ldots, T_n) \equiv 0$ 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 $k(W) \to k(V)$, F goes to 0. Since the homomorphism $k(W) \to k(V)$ is injective (any homomorphism of fields is injective) this is absurd.

In particular, taking $W = \mathbf{A}_k^1(K)$, we obtain the interpretation of elements of the field $k(V)$ as non-constant rational functions $V - \to K$ 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 $k(W) \to k(V)$ defining a rational map $f : V - \to W$ can be interpreted as the homomorphism f^* defined by the composition $\phi \mapsto \phi \circ f$.

Definition. A rational map $f : V - \to W$ is called *birational* if the corresponding field homomorphism $f^* : k(W) \to k(V)$ 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 $f : V - \to W$ is a birational map, then there exists a birational map $f : W - \to V$ 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 $f \circ f' = \mathrm{id}_U'$, $f' \circ f = \mathrm{id}_U$. 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 $V = \mathbf{A}_k^1(K)$ and $W = V(T_1^2 + T_2^2 - 1) \subset K^2$. We assume that $\mathrm{char}(k) \neq 2$. A rational map $f : V - \to W$ is given by a homomorphism $f^* : k(W) \to k(V)$. 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

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

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

Proof. Since $k(V)$ 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 $\mathrm{char}(k) = 0, k(V)$ 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 $k[T_1, \ldots, T_{n+1}] \to k(V)$ 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 $\phi : A = k[T_1, \ldots, T_{n+1}]/I \to k(V)$ 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 $Q(A) \to k(V)$. Since $k(V)$ is generated as a field by elements in the image, ϕ must be an isomorphism. Thus $k(V)$ is isomorphic to $Q(k[T_1, \ldots, T_{n+1}]/(F))$ and we are done.

Remark 3. 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 $k(V)$ 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 $k(V) \cong k(T_1, \ldots, T_n)$ 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 $k(V)$ 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 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.
6. Give an example of an irreducible algebraic k-set which is not geometrically irreducible.

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 $\mathbf{P}^n(A)'$. One can define $\mathbf{P}^n(A)'$ 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

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

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,

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

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 $A = \mathbf{R}$. Then $\mathbf{P}^1(\mathbf{R})'$ is the set of lines in $\mathbf{R}^2$ passing through the origin. By taking the intersection of the line with the unit circle we establish a bijective correspondence from $\mathbf{P}^1(\mathbf{R})$ to the points of 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 $\mathbf{P}^1(\mathbf{R})'$ to the half circle with the two ends identified. This is bijective to a circle. Similarly we can identify $\mathbf{P}^2(\mathbf{R})'$ 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 $\mathbf{RP}^2$.

2. Take $A = \mathbf{C}$. Then $\mathbf{P}^1(\mathbf{C})'$ is the set of one-dimensional linear subspaces of $\mathbf{C}^2$. We can choose a unique basis of $x \in \mathbf{P}^1(\mathbf{C})'$ of the form $(1, z)$ unless $x = (0, z), z \in \mathbf{C} \setminus \{0\}$, and $\mathbf{C}x = \mathbf{C}(0, 1)$. In this way we obtain a bijective map from $\mathbf{P}^1(\mathbf{C})'$ to $\mathbf{C} \cup \{0\}$, 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 $\mathbf{CP}^1$.

The correspondence

$$'\mathbf{P}^n : A \to \mathbf{P}^n(A)'$$

is a functor from the category of commutative rings with values in the category of sets. Indeed, 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 $1 = a_0b_0 + \ldots + a_nb_n$ 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 which is the required map $'\mathbf{P}^n(\phi)$.

By assigning to each $x = (a_1, \ldots, a_n) \in K^n$ the line $K(1, a_1, \ldots, a_n)$ in K^{n+1} we obtain an isomorphism of the functor $\mathbf{A}^n : \mathcal{R}ings \to Sets, K \to K^n$, to a subfunctor of the functor $'\mathbf{P}^n$. This shows that $'\mathbf{P}^n(A)$ is an enlargement of the set A^n, and this enlargement is functorial in A.

For our future needs we would like to enlarge the set $\mathbf{P}^n(A)'$ a little further to define the set $\mathbf{P}^n(A)$. 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 $\sum_i b_ia_i = 1$. Then the homomorphism $\phi : A^{n+1} \to M$ defined by $(\alpha_0, \ldots, \alpha_n) \mapsto (\sum_i \alpha_ib_i)x$ 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 $\mathbf{P}^n(A)'$ by adding to it not necessarily free direct summands of A^{n+1} which become free of rank 1 after "localizing" the ring.

Let 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 quotients: 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 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 $A \to A_S, a \mapsto a/1$, is a homomorphism of rings. The rule

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

equips M_S with a structure of an A_S-module. Note that $M_S = \{0\}$ if $0 \in S$. The correspondence $M \to M_S$ is a functor from the category of A-modules to the category of A_S-modules. Another way to see it is to observe that there is a natural isomorphism of A_S-modules

$$M \otimes_A A_S \to M_S, m \otimes (a/s) \mapsto am/s,$$

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

Now if we take $S = A \setminus \mathcal{M}$, where $\mathcal{M}$ is a maximal ideal, the localization A_S, denoted by $A_{\mathcal{M}}$, has the property that the ideal

$$\mathcal{M}A_{\mathcal{M}} = \{a/s : a \in \mathcal{M}, s \notin \mathcal{M}\}$$

is the unique maximal ideal of $A_{\mathcal{M}}$. Rings with only one maximal ideal are called *local.* This is equivalent to saying that each element outside this ideal is invertible. In our case this is clear because a/s is invertible if $a \notin \mathcal{M}$.

Definition. A *projective module of rank* r over A is a finitely generated module M over A such that for every maximal ideal $\mathcal{M}$ of A the localization $M_{\mathcal{M}}$ is a free module of rank r over $A_{\mathcal{M}}$. The *projective n-space* of A is the set $\mathbf{P}^n(A)$ of projective submodules of A^{n+1} of rank 1 which are direct summands of A^{n+1}.

To help you to understand the definition of a projective module, we state without prove (see, for example, N. Bourbaki, "Commutative Algebra", Chapter 2, §5) the following:

Theorem. *Let M be a finitely generated module over a ring A. Then the following is equivalent:*
(i) $M_{\mathcal{M}}$ is free over $A_{\mathcal{M}}$ for each maximal ideal $\mathcal{M}$ in A;
(ii) M is isomorphic to a direct summand of a free A-module;
(iii) for any surjective homomorphism of A-modules $\phi : N \to M$ there is a homomorphism $s : M \to N$ such that $\phi \circ s = id_M$.

Example. 3. If $K/\mathbf{Q}$ is a finite extension, and A is the subring of K of integral elements over $\mathbf{Z}$ (the ring of integers of K), then any ideal in A is a projective module of rank 1 but not necessarily a principal ideal.

It is clear that a line in A^{n+1} is a projective submodule of rank 1 and as we have shown it is also a direct summand of A^{n+1}. This shows that

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

We have the equality for example if A is any local ring, e.g., a field.

The correspondence $\mathbf{P}^n : A \to \mathbf{P}^n(A)$ is a functor from $\mathcal{R}ings$ to $\mathcal{S}ets$. For any homomorphism $\phi : A \to B$, the map $\mathbf{P}^n(A) \to \mathbf{P}^n(B)$ is defined by the extension of scalars $M \to M \otimes_A B$. Here we identify the module $A^{n+1} \otimes_A B$ with B^{n+1} by means of the canonical homomorphism $e_i \otimes 1 \to e_i$, where e_i denotes the i-th unit vector. If $M = Ax$ is the line generated by x, then

$$M \otimes_A B = Ax \otimes_A B = (x \otimes 1)A \otimes_A B \cong (1 \otimes \phi(x))A \otimes_A B \cong \phi(x)B$$

is the line generated by $\phi(x)$. Thus $'\mathbf{P}^n$ is a subfunctor of $\mathbf{P}^n$.

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

Using the previous Lemma 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 $\{f_ig_j\}_{(i,j)\in I\times J}$. It is a covering family as one sees by multiplying the two relations $1=\sum_i a_if_i, 1=\sum_j b_jg_j$. 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 $\{f_ig_j\}_{(i,j)\in I\times J}$ is a trivializing family. Moreover, if $M_{f_i}=x_iA_{f_i}, x_i\in A_{f_i}^{n+1}$ and $M_{g_j}=y_jA_{g_j}, y_j\in A_{g_j}^{n+1}$, then

$$(*)\ x_i'=\alpha_{ij}y_j' \quad \text{for some } \alpha_{ij}\in A_{f_ig_j}$$

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

We restrict the functor $\mathbf{P}^n$ to the category $\mathcal{A}lg_k$ of commutative algebras over a field k, denote it by $\mathbf{P}_k^n$ and call it the *n-dimensional projective space* over k.

First of all, we see that $\mathbf{P}_k^n$ is a natural extension of the functor $\mathbf{A}_k^n$. In fact for every k-algebra K we have the injective maps

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

Thus $\mathbf{A}_k^n$ is isomorphic to a subfunctor of $\mathbf{P}_k^n$ (in n+1 different ways).

Remark. It is easy to see that A-module M is a direct summand of A^{n+1} if and only if the transpose map $Hom_A(A^{n+1},A)\to Hom_A(M,A)$ is surjective. Since $Hom_A(M,A)$ is projective if and only if M is projective (check it by reducing the verification to modules over a local ring), we obtain a bijective correspondence between the set $\mathbf{P}^n(A)$ and the set of pairs (M,ϕ), where M is a projective module of rank 1, and $\phi: A^{n+1}\to M$ is a surjective homomorphism. This correspondence is functorial in A (make this into a precise statement). Sometimes the latter set is chosen to be the definition of $\mathbf{P}^n(A)$.

We want to extend the notion of an affine algebraic variety by considering the functor $\mathbf{P}_k^n$ as an algebraic variety (not affine anymore). Next we define a projective algebraic variety as a certain subfunctor of $\mathbf{P}_k^n$ whose values at K can be given by a set of solutions of a system of algebraic equations. Since $\mathbf{P}_k^n(K)'$ consists of lines in K^{n+1} we have to look for systems whose solutions are the union of lines. These systems are rather special, they must be given by homogeneous equations.

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:

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

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 $(*)$ above and the following

Lemma 2. *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 $a/1 = 0 in A_{f_i} \Longleftrightarrow f_i^n a_i = 0$ for some $n \geq 0$. Obviosly 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

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

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

Definition. A *projective algebraic variety* over a field k is a subfunctor X of $\mathbf{P}_k^n$ of the form $K \to PSol(S; K)$ where S is a homogeneous system of algebraic equations over k. We say that X is a *subvariety* of Y if X is a subfunctor of Y.

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 $T_2^2 T_0 + T_1^3 + T_1 T_0^2 + T_0^3$ 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 $\alpha_0 : \mathbf{A}_k^n \to \mathbf{P}_k^n$ 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. 4. Let X be given by $aT_0+bT_1+cT_2=0$, a projective subvariety of the projective plane $\mathbf{P}_k^2$. 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 1. *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) $PSol(S;K)' = \emptyset$;
(ii) $(S) \supset k[T]_{\geq r} := \sum_{d\geq r} k[T]_d$ for some $r \geq 0$;
(iii) $PSol(S;K) = \emptyset$.

Proof. (i) $\Longrightarrow$ (ii) 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 $(1,a_1,\ldots,a_n) \in PSol(S;K)'$). 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) $\Longleftarrow$ (iii) If $(S) \supset k[T]_{\geq r}$ for some $r > 0$, then all T_i^r belong to (S). Thus for every $M = K(a_0, \ldots, a_n) \in PSol(S; K)'$ 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 $PSol(S; K)' = \emptyset$ for any k-algebra K. From this we can deduce that $PSol(S; K) = \emptyset$ for all K. In fact every $M \in PSol(S; K)$ defines $M_f \in PSol(S; K_f)'$ for some $f \in K_f$.

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

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

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

A homogeneous ideal $I \subset k[T]$ containing some power of $\mathcal{M}_+$ 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 functor $K \to PSol(I, K)$. We define the *saturation* of I by

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

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

Proposition 2. *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 $\mathbf{P}_k^n(K)$. It suffices to show that they have the same set of zeroes in every $\mathbf{P}_k^n(K)'$. Clearly every zero of $(S)^{sat}$ is a zero of $I(X)$. Assume that $a = (a_0, \ldots, a_n) \in \mathbf{P}_k^n(K)'$ 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 $1 = a_0 b_0 + \ldots + b_n a_n$ 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 $(t_0, \ldots, t_n) \in Sol(S', k[T]/(S'))$, 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 $(1, z_1, \ldots, z_n) \in Sol(S'; k[Z]/(S')_0)$ where $z_i = Z_i \mod (S')_0$. By assumption, $(1, z_1, \ldots, z_n) \in Sol(S; k[Z]/(S')_0)$. 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 $\mathcal{M}_+^s G \in (S')$ 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 $\mathbf{P}_k^n$.*

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 $V \subset \mathbf{P}^n(K)$ of the form $PSol(S; K)$, where X is a system of homogeneous equations in n-variables with coefficients in k. We define the *Zariski k-topology* in $\mathbf{P}^n(K)$ by choosing closed sets to be projective algebraic k-sets. We leave the verification of the axioms to the reader.

Problems.

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

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

3*. Let $A = \mathbf{C}[T_1, T_2]/(T_1^2 - T_2(T_2 - 1)(T_2 - 2)), t_1$ 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 $I \supset \mathcal{M}_+^s$ 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 $\mathbf{P}_k^3$ 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 $F \in k[T_0, \ldots, T_n]$ be a homogeneous polynomial free of multiple factors. Show that its set of solutions in $\mathbf{P}^n(K)$, 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":

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

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

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

be the projective closures of these conics in the projective plane $\mathbf{P}_k^2$, 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 $\mathbf{P}_k^2$ given by an irreducible homogeneous equation of degree m and n, respectively, have mn common points (counting with appropriate multiplicities) in $\mathbf{P}_k^2(K)$ 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 $(A_0, \dots, A_n)$ and zeroes, and the remaining n rows are occupied with the string $(B_0, \dots, B_m)$ 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

$$(*) \quad P(Z)Q_1(Z) - Q(Z)P_1(Z) = 0.$$

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

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

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 $(a_0, \dots, a_n, b_0, \dots, b_m)$. Conversely, assume that the above determinant vanishes. Then we find a polynomial $P_1(Z)$ of degree $\le n-1$ and a polynomial $Q_1(Z)$ of degree $\le m-1$ satisfying (*). 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 $P(Z) = a_0Z^n + \dots + a_n$ and $Q(Z) = b_0Z^m + \dots + b_m$ the value of $R_{n,m}$ at $(a_0, \dots, a_n, b_0, \dots, b_m)$ 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 $\mathbf{P}^2_k$ 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*). An element of $X(K)$ is called a K-point of X. 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 $\mathbf{P}^2(K)$ 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 $\mathbf{P}^2(K)$ 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. 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 $\mathbf{P}^1(K)$. 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 $\mathbf{P}^2(K)$. 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. We say that L is tangent to the curve X at a nonsingular point $x \in \mathbf{P}^2(K)$ if $x \in L(K) \cap X(K)$ and its multiplicty ≥ 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 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 $X(K)$.

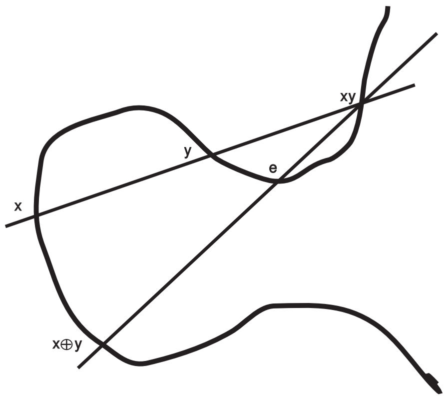

Fig.1

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:

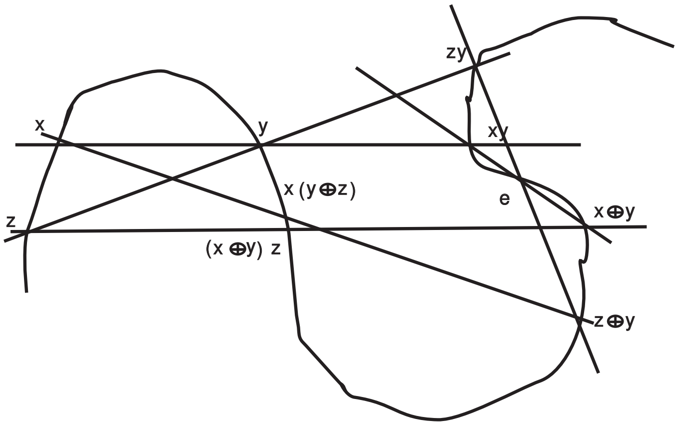

Fig.2

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 $a, b \in \mathbf{P}^2(K)$ 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

$$< y, z > \cup < xy, x \oplus y > \cup < x, y \oplus z > . \qquad (20$$

We will use the following:

Lemma. *Let $x_1, \ldots, x_8$ be eight distinct points in $\mathbf{P}^2(\bar{k})$. 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 $F = a_0T_0^3 + a_1T_0^2T_1 + \ldots = 0$ 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 $\mathbf{P}^2_k(K)$.

Remark.1 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 inflection points of the cubic curve C. The configuration of the 12 lines as above is called the *Hesse configuration of lines.*

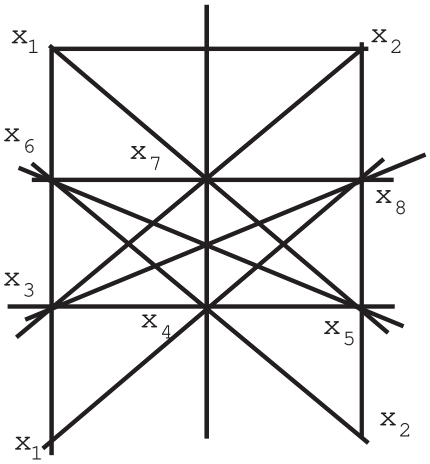

Fig. 3

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

To apply our lemma we take the eight points $e, x, y, z, zy, xy, x \oplus y, y \oplus z$ in $X(K)$. Obviously they saisfy 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 $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Remarks. 2. 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.
3. 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 $P(Z)=a_0Z^n+a_1Z^{n-1}+\ldots+a_n$ be a polynomial with coefficients in a field k, and $P'(Z)=na_0Z^{n-1}+(n-1)a_1Z^{n-2}+\ldots+a_n$ 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

$$R_{n,m}(P,Q)=\pm a_0^mb_0^n\prod_{i=1}^n\prod_{i=1}^m(\alpha_i-\beta_j)=a_0^m\prod_{i=1}^nQ(\alpha_i)=b_0^n\prod_{j=1}^mP(\beta_j).$$

3. Find explicit formulae for the group law on $X(\mathbf{C})$, where X is a cubic curve defined by the equation $T_1^2T_0-T_2^3-T_0^3=0$. 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 the Lemma.
5. Let X be given by the equation $T_1^2T_0-T_2^3=0$. 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 $T_1^2T_0-T_2^2(T_2+T_0)=0$. 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 morphism of the corresponding functors from $\mathcal{A}lg_k \to \mathcal{S}ets$. 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 map must be given by

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

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 $f : X \to Y \subset \mathbf{P}_k^n$ (of functors) from an affine variety X to a projective algebraic variety Y over a field k. To define f it is enough to define $f : X \to \mathbf{P}_k^n$ 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 $M \in \mathbf{P}_k^n(\mathcal{O}(X))$. Let $\{f_i\}_{i\in I}$ be a trivializing covering family of M. For every $i \in I$ the localization M_{f_i} is a line in $\mathcal{O}(X)_{f_i}^{n+1}$. It is generated by a vector $(p_0^{(i)}/f_i^r, \ldots, p_n^{(i)}/f_i^r) \in C_n(\mathcal{O}(X)_{f_i})$ (where we reduced the fractions to a common denominator). Note that since f_i^r is invertible in $\mathcal{O}(X)_{f_i}$ 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 by a. Since $1 = \sum_j b_j p_j^{(i)}/f_i^r$ for some $b_0, \ldots, b_n \in \mathcal{O}(X)_{f_i}$, we obtain, after clearing the denominators, that the ideal generated by $p_0^{(i)}, \ldots, p_n^{(i)}$ is equal to (f_i^d) for some $d \geq 0$. So

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

Now let K be any k-algebra and $x \in X(K)$, considered as a homomorphism $x : \mathcal{O}(X) \to K, p \to p(x)$.. Since $1 = \sum_i b_i f_i$ for some $b_i \in \mathcal{O}(X)$ we have $1 = \sum_i b_i(x) f_i(x)$, hence $f_i(x)$ is a covering family in K. The homomorphism $x : \mathcal{O}(X) \to K$ induces a homomorphism $x_i : \mathcal{O}(X)_{f_i} \to K_{f_i(x)}$, and we have the following commutative diagram:

$$\begin{array}{ccccc} X(\mathcal{O}(X)) & \to & X(\mathcal{O}(X)_{f_i}) & \to & X(K_{f_i(x)}) \\ \downarrow & & \downarrow & & \downarrow \\ Y(\mathcal{O}(X)) & \to & Y(\mathcal{O}(X)_{f_i}) & \to & Y(K_{f_i(x)}) \end{array}.$$

Here, under the composition of the upper horizontal arrows, $\mathrm{id}_{\mathcal{O}(X)} \in X(\mathcal{O}(X))$ goes to the composition $(\mathcal{O}(X) \to \mathcal{O}(X)_{f_i} \to K_{f_i(x)}) \in X(K_{f_i(x)})$. Under the left vertical arrow $\mathrm{id}_{\mathcal{O}(X)}$

goes to $M \in Y(\mathcal{O}(X))$. Then M, under the composition of the lower horizontal arrows, goes to $M_{f_i} \otimes K_{f_i(x)} \in Y(K_{f_i(x)})$. If M_{f_i} is given by $(p_0^{(i)}, \dots, p_n^{(i)}) \in \mathcal{O}(X)^{n+1}$, then $M_{f_i} \otimes K_{f_i}$ is given by $(p_0^{(i)}(x), \dots, p_n^{(i)}(x))$. This completely describes our map:

It is given by a collection

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

of elements $(p_0^{(i)}, \dots, p_n^{(i)}) \in \mathcal{O}(X)^{n+1}$ such that $(p_0^{(i)}, \dots, p_n^{(i)}) = (f_i^{d_i})$ for some $d_i \geq 0$. It satisfies the following two properties:

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

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

The map sends a K-point $x \in X(K)$ to a K-point $M(x) \in \mathbf{P}^n(K)$ which is a local line over K given by a collection $\{(p_0^{(i)}(x), \dots, p_n^{(i)}(x))\}_{i \in I}$ with respect to the trivializing family $\{f_i(x)\}_{i \in I}$. Note that since $p_0^{(i)}(x), \dots, p_n^{(i)}(x)$ generate the ideal $(f_i^{d_i})$, the elements $p_0^{(i)}(x), \dots, p_n^{(i)}(x)$ generate the ideal $(f_i(x)^{d_i})$, hence define a line over $K_{f_i(x)}$. 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 $M \in \mathbf{P}^n(\mathcal{O}(X))$ in a trivializing covering family $\{g_j\}_{j \in J}$. They agree in the folowing sense:

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

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

Consider the special case when K is a field, $x \in X(K)$. Then $K_{f_i(x)} = \{0\}$ or K dependent on whether $f_i(x) = 0$ or not. So we may choose f_i such that $f_i(x) \neq 0$, then x defines a homomorphism $ev_x : \mathcal{O}(X) \to K$ and the image of x is the point $(p_0^{(i)}(x), \dots, p_n^{(i)}(x)) \in \mathbf{P}^n(K)$. If we choose other f_j with $f_j(x) \neq 0$, then property (ii) from above implies that

$$(p_0^{(i)}(x), \dots, p_n^{(i)}(x)) = (p_0^{(j)}(x), \dots, p_n^{(j)}(x))$$

as points in $\mathbf{P}^n(K)$.

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

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

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

For any family $\{M_i\}_{i \in I}$ of A_{f_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

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

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

Lemma. *The homomorphism*

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

is an isomorphism.

Proof. The proof of injectivity is similar to the proof of Lemma 2 and is left to the reader. Let us show the surjectivity. Let

$$(m_i/f_i^{n_i})_{i\in I} \in \varinjlim_{i \in I} M_{f_i}$$

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 $i, j \in I$

$$\rho_{ij}(m/f_i^n) = \rho_{ji}(m_j/f_j^n),$$

we have

$$(f_i f_j)^r (f_j^n m_i - f_i^n m_j) = 0$$

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

$$m_i/f_i^n = p_i/f^k, f_j^k p_i = f_i^k p_j.$$

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

$$f_j^k m = \sum_i b_i f_j^k p_i = \sum_i b_i f^k p_j = 1 p_j = p_j.$$

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

Let $f : X \to Y$ be a morphism of projective algebraic varieties, $X \subset \mathbf{P}_k^m, Y \subset \mathbf{P}_k^n$. For every k-algebra K and $M \in X(K)$ we have $N = f(K)(M) \in Y(K)$. Clearly 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 $\{N_{a_i}\}_{i\in I}$. Thus our morphism $f : X \to Y$ is determined by its restriction to the subfunctor $X' : K \to \mathbf{P}^n(K)' \cap X(K)$, 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 $(t_0, \ldots, t_m)$ with at least one t_i invertible in M_{a_i}. For example we can take the covering family $\{t_0, \ldots, t_m\}$, then each t_i is invertible in K_{t_i}. Note that this is true even when $t_i = 0$ 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. Obviously $K \to X(K)''$ is a subfunctor of X.

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 $A^{(r)}$ be the factor algebra. It is clear that any homomorphism $A^{(r)} \to K, T_k/T_r \bmod I_r \to a_k$, defines a point $(a_0, \ldots, a_m) \in X(K)$. Its r-th coordinate is equal to 1. Conversely, every point $(a_0, \ldots, a_m) \in X(K)$ with $a_r \in K^*$ arises in this way. We can say it in the following "functorial" way. We have morphisms of functors

$$\underline{I}_r \to X, \underline{I}_r(K) \to X(K),$$

and each $x \in X(K)''$ belongs to the image of some $\underline{I}_r(K) \to X(K)$. Now to define the morphism $X \to Y$ it suffices to define the morphisms $\phi_r : \underline{I}_r \to Y, r = 0, \ldots, m$. This we know how to do. Each ϕ_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 $A^{(r)}$, and $f_s \in \mathrm{rad}(\{p_0^{(s)}, \dots, p_n^{(s)}\})$ for some $f_s \in A^{(r)}$. We can find a representative of $p_j^{(s)}$ in $k[T_0/T_r, \dots, T_n/T_r]$ 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 $j = 0, \dots, n$. Also by choosing appropriate representative F_s/T_r^l for f_s, we obtain that $T_r^\alpha F_s^\beta \in (P_0^{(s)}, \dots, P_n^{(s)}) + I$ Collecting all these data for each $r = 0, \dots, m$, we get that our morphism is given by a collection of

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

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

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

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 $(P_0^{(s)}(x), \dots, P_n^{(s)}(x)) \in C_n(K_{F_s(x)})$ 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 $k, j = 0, \dots, n$. Since $F(p_0^{(s)}, \dots, p_n^{(s)}) = 0$ for any F from the homogeneous ideal J defining Y, we must have

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

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

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

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

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

Then the formula:

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

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

Proof. We have to check that $(F_0(a), \dots, F_n(a)) \in C_n(K) \cap Y(K)$ for all K-algebras K. The "functoriality" 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 $G(F_0(a), \dots, F_n(a)) = 0$. It remains to show that $(F_0(a), \dots, F_n(a)) \in C_n(K)$. 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 $(F_0(a), \dots, F_n(a)) \in C_n(K)$. This proves the assertion.

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

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

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 the Proposition 1, therefore it defines an automorphism: $f : \mathbf{P}_k^n \to \mathbf{P}_k^n$. It is called a *projective automorphism*.
2. Assume $\mathrm{char}(k) \neq 2$. Let $C \subset \mathbf{A}_k^2$ 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 $\mathbf{P}_k^2$. Applying a projective automorphism of $\mathbf{P}_k^2, T_0 \to T_2, T_1 \to T_0 - T_1, T_2 \to T_0 + T_1$ we see that X is isomorphic to the curve $T_0^2 - T_1 T_2 = 0$. Let us show that X is isomorphic to $\mathbf{P}_k^1$. The corresponding morphism $f : \mathbf{P}_k^1 \to X$ is given by

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

The polynomials $T_0 T_1, T_0^2, T_1^2$, obviously satisfy the assumption of the Proposition 1. The inverse morphism $f^{-1} : X \to \mathbf{P}_k^1$ 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 $a_1, a_2 \in K^*$,

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

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

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

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

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

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

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 $\mathbf{A}_k^1$.
2. A projective subvariety E of $\mathbf{P}_k^n$ 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

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

Let $X \subset \mathbf{P}_k^n$ be such that

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

Then the map

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

defines a morphism

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

which is said to be a *linear projection* from E. Let $i : \mathbf{P}_k^{n-d-1} \to \mathbf{P}_k^n$ be the map given by $(a_0, \ldots, a_{n-d-1}) \mapsto (a_0, \ldots, a_{n-d-1}, 0, \ldots, 0)$, then we can interpret the composition $p_E : X \to \mathbf{P}_k^{n-d-1} \to \mathbf{P}_k^n$ as follows. Take a point $x \in X(K)$, find a projective subspace $E' \subset \mathbf{P}_k^n$ of dimension $d+1$ such that $E'(K)$ contains $E(K)$ and x. Then

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

We leave this verification to the reader (this is a linear algebra exercise). Here is a picture of a linear projection from a 0-dimensional subspace $E = \{x\}$:

3. We already know that $\mathbf{P}_k^1$ is isomorphic to a subvariety of $\mathbf{P}_k^2$ 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 $\mathbf{P}_k^N$ 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)

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

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 $v_{n,m}(K)' : \mathbf{P}_k^n(K)' \to \mathbf{P}_k^N(K)$ 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 $\mathbf{P}_k^N$ 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 functors:

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

To verify this it suffices to check that $v_{n,m}(K)(\mathbf{P}_k^n(K)'') = Ver_n^m(K)''$ (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 $v_{1,2} : \mathbf{P}_k^1 \to \mathbf{P}_k^2$ is given by the same formulas as the map from Example 1, and its image is a conic.

Next we want to define the Cartesian product $X \times Y$ of two projective varieties X and Y. Of course, similar to the case of affine varieties, it is natural to define the product as the functor

$$K \to X(K) \times Y(K).$$

The problem is to prove that this functor is a projective algebraic variety. Consider first the case where $X = \mathbf{P}_k^n$ and $Y = \mathbf{P}_k^m$. 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 $K^{n+1} \otimes_k K^{m+1} \cong K^{(n+1)(m+1)}$. Define a morphism of functors (the *Segre morphism*)

$$s_{n,m} : \mathbf{P}_k^n \times \mathbf{P}_k^m \to \mathbf{P}_k^N, N = (n+1)(m+1) - 1,$$

by

$$s_{n,m}(K)(M, M') = M \otimes M'.$$

Its restriction $s'_{n,m}$ to $'\mathbf{P}_k^n \times' \mathbf{P}_k^m$ is defined by the formula

$$s'_{n,m}(K)((a_0, \ldots, a_n), (b_0, \ldots, b_m)) = (a_0 b_0, \ldots, a_0 b_m, a_1 b_0, \ldots, a_1 b_m, \ldots, a_n b_0, \ldots, a_n b_m).$$

It is checked immediately that this map is well defined. It is easy to see that it is injective on the subsets $\mathbf{P}^n(K)'' \times \mathbf{P}_k^m(K)''$. 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 functor $s_{n,m}(\mathbf{P}_k^n \times \mathbf{P}_k^m)$ is contained in the subfunctor of the projective subvariety Z of $\mathbf{P}_k^N$ given by the equations:

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

in the polynomial ring $k[T_0, \ldots, T_N], T_0 = T_{00}, \ldots, T_N = T_{nm}$. Let us show that $s_{n,m}(\mathbf{P}_k^n \times \mathbf{P}_k^m) = Z$. Since we can reconstruct any $M \in \mathbf{P}^n(K)$ from its localizations, it suffices to verify that the map $s_{n,m}(K)'' : \mathbf{P}_k^n(K)'' \times \mathbf{P}_k^m(K)'' \to Z(K)''$ 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

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

This proves the assertion and we get an isomorphism of functors

$$\mathbf{P}_k^n \times \mathbf{P}_k^m \cong Z \subset \mathbf{P}_k^N.$$

At this point it is natural to generalize the notion of a projective variety:

Definition. A *projective algebraic k-variety* is a functor from $\mathcal{A}lg_k$ to $\mathcal{S}ets$ isomorphic to a functor $K \to X(K)$, where X is a system of homogeneous algebraic equations. The category of projective algebraic k-varieties is a full subcategory of $Funct(\mathcal{A}lg_k, \mathcal{S}ets)$. A subvariety is a subfunctor.

With this definition in mind we can say that the functor $\mathbf{P}_k^n \times \mathbf{P}_k^m$ is a projective algebraic variety. Note that it is equipped with the projection morphisms:

$$p_i : \mathbf{P}_k^n \times \mathbf{P}_k^m \to \mathbf{P}_k^n, i = 1, 2.$$

Now for any two projective subvarieties $X \subset \mathbf{P}_k^n$ and $Y \subset \mathbf{P}_k^m$ 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 $\mathbf{P}_k^N, N = (n+1)(m+1) - 1$, defined by the equations:

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

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

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

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 $T_{ij} = T_i T'_j, i = 0, \ldots, n (resp. T_{ij} = T'_i T_j, j = 0, \ldots, m)$.

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 objectZ 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 $\mathbf{P}_k^n$ is isomorphic to $\mathbf{P}_k^d$.
2. Prove that $\mathbf{P}_k^1 \times \mathbf{P}_k^1$ is isomorphic to a hypersurface $Q in \mathbf{P}_k^3$ 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 :

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

where the symmetric matrix (a_{ij}) is nonsingular, is isomorphic to $\mathbf{P}_k^1 \times \mathbf{P}_k^1$. Give an explicit formula for the projection maps: $p_i : Q \to \mathbf{P}_k^1$.
3. Show that Ver_1^n is isomorphic to the projective closure of the affine curve given by the equations $\{Z_n - Z_1^n = 0, \ldots, Z_2 - Z_1^2 = 0\}$ (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 $\mathbf{P}_k^3$ from a point not lying on this curve is isomorphic to a plane cubic curve. Find its equation and show that this curve is not nonsingular 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 the restriction of the functor $\mathbf{P}_k^n \times \mathbf{P}_k^m$ to the category of field extensions of k is isomorphic to the functor $K \to \{$rank 1 matrices of size $(n+1) \times (m+1)$ with coefficients in K up to proportionality$\}$. b)Show that the restriction of the functor Ver_n^2 to the category of field extensions of k is isomorphic to the functor $K \to \}$symmetric rank 1 square matrices with coefficients in K of size m up to proportionality $\}$.
7. Construct a morphism from $\mathbf{P}_k^1$ to the curve X equal to the projective closure of the affine curve $(Z_1^2 + Z_2^2)^2 - Z_2(3Z_1^2 - Z_2^2)) \subset \mathbf{A}_k^2$ Is X isomorphic to $\mathbf{P}_k^1$?

Lecture 8. QUASI-PROJECTIVE ALGEBRAIC SETS

Let k be a field and K be its algebraic closure.

Definition. A *projective algebraic set* over k (or a projective algebraic k-set) is a subset V of $\mathbf{P}^n(K)$ 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 $m^s F \in I$ for some s and $F \in k[T]_d$ then all monomials entering into F belong to m^d. In particular, $F^s \in m^{ds}$ and $F^s F = F^{s+1} \in I$. Since I is radical this implies that $F \in I$. We can consider $\mathbf{P}^n(K)$ as a projective algebraic set over any subfield k of K. Any projective algebraic k-subset of $\mathbf{P}^n(K)$ is called a closed subset of $\mathbf{P}^n(K)$. The reason for this definition is explained by the following lemma.

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

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

The topology on $\mathbf{P}^n(K)$ whose closed sets are projective algebraic subsets is said to be the *Zariski k-topology.* As is in the affine case we will drop k from the definitions if $k = K$. Every subset of $\mathbf{P}^n(K)$ will be considered as a topological subspace with respect to the induced Zariski 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. A subset V of $\mathbf{P}^n(K)$ is said to be a *quasi-projective algebraic k-set* if V is locally closed with respect to the Zariski k-topology.

In other words, a quasi-projective k-subset of $\mathbf{P}^n(K)$ 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

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

Its complement is the "coordinate hyperplane":

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

Every affine algebraic set $V \subset \mathbf{A}^n(K)$ can be naturally considered as a quasi-projective algebraic set. We view $\mathbf{A}^n(K)$ as the open subset $\mathbf{P}^n(K)_0$, then note that $V = \bar{V} \cap \mathbf{P}^n(K)_0$, 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 $\mathbf{P}^n(K)$. Also observe that $\bar{V}$ equals the closure in the sense of topology, i.e., the minimal closed subset of $\mathbf{P}^n(K)$ which contains V.

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

Definition. A map $f : V \to W \subset \mathbf{P}^m(K)$ of quasi-projective algebraic 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 the formula:

$$x \to (F_0(x), \dots, F_m(x)),$$

where $F_0(T), \dots, F_m(T)$ are homogeneous polynomials of some degree d.

This is very similar to the definition of a morphism of projective algebraic varieties, and as in the latter case, it imposes several conditions on the polynomials $F_i(T)$. We leave to the reader to list these conditions.

Example. Assume $V \subset \mathbf{P}^n(K), W = \mathbf{A}^1(K)$. A regular map $f : V \to \mathbf{A}^1(K) \subset \mathbf{P}^1(K)$ 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 set. On the opposite side we have:

Proposition 1. *Let $V \subset \mathbf{A}^n$ be an affine algebraic set considered as a quasi-projective algebraic set in $\mathbf{P}^n(K)$. Then $\mathcal{O}(V)$ is isomorphic to the algebra of regular function of the affine algebraic set V.*

Proof. 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 the map given by the 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 for which

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

Clearly,

$$(*) \quad Q_i(x)' f_i(x) = P_i(x)', x \in U_i$$

where P_i', Q_i' are the corresponding dehomogenized polynomials in $Z_i = T_i/T_0$. We may also assume that the previous equality takes place for all $x \in V$, this can be achieved by multiplying both sides of $(*)$ by a homogeneous polynomial from the ideal defining the closed subset $V \setminus U_i$. The system of equations $Q_i(Z)' = 0, i \in I$ has no solutions in V. This implies that the system

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

has no solution in $\mathbf{A}^n(K)$. By Hilbert's Nullstellensatz $1 = \sum_i A_i Q_i' + \sum_s B_s F_s$ for some polynomials $A_i, i \in I$, and $B_s, s \in S$. This shows that

$$(**) \quad 1 = \sum_i A_i(x) Q_i'(x) \quad \text{for all } x \in V.$$

Since $Q_i'(x)f(x) = P_i'(x)$ for all $x \in V$, multiplying both sides of $(**)$ by f, we obtain, for all $x \in V$,

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

This shows that f is a regular function on V in the sense of our previous definition.

An *isomorphism* (or a *biregular map*) of quasi-projective algebraic sets is an invertible regular map. Two sets are isomorphic if there exists an isomorphism from one set to another.

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

Note that an affine quasi-projective set is not an affine algebraic set in general. For example, the set $\mathbf{P}^n(K)_i, i \neq 0$, is an affine quasi-projective set but not equal to an affine algebraic set (which must be contained in $\mathbf{P}^n(K)_0$).

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

Proof. Let V be any quasi-projective algebraic subset of $\mathbf{P}^n(K)$ and $x \in V$. Obviously $x \in \mathbf{P}^n(K)_i$ for some i. Thus $x \in V \cap \mathbf{P}^n(K)_i$ which is a quasi-projective algebraic set. By definition, $V \cap \mathbf{P}^n(K)_i = Z_1 \cap \mathbf{P}^n(K)_i \setminus Z_2 \cap \mathbf{P}^n(K)_i$ where Z_1 and Z_2 are closed subsets of $\mathbf{P}^n(K)$. Let Z_1 be given by the ideal $I \subset k[T_0/T_i,\dots,T_n/T_i] = k[Z_1,\dots,Z_n]$, and F belongs to the ideal defining Z_2. Then $Z_2 \subset V(F)$, where $V(F)$ is the set of zeroes of F, hence $x \in Z_1 \setminus V(F) \subset Z_1 \setminus Z_2$. Consider an affine algebraic set W in $\mathbf{A}^{n+1}(K)$ with coordinates $(T_1,\dots,T_n,T_{n+1})$ given by the ideal $(I, FT_{n+1} - 1)$. It comes with a natural projection $p : W \to V, (a_1,\dots,a_{n+1}) \mapsto (a_1,\dots,a_n)$. It is clear that p is a regular map. Since $F(a_1,\dots,a_n)a_{n+1} = 1$ for any $a = (a_1,\dots,a_{n+1}) \in W, p$ is an isomorphism onto the subset $Z_1 \setminus V(F)$. This proves the assertion.

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

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 2. *Every quasi-projective algebraic k-set V is a Noetherian 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

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

which must stabilize with a set $V' = V \setminus (U_{i_1} \cup \ldots \cup U_{i_r})$. If it is not empty, we can subtract one more subset U_{i_j} to decrease V'. Therefore, $V' = \emptyset$ and $V = U_{i_1} \cup \ldots \cup U_{i_r}$. 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 3. *A subspace Z of $\mathbf{P}^n(K)$ is irreducible if and only if the 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 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 $\{(a,b,c)\in \mathbf{P}^2(K) : a\neq 0, b\neq 0\}\cup\{(1,0,0)\}$ quasi-projective?
2. Let V be a quasi-projective algebraic set in $\mathbf{P}^n(K), W$ be a quasi-projective algebraic set in $\mathbf{P}^r(K)$. Prove that $s_{n,m}(K)(V\times W)$ is a quasi-projective algebraic subset of $Seg_{n,m}(K) = s_{n,m}(K)(\mathbf{P}^n(K)\times \mathbf{P}^r(K))\subset \mathbf{P}^{(n+1)(m+1)-1}(K)$.
3. Let us identify the product $V\times W\subset \mathbf{P}^n(K)\times \mathbf{P}^r(K)$ 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 $\mathbf{P}^3(K)$ 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 $V(F) = \{a\in \mathbf{P}^n(K) : F(a) = 0\}$ is a hypersurface $V(G)$, where G is an irreducible factor of the homogenous polynomial $F(T)$.
7. Show that the complement to a hypersurface $V(F)$ in $\mathbf{P^n(K)}$ is an affine algebraic set.

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 $\mathbf{A}_k^2(K)$ which contains the image $f(K^2)$ is K^2 and the image is not closed there. Thus $f(\mathbf{A}_k^2(K))$ is not locally closed in $\mathbf{A}_k^2(K)$. Since K^2 is an open subset of $\mathbf{P}_k^2(K)$, $f(\mathbf{A}_k^2(K))$ is not locally closed in $\mathbf{P}_k^2(K)$, 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

$$f(V) = pr_2(\Gamma_f)$$

where

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

is the graph of f, and $pr_2 : V \times W \to W, (x, y) \mapsto y$ 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 $pr_2(Z)$ is closed in W.*

Let us prove first 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 $\Gamma_f = (f \times id_W)^{-1}(\Delta_W)$.

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 $W = \mathbf{P}_k^n(K)$. However, the diagonal $\Delta_{\mathbf{P}_k^n(K)} \subset \mathbf{P}_k^n(K) \times \mathbf{P}_k^n(K)$ is given by the system of equations:

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

in coordinates T_{ij} of the space containing the image of $\mathbf{P}_k^n(K) \times \mathbf{P}_k^n(K)$ 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 "compactness" of a projective algebraic set.

Before proving Theorem 2 let us prove the following:

Lemma. *Let V be a closed subset of $\mathbf{P}_k^n(K) \times \mathbf{P}_k^m(K)$ (resp. of $\mathbf{P}_k^n(K) \times \mathbf{A}_k^m(K)$). Then V is the set of zeroes of polynomials $P_s(T_0, \ldots, T_n, T_0', \ldots, T_m') \in k[T_0, \ldots, T_n, T_0', \ldots, T_m'], s \in S$, which are homogeneous of degree $d(s)$ in variables $T_0, \ldots, T_n$ and homogeneous of degree $d(s)'$ in the variables $T_0', \ldots, T_m'$ (resp. V is the set of zeroes of polynomials $P_s(T_0, \ldots, T_n, Z_1', \ldots, Z_m') \in k[T_0, , \ldots, T_n, Z_1', \ldots, Z_m'], s \in S$, which are homogeneous of degree $d(s)$ in variables $T_0, \ldots, T_n$). Conversely every subset of $\mathbf{P}_k^n(K) \times \mathbf{P}_k^m(K)$ (resp. of $\mathbf{P}_k^n(K) \times \mathbf{A}_k^m(K)$) 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 $\mathbf{P}_k^n(K) \times \mathbf{P}_k^m(K)$ 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 $\mathbf{P}_k^{(n+1)(m+1)-1}$ 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 $T_0, \ldots, T_n, T_0', \ldots, T_m'$ which are homogeneous in each set of variables of the same degree. If we have a system of polynomials $P_s(T_0, \ldots, T_n, T_0', \ldots, T_m')$ which are homogeneous of degree $d(s)$ in variables $T_0, \ldots, T_n$ and homogeneous of degree $d(s)'$ in variables $T_0', \ldots, T_m'$, its set of solutions in $\mathbf{P}_k^n(K) \times \mathbf{P}_k^m(K)$ is also given by the system in which we replace each P_s by ${T_i'}^{d(s)-d(s)'}P_s, i = 0, \ldots, m$, if $d(s) > d(s)'$ and by $T_i^{d(s)'-d(s)}P_s, i = 0, \ldots, n$, 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 $\mathbf{P}_k^n(K)$. Then $Z \subset V \times W$ is a closed subset of $\mathbf{P}^n(K) \times W$ and $pr_2(Z)$ equals the image of Z under the projection $\mathbf{P}_k^n(K) \times W \to W$. Thus we may assume that $V = \mathbf{P}_k^n(K)$.

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 $pr_2(Z) = \cup_{i \in I} pr_2 Z \cap (V \times U_i)$. This shows that it suffices to check that $pr_2 Z \cap (V \times U_i)$ 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 $\mathbf{A}_k^m(K), V\times W$ is closed in $V\times\mathbf{A}_k^m(K)$ and $pr_2(Z)$ is equal to the image of Z under the second projection $V\times\mathbf{A}_k^m\to\mathbf{A}_k^m$. Thus we may assume that $W=\mathbf{A}_k^m(K)$ and $V=\mathbf{P}_k^n(K)$.

Let Z be a closed subset of $\mathbf{P}_k^n(K)\times\mathbf{A}_k^m(K)$. 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 $\mathbf{P}^n(K)$ 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

$$pr_2(Z)=\{a\in K^m: X_a\neq\emptyset\}=\{a\in K^m:(T_0,\ldots,T_n)^s\not\subset I_a\quad\text{for any } s\geq 0\}$$

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

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

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

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 $\mathbf{A}_k^1$ 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 $f : V \to \mathbf{A}^1(K)$. Composing it with the inclusion $\mathbf{A}^1(K) \hookrightarrow \mathbf{P}^1_k(K)$, we obtain a regular map $f' : V \to \mathbf{P}^1_k(K)$. By Theorem 1, $f(V) = f'(V)$ is closed in $\mathbf{P}^1_k(K)$. Since $f(V) \subset \mathbf{A}^1_k(K)$, 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 $\mathbf{P}^n_k(K)$. Suppose Z is contained in an affine subset U of $\mathbf{P}^n_k(K)$. 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 $W \subset \mathbf{P}^n(K)_0 \subset \mathbf{P}^n(K)$ for some n, and $f' : V \to \mathbf{P}^n(K)$ be the composition of f and the natural inclusion $W \hookrightarrow \mathbf{P}^n(K)$. By Theorem 1, $f(V) = f'(V)$ is a closed connected subset of $\mathbf{P}^n(K)$ 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 $\mathbf{A}^N(K), N = \binom{n+d}{d}$. Find its equation when $n = d = 2$.
2. Let $X = K^2 \setminus \{0\}$. Prove that X is not isomorphic to neither projective nor affine algebraic set.
3. Same as in the previous problem but $X = \mathbf{P}^n(K) \setminus \{\text{point}\}$.

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

Lecture 10. FINITE REGULAR MAPS

In this lecture we shall prove 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." 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 $x^n + a_1x^{n-1} + \ldots + a_n = 0$ 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 $x^{n(i)}$ 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 the value of 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 $b = a_1b_1 + \ldots + a_rb_r$ where $b_1, \ldots, b_r$ is a fixed set of elements in B and $a_i \in A$. Take any $x \in B$ and write

$$xb_i = \sum_{j=1}^{r} a_{ij}b_j, i = 1, \ldots, r,$$

for some matrix $M = (a_{ij})$ with coefficients in A. Consider the linear map $T_x : B \to B$ of A-modules defined by the formula $T_x(b) = xb$. By Cayley-Hamilton theorem, T_x satisfies the characteristic equation

$$P(t) = \det[M - tI_n] = (-1)^n t^n + c_1t^{n-1} + \ldots = 0.$$

Hence $P(T_x) = T_{P(x)}$ is the zero operator. In particular $P(x)b = 0$ for every $b \in B$, hence $P(x)^2 = P(x)P(x) = 0$. Since $P(t)^2$ is a monic polynomial in t, we get that x is integral over 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 $b_i \in B, a_i \in I$. Multiplying both sides by any $b \in B$ we see that the A-module B is generated over A by $b_1, \ldots, b_n$. Since $IB = B$ we can write

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

Thus, the vector $(b_1, \ldots, b_n) \in B^n$ is a solution of a system of linear equations $(M - I_n)x = 0$ where $A = (a_{ij})$. Let $D = \det(M - I_k)$. By the Cramer rule, $Db_i = 0$ for all i. Hence $Db = 0$ for all $b \in B$. In particular, $D^2 = 0$. 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 $\mathbf{P}_k^n(K)$ 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 $\mathbf{P}_k^n(K)$ with $x_0 \notin X$ and let $f = pr_{x_0} : X \to \mathbf{P}_k^{n-1}(K)$ 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 $V = Y \cap \mathbf{P}_k^{n-1}(K)_0$ where $x_0 \neq 0$. Its preimage $U = f^{-1}(V) = X \cap \mathbf{P}_k^n(K)_0$. 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 $X \cap \mathbf{P}_k^n(k)_0$, 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 $T_i, i \le n-1$, must contain $k[T]_d$ for some $d \ge 0$. 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.

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*

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

Proof. Assume first that $X \subset \mathbf{A}_k^n(K)$ is affine. Then $D(\phi)$ is affine and is isomorphic to a closed subset of $\mathbf{A}_k^{n+1}(K)$ which is given by the equations defining X (in the first n unknowns) and one additional equation $Z_{n+1}\phi - 1$, where ϕ is any representative of ϕ in $k[Z_1, \ldots, Z_n]$. This obviously implies that

$$\mathcal{O}(D(\phi)) \cong \mathcal{O}(X)[Z_{n+1}]/(Z_{n+1}\phi - 1) \cong \mathcal{O}(X)[1/\phi] \cong \mathcal{O}(X)_\phi.$$

Now 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 completely 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*

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

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 $\phi_1, \ldots, \phi_n \in \mathcal{O}(X)$ which generate the unit ideal. Then $X = \cup_i D(\phi_i)$. Let $k[Z_1, \ldots, Z_n] \to \mathcal{O}(X)$ be a surjective homomorphism of k-algebras and I be its kernel. The set of zeroes of I in $\mathbf{A}^n(K)$ 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. Replacing Y by V, X by $f^{-1}(V)$ and Z by $Z \cap V$, we may assume that X and Y are affine. Choose $\phi \in \mathcal{O}(Y)$ such that $\phi(y) \neq 0$, so that $y \in D(\phi) \subset V$. Then by Lemma 3 we have $\mathcal{O}(D(\phi)) = \mathcal{O}(V)_\phi, \mathcal{O}(f^{-1}(D(\phi)) = \mathcal{O}(X)_{f^*(\phi)}$. Clearly $f^* : \mathcal{O}(V)_\phi \to \mathcal{O}(f^{-1}(V))_{f^*(\phi)}$ is injective and defines an integral extension (Lemma 2). Since each $D(\phi)$ as above is affine, we may assume that

$$Y = \cup_i V_i, V_i = D(\phi_i), \phi_i \in \mathcal{O}(Y),$$

$$X = \cup_i U_i, U_i = f^{-1}(V_i) = D(f^*(\phi_i)),$$

$$f_i = f|U_i : U_i \to V_i \quad \text{is a finite map of affine sets.}$$

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) for any $y \in Y$, the fibre $f^{-1}(y)$ is a finite set;
(ii) f is surjective.

Proof. Clearly, we may assume that X and Y are affine, $\mathcal{O}(X)$ is integral over $f^*(\mathcal{O}(Y))$ and f^* is injective. We assume also that $k = \bar{k}$ since our properties do not depend on k. So all points of X and Y are geometric and are closed in the Zariski topology. Since y is closed and does not contain proper non-empty closed subsets the ideal m_y of all regular functions on Y vanishing at y is maximal. By Proposition 2 the induced map $f^{-1}(y) \to y$ is a finite regular map. It is the affine closed subset of X given by the ideal $f^*(m_y)$. This ideal is proper by Lemma 2 (iv). Thus $f^{-1}(y) \neq \emptyset$, hence f is surjective. Moreover $\mathcal{O}(f^{-1}(y)) \cong \mathcal{O}(X)/f^*(m_y)$. This is an integral finitely generated algebra over $K = \mathcal{O}(Y)/m_y$. It follows from Lemma 2 (iii) that every prime ideal of this algebra is maximal. Thus the only irreducible closed subsets of $f^{-1}(y)$ are defined by maximal ideals. This obviously implies that $f^{-1}(y)$ is a finite set.

Theorem. *Let X be a projective (resp. affine) irreducible algebraic k-set. Then there exists a finite regular map $f : X \to \mathbf{P}_k^n(K)$ (resp. $\mathbf{A}_k^n(K)$).*

Proof. Assume first that X is projective. Let X be a closed subset of some $\mathbf{P}_k^r)(K)$ for some r as a closed subset. If $X = \mathbf{P}_k^r(K)$, we take for f the identity map. Let $x \in \mathbf{P}_k^r(K) \setminus X$ and $p_x : X \to \mathbf{P}_k^{r-1}(K)$ 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 $p_x(X) = \mathbf{P}_k^{r-1}(K)$, 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) $X \to \mathbf{P}_k^n(K)$ for some n.

Assume that X is affine. Then, we replace X by an isomorphic set lying as a closed subset of $\mathbf{P}_k^r(K)_0$ of some $\mathbf{P}_k^r(K)$. Let $\bar{X}$ be the closure of X in $\mathbf{P}_k^r(K)$. Projecting from a point $x \in \mathbf{P}_k^r(K) \setminus (\bar{X} \cup \mathbf{P}_k^r(K)_0)$, we define a finite map $\bar{X} \to \mathbf{P}_k^{r-1}(K)$. Since one of the equations defining x can be taken to be $T_0 = 0$, the image of $\mathbf{P}_k^r(K)_0$ is contained in $\mathbf{P}_k^{r-1}(K)_0$. Thus the image of X is contained in $\mathbf{P}_k^{r-1}(K)_0 \cong \mathbf{A}_k^{r-1}(K)$. Continuing as in the projective case, we prove the theorem.

Corollary (Noether's Normalization Theorem). *Let A be a finitely generated algebra over a field k. Then A is isomorphic to an integral extension of the polynomial algebra $k[Z_1, \ldots, Z_n]$.*

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 $f : Y \to X$ are finite:
(a) $Y = V(Z_1^2 - Z_2^3)$ be the cuspidal cubic, $X = \mathbf{A}^1$, f is defined by the formula $x \to (x^3, x^2)$;
(b) $X = Y = \mathbf{A}^2, f$ 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.

Lecture 11. DIMENSION

In this lecture we define 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. $\dim \mathbf{A}_k^1(K) = 1$. 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.

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.

$$\dim \mathbf{A}_k^n(K) = n.$$

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 $X \to \mathbf{A}_k^n(K)$.

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 $\phi_2,\ldots,\phi_n \in \mathcal{O}(X)$ such that the map $X \to \mathbf{A}_k^n(K)$ defined by the formula $x \to (\phi(x),\phi_2(x),\ldots,\phi_n(x))$ is a regular finite map.*

Proof. Replacing X by an isomorphic set, we may assume that X is a closed subset of some $\mathbf{P}_k^m(K)_0, \phi = F(T_0,\ldots,T_m)/T_0^r$ 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 $\mathbf{P}_k^m(K)$. 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 r 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 $F_1 = L^r$. Then

$$\dim \bar{X} \cap V(T_0) \cap V(F_1) < \dim \bar{X} \cap V(T_0) < n = \dim \bar{X}.$$

Continuing in this way we find n homogeneous polynomials $F_1(T),\ldots,F_{n-1}(T)$ of degree r such that

$$\bar{X} \cap V(T_0) \cap V(F) \cap V(F_1) \cap \ldots \cap V(F_{n-1}) = \emptyset.$$

Let $f : \bar{X} \to \mathbf{P}_k^n(K)$ be the regular map given by the polynomials $(T_0^r, F, F_1, \ldots, F_{n-1})$. We claim that it is finite. Indeed, replacing $\bar{X}$ by its image $v_r(\bar{X})$ under the Veronese map $v_r : \mathbf{P}_k^m(K) \to \mathbf{P}_k^N(k)$, we see that f is equal to the restriction of the linear projection map

$$pr_E : v_r(\bar{X}) \to \mathbf{P}_k^n(K)$$

where E is the linear subspace defined by the linear forms in $N+1$ unknowns corresponding to the homogeneneous forms $T_0^r, F, F_1, \ldots, F_{n-1}$. We know that the linear projection map is finite. Obviously, $f(X) \subset \mathbf{P}_k^n(K)_0$, and the restriction map $f|X : X \to \mathbf{P}_k^n(K)_0 \cong \mathbf{A}_k^n(K)$, defined by the formula

$$x \to (\frac{F}{T_0^r}(x), \frac{F_1}{T_0^r}(x), \ldots, \frac{F_{n-1}}{T_0^r}(x)) = (\phi(x), \phi_1(x), \ldots, \phi_{n-1}(x))$$

is finite.

Proof of Krull's Hauptidealsatz:

Let $f : X \to A^n(K)$ be the finite map constructed in the previous lemma. It suffices to show that the restrictions $\bar{\phi}_i$ of the functions $\phi_i (i = 1, \ldots, n-1)$ 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 $F \in k[Z_1, \ldots, Z_{n-1}] \setminus \{0\}$ be such that

$$F(\phi_1, \ldots, \phi_{n-1}) \in I(Y).$$

Choosing a function $g \notin I(Y)$ vanishing on the remaining irreducible components of $V(\phi)$, we obtain that

$$V(F(\phi_1, \ldots, \phi_{n-1})g) \supset V(\phi).$$

By the Nullstellensatz, $\phi | (F(\phi_1, \ldots, \phi_{n-1})g)^N$ for some $N > 0$. Now, we can apply Lemma 3. Identifying $k[Z_1, \ldots, Z_{n-1}, Z_n]$ with the subring of $\mathcal{O}(X)$ by means of f^*, we see that $\phi = Z_n, F(\phi_1, \ldots, \phi_{n-1}) = F(Z_1, \ldots, Z_{n-1})$, and $Z_n | F(Z_1, \ldots, Z_{n-1})^N g^N$ in $\mathcal{O}(X)$. From Lemma 4 we deduce that $Z_n | g^{jN}$ 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.

$$\dim \mathbf{P}^n(k) = n.$$

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 $\mathbf{P}_k^n(K)$ 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 $U \subset \mathbf{P}^n(k)_i$ 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 $\mathbf{P}_k^n(K), F_1, \ldots, F_r \in k[T_0, \ldots, T_n]$ 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 $X = \mathbf{P}_k^n$ and use that an algebraic set is finite if and only if it is of dimension 0 (Proposition 2).

Example. Let $C = v_3(\mathbf{P}^1(K))$ be a twisted cubic in $\mathbf{P}^3(K)$. 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.

(i) Let $\phi : Y \to \mathbf{A}^n(K)$ be a finite map and $f' = \phi \circ f$. Clearly, for any $z \in \mathbf{A}^n(K), f'^{-1}(z)$ is a disjoint union of the fibres $f^{-1}(y)$ where $y \in \phi^{-1}(z)$. Thus we may assume that $Y = \mathbf{A}^n(K)$. Each point $y = (a_1, \ldots, a_n) \in \mathbf{A}^n(K)$ 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 $\phi : X - \to Y \times \mathbf{A}^r(K)$ 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 $K' = R(Y \times \mathbf{A}^r(K))$. Replacing $Y \times \mathbf{A}^r(K)$ 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 $p : Y \times \mathbf{A}^r(K) \to Y$ 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

$$F = F(y, Z_1, \ldots, Z_r) \in \mathcal{O}(Y)[Z_1, \ldots, Z_r] \in \mathcal{O}(Y \times \mathbf{A}^r(K)).$$

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 $z \in \mathbf{A}^r(K)$ 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:

$$\begin{tikzcd} \phi^{-1}(U) \arrow[rr, "\phi"] \arrow[dr, "f"'] & & U \arrow[dl, "p"] \\ & V & \end{tikzcd}$$

The fibres of p are open subsets of fibres of the projection $Y \times \mathbf{A}^r(K) \to \mathbf{A}^r(K)$ 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

$$\text{dim} f^{-1}(y) = \text{dim} p^{-1}(y) = r = m - n.$$

The theorem is proven.

Corollary. *Let X and Y be irreducible algebraic sets. Then*

$$\text{dim}X \times Y = \text{dim}X + \text{dim}Y.$$

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 $\mathbf{P}^n(K)$. For every irreducible component Z of $X \cap Y$*

$$\text{dim}Z \geq \text{dim}X + \text{dim}Y - n.$$

Proof. Replacing X and Y by its open affine subsets, we may assume that X and Y are closed subsets of $\mathbf{A}^n(K)$. Let $\Delta : \mathbf{A}^n(K) \to \mathbf{A}^n(K) \times \mathbf{A}^n(K)$ be the diagonal map. Then Δ maps $X \cap Y$

isomorphically onto $(X \times Y) \cap \Delta_{\mathbf{A}^n(K)}$, where $\Delta_{\mathbf{A}^n(K)}$ is the diagonal of $\mathbf{A}^n(K)$. However, $\Delta_{\mathbf{A}^n(K)}$ 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

$$\operatorname{codim}(X \cap Y, \mathbf{P}^n(K)) \leq \operatorname{codim}(X, \mathbf{P}^n(K)) + \operatorname{codim}(Y, \mathbf{P}^n(K)).$$

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 $\mathbf{P}^n(K)$ or $\mathbf{A}^n(K)$ 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 $\mathbf{P}^{nm-1}(K)$ 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

$$\operatorname{codim}(Y, X) = \max\{k : \exists \text{ a chain of closed irreducible subsets } Z = Z_0 \subset Z_1 \subset \ldots \subset Z_k\}.$$

Prove that $\dim Y + \operatorname{codim}(Y, X) = \dim X$. 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 $\mathbf{P}^n(k)$ 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 $v_r(\mathbf{P}^1(K)) \subset \mathbf{P}^n(K)$ 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.