Yuriy Drozd

Intriduction to Algebraic Geometry

Kaiserslautern 1998/99

CHAPTER 1

Affine Varieties

1.1. Ideals and varieties. Hilbert's Basis Theorem

Let $\mathbf{K}$ be an algebraically closed field. We denote by $\mathbb{A}^n_{\mathbf{K}}$ (or by $\mathbb{A}^n$ if $\mathbf{K}$ is fixed) the *n-dimensional affine space* over $\mathbf{K}$, i.e. the set of all n-tuples $a = (a_1, a_2, \dots, a_n)$ with entries from $\mathbf{K}$. A subset $X \subseteq \mathbb{A}^n_{\mathbf{K}}$ is called an *affine algebraic variety* if it coincides with the set of common zeros of a set of polynomials $S = \{ F_1, F_2, \dots, F_m \} \subseteq \mathbf{K}[x_1, \dots, x_n]$. We denote this set by $V(S)$ or $V(F_1, F_2, \dots, F_m)$. We often omit the word "algebraic" and simply say "affine variety," especially as we almost never deal with other sorts of varieties. If $\mathbf{F}$ is a subfield of $\mathbf{K}$, one denotes by $X(\mathbf{F})$ the set of all points of the variety X whose coordinates belong to $\mathbf{F}$.

If S consists of a unique polynomial $F \neq 0$, the variety $V(S) = V(F)$ is called a *hypersurface* in $\mathbb{A}^n$ (a *plane curve* if $n = 2$; a *space surface* if $n = 3$).

EXERCISES 1.1.1. (1) Prove that the following subsets in $\mathbb{A}^n$ are affine algebraic varieties:
   (a) $\mathbb{A}^n$;
   (b) $\emptyset$;
   (c) $\{ a \}$ for every point $a \in \mathbb{A}^n$.
   (d) $\left\{ (t^k, t^l) \mid t \in \mathbf{K} \right\} \subset \mathbb{A}^2$, where k, l are fixed integers.
(2) Suppose that $F = F_1^{k_1} \dots F_s^{k_s}$, where F_i are irreducible polynomials. Put $X = V(F)$, $X_i = V(F_i)$. Show that $X = \bigcup_{i=1}^s X_i$.
(3) Let $\mathbf{K} = \mathbb{C}$ be the field of complex numbers, $\mathbb{R}$ be the field of real numbers. Outline the sets of points $X(\mathbb{R})$ for the plane curves $X = V(F)$, where F are the following polynomials:
   (a) $x^2 - y^2$;
   (b) $y^2 - x^3$ ("cuspidal cubic");
   (c) $y^2 - x^3 - x^2$; ("nodal cubic");
   (d) $y^2 - x^3 - x$ ("smooth cubic").
   (We write, as usually, (x, y) instead of (x_1, x_2), just as in the following exercise we write (x, y, z) instead of (x_1, x_2, x_3).)
(4) Outline the sets of points $X(\mathbb{R})$ for the space surfaces $X = V(F)$, where F are the following polynomials:
   (a) $x^2 - yz$;
   (b) xyz;

(c) $x^2 - z^3$;
(d) $x^2 + y^2 - z^3$.

We often write $\mathbf{x}^{\mathbf{m}}$, where $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{m} = (m_1, m_2, \dots, m_n)$, for the product $x_1^{m_1} \dots x_n^{m_n}$. In particular, a polynomial from $\mathbf{K}[\mathbf{x}]$ is written as a finite sum

$$\sum_{\mathbf{m}} \alpha_{\mathbf{m}} \mathbf{x}^{\mathbf{m}}, \quad \text{where } \mathbf{m} \in \mathbb{N}^n,\ \alpha_{\mathbf{m}} \in \mathbf{K}.$$

A set of polynomials S defines an ideal $\langle S \rangle = \langle F_1, F_2, \dots, F_m \rangle \subseteq \mathbf{K}[x_1, \dots, x_n]$ consisting of all "formal consequences" of these polynomials, i.e., of all linear combinations $\sum_{i=1}^m H_i F_i$, where H_i are some polynomials. Certainly, if $G \in \langle S \rangle$ and $a \in V(S)$, then also $G(a) = 0$. Hence, if S' is another set of polynomials such that $\langle S' \rangle = \langle S \rangle$, then $V(S) = V(S')$. That is, indeed, an affine variety is farther defined by an ideal of the polynomial ring.

In principle, a question arises, whether every such ideal defines an affine variety. Equivalently, the question is whether each ideal in the ring of polynomial possesses a finite set of generators. It is really so as the following theorem shows.

Theorem 1.1.2 (Hilbert's Basis Theorem). *Suppose that each ideal of a ring $\mathbf{A}$ possesses a finite set of generators. Then the same is true for the polynomial ring $\mathbf{A}[x_1, \dots, x_n]$ for every n.*

A ring $\mathbf{A}$ such that every ideal in $\mathbf{A}$ has a finite set of generators is called *noetherian.* Hence, Hilbert's Basis Theorem claims that a polynomial ring over any noetherian ring is again noetherian. As every ideal of a field $\mathbf{K}$ either is 0 or coincides with $\mathbf{K}$, it is always finitely generated (by the empty set in the former and by 1 in the latter case). Therefore, all polynomial rings with coefficients from a field are noetherian.

Proof. It is clear that we only have to prove the theorem for $n = 1$ (then a simple inductive argument works). Let $\mathbf{B} = \mathbf{A}[x]$, where the ring $\mathbf{A}$ is noetherian, and let I be an ideal of $\mathbf{B}$. Denote by I_d the set consisting of the leading coefficients of all polynomials of degree d belonging to I and of the zero element of $\mathbf{A}$. Obviously, I_d is an ideal in $\mathbf{A}$. Moreover, $I_d \subseteq I_{d+1}$: if a is the leading coefficient of a polynomial F, then it is also the leading coefficient of xF. Hence, the union $I_\infty = \bigcup_d I_d$ is again an ideal in $\mathbf{A}$ (check it!). As $\mathbf{A}$ is noetherian, I_∞ possesses a finite set of generators $T = \{ a_1, a_2, \dots, a_m \}$. Denote by F_k a polynomial from I with the leading coefficient a_k, $d_k = \deg F_k$ and by D the maximum of all d_k. Each ideal I_d for $d < D$ is also finitely generated. Let $T_d = \{ b_{id} \}$ be a set of generators for I_d and let G_{id} be a polynomial of degree d with the leading coefficient b_{id}. We claim that the (finite) set $S = \{ F_1, F_2, \dots, F_m \} \cup \{ G_{id} \mid d < D \}$ is a set of generators for I.

Namely, we will prove that every polynomial $F \in I$ belongs to $\langle S \rangle$ using induction on $d = \deg F$. If $d = 0$, then $F \in I_0$ (as it coincides with its own leading coefficient). Hence, $F \in \langle T_0 \rangle$, so $F \in \langle S \rangle$. Suppose that the claim is valid for all polynomials of degrees less than d and let $F \in I$ be any polynomial of degree d. Consider its leading coefficient a. If $d < D$, $a \in I_d$, therefore $a = \sum_i c_i b_{id}$ for some $c_i \in \mathbf{A}$. Then the polynomial $F' = \sum_i c_i G_{id}$ belongs to $\langle S \rangle$, $\deg F' = d$ and the leading coefficient of F' is also a. Thus, $\deg(F - F') < d$. Certainly, $F - F' \in I$, hence, $F - F' \in \langle S \rangle$ and $F = F' + (F - F')$ is also in $\langle S \rangle$.

Suppose now that $d \geq D$. As $a \in I_\infty$, we have that $a = \sum_k c_k a_k$ for some c_k. Put $F' = \sum_k c_k x^{d-d_k} F_k$. Again $F' \in \langle S \rangle$ and has the same degree and the same leading term as F. Therefore, just as above, $F - F'$ and thus F belong to $\langle S \rangle$ too. $\square$

This result enable us to define the affine algebraic variety $V(I)$ for every ideal $I \subseteq \mathbf{K}[\, x_1, \dots, x_n \,]$ as $V(S)$ for some (hence, any) (finite) system of generators of I.

Exercises 1.1.3.

(1) Prove that if $X_i \subseteq \mathbb{A}^n$ ($i \in S$) are affine varieties, then also $\bigcap_{i \in S} X_i$ is an affine variety. If S is finite, then also $\bigcup_{i \in S} X_i$ is an affine variety. Hence, the set of affine varieties can be considered as that of closed subsets of some topology on $\mathbb{A}^n$. This topology is called the *Zariski topology*.

Hint: Prove that if $X_i = V(I_i)$, then $\bigcap_i X_i = V(\sum_i I_i)$; if the set S is finite, then $\bigcup_i V_i = V(\prod_i I_i)$.

(2) Find all closed sets in the Zariski topology on the affine line $\mathbb{A}^1$.

(3) Show that if $C \subset \mathbb{A}^2$ is an infinite Zariski closed set, then it contains a plane curve.

Hint: Use the resultants.

(4) Let $\mathbf{F}$ be an infinite subfield in $\mathbf{K}$. Prove that $\mathbb{A}^n(\mathbf{F})$ is dense in $\mathbb{A}^n_{\mathbf{K}}$ in the Zariski topology.

(5) Let $\mathbf{F}$ be a finite subfield of $\mathbf{K}$ consisting of q elements. Find all polynomials $F \in \mathbf{K}[\,\mathbf{x}\,]$ such that $F(\mathbf{a}) = 0$ for all $\mathbf{a} \in \mathbb{A}^n(\mathbf{F})$.

Exercises 1.1.3 shows that the Zariski topology is a rather unusual one; in any case, it is non-Hausdorff if X is infinite. Nevertheless, it is useful for the purposes of algebraic geometry and in what follows, we always consider an affine variety $X \subseteq \mathbb{A}^n$ as a topological space with its Zariski topology, i.e., the topology on X induced by the Zariski topology of $\mathbb{A}^n$.

Remark. If $\mathbf{K} = \mathbb{C}$ is the field of complex numbers, the affine space and thus every affine variety can also be considered as topological space with the "usual" (Euclidean) topology. Though it is very important and widely used in complex algebraic geometry, we will only mention it in some exercises.

1.2. Regular functions and regular mappings

Let $X = V(S)$ be an affine variety. A function $f : X \to \mathbf{K}$ is said to be *regular* if it coincides with the restriction on X of some polynomial function, i.e., a function $\mathbb{A}^n \to \mathbf{K}$ mapping a point a to $F(a)$, where $F \in \mathbf{K}[x_1, \dots, x_n]$. Obviously, if f and g are two polynomial functions on X, their (pointwise) sum and product are also polynomial functions. Thus, all regular functions form a $\mathbf{K}$-algebra $\mathbf{K}[X]$ called the algebra of regular functions or the *coordinate algebra* of the affine variety X. As the field $\mathbf{K}$ is infinite, a polynomial F is completely defined by the corresponding polynomial function. That is why we do not distinguish them and often speak about "the restriction of a polynomial," "the value of a polynomial," etc.

Certainly, the mapping $\mathbf{K}[x_1, \dots, x_n] \to \mathbf{K}[X]$, putting a polynomial F to the function $a \mapsto F(a)$, is a homomorphism of algebras and even an epimorphism. Therefore, $\mathbf{K}[X] \simeq \mathbf{K}[x_1, \dots, x_n]/I(X)$, where $I(X)$ is the ideal consisting of all polynomials F such that $F(a) = 0$ for every point $a \in X$. This ideal is called the *defining ideal* of the affine variety X.

Proposition 1.2.1. (1) *For every point $a \in X$ the "evaluation mapping" $f \mapsto f(a)$ is a homomorphism of $\mathbf{K}$-algebras $v_a : \mathbf{K}[X] \to \mathbf{K}$.*

(2) *Conversely, given any homomorphism of $\mathbf{K}$-algebras $\alpha : \mathbf{K}[X] \to \mathbf{K}$, there is a unique point $a \in X$ such that $\alpha(f) = f(a)$ for each $f \in \mathbf{K}[X]$.*

Proof. The first claim is obvious. Consider any homomorphism $\alpha : \mathbf{K}[X] \to \mathbf{K}$. Denote by ξ_i the restriction on X of the polynomial x_i (the "i-th coordinate function"). Obviously, the functions ξ_i ($i = 1, \dots, n$) generate $\mathbf{K}[X]$ as $\mathbf{K}$-algebra. Put $a_i = \alpha(\xi_i)$ and $a = (a_1, a_2, \dots, a_n)$. If F is any polynomial from $I(X)$, then $F(a) = \alpha(F(\xi_1, \xi_2, \dots, \xi_n))$ as α is a homomorphism of algebras. But under the identification of $\mathbf{K}[X]$ with $\mathbf{K}[x_1, \dots, x_n]/I(X)$, the latter value coincides with the class of $F(x_1, x_2, \dots, x_n)$, i.e. equals 0. Therefore, $a \in X$. Moreover, $\xi_i(a) = \alpha(\xi_i)$ by definition, whence $f(a) = \alpha(f)$ as ξ_i generate the algebra $\mathbf{K}[X]$. If b is another point such that $\alpha(f) = f(b)$ for all regular functions f, then, in particular, $\xi_i(b) = \alpha(\xi_i) = a_i$, i.e. all coordinates of b coincide with those of a, hence, $b = a$. $\square$

Let Y be another affine variety and $f : Y \to X$ a mapping. If $a \in Y$, then $f(a)$ is a point of $\mathbb{A}^n$, hence, its coordinates $f_1(a), \dots, f_n(a)$ are defined. In other words, f defines n "coordinate mappings" $f_i : Y \to \mathbf{K}$. The mapping f is said to be *regular* or a *morphism of affine varieties* if all these coordinate mappings are regular functions.

It is obvious that if $f : Y \to X$ and $g : Z \to Y$ are regular mappings of affine varieties, their composition $f \circ g : Z \to X$ is also a regular mapping. As usually, a regular mapping f having a regular inverse f^{-1} is called an *isomorphism* of affine varieties. If an isomorphism $f : X \xrightarrow{\sim} Y$ exists, the varieties X and Y are called *isomorphic* and we write: $X \simeq Y$.

PROPOSITION 1.2.2. (1) *A mapping $f : Y \to X$ is regular if and only if the function $\varphi \circ f : Y \to \mathbf{K}$ is regular for each regular function $\varphi : X \to \mathbf{K}$. Moreover, the mapping $f^* : \mathbf{K}[X] \to \mathbf{K}[Y]$ such that $f^*(\varphi) = \varphi \circ f$ is a homomorphism of $\mathbf{K}$-algebras.*

(2) *Conversely, each homomorphism of $\mathbf{K}$-algebras $\mathbf{K}[X] \to \mathbf{K}[Y]$ is of the form f^* for a unique regular mapping $f : Y \to X$.*

PROOF. If $f(a) = (f_1(a), \dots, f_n(a))$, where f_i is the restriction on Y of some polynomial F_i and φ is the restriction on X of a polynomial G then $\varphi \circ f$ is the restriction on Y of the polynomial $G(F_1(a), \dots, F_n(a))$, i.e., is a regular function. Conversely, suppose that $\varphi \circ f$ is a regular function for each $\varphi \in \mathbf{K}[X]$. Put $\varphi = x_i$, the i-th coordinate function on $\mathbb{A}^n$. Then $\varphi \circ f(a)$ is the i-th coordinate of the point $f(a)$. Hence, all these coordinates are regular functions and the mapping f is regular. It is quite obvious that $(\varphi + \psi) \circ f = \varphi \circ f + \psi \circ f$ and $(\varphi\psi) \circ f = (\varphi \circ f)(\psi \circ f)$, so f^* is indeed a homomorphism of $\mathbf{K}$-algebras.

Let now $\gamma : \mathbf{K}[X] \to \mathbf{K}[Y]$ be any homomorphism of $\mathbf{K}$-algebras and $a \in Y$. Then the composition $v_a \circ \gamma$, where v_a is the evaluation mapping, is a homomorphism $\mathbf{K}[X] \to \mathbf{K}$, thus defines a unique point $b \in X$ such that $v_a \circ \gamma = v_b$. Hence, there is a unique mapping $f : Y \to X$ such that $v_a \circ \gamma = v_{f(a)}$ for every $a \in Y$. In particular, if $f(a) = (f_1(a), \dots, f_n(a))$, then $f_i(a) = v_{f(a)}(\xi_i) = v_a(\gamma(\xi_i)) = \gamma(\xi_i)(a)$, where ξ_i are the coordinate functions on X. As it is true for every point $a \in Y$, we have that $f_i = \gamma(\xi_i)$ are regular functions on Y, so f is a regular mapping and $\gamma(\xi_i) = f^*(\xi_i)$. As ξ_i generate $\mathbf{K}[X]$, $\gamma = f^*$. The uniqueness of f is evident. □

COROLLARY 1.2.3. *Affine algebraic varieties X and Y are isomorphic if and only if the algebras $\mathbf{K}[X]$ and $\mathbf{K}[Y]$ are isomorph. Moreover, a morphism $f : X \to Y$ is an isomorphism if and only if so is the homomorphism f^*.*

EXERCISES 1.2.4. (1) For every regular function f on an affine variety X, put $D(f) = \{\, x \in X \mid f(x) \neq 0 \,\}$. The sets $D(f)$ are called *principal open sets* (of the variety X). Prove that the principal open sets form a base of the Zariski topology, i.e., every open set is a union of principal open sets.

(2) Prove that every regular mapping is continuous (in the Zariski topology).

(3) An *affine transformation* of $\mathbb{A}^n$ is a mapping $\mathbb{A}^n \to \mathbb{A}^n$ of the form $a \mapsto Aa + b$, where A is an invertible $n \times n$ matrix and b is a fixed vector. Show that such a transformation is an automorphism of $\mathbb{A}^n$ (i.e., an isomorphism to itself).
(4) Show that the only automorphisms of the affine line $\mathbb{A}^1$ are the affine transformations. Is it still true for $n > 1$?
(5) Consider the plane curves given by the following equations:
  (a) $x^2 - y$;
  (b) xy;
  (c) $xy - 1$;
  (d) $x^2 - y^3$.
  Prove that they are pairwise non-isomorph. Which of them is isomorphic to the affine line?
(6) Let X be the plane curve defined by the equation $x^2 - y^3$, $f : \mathbb{A}^1 \to X$ be the regular mapping such that $f(\lambda) = (\lambda^3, \lambda^2)$ for each $\lambda \in \mathbf{K}$. Prove that f is bijective, but its inverse is not regular.
(7) Suppose that $\operatorname{char} \mathbf{K} = p$, a positive prime number. Show that the mapping $\Phi : \mathbb{A}^n \to \mathbb{A}^n$ such that $\Phi(a_1, a_2, \dots, a_n) = (a_1^p, a_2^p, \dots, a_n^p)$ is regular and bijective, but its inverse is not regular. This mapping is called the *Frobenius mapping*.
(8) In the situation of the preceding exercise, suppose that $X = X(S)$ for some set $S \subseteq \mathbf{F}[\mathbf{x}]$, where $\mathbf{F}$ is the prime subfield of $\mathbf{K}$. Show that $\Phi(X) = X$, where Φ is the Frobenius mapping.

1.3. Hilbert's Nullstellensatz

Above we have defined the correspondence between the ideals I of the polynomial ring $\mathbf{K}[x_1, \dots, x_n]$ and the affine varieties $X \subseteq \mathbb{A}^n_{\mathbf{K}}$: to every ideal I corresponds the variety $V(I)$ of its zeros and to every variety X corresponds the ideal $I(X)$ of polynomials vanishing on X. It is clear that $V(I(X)) = X$: if a point a does not belong to X, then, by definition, there is a polynomial F vanishing on X (hence, lying in $I(X)$) but not vanishing at a; thus, $a \notin V(I(X))$. On the other hand, simple examples show that $I(V(I)) \neq I$ can happen. For instance, if $I = \langle F^2 \rangle$ for some polynomial F, then $F \in I(V(I))$ but $F \notin I$.

Exercise 1.3.1. Suppose that $I = \langle F \rangle$. Find $I(V(I))$ using the decomposition of F into a product of irreducible polynomials (remind that such a decomposition is unique up to permutation and constant multipliers).

The last example can be easily generalized. Namely, denote by $\sqrt{I}$ the set of all polynomials F such that $F^k \in I$ for some integer k. This set is called the *root* of the ideal I.

Exercise 1.3.2. Check that $\sqrt{I}$ is again an ideal.

Obviously, $\sqrt{I} \subseteq I(V(I))$. A remarkable theorem by Hilbert shows that these two ideals indeed coincide.

THEOREM 1.3.3 (Hilbert's Nullstellensatz). *If the field* $\mathbf{K}$ *is algebraically closed, then* $I(V(I)) = \sqrt{I}$ *for every ideal* $I \subseteq \mathbf{K}[\,x_1, \dots, x_n\,]$.

An ideal I of a ring $\mathbf{A}$ is called a *radical ideal* if $I = \sqrt{I}$. In particular, Hilbert Nullstellensatz claims that an ideal $I \subseteq \mathbf{K}[\,\mathbf{x}\,]$ is the defining ideal of an affine variety if and only if it is a radical ideal.

First note the following special case of this theorem.

COROLLARY 1.3.4. $V(I) = \emptyset$ *if and only if* $I = \mathbf{K}[\,x_1, \dots, x_n\,]$.

Indeed, $V(I) = \emptyset$ means that all polynomials vanish on $V(I)$. In particular, $1 \in I(V(I))$. But it means that $1 \in I$ as $1^k = 1$. Then certainly I contains all polynomials. The converse is evident.

The following trick shows that Hilbert's Nullstellensatz is indeed a consequence of this special case.

PROPOSITION 1.3.5 (Rabinovich's Lemma). *If Corollary 1.3.4 is valid, then Theorem 1.3.3 is valid too.*

PROOF. Let $F \in I(V(I))$. Consider the ideal $J \subseteq \mathbf{K}[\,x_1, \dots, x_{n+1}\,]$ generated by all polynomials from I and by $x_{n+1}F - 1$. Obviously, $V(J) = \emptyset$. Hence, $1 \in J$, i.e.

$$1 = \sum_{i=1}^{m} H_i F_i + H_{m+1}(x_{n+1}F - 1) \tag{1.3.1}$$

for some polynomials $H_i \in \mathbf{K}[\,x_1, \dots, x_{n+1}\,]$ and some polynomials $F_i \in I$. The equality (1.3.1) is a formal equality of polynomials, so we can replace in it the variables x_i by any values taken from any $\mathbf{K}$-algebra. Replacing x_{n+1} by $1/F$, we get:

$$1 = \sum_{i=1}^{m} H_i(x_1, \dots, x_n, 1/F) F_i(x_1, \dots, x_n)\,.$$

Multiplying this equality by the common denominator, which is F^k for some integer k, we get:

$$F^k = \sum_{i=1}^{m} G_i F_i \in I\,,$$

where G_i stands for $F^k H_i(x_1, \dots, x_n, 1/F)$. □

We are going now to prove Corollary 1.3.4 (which is also often called "Nullstellensatz"). Moreover, we shall give an equivalent formulation of it, which will be valid for *any* field $\mathbf{K}$, not only for algebraically closed one. (And in the remainder of this section, as well as in the next one, we do not suppose the field $\mathbf{K}$ being algebraically closed.)

First make the following simple remarks.

PROPOSITION 1.3.6. *Let* $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ *be an increasing chain of ideals of a noetherian ring (e.g. of* $\mathbf{K}[x_1, \dots, x_n]$*). Then it stabilizes, i.e., there is a number* r *such that* $I_r = I_s$ *for all* $s > r$.

PROOF. As we have remarked before, the union $I = \bigcup_i I_i$ is again an ideal. As the ring is noetherian, $I = \langle a_1, \dots, a_m \rangle$ for some finite set. Each of a_k belongs to some ideal I_{i_k}. Then we can put $r = \max_k i_k$: obviously, $I_r = I = I_s$ for all $s > r$. $\square$

COROLLARY 1.3.7. *For every proper ideal* $I \subset \mathbf{A}$ *of a noetherian ring* $\mathbf{A}$*, there is a maximal ideal containing* I.

Remind that a *maximal ideal* is a proper ideal $J \subset \mathbf{A}$ such that there are no proper ideals J' with $J \subset J'$.

PROOF. If I is not maximal, there is a proper ideal $I_1 \supset I$. If I_1 is not maximal, there is a proper ideal $I_2 \supset I_1$, etc. Hence, if there is no maximal ideal containing I, we get an increasing chain of ideals which never stabilizes. It contradicts Proposition 1.3.6. $\square$

REMARK. Indeed, the last corollary is valid for *any* ring, no matter whether it is noetherian or not, but its proof requires some “transfinite” set-theoretical tools like Zorn Lemma or something equivalent. We will never use it for non-noetherian rings.

PROPOSITION 1.3.8. *If* 0 *is the unique proper ideal of a ring* $\mathbf{A}$*, then* $\mathbf{A}$ *is a field.*

PROOF. Let $a \neq 0$ be an element of $\mathbf{A}$, $I = \langle a \rangle$. As $I \neq 0$, we have that $I = \mathbf{A}$. In particular, $1 \in I$, i.e., there is an element $b \in \mathbf{A}$ such that $ab = 1$; so a is invertible. $\square$

COROLLARY 1.3.9. *A proper ideal* $I \subset \mathbf{A}$ *is maximal if and only if* $\mathbf{A}/I$ *is a field.*

PROOF. I is maximal if and only if there are no proper ideals in $\mathbf{A}/I$ except of 0. $\square$

Now we are ready to reformulate Corollary 1.3.4 in the following way:

THEOREM 1.3.10. *If* I *is a maximal ideal of the polynomial ring* $\mathbf{K}[\mathbf{x}]$*, where* $\mathbf{K}$ *is any field, then the field* $\mathbf{K}[\mathbf{x}]/I$ *is an algebraic extension of* $\mathbf{K}$.

Show that this theorem really implies Corollary 1.3.4. Indeed, let I be a proper ideal from $\mathbf{K}[\mathbf{x}]$, where $\mathbf{K}$ is algebraically closed, and J be a maximal ideal containing I. As $\mathbf{K}$ has no proper algebraic extensions, then $\mathbf{K}[\mathbf{x}]/J = \mathbf{K}$. Hence, we obtain a homomorphism $\mathbf{K}[\mathbf{x}] \to \mathbf{K}$ with the kernel $J \supseteq I$ or, the same, a homomorphism $\mathbf{K}[\mathbf{x}]/I \to \mathbf{K}$. Then Proposition 1.2.1 shows that $V(I) \neq \emptyset$.

We shall reformulate Theorem 1.3.10 once more. Note that the factor-algebra $\mathbf{K}[\mathbf{x}]/I$ for every ideal I is a finitely generated $\mathbf{K}$-algebra. In view of Corollary 1.3.9, we see that Theorem 1.3.10 is equivalent to the following one:

THEOREM 1.3.11. *If a finitely generated* $\mathbf{K}$*-algebra* $\mathbf{A}$ *is a field, it is an algebraic extension of* $\mathbf{K}$*.*

The last theorem will be proved in the next section using rather powerful and important tools called "integral dependence" and "Noether normalization."

1.4. Integral dependence

In this section we do not suppose the field $\mathbf{K}$ *to be algebraically closed.*

DEFINITION 1.4.1. Let $\mathbf{A} \subseteq \mathbf{B}$ be an extension of rings.

(1) An element $b \in \mathbf{B}$ is called *integral over* $\mathbf{A}$ if $F(b) = 0$ for some polynomial $F \in \mathbf{A}[x]$ with the leading coefficient 1.
(2) The ring $\mathbf{B}$ is called an *integral extension* of $\mathbf{A}$ if every element of $\mathbf{B}$ is integral over $\mathbf{A}$,

If $\mathbf{A}$ is a field, "integral" coincides with "algebraic," as we can always divide any non-zero polynomial by its leading coefficient. Indeed, we shall see that many features of integral extensions of rings are similar to those of algebraic extensions of fields. Before studying this notion more detailed, we show how to use it for the proof of Hilbert's Nullstellensatz. First make the following simple observation.

PROPOSITION 1.4.2. *Suppose that an integral extension* $\mathbf{B}$ *of a ring* $\mathbf{A}$ *is a field. Then* $\mathbf{A}$ *is also a field.*

PROOF. Let a be a non-zero element of $\mathbf{A}$, $b = a^{-1}$ its inverse in the field $\mathbf{B}$. As the latter is integral over $\mathbf{A}$, there are such elements $c_i \in \mathbf{A}$ that $b^m + c_1 b^{m-1} + \dots + c_m = 0$. Multiplying this equality by a^{m-1}, we get: $b = -c_1 - \dots - c_m a^{m-1} \in \mathbf{A}$, so a is invertible in $\mathbf{A}$. □

The following result plays the decisive role in the proof of Hilbert's Nullstellensatz, as well as in the dimension theory of algebraic varieties.

THEOREM 1.4.3 (Noether's Normalization Lemma). *If* $\mathbf{B}$ *is a finitely generated* $\mathbf{K}$*-algebra, then there is a subalgebra* $\mathbf{A} \subseteq \mathbf{B}$ *isomorphic to a polynomial algebra* $\mathbf{K}[x_1, \dots, x_d]$ *and such that* $\mathbf{B}$ *is an integral extension of* $\mathbf{A}$*.*

The last theorem immediately implies Nullstellensatz. Indeed, suppose that $\mathbf{B}$ is a field. Then $\mathbf{A}$ is also a field by Proposition 1.4.2, hence, $\mathbf{A} = \mathbf{K}$ and $\mathbf{B}$ is an algebraic extension of $\mathbf{K}$.

To prove Noether's Normalization Lemma (thus, Hilbert's Nullstellensatz), we need some elementary properties of integral extensions, as well as of modules over noetherian rings. Remind the following definition.

Definition 1.4.4. A *module* over a ring $\mathbf{A}$ (or an $\mathbf{A}$-*module*) is an abelian group M together with a "multiplication law" $\mathbf{A} \times M \to M$, $(a, v) \mapsto av$, such that the following conditions hold:

(1) $a(bv) = (ab)v$ for all $a, b \in \mathbf{A}$ and $v \in M$.
(2) $1v = v$ for every $v \in M$.
(3) $(a + b)v = av + bv$ for all $a, b \in \mathbf{A}$ and $v \in M$.
(4) $a(u + v) = au + av$ for all $a \in \mathbf{A}$ and $u, v \in M$.

Note that if $\mathbf{A}$ is a field, this notion coincides with that of the vector space over $\mathbf{A}$. Certainly, any extension $\mathbf{B}$ of a ring $\mathbf{A}$ can be considered as an $\mathbf{A}$-module, as well as any ideal of the ring $\mathbf{A}$. One can also define the notions of *submodule, factor-module*, etc., in the usual way and we shall use them freely, as well as their elementary properties, which are the same as for abelian groups or vector spaces. In particular, an ideal of $\mathbf{A}$ is just a submodule of $\mathbf{A}$ considered as a module over itself.

Definitions 1.4.5. Let M be a module over a ring $\mathbf{A}$.

(1) A subset $S \subseteq M$ is called a *generating set* of the module M if for every $v \in M$ there are elements $a_i \in \mathbf{A}$ and $u_i \in S$ such that $v = \sum_i a_i u_i$.
(2) A module is called *finitely generated* if it has a finite generating set.
(3) For every subset $S \subseteq M$ denote by $\langle S \rangle$, or $\langle S \rangle_{\mathbf{A}}$ if it is necessary to precise the ring, the *submodule of M generated by S*. i.e., the set of all linear combinations $\sum_i a_i u_i$, where a_i run through $\mathbf{A}$ and u_i run through S.
(4) A module M is called *noetherian* if every submodule $N \subseteq M$ is finitely generated, i.e., has a finite generating set.

In particular, the ring $\mathbf{A}$ is noetherian if and only if it is noetherian when considered as a module over itself.

Proposition 1.4.6. (1) *Every submodule and factor-module of a noetherian module is noetherian.*
(2) *If a submodule N of a module M and the factor-module M/N are both noetherian, then M is also noetherian.*
(3) *If the ring $\mathbf{A}$ is noetherian, then every finitely generated $\mathbf{A}$-module is noetherian too.*

Proof. Let M be an $\mathbf{A}$-module, N its submodule and $L = M/N$.

1. It is evident that if M is noetherian, N is noetherian as well. Consider any submodule $L' \subseteq L$. It is of the form N'/N for some submodule N' such that $N' \supseteq N$. As M is noetherian, N' has a finite generating set $\{u_1, u_2, \dots, u_r\}$. Then the set of the classes $\{u_1 + N, \dots, u_r + N\}$ is generating for L'. Hence, L is noetherian.

2. Suppose that both N and L are noetherian. Let M' be any submodule of M. Then $M' \cap N$ has a finite generating set $\{u_1, u_2, \dots, u_r\}$. The factor-module $M'/(M' \cap N)$, isomorphic to the submodule $(M' + N)/N$ of M/N, also has a finite generating set $\{w_1, w_2, \dots, w_t\}$. Let $w_i = v_i + (M' \cap N)$. We show that the set $\{v_1, v_2, \dots, v_t, u_1, u_2, \dots, u_r\}$ is generating for M'.

Indeed, consider any element $v \in M'$ and its class $w = v + (M' \cap N)$ in $M'/(M' \cap N)$. Then $w = \sum_i a_i w_i$ for some $a_i \in \mathbf{A}$. Put $v' = \sum_i a_i v_i$. The class of the element $v - v'$ in the factor-module $M'/(M' \cap N)$ is zero, i.e., $v - v' \in M' \cap N$. Therefore, $v - v' = \sum_j b_j u_j$ for some $b_j \in \mathbf{A}$, whence $v = \sum_i a_i v_i + \sum_j b_j u_j$.

3. Let now the ring $\mathbf{A}$ be noetherian. Consider any finite generating set $S = \{u_1, u_2, \dots, u_r\}$ of the module M. We prove that M is noetherian using the induction by r. If $r = 1$, the mapping $\varphi : \mathbf{A} \to M$ such that $\varphi(a) = au_1$ is an epimorphism, whence $M \simeq \mathbf{A}/\operatorname{Ker}\varphi$ is noetherian. Suppose that the claim is valid for the modules having $r - 1$ generators. Put $N = \langle u_1, u_2, \dots, u_{r-1} \rangle$. Then N is noetherian and $\{u_r + N\}$ is a generating set for M/N. Thus, M/N is also noetherian and M is noetherian as well. □

Now we use these facts to establish some basic properties of integral extensions. We also use the following notions.

Definitions 1.4.7. Let M be an $\mathbf{A}$-module.

(1) For any subset $S \subseteq M$, call the *annihilator* of S in $\mathbf{A}$ the set $\operatorname{Ann}_{\mathbf{A}}(S) = \{a \in \mathbf{A} \mid au = 0 \text{ for all } u \in S\}$.
(2) For any subset $T \subseteq \mathbf{A}$, call the *annihilator* of T in M the set $\operatorname{Ann}_M(T) = \{u \in M \mid au = 0 \text{ for all } a \in T\}$.
(3) The module M is called *faithful* if $\operatorname{Ann}_{\mathbf{A}}(M) = 0$.

Proposition 1.4.8. *Let $\mathbf{A} \subseteq \mathbf{B}$ be an extension of rings, $b \in \mathbf{B}$. The following conditions are equivalent:*

(1) *The element $b \in \mathbf{B}$ is integral over $\mathbf{A}$.*
(2) *The subring $\mathbf{A}[b]$ is finitely generated as $\mathbf{A}$-module.*
(3) *There is a finitely generated $\mathbf{A}$-submodule $M \subseteq \mathbf{B}$ such that $bM \subseteq M$ and $1 \in M$.*
(4) *There is a finitely generated $\mathbf{A}$-submodule $M \subseteq \mathbf{B}$ such that $bM \subseteq M$ and $\operatorname{Ann}_{\mathbf{B}}(M) = 0$.*

Proof. *1⇒2*: If $b^m + a_1 b^{m-1} + \dots + a_m = 0$, where $a_i \in \mathbf{A}$, then $\{1, b, \dots, b^{m-1}\}$ is a generating set of $\mathbf{A}[b]$ as of $\mathbf{A}$-module.

2⇒3: One can take $\mathbf{A}[b]$ for M.

3⇒4 is trivial.

4⇒1: Let $\{u_1, u_2, \dots, u_m\}$ be a generating set of M. Then $bu_j = \sum_i a_{ij}u_i$ for some $a_{ij} \in \mathbf{A}$ ($j = 1, \dots, m$). These equalities can be written in the matrix form as $(bI - A)\mathbf{u} = 0$, where $A = (a_{ij})$, I is the $m \times m$ identity matrix and $\mathbf{u}$ is the column $(u_1, u_2, \dots, u_m)^\top$. Multiplying the last equality by the *adjoint* matrix $(bI - A)$, one gets $\det(bI - A)\mathbf{u} = 0$ or $\det(bI - A)u_i = 0$ for all i. Then $\det(bI - A)M = 0$, whence $\det(bI - A) = 0$. But $\det(bI - A)$ is of the form $b^m + c_1b^{m-1} + \dots + c_m$ with $c_i \in \mathbf{A}$. Hence, b is integral over $\mathbf{A}$. □

COROLLARY 1.4.9. *Let $\mathbf{A} \subseteq \mathbf{B}$ be an extension of rings.*

(1) *The set of all elements from $\mathbf{B}$ which are integral over $\mathbf{A}$ is a subring of $\mathbf{B}$.*
 This subring is called the *integral closure* of $\mathbf{A}$ in $\mathbf{B}$.
(2) *If $\mathbf{B}$ is integral over $\mathbf{A}$, $\mathbf{C} \supseteq \mathbf{B}$ is an extension of $\mathbf{B}$ and an element $c \in \mathbf{C}$ is integral over $\mathbf{B}$, then c is integral over $\mathbf{A}$ as well. In particular, if $\mathbf{B}$ is integral over $\mathbf{A}$ and $\mathbf{C}$ is integral over $\mathbf{B}$, then $\mathbf{C}$ is also integral over $\mathbf{A}$.*

PROOF. *1.* Let $b, c \in \mathbf{B}$ be both integral over $\mathbf{A}$. Find finitely generated $\mathbf{A}$-submodules $M, N \subseteq \mathbf{B}$ such that $bM \subseteq M$, $cN \subseteq N$ and both M and N contain 1. Consider the set $MN = \{\sum_i u_iv_i \mid u_i \in M, v_i \in N\}$. One can easily check that it is also a finitely generated $\mathbf{A}$-submodule and $1 \in MN$. Moreover, both $bMN \subseteq MN$ and $cMN \subseteq MN$, whence both $(b + c)MN \subseteq MN$ and $(bc)MN \subseteq MN$. Hence, $b + c$ and bc are integral over $\mathbf{A}$.

2. Let $c^m + b_1c^{m-1} + \dots + b_m = 0$, where $b_i \in \mathbf{B}$. Just as above, one can find a finitely generated $\mathbf{A}$-submodule $M \subseteq \mathbf{B}$ such that $b_iM \subseteq M$ for all $i = 1, \dots, m$ and $1 \in M$. Put $N = \sum_{i=0}^{m-1} c^iM$. It is a finitely generated $\mathbf{A}$-submodule in $\mathbf{C}$ containing 1 and $cN \subseteq N$. Hence, c is integral over $\mathbf{A}$. □

To prove Noether's Normalization Lemma, we also need the following simple fact about polynomial algebras.

LEMMA 1.4.10. *Let $F \in \mathbf{K}[x_1, \dots, x_n]$ be a polynomial of positive degree. There is an automorphism φ of the polynomial algebra $\mathbf{K}[x_1, \dots, x_n]$ such that*

$$\varphi(F) = \lambda x_n^d + \sum_{i=1}^{d-1} G_i x_n^i, \tag{1.4.1}$$

where $G_i \in \mathbf{K}[x_1, \dots, x_{n-1}]$ and $\lambda \neq 0$ is an element of $\mathbf{K}$.

PROOF. Let k be the maximal integer such that x_i^k occurs in F for some i, $t = k + 1$. Consider the automorphism φ defined as follows:

$$\varphi(x_i) = x_i + x_n^{t^i} \text{ for } i < n\,;$$
$$\varphi(x_n) = x_n\,.$$

Then, for any $\mathbf{m} = (m_1, m_2, \dots, m_n)$, $\varphi(\mathbf{x}^{\mathbf{m}}) = x_n^{\nu(\mathbf{m})} + H$, where $\nu(\mathbf{m}) = m_n + m_1 t + m_2 t^2 + \cdots + m_{n-1} t^{n-1}$ and H only contains x_n in the degrees less than $\nu(\mathbf{m})$. If this monomial occurs in F, then all $m_i < t$. Therefore, the values $\nu(\mathbf{m})$ are different for different monomials occurring in F, thus, $\varphi(F)$ is of the form (1.4.1), where d is the maximal value of $\nu(\mathbf{m})$. □

PROOF OF NOETHER'S NORMALIZATION LEMMA. Let $\mathbf{B} = \mathbf{K}[\,\mathbf{b}\,]$ be a finitely generated $\mathbf{K}$-algebra, where $\mathbf{b} = (b_1, b_2, \dots, b_n)$. There are epimorphisms $f : \mathbf{K}[\,\mathbf{x}\,] \to \mathbf{B}$ (for instance one mapping x_i to b_i). Consider one of them. Then $\mathbf{B} \simeq \mathbf{K}[\,\mathbf{x}\,]/I$, where $I = \operatorname{Ker} f$. If $I = 0$, $\mathbf{B} \simeq \mathbf{K}[\,\mathbf{x}\,]$. Suppose that I contains a polynomial F of positive degree. By Lemma 1.4.10, there is an automorphism φ of $\mathbf{K}[\,\mathbf{x}\,]$ such that $\varphi(F)$ is of the form (1.4.1). Replacing f by $f \circ \varphi$, we may suppose that F itself is of this form. As the images $f(x_i)$ generate the $\mathbf{K}$-algebra $\mathbf{B}$, we may also suppose that $f(x_i) = b_i$. Hence, $\lambda b_n^d + g_1 b_n^{d-1} + \cdots + g_d = 0$, where $g_i = G_i\,(b_1, b_2, \dots, b_{n-1})$. As λ is invertible, the element b_n is integral over the subring $\mathbf{B}' = \mathbf{K}[\,b_1, \dots, b_{n-1}\,]$. Now a simple induction (using Lemma 1.4.9(2)) accomplishes the proof. □

EXERCISES 1.4.11. (1) Find an example of a finitely generated module containing a submodule which is not finitely generated.

Hint: Consider the polynomial ring in infinitely many variables.

(2) Suppose that the ring extension $\mathbf{B} \supseteq \mathbf{A}$ is *of finite type*, i.e. $\mathbf{B} = \mathbf{A}[\,b_1, \dots, b_n\,]$ for some $b_i \in \mathbf{B}$. Prove that if every b_i is integral over $\mathbf{A}$, then $\mathbf{B}$ is finitely generated as $\mathbf{A}$-module and, hence, is integral over $\mathbf{A}$.

(3) Prove that if the field $\mathbf{K}$ is infinite, the automorphism φ in Lemma 1.4.10 can be chosen *linear*, i.e., such that $\varphi(x_j) = \sum_i \alpha_{ij} x_i$, where $A = (\alpha_{ij})$ is an invertible $n \times n$ matrix over $\mathbf{K}$.

Hint: Find an n-tuple $\mathbf{a} \in \mathbb{A}^n_{\mathbf{K}}$ such that $F_d(\mathbf{a}) \neq 0$, where F_d is the sum of all terms of degree d from F, and an invertible matrix A such that $\mathbf{a}$ is its last column.

1.5. Geometry and algebra

Again we suppose $\mathbf{K}$ to be an algebraically closed field. First we establish some consequences of Hilbert Nullstellensatz.

Proposition 1.5.1. *A* $\mathbf{K}$*-algebra* $\mathbf{A}$ *is isomorphic to a coordinate algebra of an affine algebraic variety if and only if it is finitely generated and* reduced, *i.e., has no non-zero nilpotent elements.*
In what follows, finitely generated reduced $\mathbf{K}$-algebras are called *affine algebras* (over $\mathbf{K}$).

Proof. The "only if" claim is obvious from the definition. Suppose now $\mathbf{A} = \mathbf{K}[\,a_1, \dots, a_n\,]$ to be an affine algebra. Consider the homomorphism $\varphi : \mathbf{K}[\,\mathbf{x}\,] \to \mathbf{A}$ mapping F to $F\,(a_1, a_2, \dots, a_n)$. It is an epimorphism, hence, $\mathbf{A} \simeq \mathbf{K}[\,\mathbf{x}\,]/I$, where $I = \operatorname{Ker}\varphi$. Moreover, $\sqrt{I} = I$. Indeed, if $F \in \sqrt{I}$, then $\varphi(F^k) = (\varphi(F))^k = 0$ for some k, whence $\varphi(F) = 0$ as $\mathbf{A}$ is reduced, so $F \in I$. By Hilbert Nullstellensatz, then $I = I(X)$, where $X = V(I)$, and $\mathbf{A} \simeq \mathbf{K}[\,X\,]$. □

Let $X \subseteq \mathbb{A}^n$ be an affine variety, $\mathbf{A} = \mathbf{K}[\,\mathbf{x}\,]/I(X)$ be its coordinate algebra. We show that both the variety X and its Zariski topology are completely defined by the algebra $\mathbf{A}$. For every subset $Y \subseteq X$, put $I(Y) = \{\, a \in \mathbf{A} \mid a(y) = 0 \text{ for all } y \in Y \,\}$. Obviously, $I(Y)$ is a radical ideal in $\mathbf{A}$. If $Y = \{\, x \,\}$ consists of a single point, we write $\mathfrak{m}_x$ instead of $I(\{\, x \,\})$. Conversely, for every subset $S \subseteq \mathbf{A}$, put $V(S) = \{\, x \in X \mid a(x) = 0 \text{ for all } a \in S \,\}$. It is a closed set in the Zariski topology, i.e., is also an affine variety, namely, $V(S) = V(I \cup \tilde{S})$, where $\tilde{S}$ consists of (some) preimages in $\mathbf{K}[\,\mathbf{x}\,]$ of the functions $a \in S$. Certainly, if $X = \mathbb{A}^n$, we get the "old" definitions of Section 1.1. Moreover, we can generalize Hilbert Nullstellensatz to this situation as follows.

Corollary 1.5.2.
(1) *$V(I(Z)) = Z$ for every Zariski closed subset $Z \subseteq X$.*
(2) *$I(V(I)) = \sqrt{I}$ for every ideal $I \subseteq \mathbf{A}$; thus, if I is a radical ideal, then $I(V(I)) = I$.*

In particular, $V(I) = \emptyset$ if and only if $I = \mathbf{A}$.

Proof. Exercise. □

Thus, we get a 1-1 correspondence between Zariski closed subsets of X and radical ideals in $\mathbf{A}$. Moreover, it immediately follows from the definition that $\mathbf{K}[\,Z\,] = \mathbf{K}[\,X\,]/I(Z)$ for every closed $Z \subseteq X$.

Proposition 1.5.3.
(1) *For every point $x \in X$, the ideal $\mathfrak{m}_x$ is maximal.*
(2) *Conversely, for every maximal ideal $\mathfrak{m} \subset \mathbf{A}$ there is a unique point $x \in X$ such that $\mathfrak{m} = \mathfrak{m}_x$.*

Proof. *1*. Consider the evaluation homomorphism $v_x : \mathbf{A} \to \mathbf{K}$ ($v_x(a) = a(x)$). Obviously, it is an epimorphism and $\mathfrak{m}_x = \operatorname{Ker} v_x$. Hence, $\mathbf{A}/\mathfrak{m}_x \simeq \mathbf{K}$ is a field and $\mathfrak{m}_x$ is a maximal ideal.

2. As $\mathfrak{m} \neq \mathbf{A}$, there is a point $x \in X$ such that $a(x) = 0$ for all $a \in \mathfrak{m}$. Hence, $\mathfrak{m} \subseteq \mathfrak{m}_x$ and $\mathfrak{m} = \mathfrak{m}_x$ as it is a maximal ideal. The uniqueness of x is evident. □

Thus, we can (and often will) identify an affine variety X with the set $\operatorname{Max}\mathbf{A}$ of maximal ideals of its coordinate algebra $\mathbf{A}$. The latter is called the *maximal spectrum* of the ring $\mathbf{A}$. Moreover, the Zariski topology on X can be obtained in a "purely algebraic" way as follows:

PROPOSITION 1.5.4. *Let $Z \subseteq X$ be a Zariski closed subset, $I = I(Z)$. Then $x \in Z$ if and only if $\mathfrak{m}_x \supseteq I$.*

In other words, Zariski closed subsets of X correspond to the subsets of $\operatorname{Max}\mathbf{A}$ of the form $\{\, \mathfrak{m} \mid \mathfrak{m} \supseteq I \,\}$, where I runs through radical ideals of $\mathbf{A}$.

PROOF is evident. □

DEFINITIONS 1.5.5. Let X be a topological space.

(1) X is called *noetherian* if every decreasing chain of its closed subsets $Z_1 \supseteq Z_2 \supseteq Z_3 \supseteq \dots$ stabilizes, i.e., there is an integer r such that $Z_s = Z_r$ for all $s > r$.
(2) X is called *irreducible* if it is non-empty and $Y \cup Z \neq X$ for any proper closed subsets $Y, Z \subset X$.
Equivalently, X is irreducible if and only if any non-empty open subset $U \subseteq X$ is *dense* in X, i.e., $U \cap U' \neq \emptyset$ for any other non-empty open $U' \subseteq X$.

PROPOSITION 1.5.6. (1) *Any affine algebraic variety is a noetherian topological space.*
(2) *An affine algebraic variety is irreducible if and only if its coordinate algebra is* integral*, i.e., is non-zero and contains no non-zero zero divisors.*

PROOF. *1* follows from Proposition 1.3.6, as any decreasing chain of closed subsets $Z_1 \supseteq Z_2 \supseteq Z_3 \supseteq \dots$ defines the increasing chain of ideals in the coordinate ring: $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$, where $I_i = I(Z_i)$. The latter stabilizes: there is some r such that $I_s = I_r$ for $s > r$. Then $Z_s = V(I_s) = V(I_r) = Z_r$.

2. Let X be a non-empty affine variety, $\mathbf{A}$ its coordinate algebra. Suppose that $\mathbf{A}$ is integral and $Y, Z \subset X$ are proper closed subsets. Put $I = I(Y)$, $J = I(Z)$. Then $I \neq 0$ and $J \neq 0$. Let $a \in I$ and $b \in J$ be non-zero. Then $ab \neq 0$ and $ab \in I(Y \cup Z)$. Hence, $I(Y \cup Z) \neq 0$ and $Y \cup Z \neq X$, i.e., X is irreducible.

Suppose now that X is irreducible and $a, b \in \mathbf{A}$ are non-zero elements. Then $Y = V(a)$ and $Z = V(b)$ are proper closed subsets, thus, $V(ab) = Y \cup Z \neq X$. Hence, $ab \neq 0$ and $\mathbf{A}$ is integral. □

Corollary 1.5.7. *A closed subset $Z \subseteq X$ is irreducible if and only if the corresponding ideal $I(Z) \subseteq \mathbf{K}[X]$ is* prime, *i.e., is a proper ideal such that if a and b do not belong to it, its product also does not belong to it.*

Certainly, every subset of a noetherian space is noetherian in the induced topology. For noetherian spaces we can often use the so called "*noetherian induction*": to prove some proposition, check first that it holds for the empty set and then prove that it holds for X whenever it holds for every proper closed subset $Y \subset X$. Then our proposition is valid for any noetherian space. As an example, we prove the following result.

Theorem 1.5.8. *Let X be a noetherian topological space. Then there are irreducible closed subsets $X_1, X_2, \dots, X_s \subseteq X$ such that $X = \bigcup_{i=1}^s X_i$ and $X_i \nsubseteq X_j$ for $i \neq j$. Moreover, these X_i are unique: if $X = \bigcup_{i=1}^r Y_i$, where Y_i are irreducible closed subsets and $Y_i \nsubseteq Y_j$ for $i \neq j$, then $r = s$ and there is a substitution σ such that $X_i = Y_{\sigma(i)}$ for all i.*

The closed subsets X_i are called the *irreducible components* (or simply *components*) of X and the equality $X = \bigcup_{i=1}^s X_i$ is called the *irreducible decomposition* of X.

Proof. First prove the existence of such a decomposition. If $X = \emptyset$, the claim is obvious. Suppose that it is valid for any proper closed subset of X. If X is irreducible itself, we put $s = 1$, $X_1 = X$. Let $X = Y \cup Z$ for two proper closed subsets Y and Z. Then, by the supposition, $Y = \bigcup_{i=1}^k X_i$ and $Z = \bigcup_{i=k+1}^s X_i$, where all X_i are irreducible closed subsets. Hence, $X = \bigcup_{i=1}^s X_i$. If $X_i \subseteq X_j$ for some $i \neq j$, we can cross out X_i from this decomposition. After a finite number of such crossings, we get a decomposition of the necessary kind.

Now we prove the uniqueness. Let $X = \bigcup_{i=1}^s X_i = \bigcup_{i=1}^r Y_i$ be two irreducible decompositions. Then, for each i, $X_i = \bigcup_{j=1}^r (X_i \cap Y_j)$. As X_i is irreducible, $X_i \subseteq Y_j$ for some j. Just in the same way, $Y_j \subseteq X_k$ for some k, whence $X_i \subseteq X_k$. Therefore, $i = k$, so $X_i = Y_j$. Obviously, such a number j is unique; moreover, different i give different j. Hence, $s = r$ and the mapping $i \mapsto j$ defines a substitution σ such that $X_i = Y_{\sigma(i)}$ for all i. □

Using the 1-1 correspondence between radical ideals in an affine algebra and closed subsets of the corresponding variety, we can reformulate Theorem 1.5.8 in the following way.

Corollary 1.5.9. *For any radical ideal I of an affine algebra, there are prime ideals $P_1, P_2, \dots, P_s$ such that $I = \bigcap_{i=1}^s P_i$ and $P_i \nsupseteq P_j$ for $i \neq j$. Moreover, these P_i are unique: if $I = \bigcap_{i=1}^r Q_i$, where Q_i are prime ideals and $Q_i \nsupseteq Q_j$ for $i \neq j$, then $r = s$ and there is* *a substitution* σ *such that* $P_i = Q_{\sigma(i)}$ *for all* i .

The prime ideals P_i are called the *prime components* of the radical ideal I and the equality $I = \bigcap_{i=1}^s P_i$ is called the *prime decomposition* of I .

EXERCISE 1.5.10. Prove that Corollary 1.5.9 is valid for radical ideals of an arbitrary noetherian ring.

REMARK. There is a more refined version of Corollary 1.5.9 concerning all ideals of a noetherian ring (in particular, of an affine algebra), where prime ideals are replaced by the so called *primary* ones, but we do not need this refinement.

EXERCISES 1.5.11.

(1) Prove that, for every radical ideal I of an affine algebra $\mathbf{A}$, $I = \bigcap_{\mathfrak{m} \in \operatorname{Max} \mathbf{A},\, \mathfrak{m} \supseteq I} \mathfrak{m}$.
(2) Find an example showing that the preceding assertion can be wrong for arbitrary noetherian rings.
    Hint: You may consider the ring of formal power series in one variable.
(3) Let $\gamma : \mathbf{A} \to \mathbf{B}$ be a homomorphism of affine algebras and $\mathfrak{m}$ be a maximal ideal of $\mathbf{B}$. Prove that $\gamma^{-1}(\mathfrak{m})$ is a maximal ideal of $\mathbf{A}$.
(4) Find an example showing that the preceding assertion can be wrong for arbitrary noetherian rings.
(5) Prove that any noetherian topological space is quasi-compact. (It means that every open covering of such a space contains a finite subcovering.)
(6) Prove that irreducible components of a hypersurface $V(F)$ are just the hypersurfaces $V(F_i)$, where F_i run through the prime divisors of F .
(7) Find the irreducible components of the following affine varieties in $\mathbb{A}^3_{\mathbb{C}}$:
    (a) $X = V(x^2 + yz, x^2 + y^2 + z^2 - 1)$;
    (b) $X = V(x^2 - yz, x^3 - z^2)$.
(8) Let $f : Y \to X$ be a morphism of affine varieties.
    (a) Show that f^* is surjective if and only if f is a *closed embedding*, i.e., induces an isomorphism of Y onto a closed subvariety of X .
    (b) Show that f^* is injective if and only if f is *dominant*, i.e., its image is dense in X .

1.6. Structure sheaf. Rings of fractions

Remind the notion of a *sheaf* on a topological space.

DEFINITION 1.6.1. A sheaf $\mathcal{F}$ on a topological space X consists of sets $\mathcal{F}(U)$, given for every open subset $U \subseteq X$, and of mappings

$\mathcal{F}^U_V : \mathcal{F}(U) \to \mathcal{F}(V)$, given for every pair $V \subseteq U$ of open subsets, such that the following conditions hold:

(1) $\mathcal{F}^U_U$ is the identity mapping for every U.
(2) $\mathcal{F}^U_W = \mathcal{F}^V_W \circ \mathcal{F}^U_V$ for every triple $W \subseteq V \subseteq U$ of open sets.
(3) Given any open covering $U = \bigcup_i U_i$ of an open set U and any elements $f_i \in \mathcal{F}(U_i)$ such that $\mathcal{F}^{U_i}_{U_i \cap U_j}(f_i) = \mathcal{F}^{U_j}_{U_i \cap U_j}(f_j)$ for all i, j, there is a unique element $f \in \mathcal{F}(U)$ such that $f_i = \mathcal{F}^U_{U_i}(f)$ for all i.

The elements of $\mathcal{F}(U)$ are called the *sections* of the sheaf $\mathcal{F}$ over the open set U. The mappings $\mathcal{F}^U_V$ are called the *restriction mappings*.

If all $\mathcal{F}(U)$ are groups (rings, algebras, etc.) and all $\mathcal{F}^U_V$ are homomorphisms of groups (resp., rings, algebras, etc.), then $\mathcal{F}$ is called a sheaf of groups (resp., rings, algebras, etc.).

For every affine algebraic variety X with the coordinate algebra $\mathbf{A}$ we define its *structure sheaf* $\mathcal{O}_X$ (or $\mathcal{O}$ if X is fixed) in the following way. The set $\mathcal{O}(U)$ consists of all functions $f : U \to \mathbf{K}$ satisfying the following condition:

For every point $x \in U$, there is a neighbourhood $V \subseteq U$ and two functions $a, b \in \mathbf{A}$ such that, for all $y \in V$, $b(y) \neq 0$ and $f(y) = a(y)/b(y)$.

The mapping $\mathcal{O}^U_V$ maps every function $f \in \mathcal{F}(U)$ to its restriction on V.

Exercise 1.6.2. Verify that $\mathcal{O}_X$ is indeed a sheaf of $\mathbf{K}$-algebras.

The functions from $\mathcal{O}_X(U)$ are called the *regular functions* on U and the structure sheaf $\mathcal{O}_X$ is also called the *sheaf of regular functions*.

Usually, it is not so easy to calculate the algebra $\mathcal{O}(U)$. Nevertheless, in some cases it can be done. First of all it is so for the "global sections."

Proposition 1.6.3. $\mathcal{O}_X(X) = \mathbf{K}[\,X\,]$.

Proof. Suppose that $f \in \mathcal{O}(X)$. Then there is an open covering $X = \bigcup_i U_i$ and regular functions a_i, b_i such that $b_i(x) \neq 0$ and $f(x) = a_i(x)/b_i(x)$ for all i and for all $x \in U_i$. As X is quasi-compact and principal open sets form a base of the Zariski topology (cf. Exercise 1.2.4(1)), we can suppose that this covering is finite and each U_i is a principle open set $D(g_i) = \{\, x \in X \mid g_i(x) \neq 0 \,\}$. As $b_i(y) \neq 0$ for every $y \in D(g_i)$, i.e., $b_i(x) = 0$ implies $g_i(x) = 0$, Hilbert Nullstellensatz gives that $g_i^k = b_i c_i$ for some k and some regular function c_i. Therefore, $f = a_i c_i / g_i^k$ on $U_i = D(g_i) = D(g_i^k)$, so we may suppose that already $U_i = D(b_i)$. Then $U_i \cap U_j = D(b_i b_j)$. As $a_i/b_i = a_j/b_j$ on this intersection, we have that $a_i b_j = a_j b_i$ on $D(b_i b_j)$ or, the same $a_i b_i b_j^2 = a_j b_j b_i^2$ everywhere. But $f = a_i/b_i = a_i b_i / b_i^2$ on U_i, hence, replacing a_i by a_ib_i and b_i by b_i^2, we may suppose that $a_ib_j = a_jb_i$ everywhere. Then $b_if = b_ia_j/b_j = a_i$ on each U_j, i.e., everywhere.

Note now that $X = \bigcup_i D(b_i)$, thus, $V(\{ b_i \}) = \emptyset$. By Hilbert Nullstellensatz, there are regular functions h_i such that $\sum_i h_ib_i = 1$, whence $f = \sum_i h_ib_if = \sum_i h_ia_i$ is a regular function on X. $\square$

Almost the same can be done for principle open sets, but before we need some algebraic preliminaries, namely, the notion of *rings of fractions*.

Consider an arbitrary ring $\mathbf{A}$. A subset $S \subseteq \mathbf{A}$ is called *multiplicative* if $1 \in S$ and $st \in S$ for every $s, t \in S$. Given a multiplicative subset $S \subseteq \mathbf{A}$, construct a new ring as follows:

(1) Consider the set of pairs $\mathbf{A}\times S$ and the equivalence relation on it: $(a, s) \sim (b, t)$ if and only if there is an element $r \in S$ such that $atr = bsr$. Denote by $\mathbf{A}[S^{-1}]$ the set of the equivalence classes of this relation and by a/s the class of the pair (a, s) in $\mathbf{A}[S^{-1}]$.

(2) For two elements, a/s and b/t of $\mathbf{A}[S^{-1}]$, put $a/s + b/t = (at + bs)/st$ and $(a/s)(b/t) = ab/st$.

EXERCISES 1.6.4. (1) Verify that $\sim$ is indeed an equivalence relation on $\mathbf{A} \times S$.

(2) Verify that the definitions of sum and product do not depend on the choice of the pairs (a, s) and (b, t) in their classes.

(3) Verify that $\mathbf{A}[S^{-1}]$ with these definitions of sums and products becomes a ring.

The ring $\mathbf{A}[S^{-1}]$ is called the *ring of fractions of* $\mathbf{A}$ *with respect to the multiplicative subset* S.

If S consists of all non-zero-divisors of $\mathbf{A}$, the ring of fractions $\mathbf{A}[S^{-1}]$ is called the *full ring of fractions* of $\mathbf{A}$. Certainly, if $\mathbf{A}$ is integral, the full ring of fractions is just the field of fractions of $\mathbf{A}$.

EXERCISES 1.6.5. (1) Check that the mapping $\rho_S : \mathbf{A} \to \mathbf{A}[S^{-1}]$ such that $\rho_S(a) = a/1$ is a homomorphism of rings and $\operatorname{Ker} \rho_S = \{ a \in \mathbf{A} \mid as = 0 \text{ for some } s \in S \}$. In particular, $\mathbf{A}[S^{-1}]$ is a zero ring if and only if $0 \in S$; ρ_S is an embedding if and only if S does not contain any zero divisors. (In the last case, we usually identify $\mathbf{A}$ with its image in $\mathbf{A}[S^{-1}]$ and write a for $a/1$.)

(2) Let T be another multiplicative subset in $\mathbf{A}$, $T/1 = \{ t/1 \mid t \in T \}$ its image in $\mathbf{A}[S^{-1}]$. Prove that $A[S^{-1}][(T/1)^{-1}] \simeq \mathbf{A}[(ST)^{-1}]$, where $ST = \{ st \mid s \in S,\, t \in T \}$.

(3) Prove that if S contains no zero divisors, $\mathbf{A}[S^{-1}]$ is canonically isomorphic to a subring of the full ring of fractions. (We will usually identify them.) In particular, if $\mathbf{A}$ is integral and

$0 \notin S$, the ring $\mathbf{A}[S^{-1}]$ can be considered as a subring of the field of fractions of $\mathbf{A}$.

If g is an element of $\mathbf{A}$, $S = \{\, g^k \mid k \in \mathbb{N} \,\}$, the ring of fractions $\mathbf{A}[S^{-1}]$ is also denoted by $\mathbf{A}[\, g^{-1}\,]$ and the mapping ρ_S is denoted by ρ_g.

Exercise 1.6.6. Let X be an affine algebraic variety, $\mathbf{A} = \mathbf{K}[\, X\,]$. The aim of this exercise is to prove that, for each principle open subset $U = D(g)$, $\mathcal{O}_X(U) \simeq \mathbf{A}[g^{-1}]$ and, under their identification, the restriction $\mathcal{O}_U^X$ coincides with ρ_g. We follow the proof of Proposition 1.6.3.

(1) Verify that every element of $\mathbf{A}[g^{-1}]$ can be considered as a regular function on U and different elements of $\mathbf{A}[g^{-1}]$ define different functions. Hence, $\mathbf{A}[g^{-1}]$ can be identified with a subring of $\mathcal{O}_X(U)$. Check that, under this identification, ρ_g coincides with $\mathcal{O}_U^X$.
(2) Verify that if $U = \bigcup_i U_i$, is an open covering, there are principle open sets $D(g_i) \subseteq U_i$ such that U is a finite union of some of $D(g_i)$.
Thus, if a function $f : U \to \mathbf{K}$ is regular, there is a finite set $\{\, g_1, g_2, \dots, g_m \,\}$ such that $U = \bigcup_i U_i$, where $U_i = D(g_i)$, and $f(x) = a_i(x)/b_i(x)$ for every $x \in U_i$, where $a_i, b_i \in \mathbf{A}$ and $b_i(x) \neq 0$ for every $x \in U_i$.
(3) Let f be any regular function on U; $U_i = D(g_i)$, a_i and b_i are defined as above. Check that, changing the elements a_i, b_i, g_i, one may suppose that $b_i = g_i$.
(4) Considering the restriction of f onto $D(b_i b_j)$, check that one may suppose that $a_i b_j = a_j b_i$, whence $b_i f = a_i$ on U.
(5) Prove that $g^k = \sum_i h_i b_i$ for some integer k and some $h_i \in \mathbf{A}$, whence $f \in \mathbf{A}[g^{-1}]$.

CHAPTER 2

Projective and Abstract Varieties

2.1. Projective varieties and homogeneous ideals

Remind that the *n-dimensional projective space* $\mathbb{P}^n_{\mathbf{K}}$ over the filed $\mathbf{K}$[1] (or simply $\mathbb{P}^n$ if $\mathbf{K}$ is fixed) is, by definition, the set of equivalence classes $(\mathbf{A}^{n+1} \setminus \{ 0 \})/\sim$, where $(a_0, a_1, \dots, a_n) \sim (b_0, b_1, \dots, b_n)$ means that $a_i = \lambda b_i$ for all i and some non-zero $\lambda \in \mathbf{K}$. The equivalence class of $(a_0, a_1, \dots, a_n)$ in $\mathbb{P}^n$ is denoted by $(a_0 : a_1 : \dots : a_n)$; the elements a_i are called the *homogeneous coordinates* of the point $\mathbf{a} = (a_0 : a_1 : \dots : a_n) \in \mathbb{P}^n$.

Again we are going to define a projective algebraic variety as the set of common zeros of some polynomials. However, as the homogeneous coordinates of a point are only defined up to a common multiple, we cannot consider arbitrary polynomials and have to restrict ourselves by *homogeneous* ones, i.e., such polynomials F that all monomials occurring in F are of the same degree. Of course, if F is homogeneous and $F(a_0, a_1, \dots, a_n) = 0$, then also $F(\lambda a_0, \lambda a_1, \dots, \lambda a_n) = 0$, i.e., we may say that $F(\mathbf{a}) = 0$ for a point $\mathbf{a}$ of the projective space.

EXERCISE 2.1.1. Let F be an arbitrary polynomial, F_d denote its *homogeneous* component of degree d, i.e., the sum of all monomials of degree d occurring in F. Suppose that $F(\lambda a_0, \lambda a_1, \dots, \lambda a_n) = 0$ for every non-zero $\lambda \in \mathbf{K}$. Prove that $F_d(a_0, a_1, \dots, a_n) = 0$ for all d.

A subset $X \subseteq \mathbb{P}^n_{\mathbf{K}}$ is called a *projective algebraic variety* if it coincides with the set $PV(S)$ of common zeros of a set S of homogeneous polynomials. Again we often omit the word "algebraic" and simply say "projective variety." If $\mathbf{F}$ is a subfield of $\mathbf{K}$, one denotes again by $X(\mathbf{F})$ the set of all points of the variety X whose coordinates belong to $\mathbf{F}$. If S consists of a single polynomial F, we call $PV(F)$ a *(projective) hypersurface* (*plane curve* if $n = 1$, *space surface* if $n = 2$).

An ideal $I \subset \mathbf{K}[x_0, x_1, \dots, x_n]$ is called *homogeneous* if, for every $F \in I$, all homogeneous components of F also belong to I. In other words, $I = \oplus_d I_d$, where I_d denotes the set of all homogeneous polynomials of degree d belonging to I (including 0).

[1] Just as before, we usually suppose this field being algebraically closed.

EXERCISES 2.1.2. (1) Show that an ideal $I \subset \mathbf{K}[\,\mathbf{x}\,]$ is homogeneous if and only if it has a set of generators consisting of homogeneous polynomials.
(2) Show that any divisor of a homogeneous polynomial is again homogeneous. In particular, a homogeneous polynomial is irreducible if and only if it has no proper homogeneous divisors.
(3) Prove that if an ideal I is homogeneous, its radical $\sqrt{I}$ is homogeneous too.

One can easily see, just as in the affine case, that any intersection and any finite union of projective varieties in $\mathbb{P}^n$ is again a projective variety. Hence, we can define the *Zariski topology* on $\mathbb{P}^n$ taking projective varieties for its closed sets. We always consider projective space and all its subsets (in particular, projective varieties) with this topology.

It is obvious that if $I = \langle\, S \,\rangle$, where S is a set of homogeneous polynomials, then $F(\mathbf{a}) = 0$ for every $F \in I$ and $\mathbf{a} \in PV(S)$. Moreover, $PV(S) = PV(S')$ for every set of homogeneous generators of the ideal I. That is why we also denote $PV(S)$ by $PV(I)$. On the other hand, for every subset $X \subseteq \mathbb{P}^n$, we can define the homogeneous ideal $I(X)$ as

$$\{\, F \in \mathbf{K}[\,\mathbf{x}\,] \mid F(\mathbf{a}) = 0 \text{ for all } \mathbf{a} \in X \,\}\ .$$

(Note that this ideal is always homogeneous in view of Exercise 2.1.1.) It is quite obvious that $PV(I(X)) = X$ if and only if X is a projective variety and that $I(X)$ is always a radical ideal. Nevertheless, there are some proper homogeneous ideals I such that $PV(I) = \emptyset$. This is the case, for instance, for the ideal $I_+ = \langle\, x_0, x_1, \dots, x_n \,\rangle$. (This ideal consists of all polynomials with zero constant term. One can easily see that any proper homogeneous ideal is contained in I_+.) The following version of Hilbert Nullstellensatz shows that this is, in some sense, the only exception.

THEOREM 2.1.3 (Projective Hilbert Nullstellensatz). *Let $I \subset \mathbf{K}[\,\mathbf{x}\,]$ be a proper homogeneous ideal. Then*
(1) *$PV(I) = \emptyset$ if and only if $\sqrt{I} = I_+$, or, the same, $I_+^k \subseteq I$ for some k.*
(2) *If $PV(I) \neq \emptyset$, then $I(PV(I)) = \sqrt{I}$.*

PROOF. Consider the affine variety $V(I) \subseteq \mathbb{A}^{n+1}$. (It is called the *(affine) cone* over the projective variety $PV(I)$.) It always contains 0 as all polynomials from I have zero constant term. If $PV(I) = \emptyset$, then $V(I) = \{\, 0 \,\}$, whence $I(V(I)) = \sqrt{I} = I_+$. On the other hand, if $PV(I) \neq \emptyset$, then, obviously, $I(PV(I)) = I(V(I)) = \sqrt{I}$, in view of Hilbert Nullstellensatz. □

COROLLARY 2.1.4. *There is a 1-1 correspondence between projective varieties in $\mathbb{P}^n$ and radical homogeneous ideals in $\mathbf{K}[\,x_0, x_1, \dots, x_n\,]$.*

One call a proper homogeneous ideal $I \subset \mathbf{K}[\mathbf{x}]$ *essential* if $\sqrt{I} \neq I_+$; thus, essential ideals define non-empty projective varieties.

Denote by $\mathbb{A}_i^n$ the subset of $\mathbb{P}^n$ consisting of all points $\mathbf{a} = (a_0 : a_1 : \dots : a_n)$ such that $a_i \neq 0$. Such points can be uniquely presented in the following way: $\mathbf{a} = (a_0/a_i : \dots : 1 : \dots : a_n/a_i)$, where 1 is at the i-th place. Hence, we may identify $\mathbb{A}_i^n$ with the n-dimensional affine space and we will always do it. Certainly, $\mathbb{P}^n = \bigcup_{i=0}^n \mathbb{A}_i^n$ and $\mathbb{A}_i^n$ are open in the Zariski topology of $\mathbb{P}^n$. One calls them the *canonical affine covering* of $\mathbb{P}^n$.

Proposition 2.1.5. *The Zariski topology of $\mathbb{A}_i^n$ as an affine space coincides with that induced from $\mathbb{P}^n$. In other words, if X is a closed subset of $\mathbb{P}^n$, then $X \cap \mathbb{A}_i^n$ is closed in $\mathbb{A}_i^n$, and every closed subset of $\mathbb{A}_i^n$ is of the form $X \cap \mathbb{A}_i^n$ for some closed subset of $\mathbb{P}^n$.*

Proof. Let $\mathbf{P}_i$ be the polynomial ring in the variables t_j for $0 \leq j \leq n$, $j \neq i$. We consider $\mathbf{P}_i$ as the coordinate algebra of $\mathbb{A}_i^n$ in the obvious way. We also put $t_i = 1$. For every homogeneous polynomial $F \in \mathbf{K}[x_0, x_1, \dots, x_n]$ of degree d, put $F^{(i)} = F(t_0, t_1, \dots, t_n) \in \mathbf{P}_i$. On the other hand, for every polynomial $G \in \mathbf{P}_i$ of degree d, put $G^* = x_i^d G(x_0/x_i, \dots, x_n/x_i)$ (of course, x_i/x_i should be omitted here). G^* is always a homogeneous polynomial of degree d from $\mathbf{K}[\mathbf{x}]$. For every set $S \subseteq \mathbf{K}[\mathbf{x}]$ of homogeneous polynomials, put $S^{(i)} = \left\{ F^{(i)} \mid F \in S \right\}$ and for every subset $T \subseteq \mathbf{P}_i$ put $T^* = \{ G^* \mid G \in T \}$.

Consider a point $\mathbf{a} = (a_0 : a_1 : \dots : a_n) \in \mathbb{A}_i^n$. As $a_i \neq 0$, $F(\mathbf{a}) = 0$ if and only if $F^{(i)}(a_0/a_i, \dots, a_n/a_i) = 0$. Hence, for every set S of homogeneous polynomials, $PV(S) \cap \mathbb{A}_i^n = V(S^{(i)})$ is a closed subset of $\mathbb{A}_i^n$. On the other hand, if $\mathbf{b} = (b_0, \dots, \check{b}_i, \dots, b_n)$ is a point of $\mathbb{A}_i^n$, then $G(\mathbf{b}) = 0$ if and only if $G^*(b_0, \dots, 1, \dots, b_n) = 0$ (1 on the i-th place). Hence, for every subset $T \subseteq \mathbf{P}_i$, $V(T) = PV(T^*) \cap \mathbb{A}_i^n$. $\square$

Remark. As $\mathbb{P}^n = \bigcup_{i=0}^m \mathbb{A}_i^n$ is an open covering, a subset $X \subseteq \mathbb{P}^n$ is closed (open) if and only if $X \cap \mathbb{A}_i^n$ is closed (resp., open) in $\mathbb{A}_i^n$ for each $i = 0, \dots, n$. Moreover, for any closed subset $Y \subseteq \mathbb{A}_i^n$, $Y = \overline{Y} \cap \mathbb{A}_i^n$, where $\overline{Y}$ is its closure in $\mathbb{P}^n$, and Y is open in $\overline{Y}$.

In particular, if $X \subseteq \mathbb{P}^n$ is a projective variety, then $X_i = X \cap \mathbb{A}_i^n$ are affine varieties, which form an open covering of X. This covering is also called the *canonical affine covering* of X.

Example 2.1.6. Consider the projective plane curve ("projective conic") $Q = PV(x_0^2 + x_1^2 + 2x_0x_2)$. We calculate its "affine parts" $Q_i = Q \cap \mathbb{A}_i^2$ ("affine conics"). For $\mathbb{A}_0^2$, put $x = x_1/x_0$, $y = x_2/x_0$; then $Q_0 = V(x^2 + 2y + 1)$ ("parabola"). For $\mathbb{A}_1^2$, put $x = x_0/x_1$, $y = x_2/x_1$; then $Q_1 = V(x^2 + 2xy + 1)$ ("hyperbola"). At last, for $\mathbb{A}_2^2$, put $x = x_0/x_2$, $y = x_1/x_2$; then $Q_2 = V(x^2 + y^2 + 2y)$ ("ellipse," or even "circle").

EXERCISES 2.1.7. (1) Let $X \subseteq \mathbb{P}^n$ be a projective variety such that $X_i = X \cap \mathbb{A}^n_i \neq \emptyset$. Prove that X is irreducible (in the Zariski topology) if and only if X_i is irreducible and $X = \overline{X}_i$.

(2) Identifying $\mathbb{A}^2$ with $\mathbb{A}^2_0 \subset \mathbb{P}^2$, find the projective closure C of the nodal cubic $C_0 = V(y^2 - x^3 - x^2)$. Find two other "affine parts," C_1, C_2, of C.

EXERCISES 2.1.8. For a homogeneous polynomial F from $\mathbf{K}[\,\mathbf{x}\,] = \mathbf{K}[\,x_0, x_1, \dots, x_n\,]$, put $F^{\downarrow i} = F(t_1, \dots, \overset{i}{1}, \dots, t_n)$, and for a polynomial G of degree d from $\mathbf{K}[\,\mathbf{t}\,] = \mathbf{K}[\,t_1, \dots, t_n\,]$, put $G^{\uparrow i} = x_i^d G(x_0/x_i, \dots, \check{x_i/x_i}, \dots, x_n/x_i)$. For a homogeneous ideal $I \subseteq \mathbf{K}[\,\mathbf{x}\,]$, denote by $\tilde{I}$ the set of all homogeneous polynomials from I.

(1) For any homogeneous ideal $I \subset \mathbf{K}[\,\mathbf{x}\,]$, show that $I^{\downarrow i} = \left\{ F^{\downarrow i} \,\middle|\, F \in \tilde{I} \right\}$ is an ideal in $\mathbf{K}[\,\mathbf{t}\,]$, and for any ideal $J \subset \mathbf{K}[\,\mathbf{t}\,]$, show that $\left\{ G^{\uparrow i} \mid G \in J \right\} = \widetilde{J^{\uparrow i}}$ for some homogeneous ideal $J^{\uparrow i} \subset \mathbf{K}[\,\mathbf{x}\,]$.

(2) Prove that if I (J) is a radical ideal, then $I^{\downarrow i}$ (resp., $J^{\uparrow i}$) is also radical. Is the converse also true? (Prove it or find a counterexample.)

(3) Prove that $I = \bigcap_{i=0}^n I^{\downarrow i \uparrow i}$ for any essential radical homogeneous ideal $I \subset \mathbf{K}[\,\mathbf{x}\,]$. Does this equality hold for arbitrary essential homogeneous ideals? (Prove it or find a counterexample.)

Hint: Prove that $PV(I) \cap \mathbb{A}^n_i = V(I^{\downarrow i})$ and $\overline{V(J)} = PV(J^{\uparrow i})$.

Using the canonical affine covering $X = \bigcup_{i=0}^n X_i$ of a projective variety X, we define the *structure sheaf* $\mathcal{O}_X$ (or $\mathcal{O}$ if X is fixed) in the following way. For each open subset $U \subseteq X$, $\mathcal{O}_X(U)$ is the set of all functions $f : U \to \mathbf{K}$ such that, for every $i = 0, \dots, n$, the restriction of f onto $U \cap X_i$ is a regular function on this intersection (in the sense of Section 1.6), while the mapping $\mathcal{O}^U_V$ maps a function f to its restriction onto V.

EXERCISE 2.1.9. Check that $\mathcal{O}_X$ is indeed a sheaf.

Of course, the structure sheaf of each affine part X_i of X is just the restriction onto X_i of $\mathcal{O}_X$, i.e. $\mathcal{O}_{X_i}(U) = \mathcal{O}_X(U)$ for every open subset $U \subseteq X_i$. (Note that such U is also open in X).

An important feature of projective varieties is that there are very few "globally regular" functions on them.

EXERCISE 2.1.10. Show that $\mathcal{O}_{\mathbb{P}^n}(\mathbb{P}^n) = \mathbf{K}$, i.e., the only regular functions on the projective space are constants.

Hint: Consider the restriction of $f \in \mathcal{O}_{\mathbb{P}^n}(\mathbb{P}^n)$ onto $\mathbb{A}_i^n$ and prove that it is of the form $F_i(x_0, x_1, \dots, x_n)/x_i^d$, where F_i is a homogeneous polynomial of degree d. Compare these restrictions on $\mathbb{A}_i^n \cap \mathbb{A}_j^n$.

Remark. Later (in Section 2.4) we shall see that the same is true for any connected projective variety.

2.2. Abstract algebraic varieties

An open subset of a projective variety is called a *quasi-projective* variety. Any projective, as well as any affine variety is a quasi-projective one. Quasi-projective varieties form a natural class of objects in the algebraic geometry and one could restrict oneself by studying them. Nevertheless, it is convenient to consider a wider class of objects and to define algebraic varieties as topological spaces with sheaves of algebras, which are locally isomorphic to affine varieties.

First introduce some necessary definitions. We always consider the field $\mathbf{K}$ with its Zariski topology. The proper closed sets in this topology are just the finite ones.

Definitions 2.2.1. (1) For a topological space X denote by $\mathcal{F}un_{X,\mathbf{K}}$ (or simply by $\mathcal{F}un$ if X and $\mathbf{K}$ are fixed) the sheaf of $\mathbf{K}$-algebras on X such that $\mathcal{F}un(U)$ is the set of all functions $U \to \mathbf{K}$ and $\mathcal{F}un_V^U$ are just the usual restriction of functions.

(2) A *space with functions* (over the field $\mathbf{K}$) is a pair $(X, \mathcal{O}_X)$, where X is a topological space and $\mathcal{O}_X$ is a subsheaf of algebras of the sheaf $\mathcal{F}un_{X,\mathbf{K}}$ satisfying the following conditions:
   (a) If $f \in \mathcal{O}_X(U)$, then the function f is continuous.
   (b) If $f \in \mathcal{O}_X(U)$ is such that $f(p) \neq 0$ for all $p \in U$, then also $1/f \in \mathcal{O}_X(U)$.

   The functions from $\mathcal{O}_X(U)$ are called *regular functions* on U.

(3) A *morphism* of spaces with functions $\varphi : (Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$ is a continuous mapping $\varphi : Y \to X$ such that, for every open subset $U \subseteq X$ and for every function $f \in \mathcal{O}_X(U)$, the function $f \circ \varphi$ belongs to $\mathcal{O}_Y(\varphi^{-1}(U))$.
   In this situation we denote by $\varphi^*(U) : \mathcal{O}_X(U) \to \mathcal{O}_Y(\varphi^{-1}(U))$ the homomorphism mapping f to $f \circ \varphi$.

Remark. As Zariski closed subsets of $\mathbf{K}$, except $\mathbf{K}$ itself, are finite, a function $f : U \to \mathbf{K}$ is continuous if and only if the set $\{ p \in U \mid f(p) \neq \alpha \}$ is open in X for each $\alpha \in \mathbf{K}$. Therefore, the restriction of a function $f \in \mathcal{O}_X(U)$ onto $D(f) = \{ p \in U \mid f(p) \neq 0 \}$ is invertible in $\mathcal{O}_X(D(f))$.

Obviously, if $\varphi : (Y, \mathcal{O}_Y) \to (X, \mathcal{O}_X)$ and $\psi : (Z, \mathcal{O}_Z) \to (Y, \mathcal{O}_Y)$ are morphisms of spaces with functions, their composition $\varphi \circ \psi$ is also a morphism of spaces with functions $(Z, \mathcal{O}_Z) \to (X, \mathcal{O}_X)$. A morphism

φ having an inverse morphism φ^{-1} is called an *isomorphism* of spaces with functions.

In what follows, we often speak of a "space with functions X," omitting $\mathcal{O}_X$ when it is clear ariety, in view of Proposition **??**.

Remind that a subset Y of a topological space X is said to be *locally closed* if it is the intersection of an open and a closed subsets of X, or, the same, if Y is open in its closure $\overline{Y}$.

COROLLARY 2.2.2. *Let $(X, \mathcal{O}_X)$ be an algebraic variety, $Y \subseteq X$ be a locally closed subset. Then Y is also an algebraic variety (considered as a space with functions via the restriction from X).*

In this situation Y is called *subvariety* of X. If Y is closed (open) in X, it is called *closed* (resp., *open*) *subvariety*.

PROOF. If $X = \bigcup_i U_i$, where each of U_i is an affine variety, then $Y = \bigcup_i (Y \cap U_i)$. If Y is closed in X, then each $Y \cap U_i$ is also an affine variety as it is closed in U_i. Thus, we may suppose $\overline{Y} = X$, so Y is open in X. In this case $Y \cap U_i$ is open in U_i, hence, is a finite union of principle open subsets of U_i, which are also affine varieties. □

DEFINITION 2.2.3. A morphism $f : Y \to X$ of algebraic varieties is called an *immersion* if $\operatorname{Im} f$ is a subvariety of X and f induces an isomorphism $Y \to \operatorname{Im} f$. If, moreover, $\operatorname{Im} f$ is closed (open) in X, f is called a *closed* (resp., *open*) immersion.

EXERCISES 2.2.4.

(1) Let $X = \mathbb{A}^n \setminus \{ p \}$ for some point p. Prove that if $n > 1$, X is not isomorphic to any affine variety.

Hint: Show that any regular function on X is the restriction of a unique regular function on $\mathbb{A}^n$; in particular, one can define the "value" $f(p)$ of this function at p. Then prove that $I = \{ f \in \mathcal{O}_X(X) \mid f(p) = 0 \}$ is a proper ideal in $\mathcal{O}_X(X)$ but $\{ a \in X \mid f(a) = 0 \text{ for all } f \in I \} = \emptyset$.

(2) Prove the same for $X = \mathbb{P}^n \setminus \{ p \}$ ($n > 1$).

REMARK. These varieties are also not projective ones as they are not closed in $\mathbb{P}^n$ (cf. Section 2.4).

Now we prove an important feature distinguishing affine varieties among all spaces with functions. We denote by $\operatorname{Mor}_{\mathrm{Space}}(Y, X)$ the set of morphisms of spaces with functions $Y \to X$ and by $\operatorname{Mor}_{\mathrm{Alg}}(\mathbf{A}, \mathbf{B})$, the set of homomorphisms of $\mathbf{K}$-algebras $\mathbf{A} \to \mathbf{B}$.

THEOREM 2.2.5. *A space with functions $(X, \mathcal{O}_X)$ is an affine variety if and only if $\mathcal{O}_X(X)$ is an affine algebra and the mapping $\gamma : \operatorname{Mor}_{\mathrm{Space}}(Y, X) \to \operatorname{Mor}_{\mathrm{Alg}}(\mathcal{O}_X(X), \mathcal{O}_Y(Y))$, $\varphi \mapsto \varphi^*(X)$, is bijective for every space with functions Y.*

(As we shall see from the proof, it is enough to take for Y algebraic and even affine varieties.)

PROOF. We denote $\mathbf{A} = \mathcal{O}_X(X)$. First suppose that $X \subseteq \mathbb{A}^n$ is an affine variety; then $\mathbf{A} = \mathbf{K}[X] = \mathbf{K}[\mathbf{x}]/I(X)$ is the coordinate algebra of X (cf. Proposition 1.6.3). Put $\xi_i = x_i + I(X)$, the coordinate functions on X. Let Y be an arbitrary space with functions, $\mathbf{B} = \mathcal{O}_Y(Y)$ and $h : \mathbf{A} \to \mathbf{B}$ be a homomorphism of algebras. Put $h_i = h(\xi_i)$ and, for any point $y \in Y$, put $\varphi(y) = (h_1(y), \dots, h_n(y)) \in \mathbb{A}^n$. If $F \in I(X)$, then $F(\varphi(y)) = h(F(\xi_1, \dots, \xi_n))(y) = 0$ as h is a homomorphism of algebras and $F(\xi_1, \dots, \xi_n) = F + I(X) = 0$. Therefore, $\operatorname{Im} \varphi \subseteq X$, so φ can be considered as a mapping $Y \to X$. Moreover, $\varphi^*(a) = h(a)$ for every function $a \in \mathbf{A}$.

Consider an open subset $U \subseteq X$ and a function $f \in \mathcal{O}_X(U)$. If $y_0 \in \mathcal{O}_Y(\varphi^{-1}(U))$, then $\varphi(y_0) \in U$, thus, by definition of $\mathcal{O}_X$, there is an open V, $\varphi(y_0) \in V \subseteq U$, and two functions $a, b \in \mathbf{A}$ such that $b(p) \neq 0$ and $f(p) = a(p)/b(p)$ for all $p \in V$. Then $y_0 \in \varphi^{-1}(V) \subseteq \varphi^{-1}(U)$, $h(a), h(b) \in \mathbf{B}$ and, for every $y \in \varphi^{-1}(V)$, $h(b)(y) = b(\varphi(y)) \neq 0$ and $f(\varphi(y)) = a(\varphi(y))/b(\varphi(y)) = h(a)(y)/h(b)(y)$. By the condition (b) of Definition 2.2.1(2), $f \circ \varphi \in \mathcal{O}_Y(\varphi^{-1}(U))$, hence, φ is a morphism of spaces with functions such that $\varphi^*(X) = h$. This construction gives us the inverse mapping to γ.

Now suppose that $\mathbf{A} = \mathcal{O}_X(X)$ is an affine algebra and γ is bijective for every Y. Take for Y the affine variety such that $\mathbf{A} \simeq \mathbf{B} = \mathbf{K}[Y]$ and let $\theta : Y \to X$ be such that θ^* is an isomorphism $\mathbf{A} \xrightarrow{\sim} \mathcal{O}_Y(Y) = \mathbf{B}$. Let $h = (\theta^*)^{-1} : \mathbf{B} \xrightarrow{\sim} \mathbf{A}$ and $\varphi : X \to Y$ be such that $h = \varphi^*$. Then $(\theta \circ \varphi)^* = \varphi^* \circ \theta^* = \mathrm{id}_{\mathbf{A}} = (\mathrm{id}_X)^*$, whence $\theta \circ \varphi = \mathrm{id}_X$, and in the same way, $\varphi \circ \theta = \mathrm{id}_Y$, so θ is an isomorphism. □

EXERCISES 2.2.6. (1) Let $X = V(S) \subseteq \mathbb{A}^n$ be an affine variety defined by a set of polynomials $S \subseteq \mathbf{K}[x_1, \dots, x_n]$. Show that a morphism $f : Y \to X$, where Y is a space with functions, is the same as an n-tuple $(f_1, f_2, \dots, f_n)$ of regular functions on Y such that $F(f_1, f_2, \dots, f_n) = 0$ for every $F \in S$.

(2) Let $X = PV(S) \subseteq \mathbb{P}^n$ be a projective variety defined by a set of homogeneous polynomials $S \subseteq \mathbf{K}[x_0, x_1, \dots, x_n]$. Show that to define a morphism $f : Y \to X$, where Y is a space with functions, one has to give an open covering $Y = \bigcup_i U_i$ and, for each i, an $(n+1)$-tuple $(f_{i0}, f_{i1}, \dots, f_{in})$ of regular functions on U_i satisfying the following conditions:
- $F(f_{i0}, f_{i1}, \dots, f_{in}) = 0$ for every $F \in S$ and every i;
- for each point $p \in U_i$, there is an index k such that $f_{ik}(p) \neq 0$;
- for each pair i, j, $\mathcal{O}^{U_i}_{U_i \cap U_j}(f_{ik} f_{jl}) = \mathcal{O}^{U_j}_{U_i \cap U_j}(f_{jk} f_{il})$ for all k, l.

On the other hand, given such data (U_i, f_{ik}), one defines a unique morphism $Y \to X$. When do two such data, (U_i, f_{ik}) and (V_j, g_{jk}), define the same morphism?

(3) Show that if $Y \subseteq \mathbb{P}^m$ is a quasi-projective variety, the regular functions f_{ik} in the previous exercise can be replaced by homogeneous polynomials $F_{ik} \in \mathbf{K}[x_0, x_1, \dots, x_m]$ of the same degree for any given i.

(4) Let $X = \mathbb{P}^1$, $Y = V(x^2+y^2-1) \subset \mathbb{A}^2$ and $f : Y \to X$ is given by the following data (check that they satisfy the conditions of Exercise 2 above):

$$U_1 = D(x-1),\ U_2 = D(x+1);$$
$$f_{10} = x-1,\ f_{11} = y,\ f_{20} = -y,\ f_{21} = x+1.$$

Check that f cannot be defined by a "common" rule of the sort: $f(y) = (g_1(y) : g_2(y))$ for all $y \in Y$ with $g_1, g_2 \in \mathbf{K}[Y]$. Try to find the geometric meaning of this mapping.

Remark. Let $(X, \mathcal{O}_X)$ be a space with functions, U be an open subset of X. It follows from the definition of the sheaf that a function $f : U \to \mathbf{K}$ belongs to $\mathcal{O}_X(U)$ if and only if, for every point $p \in U$, there is an open V such that $p \in V \subseteq U$ and $\mathcal{O}_V^U(f) \in \mathcal{O}_X(V)$. Therefore, one can define morphisms of spaces with functions "locally." The following lemma is an exact version of the latter claim. Its proof, quite straitforward, is left to the reader.

Lemma 2.2.7. *Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be two spaces with functions. Supposed given an open covering $Y = \bigcup_i Y_i$ of Y and, for each index i, a morphism $\varphi_i : Y_i \to X$ such that, for each pair i, j, the restrictions of φ_i and φ_j onto $Y_i \cap Y_j$ coincide. Then there is a unique morphism $\varphi : Y \to X$ such that $\varphi_i = \varphi|_{Y_i}$ for each i.*

One calls φ the *gluing* of the morphisms φ_i.

2.3. Products of varieties

Having the general notion of algebraic varieties, we are able to define their *direct products*. We even do it for any spaces with functions over $\mathbf{K}$. First, we introduce the following notations.

Notations 2.3.1. (1) If $f : X \to \mathbf{K}$ and $g : Y \to \mathbf{K}$ are two functions, denote by $f \otimes g$ the function $X \times Y \to \mathbf{K}$ such that $(f \otimes g)(a, b) = f(a)g(b)$ for every $a \in X$, $b \in Y$.

(2) If $A \subseteq \mathcal{F}un(X)$ and $B \subseteq \mathcal{F}un(Y)$ are two subspaces, denote by $A \otimes B$ the set of all finite sums $\{ \sum_i f_i \otimes g_i \mid f_i \in A,\ g_i \in B \}$.

One immediately check that $A \otimes B$ is a subspace of $\mathcal{F}un(X \times Y)$; if both A and B are subalgebras, then $A \otimes B$ is also a subalgebra in $\mathcal{F}un(X \times Y)$ as $(f \otimes g)f' \otimes g') = ff' \otimes gg'$.

REMARK. Indeed, the operation "$\otimes$" is a special case of *tensor product* of vector spaces, but we do not suppose the reader to know the latter.

DEFINITION 2.3.2. Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be two spaces with functions over the field $\mathbf{K}$. Define their *product* (as of spaces with functions) in the following way.

(1) For each open subsets $U \subseteq X$, $V \subseteq Y$ and each function $g \in \mathcal{O}_X(U) \otimes \mathcal{O}_Y(V)$, put $D(U, V, g) = \{ p \in U \times V \mid g(p) \neq 0 \}$. Define the topology on $X \times Y$ taking all possible $D(U, V, g)$ for its base.

(2) Define $\mathcal{O}_{X \times Y}(W)$, where W is an open subset of $X \times Y$ in the just defined topology, as the set of all functions $f : W \to \mathbf{K}$ with the following property:

For every point $w \in W$, there are a set $D(U, V, g)$ and two functions $a, b \in \mathcal{O}_X(U) \otimes \mathcal{O}_Y(V)$ such that $w \in D(U, V, g) \subseteq W$, $b(p) \neq 0$ and $f(p) = a(p)/b(p)$ for all points $p \in D(U, V, g)$.

REMARK. We always consider $X \times Y$ as a topological space with the topology defined above and never with the product of topologies of X and Y (where a base of open subsets is formed by $U \times V$ with U open in X, V open in Y). The latter one is obviously weaker (i.e., has less open subsets) and, for algebraic varieties in Zariski topology, is usually strongly weaker.

One defines two *canonical projections* (or simply *projections*) of the product $X \times Y$ onto the factors X and Y:

$$\mathrm{pr}_X : X \times Y \to X, \text{ mapping } (x, y) \mapsto x,$$
$$\mathrm{pr}_Y : X \times Y \to Y, \text{ mapping } (x, y) \mapsto y.$$

EXERCISE 2.3.3. Verify that pr_X and pr_Y are indeed morphisms of spaces with functions.

The main property of the so defined product is its following "categorical characterization."

THEOREM 2.3.4. (1) *Let $(X, \mathcal{O}_X)$, $(Y, \mathcal{O}_Y)$ be two spaces with functions. Then, for each space with functions $(Z, \mathcal{O}_Z)$, the mapping $\mathrm{Mor}_{\mathrm{Space}}(Z, X \times Y) \to \mathrm{Mor}_{\mathrm{Space}}(Z, X) \times \mathrm{Mor}_{\mathrm{Space}}(Z, Y)$, $\varphi \to (\mathrm{pr}_X \circ \varphi, \mathrm{pr}_Y \circ \varphi)$ is bijective.*

(2) *On the other hand, suppose given a space with functions $(P, \mathcal{O}_P)$ and two morphisms, $\theta_1 : P \to X$ and $\theta_2 : P \to Y$, such that, for any Z, the mapping $\mathrm{Mor}_{\mathrm{Space}}(Z, P) \to \mathrm{Mor}_{\mathrm{Space}}(Z, X) \times \mathrm{Mor}_{\mathrm{Space}}(Z, Y)$, $\varphi \to (\theta_1 \circ \varphi, \theta_2 \circ \varphi)$ is bijective. Then $P \simeq X \times Y$.*

PROOF. *1*. We construct the inverse mapping. Consider any two morphisms, $\varphi_1 : Z \to X$ and $\varphi_2 : Z \to Y$, and define the mapping

$\varphi : Z \to X \times Y$ as follows: $\varphi(z) = (\varphi_1(z), \varphi_2(z))$. We check that it is a morphism of spaces with functions; then $(\varphi_1, \varphi_2) \mapsto \varphi$ is the desired inverse mapping.

Let $U \subseteq X$, $V \subseteq Y$ be open subsets, $W = \varphi^{-1}(U \times V) = \varphi_1^{-1}(U) \cap \varphi_2^{-1}(V)$. Then, for every function $g = \sum_i a_i \otimes b_i \in \mathcal{O}_X(U) \otimes \mathcal{O}_Y(V)$, the function $g \circ \varphi = \sum_i (a_i \circ \varphi_1)(b_i \circ \varphi_2)$ belongs to $\mathcal{O}_Z(W)$. In particular, $W' = \varphi^{-1}(D(U, V, g)) = \{ z \in W \mid g(\varphi(z)) \neq 0 \}$ is an open set in Z, hence, φ is continuous. Moreover, if f is another function from $\mathcal{O}_X(U) \otimes \mathcal{O}_Y(V)$, then $(f/g) \circ \varphi = (f \circ \varphi)/(g \circ \varphi)$ belongs to $\mathcal{O}_Z(W')$, hence, φ is indeed a morphism of spaces with functions.

2. There is a mapping $\varphi : P \to X \times Y$ such that $\mathrm{pr}_X \circ \varphi = \theta_1$ and $\mathrm{pr}_Y \circ \varphi = \theta_2$. On the other hand, there is a mapping $\psi : X \times Y \to P$ such that $\theta_1 \circ \psi = \mathrm{pr}_X$ and $\theta_2 \circ \psi = \mathrm{pr}_Y$. Then $\mathrm{pr}_X \circ \varphi \circ \psi = \mathrm{pr}_X$ and $\mathrm{pr}_Y \circ \varphi \circ \psi = \mathrm{pr}_Y$, whence $\varphi \circ \psi = \mathrm{id}_{X \times Y}$. Just in the same way, $\psi \circ \varphi = \mathrm{id}_P$, i.e., φ and ψ are isomorphisms. □

Consider some examples. First, for the affine spaces, we have the following result concordant with the intuition.

Proposition 2.3.5. $\mathbb{A}^m \times \mathbb{A}^n \simeq \mathbb{A}^{m+n}$.

Proof. We apply Theorem 2.3.4(2) to the pair of morphisms $\theta_1 : \mathbb{A}^{m+n} \to \mathbb{A}^m$, $(x_1, x_2, \dots, x_{m+n}) \mapsto (x_1, x_2, \dots, x_m)$, and $\theta_2 : \mathbb{A}^{m+n} \to \mathbb{A}^n$, $(x_1, x_2, \dots, x_{m+n}) \mapsto (x_{m+1}, \dots, x_{m+n})$. Let Z be any space with functions, $\varphi_1 : Z \to \mathbb{A}^m$ and $\varphi_2 : Z \to \mathbb{A}^n$ be any two morphisms. Put $\mathbf{A} = \mathcal{O}_Z(Z)$. In view of Proposition 1.2.2, they are uniquely defined by homomorphisms of algebras $\varphi_1^* : \mathbf{K}[x_1, \dots, x_m] \to \mathbf{A}$ and $\varphi_2^* : \mathbf{K}[x_1, \dots, x_n] \to \mathbf{A}$. These homomorphisms are given by the m-tuple $(a_1, a_2, \dots, a_m)$ and the n-tuple $(b_1, b_2, \dots, b_n)$ of functions from $\mathbf{A}$, where $a_i = \varphi_1^*(x_i)$, $b_j = \varphi_2^*(x_j)$. Define the homomorphism $\gamma : \mathbf{K}[x_1, \dots, x_{m+n}]$ putting $\gamma(x_i) = a_i$ for $1 \le i \le m$ and $\gamma(x_i) = b_{i-m}$ for $m < i \le m+n$. We know that $\gamma = \varphi^*$ for a uniquely defined $\varphi : Z \to \mathbb{A}^{m+n}$. Obviously, $\theta_1 \circ \varphi = \varphi_1$ and $\theta_2 \circ \varphi = \varphi_2$ and the mapping $(\varphi_1, \varphi_2) \mapsto \varphi$ is inverse to $\mathrm{Mor}_{\mathsf{Space}}(Z, \mathbb{A}^{m+n}) \to \mathrm{Mor}_{\mathsf{Space}}(Z, \mathbb{A}^m) \times \mathrm{Mor}_{\mathsf{Space}}(Z, \mathbb{A}^n)$. □

Proposition 2.3.6. *Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be two spaces with functions, $X' \subseteq X$ and $Y' \subseteq Y$ be their subsets considered as spaces with functions with respect to the restrictions, respectively, from X and Y. Then the structure of product of spaces with functions $X' \times Y'$ coincides with that of the restriction from the product $X \times Y$.*

Proof. Consider $X' \times Y'$ as the restriction from $X \times Y$. In view of Proposition **??**, a morphism $Z \to X' \times Y'$ is the same as a morphism $Z \to X \times Y$ with the image contained in $X' \times Y'$. In view of Theorem 2.3.4, such a morphism is the same as a pair of morphisms $Z \to X$ and $Z \to Y$ with the images contained, respectively, in X' and in Y', i.e., a pair of morphisms $Z \to X'$ and $Z \to Y'$. Hence, this restriction coincides with the product of X' and Y' as of spaces with functions. $\square$

REMARK. As the topology of $X \times Y$ as of spaces with functions is stronger than the product of the topologies of X and Y, the product of closed (open) subsets is closed (open) in the product of spaces with functions $X \times Y$.

COROLLARY 2.3.7. *Let X, Y be affine varieties. Then $X \times Y$ is also an affine variety.*

COROLLARY 2.3.8. *If X, Y are algebraic varieties, their product (as of spaces with functions) is also an algebraic variety.*

The situation seems to be more complicated for projective varieties. At least, there is no natural 1-1 correspondence between $\mathbb{P}^m \times \mathbb{P}^n$ and $\mathbb{P}^{m+n}$. Later we shall see that these spaces are indeed non-isomorphic (cf. Exercise 2.5.5(2)). Nevertheless, we shall prove that the product of projective varieties is also projective. (Hence, the product of quasi-projective varieties is also quasi-projective.) We start with the case of projective spaces using an old observation of Segre.

PROPOSITION 2.3.9 (Segre embedding). *Put $N = m + n + mn$ and consider the points of $\mathbb{P}^N$ as non-zero $(m+1) \times (n+1)$ matrices (a_{ij}) (certainly, identifying the matrices (a_{ij}) and (λa_{ij}) for non-zero $\lambda \in \mathbf{K}$). In particular, the homogeneous coordinates in $\mathbb{P}^N$ are denoted by x_{ij} $(0 \le i \le m,\ 0 \le j \le n)$. Define a mapping $\sigma : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^N$ which maps a pair (a, b), where $a = (a_0 : a_1 : \dots : a_n)$, $b = (b_0 : b_1 : \dots : b_m)$, to the matrix $a^\top b = (a_i b_j)$. Then σ is a closed embedding, i.e., its image is closed in $\mathbb{P}^N$ and φ induces an isomorphism $\mathbb{P}^m \times \mathbb{P}^n \xrightarrow{\sim} \operatorname{Im} \varphi$.*

σ is called the *Segre embedding*.

PROOF. Let $S = \{\, x_{ij}x_{kl} - x_{il}x_{kj} \mid 0 \le i, k \le m;\ 0 \le j, l \le n \,\}$ and $\mathbb{S} = PV(S) \subset \mathbb{P}^N$ (the *Segre variety*; if one has to specify m, n, one writes $\mathbb{S}(m,n)$).[2] We prove that σ is an isomorphism $\mathbb{P}^m \times \mathbb{P}^n \xrightarrow{\sim} \mathbb{S}$. Indeed, the inclusion $\operatorname{Im} \sigma \subseteq \mathbb{S}$ is evident. To check that σ is a morphism and to construct the inverse morphism φ, consider the restriction σ_{kl} of σ onto the open set $U_{kl} = \mathbb{A}^m_k \times \mathbb{A}^n_l$ (the product of the affine spaces from the canonical affine coverings of $\mathbb{P}^m$ and $\mathbb{P}^n$). It maps a pair (a, b), where $a = (a_0 : \dots : 1 : \dots : a_m)$ (1 on the i-th place), $b = (b_0 : \dots : 1 : \dots : b_n)$ (1 on the j-th place) to the matrix $a^\top b = (a_i b_j)$, which has 1 on the (ij)-th place. Hence, this matrix belongs to $\mathbb{S}_{kl} = \mathbb{S} \cap \mathbb{A}^N_{kl}$, where $\mathbb{A}^N_{kl} = \{\, a \in \mathbb{P}^N \mid a_{kl} \ne 0 \,\}$ (the affine space from the canonical affine covering of $\mathbb{P}^N$). As the coordinates

[2]Obviously, the equations for $\mathbb{S}$ mean that the matrices $z \in \mathbb{S}$ are just those of rank 1.

of $\sigma_{kl}(a,b)$ are polynomials of the coordinates of a and b, σ_{kl} is a morphism $\mathbb{A}^m_k \times \mathbb{A}^n_l \to \mathbb{S}_{kl}$. Therefore, σ is a morphism $\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{S}$.

On the other hand, if a matrix $z = (z_{ij})$ belongs to $\mathbb{S}_{kl}$, one may suppose that $z_{kl} = 1$, whence $z_{ij} = z_{il}z_{kj}$. Therefore, one can define the morphism $\varphi_{kl} : \mathbb{S}_{kl} \to \mathbb{A}^m_k \times \mathbb{A}^n_l$ inverse to σ_{kl} putting

$$\varphi_{kl}(z) = ((z_{0l} : z_{1l} : \dots : z_{ml}), (z_{k0} : z_{k1} : \dots : z_{kn}))\,.$$

Note that this definition is even valid if $z_{kl} \neq 1$, as far as we consider all coordinates as homogeneous ones. Suppose that also $z \in \mathbb{S}_{rs}$ for another pair (rs). Then

$$\varphi_{rs}(z) = ((z_{0s} : z_{1s} : \dots : z_{ms}), (z_{r0} : z_{r1} : \dots : z_{rn}))\,.$$

But the equalities $z_{il}z_{js} = z_{is}z_{jl}$ and $z_{ki}z_{rj} = z_{kj}z_{ri}$, which are valid on $\mathbb{S}$, show that, in this case, $\varphi_{rs}(z) = \varphi_{kl}(z)$. Hence, we can define the morphism $\varphi : \mathbb{S} \to \mathbb{P}^m \times \mathbb{P}^n$ inverse to σ as the gluing of all φ_{kl} (cf. Lemma 2.2.7). □

Corollary 2.3.10. *If X and Y are projective (quasi-projective) varieties, then $X \times Y$ is also a projective (resp., quasi-projective) variety.*

Exercises 2.3.11.

(1) Show that the Segre variety $\mathbb{S}(1,1)$ (isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$) is a quadric space surface and outline $\mathbb{S}(\mathbb{R})$.

(2) What are the images under the Segre embedding $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ of the "lines" $a \times \mathbb{P}^1$ and $\mathbb{P}^1 \times b$ for fixed points $a, b \in \mathbb{P}^1$?

(3) Denote the homogeneous coordinates in $\mathbb{P}^m$ by $(x_0 : x_1 : \dots : x_m)$ and in $\mathbb{P}^n$ by $(y_0 : y_1 : \dots : y_n)$. Check that any closed subset of $\mathbb{P}^m \times \mathbb{P}^n$ is just the set of common zeros of a set of polynomials $S \subseteq \mathbf{K}[x_0, x_1, \dots, x_m, y_0, y_1, \dots, y_n]$, where every polynomial $F \in S$ is homogeneous (separately) both in x_i and in y_j.

(4) Denote the homogeneous coordinates in $\mathbb{P}^m$ by $(x_0 : x_1 : \dots : x_m)$ and the coordinates in $\mathbb{A}^n$ by $(y_1, y_2, \dots, y_n)$. Check that any closed subset of $\mathbb{P}^m \times \mathbb{A}^n$ is just the set of common zeros of a set of polynomials $S \subseteq \mathbf{K}[x_0, x_1, \dots, x_m, y_0, y_1, \dots, y_n]$, where every polynomial $F \in S$ is homogeneous in x_i.

(5) Prove that the image of the diagonal $\Delta = \{\, (p,p) \mid p \in \mathbb{P}^n \,\}$ under the Segre embedding $\mathbb{P}^n \times \mathbb{P}^n \to \mathbb{S}(n,n)$ coincides with the set $\{\, (z_{ij}) \in \mathbb{S}(n,n) \mid z_{ij} = z_{ji}$ for all $i \neq j \,\}$ (symmetric matrices of rank 1).

(6) Consider all monomials $\mathbf{x}^{\mathbf{k}} = x_0^{k_0} x_1^{k_1} \dots x_n^{k_n}$ of degree d; it is known that there are $\binom{n+d}{n}$ of them. Put $N = \binom{n+d}{n} - 1$. We denote the homogeneous coordinates in $\mathbb{P}^N$ by $w_{\mathbf{k}}$, where $\mathbf{k}$ runs through all $(n+1)$-tuples $(k_0, k_1, \dots, k_n) \in \mathbb{N}^n$ with $\sum_i k_i = d$.

(a) Verify that the rule $\mathbf{a} \mapsto (\mathbf{a}^{\mathbf{k}})$ defines a regular mapping $\rho_d : \mathbb{P}^n \to \mathbb{P}^N$. This mapping is called the (d-fold) *Veronese embedding*.
(b) Prove that $\operatorname{Im} \rho_d = V(S)$, where S is the set of all differences $w_{\mathbf{k}} w_{\mathbf{m}} - w_{\mathbf{r}} w_{\mathbf{s}}$ taken for all $\mathbf{k}, \mathbf{m}, \mathbf{r}, \mathbf{s}$ with $k_i + m_i = r_i + s_i$ for all $i = 0, \dots, n$.
The set $\mathbb{V}(n,d) = V(S)$ is called the (n-dimensional d-fold) *Veronese variety*.
(c) Prove that ρ_d defines an isomorphism of $\mathbb{P}^n$ onto the Veronese variety $\mathbb{V}(n,d)$.
(d) Prove that $X \subset \mathbb{P}^n$ is a hypersurface of degree d if and only if $\rho_d(X) = \mathbb{V}(n,d) \cap H$, where H is a *hyperplane* (i.e., is defined by one linear equation).

(7) Let $X \subseteq \mathbb{P}^n$ be a projective variety, $F \in \mathbf{K}[\mathbf{x}]$ a homogeneous polynomial and $D(F) = \{ a \in X \mid F(a) \neq 0 \}$. Prove that $D(F)$ is an affine variety.
Hint: First check it when F is linear, then use the Veronese embedding.

(8) Check that $\mathbb{V}(1,2)$ is a *conic* (i.e., a plane quadric). Prove that every irreducible projective conic is isomorphic to $\mathbb{P}^1$.

(9) Put $\mathbf{C} = \mathbf{K}[x_0, x_1, x_2]/I(C)$, where C is an irreducible projective conic. Prove that $\mathbf{C} \not\simeq \mathbf{K}[x,y]$. (Thus, the "projective analogue" of Corollary 1.2.3 does not hold.)
Hint: Prove that the maximal ideal $\langle x_0, x_1, x_2 \rangle$ of $\mathbf{C}$ cannot be generated by two elements.

2.4. Separated and complete varieties

We first use the notion of the product to distinguish an important (maybe, the only important) class of algebraic varieties. In some sense, it is the "algebraic analogue" of Hausdorff topological spaces.

DEFINITION 2.4.1. A space with functions X (in particular, an algebraic variety) is called *separated* if the diagonal $\Delta_X = \{ (p,p) \mid p \in X \}$ is closed in $X \times X$.

REMARK. One can easily check that, for "usual" topological spaces, a space X is Hausdorff if and only if the diagonal is closed in $X \times X$ with respect to the product of topologies. So "separated" is indeed a weakened analogue of "Hausdorff."

In view of the definition of the topology on $X \times X$, one can give an "explicit version" of this definition as follows.

PROPOSITION 2.4.2. *A space with functions X is separated if and only if, for every pair of different points $p, q \in X$, there are two open subsets, $U \ni p$ and $V \ni q$, and functions $a_i \in \mathcal{O}_X(U)$, $b_i \in \mathcal{O}_X(V)$ such that $\sum_i a_i(p) b_i(q) \neq 0$ but $\sum_i a_i(z) b_i(z) = 0$ for every $z \in U \cap V$.*

PROOF is evident. □

EXERCISE 2.4.3. Consider the space with functions X defined as follows:

- As the set, $X = \mathbb{A}^1 \cup \{ 0' \}$, where $0'$ is a new symbol.
- A subset $U \subseteq X$ is open in X if and only if $U \setminus \{ 0' \}$ is open in $\mathbb{A}^1$.
- For every function $f : U \to \mathbf{K}$, where $U \subseteq \mathbb{A}^1$, define $\tilde{f}$ as its prolongation to the set $\tilde{U} = U \cup \{ 0' \}$ such that $\tilde{f}(0') = f(0)$.
- For every open subset $U \subseteq \mathbb{A}^1$, put $\mathcal{O}_X(U) = \mathcal{O}_{\mathbb{A}^1}(U)$ and $\mathcal{O}_X(\tilde{U}) = \left\{ \tilde{f} \mid f \in \mathcal{O}_{\mathbb{A}^1}(U) \right\}$.

Check that X is indeed a space with functions; moreover, it is an algebraic variety, which is not separated.

This example ("the affine line with a doubled point") is rather typical for non-separated varieties. We restrict our further considerations by separated varieties only, though we always mention the separation property explicitly. Fortunately, the non-separated varieties cannot occur among "natural ones" as the following proposition show.

PROPOSITION 2.4.4. *Let $(X, \mathcal{O}_X)$ be a separated space with functions, $Y \subseteq X$. Then Y is also separated considered as a space with functions under the restriction from X.*

PROOF is evident. □

COROLLARY 2.4.5. *Any quasi-projective (in particular, any affine or projective) variety is separated.*

PROOF follows from Proposition 2.4.4 and Exercise 2.3.11(5). □

We mention the following useful property of separated varieties.

PROPOSITION 2.4.6. *Let X be a separated algebraic varieties, $Y, Z \subseteq X$ be its affine subvarieties. Then $Y \cap Z$ is also an affine variety.*

PROOF. As we knows, $Y \times Z$ is an affine variety. But $Y \cap Z \simeq (Y \times Z) \cap \Delta_X$. This intersection is closed in $Y \times Z$, hence, is an affine variety too. □

Now we are going to establish an important property of projective varieties, distinguishing them among all quasi-projective ones, namely, their *completeness* in the sense of the following definition.

DEFINITION 2.4.7. A separated algebraic variety X is said to be *complete* if, for any algebraic variety Y, the projection $\mathrm{pr}_Y : X \times Y \to Y$ is a closed mapping, i.e., $\mathrm{pr}_Y(Z)$ is closed for every closed $Z \subseteq X \times Y$.

EXAMPLE 2.4.8. The projection $\mathrm{pr} : \mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1$, $\mathrm{pr}(a, b) = b$, is not closed: the image of the hyperbola $V(xy - 1)$ is $D(x) = \mathbb{A}^1 \setminus \{ 0 \}$, which is not closed. Hence, the affine line is not complete.

On the other hand, the following result is rather obvious.

PROPOSITION 2.4.9. *For any spaces with functions, the projection* $\mathrm{pr}_Y : X \times Y \to Y$ *is open.*

PROOF. It is enough to prove that the image $W = \mathrm{pr}_Y(D(U,V,g))$ is open in Y for every open $U \subseteq X$, $V \subseteq Y$ and any $g = \sum_i a_i \otimes b_i$, where $a_i \in \mathcal{O}_X(U)$, $b_i \in \mathcal{O}_Y(V)$. But this image is the union $\bigcup_{p\in U} W_p$, where all $W_p = \{\, q \in Y \mid \sum_i a_i(p)b_i(q) \neq 0 \,\}$ are open in Y. Hence, W is also open. □

Here are some useful properties of complete varieties.

PROPOSITION 2.4.10. (1) *Any closed subvariety of a complete variety is also complete.*
(2) *If the varieties X, Y are complete, so is $X \times Y$.*
(3) *An algebraic variety X is complete if and only if the projection $\mathrm{pr}_{\mathbb{A}^m} : X \times \mathbb{A}^m \to \mathbb{A}^m$ is closed for every m.*
(4) *If X is a complete and Y is a separated variety, then every regular mapping $f : X \to Y$ is closed.*
(5) *If a quasi-projective variety $X \subseteq \mathbb{P}^n$ is complete, it is closed in $\mathbb{P}^n$ (thus, projective).*
(6) *If a complete variety X is* connected, *then $\mathcal{O}_X(X) = \mathbf{K}$, i.e. the only regular functions on the whole X are constants.*

PROOF. *1* and *2* are obvious.

3. Let first Y be an affine variety, a closed subset of $\mathbb{A}^m$. Then any closed subset $Z \subseteq X \times Y$ is also closed in $X \times \mathbb{A}^m$, hence, $\mathrm{pr}_Y(Z) = \mathrm{pr}_{\mathbb{A}^m}(Z)$ is closed in Y. Now, for any variety Y, there is an open covering $Y = \bigcup_i Y_i$, where Y_i are affine varieties. If Z is a closed subset in $X \times Y$, then $Z = \bigcup_i Z_i$, where $Z_i = Z \cap (X \times Y_i)$, and $\mathrm{pr}_Y(Z) \cap Y_i = \mathrm{pr}_Y(Z_i)$. As we have just proved, each $\mathrm{pr}_Y(Z_i)$ is closed in Y_i, whence $\mathrm{pr}_Y(Z)$ is closed in Y. So the mapping pr_Y is closed.

4. In view of (*1*), it is enough to prove that the image of f is closed in Y. Denote by $\Gamma \subseteq X \times Y$ the *graph* of f, i.e., $\Gamma = \{\, (p, f(p)) \mid p \in X \,\}$. Define a morphism $g : X \times Y \to Y \times Y$ putting $g(p,q) = (f(p), q)$. Then $\Gamma = g^{-1}(\Delta_Y)$, hence, it is closed in $X \times Y$ (as Y is separated). Therefore, $f(X) = \mathrm{pr}_Y(\Gamma)$ is closed.

5 is a partial case of *4*.

6. Let $f : \mathbf{X} \to \mathbf{K}$ be a regular function. Identifying $\mathbf{K}$ with $\mathbb{A}^1_0 \subset \mathbb{P}^1$, we may consider f as a morphism $X \to \mathbb{P}^1$. Hence, $\operatorname{Im} f$ is closed. As it does not coincide with the whole $\mathbb{P}^1$, it is finite: $\operatorname{Im} f = \{\, a_1, a_2, \dots, a_m \,\}$. Then $X = \bigcup_{i=1}^m f^{-1}(a_i)$. As all $f^{-1}(a_i)$ are closed and X is connected, $m = 1$, i.e., f is constant. □

EXAMPLE 2.4.11. Consider the regular mapping $f : \mathbb{A}^2 \to \mathbb{A}^2$, $f(a,b) = (a^2b, ab^2)$. Find its image. Is it closed? open? locally closed?

We shall obtain more information on images of regular mappings in Section 3.1 (Theorem 3.1.17).

THEOREM 2.4.12. *Every projective algebraic variety is complete.*

PROOF. In view of Proposition 2.4.10, we only have to prove that the projection $\mathrm{pr} = \mathrm{pr}_{\mathbb{A}^m} : \mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m$ is closed. We denote the homogeneous coordinates in $\mathbb{P}^n$ by $\mathbf{x} = (x_0 : x_1 : \cdots : x_n)$ and the coordinates in $\mathbb{A}^m$ by $\mathbf{y} = (y_1, y_2, \dots, y_m)$. Let Z be a closed subset of $\mathbb{P}^n \times \mathbb{A}^m$. It coincides with the set of common zeros of a set of polynomials $S = \{ F_1, F_2, \dots, F_r \} \subseteq \mathbf{K}[x_0, x_1, \dots, x_n, y_1, y_2, \dots, y_m]$ which are homogeneous in $x_0, x_1, \dots, x_n$. A point $q \in \mathbb{A}^m$ belongs to $\mathrm{pr}(Z)$ if and only if there is a point $p \in \mathbb{P}^n$ such that $(p, q) \in Z$, i.e., $F_i(p, q) = 0$ for all $i = 1, \dots, r$. Hence, $q \notin \mathrm{pr}(Z)$ if and only if $PV(S_q) = \emptyset$, where $S_q = \{ F_1(\mathbf{x}, q), \dots, F_r(\mathbf{x}, q) \}$. By Projective Hilbert Nullstellensatz (Theorem 2.1.3), it means that $I_+^k \subseteq \langle S_q \rangle$ for some k, i.e., every monomial of degree k can be presented in the form $\sum_{i=1}^r H_i F_i(\mathbf{x}, q)$ for some homogeneous polynomials $H_i(x_0, x_1, \dots, x_n)$. Denote by P_k the vector space of all homogeneous polynomials of degree k from $\mathbf{K}[\mathbf{x}]$. The last condition means that the set

$$\{ w_i F_i(\mathbf{x}, q) \mid i = 1, \dots, r; \\ w_i \text{ runs through all monomials of degree } k - \deg F_i \}$$

generates P_k, or, the same, that $\mathrm{rk}\, M_k = \dim P_k$, where M_k is the matrix whose rows consist of the coefficients of all possible $w_i F_i$ (written in a prescribed order). Denote $D = \dim P_k$. As always $\mathrm{rk}\, M_k \le \dim P_k$, the last condition means that at least one $D \times D$ minor of M_k is non-zero. The entries of the matrix M are polynomials in q, hence, the set $U_k = \{ q \in \mathbb{A}^m \mid \mathrm{rk}\, M_k = \dim P_k \}$ is open in $\mathbb{A}^m$. Therefore, the set $U = \bigcup_{k=1}^\infty U_k$ is also open. But, as we have seen, $U = \mathbb{A}^n \setminus \mathrm{pr}(Z)$, so $\mathrm{pr}(Z)$ is closed. □

There are examples of complete varieties X which are not projective (a fortiori, also not quasi-projective). It is also known (a theorem of Nagata) that every algebraic variety is isomorphic to an open subvariety of a complete variety.

EXERCISES 2.4.13. (1) Prove that if X is a connected complete and Y is an affine variety, then any mapping $f : X \to Y$ is constant (i.e. $\mathrm{Im}\, f$ consists of a unique point).

(2) Let $X \subseteq \mathbb{P}^n$ be an infinite projective variety, $H \subseteq \mathbb{P}^n$ be a hypersurface. Prove that $X \cap H \neq \emptyset$.
Hint: Use the previous exercise as well as Exercise 2.3.11(7).

(3) Consider the set of homogeneous polynomials of degree d in n variables. Identifying F and λF for $\lambda \neq 0$, get a projective space $P(d, n)$. Prove that the set $R(d, n)$ of the classes of *reducible* polynomials is closed in $P(d, n)$.

(4) Find a set of equations defining $R(2, n)$.

2.5. Rational mappings

Now we introduce the so called "*rational mappings*" of algebraic varieties. Indeed, they are *not* mappings of varieties themselves, but of their open dense subsets.

DEFINITION 2.5.1. (1) Let X, Y be algebraic varieties. Denote by $\widetilde{\mathrm{Mor}}(X,Y)$ the set of morphisms $f : U \to Y$, where U is an open subset of X. Call two such morphisms $f : U \to Y$ and $g : V \to Y$ *equivalent* and write $f \sim g$ if $f|_{U\cap V} = g|_{U\cap V}$. A class of equivalence of $\widetilde{\mathrm{Mor}}(X,Y)$ is called a *rational mapping* from X to Y. The set of all rational mappings from X to Y is denoted by $\mathrm{Rat}(X,Y)$.

(2) A rational mapping $X \to \mathbf{K}$ is called a *rational function* on X. The set of all rational functions on X is denoted by $\mathbf{K}(X)$.

(3) One says that a rational mapping $f \in \mathrm{Rat}(X,Y)$ *is defined* at a point $p \in X$ if there is a mapping $\tilde{f} \in \widetilde{\mathrm{Mor}}(X,Y)$ in the class f such that $\tilde{f} : U \to Y$ and $p \in U$. The set of all points $p \in X$ such that f is defined at p is called the *domain of definition* of f and denoted by $\mathrm{Dom}(f)$.

Certainly, $\mathrm{Dom}(f)$ is an open dense subset of X and f can be considered as a morphism $X \to Y$. The points from $\mathrm{Dom}(f)$ are also called the *regular points* and those from the set $\mathrm{Ind}(f) = X \setminus \mathrm{Dom}(f)$ the *special points* of the rational mapping f.

The following proposition give a description of rational functions on an algebraic variety. Note first, that if $U \subseteq X$ is any open dense subset, then evidently, $\mathbf{K}(X) \simeq \mathbf{K}(U)$; the isomorphism is defined by the restriction of functions.

PROPOSITION 2.5.2. (1) *If X is an irreducible algebraic variety, $U \subseteq X$ an open affine subvariety and $\mathbf{A} = \mathbf{K}[U]$, then $\mathbf{K}(X)$ is isomorphic to the field of fractions of the ring $\mathbf{A}$.*

(2) *If $X = \bigcup_{i=1}^{s} X_i$ is the irreducible decomposition of X, then $\mathbf{K}(X) \simeq \prod_{i=1}^{s} \mathbf{K}(X_i)$.*

PROOF. *1.* In this case any non-empty open subset is dense. So we may suppose that $X = U$ is an affine variety with the coordinate algebra $\mathbf{A}$. If a/b, is an element of the field of fractions $\mathbf{Q}$ of $\mathbf{A}$, then f defines a rational function $D(b) \to \mathbf{K}$. Hence, we get a homomorphism $\mathbf{Q} \to \mathbf{K}(X)$. As $\mathbf{Q}$ is a field, it is a monomorphism. Consider any rational function $f \in \mathbf{K}(X)$. The open set $\mathrm{Dom}(f)$ contains a principal open subset $D(g)$ for some $g \in \mathbf{A}$. Moreover, as f is a regular function on $D(g)$, it is of the form a/g^k for some $a \in \mathbf{A}$, $k \in \mathbb{N}$ (cf. Exercises 1.6.6). So f belongs to the image of $\mathbf{Q}$, thus, the inclusion $\mathbf{Q} \to \mathbf{K}(X)$ is an isomorphism.

2. Put $U_i = X \setminus (\bigcup_{j\neq i} X_j)$. It is an open non-empty, hence, dense subset in X_i, so $\mathbf{K}(X_i) = \mathbf{K}(U_i)$. $V = \bigcup_i U_i$ is an open dense subset in X, so $\mathbf{K}(X) = \mathbf{K}(V)$. But as $U_i \cap U_j = \emptyset$ for $i \neq j$, it is evident that $\mathbf{K}(V) = \prod_i \mathbf{K}(U_i)$. □

If $f : X \to Y$ and $g : Y \to Z$ are two rational mappings, we cannot define, in general, their product $g \circ f$, as the whole image of f can belong to the set of special points of g. The latter is impossible if f is *dominant*, which means, by definition, that $f(\mathrm{Dom}(f))$ is dense in Y. Thus, we can always define compositions of *dominant rational* mappings. In particular, a rational mapping $f : X \to Y$ is called *birational* if it is dominant and there is a dominant rational mapping $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$ (as rational mappings). If a birational mapping $X \to Y$ exists, one calls the varieties X and Y *birationally equivalent*. In algebraic geometry they often consider varieties up to birational equivalence further than up to isomorphism. Indeed, to say that X and Y are birationally equivalent is the same as to say that they contain isomorphic open dense subsets (which can always be chosen even affine).

PROPOSITION 2.5.3. *Algebraic varieties X and Y are birationally equivalent if and only if $\mathbf{K}(X) \simeq \mathbf{K}(Y)$.*

PROOF. In view of Proposition 2.5.2, we can suppose X and Y affine and irreducible. Put $\mathbf{A} = \mathbf{K}[X]$ and $\mathbf{B} = \mathbf{K}[Y]$. They are finitely generated $\mathbf{K}$-algebras: $\mathbf{A} = \mathbf{K}[a_1, \dots, a_n]$ and $\mathbf{B} = \mathbf{K}[b_1, \dots, b_m]$. If $U \subseteq X$ and $V \subseteq Y$ are open dense subsets and $U \simeq V$, then $\mathbf{K}(X) \simeq \mathbf{K}(U) \simeq \mathbf{K}(V) \simeq \mathbf{K}(Y)$. On the contrary, let $\varphi : \mathbf{K}(X) \xrightarrow{\sim} \mathbf{K}(Y)$ be an isomorphism, $a_i' = \varphi(a_i)$ and $b_j' = \varphi^{-1}(b_j)$. We consider $\mathbf{K}(X)$ ($\mathbf{K}(Y)$) as the field of fractions of $\mathbf{A}$ (resp., of $\mathbf{B}$) and denote by d (resp., by c) a common denominator of all a_i' (resp., b_j'). Then a_i' are regular functions on $V = D(d)$ and b_j are regular functions on $U = D(c)$. They define regular mappings $f : V \to X$ and $g : U \to Y$ correspondingly, such that $f^*(a_i) = a_i'$ and $g^*(b_j) = b_j'$. Hence, $g \circ f = \mathrm{id}$ on $V \cap g^{-1}(U)$ and $f \circ g = \mathrm{id}$ on $U \cap f^{-1}(V)$, i.e., considered as rational mappings, they are birational. □

The following result is rather simple, but often useful.

PROPOSITION 2.5.4. *Any irreducible algebraic variety is birationally equivalent either to an affine (to a projective) space or to an affine (to a projective) hypersurface.*

PROOF. The field $\mathbf{Q}$ of rational functions on an irreducible variety X is always a finitely generated extension of $\mathbf{K}$. By Proposition A.4, there are two possible cases:

1) $\mathbf{Q} \simeq \mathbf{K}(x_1, \dots, x_n)$. Then X is birationally equivalent to $\mathbb{A}^n$ (and to $\mathbb{P}^n$).

2) $\mathbf{Q} = \mathbf{K}(\alpha_1, \dots, \alpha_n)$, where $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ are algebraically independent over $\mathbf{K}$ and α_n is algebraic over $\mathbf{R} = \mathbf{K}(\alpha_1, \dots, \alpha_{n-1})$. Moreover, in this case there is a unique irreducible polynomial F such that $F(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$ (cf. Lemma A.2). Put $Y = V(F) \subset \mathbb{A}^n$. Then $I(Y) = I = \langle F \rangle$ and $\mathbf{K}[Y] = \mathbf{K}[\xi_1, \xi_2, \dots, \xi_n]$ for $\xi_i = x_i + I$. As F cannot divide any polynomial in $x_1, x_2, \dots, x_{n-1}$, $\xi_1, \xi_2, \dots, \xi_{n-1}$ are algebraically independent in $\mathbf{K}(Y)$. So $\mathbf{K}(Y) \simeq \mathbf{Q}$, whence Y is birationally equivalent to X. □

EXERCISES 2.5.5. (1) One calls a variety X *rational* if it is birationally equivalent to an affine (or, the same, to a projective) space. Prove that:
 (a) The product of rational varieties is rational.
 (b) Any irreducible conic is rational.
 (c) The nodal cubic $V(y^2 - x^3 - x^2)$ as well as the cuspidal cubic $V(y^2 - x^3)$ are rational.
 Hint: It can be useful to consider the projective closure of the nodal cubic and another affine part of this closure.

(2) Prove that if $X, Y\mathbb{P}^2$ are plane projective curves, then $X \cap Y \neq \emptyset$. Deduce that $\mathbb{P}^1 \times \mathbb{P}^1 \not\simeq \mathbb{P}^2$.

(3) Prove that the *quadratic Cremona transformation* $\varphi : \mathbb{P}^2 \to \mathbb{P}^2$, $\varphi(x_0 : x_1 : x_2) = (x_1x_2 : x_0x_2 : x_0x_1)$ is birational. Find $\mathrm{Dom}(\varphi)$ and $\mathrm{Dom}\,\varphi^{-1}$.

2.6. Grassmann varieties and vector bundles

The projective space $\mathbb{P}^{n-1}$ can be considered as the set of all one-dimensional linear subspaces of $\mathbf{K}^n$. We are going now to implement the structure of a projective variety into the set of all subspaces of dimension d of $\mathbf{K}^n$ for arbitrary d. To do it, we use the so called *Grassmann coordinates* of such subspaces (sometimes they are also called the *Plücker coordinates*). Put $N = \binom{n}{d} - 1$ and fix some order on the set of all d-tuples $k_1k_2\dots k_d$ with $1 \le k_1 < k_2 < \dots < k_d \le n$ (there are just $N+1$ of them).

DEFINITION 2.6.1. Let V be a d-dimensional subspace of $\mathbf{K}^n$ with a basis $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_d$, where $\mathbf{v}_k = (a_{k1}, \dots, a_{kn})$. The *Grassmann coordinates* of V determined by this basis are defined as the vector $(p_{k_1k_2\dots k_d})$, where

$$p_{k_1k_2\dots k_d} = \begin{vmatrix} a_{1k_1} & a_{1k_2} & \dots & a_{1k_d} \\ a_{2k_1} & a_{2k_2} & \dots & a_{2k_d} \\ \dots & \dots & \dots & \dots \\ a_{dk_1} & a_{dk_2} & \dots & a_{dk_d} \end{vmatrix}. \tag{2.6.1}$$

PROPOSITION 2.6.2. *If* $(p_{k_1k_2\dots k_d})$ *and* $(p'_{k_1k_2\dots k_d})$ *are Grassmann coordinates of the same subspace* V *determined by two bases, there* *is a non-zero* $\lambda \in \mathbf{K}$ *such that* $p'_{k_1k_2\dots k_d} = \lambda p_{k_1k_2\dots k_d}$ *for all* d*-tuples* $k_1k_2\dots k_d$ *.*

Proof. Indeed, if $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_d$ and $\mathbf{v}'_1, \mathbf{v}'_2, \dots, \mathbf{v}'_d$ are the bases determining these coordinates, there is an invertible $d \times d$ matrix A such that $A\,(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_d)^\top = (\mathbf{v}'_1, \mathbf{v}'_2, \dots, \mathbf{v}'_d)^\top$. Then, for every d-tuple $k_1k_2\dots k_d$, $p'_{k_1k_2\dots k_d} = (\det A) p_{k_1k_2\dots k_d}$. □

Hence, if we consider the point of the projective space corresponding to the Grassmann coordinates of a subspace V , it does not depend on the choice of a basis in V . So we obtain a mapping γ from the set $\mathbb{G}\mathsf{r}(d,n)$ of all subspaces of dimension d to $\mathbb{P}^N$. We denote the homogeneous coordinates in $\mathbb{P}^N$ by $x_{k_1k_2\dots k_d}$ ($1 \le k_1 < k_2 < \dots < k_d \le n$). The following theorem shows that this mapping is injective and its image is a projective variety. Remark first that the formula (2.6.1) define $p_{k_1k_2\dots k_d}$ for any d-tuple $k_1k_2\dots k_d$ with $1 \le k_i \le n$, but all of them can be calculated through Grassmann coordinates and the "alternating rules": $p_{k_1k_2\dots k_d} = 0$ if $k_i = k_j$ for some $i \ne j$ and $p_{k_1k_2\dots k_d} = -p_{k'_1k'_2\dots k'_d}$ if the d-tuple $k'_1k'_2\dots k'_d$ is obtained from $k_1k_2\dots k_d$ by transposing two elements.

Theorem 2.6.3. (1) *If* $(p_{k_1k_2\dots k_d})$ *are Grassmann coordinates of a subspace* V *, then* V *coincides with the set of all vectors* $\mathbf{v} = (a_1, a_2, \dots, a_n)$ *such that*

$$\sum_{i=1}^{d+1} (-1)^{i-1} a_{k_i} p_{k_1\dots\check{k}_i\dots k_{d+1}} = 0 \ \text{ for all } (d+1)\text{-tuples} \quad k_1k_2\dots k_{d+1} \text{ with } 1 \le k_1 < k_2 < \dots < k_{d+1} \le n. \tag{2.6.2}$$

In particular, different subspaces have different Grassmann coordinates.

(2) $\operatorname{Im}\gamma = PV(S)$ *, where* S *is the set of all equations of the following form:*

$$\sum_{i=1}^{d+1} (-1)^{i-1} x_{k_1k_2\dots k_{d-1}l_i} x_{l_1\dots\check{l}_i\dots l_{d+1}} = 0\,, \tag{2.6.3}$$

for all possible $1 \le k_1 < \dots < k_{d-1} \le n$ and $1 \le l_1 < \dots < l_{d+1} \le n$.

Proof. *1*. Suppose that the Grassmann coordinates have been determined via a basis $(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_d)$. Then $\mathbf{v} \in V$ if and only if the rank of the matrix with the rows $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_d, \mathbf{v}$ equals d . It means that all its $(d+1) \times (d+1)$-minors equal 0 . But the last condition coincides with the equations (2.6.2).

2. If $p=(p_{k_1k_2\dots k_d})$ is given by the formula (2.6.1), then we have: $p_{k_1k_2\dots k_{d-1}l_i}=\sum_{j=1}^d A_j a_{jl_i}$, where

$$A_j=(-1)^{d+j}\begin{vmatrix} a_{1k_1} & \dots & a_{1k_{d-1}} \\ \dots & \dots & \dots \\ a_{(j-1)k_1} & \dots & a_{(j-1)k_{d-1}} \\ a_{(j+1)k_1} & \dots & a_{(j+1)k_{d-1}} \\ \dots & \dots & \dots \\ a_{dk_1} & \dots & a_{dk_{d-1}} \end{vmatrix}$$

does not depend on i . Therefore,

$$\sum_{i=1}^{d+1}(-1)^{i-1}p_{k_1k_2\dots k_{d-1}l_i}p_{l_1\dots\check{l}_i\dots l_{d+1}}=\sum_{j=1}^{d}A_j\sum_{i=1}^{d+1}(-1)^{i-1}a_{jl_i}p_{l_1\dots\check{l}_i\dots l_{d+1}}\,.$$

But

$$\sum_{i=1}^{d+1}(-1)^{i-1}a_{jl_i}p_{l_1\dots\check{l}_i\dots l_{d+1}}=\begin{vmatrix} a_{jl_1} & \dots & a_{jl_{d+1}} \\ a_{1l_1} & \dots & a_{1l_{d+1}} \\ \dots & \dots & \dots \\ a_{dl_1} & \dots & a_{dl_{d+1}} \end{vmatrix}=0$$

as this determinant has two equal rows. Hence, $p\in PV(S)$.

Let now $p\in PV(S)$. Fix some d-tuple $k_1k_2\dots k_d$ such that $p_{k_1k_2\dots k_d}\neq 0$. For the sake of simplicity, we suppose that $k_1k_2\dots k_d=12\dots d$ and $p_{12\dots d}=1$. Consider the subspace V with the basis $\mathbf{v}_1,\mathbf{v}_2,\dots,\mathbf{v}_d$ such that the coordinates a_{ki} of $\mathbf{v}_k$ are the following:

$$a_{ki}=\begin{cases}1 & \text{if } i=k\le d\,,\\ 0 & \text{if } i\neq k\le d\,,\\ (-1)^{d-i}p_{1\dots\check{i}\dots dk} & \text{if } k>d\,.\end{cases}$$

Denote by $q=(q_{k_1k_2\dots k_d})$ the Grassmann coordinates of V . Evidently, $q_{12\dots d}=1$ and $q_{1\dots\check{i}\dots dk}=p_{1\dots\check{i}\dots dk}$ for each k . Prove that $q_{k_1k_2\dots k_d}=p_{k_1k_2\dots k_d}$ for any $k_1k_2\dots k_d$. Denote by m the number of indices from $k_1k_2\dots k_d$ which are greater than d and use the induction on m . The cases $m\le 1$ have just been considered. Suppose that the claim is valid for all d-tuples with the smaller value of m . Take, in the d-tuple $k_1k_2\dots k_d\neq 12\dots d$, some index $k_j>d$. Then, in view of (2.6.3) for $k_1\dots\check{k}_j\dots k_d$ and $12\dots dk_j$,

$$q_{k_1k_2\dots k_d}=(-1)^{d-j}q_{k_1\dots\check{k}_j\dots k_dk_j}q_{12\dots d}=\sum_{i\neq j}(-1)^{i+j}q_{k_1\dots\check{k}_j\dots k_di}q_{1\dots\check{i}\dots dk_j}\,.$$

Evidently, all d-tuples occurring in the latter sum have smaller value of m . Hence, the corresponding coordinates of q coincide with those of p . Thus, also $q_{k_1k_2\dots k_d}=p_{k_1k_2\dots k_d}$, so $p=q\in\operatorname{Im}\gamma$. $\square$

We always identify $\mathbb{G}\mathsf{r}(d,n)$ with its image in $\mathbb{P}^N$, hence, consider it as a projective variety (called the *Grassmann variety* or *Grassmannian*). On the other hand, we identify every point of the Grassmannian with the corresponding subspace.

PROPOSITION 2.6.4. *For every d,n, the Grassmann variety $\mathbb{G}\mathsf{r}(d,n)$ is irreducible.*

PROOF. Consider in the affine space of all $d\times n$ matrices the open subset U of the matrices of rank d. It is irreducible as $\mathbb{A}^{dn}$ is irreducible. But the formulae (2.6.1) define a surjective morphism $U\to\mathbb{G}\mathsf{r}(d,n)$. Hence, $\mathbb{G}\mathsf{r}(d,n)$ is also irreducible as the image of an irreducible space under a continuous mapping. $\square$

EXERCISES 2.6.5.

(1) Let W be an m-dimensional subspace in $\mathbf{K}^n$. Prove that, for each r, $\{\, V\in\mathbb{G}\mathsf{r}(d,n) \mid \dim(V+W)\le r \,\}$ is closed in $\mathbb{G}\mathsf{r}(d,n)$. In particular, the following subsets are closed:
   (a) $\{\, V\in\mathbb{G}\mathsf{r}(d,n) \mid V+W\ne\mathbf{K}^n \,\}$,
   (b) $\{\, V\in\mathbb{G}\mathsf{r}(d,n) \mid V\cap W\ne\{\,0\,\} \,\}$.
   Note that, if $d+m\ge n$, the set (a), and if $d+m\le n$, the set (b) does not coincide with the whole $\mathbb{G}\mathsf{r}(d,n)$. As $\mathbb{G}\mathsf{r}(d,n)$ is irreducible, it means that they are "very small": there complements are open and dense.
(2) Let $d'<d$. Prove that the set $\{\,(V,W) \mid W\subset V\,\}$ is closed in $\mathbb{G}\mathsf{r}(d,n)\times\mathbb{G}\mathsf{r}(d',n)$.
(3) A *flag* of type $(d_1,d_2,\dots,d_m)$, where $0<d_1<d_2<\dots<d_m<n$ is a tower of subspaces $\{\,0\}\subset V_1\subset V_2\subset\dots\subset V_m\subset\mathbf{K}^n$ such that $\dim V_i=d_i$ for $i=1,\dots,m$. Show that the set of all flags of a prescribed type can be considered as a projective variety.

Grassmann varieties are closely related to *vector bundles*.

DEFINITION 2.6.6. A *vector bundle* of rank d on an algebraic variety X is a morphism $\xi : B\to X$ such that the following conditions hold:

(1) There is an open covering $X=\bigcup_i U_i$ and isomorphisms $\varphi_i : U_i\times\mathbf{K}^d \xrightarrow{\sim} \xi^{-1}(U_i)$ such that $\xi\circ\varphi_i=\mathrm{pr}_X$ on U_i.
(2) For each pair i,j, there is a regular mapping $\theta_{ij} : U_i\cap U_j\to \mathrm{GL}(d,\mathbf{K})$ such that, for every point $(p,v)\in(U_i\cap U_j)\times\mathbf{K}^d$, $\varphi_i^{-1}\circ\varphi_j(p,v)=(p,\theta_{ij}(p)v)$.

The data $\{\,U_i,\varphi_i,\theta_{ij}\,\}$ are called a *trivialization* of the vector bundle ξ. (Obviously, the mappings θ_{ij} can be uniquely recovered by $\{\,U_i,\varphi_i\,\}$.)

The simplest example of a vector bundle is, of course, the projection pr_X of the product $X\times\mathbf{K}^d$. In what follows, we speak of this product as of vector bundle, not mentioning the projection explicitly. Given a vector bundle ξ, we consider every fibre $\xi^{-1}(p)$ as a d-dimensional vector space using the isomorphism $\xi^{-1}(p) \simeq \mathbf{K}^d$ induced by φ_i, where $p \in U_i$. Note that the choice of another $U_j \ni p$ gives an isomorphic structure of vector space on $\xi^{-1}(p)$. Certainly, if we subdivide the open subsets U_i: $U_i = \bigcup_k V_{ik}$ for some open V_{ik}, then the restrictions of φ_i and θ_{ij} onto this subdivision also define a trivialization of ξ. In particular, dealing with several vector bundles on X, we can always consider their trivializations with a *common* open covering of X.

Definition 2.6.7. Given two vector bundles $\xi : B \to X$ and $\xi' : B' \to X$ of ranks, respectively, d and d', with trivializations, respectively, $\{ U_i, \varphi_i \}$ and $\{ U_i, \varphi'_i \}$, a *morphism of vector bundles* from ξ to ξ' is defined as a regular mapping $f : B \to B'$ such that $\xi = \xi' \circ f$ and, for every i, there is a regular mapping $g_i : U_i \to \mathrm{Mat}(d' \times d, \mathbf{K})$ such that, for every point $(p, v) \in U_i \times \mathbf{K}^d$, $\varphi_i'^{-1} \circ f \circ \varphi_i(p, v) = (p, g_i(p)v)$.

In particular, if $B \subseteq B'$ and the embedding $B \to B'$ is a morphism of vector bundles, one calls ξ a *sub-bundle* of ξ'.

One can check that if this condition hold for *some* trivializations, it holds also for *any* trivializations of ξ and xi'. In particular, one has a notion of *isomorphism* of vector bundles. A vector bundle isomorphic to the product $X \times \mathbf{K}^n$ is called *trivial*. The first condition from the definition show that every vector bundle is "*locally trivial*": its restriction on each U_i from a trivialization is indeed trivial.

Example 2.6.8. Let $\mathbb{G} = \mathbb{G}\mathsf{r}(d, n)$. Consider the following subset $\mathbb{B} = \mathbb{B}(d, n) \subseteq \mathbb{G} \times \mathbf{K}^n$: $\mathbb{B} = \{ (p, v) \,|\, v \in V_p \}$, where V_p denote the d-dimensional subspace of $\mathbf{K}^n$ corresponding to the point $p \in \mathbb{G}$. Theorem 2.6.3(1) shows that $\mathbb{B}$ is closed in $\mathbb{G} \times \mathbf{K}^n$, so it is an algebraic (even quasi-projective) variety. Denote by $\pi = \pi(d, m) : \mathbb{B} \to \mathbb{G}$ the restriction on $\mathbb{B}$ of $\mathrm{pr}_{\mathbb{G}}$. Check that $\pi\mathbb{B} \to \mathbb{G}$ is a vector bundle of rank d.

Namely, for every d-tuple $\mathbf{k} = k_1 k_2 \dots k_d$ ($1 \le k_1 < k_2 < \dots < k_d \le n$), put $\mathbb{G}_{\mathbf{k}} = D(x_{\mathbf{k}})$ (the canonical affine covering of $\mathbb{G}$) and $\mathbb{B}_{\mathbf{k}} = \pi^{-1}(\mathbb{G}_{\mathbf{k}})$. For every point $p \in \mathbb{G}_{\mathbf{k}}$, denote by $\{ \mathbf{v}_1^p, \mathbf{v}_2^p, \dots, \mathbf{v}_d^p \}$ the basis of V_p, such that the j-th coordinate of $\mathbf{v}_i^p$ is $p_{k_1 \dots j \dots k_d}$ (j is on the i-th place). (This basis coincide, up to the multiple $p_{\mathbf{k}}$, with that constructed in the proof of Theorem 2.6.3(2)). Then the rule: $\gamma_{\mathbf{k}}(p, (\lambda_1, \lambda_2, \dots, \lambda_d)) = (p, \sum_{i=1}^d \lambda_i \mathbf{v}_i^p)$ define an isomorphism $\gamma_{\mathbf{k}} : \mathbb{G}_{\mathbf{k}} \times \mathbf{K}^n \xrightarrow{\sim} \mathbb{B}_{\mathbf{k}}$ such that $\pi \circ \gamma = \mathrm{pr}_{\mathbb{G}}$. Moreover, one can easily see that, if $p \in \mathbb{G}_{\mathbf{k}} \cap \mathbb{G}_{\mathbf{l}}$ and $\{ \mathbf{u}_1^p, \mathbf{u}_2^p, \dots, \mathbf{u}_d^p \}$ is the basis of V_p constructed with respect to $\mathbb{G}_{\mathbf{l}}$, then $\mathbf{u}_j^p = \sum_{i=1}^d p_{\mathbf{k}}^{-1} p_{l_1 \dots k_i \dots l_d} \mathbf{v}_i^p$ (k_i is on the j-th place). It gives the necessary regular mappings $(\mathbb{G}_{\mathbf{k}} \cap \mathbb{G}_{\mathbf{l}}) \to \mathrm{GL}(d, \mathbf{K})$.

Again we often speak of $\mathbb{B}(d, n)$ as of vector bundle on $\mathbb{G}\mathsf{r}(d, n)$ without mentioning $\gamma(d, n)$ explicitly.

The vector bundle $\pi : \mathbb{B}(d,n) \to \mathbb{G}(d,n)$ is called the *canonical vector bundle* on the Grassmannian $\mathbb{G}(d,n)$. The following considerations show its special role in the theory of vector bundles.

PROPOSITION 2.6.9. *Let $\xi : B \to X$ be a vector bundle of rank d and $f : Y \to X$ be a regular mapping. Denote by $f * (B)$ the subset $\{ (y,b) \mid f(y) = \xi(b) \} \subseteq Y \times B$ and by $f^*(\xi)$ the restriction onto $f^*(B)$ of the projection pr_Y. Then $f^*(\xi) : f^*(B) \to Y$ is also a vector bundle of rank d.*
The vector bundle $f^*(\xi)$ is called the *inverse image* of ξ under f.

PROOF. Let $\{ U_i, \varphi_i, \theta_{ij} \}$ be a trivialization of ξ. Put $V_i = f^{-1}(U_i)$ and, for every point $y \in V_i$, $\psi_i(y,v) = (y, \varphi_i(f(y),v))$. This pair belongs to $f^*(B)$ as $\xi \circ \varphi_i(f(y),v) = \mathrm{pr}_X(f(y),v) = f(y)$. At last, put $\tau_{ij} = \theta_{ij} \circ f : V_i \cap V_j \to \mathrm{GL}(d, \mathbf{K})$. Then one can check that $\{ V_i, \psi_i, \tau_{ij} \}$ is a trivialization of $f^*(\xi)$ (we remain it to the reader). □

If $B = X \times \mathbf{K}^d$ is a trivial vector bundle, its inverse image under f is canonically isomorphic to the trivial vector bundle $Y \times \mathbf{K}^d$: one should map a point (y,p,v) from $f^*(B)$ to (y,v) (note that $p = f(y)$). We always identify these vector bundles.

Note that $\mathbb{B}(d,n)$ has arisen as a sub-bundle of the trivial bundle $\mathbb{G} \times \mathbf{K}^n$. It happens that the vector bundles $\mathbb{B}(d,n)$ are indeed the "*universal*" examples of sub-bundles of trivial bundles.

THEOREM 2.6.10. *Suppose that $\xi : B \to X$ is a sub-bundle of the trivial vector bundle $X \times \mathbf{K}^n$. Then there is a unique morphism $f : X \to \mathbb{G}\mathsf{r}(d,n)$ such that $B = (f \times 1)^{-1}(\mathbb{B}(d,n))$, where $\mathbb{B}(d,n)$ is considered as subset of $\mathbb{G}\mathsf{r}(d,n) \times \mathbf{K}^n$.*

PROOF. For every point $p \in X$, $\xi^{-1}(p)$ is a d-dimensional subspace of $\mathbf{K}^n$. Denote by $f(p)$ the corresponding point of $\mathbb{G}\mathsf{r}(d,n)$. Then, obviously, $B = (f \times 1)^{-1}(\mathbb{B}(d,n))$, so one only has to check that the mapping $f : X \to \mathbb{G}\mathsf{r}(d,n)$ is regular.

Consider a trivialization $\{ U_i, \varphi_i, \theta_{ij} \}$ of ξ. If $\{ \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_d \}$ is a basis of $\mathbf{K}^d$, then $\{ \varphi_i(\mathbf{e}_1), \dots, \varphi_i(\mathbf{e}_d) \}$ is a basis of $\xi^{-1}(p)$ for every $p \in U_i$. Moreover, as φ_i is regular, the coordinates of the vectors $\varphi_i(\mathbf{e}_j)$ are regular functions on U_i. Hence, the Grassmann coordinates of the subspace $\xi^{-1}(p)$, i.e., the coordinates of the point $f(p)$ are regular functions on U_i. So f is indeed regular. □

A. Appendix: Degree of transcendence

Remind the main facts concerning algebraic dependence and degree of transcendence. In what follows, $\mathbf{Q} \supseteq \mathbf{K}$ is an extension of fields (we do not suppose $\mathbf{K}$ being algebraically closed).

DEFINITIONS A.1. (1) A set $S \subseteq \mathbf{Q}$ is called *algebraically independent* (over $\mathbf{K}$) if $F(\alpha_1, \alpha_2, \dots, \alpha_n) \neq 0$ for any elements

$\alpha_1, \alpha_2, \dots, \alpha_n \in S$ and any non-zero polynomial $F \in \mathbf{K}[\mathbf{x}]$. Otherwise S is called *algebraically dependent*.

(2) The *degree of transcendence* of $\mathbf{Q}$ (over $\mathbf{K}$) is, by definition, the maximal cardinality of algebraically independent subsets $S \subseteq \mathbf{Q}$ (number of elements in S, if it is finite). It is denoted by $\operatorname{tr.deg}(\mathbf{Q}/\mathbf{K})$ or $\operatorname{tr.deg}\mathbf{Q}$ if $\mathbf{K}$ is fixed.

(3) A subset $S \subseteq \mathbf{Q}$ is called a *transcendence base* of $\mathbf{Q}$ (over $\mathbf{K}$) if it is algebraically independent and $\mathbf{Q}$ is an algebraic extension of $\mathbf{K}(S)$.

(4) $\mathbf{Q}$ is called *pure transcendent* over $\mathbf{K}$ if it is isomorph to the field of rational functions $\mathbf{K}(x_1, \dots, x_n)$ for some n.

Certainly, $\operatorname{tr.deg}(\mathbf{Q}/\mathbf{K}) = 0$ if and only if $\mathbf{Q}$ is an algebraic extension of $\mathbf{K}$.

Lemma A.2. *Suppose that the set $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq \mathbf{Q}$ is algebraically independent and the set $\{\alpha_1, \alpha_2, \dots, \alpha_n, \beta\}$ is algebraically dependent. Then:*

(1) *There is a unique (up to a scalar multiple) irreducible polynomial $F \in \mathbf{K}[x_1, \dots, x_{n+1}]$ such that $F(\alpha_1, \alpha_2, \dots, \alpha_n, \beta) = 0$.*

(2) *For every $i = 0, 1, \dots, n$, either β is algebraic over $\mathbf{K}(\alpha_1, \dots, \check{\alpha}_i, \dots, \alpha_n)$ or the set $\{\alpha_1, \dots, \check{\alpha}_i, \dots, \alpha_n, \beta\}$ is algebraically independent, while α_i is algebraic over $\mathbf{K}(\alpha_1, \dots, \check{\alpha}_i, \dots, \alpha_n, \beta)$.*

Proof. *1*. The existence of F is evident. Let G be another irreducible polynomial such that $G(\alpha_1, \alpha_2, \dots, \alpha_n, \beta) = 0$. If $G \neq \lambda F$ for any $\lambda \in \mathbf{K}$, they are coprime in $\mathbf{K}[x_1, \dots, x_{n+1}]$, hence, also in $\mathbf{K}(x_1, \dots, x_n)[x_{n+1}]$. Therefore, there are two polynomials $A, B \in \mathbf{K}(x_1, \dots, x_n)[x_{n+1}]$ such that $AF + BG = 1$. Multiplying by the common denominator, we get an equality $CF + DG = H$, where $C, D \in \mathbf{K}[x_1, \dots, x_{n+1}]$ and $H \in \mathbf{K}[x_1, \dots, x_n]$. Hence, $H(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$, which is impossible.

2. Suppose that β is not algebraic over $\mathbf{K}(\alpha_1, \dots, \check{\alpha}_i, \dots, \alpha_n)$. Then the irreducible polynomial F such that $F(\alpha_1, \alpha_2, \dots, \alpha_n, \beta) = 0$ contains x_i, whence α_i is algebraic over $\mathbf{K}(\alpha_1, \dots, \check{\alpha}_i, \dots, \alpha_n, \beta)$. Suppose that the set $\{\alpha_1, \dots, \check{\alpha}_i, \dots, \alpha_n, \beta\}$ is algebraically dependent. Then $G(\alpha_1, \dots, \check{\alpha}_i, \dots, \alpha_n, \beta) = 0$ for some irreducible polynomial $G(x_1, \dots, \check{x}_i, \dots, x_{n+1})$, which contradicts (*1*), as $G \neq \lambda F$ for any $\lambda \in \mathbf{K}$. □

Corollary A.3. (1) *If S is a transcendence base of $\mathbf{Q}$ and T is any algebraically independent subset, then $\#(T) \leq \#(S)$.*

(2) *For any transcendence base S, $\#(S) = \operatorname{tr.deg}\mathbf{Q}$.*

(3) *In a tower of field extensions, $\mathbf{K} \subseteq \mathbf{Q} \subseteq \mathbf{L}$, if S is a transcendence base of $\mathbf{L}$ over $\mathbf{Q}$ and T is a transcendence base of $\mathbf{Q}$ over $\mathbf{K}$, then $S \cup T$ is a transcendence base of $\mathbf{L}$ over $\mathbf{K}$.*

(4) $\operatorname{tr.deg}(\mathbf{L}/\mathbf{K}) = \operatorname{tr.deg}(\mathbf{L}/\mathbf{Q}) + \operatorname{tr.deg}(\mathbf{Q}/\mathbf{K})$.

PROOF. We only consider the case when both S and T are finite sets (we need not other ones). Let $S = \{ \alpha_1, \alpha_2, \dots, \alpha_n \}$, $T = \{ \beta_1, \beta_2, \dots, \beta_m \}$.

1. We prove (by induction on k) that, up to a permutation of the elements of S , the sets $S_k = \{ \beta_1, \beta_2, \dots, \beta_k, \alpha_{k+1}, \dots, \alpha_n \}$ are transcendence bases too. It is true for $S_0 = S$. Suppose that it is true for S_k . In particular, S_k is algebraically independent, while $S_k \cup \{ \beta_{k+1} \}$ is algebraically dependent. As β_{k+1} is not algebraic over $\mathbf{K}(\beta_1, \dots, \beta_k)$, Proposition A.2 implies that, for some i ($k < i \le n$), the set $S' = (S_k \cup \{ \beta_{k+1} \}) \setminus \{ \alpha_i \}$ is algebraically independent, while α_i is algebraic over $\mathbf{K}(S')$. Hence, S' is a transcendence base of $\mathbf{Q}$. As we have allowed permutations, we may suppose that $i = k+1$, i.e. $S' = S_{k+1}$.

Now the claim is obvious, as, if $m > n$, we get that β_{n+1} is algebraic over $\mathbf{K}(\beta_1, \dots, \beta_n)$, which is impossible.

2 obviously follows from *1*.

3. $\mathbf{L}$ is algebraic over $\mathbf{Q}(S)$ and $\mathbf{Q}$ is algebraic over $\mathbf{K}(T)$. Hence, $\mathbf{Q}(S)$ and, a fortiori, also $\mathbf{L}$ are algebraic over $\mathbf{K}(S \cup T)$. On the other hand, as T is algebraically independent over $\mathbf{K}$, $\mathbf{K}(T) \simeq \mathbf{K}(x_1, \dots, x_m)$ and, as S is algebraically independent over $\mathbf{K}(T)$, $\mathbf{K}(S \cup T) \simeq \mathbf{K}(T)(x_1, \dots, x_n) \simeq \mathbf{K}(x_1, \dots, x_{m+n})$, i.e., $S \cup T$ is algebraically independent over $\mathbf{K}$.

4 is an obvious consequence of *3*. ☐

We shall also use the following result.

PROPOSITION A.4. *Let $\mathbf{Q}$ be a finitely generated extension of an algebraically closed field $\mathbf{K}$, $n = \operatorname{tr.deg}(\mathbf{Q}/\mathbf{K})$ and $\mathbf{R} = \mathbf{K}(x_1, \dots, x_n)$. Then either $\mathbf{Q} \simeq \mathbf{R}$ or $\mathbf{Q} \simeq \mathbf{R}(\alpha)$, where α is algebraic and separable over $\mathbf{R}$.*

PROOF. Let $\mathbf{Q} = \mathbf{K}(\alpha_1, \dots, \alpha_m)$. We use the induction on m . For $m = 1$, the claim is obvious. Suppose that it holds for $\mathbf{L} = \mathbf{K}(\alpha_1, \dots, \alpha_{m-1})$. Put $l = \operatorname{tr.deg}(\mathbf{L}/\mathbf{K})$ and $\mathbf{S} = \mathbf{K}(x_1, \dots, x_l)$. Then we can suppose that either $\mathbf{L} = \mathbf{S}$ or $\mathbf{L} = \mathbf{S}(\beta)$ with β algebraic and separable over $\mathbf{S}$. In the first case, $\mathbf{Q} = \mathbf{S}(\alpha_m)$, in the second one $\mathbf{Q} = \mathbf{S}(\beta, \alpha_m)$. If α_m is transcendent over $\mathbf{S}$, the claim is obvious as $\mathbf{S}(\alpha_m) \simeq \mathbf{R}$. So suppose that α_m is algebraic over $\mathbf{S}$ (hence, $l = n$). Then there is an element $\gamma \in \mathbf{Q}$ such that $\mathbf{Q} = \mathbf{S}(\gamma)$: in the first case $\gamma = \alpha_m$, in the second one its existence follows from the theorem on primitive element in an algebraic extension (as β is separable).

Consider the irreducible polynomial $F \in \mathbf{K}[x_1, \dots, x_{n+1}]$ such that $F(x_1, x_2, \dots, x_n, \gamma) = 0$. If $\partial F / \partial x_{n+1} \ne 0$, γ is separable over $\mathbf{S} = \mathbf{R}$. If $\partial F / \partial x_i \ne 0$ for some $i \le n$, we can replace x_i by γ and vice versa. Suppose that $\partial F / \partial x_i = 0$ for all i . It is impossible if $\operatorname{char} \mathbf{K} = 0$. If $\operatorname{char} \mathbf{K} = p > 0$, it means that indeed

$F = G(x_1^p, x_2^p, \dots, x_{n+1}^p)$ for some polynomial G. But then $F = H^p$, where H is obtained from G by replacing each coefficient by the p-th root of it. It is again impossible as F is irreducible. $\square$

REMARK. Indeed, we have only used the fact that $\mathbf{K}$ is *perfect*, i.e., either $\operatorname{char} \mathbf{K} = 0$ or $\operatorname{char} \mathbf{K} = p > 0$ and the equation $x^p = a$ has a solution for every $a \in \mathbf{K}$.

CHAPTER 3

Dimension Theory

3.1. Finite morphisms

The source point of the dimension theory of algebraic varieties is Noether's Normalization Lemma (Theorem 1.4.3). As we are going to use it for abstract varieties, we first introduce the corresponding definitions.

DEFINITIONS 3.1.1. (1) An extension of rings $\mathbf{A} \supseteq \mathbf{B}$ is called *finite* if $\mathbf{A}$ is finitely generated as $\mathbf{B}$-module. (Equivalently, in view of Exercise 1.4.11(2), $\mathbf{A} = \mathbf{B}[\, b_1, b_2, \dots, b_m \,]$, where all b_i are integral over $\mathbf{A}$).

(2) A morphism $f : Y \to X$ of algebraic varieties is said to be *finite* if every point $p \in X$ has an affine neighbourhood U such that $f^{-1}(U)$ is also affine and $\mathcal{O}_Y(f^{-1}(U))$ is a finite extension of $\operatorname{Im} f^*(U)$.

REMARK. (1) If $\mathbf{A} \supseteq \mathbf{B}$ is a finite extension and the ring $\mathbf{B}$ is noetherian, the ring $\mathbf{A}$ is a noetherian $\mathbf{B}$-module by Proposition 1.4.6, hence, it is also a noetherian ring.

(2) As every affine algebra is finitely generated, in the definition of a finite morphism one can replace the words "finite extension" by "integral extension."

The following result shows that in the definition of finite morphisms one can choose *any* affine covering.

THEOREM 3.1.2. *Let $f : Y \to X$ be a morphism of separated algebraic varieties. Suppose that there is an open affine covering of X : $X = \bigcup_i X_i$ such that all preimages $Y_i = f^{-1}(X_i)$ are also affine. Then, for every affine subvariety $X' \subseteq X$, the preimage $f^{-1}(X')$ is also affine.*

COROLLARY 3.1.3. *If $f : Y \to X$ is a finite morphism and X is affine, Y is affine as well.*

The proof of Theorem 3.1.2 is proposed to the reader as a series of exercises. We start with the following simple observation.

EXERCISE 3.1.4. If $f : Y \to X$ is a morphism of separated varieties, Y is affine and $X' \subseteq X$ is an affine subvariety, then $Y' = f^{-1}(X')$ is also affine.

Hint: Y' is isomorphic to the preimage of Δ_X under the mapping $Y \times X' \to X \times X : \ (p,q) \to (f(p),q)$.

Now, in the situation of Theorem 3.1.2, all the intersections $X'_i = X' \cap X_i$ are affine (as X is separated). Hence, their preimages $f^{-1}(X'_i)$ are also affine (apply Exercise 3.1.4 to $Y_i \to X_i$). Hence, we only have to consider the case when $X = X'$ is affine and to prove that Y is also affine. Moreover, diminishing X_i, we can suppose them *principal open* subsets: $X_i = D(g_i)$. As X is quasi-compact, one may also suppose that there is only finitely many of these subsets: $X = \bigcup_{i=1}^k D(g_i)$. In what follows, we keep these restrictions and denote:

$$\begin{aligned}
&\mathbf{A} = \mathcal{O}_Y(Y);\\
&D(g) = \{\, p \in Y \mid g(p) \neq 0 \,\}, \text{ where } g \in \mathbf{A};\\
&d_i = f^*(X)(g_i) \in \mathbf{A}.
\end{aligned}$$

Exercise 3.1.5. Check that $Y_i = D(d_i)$ and $\langle\, d_1, d_2, \dots, d_k \,\rangle = \langle\, 1 \,\rangle$ in $\mathbf{A}$.

Hence, we have to prove the following:

Theorem 3.1.6. *Let Y be a separated variety, $\{\, d_1, d_2, \dots, d_k \,\}$ be a set of elements of the ring $\mathbf{A} = \mathcal{O}_Y(Y)$ generating the unit ideal. Suppose that all open sets $Y_i = D(d_i)$ are affine varieties. Then Y is also affine.*

In what follows, we keep the notations and assumptions of Theorem 3.1.6 and denote $\mathbf{A}_i = \mathcal{O}_Y(Y_i)$

Exercise 3.1.7. Prove that, for any $g \in \mathbf{A}$, $\mathcal{O}_Y(D(g)) \simeq \mathbf{A}[\, g^{-1} \,]$ and the restriction $\mathcal{O}^Y_{D(g)}$ coincides with the natural homomorphism $\rho : \mathbf{A} \to \mathbf{A}[\, g^{-1} \,]$.
Hint: Follow Exercise 1.6.6 using the covering $Y = \bigcup_i Y_i$.

Exercise 3.1.8. Prove that $\mathbf{A}$ is an affine algebra.
Hint: Find $a_{ij} \in \mathbf{A}$ ($i = 1, \dots, k$, $j = 1, \dots, l_i$) such that $\mathbf{A}_i = \mathbf{K}[\, a_{ij}/1, 1/d_i \,]$. Then find h_i such that $\sum_i h_i d_i = 1$ and show that $\mathbf{A} = \mathbf{K}[\, a_{ij}, h_i, d_i \,]$.

Exercise 3.1.9. Let Z be an affine variety such that $\mathbf{K}[\, Z \,] \simeq \mathbf{A}$, $\varphi : Y \to Z$ be a morphism such that $\varphi^*(Z)$ is an isomorphism. Prove that φ is isomorphism too.
Hint: Check that the restriction of φ onto Y_i is an isomorphism $Y_i \to D(\varphi^*(d_i))$.

Exercises 3.1.10. Prove that:

(1) Any closed immersion is a finite morphism.
(2) If $f_1 : Y_1 \to X_1$ and $f_2 : Y_2 \to X_2$ are finite morphisms, then $f_1 \times f_2 : Y_1 \times Y_2 \to X_1 \times X_2$ is also a finite morphism.

(3) If both $f : Y \to X$ and $g : Z \to Y$ are finite morphisms, then $f \circ g : Z \to X$ is also a finite morphism.
(4) If $f : Y \to X$ is a finite morphism and Z is a subvariety of X, then the induced mapping $f^{-1}(Z) \to Z$ is also a finite morphism.

Hint: First prove this claim when X is affine and Z is a principal open subset of X.

For affine varieties, finiteness can always be defined globally.

PROPOSITION 3.1.11. *A morphism of affine varieties $f : Y \to X$ is finite if and only if $\mathbf{K}[\,Y\,]$ is integral over $\operatorname{Im} f^*(X)$.*

REMARK. Indeed, if $f : Y \to X$ is finite and X is affine, Y is affine as well, but we shall not use this fact.

PROOF. Replacing X by $\overline{\operatorname{Im} f}$, we may suppose that f is dominant (i.e., $\operatorname{Im} f$ is dense), hence, $f^*(X)$ is a monomorphism (cf. Exercise 1.5.11(8b)). So we identify $\mathbf{K}[\,X\,]$ with its image $\mathbf{A}$ in $\mathbf{B} = \mathbf{K}[\,Y\,]$. There is an open affine covering $X = \bigcup_i U_i$ such that, for every i, $V_i = f^{-1}(U_i)$ is also affine and $\mathbf{K}[\,V_i\,]$ is a finitely generated module over $\operatorname{Im} f^*(U_i)$. In view of Exercise 3.1.10(4), one may suppose that all U_i are principal open subsets: $U_i = D(g_i)$ for some $g_i \in \mathbf{A}$; moreover, as X is quasi-compact, there is only finitely many of them. Evidently, $f^{-1}(D(g_i)) = D(f^*(g_i))$ is also a principal open subset in Y (defined by the same g_i but considered as the element of $\mathbf{B}$). Hence, $\mathcal{O}_X(U_i) = \mathbf{A}[g_i^{-1}]$ and $\mathcal{O}_U(V_i) = \mathbf{B}[g_i^{-1}]$. Let $\{\, b_{ij}/g_i^k \,\}$ be a set of generators of $\mathbf{B}[g_i^{-1}]$ as of $\mathbf{A}[g_i^{-1}]$-module (certainly, we may suppose that the degree k is common). We claim that $\{\, b_{ij} \,\}$ is a set of generators of $\mathbf{B}$ as of $\mathbf{A}$-module.

Indeed, let $b \in \mathbf{B}$. Then, in $\mathbf{B}[g_i^{-1}]$, $b/1 = \sum_j a_{ij} b_{ij}/g_i^l$ for some $a_{ij} \in \mathbf{A}$ and some integer l, or, the same, in $\mathbf{B}$, $g_i^r b = \sum_j a_{ij} b_{ij}$ for some r. As $\bigcup_i D(g_i) = \mathbf{A}$, there are some $h_i \in \mathbf{A}$ such that $\sum_i h_i g_i^r = 1$. So $b = \sum_i h_i g_i^r b = \sum_{ij} a_{ij} b_{ij}$. □

The main feature of finite morphisms, partially explaining their name, is the following.

THEOREM 3.1.12. *Let $f : Y \to X$ be a finite morphism of algebraic varieties. Then it is closed and, for every $p \in X$, the fibre $f^{-1}(p)$ is finite.*

PROOF. In view of Exercises 3.1.10, we may suppose f being dominant, i.e., $\overline{\operatorname{Im} f} = X$, and show that, for every point $p \in X$, its preimage $f^{-1}(p)$ is finite and non-empty. Moreover, we may suppose X and Y being affine with the coordinate algebras, respectively, $\mathbf{A}$ and $\mathbf{B}$, and identify $\mathbf{A}$ with $\operatorname{Im} f^*(X) \subseteq \mathbf{B}$. Then $\mathbf{B}$ is a finitely generated $\mathbf{A}$-module. Consider two points, $p \in X$, $q \in Y$, and the corresponding maximal ideals $\mathfrak{m}_p \subset \mathbf{A}$ and $\mathfrak{m}_q \subset \mathbf{B}$ (cf. Proposition 1.5.3). Obviously, $p = f(q)$ if and only if $\mathfrak{m}_p \subseteq \mathfrak{m}_q$. Therefore, Theorem 3.1.12 is a special case of the following result of commutative algebra.

LEMMA 3.1.13. *Let $\mathbf{B} \supseteq \mathbf{A}$ be a finite extension of noetherian rings. Then, for every maximal ideal $\mathfrak{m} \subset \mathbf{A}$, the set $M = \{\, \mathfrak{n} \in \operatorname{Max} \mathbf{B} \mid \mathfrak{n} \supseteq \mathfrak{m} \,\}$ is non-empty and finite.*[1]

PROOF. First we prove that $M \neq \emptyset$. In view of Corollary 1.3.7, it is enough to show that $\mathfrak{m}\mathbf{B} \neq \mathbf{B}$. Let $\mathbf{B} = \langle\, b_1, b_2, \dots, b_m \,\rangle$ as $\mathbf{A}$-module. Suppose that $\mathfrak{m}\mathbf{B} = \mathbf{B}$. Then, for every index j, $b_j = \sum_{i=1}^m c_{ij} b_i$ with $c_{ij} \in \mathfrak{m}$. These equations can be rewritten in the matrix form as $(E - C)\mathbf{b} = 0$, where E is the identity $n \times n$ matrix, $C = (c_{ij})$ and $\mathbf{b} = (b_1, b_2, \dots, b_m)^\top$. Multiplying this matrix equality by the adjoint matrix to $(E - C)$, one gets that $\det(E - C) b_i = 0$ for all i, whence $\det(E - C) = 0$. But the last determinant is, evidently, of the form $1 + a$ with $a \in \mathfrak{m}$, which is impossible as $1 \notin \mathfrak{m}$.

Now we prove that M is finite. We use the following lemma.

LEMMA 3.1.14. *Let $\mathbf{B} \supseteq \mathbf{A}$ be an integral extension of rings, $\mathfrak{q} \subset \mathfrak{p}$ be prime ideals from $\mathbf{B}$. Then $\mathfrak{q} \cap \mathbf{A} \subset \mathfrak{p} \cap \mathbf{A}$.*

PROOF. Replacing $\mathbf{B}$ by $\mathbf{B}/\mathfrak{q}$ and $\mathbf{A}$ by $\mathbf{A}/(\mathfrak{q} \cap \mathbf{A})$, we may suppose that $\mathfrak{q} = \{\, 0 \,\}$ and both $\mathbf{B}$ and $\mathbf{A}$ are integral. Then we have to show that $\mathfrak{p} \cap \mathbf{A} \neq \{\, 0 \,\}$. Take any non-zero element $a \in \mathfrak{p}$ and consider an equation $a^m + b_1 a^{m-1} + \dots + b_m$ with $b_i \in \mathbf{A}$ of the smallest possible degree. Then $b_m \neq 0$ and $b_m \in \mathfrak{p} \cap \mathbf{A}$. $\square$

As $\mathfrak{m}$ is maximal, $\mathfrak{p} \cap \mathbf{A} = \mathfrak{m}$ for every prime ideal $\mathfrak{p} \subset \mathbf{B}$ containing $\mathfrak{m}$. Take a maximal ideal $\mathfrak{n} \supseteq \mathfrak{p}$. Then also $\mathfrak{n} \cap \mathbf{A} = \mathfrak{m}$, hence, $\mathfrak{p} = \mathfrak{n}$, i.e., all prime ideals from $\mathbf{B}$ containing $\mathfrak{m}$ are maximal. Thus, maximal ideals containing $\mathfrak{m}$ are just minimal among the prime ideals containing $\sqrt{\mathfrak{m}\mathbf{B}}$, or, the same, the prime components of $\sqrt{\mathfrak{m}\mathbf{B}}$ (cf. Corollary 1.5.9 and Exercise 1.5.10). So there is only a finite number of such ideals. $\square$

EXERCISE 3.1.15. Prove that if $\mathbf{B} \supseteq \mathbf{A}$ is an integral extension of rings and $\mathfrak{m} \subset \mathbf{B}$ is a maximal ideal, there is a maximal ideal $\mathfrak{n} \subset \mathbf{A}$ such that $\mathfrak{n} \cap \mathbf{A} = \mathfrak{m}$.

Hint: Suppose that $\mathfrak{m}\mathbf{B} = \mathbf{B}$ and prove that then $\mathfrak{m}\mathbf{B}' = \mathbf{B}'$ for a subring $\mathbf{B}'$ which is finitely generated as $\mathbf{A}$-module.

EXERCISE 3.1.16. Let $f : Y \to X$ be a finite morphism of algebraic varieties. Prove that:

[1]This lemma is valid for non-noetherian rings too, though the second part of the proof should be changed.

(1) X is separated if and only if Y is separated.
Hint (to the "only if" part): Let X be separated, $p \neq q$ two points of Y. Prove that either $f(p) \neq f(q)$ or they both belong to an affine open subset $V \subseteq Y$. Then use the separateness of affine varieties.
(2) X is complete if and only if Y is complete.

Theorem 3.1.12 allows, in particular, to precise the structure of the image of a regular mapping. Remind that a subset Z of a topological space X is said to be *constructible* if it is a finite union of locally closed subsets. For instance, a constructible subset of an affine (or a projective) space is a finite union of subvarieties, or, the same, a subset which can be defined by a (finite) system of polynomial equalities and inequalities.

THEOREM 3.1.17 (Chevalley's Theorem). *If $f : Y \to X$ is a morphism of algebraic varieties and $Z \subseteq Y$ is a constructible subset, then $f(Z)$ is also constructible. (In particular, $\operatorname{Im} f$ is constructible.)*

PROOF. As any locally closed subset of an algebraic variety is also an algebraic variety (cf. Corollary 2.2.2), it is enough to prove that $f(Y)$ is constructible. Moreover, one may suppose Y and X being affine and irreducible. We use the Noetherian induction. The claim is trivial if $Y = \emptyset$. Suppose that it is valid for all proper closed subsets of Y. Replacing X by $\overline{\operatorname{Im} f}$, we may suppose f being dominant, i.e., f^* being injective, and we identify $\mathbf{A} = \mathbf{K}[X]$ with its image in $\mathbf{B} = \mathbf{K}[Y]$ under f^*. Put also $\mathbf{R} = \mathbf{K}(X)$, $\mathbf{Q} = \mathbf{K}(Y)$ and $d = \operatorname{tr.deg}(\mathbf{Q}/\mathbf{R})$.

We prove first that $\operatorname{Im} f$ contains an open non-empty subset of X. Choose a transcendence base $\{ b_1, b_2, \dots, b_d \}$ of $\mathbf{Q}$ over $\mathbf{R}$. Certainly, one may suppose that $b_i \in \mathbf{B}$. Let $\mathbf{B} = \mathbf{A}[b_1, b_2, \dots, b_d, c_1, c_2, \dots, c_r]$. All c_i are algebraic over $\mathbf{R}$, hence, satisfy an equation $a_{i0}c_i^{m_i} + a_{i1}c_i^{m_i-1} + \dots + a_{im_i} = 0$ with $a_i \in \mathbf{A}[b_1, \dots, b_d]$ and $a_{i0} \neq 0$. Let $g = \prod_i a_{i0}$. Then $\mathbf{B}[g^{-1}]$ is a finite extension of $\mathbf{A}[g^{-1}][b_1, \dots, b_d]$. Consider the variety $X \times \mathbb{A}^d$ and identify its coordinate algebra with $\mathbf{A}[b_1, \dots, b_d] \subseteq \mathbf{B}$. The embedding $\mathbf{A} \to \mathbf{A}[b_1, \dots, b_d]$ corresponds to the projection $\operatorname{pr}_X : X \times \mathbb{A}^d \to X$, so f decomposes into the product $Y \xrightarrow{\varphi} X \times \mathbb{A}^d \xrightarrow{\operatorname{pr}_X} X$, where φ^* is the embedding of $\mathbf{A}[b_1, \dots, b_d]$ into $\mathbf{B}$. The restriction of φ onto $\varphi^{-1}(D(g))$ is a finite mapping, hence, $\operatorname{Im} \varphi \supseteq D(g)$. As pr_X is an open mapping (cf. Proposition 2.4.9), $\operatorname{Im} f$ contains the open non-empty subset $U = \operatorname{pr}_X(D(g))$.

Now, put $X' = X \setminus U$ and $Y' = f^{-1}(X')$. They are closed, respectively, in X and Y. Let $f' : Y' \to X'$ be the restriction of f onto Y'. It is also a regular mapping. By the inductive hypothesis, $\operatorname{Im} f'$ is a constructible subset of X' (hence, of X). Thus, $\operatorname{Im} f = U \cup \operatorname{Im} f'$ is also constructible. □

EXERCISES 3.1.18. Let $o = (c_0 : c_1 : \dots : c_n)$ be a point of the projective space $\mathbb{P}^n$, $L = PV(\sum_{i=0}^n \lambda_i x_i)$ be a hyperplane in $\mathbb{P}^n$ such that $o \notin L$. For any point $p = (a_0 : a_1 : \dots : a_n) \neq o$ denote by $\overline{op}$ the *projective line* passing through o and p, i.e., the set of all points of $\mathbb{P}^n$ having the form

$$(\xi c_0 + \eta a_0 : \xi c_1 + \eta a_1 : \dots : \xi c_n + \eta a_n),$$

where $(\xi : \eta) \in \mathbb{P}^1$.

(1) Prove that $L \cap \overline{op}$ consists of a unique point, which we denote by $\pi(p)$ and call the *projection* of p onto L *from the center* o.
(2) Check that $\pi : \mathbb{P}^n \setminus \{ o \} \to L$ is a regular mapping ("*central projection*").
(3) Let $X \subset \mathbb{P}^n$ be a projective variety such that $o \notin X$. Prove that the restriction $\pi|_X$ is a finite mapping.
(4) ("Projective Noether's Normalization Lemma.") Deduce that for every projective variety X there is a finite mapping $X \to \mathbb{P}^d$ for some d.

Hint: Use a linear automorphism of $\mathbb{P}^n$ to reduce the problem to the case when $o = (1 : 0 : \dots : 0)$ and $L = PV(x_0)$.

EXERCISE 3.1.19. (1) Let $L_0, L_1, \dots, L_m \in \mathbf{K}[x_0, x_1, \dots, x_n]$ be linear forms, $H = PV(L_0, L_1, \dots, L_m)$ and $X \subseteq \mathbb{P}^n$ be a projective variety such that $X \cap H = \emptyset$. Prove that the mapping $\varphi : X \to \mathbb{P}^m$ such that $\varphi(p) = (L_0(p) : \dots : L_m(p))$ is finite.

Hint: Use a linear automorphism of $\mathbb{P}^n$ to reduce the problem to the case when $L_i = x_i$; then use Exercise 3.1.18 and induction.

(2) Let $F_0, F_1, \dots, F_m \in \mathbf{K}[x_0, x_1, \dots, x_n]$ be homogeneous polynomials of degree $d > 0$ and $X \subseteq \mathbb{P}^n$ be a projective variety such that $X \cap PV(F_0, F_1, \dots, F_m) = \emptyset$. Prove that the mapping $\varphi : X \to \mathbb{P}^m$ such that $\varphi(p) = (F_0(p) : \dots : F_m(p))$ is finite.

Hint: Use (1) and Veronese embedding (Exercise 2.3.11(6)).

3.2. Dimensions

DEFINITION 3.2.1. Let X be a noetherian topological space (for instance, an algebraic variety). The *combinatorial dimension* of X is, by definition, the upper bound for the lengths l of chains of its irreducible closed subsets $X_0 \supset X_1 \supset \dots \supset X_l$. This dimension is denoted by $\operatorname{c.dim} X$. We also put $\operatorname{c.dim} \emptyset = -1$.

Taking into account the correspondence between irreducible closed subsets and prime ideals (cf. Corollary 1.5.7), we deduce that the combinatorial dimension of an *affine* variety can be defined "pure algebraically."

DEFINITIONS 3.2.2. Let $\mathbf{A}$ be a ring.

(1) The set of all prime ideals of $\mathbf{A}$ is called the *spectrum* of $\mathbf{A}$ and denoted by $\operatorname{Spec}\mathbf{A}$.
(2) The *height* $\operatorname{ht}\mathfrak{p}$ of a prime ideal $\mathfrak{p}\in\operatorname{Spec}\mathbf{A}$ is, by definition, the upper bound of lengths l of chains of prime ideals $\mathfrak{p}_0\subset\mathfrak{p}_1\subset\ldots\subset\mathfrak{p}_l=\mathfrak{p}$.
(3) The *Krull dimension* $\mathrm{K.dim}\,\mathbf{A}$ of the ring $\mathbf{A}$ is defined as $\sup\{\operatorname{ht}\mathfrak{p}\mid\mathfrak{p}\in\operatorname{Spec}\mathbf{A}\}$.

PROPOSITION 3.2.3. *If X is an affine algebraic variety, $\mathbf{A}=\mathbf{K}[X]$, then* $\mathrm{c.dim}\,X=\mathrm{K.dim}\,\mathbf{A}$.

We are going to give equivalent definitions of these dimensions. First note the following simple result.

EXERCISES 3.2.4. Prove that, for any noetherian topological space X:

(1) $\mathrm{c.dim}\,X=\sup\{\mathrm{c.dim}\,X_i\mid X_i$ irreducible component of $X\}$.
(2) If $X=\bigcup_i U_i$ is an open covering of X, then $\mathrm{c.dim}\,X=\sup\{\mathrm{c.dim}\,U_i\}$.

Now the following theorem precise the notion of dimension for algebraic varieties.

THEOREM 3.2.5. *Let X be an algebraic variety.*

(1) *If X is affine (projective),* $\mathrm{c.dim}\,X$ *coincides with such integer d that there is a finite dominant morphism $X\to\mathbb{A}^d$ (resp., $X\to\mathbb{P}^d$).*
(2) *If X is irreducible, then* $\mathrm{c.dim}\,X=\mathrm{tr.deg}(\mathbf{K}(X)/\mathbf{K})$.

The combinatorial dimension of an algebraic variety X is called its *dimension* and denoted by $\dim X$.

PROOF. If $X=\bigcup_i X_i$ is the irreducible decomposition of X, Y is irreducible and $f:X\to Y$ is a finite dominant morphism, then, by Theorem 3.1.12, $Y=\operatorname{Im}f=\bigcup_i f(X_i)$ and all $f(X_i)$ are closed, hence, $f(X_i)=Y$ for some i. In view of Exercises 3.1.10, the restriction of f onto X_i is also finite. Hence, one only has to prove the assertion *1* for irreducible varieties. In view of Exercises 3.2.4, one may even suppose X being affine. Then, if $X\to\mathbb{A}^d$ is a finite dominant morphism, $\mathbf{K}[X]$ is integral over $\mathbf{K}[x_1,\ldots,x_d]$, thus, $\mathbf{K}(X)$ is algebraic over $\mathbf{K}(x_1,\ldots,x_d)$ and $\mathrm{tr.deg}(\mathbf{K}(X)/\mathbf{K})=d$. Now, Theorem 3.2.5 follows from Noether's Normalization Lemma (or its projective analogue, cf. Exercise 3.1.18(4)) and two following assertions:

THEOREM 3.2.6. $\mathrm{K.dim}\,\mathbf{K}[x_1,\ldots,x_n]=n$.

THEOREM 3.2.7. *If* $\mathbf{A} \supseteq \mathbf{B}$ *is a finite extension of noetherian rings, then* $\mathrm{K.dim}\,\mathbf{A} = \mathrm{K.dim}\,\mathbf{B}$.[2]

PROOF OF THEOREM 3.2.7. It is a consequence of the following result.

THEOREM 3.2.8 (Going-Up Principle). *Let* $\mathbf{A} \supseteq \mathbf{B}$ *be a finite extension of noetherian rings,* $\mathfrak{p} \subset \mathbf{B}$ *be a prime ideal. Then there is a prime ideal* $\mathfrak{P} \subset \mathbf{A}$ *such that* $\mathfrak{P} \cap \mathbf{B} = \mathfrak{p}$.

Indeed, note first a simple corollary of Theorem 3.2.8.

COROLLARY 3.2.9. *Let* $\mathbf{A} \supseteq \mathbf{B}$ *be a finite extension of noetherian rings,* $\mathfrak{q} \subset \mathfrak{p} \subset \mathbf{B}$ *be prime ideals and* $\mathfrak{Q} \subset \mathbf{A}$ *be such a prime ideal that* $\mathfrak{Q} \cap \mathbf{B} = \mathfrak{q}$. *Then there is a prime ideal* $\mathfrak{P} \subset \mathbf{A}$ *such that* $\mathfrak{Q} \subset \mathfrak{P}$ *and* $\mathfrak{P} \cap \mathbf{B} = \mathfrak{p}$.

PROOF. Evidently, $\mathbf{B}/\mathfrak{q}$ can be considered as a subring of $\mathbf{A}/\mathfrak{Q}$, both of them are also noetherian and the extension $\mathbf{A}/\mathfrak{Q} \supseteq \mathbf{B}/\mathfrak{q}$ is finite. So, by Theorem 3.2.8, there is a prime ideal $\overline{\mathfrak{P}} \subset \mathbf{A}/\mathfrak{Q}$ such that $\overline{\mathfrak{P}} \cap \mathbf{B}/\mathfrak{q} = \mathfrak{p}/\mathfrak{q}$. Then $\overline{\mathfrak{P}} = \mathfrak{P}/\mathfrak{Q}$ for some prime ideal $\mathfrak{P} \supset \mathfrak{Q}$ and $\mathfrak{P} \cap \mathbf{B} = \mathfrak{p}$. □

Now an evident induction shows that if there is a chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_l$ in $\mathbf{B}$, there is also a chain of prime ideals $\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \dots \subset \mathfrak{P}_l$ in $\mathbf{A}$ such that $\mathfrak{P}_i \cap \mathfrak{B} = \mathfrak{p}_i$, whence $\mathrm{K.dim}\,\mathbf{A} \geq \mathrm{K.dim}\,\mathbf{B}$. On the other hand, Lemma 3.1.14 implies that any chain of prime ideals $\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \dots \subset \mathfrak{P}_l$ in $\mathbf{A}$ produces a chain of prime ideals in $\mathbf{B}$: $\mathfrak{P}_0 \cap \mathbf{B} \subset \mathfrak{P}_1 \cap \mathbf{B} \subset \dots \subset \mathfrak{P}_l \cap \mathbf{B}$ (cf. Lemma 3.1.14), so $\mathrm{K.dim}\,\mathbf{B} \geq \mathrm{K.dim}\,\mathbf{A}$. □

PROOF OF THEOREM 3.2.6. Consider a maximal ideal from $\mathbf{K}[\mathbf{x}] = \mathbf{K}[x_1, \dots, x_n]$. It coincides with $\mathfrak{m}_p$ for some point $p = (a_1, \dots, a_n) \in \mathbb{A}^n$ (cf. Proposition 1.5.3). Certainly, $\mathfrak{m}_p = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. For every $k \leq n$, put $\mathfrak{p}_k = \langle x_1 - a_1, \dots, x_k - a_k \rangle$ (in particular, $\mathfrak{p}_0 = \{0\}$ and $\mathfrak{p}_n = \mathfrak{m}_p$). Evidently, $\mathbf{K}[\mathbf{x}]/\mathfrak{p}_k \simeq \mathbf{K}[x_{k+1}, \dots, x_n]$. As all these factor-rings are integral, the ideals $\mathfrak{p}_k$ are prime, whence $\mathrm{K.dim}\,\mathbf{K}[\mathbf{x}] \geq \mathrm{ht}\,\mathfrak{m}_p \geq n$. Now Theorem 3.2.6 follows from the following result.

PROPOSITION 3.2.10. *If a prime ideal* $\mathfrak{p}$ *of a noetherian ring* $\mathbf{A}$ *is generated by* n *elements, then* $\mathrm{ht}\,\mathfrak{p} \leq n$.

In turn, Proposition 3.2.10 is an inductive consequence of the so called "*Krull Hauptidealsatz*":

THEOREM 3.2.11 (Krull Hauptidealsatz). *Let* $\mathbf{A}$ *be a noetherian ring,* $a \in \mathbf{A}$ *be neither invertible nor a zero divisor and* $\mathfrak{p}$ *be a prime ideal which is minimal among the prime ideals containing* a. *Then* $\mathrm{ht}\,\mathfrak{p} = 1$.

[2]It is also valid for arbitrary integral extensions of noetherian rings.

We shall prove Going-Up Principle and Krull Hauptidealsatz (as well as Proposition 3.2.10) in the following section in context of studying the so called *local rings*.

EXERCISE 3.2.12. Prove that the Grassmann variety $\mathbb{G}\mathsf{r}(d,n)$ is a rational variety of dimension $d(n-d)$.
Hint: Consider the open subset: $p_{12\dots d} \neq 0$.

3.3. Local rings

DEFINITION 3.3.1. A ring $\mathbf{A}$ is said to be *local* if it has a unique maximal ideal $\mathfrak{m}$. The field $\mathbf{k} = \mathbf{A}/\mathfrak{m}$ is called the *residue field* of the local ring $\mathbf{A}$.

It is clear that a ring $\mathbf{A}$ is local if and only if the set of all its non-invertible elements is an ideal (then it is just the unique maximal ideal of $\mathbf{A}$).

The main origin of local rings in algebraic geometry are the *stalks* of the sheaves of regular functions. Remind the corresponding definition.

DEFINITION 3.3.2. Let $\mathcal{F}$ be a sheaf on a topological space X, $p \in X$. The *stalk* $\mathcal{F}_p$ of the sheaf $\mathcal{F}$ at the point p is, by definition, the *direct limit* $\varinjlim_{U \ni p} \mathcal{F}(U)$. In other words, $\mathcal{F}_p$ is defined as the set of the equivalence classes of $\bigcup_{U \ni p} \mathcal{F}(U)$ under the following equivalence relation:

$$a \sim b\,, \text{ where } a \in \mathcal{F}(U),\, b \in \mathcal{F}(V), \text{ if and only if there is } W \subseteq U \cap V \text{ such that } \mathcal{F}^U_W(a)\mathcal{F}^V_W(b)\,.$$

The natural mapping $\mathcal{F}(U) \to \mathcal{F}_p$, where $p \in U$, which maps an element from $\mathcal{F}(U)$ to its class in $\mathcal{F}_p$, is denoted by $\mathcal{F}^U_p$.

If $\mathcal{F}$ is a sheaf of groups, or rings, or algebras, then the stalk $\mathcal{F}_p$ is also a group, or ring, or algebra. For instance, if $(X, \mathcal{O}_X)$ is a space with functions over a field $\mathbf{K}$, the stalks $\mathcal{O}_{X,p}$ are also $\mathbf{K}$-algebras.

PROPOSITION 3.3.3. *For every point p of a space with functions X, the stalk $\mathcal{O}_{X,p}$ is a local algebra, whose maximal ideal coincides with the set* $\mathfrak{m}_{X,p} = \left\{ \mathcal{O}^U_p(f) \,|\, p \in U,\ f(p) = 0 \right\}$.

PROOF. It is obvious that $\mathfrak{m}_{X,p}$ is a proper ideal of $\mathcal{O}_{X,p}$. On the other hand, if $f \in \mathcal{O}_X(U)$ and $f(p) \neq 0$, then $V = \{\, v \in U \,|\, f(v) \neq 0 \,\}$ is open and contains p. Put $f' = \mathcal{O}^U_V(f)$. By definition of space with functions, $1/f' \in \mathcal{O}_X(V)$. Obviously, $\mathcal{O}^U_p(f) = \mathcal{O}^V_p(f')$, so $\mathcal{O}^V_p(1/f')$ is the inverse of this element in $\mathcal{O}_{X,p}$. Hence, all elements not belonging to $\mathfrak{m}_{X,p}$ are invertible and $\mathfrak{m}_{X,p}$ is the unique maximal ideal in $\mathcal{O}_{X,p}$. $\square$

EXERCISE 3.3.4. Let X, Y are algebraic varieties, $p \in X$, $q \in Y$. Show that $\mathcal{O}_{X,p} \simeq \mathcal{O}_{Y,q}$ if and only if there are isomorphic open subsets $U \ni p$ and $V \ni q$, respectively, in X and Y. (In particular, if X, Y are irreducible, they are birationally equivalent.)

There is a natural procedure, called *localization*, of getting local rings. Before introducing it, we consider some properties of ideals in rings of fractions.

NOTATIONS 3.3.5. Let $\mathbf{A}$ be a ring, $S \subseteq \mathbf{A}$ be a multiplicative subset and $\mathbf{B} = \mathbf{A}[S^{-1}]$.

(1) For any ideal $I \subseteq \mathbf{A}$, put $I[S^{-1}] = I\mathbf{B} = \{ a/s \mid a \in I,\ s \in S \} \subseteq \mathbf{B}$.
(2) For every ideal $J \subseteq \mathbf{B}$, put $J \cap \mathbf{A} = \{ a \in \mathbf{A} \mid a/1 \in J \}$ (if S contains no zero divisors and we identify $a \in \mathbf{A}$ with $a/1 \in \mathbf{B}$, it is indeed the intersection of J and $\mathbf{A}$).

PROPOSITION 3.3.6. *Let $\mathbf{A}$ be a ring, $S \subseteq \mathbf{A}$ be a multiplicative subset and $\mathbf{B} = \mathbf{A}[S^{-1}]$.*

(1) $J = (J \cap \mathbf{A})[S^{-1}]$ *for every ideal* $J \subseteq \mathbf{B}$.
(2) $I[S^{-1}] \cap \mathbf{A} = \{ a \in \mathbf{A} \mid sa \in I \text{ for some } s \in S \}$ *for every ideal* $I \subseteq \mathbf{A}$. *In particular, if I is prime and $I \cap S = \emptyset$, then* $I = I[S^{-1}] \cap \mathbf{A}$.

PROOF. *1.* If $a/s \in J$, ($a \in \mathbf{A},\ s \in S$) then $a/1 = (a/s)(s/1) \in J$, whence $a \in J \cap \mathbf{A}$ and $a/s \in (J \cap \mathbf{A})[S^{-1}]$. So $J \subseteq (J \cap \mathbf{A})[S^{-1}]$ The inverse inclusion is obvious.

2. If $a/1 = b/s$, where $b \in I,\ s \in S$, then $ra = rsb \in I$ for some $r \in S$ and $rs \in S$ too. On the other hand, if $as \in I$ and $s \in S$, then $a/1 = as/s \in I[S^{-1}] \cap \mathbf{A}$. The claim concerning prime ideal is now obvious. □

COROLLARY 3.3.7. *If the ring $\mathbf{A}$ is noetherian, the ring of fractions $\mathbf{B} = \mathbf{A}[S^{-1}]$ is noetherian as well.*

PROOF. Let J be an ideal of $\mathbf{B}$, $I = J \cap \mathbf{A}$ and $\{ a_1, a_2, \dots, a_m \}$ be a generating set for I. Then, evidently, $\{ a_1/1, a_2/1, \dots, a_m/1 \}$ is a generating set for $I[S^{-1}] = J$. □

If $S = \mathbf{A} \setminus \mathfrak{p}$, where $\mathfrak{p} \subset \mathbf{A}$ is a prime ideal, the ring of fractions $\mathbf{A}[S^{-1}]$ is denoted by $\mathbf{A}_{\mathfrak{p}}$ and called the *localization* of $\mathbf{A}$ with respect to the prime ideal $\mathfrak{p}$. The following result explains a bit this term.

COROLLARY 3.3.8. *If $\mathfrak{p} \subset \mathbf{A}$ is a prime ideal, then the prime ideals of $\mathbf{A}_{\mathfrak{p}}$ are just $\mathfrak{q}\mathbf{A}_{\mathfrak{p}}$, where $\mathfrak{q}$ runs through prime ideals of $\mathbf{A}$ contained in $\mathfrak{p}$. In particular, $\mathfrak{p}\mathbf{A}_{\mathfrak{p}}$ is the unique maximal ideal of the ring $\mathbf{A}_{\mathfrak{p}}$, so this ring is local.*

The stalks of structure sheaf of an algebraic variety can always be obtained using localizations. Namely, if U is an affine neighbourhood of a point p of an algebraic variety X, then, of course, $\mathcal{O}_{U,p} = \mathcal{O}_{X,p}$ (if we consider U as an open subvariety of X). So we only have to calculate stalks $\mathcal{O}_{X,p}$ for *affine* X.

PROPOSITION 3.3.9. *Let X be an affine variety, $\mathbf{A} = \mathbf{K}[X]$, $p \in X$ and $\mathfrak{m} = \mathfrak{m}_p$. Then $\mathcal{O}_{X,p} = \mathbf{A}_{\mathfrak{m}}$.*

PROOF. As principal open subsets form a base of the Zariski topology, every element from $\mathcal{O}_{X,p}$ has the form $\mathcal{O}_p^U(f)$ for some $U = D(g)$, where $g(p) \neq 0$ (or, the same, $g \notin \mathfrak{m}$) and $f \in \mathcal{O}_X(U) = \mathbf{A}[g^{-1}]$ (cf. Exercise 1.6.6). So, $f = (a/g^k)|_U$, where $a \in \mathbf{A}$. As $D(g) = D(g^k)$, one may put $k = 1$. Suppose that $\mathcal{O}_p^U(f) = \mathcal{O}_p^V(f')$, where $V = D(h)$, $h(p) \neq 0$ and $f' = (b/h)|_V$. Then there is a principal open $W = D(r) \subseteq U \cap V = D(gh)$ such that $r(p) \neq 0$ and $f|_W = f'|_W$. By Hilbert Nullstellensatz, $r^d = sgh$ for some integer d and some $s \in \mathbf{A}$, and one may again put $d = 1$. Then, on W, $f = sah/r = sbg/r$. This equality in the ring $\mathcal{O}_X(W) = \mathbf{A}[r^{-1}]$ means that $r^l sah = r^l sbg$ in $\mathbf{A}$. As $r^l s \notin \mathfrak{m}$, it implies that $a/g = b/h$ in $\mathbf{A}_{\mathfrak{m}}$. Therefore, we get a homomorphism $\varphi : \mathcal{O}_{X,p} \to \mathbf{A}_{\mathfrak{m}}$ putting $\varphi(\mathcal{O}_p^U(f)) = a/g$ as above.

On the other hand, given any element $a/s \in \mathbf{A}_{\mathfrak{m}}$, where $a, s \in \mathbf{A}$, $s \notin \mathfrak{m}$, we can consider it as a function on $U = D(s) \ni p$, hence, define its image $\mathcal{O}_p^U(a/s)$ in $\mathcal{O}_{X,p}$. Evidently, it gives the homomorphism $\mathbf{A}_{\mathfrak{m}} \to \mathcal{O}_{X,p}$, inverse to φ. $\square$

EXERCISE 3.3.10. (1) Let $C = V(y^2 - x^3)$ be a cuspidal cubic, $p = (0,0)$. Show that $\mathcal{O}_{C,p}$ is isomorphic to the subalgebra of $\mathbf{K}(t)$ consisting of all fractions $r(t) = f(t)/g(t)$ such that $g(0) \neq 0$ and $r'_t(0) = 0$.

Hint: Use Exercise 1.2.4(6).

(2) Let $X = V(xy) \subset \mathbb{A}^2$, $p = (0,0)$. Prove that $\mathcal{O}_{X,p}$ is isomorphic to the subring of $\mathbf{K}[x] \times \mathbf{K}[y]$ consisting of all pairs $(f(x), g(y))$ such that $f(0) = g(0)$.

(3) Describe $\mathcal{O}_{X,p}$, where p is the coordinate origin and X is one of the following varieties:

(a) $V(xy(x-y)) \subset \mathbb{A}^2$;

(b) The union of three coordinate axes in $\mathbb{A}^3$.

Are these two algebras isomorphic?

We are now going to use localizations for proving Going-Up Principle and Krull Hauptidealsatz. First establish the following important property of modules over local rings.

LEMMA 3.3.11 (Nakayama's Lemma). *Suppose that $\mathbf{A}$ is a local ring with the maximal ideal $\mathfrak{m}$ and M is a finitely generated $\mathbf{A}$-module such that $\mathfrak{m}M = 0$. Then $M = 0$.*

PROOF. Let $M = \langle u_1, u_2, \dots, u_m \rangle$. We prove that also $M = \langle u_1, u_2, \dots, u_{m-1} \rangle$. Then, step by step, we get that M is generated by the empty set, i.e., $M = 0$.

Indeed, as $\mathfrak{m}M = M$, there are elements $a_i \in \mathfrak{m}$ such that $u_m = \sum_{i=1}^m a_i u_i$ or $(1 - a_m)u_m = \sum_{i=1}^{m-1} a_i u_i$. But $1 - a_m \notin \mathfrak{m}$, hence, it is invertible and $u_m \in \langle u_1, u_2, \dots, u_{m-1} \rangle$. Thus, $M = \langle u_1, u_2, \dots, u_{m-1} \rangle$. □

The following corollary is also often cited as "Nakayama's Lemma."

COROLLARY 3.3.12. *Suppose that* $\mathbf{A}$ *is a local ring with the maximal ideal* $\mathfrak{m}$ *and* M *is a finitely generated* $\mathbf{A}$*-module. If* $N \subseteq M$ *is a submodule such that* $N + \mathfrak{m}M = M$, *then* $N = M$.

PROOF. One only has to apply Lemma 3.3.11 to the factor-module M/N. □

For a finitely generated $\mathbf{A}$-module M, denote by $\#_{\mathbf{A}}(M)$ the smallest possible number of elements in generating sets of M (it is called "the *number of generators*") of M.

COROLLARY 3.3.13. *Suppose that* $\mathbf{A}$ *is a local ring with the maximal ideal* $\mathfrak{m}$ *and residue field* $\mathbf{k}$. *Then, for every finitely generated* $\mathbf{A}$*-module* M, $\#_{\mathbf{A}}(M) = \dim_{\mathbf{k}} M/\mathfrak{m}M$.

PROOF. Indeed, in view of Corollary 3.3.12, $M = \langle u_1, u_2, \dots, u_m \rangle$ if and only if $M/\mathfrak{m}M = \langle \overline{u}_1, \overline{u}_2, \dots, \overline{u}_m \rangle$, where $\overline{u}_i = u_i + \mathfrak{m}M$. □

Let now $\mathbf{A}$ be a noetherian ring, $\mathfrak{p} \subset \mathbf{A}$ be a prime ideal. Consider the localization $\mathbf{B} = \mathbf{A}_{\mathfrak{p}}$. In view of Corollaries 3.3.7 and 3.3.8, it is local and noetherian with the maximal ideal $\mathfrak{m} = \mathfrak{p}\mathbf{B}$. Put

$$\mathfrak{p}^{(k)} = \mathfrak{m}^k \cap \mathbf{A} = \left\{ a \in \mathbf{A} \mid sa \in \mathfrak{p}^k \text{ for some } s \notin \mathfrak{p} \right\}$$

(cf. Proposition 3.3.6). The ideal $\mathfrak{p}^{(k)}$ is called the k-th *symbolic power* of $\mathfrak{p}$. It contains $\mathfrak{p}^k$ and $\mathfrak{m}^k = \mathfrak{p}^{(k)}\mathbf{B}$ by Proposition 3.3.6. The following result is an immediate consequence of this equality and Nakayama's Lemma.

COROLLARY 3.3.14. *Let* $\mathfrak{p}$ *be a prime ideal of a noetherian ring* $\mathbf{A}$. $\mathfrak{p}^{(k)} = \mathfrak{p}^{(k+1)}$ *for some* k *if and only if* $\mathfrak{p}$ *is minimal.*

PROOF. By Nakayama's Lemma, $\mathfrak{p}^{(k)} = \mathfrak{p}^{(k+1)}$ if and only if $(\mathfrak{p}\mathbf{A}_{\mathfrak{p}})^k = \{0\}$, i.e., $\mathfrak{p}\mathbf{A}_{\mathfrak{p}} = \sqrt{0}$ in $\mathbf{A}_{\mathfrak{p}}$. It means that $\mathfrak{p}\mathbf{A}_{\mathfrak{p}}$ is minimal prime in $\mathbf{A}_{\mathfrak{p}}$ or, by Proposition 3.3.6, $\mathfrak{p}$ is minimal prime in $\mathbf{A}$. □

EXERCISE 3.3.15. Let $X = V(xy - z^2) \subset \mathbb{A}^3$, $\mathbf{A} = \mathbf{K}[X]$, $\overline{f}$ denote the class of a polynomial f in $\mathbf{A}$ and $\mathfrak{p} = I(Y) \subset \mathbf{A}$, where $Y \subset X$ is the y-axis. Prove that $\overline{x} \in \mathfrak{p}^{(2)}$, but $\overline{x} \notin \mathfrak{p}^2$. Check also that $z \notin \mathfrak{p}^{(2)}$; so $\mathfrak{p} \supset \mathfrak{p}^{(2)} \supset \mathfrak{p}^2$.

We also need the following simple but important result.

Lemma 3.3.16. *Let* $\mathbf{A}$ *be a noetherian ring with a unique prime ideal* $\mathfrak{m}$ *. Then* $\mathbf{A}$ *is an* artinian ring*, i.e. every* descending *chain of ideals* $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$ *stabilizes.*

Proof. In view of Exercise 1.5.10, $\mathfrak{m} = \sqrt{0}$, hence, it is nilpotent: $\mathfrak{m}^m = 0$. Consider the chain of ideals $\mathfrak{m} \supset \mathfrak{m}^2 \supset \dots \supset \mathfrak{m}^m = 0$. All factor-modules $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ can be considered as vector spaces over the residue field $\mathbf{A}/\mathfrak{m}$, which are finite dimensional as all ideals are finitely generated. Hence, for every j, there is such k that $I_k \cap \mathfrak{m}^j + \mathfrak{m}^{j+1} = I_l \cap \mathfrak{m}^j + \mathfrak{m}^{j+1}$ for all $l > k$. As $\mathfrak{m}^j = 0$ for $j \geq m$, we can even choose a common value of k, valid for all j. We show that $I_l = I_k$ for all $l > k$. Indeed, otherwise there is the biggest value j such that $I_k \cap \mathfrak{m}^j \not\subseteq I_l$. Let $a \in I_k \cap \mathfrak{m}^j \setminus I_l$. There are $b \in I_l$ and $c \in \mathfrak{m}^{j+1}$ such that $a = b + c$, whence $c = a - b \in I_k \cap \mathfrak{m}^{j+1} \setminus I_l$, in contradiction with the choice of j. $\square$

Now we return to our proofs. Each time we keep the notations from the corresponding theorem.

Proof of Theorem 3.2.8. Consider the multiplicative subset $S = \mathbf{B} \setminus \mathfrak{p}$ and the rings of fractions $\mathbf{A}_\mathfrak{p} = \mathbf{A}[\,S^{-1}\,] \supseteq \mathbf{B}_\mathfrak{p} = \mathbf{B}[\,S^{-1}\,]$. They are also noetherian (cf. Corollary 3.3.7), $\mathbf{B}_\mathfrak{p}$ is local with the maximal ideal $\mathfrak{m} = \mathfrak{p}\mathbf{B}_\mathfrak{p}$ (cf. Corollary 3.3.8) and this extension is evidently finite. Hence, by Lemma 3.1.13, there is a maximal ideal $\mathfrak{M} \subset \mathbf{A}_\mathfrak{p}$ such that $\mathfrak{M} \cap \mathbf{B}_\mathfrak{p} = \mathfrak{m}$. So we can put $\mathfrak{P} = \mathfrak{M} \cap \mathbf{A}$. $\square$

Proof of Theorem 3.2.11. As we are only interested in prime ideals $\mathfrak{q} \subseteq \mathfrak{p}$, we may replace $\mathbf{A}$ by its *localization* $\mathbf{A}_\mathfrak{p}$ (cf. Corollary 3.3.8). Hence, in what follows, we suppose that the ring $\mathbf{A}$ is *local* with the unique maximal ideal $\mathfrak{p}$ and $a \notin \mathfrak{q}$ for any prime ideal $\mathfrak{q} \neq \mathfrak{p}$. Replacing $\mathbf{A}$ by $\mathbf{A}/\sqrt{0}$, one may suppose that $\mathbf{A}$ is *reduced* (contains no nilpotents) or, the same, $\{\,0\,\}$ is a radical ideal. Consider its prime decomposition (cf. Corollary 1.5.9 and Exercise 1.5.10): $\{\,0\,\} = \bigcap_{i=1}^s \mathfrak{p}_i$. Then $\prod_{i=1}^s \mathfrak{p}_i = \{\,0\,\}$, hence, $\mathfrak{p}$ contains one of $\mathfrak{p}_i$ and $a \notin \mathfrak{p}_i$ as all elements from $\mathfrak{p}_i$ are zero divisors. Therefore, $\operatorname{ht}\mathfrak{p} > 0$. Suppose that $\mathfrak{p} \supset \mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal. Consider the factor-ring $\mathbf{A}/a\mathbf{A}$. It has a unique prime ideal $\mathfrak{p}/a\mathbf{A}$, hence, it is artinian by Lemma 3.3.16. It means that any descending chain of ideals of $\mathbf{A}$ containing a stabilizes. In particular, this is the case for the chain consisting of the ideals $a\mathbf{A} + \mathfrak{q}^{(k)}$, so, there is an integer k such that $a\mathbf{A} + \mathfrak{q}^{(k)} = a\mathbf{A} + \mathfrak{q}^{(k+1)}$. Taking any $b \in \mathfrak{q}^{(k)}$, we get $b = ac + d$ for some $c \in \mathbf{A}$, $d \in \mathfrak{q}^{(k)}$, whence $ac \in \mathfrak{q}^{(k)}$ and $sac \in \mathfrak{q}^k$ for some $s \notin \mathfrak{q}$ by Proposition 3.3.6(2). But $sa \notin \mathfrak{q}$, hence, also $c \in \mathfrak{q}^{(k)}$ and $\mathfrak{q}^{(k)} = a\mathfrak{q}^{(k)} + \mathfrak{q}^{(k+1)}$. By Corollary 3.3.12, $\mathfrak{q}^{(k)} = \mathfrak{q}^{(k+1)}$ (as $a \in \mathfrak{p}$), so $\mathfrak{q}$ is minimal by Corollary 3.3.14 and $\operatorname{ht}\mathfrak{p} = 1$. $\square$

The following corollary of Krull Hauptidealsatz precise Proposition 3.2.10.

COROLLARY 3.3.17. *Let* $a_1, a_2, \dots, a_m$ *be elements of a noetherian ring* $\mathbf{A}$, $\mathfrak{p}$ *be a minimal among prime ideals of* $\mathbf{A}$ *containing* $\langle a_1, a_2, \dots, a_m \rangle$. *Then* $\operatorname{ht} \mathfrak{p} \le m$.

To prove this corollary, we use some auxiliary results.

LEMMA 3.3.18. *Let* $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ *be prime ideals of a ring* $\mathbf{A}$, I *an ideal of* $\mathbf{A}$ *such that* $I \not\subseteq \mathfrak{p}_i$ *for all* i. *Then* $I \not\subseteq \bigcup_{i=1}^m \mathfrak{p}_i$.

PROOF. Use induction on m, the case $m = 1$ being trivial. Suppose the lemma valid for $m-1$ prime ideals. One may suppose that $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for $i \ne j$. Then $I\mathfrak{p}_m \not\subseteq \mathfrak{p}_i$ for $i < m$, hence, $I\mathfrak{p}_m \not\subseteq \bigcup_{i=1}^{m-1} \mathfrak{p}_i$. Let $a \in I\mathfrak{p}_m$ and $a \notin \bigcup_{i=1}^{m-1} \mathfrak{p}_i$. On the other hand, $I\mathfrak{p}_1 \dots \mathfrak{p}_{m-1} \not\subseteq \mathfrak{p}_m$. Take $b \in I\mathfrak{p}_1 \dots \mathfrak{p}_{m-1}$, and $b \notin \mathfrak{p}_m$. Then $a + b \in I$ and $a + b \notin \mathfrak{p}_i$ for all i, i.e., $a + b \notin\subseteq \bigcup_{i=1}^m \mathfrak{p}_i$. □

COROLLARY 3.3.19. *Let* $\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_m$ *be prime ideals of a noetherian ring* $\mathbf{A}$ *and* $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \dots \supset \mathfrak{p}_l$ *be a chain of prime ideals of* $\mathbf{A}$ *such that* $\mathfrak{p}_0 \not\subseteq \mathfrak{q}_i$ *for all* i. *Then there is a chain of prime ideals* $\mathfrak{p}_0 \supset \mathfrak{p}'_1 \supset \dots \supset \mathfrak{p}'_{l-1} \supset \mathfrak{p}_l$ *such that* $\mathfrak{p}'_j \not\subseteq \mathfrak{q}_i$ *for all* i, j.

PROOF. One may suppose that $\mathfrak{p}_l \subseteq \mathfrak{q}_i$ for all i, hence, replacing $\mathbf{A}$ by $\mathbf{A}/\mathfrak{p}_l$, that $\mathfrak{p}_l = \{0\}$. Using induction on l, one can also suppose that $\mathfrak{p}_{l-2} \not\subseteq \mathfrak{q}_i$ for all i, hence, there is $a \in \mathfrak{p}_{l-2}$, $a \notin \bigcup_{i=1}^m \mathfrak{q}_i$. Let $\mathfrak{p}'_{l-1}$ be a minimal prime ideal contained in $\mathfrak{p}_{l-2}$ and containing a. As $\operatorname{ht} \mathfrak{p}'_{l-1} = 1$, $\mathfrak{p}'_{l-1} \ne \mathfrak{p}_{l-2}$ and we get the necessary chain. □

PROOF OF COROLLARY 3.3.17. Use the induction on m, the case $m = 1$ following from Krull Hauptidealsatz. Let $\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_k$ be all minimal prime ideals containing $I = \langle a_1, a_2, \dots, a_{m-1} \rangle$ (the prime components of $\sqrt{I}$). If $\mathfrak{p} = \mathfrak{q}_i$ for some i, then $\operatorname{ht} \mathfrak{p} \le m - 1$. Suppose that $\mathfrak{p} \ne \mathfrak{q}_i$. Consider any chain of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \dots \supset \mathfrak{p}_l$, $l > 1$. By Corollary 3.3.19, one may suppose that $\mathfrak{p}_{l-1} \not\subseteq \mathfrak{q}_i$ for all i. Put $\overline{\mathbf{A}} = \mathbf{A}/I$, $\overline{a} = a + I \in \overline{\mathbf{A}}$, $\overline{\mathfrak{q}}_i = \mathfrak{q}_i/I$ and $\overline{\mathfrak{p}}_i = (\mathfrak{p}_i + I)/I$. Then $\overline{\mathfrak{p}} = \overline{\mathfrak{p}}_0$ is minimal among prime ideals of $\overline{\mathbf{A}}$ containing $\overline{a}_m$, hence, $\operatorname{ht} \overline{\mathfrak{p}} \le 1$. As $\overline{\mathfrak{q}}_i$ are all minimal prime ideals of $\overline{\mathbf{A}}$ and $\overline{\mathfrak{p}}_{l-1} \not\subseteq \overline{\mathfrak{q}}_i$, $\overline{\mathfrak{p}}$ is minimal among prime ideals of $\overline{\mathbf{A}}$ containing $\overline{\mathfrak{p}}_{l-1}$. Therefore, in $\mathbf{A}/\mathfrak{p}_{l-1}$, $\mathfrak{p}/\mathfrak{p}_{l-1}$ is minimal among the prime ideals containing all classes $a_i + \mathfrak{p}_{l-1}$ ($i = 1, \dots, m-1$). By the inductive hypothesis, $\operatorname{ht} \mathfrak{p}/\mathfrak{p}_{l-1} \le m - 1$, i.e., $l - 1 \le m - 1$ and $l \le m$. □

COROLLARY 3.3.20. $\operatorname{ht} \mathfrak{p} < \infty$ *for every prime ideal of a noetherian ring* $\mathbf{A}$. *In particular, any descending chain of prime ideals of a noetherian ring stabilizes.*
(Hence, any *ascending* chain of irreducible closed subsets of an algebraic variety stabilizes too.)

COROLLARY 3.3.21. $\operatorname{K.dim} \mathbf{A} < \infty$ *for any local noetherian ring* $\mathbf{A}$.

EXERCISES 3.3.22. (1) Let $a_1, a_2, \ldots, a_m$ be elements of a noetherian ring $\mathbf{A}$. Put, for $k \le m$, $I_k = \sqrt{\langle a_1, a_2, \ldots, a_k \rangle}$, in particular, $I_0 = \{0\}$. Suppose that $\langle a_1, a_2, \ldots, a_m \rangle \ne \mathbf{A}$. Prove that $\operatorname{ht} \mathfrak{p} = m$ for every minimal prime ideal $\mathfrak{p}$ among those containing $\langle a_1, a_2, \ldots, a_m \rangle$ if and only if, for every $k = 1, \ldots, m$, the class $a_k + I_{k-1}$ is non-zero-divisor in $\mathbf{A}/I_{k-1}$.

(2) Let $\mathfrak{p}$ be a prime ideal of a noetherian ring, $h = \operatorname{ht} \mathfrak{p}$. Prove that there are elements $a_1, a_2, \ldots, a_h \in \mathfrak{p}$ such that $\mathfrak{p}$ is minimal among prime ideals containing $\langle a_1, a_2, \ldots, a_h \rangle$ and, moreover, $\operatorname{ht} \mathfrak{q} = h$ for every prime ideal $\mathfrak{q}$ which is minimal among those containing $\langle a_1, a_2, \ldots, a_h \rangle$.

There is an important case when Krull Hauptidealsatz can be reversed. Remind some definitions.

DEFINITIONS 3.3.23. Let $\mathbf{A}$ be an integral ring.

(1) A non-zero, non-invertible element $a \in \mathbf{A}$ is called *irreducible* if, whenever $a = bc$ for some $b, c \in \mathbf{A}$, either b or c is invertible.

(2) The ring $\mathbf{A}$ is said to be *factorial* if every non-zero, non-invertible element from $\mathbf{A}$ is a product of irreducible elements and from $a_1 a_2 \ldots a_m = b_1 b_2 \ldots b_m$, where elements a_i and b_j are irreducible, it follows that $l = m$ and there is a permutation σ such that $b_i = u_i a_{\sigma(i)}$ for some invertible elements u_i and for all $i = 1, \ldots, m$.[3]

The most known examples of factorial rings are the polynomial rings $\mathbf{K}[x_1, \ldots, x_n]$ and the ring of integers $\mathbb{Z}$.

PROPOSITION 3.3.24. *Suppose that* $\mathbf{A}$ *is a* factorial *ring and* $\mathfrak{p} \subset \mathbf{A}$ *is a prime ideal of height* 1. *Then* $\mathfrak{p}$ *is a principal ideal:* $\mathfrak{p} = \langle a \rangle$ *for some irreducible element* a.

PROOF. As $\mathfrak{p}$ is prime, it contains an irreducible element a. But in a factorial ring the principle ideal $\langle a \rangle$ generated by an irreducible element is prime. As $\mathfrak{p} \supseteq \langle a \rangle \supset \{0\}$ and $\operatorname{ht} \mathfrak{p} = 1$, $\mathfrak{p} = \langle a \rangle$. □

EXERCISES 3.3.25. (1) Let $X \subseteq \mathbb{A}^n$ be a closed subvariety such that all its irreducible components are of dimension $n-1$. Prove that X is a hypersurface in $\mathbb{A}^n$.

(2) Prove that a noetherian ring $\mathbf{A}$ is factorial if and only if every prime ideal $\mathfrak{p} \subset \mathbf{A}$ of height 1 is principal.

Hint: It is enough to prove that, for any irreducible element $a \in \mathbf{A}$, the ideal $\langle a \rangle$ is prime.

[3] Note that if a ring $\mathbf{A}$ is *noetherian*, every non-zero, non-invertible element of $\mathbf{A}$ *is* a product of irreducible elements, so the only question is about the *uniqueness* of such a decomposition.

3.4. Normal varieties

To get more information about dimensions of algebraic varieties, we first consider a special class of rings and varieties, which is important in lots of questions.

DEFINITIONS 3.4.1. (1) An integral ring $\mathbf{A}$ with the field of fractions $\mathbf{Q}$ is called *normal* (or *integrally closed*) if all elements of $\mathbf{Q}$ which are integral over $\mathbf{A}$ belong to $\mathbf{A}$.

(2) An irreducible algebraic variety X is called *normal* if all local rings $\mathcal{O}_{X,p}$ ($p \in X$) are normal.

First we establish that for affine varieties these two definitions coincide.

PROPOSITION 3.4.2. (1) *If a ring $\mathbf{A}$ is normal, then the ring of fraction $\mathbf{A}[S^{-1}]$ for any multiplicative subset $S \subset \mathbf{A}$ is normal.*

(2) *A noetherian integral ring $\mathbf{A}$ is normal if and only if all its localizations $\mathbf{A}_\mathfrak{m}$, where $\mathfrak{m} \in \operatorname{Max} \mathbf{A}$, are normal.*

PROOF. *1.* We identify $\mathbf{A}[S^{-1}]$ with the subring $\{a/s \mid s \in S\}$ of $\mathbf{Q}$. Suppose that $r \in \mathbf{Q}$ is integral over $\mathbf{A}[S^{-1}]$, i.e., $r^m + c_1 r^{m-1} + \dots + c_m = 0$ with $c_i = a_i/s$ ($a_i \in \mathbf{A}, s \in S$; certainly, we can choose a common denominator for all c_i). Then $(sr)^m + a_1(sr)^{m-1} + sa_2(sr)^{m-2} \dots + s^{m-1}a_m = 0$, whence $sr \in \mathbf{A}$ and $r = sr/s \in \mathbf{A}[S^{-1}]$.

2. Let $r \in \mathbf{Q}$ be integral over $\mathbf{A}$. Then it is integral over all $\mathbf{A}_\mathfrak{m}$ for $\mathfrak{m} \in \operatorname{Max} \mathbf{A}$, whence $r \in \bigcap_{\mathfrak{m} \in \operatorname{Max} \mathbf{A}} \mathbf{A}_\mathfrak{m}$. So the following lemma accomplishes the proof:

LEMMA 3.4.3. *If $\mathbf{A}$ is an arbitrary integral noetherian ring, then $\mathbf{A} = \bigcap_{\mathfrak{m} \in \operatorname{Max} \mathbf{A}} \mathbf{A}_\mathfrak{m}$.*

PROOF. Let $r \in \bigcap_{\mathfrak{m} \in \operatorname{Max} \mathbf{A}} \mathbf{A}_\mathfrak{m}$. Put $I = \{a \in \mathbf{A} \mid ar \in \mathbf{A}\}$. It is an ideal in $\mathbf{A}$ and, for every maximal ideal $\mathfrak{m} \subset \mathbf{A}$, $I \not\subseteq \mathfrak{m}$ (as $r \in \mathbf{A}_\mathfrak{m}$, it can be written as $r = b/a$ with $a \in \mathbf{A} \setminus \mathfrak{m}, b \in \mathbf{A}$, whence $a \in I \setminus \mathfrak{m}$). Therefore, $I = \mathbf{A}$, so $1 \in I$ and $r = 1r \in \mathbf{A}$. □

An important example of normal ring are factorial ones, as the following result shows.

PROPOSITION 3.4.4. *Any factorial ring is normal.*

In particular, the rings of polynomials $\mathbf{K}[x_1, \dots, x_n]$ are normal, thus, affine (and projective) spaces are normal varieties.

PROOF. Let $\mathbf{Q}$ denote the field of fractions of a factorial ring $\mathbf{A}$ and $q = a/b \in \mathbf{Q}$ ($a, b \in \mathbf{A}$) be integral over $\mathbf{A}$: $q^m + c_1 q^{m-1} + \dots + c_m = 0$, where $c_i \in \mathbf{A}$. One may suppose that a and b have no common divisors (except invertible elements). But $a^m + c_1 a^{m-1} b + \dots + b^m c_m = 0$, so a^m is divisible by b, which is impossible, whenever b is not invertible. Hence, $1/b \in \mathbf{A}$ and $q \in \mathbf{A}$ too. □

Let $\mathbf{L}$ be a finite extension of a field $\mathbf{Q}$. If $a \in \mathbf{L}$, denote by $\mu_a(x)$ the *minimal polynomial* of a over $\mathbf{Q}$, i.e., the polynomial from $\mathbf{Q}[\,x\,]$ with the leading coefficient 1 of the smallest possible degree such that $\mu_a(a) = 0$. It is well known that such a polynomial is always irreducible and unique.

In what follows, we call polynomials with the leading coefficient 1 *monic polynomials*.

LEMMA 3.4.5. *If $\mathbf{A}$ is a normal ring with the field of fractions $\mathbf{Q}$ and a is an element of a finite extension $\mathbf{L}$ of $\mathbf{Q}$, which is integral over $\mathbf{A}$, then $\mu_a(x) \in \mathbf{A}[\,x\,]$.*

PROOF. Consider an extension $\mathbf{L}'$ of $\mathbf{L}$ such that $\mu_a(x) = \prod_{i=1}^m (x - a_i)$ for some $a_i \in \mathbf{L}'$. As $\mu_a(x)$ is irreducible, $\mathbf{Q}(a_i) \simeq \mathbf{Q}(a)$ and this isomorphism is identity on $\mathbf{Q}$. Hence, every a_i is also integral over $\mathbf{A}$. But the coefficients of $\mu_a(x)$ are polynomials of a_i with integral coefficients ("elementary symmetric polynomials"), so they are also integral over $\mathbf{A}$ (cf. Corollary 1.4.9). As $\mathbf{A}$ is normal, they belong to $\mathbf{A}$. $\square$

COROLLARY 3.4.6 (Lemma of Gauss). *Let $\mathbf{A}$ be a normal ring with the field of fractions $\mathbf{Q}$, $f \in \mathbf{A}[\,x\,]$ be a monic polynomial and $f = gh$, where $g \in \mathbf{Q}[\,x\,]$ is also monic. Then $g \in \mathbf{A}[\,x\,]$.*

PROOF. Certainly, it is enough to prove this claim for an *irreducible* g. Consider any root a of $g(X)$ in some extension of $\mathbf{Q}$. As $f(a) = 0$, a is integral over $\mathbf{A}$. But $g(x) = \mu_a(x)$ (as g is irreducible), so $g \in \mathbf{A}[\,x\,]$ by Lemma 3.4.5. $\square$

We also need the following version of Proposition 1.4.8.

LEMMA 3.4.7. *Let $\mathbf{A} \supseteq \mathbf{B}$ be an extension of rings, $M \subseteq \mathbf{A}$ be a finitely generated $\mathbf{B}$-submodule such that $\operatorname{Ann}_{\mathbf{A}}(M) = \{\,0\,\}$ and $aM \subseteq IM$, where I is an ideal from $\mathbf{B}$. Then:*

1. *There are elements $b_1, b_2, \dots, b_m \in I$ such that $f(a) = 0$, where $f(x) = x^m + b_1 x^{m-1} + \dots + b_m = 0$.*
2. *If I is a prime ideal and $\mathbf{B}$ is normal, all coefficients of $\mu_a(x)$ belong to I.*

PROOF. The proof of *1* is a slight modification of the proof of Proposition 1.4.8 (implication $4 \Rightarrow 1$). Namely, if $M = \langle\, u_1, u_2, \dots, u_m \,\rangle$ as $\mathbf{B}$-module, there are elements $c_{ij} \in I$ such that $au_j = \sum_i c_{ij} u_i$, whence $\det(aE - C) = 0$, where $C = (c_{ij})$. So we can put $f(x) = \det(xE - C)$.

2. One has $f(x) = \mu_a(x) g(x)$, where $f(x)$ is the polynomial constructed above and all polynomials are monic. Lemma of Gauss implies that both $\mu_a(x)$ and $g(x)$ belong to $\mathbf{B}[\,x\,]$. Modulo I this equality gives: $x^m \equiv \mu_a(x) g(x) \pmod{I}$. As $\mathbf{B}/I$ is integral, it implies that $\mu_a(x) \equiv x^d \pmod{I}$ ($d = \deg \mu_a$). $\square$

We are going to give a characterization of normal rings using their localizations with respect to *prime ideals of height* 1. First we prove some simple but useful facts concerning the so called *discrete valuation rings*.

DEFINITION 3.4.8. A *discrete valuation ring* is, by definition, an integral local ring of principal ideals, which is not a field.

PROPOSITION 3.4.9. *Let* $\mathbf{A}$ *be a local integral noetherian ring, which is not a field.* $\mathbf{A}$ *is a discrete valuation ring if and only if its maximal ideal* $\mathfrak{m}$ *is principal.*

PROOF. $\square$

THEOREM 3.4.10. *Let* $\mathbf{A}$ *be a local integral noetherian ring with the maximal ideal* $\mathfrak{m} \neq \{0\}$, $\mathbf{Q}$ *be the full ring of quotients of* $\mathbf{A}$. *The following conditions are equivalent:*

1. $\mathbf{A}$ *is normal of Krull dimension 1.*
2. $\mathbf{A}$ *is a discrete valuation ring.*
3. $\mathfrak{m}$ *is a principal ideal.*
4. $\mathbf{A}$ *is normal and there is an element* $r \in \mathbf{Q}$ *such that* $r \notin \mathbf{A}$ *but* $r\mathfrak{m} \subseteq \mathfrak{m}$.

In this case all proper non-zero ideals of $\mathbf{A}$ *coincide with* $\mathfrak{m}^k$ *for some* k.

PROOF. *2*$\Rightarrow$*1*: As $\mathbf{A}$ is principal ideal rings, it is factorial, hence, normal. As $\mathfrak{m}$ is principal, $\mathrm{K.dim}\,\mathbf{A} = \mathrm{ht}\,\mathfrak{m} = 1$ by Krull Hauptidealsatz.

3$\Rightarrow$*2*: Let $\mathfrak{m} = t\mathbf{A}$ for some t. Then $\mathfrak{m}^k = t^k\mathbf{A} \simeq \mathbf{A}$ as $\mathbf{A}$-module, so $\mathfrak{m}^{k+1}$ is the unique maximal submodule in $\mathfrak{m}^k$. Let I be any non-zero proper ideal in $\mathbf{A}$. Then $I \subseteq \mathfrak{m}$ and if $I \subseteq \mathfrak{m}^k$, then either $I \subseteq \mathfrak{m}^{k+1}$ or $I = \mathfrak{m}^k$. As $\mathrm{ht}\,\mathfrak{m} = 1$, $\mathfrak{m} = \sqrt{I}$, so $\mathfrak{m}^k \subseteq I$ for some k, whence $I \nsubseteq \mathfrak{m}^{k+1}$. Thus, there is k such that $I = \mathfrak{m}^k = \langle t^k \rangle$.

4$\Rightarrow$*3*: If $r\mathfrak{m} \subseteq \mathfrak{m}$, then r is integral over $\mathbf{A}$, thus $r \in \mathbf{A}$. Hence, $r\mathfrak{m} = \mathbf{A}$, i.e., $r^{-1} \in \mathbf{A}$ and $\mathfrak{m} = r^{-1}\mathbf{A}$.

1$\Rightarrow$*4*: Let a be a non-zero element from $\mathfrak{m}$. As $\mathrm{ht}\,\mathfrak{m} = \mathrm{K.dim}\,\mathbf{A} = 1$, $\mathfrak{m}$ is the unique minimal prime ideal containing a, thus $\mathfrak{m} = \sqrt{\langle a \rangle}$ and $\mathfrak{m}^k \subseteq \langle a \rangle$ for some k. Choose minimal possible k and an element $b \in \mathfrak{m}^{k-1} \setminus \langle a \rangle$. Put $r = b/a$. Then $b\mathfrak{m} \subseteq a\mathbf{A}$, thus, $r\mathfrak{m} \subseteq \mathbf{A}$ and $r \notin \mathbf{A}$. $\square$

THEOREM 3.4.11. *Let* $\mathbf{A}$ *be an integral noetherian ring, which is not a filed,* $P = \{\, \mathfrak{p} \in \mathrm{Spec}\,\mathbf{A} \mid \mathrm{ht}\,\mathfrak{p} = 1 \,\}$ *and* $\mathbf{Q}$ *be the field of quotients of* $\mathbf{A}$. $\mathbf{A}$ *is normal if and only if* $\mathbf{A} = \bigcap_{\mathfrak{p}\in P} \mathbf{A}_{\mathfrak{p}}$ *and every* $\mathbf{A}_{\mathfrak{p}}$, *where* $\mathfrak{p} \in P$, *is a discrete valuation ring.*

PROOF. Suppose all $\mathbf{A}_{\mathfrak{p}}$ ($\mathfrak{p} \in P$) being discrete valuation rings and $\mathbf{A} = \bigcap_{\mathfrak{p}\in P} \mathbf{A}_{\mathfrak{p}}$. If $r \in \mathbf{Q}$ is integral over $\mathbf{A}$, it is integral over each $\mathbf{A}_\mathfrak{p}$, hence, $r \in \mathbf{A}_\mathfrak{p}$ for every $\mathfrak{p} \in P$ as $\mathbf{A}_\mathfrak{p}$ is normal. Thus $r \in \bigcap_{\mathfrak{p}\in P} \mathbf{A}_\mathfrak{p} = \mathbf{A}$.

Suppose now $\mathbf{A}$ normal. Then all $\mathbf{A}_\mathfrak{p}$ are also normal, hence, if $\mathfrak{p} \in P$, they are discrete valuation rings by Theorem 3.4.10. Let $r \in \bigcap_{\mathfrak{p}\in P} \mathbf{A}_\mathfrak{p}$ but $r \notin \mathbf{A}$. Put $I = \{\, a \in \mathbf{A} \mid ar \in \mathbf{A} \,\}$. It is a proper ideal in $\mathbf{A}$ and $I \nsubseteq \mathfrak{p}$ for every $\mathfrak{p} \in P$. Let $\mathfrak{m}$ be a minimal prime ideal containing I. Then $r \notin \mathbf{A}_\mathfrak{m}$ and $\operatorname{K.dim} \mathbf{A}_\mathfrak{m} = \operatorname{ht} \mathfrak{p} > 1$. Moreover, $\mathfrak{m}\mathbf{A}_\mathfrak{m} = \sqrt{I\mathbf{A}_\mathfrak{m}}$, so $\mathfrak{m}^k\mathbf{A}_\mathfrak{m} \subseteq I\mathbf{A}_\mathfrak{m}$ for some k, which means $\mathfrak{m}^k\mathbf{A}_\mathfrak{m} r \subseteq \mathbf{A}_\mathfrak{m}$. Choose the minimal possible k and an element $a \in \mathfrak{m}^{k-1}\mathbf{A}_\mathfrak{m}$ such that $ar \notin \mathbf{A}_\mathfrak{m}$. Then $ar\mathfrak{m}\mathbf{A}_\mathfrak{m} \subseteq \mathbf{A}_\mathfrak{m}$, and $\mathbf{A}_\mathfrak{m}$ is normal, hence, it is of Krull dimension 1 by Theorem 3.4.10. Thus, we have got a contradiction, so $\mathbf{A} = \bigcap_{\mathfrak{p}\in P} \mathbf{A}_\mathfrak{p}$. □

This theorem allows an obvious "globalization":

Corollary 3.4.12. *Let X be an irreducible algebraic variety. X is normal if and only if the following two conditions hold:*

(1) *For every irreducible closed subvariety $Y \subset X$ of codimension 1, there is an open affine set $U \subseteq X$ such that $U \cap Y \neq \emptyset$ and the ideal $I(Y \cap U)$ is principal in $\mathbf{K}[\,U\,]$.*
(2) *If $p \in X$ and $f \in \mathbf{K}(X)$ are such that, for every irreducible closed $Y \subseteq X$ of codimension 1 with $p \in Y$, $\operatorname{Dom}(f) \cap Y \neq \emptyset$, then $p \in \operatorname{Dom}(f)$.*

Proof. Obviously, we can replace X by an open affine subset (intersecting Y for *1* and containing p for *2*). So we suppose X affine and put $\mathbf{A} = \mathbf{K}[\,X\,]$.

Suppose X normal. Let $Y \subseteq X$ be an irreducible closed subvariety of codimension 1. The ideal $\mathfrak{p} = I(Y)$ is of height 1 in the ring $\mathbf{A}$, hence, $\mathfrak{p}\mathbf{A}_\mathfrak{p} = t\mathbf{A}_\mathfrak{p}$ for some element $t \in \mathbf{A}$. Choose a set of generators of $\mathfrak{p}$: $\mathfrak{p} = \langle\, a_1, a_2, \dots, a_m \,\rangle$. Then $a_m = tb_m/s$, where $b_i \in \mathbf{A}$, $s \in \mathbf{A} \setminus \mathfrak{p}$. Put $U = D(s)$. Then $U \cap Y \neq \emptyset$ as $s \notin \mathfrak{p}$ and s is invertible on U. Therefore, in $\mathbf{K}[\,U\,]$, $I(U \cap Y) = \mathfrak{p}\mathbf{K}[\,U\,] = t\mathbf{K}[\,U\,]$, so, the condition *1* holds.

Let $f \in \mathbf{K}(X)$ is as in *2*, $\mathfrak{m} = \mathfrak{m}_p$ in $\mathbf{A} = \mathbf{K}[\,X\,]$. The prime ideals of $\mathbf{A}_\mathfrak{m}$ of height 1 are of the form $\mathfrak{p}\mathbf{A}_\mathfrak{m}$, where $\mathfrak{p}$ is a prime ideal of $\mathbf{A}$ of height 1 contained in $\mathfrak{m}$. Put $Y = V(\mathfrak{p})$. It is an irreducible subvariety of X of codimension 1, hence, there is a point $y \in Y \cap \operatorname{Dom}(f)$. It means that there are regular functions $a, b \in \mathbf{A}$ such that $b(y) \neq 0$ and $f = a/b$. Then $b \notin \mathfrak{m}_y \supseteq \mathfrak{p}$, hence, $f \in \mathbf{A}_\mathfrak{p}$. As it holds for every prime ideal $\mathfrak{p} \subseteq \mathfrak{m}$, $f \in \mathbf{A}_\mathfrak{m}$, i.e., $f = c/d$, where $c, d \in \mathbf{A}$, $d(p) \neq 0$, so $p \in \operatorname{Dom}(f)$.

Suppose now that *1* and *2* hold. Let $\mathfrak{p}$ be a prime ideal of $\mathbf{A}$ of height 1, $Y = V(\mathfrak{p})$ be the corresponding closed subvariety, which is irreducible and of codimension 1. Choose U as in 1; obviously, one may suppose it principal open: $U = D(g)$. As $U \cap Y \neq \emptyset$, $g \notin \mathfrak{p}$. Hence, $\mathbf{A}[\,g^{-1}\,] \subseteq \mathbf{A}_\mathfrak{p}$. But $\mathfrak{p}\mathbf{A}[\,g^{-1}\,] = t\mathbf{A}[\,g^{-1}\,]$ for some

t, so $\mathfrak{p}\mathbf{A}_\mathfrak{p} = (a/g^k)\mathbf{A}_\mathfrak{p}$ too and $\mathbf{A}_g P$ is a discrete valuation ring by Theorem 3.4.10.

Let $f \in \bigcap_{\mathfrak{p}\in P} \mathbf{A}_\mathfrak{p}$. It means that, for every closed irreducible Y of codimension 1, $\mathrm{Dom}(f) \cap Y \neq \emptyset$. Then $\mathrm{Dom}(f) = X$, so $f \in \mathbf{A}$. Hence, $\mathbf{A}$ is normal. □

We also note the following important property of normal varieties.

Corollary 3.4.13. *Let $f : X \to Y$ be a rational mapping, where the variety X is normal and Y is projective. Then* $\operatorname{codim} \operatorname{Irr}(f) > 1$.

Proof. One only have to prove that, for any irreducible closed $Z \subset X$ of codimension 1, $Z \cap \mathrm{Dom}(f) \neq \emptyset$. By Corollary 3.4.12, one may suppose that the ideal $\mathfrak{p} = I(Z)$ is principal in $\mathbf{A} = \mathbf{K}[\,X\,]$: $\mathfrak{p} = \langle\, t\,\rangle$. By Exercise 2.2.6(2), on an open subset $U \subseteq \mathrm{Dom}(f)$ f is given by the rule: $p \mapsto (f_0(p) : f_1(p) : \cdots : f_n(p))$, where $f_i \in \mathbf{A}$. In $\mathbf{A}_\mathfrak{p}$ we have: $\langle\, f_i\,\rangle = \langle\, t^{d_i}\,\rangle$ for some d_i. Let $d = \min\{\, d_i\,\}$. Then $g_i = t^{-d} f_i \in \mathbf{A}_\mathfrak{p}$ and at least one of these elements is invertible in $\mathbf{A}_\mathfrak{p}$. It means that $g_i = a_i/b$, where $a_i, b \in \mathbf{A}$ and there is a point $p \in Z$ such that $b(p) \neq 0$ and $a_j(p \neq 0)$ for at least one j. Then, on the open subset $U \cap D(t) \cap D(b) \cap D(a_j)$, f can be given by the rule: $p \mapsto (a_0(p) : a_1(p) : \cdots : a_n(p))$. But the latter rule defines a rational mapping on $U \cap D(b) \cap D(a_j)$ and this open set contains p. Hence, $p \in \mathrm{Dom}(f) \cap Z$. □

If X is a *curve*, there are no subvarieties of codimension 2, which gives the following results:

Corollary 3.4.14.
1. *Any rational mapping from a normal curve into a projective variety is regular.*
2. *If two normal projective curves are birationally equivalent, they are isomorphic.*

3.5. Dimensions of affine and projective varieties

The main fact concerning dimensions of algebraic varieties is the following theorem.

Theorem 3.5.1. *Let $\mathbf{A}$ be an integral affine algebra, $\mathfrak{p} \subset \mathbf{A}$ be a prime ideal. Then* $\mathrm{K.dim}\,\mathbf{A} = \mathrm{ht}\,\mathfrak{p} + \mathrm{K.dim}\,\mathbf{A}/\mathfrak{p}$.

This theorem can be “globalized” using the following notion.

Definition 3.5.2. Let Y be an irreducible subvariety of an algebraic variety X. The *codimension*, of Y $\operatorname{codim} Y$, is, by definition, the maximum of lengths l of chains of irreducible subvarieties $Y = Y_0 \supset Y_1 \supset Y_2 \supset \ldots \supset Y_l$. For an arbitrary subvariety $Y \subseteq X$ its *codimension* is defined as minimum of codimensions of its irreducible components.

The following theorem is just an obvious reformulation of Theorem 3.5.1 (using Proposition 3.2.3).

THEOREM 3.5.3. *Let* X *be an irreducible algebraic variety,* Y *its irreducible subvariety. Then* $\dim Y + \operatorname{codim} Y = \dim X$.

Its proof use Noether's Normalization Lemma and the following results precising Going-Up Principle for extensions of normal rings.

LEMMA 3.5.4. *Let* $\mathbf{A} \supseteq \mathbf{B}$ *be a finite extension of integral noetherian rings and* $\mathbf{B}$ *be normal. If* $\mathfrak{p}$ *is a prime ideal of* $\mathbf{B}$ *and* $\mathfrak{P}$ *is a minimal prime ideal of* $\mathbf{A}$ *containing* $\mathfrak{p}$ *, then* $\mathfrak{P} \cap \mathbf{B} = \mathfrak{p}$ *.*

PROOF. Put $J = \sqrt{\mathfrak{p}\mathbf{A}}$. Then minimal prime ideals of $\mathbf{A}$ containing $\mathfrak{p}$ are just prime components of J in the sense of Corollary 1.5.9 and Exercise 1.5.10. So there is finitely many of them: $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_r$, and $J = \bigcap_{i=1}^r \mathfrak{P}_i$. As $\mathfrak{P}_i \not\subseteq \mathfrak{P}$ for $i > 1$, also $P = \prod_{i=1}^r \mathfrak{P}_i \not\subseteq \mathfrak{P}$. Let $a \in P \setminus \mathfrak{P}$. Suppose that $\mathfrak{P} \cap \mathbf{B} = \mathfrak{p}' \supset \mathfrak{p}$ and $b \in \mathfrak{p}' \setminus \mathfrak{p}$. Then $ab \in \prod_{i=1}^r \mathfrak{P}_i \subseteq J$, hence, $a^k b^k \in \mathfrak{p}\mathbf{B}$ for some k . As $a^k \notin \mathfrak{P}$ and $b^k \in \mathfrak{p}' \setminus \mathfrak{p}$, we may (and do) suppose that already $ab \in \mathfrak{p}\mathbf{A}$. Hence, the minimal polynomial of ab is of the form $x^m + c_1 x^{m-1} + \dots + c_m$ with $c_i \in \mathfrak{p}$. In this case, the minimal polynomial of a is $x^m + d_1 x^{m-1} + \dots + d_m$, where $c_i = b^i d_i$. As $b \notin \mathfrak{p}$, then $d_i \in \mathfrak{p}$ for all i , whence $a^m \in \mathfrak{p}\mathbf{A} \subseteq \mathfrak{P}$, which is impossible as $a \notin \mathfrak{P}$. □

COROLLARY 3.5.5. *Let* $\mathbf{A} \supseteq \mathbf{B}$ *be a finite extension of integral noetherian rings and* $\mathbf{B}$ *be normal. If* $\mathfrak{q} \subset \mathfrak{p}$ *are prime ideals of* $\mathbf{B}$ *and* $\mathfrak{P}$ *is a prime ideal of* $\mathbf{A}$ *containing* $\mathfrak{p}$ *, there is a prime ideal* $\mathfrak{Q} \subset \mathfrak{P}$ *of* $\mathbf{A}$ *such that* $\mathfrak{Q} \cap \mathbf{B} = \mathfrak{q}$ *.*

PROOF. One can take for $\mathfrak{Q}$ any minimal prime ideal of $\mathbf{A}$ containing $\mathfrak{q}$ and contained in $\mathfrak{P}$. (Such ideals exist in view of Corollary 3.3.20.) □

COROLLARY 3.5.6. *Let* $\mathbf{A} \supseteq \mathbf{B}$ *be a finite extension of integral noetherian rings and* $\mathbf{B}$ *be normal. For any prime ideal* $\mathfrak{P}$ *of* $\mathbf{A}$ *,* $\operatorname{ht} \mathfrak{P} = \operatorname{ht}(\mathfrak{P} \cap \mathbf{B})$ *.*

PROOF. Put $\mathfrak{p} = \mathfrak{P} \cap \mathbf{B}$. Let $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_l$ be any chain of prime ideals in $\mathbf{B}$. Corollary 3.5.5 implies that in $\mathbf{A}$ there is a chain of prime ideals $\mathfrak{P} = \mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \dots \subset \mathfrak{P}_l$ such that $\mathfrak{P}_i \cap \mathbf{B} = \mathfrak{p}_i$. Hence, $\operatorname{ht} \mathfrak{P} \geq \operatorname{ht} \mathfrak{p}$. On the other hand, if $\mathfrak{P} = \mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \dots \subset \mathfrak{P}_l$ is a chain of prime ideals in $\mathbf{A}$ and $\mathfrak{p}_i = \mathfrak{P}_i \cap \mathbf{B}$, then in $\mathbf{B}$ we get a chain of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_l$ (cf. Lemma 3.1.14). Hence, also $\operatorname{ht} \mathfrak{p} \geq \operatorname{ht} \mathfrak{P}$. □

PROOF OF THEOREM 3.5.1. Put $d = \mathrm{K.}\dim \mathbf{A}$, $h = \operatorname{ht} \mathfrak{p}$. First we prove this theorem for the case $h = 1$. Using Noether's Normalization Lemma, find a subalgebra $\mathbf{B} \subseteq \mathbf{A}$ such that $\mathbf{B} \simeq \mathbf{K}[x_1, \dots, x_d]$

and $\mathbf{A}$ is integral over $\mathbf{B}$. As $\mathbf{B}$ is factorial, hence, normal, also $\operatorname{ht}\mathfrak{p}\cap\mathbf{B} = 1$ by Corollary 3.5.6. So, $\mathfrak{p}\cap\mathbf{B}$ is a principal ideal by Proposition 3.3.24: $\mathfrak{p}\cap\mathbf{B} = \langle f \rangle$, where f is an irreducible polynomial. In view of Lemma 1.4.10, one may suppose that $f = x_d^m + g_1x_d^{m-1} + \dots + g_m$, where $g_i \in \mathbf{K}[x_1,\dots,x_{d-1}]$. Then the subring $\mathbf{B}' = \mathbf{K}[x_1,x_2,\dots,x_{d-1},f]$ is also isomorphic to $\mathbf{K}[x_1,\dots,x_d]$ and $\mathbf{B}$ is integral over $\mathbf{B}'$, hence also $\mathbf{A}$ is integral over $\mathbf{B}'$ (cf. Corollary 1.4.9). Therefore, one may suppose that $\mathbf{B} = \mathbf{B}'$, so $\mathfrak{p}\cap\mathbf{B} = \langle x_d \rangle$ and $\overline{\mathbf{B}} = \mathbf{B}/(\mathfrak{p}\cap\mathbf{B}) \simeq \mathbf{K}[x_1,\dots,x_{d-1}]$. But $\mathbf{A}/\mathfrak{p}$ is integral over $\overline{\mathbf{B}}$, so $\operatorname{K.dim}\mathbf{A}/\mathfrak{p} = \operatorname{K.dim}\overline{\mathbf{B}} = d-1$ by Theorems 3.2.7 and 3.2.6.

Now we use the induction on d. The case $d = 1$ is covered by the preceding consideration. So suppose that the claim is valid for affine algebras of dimension $d-1$. Let $\operatorname{ht}\mathfrak{p} = h$. Consider one of the longest chains of prime ideals ending at $\mathfrak{p}$: $\langle 0 \rangle = \mathfrak{p}_0 \subset \mathfrak{q} = \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \dots \subset \mathfrak{p}_h = \mathfrak{p}$. Then $\operatorname{ht}\mathfrak{q} = 1$, so $\operatorname{K.dim}\mathbf{A}/\mathfrak{q} = d-1$. But $\operatorname{ht}\mathfrak{p}/\mathfrak{q} = h-1$, therefore, by the inductive hypothesis, $\operatorname{K.dim}\mathbf{A}/\mathfrak{p} = \operatorname{K.dim}(\mathbf{A}/\mathfrak{q})/(\mathfrak{p}/\mathfrak{q}) = (d-1)-(h-1) = d-h$. □

Corollary 3.5.7. *Let X be an irreducible affine variety of dimension d, $Y = V(S) \subseteq X$, where $S = \{f_1,f_2,\dots,f_m\} \subset \mathbf{K}[X]$. If $Y \neq \emptyset$, then $\dim Y_i \geq d-m$ for every irreducible component Y_i of Y.* (In particular, if $m < d$, Y is *infinite*.)

Proof. Let $Y = \bigcup_i Y_i$ be the irreducible decomposition of Y, $I = I(Y) = \sqrt{\langle S \rangle}$ and $\mathfrak{p}_i = I(Y_i)$. Then $\mathfrak{p}_i$ are the prime components of I. Hence, they are minimal prime ideals containing S, so $\operatorname{ht}\mathfrak{p}_i \leq m$ by Corollary 3.3.17 and $\dim Y_i = \operatorname{K.dim}\mathbf{K}[X]/\mathfrak{p}_i \geq d-m$ by Theorem 3.5.1. □

Exercises 3.5.8. Let X be an irreducible affine variety of dimension n, $\mathbf{A} = \mathbf{K}[X]$ and Y be a closed subvariety of X.

(1) Suppose that $Y = V(f_1,f_2,\dots,f_m)$, where $f_i \in \mathbf{A}$. Prove that all components of Y have dimension $n-m$ if and only if, for every $k = 1,\dots,m$, the class of f_k in $\mathbf{K}[\mathbf{x}]/\sqrt{\langle f_1,f_2,\dots,f_{k-1} \rangle}$ is non-zero-divisor.
In this case one says that Y is a *set complete intersection* in X. If, moreover, $\langle S \rangle = I(Y)$, one says that Y is a *complete intersection* in X. $k = 1,\dots,m$, the class of f_k in $\mathbf{K}[\mathbf{x}]/\sqrt{\langle f_1,f_2,\dots,f_{k-1} \rangle}$ is non-zero-divisor.
In this case one says that Y is a *set complete intersection* in X. If, moreover, $\langle S \rangle = I(Y)$, one says that Y is a *complete intersection* in X.

(2) If Y is irreducible and $\operatorname{codim} Y = m$, prove that there are elements $f_1,f_2,\dots,f_m \in \mathbf{A}$ such that Y is a component of $Z = V(f_1,f_2,\dots,f_m)$ and all components of Z are of codimension m too.

In particular, for every point $p \in X$, there are n elements $f_1, f_2, \dots, f_n \in \mathbf{A}$ such that $V(f_1, f_2, \dots, f_n)$ is finite and contains p.

(3) Let $X = V(xy - z^2) \subset \mathbb{A}^3$, $Y = V(\overline{x}) \subset X$, where $\overline{x}$ is the image of x in $\mathbf{K}[X]$. Show that Y is a set complete intersection, but not a complete intersection in X.

Hint: Use Exercise 3.3.15.

Note one more property of subvarieties of *affine spaces*.

Exercise 3.5.9. Let X, Y be irreducible subvarieties of $\mathbb{A}^n$ of dimensions, respectively, m and k, such that $X \cap Y \neq \emptyset$. Prove that if Z is an irreducible component of $X \cap Y$, then $\dim Z \geq m + k - n$.
Hint: Use the isomorphism $Z \simeq X \times Y \cap \Delta_{\mathbb{A}^n} \subseteq \mathbb{A}^n \times \mathbb{A}^n \simeq \mathbb{A}^{2n}$ and write the equations defining $\Delta^n_{\mathbb{A}}$ inside $\mathbb{A}^{2n}$.

Analogous, and to some extent even better results can be obtained for *projective* varieties. Let $X = PV(S) \subseteq \mathbb{P}^n$ be a projective variety, where $S \subseteq \mathbf{K}[\mathbf{x}] = \mathbf{K}[x_0, x_1, \dots, x_n]$. Remind that the *(affine) cone* over X is, by definition, the affine variety $\tilde{X} = V(S) \subseteq \mathbb{A}^{n+1}$. Certainly, a closed subvariety $Z \subseteq \mathbb{A}^{n+1}$ is a cone over some projective variety if and only if $I(Z)$ is a homogeneous ideal. We also consider $\{0\}$ as the affine cone over the empty set.

Proposition 3.5.10. *Let $X \subseteq \mathbb{P}^n$ be a projective variety, $\tilde{X}$ be the affine cone over X. Then:*

(1) *X is irreducible if and only if so is $\tilde{X}$.*
(2) *Irreducible components of $\tilde{X}$ coincide with the affine cones over irreducible components of X.*
(3) *If X is irreducible, then $\mathbf{K}(\tilde{X}) \simeq \mathbf{K}(X)(t)$, where t is transcendent over $\mathbf{K}(X)$. (In particular, $\tilde{X}$ is also irreducible).*
(4) $\dim \tilde{X} = \dim X + 1$.

Proof. *1* follows from the equality $I(\tilde{X}) = I(X)$ as an affine or projective variety is irreducible if and only if its ideal is prime.

2. Let $X = \bigcup_i X_i$ be the irreducible decomposition of X. Then $\tilde{X} = \bigcup_i \tilde{X}_i$ and all $\tilde{X}_i$ are irreducible. Hence, it is the irreducible decomposition of $\tilde{X}$.

3. Suppose that X is irreducible and choose i such that $X \cap \mathbb{A}^n_i = U \neq 0$. Then U is open dense in X, so $\mathbf{K}(X) = \mathbf{K}(U)$. To simplify the notations, suppose that $i = 0$. The affine coordinates on U are x_i/x_0 ($i = 1, \dots, n$), hence, rational functions on U are restrictions of rational fractions F/G, where $F, G \in \mathbf{K}[\mathbf{x}]$ are both homogeneous and $\deg F = \deg G$. The affine coordinates on $\tilde{X}$ are $x_0, x_1, \dots, x_n$, so $\mathbf{K}(\tilde{X}) = \mathbf{K}(U)(t)$, where t denotes the restriction of x_0 onto $\tilde{X}$ (it is non-zero as $X \cap \mathbb{A}^n_0 \neq \emptyset$). Suppose that $t^k + a_1 t^{k-1} + \dots + a_k = 0$, where $a_i \in \mathbf{K}(U)$. This equality means that $F_0 x_0^k + F_1 x_0^{k-1} + \dots + F_k \in I(X)$

for some homogeneous polynomials F_i, which all have the same degree and $F_0 \neq 0$. As $I(X)$ is homogeneous, it implies that $F_0 x_0^k \in I(X)$, hence, $x_0 \in I(X)$ as $I(X)$ is prime. Then $X \cap \mathbb{A}_0^n = \emptyset$, which contradicts our choice. Therefore, t is transcendent over $\mathbf{K}(X)$.

4 evidently follows from *2* and *3*. □

Now we are able to translate all "affine" results to the projective case.

COROLLARY 3.5.11. *Let $X \subseteq \mathbb{P}^n$ be an irreducible projective variety of dimension d, $Y = PV(S) \cap X$, where $S = \{ F_1, F_2, \dots, F_m \}$ and $m \le d$. Then $Y \neq \emptyset$ and $\dim Y_i \ge d - m$ for every irreducible component Y_i of Y.*
In particular, if $m = 1$ and $X \nsubseteq PV(S)$, $\dim Y_i = m - 1$.

PROOF. Certainly, $\tilde{Y} = V(S) \cap \tilde{X}$. In particular, as S consists of homogeneous polynomials, $\tilde{Y} \neq \emptyset$. As $\dim \tilde{X} = d+1$, Corollary 3.5.7 implies that all components of $\tilde{Y}$ are of dimension $d+1-m > 0$. In particular, $\tilde{Y} \neq \{ 0 \}$, so $Y \neq \emptyset$. By Proposition 3.5.10, all components of Y are of dimension $d - m$. □

EXERCISES 3.5.12.
(1) Let $X \subset \mathbb{P}^n$ be a projective variety such that all components of X are of dimension $n-1$. Prove that X is a hypersurface in $\mathbb{P}^n$.
(2) Let $X, Y \subseteq \mathbb{P}^n$ are irreducible subvarieties of dimensions, respectively, m and k. Prove that, if $m + k \le n$, $X \cap Y \neq \emptyset$ and $\dim Z \ge m + k - n$ for each component Z of $X \cap Y$.
(3) Let $X\mathbb{P}^n$ be a projective variety. Prove that $\dim X = m - 1$, where m is the minimal integer such that there are m hypersurfaces $H_1, H_2, \dots, H_m \subset \mathbb{P}^n$ with $X \cap (\bigcap_{i=1}^m H_i) = \emptyset$.
(4) Prove that, for any m, n, $\mathbb{P}^m \times \mathbb{P}^n \not\simeq \mathbb{P}^{m+n}$.

3.6. Dimensions of fibres

Let $f : X \to Y$ be a morphism of algebraic varieties. For every point $p \in Y$, the fibre $f^{-1}(p)$ is a closed subvariety of X. The following result describe the possibilities for its dimension.

THEOREM 3.6.1. *Let $f : X \to Y$ be a dominant morphism of irreducible algebraic varieties. Then:*
(1) *For every $p \in \operatorname{Im} f$ and for every component Z of $f^{-1}(p)$, $\dim Z \ge \dim X - \dim Y$.*
(2) *Y contains an open dense subset $U \subseteq \operatorname{Im} f$ such that $\dim f^{-1}(p) = \dim X - \dim Y$ (hence, $\dim Z = \dim X - \dim Y$ for every component Z of $f^{-1}(p)$).*

PROOF. Replacing Y by an affine neighbourhood of p and X by an affine neighbourhood of an arbitrary point $z \in f^{-1}(p)$, one may suppose that X and Y are affine. Then there is a finite dominant mapping $\varphi : Y \to \mathbb{A}^n$, where $m = \dim Y$ (Theorem3.2.5). For every point $q \in \mathbb{A}^n$, $\varphi^{-1}(q)$ is finite (cf. Theorem 3.1.12): $\varphi^{-1}(q) = \{ p_1, p_2, \dots, p_k \}$. Hence, $(\varphi \circ f)^{-1}(q) = \bigsqcup_{i=1}^k f^{-1}(p_i)$ (disjoint union) and irreducible components of each $f^{-1}(p_i)$ are also irreducible components of $(\varphi \circ f)^{-1}(q)$. Thus, one may suppose $Y = \mathbb{A}^n$. For every point $p \in \mathbb{A}^n$, $\mathfrak{m}_p$ is generated by n polynomials: $\mathfrak{m}_p = \langle h_1, h_2, \dots, h_n \rangle$. Hence, $f^{-1}(p) = V(f^*(h_1), \dots, f^*(h_n))$, so the assertion *1* follows from Corollary 3.5.7.

To prove *2*, use the same observations as in Chevalley's Theorem (Theorem 3.1.17). Namely, consider $\mathbf{B} = \mathbf{K}[x_1, \dots, x_n]$ as the subalgebra of $\mathbf{A} = \mathbf{K}[X]$ (the image of f^*), choose a transcendence basis $\{ b_1, b_2, \dots, b_d \}$ of $\mathbf{K}(X)$ over $\mathbf{K}(x_1, \dots, x_m)$ such that $a_i \in \mathbf{A}$ and consider algebraic equations $c_{i0} a_i^k + c_{i1} a_i^{k-1} + \dots + \dots c_{ik} = 0$ for a set of generators $\{ a_1, a_2, \dots, a_r \}$ of $\mathbf{A}$ over $\mathbf{B}[a_1, \dots, a_d] = \mathbf{K}[[_1, \dots, [\,]d + n]$ and $c_{ij} \in \mathbf{K}[[_1, \dots, [\,]d + n]$. Then $d = m - n$, where $m = \operatorname{tr.deg} \mathbf{K}(X) = \dim X$ (cf. Corollary A.3). Moreover, if $V = D(g) \subseteq \mathbb{A}^n$, where $g = \prod_{i=1}^k c_{i0}$, the restriction of f onto $f^{-1}(V)$ decomposes as $f^{-1}(V) \xrightarrow{\varphi} V \overset{\pi\, n}{\mathbb{A}}$, where φ is a finite mapping and π is the projection. Put $U = \pi(V)$. It is open (hence, dense) and, for any $p \in U$, the restriction of φ onto $f^{-1}(p)$ induces a finite mapping $f^{-1}(p) \to \pi^{-1}(p) \simeq \mathbb{A}^d$ (cf. Exercise 3.1.10(4)). Therefore, $\dim f^{-1}(p) = d = m - n$. $\square$

Corollary 3.6.2. *Let $f : X \to Y$ be a surjective morphism of irreducible algebraic varieties. Put $Y_d = \{ p \in Y \mid \dim f^{-1}(y) \geq d \}$. Then all subsets Y_d are closed in Y.*
In other words, the function $Y \to \mathbb{N}$, $p \mapsto \dim f^{-1}(p)$ is *upper semicontinuous*.

Proof. By Theorem 3.6.1, $Y_d = Y_{m-n}$ is closed if $d \leq m - n$, where $m = \dim X$, $n = \dim Y$, and there is a proper closed subset $Z \subseteq Y$ such that $Y_d \subseteq Z$ for $d > n - m$. Let $Z = \bigcup_{i=1}^k$ be the irreducible decomposition of Z. Using the noetherian induction, we may suppose that, for every d, $Z_{id} = \{ z \in Z_i \mid \dim f^{-1}(z) \geq d \}$ is closed in Z_i, hence, in Y. As $Y_d = \bigcup_{i=1}^k Z_{id}$, it is also closed. $\square$

Exercise 3.6.3. Consider the quadratic Cremona transformation mapping $\varphi : \mathbb{P}^2 \to \mathbb{P}^2$, $\varphi(x_0, x_1, x_2) = (x_1 x_2 : x_2 x_0 : x_0 x_1)$. Find all fibres $\varphi^{-1}(p)$. Where $\dim \varphi^{-1}(p) \neq 0$?

We apply Theorem 3.6.1 to the *action of algebraic groups.* First introduce the necessary definitions.

Definitions 3.6.4. (1) An *algebraic group* is an algebraic variety G together with a multiplication law $\mu : G \times G \to G$, $(g, h) \mapsto gh$ such that:
(a) G with the multiplication law μ is a group;

   (b) mappings μ and $\delta : G \to G$, $\delta(g) = g^{-1}$ are regular.
(2) Let G be an algebraic group, X an algebraic variety. An *action* of G on X is a regular mapping $G\times X \to X$, $(g,p) \to gp$, such that:
   (a) $1p = p$ for all $p \in X$ (1 denotes the *unit* of the group G);
   (b) $g(hp) = (gh)p$ for all $g,h \in G$, $p \in X$.
(3) Let an algebraic group G act on a variety X. The *stabilizer* of an element $p \in X$ in the group G is the subgroup $\operatorname{St} p = \{\, g \in G \mid gp = p \,\}$. The *orbit* Gp of this element is the set $\{\, gp \mid g \in G \,\}$.

EXAMPLE 3.6.5. Consider the *full linear group* $G = \mathrm{GL}(n, \mathbf{K})$. It coincides with the principle open subset $D(\det) \subset \mathrm{Mat}(n \times n, \mathbf{K}) \simeq \mathbb{A}^{n^2}$. Thus, G is an affine variety and $\mathbf{K}[\,G\,] = \mathbf{K}[\,x_{ij}\,][\,\det^{-1}\,]$. Then the formulae for the product of matrices and of the inverse matrix show that G is indeed an algebraic group.

A lot of groups arise as closed subgroups of $\mathrm{GL}(n, \mathbf{K})$. For instance, the *special linear group* $\mathrm{SL}(n, \mathbf{K}) = \{\, g \in \mathrm{GL}(n, \mathbf{K}) \mid \det g = 1 \,\}$; the *orthogonal group* $\mathbf{O}(n, \mathbf{K}) = \left\{\, g \in \mathrm{GL}(n, \mathbf{K}) \mid gg^\top = 1 \,\right\}$, etc. One can prove that any *affine group*, i.e., an algebraic group whose underlying variety is affine, is isomorphic to a closed subgroup of $\mathrm{GL}(n, \mathbf{K})$.

Note the following obvious facts.

PROPOSITION 3.6.6. *Let an algebraic group G act on a variety X. For any element $p \in X$:*
(1) *$\operatorname{St} p$ is a closed subgroup in G.*
(2) *Gp is a subvariety (i.e., a locally closed subset) in X.*
(3) *$\dim Gp = \dim G - \dim \operatorname{St} p$.*

PROOF. Consider the mapping $f : G \to X$, $g \to gp$. It is regular. Now *1* is evident as $\operatorname{St} p = f^{-1}(p)$. By Theorem 3.1.17, Gp is constructible, hence, contains an open subset V of its closure $\overline{Gp}$. Choose a point $v \in V$. Then $\overline{Gp = Gv}$. If $z \in Gv$, $z = gv$, then $z \in gV$ and gV is open in $g(\overline{Gp}) = \overline{g(Gp)} = \overline{Gp}$, as the mapping $x \to gx$ is an automorphism of the algebraic variety X. Hence, $Gp = \bigcup_{g\in G} gV$ is open in $\overline{Gp}$, i.e., locally closed in X, which proves *2*. To prove *3*, suppose first G irreducible. Then Gp is irreducible as well. If $y = gp \in Gp$, one easily check that $f^{-1}(y) = g \operatorname{St} p \simeq \operatorname{St} p$ (as varieties). Hence, by Theorem 3.6.1, $\dim Gp = \dim G - \dim \operatorname{St} p$. General case is obtained from the following simple observation, which is proposed as a simple exercise.

EXERCISES 3.6.7. (1) Let G be an algebraic group, G° be its irreducible component containing 1. Then G° is a normal closed subgroup of finite index in G and every irreducible component of G is of the form gG° for some $g \in G$.

(2) Two different irreducible components have no common points. So, particular, the irreducible components coincide with the *connected components* of G. In particular, G is irreducible if and only if it is connected.
(3) Accomplish the proof of Proposition 3.6.6 for reducible group G.

$\square$

The following result is often useful.

PROPOSITION 3.6.8. *Let an algebraic group G act on an irreducible algebraic variety X. Then there is an open set $V \subseteq X$ such that $\dim Gv = \max\{\,\dim Gp \mid p \in X\,\}$ for every $v \in V$.*

PROOF. We consider the case when G is connected (or, the same, irreducible); the non-connected case being left as an easy exercise. Consider the regular mapping $\varphi : G \times X \to X \times X$, $\varphi(g,p) = (gp,p)$. Let $\Gamma = \varphi^{-1}(\Delta_X)$ and $\psi = \mathrm{pr}_X \circ \varphi|_\Gamma$ (never mind, which of two projections we choose). Then ψ is surjective and, for every point $p \in X$, $\psi^{-1}(p) = \mathrm{St}\, p \times \{\,p\,\} \simeq \mathrm{St}\, p$. By Theorem 3.6.1, there is an open subset $V \subseteq X$ such that $\dim \mathrm{St}\, v = \min\{\,\dim \mathrm{St}\, p \mid p \in X\,\}$ for any $v \in V$. Then, by Proposition 3.6.6, $\dim Gv = \max\{\,\dim Gp \mid p \in X\,\}$. $\square$

Note one more useful corollary.

COROLLARY 3.6.9. *Let an algebraic group G act on an irreducible variety X and there are only finitely many orbits of G on X. Then there is an open orbit and $\dim X \le \dim G - \min\{\,\dim \mathrm{St}\, p \mid p \in X\,\}$.*

PROOF. We have $X = \bigcup_{i=1}^m Gp_i$, hence $X = \bigcup_{i=1}^m \overline{Gp_i}$. As X is irreducible, there is j such that $X = \overline{Gp_j}$. Then Gp_j is open in X by Proposition 3.6.6 and $\dim X = \dim Gp_j = \dim G - \dim \mathrm{St}\, p_j$. $\square$

EXERCISES 3.6.10.

3.7. Normalization

There is a rather simple procedure allowing to reduce a lot of question concerning algebraic varieties to the case of normal ones. We introduce first the corresponding definition.

DEFINITION 3.7.1. Let X be an algebraic variety. The *normalization* of X is, by definition, a finite mapping $\nu : \tilde{X} \to X$ such that $\tilde{X}$ is normal and ν is birational.

THEOREM 3.7.2. *For every irreducible algebraic variety X there is a normalization $\nu : \tilde{X} \to X$. Moreover, if $\nu' : X' \to X$ is another normalization, there is a unique isomorphism $f : X' \to \tilde{X}$ such that $\nu' = \nu \circ f$.*

One often calls $\tilde{X}$ itself *"the" normalization* of X (especially, taking into account the uniqueness of ν up to an automorphism of $\tilde{X}$).

Proof. Let X be an affine variety, $\mathbf{A} = \mathbf{K}[X]$, $\mathbf{Q}$ be the field of fraction of $\mathbf{A}$ and $\tilde{\mathbf{A}}$ be the integral closure of $\mathbf{A}$ in $\mathbf{Q}$, i.e., the set of all elements of $\mathbf{Q}$ which are integral over $\mathbf{A}$. We use the following lemma, which will be proved further.

Lemma 3.7.3. *Let $\mathbf{A}$ be an integral affine algebra, $\mathbf{Q}$ its field of fractions, $\mathbf{F}$ a finite extension of $\mathbf{Q}$ and $\mathbf{B}$ the integral closure of $\mathbf{A}$ in $\mathbf{F}$. Then $\mathbf{B}$ is finitely generated as an $\mathbf{A}$-module. (In particular, it is also an affine algebra.)*

Accordingly to this lemma, $\tilde{\mathbf{A}}$ is an affine algebra, hence, $\tilde{\mathbf{A}} = \mathbf{K}[\tilde{X}]$ for some *normal* algebraic variety $\tilde{X}$. The inclusion $\mathbf{A} \to \tilde{\mathbf{A}}$ induces a finite morphism $\nu : \tilde{\mathbf{A}} \to \mathbf{A}$. It is also birational as the filed of fractions of $\tilde{\mathbf{A}}$ coincides with $\mathbf{Q}$. Hence, ν is a normalization of X . Suppose that $\nu' : X' \to X$ is another normalization. Then X' is also an affine variety (cf. Corollary 3.1.3). Put $\mathbf{A}' = \mathbf{K}[X']$. As ν' is dominant, it induces the embedding $\nu'^* : \mathbf{A}' \to \mathbf{A}$. Moreover, as ν' is birational, ν'^* induces an isomorphism $\mathbf{Q}' \to \mathbf{Q}$, where $\mathbf{Q}'$ is the field of fractions of $\mathbf{A}'$. We denote this isomorphism by φ and consider $\varphi(\mathbf{A}')$ as a subring of $\mathbf{Q}$. It contains $\mathbf{A}$ and is integral over $\mathbf{A}$, hence, it is contained in $\tilde{\mathbf{A}}$. Moreover, $\tilde{\mathbf{A}}$ is integral over $\varphi(\mathbf{A}')$ (as it is integral over $\mathbf{A}$), hence, $\tilde{\mathbf{A}} = \varphi(\mathbf{A}')$ (as $\mathbf{A}'$ is normal), i.e., φ induces an isomorphism of $\mathbf{A}'$ onto $\tilde{\mathbf{A}}$. By Proposition 1.2.2, there is an isomorphism $f : X' \to \tilde{X}$ such that $f^* : \tilde{\mathbf{A}} \to \mathbf{A}'$ is the isomorphism inverse to φ . Then $\nu' = \nu \circ f$. The uniqueness of f follows immediately from the fact that both ν and ν' are dominant.

Let now X be an arbitrary irreducible variety, $X = \bigcup_{i=1}^m X_i$ be its open affine covering. First prove the *uniqueness* of a normalization (provided it exists). Indeed, let $\nu : \tilde{X} \to X$ and $\nu' : X' \to X$ are two normalizations, $\tilde{X}_i = \nu^{-1}(X_i)$ and $X'_i = \nu'^{-1}(X_i)$. Then both $\tilde{X}_i$ and X'_i are normalization of X_i , hence, there are unique isomorphisms $f_i : X'_i \xrightarrow{\sim} \tilde{X}_i$ such that $\nu'_{X'_i} = \nu_i|_{\tilde{X}_i} \circ f_i$. Obviously, f_i and f_j coincide on $X'_i \cap X'_j$, hence, one can glue them into an isomorphism $f : x' \to \tilde{X}$.

To prove the *existence*, denote by $\nu_i : \tilde{X}_i \to X_i$ a normalization of X_i , $\tilde{X}_{ij} = \nu_i^{-1}(X_i \cap X_j)$. The restriction ν_{ij} of ν_i onto $\tilde{X}_{ij}$ is obviously a normalization of $X_i \cap X_j$. In view of the uniqueness of a normalization, there is a unique isomorphism $\varphi_{ij} : \tilde{X}_{ij} \to \tilde{X}_{ji}$ such that $\nu_{ij} = \nu_{ji} \circ \varphi_{ij}$. Moreover, for any three indices i, j, k , $\varphi_{ik} = \varphi_{jk} \circ \varphi ij$ on the preimage $\varphi_{ij}^{-1}(\tilde{X}_{jk}) = \nu_i^{-1}(X_i \cap X_j \cap X_k)$ (as ν_{ij} are all surjective). Certainly, also $\tilde{X}_{ii} = \tilde{X}_i$ and $\varphi_{ii} = \mathrm{id}$. Therefore, we are able to apply the following "*gluing procedure*":

Proposition 3.7.4. *Suppose given a set of spaces with functions* Z_i *, open subsets* $Z_{ij} \subseteq Z_{ij}$ *given for every pair* i, j *and isomorphisms* $\eta_{ij} : Z_{ij} \xrightarrow{\sim} Z_{ji}$ *satisfying the following conditions:*

(1) $Z_{ii} = Z_i$ *and* $\eta_{ii} = \mathrm{id}$ *for each* i .
(2) *For every triple of indices* i, j, k , $Z_{ij} \cap \eta_{ji}(Z_{jk}) \subseteq Z_{ik}$ *and the restrictions of* η_{ik} *and of* $\eta_{jk} \circ \eta_{ij}$ *onto this intersection coincide.*

Put $Z = \bigcup_i Z_i / \sim$ *, where* $z \sim z'$ *means that, for some pair* i, j , $z \in Z_{ij}$ *and* $z' = \eta_{ij}(z)$ *. Call a subset* $U \subseteq Z$ open *if* $U \cap Z_i$ *is open for every* Z_i *and define* $\mathcal{O}_Z(U)$ *to be the set of all functions* $f : U \to \mathbf{K}$ *such that* $f|_{U \cap Z_i} \in \mathcal{O}_{Z_i}(()U \cap Z_i)$ *for every* i *. Then:*

(1) $(Z, \mathcal{O}_Z)$ *is a space with functions.*
(2) *For every* $z \in Z_i$, $\mathcal{O}_z^{Z_i} \simeq \mathcal{O}_z^{Z}$.
(3) *If every* U *is an algebraic variety and there is only finitely many of them,* Z *is also an algebraic variety.*
(4) *Given for every* i *a morphism of spaces with function* f_i : $Z_i \to X$ *such that* $f_i|_{Z_{ij}} = f_j \circ \eta_{ij}|_{Z_{ij}}$ *for all* i, j *, there is a unique morphism* $f : Z \to X$ *such that* $f|_{Z_i} = f_i$ *for all* i .

The proof of this proposition, which consists of routine verifications, is left as an exercise.

Applying Proposition 3.7.4 to the varieties $\tilde{X}_i$ and isomorphisms φ_{ij} , we get an algebraic variety $\tilde{X}$, which is normal as all $\tilde{X}_i$ are normal. Moreover, one gets a morphism $\nu : \tilde{X} \to X$ such that $\nu|_{\tilde{X}_i} = \nu_i$. As every of ν_i is finite, ν is finite as well. It is also birational as each X_i is dense in X and $\tilde{X}_i$ is dense in $\tilde{X}$. Hence, $\nu : \tilde{X} \to X$ is a normalization. $\square$

Note that, in view of Exercises 3.1.16, a normalization of a separated variety is separated and a normalization of a complete variety is complete. Indeed, one can prove that a normalization of a projective (quasi-projective) variety is always projective (quasi-projective). Nevertheless, this prove is rather sharpened and we are not going to put it here. In the contrary, the case of *curves* is much simpler and can be handled with the help of the following lemma, which is of independent interest as well.

Lemma 3.7.5 (Chow's Lemma). *For every irreducible variety* X *there is a quasi-projective variety* X' *and a surjective morphism* f : $X' \to X$ *which is a birational mapping. If* X *is complete,* X' *can be chosen projective.*

Proof. Let $X = \bigcap_{i=1}^k U_i$ be an open affine covering of X , $U = \bigcup_{i=1}^k U_i$. As X is irreducible, U is dense. One can embed every U_i in a projective space. Denote by X_i its closure there; they are projective varieties, hence, their product $P = \prod_{i=1}^k X_i$ is projective as well. Consider the "diagonal" mapping $\varphi : U \to X \times P$: $p \to (p, p, \dots, p)$, and put $X' = \overline{\operatorname{Im}\varphi}$ (the closure). Let f and g be the restrictions on X' of the projections pr_X and pr_P respectively. We prove that f is birational and g is an immersion. It proves the lemma. (Note that, if X is complete, so is X'; hence, in this case, $\operatorname{Im} g \simeq X'$ is a projective variety.)

Let $V = f^{-1}(U) = X' \cap (U \times P)$. As $\operatorname{Im}\varphi$ coincides with the graph of the diagonal mapping $U \to P$, it is closed in $U \times P$, hence, $V = X' \cap (U \times P) = \operatorname{Im}\varphi$ and the projection $V \to U$ is an isomorphism. As U and V are dense, respectively, in X and X', f is birational.

Let now $\mathrm{pr}_i = \mathrm{pr}_{X_i} : P \to X_i$ and $V_i = \mathrm{pr}_i^{-1}(U_i)$. The restriction of $\mathrm{pr}_i \circ g$ onto $V = f^{-1}(U)$ coincides with $f|_V : V \to U$. As V is dense, they also coincide on U_i, i.e., $g^{-1}(V_i) = f^{-1}(U_i)$ and $\bigcap_{i=1}^k g^{-1}(V_i) = X'$. Therefore, one only has to show that the restriction of g onto $g^{-1}(V_i)$ is an immersion (as the notion of an immersion is obviously local). Put $P_i = \prod_{j \neq i} X_j$. Then $V_i \subseteq U_i \times P_i$ and $g^{-1}(V_i) \subseteq X \times U_i \times P_i$. Moreover, $g^{-1}(V_i)$ coincides with the intersection of X' with the graph Z_i of the composition $U_i \times P_i \xrightarrow{\mathrm{pr}_i} U_i \to X$, the second arrow denoting the embedding. But Z_i is closed in $X \times U_i \times P_i$ and pr_P maps it isomorphically onto $V_i = U_i \times P_i$. As $g^{-1}(V_i) = X' \cap Z_i$ is closed in Z_i, $g|_{g^{-1}(V_i)}$ is an immersion. $\square$

COROLLARY 3.7.6. *A complete normal curve is projective. I particular, a normalization of a complete (for instance, of a projective) curve is projective.*

PROOF. If $f : X' \to X$ is a birational morphism, X' is projective and X is normal, then the inverse rational mapping $f^{-1} : X \to X'$ is regular (cf. Corollary 3.4.14), i.e., f is an isomorphism. $\square$

EXERCISE 3.7.7. Prove that, for every finitely generated extension $\mathbf{L} \supset \mathbf{K}$ of transcendence degree 1, there is a unique projective normal curve X such that $\mathbf{L} = \mathbf{K}(X)$. Moreover, if $\mathbf{L}' \subset \mathbf{K}$ is another finitely generated extension of transcendence degree one, $\mathbf{L}' \simeq \mathbf{K}(X')$ for a normal projective curve X', then every homomorphism $\mathbf{L} \to \mathbf{L}'$ is induced by a unique morphism $X' \to X$.

(One can say that the *category* of finitely generated extensions of $\mathbf{K}$ of transcendence degree 1 is *dual* to that of normal projective curves. So, in a sense, the theory of normal projective curves is a chapter of the field theory.)

EXERCISE 3.7.8. Let Y be a normal, X a complete variety and $f : Y \to X$ be a rational mapping. Prove that $\operatorname{codim} Z \geq 2$ for every component Z of $\operatorname{Irr}(f)$.

EXERCISE 3.7.9. Let X be an algebraic variety, $X = \bigcup_{i=1}^m$ be its irreducible decomposition. Show that the mapping $\bigsqcup_{i=1}^m X_i \to X$ ($\bigsqcup$ denotes the *disjoint union*), which is identity on every X_i, is finite and birational. Conclude that there is a finite birational mapping $\nu : \bigsqcup_{i=1}^{m} \tilde{X}_i \to X$, where $\tilde{X}_i$ is a normalization of X_i.

We still have to prove Lemma 3.7.3. To do it, we first precise a bit Noether's Normalization Lemma.

LEMMA 3.7.10. *Let* $\mathbf{A}$ *be an integral affine algebra,* $\mathbf{Q}$ *be its field of fractions. There is a subalgebra* $\mathbf{B} \subseteq \mathbf{A}$ *such that:*

(1) $\mathbf{B} \simeq \mathbf{K}[x_1, \dots, x_n]$.
(2) $\mathbf{A}$ *is integral over* $\mathbf{B}$.
(3) $\mathbf{Q}$ *is separable over the field of fractions* $\mathbf{F}$ *of* $\mathbf{B}$.

PROOF. We follow the proof of Noether's Normalization Lemma with small changes. Certainly, one only has to consider the case when $\operatorname{char} \mathbf{K} = p > 0$.

Let $\mathbf{A} = \mathbf{K}[a_1, \dots, a_n]$. Just as in the proof of Noether's Normalization Lemma, find a polynomial F such that $F(a_1, a_2, \dots, a_n) = 0$. As $\mathbf{A}$ is integral, F can be chosen irreducible. Then there is an index i such that $\partial F/\partial x_i \neq 0$ (cf. the proof of Proposition A.4). One may suppose $i = n$. Apply an automorphism of $\mathbf{K}[x_1, x_2, \dots, x_n]$, as in Lemma 1.4.10, but with t a multiple of p. Then $\partial(\varphi(F))/\partial x_n = \partial F/\partial x_n \neq 0$. Hence, one may suppose that $\mathbf{A}$ is integral over $\mathbf{A}' = \mathbf{K}[a_1, \dots, a_{n-1}]$ and $\mathbf{Q}$ is separable over the ring of fractions of $\mathbf{A}'$. An obvious induction accomplishes the proof. □

Now Lemma 3.7.3 is an immediate corollary of the following general result.

PROPOSITION 3.7.11. *Let* $\mathbf{A}$ *be a normal noetherian ring with the field of fractions* $\mathbf{Q}$, $\mathbf{L}$ *be a finite separable extension of* $\mathbf{Q}$. *Then the integral closure* $\mathbf{B}$ *of* $\mathbf{A}$ *in* $\mathbf{L}$ *is finitely generated as* $\mathbf{A}$*-module.*

PROOF. Remind that an extension $\mathbf{L} \subseteq \mathbf{Q}$ is separable if and only if the bilinear form $\mathbf{L} \times \mathbf{L} \to \mathbf{K}$, $(a, b) \to \operatorname{Tr}(ab)$ is non-degenerated. Let $\{a_1, a_2, \dots, a_n\}$ be a base of $\mathbf{L}$ over $\mathbf{Q}$ such that all a_i are integral over $\mathbf{A}$, $\{a_1^*, a_2^*, \dots, a_n^*\}$ be the *dual base*, i.e., such that $Tr(a_i a_j^*) = \delta_{ij}$. If an element $b = \sum_{i=1}^{n} c_i a_i^* \in \mathbf{L}$ ($c_i \in \mathbf{A}$) is integral over $\mathbf{A}$, so are all products ba_i. In particular, $\operatorname{Tr}(ba_i) = c_i \in \mathbf{A}$ (as $\mathbf{A}$ is normal, cf. Lemma 3.4.5). Therefore, $\mathbf{B}$ is a submodule of the finitely generated $\mathbf{A}$-module $\langle a_1^*, a_2^*, \dots, a_n^* \rangle$, hence, is finitely generated itself (cf. Proposition 1.4.6). □

CHAPTER 4

Regular and singular points

4.1. Regular rings and smooth varieties

Definitions 4.1.1. Let $\mathbf{A}$ be a local noetherian ring with the maximal ideal $\mathfrak{m}$.

(1) Call the *embedding dimension* of $\mathbf{A}$ the number of generators $\#_{\mathbf{A}}(M)$ of $\mathfrak{m}$ as of $\mathbf{A}$-module. Denote the embedding dimension of $\mathbf{A}$ by $\mathrm{e.dim}\,\mathbf{A}$.
Accordingly to Corollary 3.3.17, $\mathrm{e.dim}\,\mathbf{A} \geq \mathrm{K.dim}\,\mathbf{A}$.

(2) Call the ring $\mathbf{A}$ *regular* if $\mathrm{e.dim}\,\mathbf{A} = \mathrm{K.dim}\,\mathbf{A}$.

Remind that $\mathrm{e.dim}\,\mathbf{A} = \dim_{\mathbf{K}} \mathfrak{m}/\mathfrak{m}^2$, where $\mathbf{K} = \mathbf{A}/\mathfrak{m}$ (cf. Corollary 3.3.13).

Definitions 4.1.2. Let X be an algebraic variety, $p \in X$.

(1) Call the point p *regular* (on X) if the local ring $\mathcal{O}_{X,p}$ is regular. Otherwise call this point *singular* (on X). Denote by X_{reg} the set of all regular points and by X_{sing} that of all singular points of the variety X.

(2) Call the variety X *smooth* (or *regular*) if all points $p \in X$ are regular. Otherwise, call X *singular*.

Example 4.1.3. Affine space $\mathbb{A}^n$ and projective space $\mathbb{P}^n$ are smooth varieties. Indeed, $\dim \mathbb{A}^n = n$ and the maximal ideal of every point of $\mathbb{A}^n$ in $\mathbf{K}[\mathbb{A}^n] = \mathbf{K}[x_1, \dots, x_n]$ has n generators. Every point of $\mathbb{P}^n$ has a neighbourhood isomorphic to $\mathbb{A}^n$.

Note the following simple result.

Proposition 4.1.4. *The Krull dimension* $\mathrm{K.dim}\,\mathcal{O}_{X,p}$ *coincide with* $\max \dim X_i$, *where* X_i *runs through all components of* X *containing the point* p.
(One denotes this maximum by $\dim_p X$ and call it the *dimension of the variety* X *at the point* p.)

Proof. Evidently, one may suppose X affine. Let $\mathbf{A}$ be its coordinate algebra, $\mathfrak{m}_p \subset \mathbf{A}$ the maximal ideal corresponding to the point p, $\mathbf{A}_p = \mathbf{A}_{\mathfrak{m}_p} = \mathcal{O}_{X,p}$ (cf. Proposition 3.3.9). Then $\mathfrak{m} = \mathfrak{m}_p \mathbf{A}_p$ is the maximal ideal of $\mathbf{A}_p$ and every chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_l$ in $\mathbf{A}_p$ corresponds to a chain of prime ideals of $\mathbf{A}$ contained in $\mathfrak{m}_p$ (cf. Corollary 3.3.8). But such a chain is the same as a chain of irreducible subvarieties of X containing p, which is always contained in some irreducible component (certainly, containing p). So, indeed, $\mathrm{K.dim}\,\mathcal{O}_{X,p} = \max \dim X_i$. $\square$

In what follows, we denote by $\mathfrak{m}_{X,p}$ the maximal ideal of the local ring $\mathcal{O}_{X,p}$ and put $\mathrm{e.dim}_p X = \mathrm{e.dim}\,\mathcal{O}_{X,p}$ (the *embedding dimension of* X at the point p). Hence, the point p is regular on X if and only if $\dim_p X = \mathrm{e.dim}_p X$.

EXERCISE 4.1.5. Let X be a normal variety, Z be a component of the set X_{sing} of its singular points. Prove that $\operatorname{codim} Z \geq 2$.

Hint: If $\operatorname{codim} Z = 1$, one may suppose that X is affine and $I(Z)$ is principal in $\mathbf{K}[X]$. Show that if z is a regular point of Z, it is a regular point of X as well.

We are going to establish a *criterion* for a point of an algebraic variety to be regular. As this notion is local, we only have to consider the affine case.

THEOREM 4.1.6 (Jacobian criterion). *Let $X \subseteq \mathbb{A}^n$ be an affine variety, $I = I(X) = \langle F_1, F_2, \dots, F_m \rangle$ and $p \in X$. The point p is simple on X if and only if $\mathrm{Jrk}_p(I) = n - \dim_p X$, where $\mathrm{Jrk}_p(I)$ denotes the rank of the matrix $\left(\dfrac{\partial F_i}{\partial x_j}(p) \right)$ ($i = 1, \dots, m$, $j = 1, \dots, n$).*

PROOF. To simplify the notations, we suppose that $p = (0, \dots, 0)$. Let $\mathbf{A} = \mathbf{K}[X] = \mathbf{K}[x_1, \dots, x_n]/I$, $\mathfrak{m} = \mathfrak{m}_p = \mathfrak{n}/I$, where $\mathfrak{n} = \langle x_1, x_2, \dots, x_n \rangle \subset \mathbf{K}[\mathbf{x}]$. Then $\mathrm{e.dim}\,\mathbf{A} = \dim_{\mathbf{K}} \mathfrak{m}/\mathfrak{m}^2 = \dim_{\mathbf{K}} \mathfrak{n}/(\mathfrak{n}^2 + I) = \dim_{\mathbf{K}} \mathfrak{n}/\mathfrak{n}^2 - \dim_{\mathbf{K}}(\mathfrak{n}^2 + I)/\mathfrak{n}^2 = n - \dim_{\mathbf{K}}(\mathfrak{n}^2 + I)/\mathfrak{n}^2$. The last dimension, obviously, equals the number of linear independent among $F_1^{(1)}, F_2^{(1)}, \dots, F_m^{(1)}$, where $F_i^{(1)}$ denotes the linear part of F_i, which equals $\sum_{j=1}^n x_j \partial F_i/\partial x_j(p)$. It implies the assertion of the theorem. $\square$

EXERCISE 4.1.7 (Projective Jacobian criterion). Let $X \subset \mathbb{P}^n$ be a projective variety, $I(X) = \langle F_1, F_2, \dots, F_m \rangle$. Prove that a point $p \in X$ is regular if and only if $\mathrm{rk}(\partial F_i/\partial x_j)(p) = n - \dim_p X$.

Hint: Consider the canonical affine covering. Use the Jacobian criterion for affine varieties and the Euler formula: $\sum_{j=0}^n \partial F/\partial x_j = dF$ if F is a homogeneous polynomial of degree d.

COROLLARY 4.1.8. *If X is an irreducible variety, X_{reg} is an open dense subset in X.*[1]

PROOF. Again one may assume X affine. Theorem 4.1.6 obviously implies that X_{reg} is open, so one only has to show that it is non-empty. According to Proposition 2.5.4, X is birationally equivalent either to $\mathbb{A}^n$ or to a hypersurface in $\mathbb{A}^{n+1}$, where $n = \dim X$. As $\mathbb{A}^n$ is smooth, one only has to prove that $X_{\mathrm{reg}} \neq \emptyset$ if $X = V(F) \subset \mathbb{A}^{n+1}$, where F is an irreducible polynomial.

[1] We will see later that it is also true for *arbitrary* varieties.

But $\partial F/\partial x_i \neq 0$ for some i (cf. the proof of Proposition A.4), hence, $\partial F_i/\partial x_i \notin \langle F \rangle$ (as it is of a smaller degree). Therefore, there is a point $p \in X$ such that $\partial F/\partial x_i(p) \neq 0$. By Theorem 4.1.6, this point is regular. $\square$

4.2. Structure of regular local rings

THEOREM 4.2.1 (Artin–Rees Theorem). *Let $\mathbf{A}$ be a noetherian ring, M be a finitely generated $\mathbf{A}$-module, I be an ideal in $\mathbf{A}$ and N be a submodule in M. There is an integer $k \geq 0$ such that, for all integers $n \geq 0$, $I^{n+k}M \cap N = I^n(I^k \cap N)$.*

PROOF. Put $\mathbf{B} = \bigoplus_{n=0}^{\infty} I^n$. As $I^n I^m \subseteq I^{n+m}$, $\mathbf{B}$ can be considered as a ring. To precise the "position" of an element $b \in I^n$ in this ring, we shall often denote it by $b(n)$. If $\{ a_1, a_2, \dots, a_m \}$ is a generating set of the ideal I, the elements $a_1(1), \dots, a_m(1)$ generate $\mathbf{B}$ as $\mathbf{A}$-algebra. Hence, $\mathbf{B}$ is isomorphic to a factor-algebra of $\mathbf{A}[x_1, \dots, x_m]$, hence, it is noetherian (by Hilbert's Basis Theorem). In the same way, putting $\mathbf{M} = \bigoplus_{n=1}^{\infty} I^n M$, we get a finitely generated $\mathbf{B}$-module. By Proposition 1.4.6, it is also noetherian. Thus its submodule $\mathbf{N} = \bigoplus_{n=1}^{\infty} I^n M \cap N$ is finitely generated. Let $\{ u_1(k_1), u_2(k_2), \dots, u_r(k_r) \}$ be its generating set, $k = \max k_i$. Then, for every $n \geq 0$ and every element $v \in I^{k+n}M \cap N$, there are elements $b_i \in I^{k+n-k_i}$ such that $v = \sum_{i=1}^{r} b_i u_i$, whence $v \in I^n(I^k M \cap n)$. $\square$

COROLLARY 4.2.2. *Let $\mathbf{A}$ be a noetherian ring, M a finitely generated $\mathbf{A}$-module and I an ideal of $\mathbf{A}$ such that $\mathrm{Ann}_M(1+a) = \{ 0 \}$ for every $a \in I$. Then $\bigcap_{i=1}^{n} I^n M = \{ 0 \}$.*

PROOF. Put $N = \bigcap_{i=1}^{n} I^n M$. By Artin–Rees Theorem, there is k such that $N = I^{k+1}M \cap N = I(I^k M \cap N) = IN$. Let $N = \langle u_1, u_2, \dots, u_m \rangle$. Then, for every j, $u_j = \sum_{i=1}^{m} a_{ij} u_i$ with $a_{ij} \in I$. Standard (and a lot of times yet used) arguments show that $\det(E - (a_i j))u_i = 0$ for all i. As this determinant is of the form $1 + a$ with $a \in I$, $u_i = 0$ and $N = \{ 0 \}$. $\square$

This corollary is evidently applicable, when $\mathbf{A} = M$ is a local noetherian ring and $I = \mathfrak{M}$ is its maximal ideal.

COROLLARY 4.2.3. *If $\mathbf{A}$ is a local noetherian ring with the maximal ideal $\mathfrak{M}$, then $\bigcap_{n=1}^{\infty} \mathfrak{M}^n = \{ 0 \}$.*

COROLLARY 4.2.4. *In the situation of Corollary 4.2.3, for every finitely generated $\mathbf{A}$-module M and its submodule N, $N = \bigcap_{k=1}^{\infty} (\mathfrak{m}^k M + N)$.*

PROOF. One should only apply Corollary 4.2.2 to the factor-module M/N. $\square$

Let now $\mathbf{A}$ be a local noetherian ring, $\mathfrak{m}$ be its maximal ideal, $\mathbf{K} = \mathbf{A}/\mathfrak{m}$ and $\{t_1, t_2, \dots, t_n\}$ be a minimal set of generators of $\mathfrak{m}$ (so, $n = \operatorname{e.dim} \mathbf{A} \geq \operatorname{K.dim} \mathbf{A}$). Fix, for every class $\lambda \in \mathbf{K}$, its representative $\hat{\lambda}$ in $\mathbf{A}$. In particular, we suppose that $\hat{0} = 0$ and $\hat{1} = 1$. Consider any formal power series $F \in \mathbf{K}[[x_1, \dots, x_n]]$:

$$F = \sum_{\mathbf{k}} \lambda_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} = \sum_{k_1, k_2, \dots, k_n} \lambda_{k_1 k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}.$$

We write $a \equiv \hat{F}(t_1, t_2, \dots, t_n) \pmod{\mathfrak{m}^k}$ if $a \equiv \sum_{|\mathbf{k}|<k} \hat{\lambda}_{\mathbf{k}} \mathbf{t}^{\mathbf{k}} \pmod{\mathfrak{m}^k}$. (Here, as usual, $\mathbf{k} = (k_1, k_2, \dots, k_n)$, $|\mathbf{k}| = k_1 + \dots + k_n$ and $\mathbf{t}^{\mathbf{k}} = t_1^{k_1} \dots t_n^{k_n}$.)

PROPOSITION 4.2.5. *For every element $a \in \mathbf{A}$ there is a power series $F \in \mathbf{K}[[x_1, \dots, x_n]]$ such that, for every k, $a \equiv \hat{F}(t_1, t_2, \dots, t_n) \pmod{\mathfrak{m}^k}$. Moreover, if $a \neq 0$, also $F \neq 0$.*

We call a power series F_a with these properties a *Taylor series* of the element a and write $a \equiv F$.

PROOF. We construct $F_a = \sum_{k=1}^{\infty} F_k$, where F_k is a form of degree k, using the induction by k. Note that the congruence $a \equiv \hat{F}(t_1, t_2, \dots, t_n) \pmod{\mathfrak{m}^k}$ only depends on $F_0, F_1, \dots, F_{k-1}$. Put $F_0 = a + \mathfrak{m} \in \mathbf{K}$. Suppose now that $F_0, F_1, \dots, F_{k-1}$ have already been constructed. Then the element $b = a - \sum_{d=1}^{k-1} \hat{F}_d(t_1, t_2, \dots, t_n)$ belongs to $\mathfrak{m}^k$, hence, $b = \sum_{|\mathbf{k}|=k} b_k \mathbf{t}^{\mathbf{k}}$ and one can put $F_k = \sum_{|\mathbf{k}|=k} \lambda_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}$, where $\lambda_{\mathbf{k}} = b_{\mathbf{k}} + \mathfrak{m}$.

If $a \equiv 0$, then $a \in \mathfrak{m}^k$ for every k, so, $a = 0$ by Corollary 4.2.3. □

Certainly, one cannot guarantee the *uniqueness* of a Taylor series. Indeed, let $A = \mathcal{O}_{X,p}$, where $X = V(x^2 - y^3) \subset \mathbb{A}^2$ and $p = (0, 0)$. Then $\mathfrak{m} = \langle x, y \rangle$. (Note that p is a singular point of X, so, $\operatorname{e.dim} \mathbf{A} > \operatorname{K.dim} \mathbf{A} = 1$.) Hence, 0 and $x^2 - y^3$ are two different Taylor series of 0. We shall see now that the only reason of this phenomenon is the singularity of the point p.

THEOREM 4.2.6. *Let $\mathbf{A}$ be a local noetherian ring, $\mathfrak{m} = \langle t_1, t_2, \dots, t_n \rangle$ be its maximal ideal ($n = \operatorname{e.dim} \mathbf{A}$). The following conditions are equivalent:*

(1) *$\mathbf{A}$ is regular (i.e., $\operatorname{K.dim} \mathbf{A} = n$).*
(2) *For every element $a \in \mathbf{A}$, the Taylor series of a is unique.*
(3) *For every $i = 1, \dots, n$, the class of the element t_i is non-zero-divisor in $\mathbf{A}/\langle x_1, \dots, x_{i-1} \rangle$. (For $i = 1$, it means that x_1 is non-zero-divisor in $\mathbf{A}$.)*

PROOF. *1 ⇒ 2* will only be proved for the case of an *infinite residue field* $\mathbf{K}$. (Note that it is always so in the "geometric" situation, when $\mathbf{A} = \mathcal{O}_{X,p}$.) For the case of a finite residue field cf. Exercise 4.2.10.

Certainly, one only has to prove that if $0 \equiv F$, then $F = 0$. Suppose that $F \neq 0$ and k is the minimal integer such that there are terms of degree k in F. Let F_k be the sum of all these terms. As $\mathbf{K}$ is infinite, there is a point $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{A}^n_{\mathbf{K}}$ such that $F_k(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$. A linear change of variables maps this point to $(0, \ldots, 0, 1)$. Such a change correspond to another choice of a minimal set of generators of $\mathfrak{m}$. So, one may suppose $F_k(0, \ldots, 0, 1) \neq 0$, i.e., $F_k = \lambda x_n^k + F'$, where $\lambda \neq 0$ and every term from F' contains some x_i with $i < n$. As $0 \equiv F$, it gives that $\hat{\lambda} t_n^k + \sum_{i=1}^{n-1} b_i t_i \in \mathfrak{m}^{k+1}$ for some $b_i \in \mathbf{A}$, where $\hat{\lambda} \notin \mathfrak{m}$. Therefore, $\hat{\lambda} t_n^k = c t_n^{k+1} + \sum_{i=1}^{n-1} c_i t_i$ for some $c_i \in \mathbf{A}$. But $\hat{\lambda} - c t_n \notin \mathfrak{m}$, so it is invertible and $t^k \in \langle t_1, t_2, \ldots, t_{n-1} \rangle$. Hence, we get $\mathfrak{m}^k \subseteq \langle t_1, t_2, \ldots, t_{n-1} \rangle$, whence $\mathfrak{m} = \sqrt{\langle t_1, t_2, \ldots, t_{n-1} \rangle}$ and $\mathrm{K.dim}\,\mathbf{A} = \mathrm{ht}\,\mathfrak{m} \leq n-1$ by Corollary 3.3.17, which contradicts the assumption: $\mathrm{K.dim}\,\mathbf{A} = n$.

2⇒3. Suppose that $a \notin I = \langle t_1, t_2, \ldots, t_{i-1} \rangle$. Then, by Corollary 4.2.4, $a \notin I + \mathfrak{m}^k$ for some k. Consider the Taylor series F of a. Among its terms of degrees less than k at least one contains neither of the variables $x_1, x_2, \ldots, x_{i-1}$. But, obviously, the Taylor series of $t_i a$ is $x_i F$, whence $t_i a \notin I$ (even $t_i a \notin I + \mathfrak{m}^{k+1}$).

3⇒1 will be proved by induction on $n = \mathrm{e.dim}\,\mathbf{A}$. If $n = 1$, then $\mathrm{K.dim}\,\mathbf{A} = \mathrm{ht}\,\mathfrak{m} = 1$ by Krull Hauptidealsatz(as t_1 is non-zero-divisor). Hence, $\mathbf{A}$ is regular. Suppose the assertion valid for $\mathrm{e.dim}\,\mathbf{A} = n-1$. Consider the ring $\overline{\mathbf{A}} = \mathbf{A}/\langle t_1 \rangle$. Denote by $\bar{a}$ the class of a in $\overline{\mathbf{A}}$. The maximal ideal of $\overline{\mathbf{A}}$ is generated by $\bar{t}_2, \ldots, \bar{t}_n$ and the class of $\bar{t}_i$ in $\overline{\mathbf{A}}/\langle \bar{t}_2, \ldots, \bar{t}_{i-1} \rangle$ is non-zero-divisor for all $i = 2, \ldots, n$. By the inductive hypothesis, $\mathrm{K.dim}\,\overline{\mathbf{A}} = n-1$. As $\mathrm{ht}\,\mathfrak{p} = 1$ for every minimal prime ideal $\mathfrak{p}$ containing t_1 (cf. Krull Hauptidealsatz), $\mathrm{K.dim}\,\mathbf{A} \geq \mathrm{K.dim}\,\overline{\mathbf{A}} + 1 = n$. As always $\mathrm{K.dim}\,\mathbf{A} \leq \mathrm{e.dim}\,\mathbf{A}$, it proves that $\mathrm{K.dim}\,\mathbf{A} = n$. □

Corollary 4.2.7. *Any regular local ring is* reduced *(i.e., contains no zero divisors). Moreover, if $a \in \mathfrak{m}^k \setminus \mathfrak{m}^{k+1}$ and $b \in \mathfrak{m}^l \setminus \mathfrak{m}^{l+1}$, then $ab \in \mathfrak{m}^{k+l} \setminus \mathfrak{m}^{k+l+1}$.*
(Note that, by Corollary 4.2.3, such numbers k and l always exist for non-zero a and b.)

Proof. Let $a \equiv F$, $b \equiv G$ and $a \neq 0, b \neq 0$. As a Taylor series is unique and $a \in \mathfrak{m}^k \setminus \mathfrak{m}^{k+1}$, F contain terms of degree k and does not contain terms of smaller degrees. Correspondingly, G contains terms of degree l and does not contain terms of smaller degrees. Then $ab \equiv FG \pmod{\mathfrak{m}}^{k+l+1}$ and FG contains terms of degree $k+l$. The uniqueness of the Taylor series implies that $ab \notin \mathfrak{m}^{k+l}$. □

Corollary 4.2.8. *Let $\{t_1, t_2, \ldots, t_n\}$ be a minimal set of generators of the maximal ideal of a local ring $\mathbf{A}$. Then, for every $k =$*

$1, \dots, n$ *, the factor-ring* $\mathbf{A}/\langle t_1, t_2, \dots, t_k \rangle$ *is regular local ring of Krull dimension* $n-k$ *.*

If p is a point of an algebraic variety X, then $\mathcal{O}_{X,p}$ is reduced if and only if p only belongs to one component: otherwise, one can check two functions f_1 and f_2 such that $f_1|_Y \neq 0$, $f_1|_Z = 0$, $f_2|_Y = 0$, $f_2|_Z \neq 0$, where Y is one component, Z is the union of all other component containing p, whence $f_1 \neq 0$, $f_2 \neq 0$ in $\mathcal{O}_{X,p}$ but $f_1 f_2 = 0$.

COROLLARY 4.2.9. (1) *If a point* $p \in X$ *is regular, it only belongs to one component of* X *.*
(2) X_{reg} *is an open dense subset of* X *.*

PROOF. *1* is evident now. Let $X = \bigcup_i X_i$ be the irreducible decomposition, $Y = \bigcup_{i \neq j}(X_i \cap X_j)$, $U = X \setminus Y$. Then $X_{\mathrm{reg}} \subseteq U$ and U is open dense in X. Moreover, U is the disjoint union of its components $X_i \setminus Y$, so *2* follows from Corollary 4.1.8. □

EXERCISE 4.2.10 ("Non-ramified extensions"). Let $\mathbf{A}$ be a local noetherian ring with the maximal ideal $\mathfrak{m}$ and the residue field $\mathbf{K} = \mathbf{A}/\mathfrak{m}$, $f(x) \in \mathbf{A}[x]$ be a monic polynomial such that its image $\overline{f}(x)$ in $\mathbf{K}[x]$ is irreducible. Put $\mathbf{B} = \mathbf{A}[x]/\langle f(x) \rangle$, $\xi = x + \langle f(x) \rangle \in \mathbf{B}$. Prove that:

(1) Every element of $\mathbf{B}$ can be uniquely presented in the form $a_1\xi^{k-1} + a_2\xi^{k-2} + \dots + a_k$, where $k = \deg f$, $a_i \in \mathbf{A}$, and this element is invertible in $\mathbf{B}$ if and only if $a_i \notin \mathfrak{m}$ for some i.
(2) $\mathbf{B}$ is a local ring with the maximal ideal $\mathfrak{m}\mathbf{B}$ and the residue field $\mathbf{K}' \simeq \mathbf{K}[x]/\langle \overline{f}(x) \rangle$.
(3) If $\mathbf{A}$ is regular, so is $\mathbf{B}$. (Note that $\mathbf{B}$ is a finite extension of $\mathbf{A}$.)

4.3. Tangent space

In this section $\mathbf{A}$ denotes a local noetherian ring with the maximal ideal $\mathfrak{m}$ and the residue field $\mathbf{K} = \mathbf{A}/\mathfrak{m}$.

DEFINITIONS 4.3.1. (1) The $\mathbf{K}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is called the *cotangent space* of $\mathbf{A}$ and denoted by $\Theta^*_{\mathbf{A}}$. Its dual $\Theta = \mathrm{Hom}_{\mathbf{K}}(\Theta^*_{\mathbf{A}}, \mathbf{K})$ is called the *tangent space* to $\mathbf{A}$.
(2) If $\mathbf{A} = \mathcal{O}_{X,p}$, where p is a point of an algebraic variety X, the spaces $\Theta_{\mathbf{A}}$ and $\Theta^*_{\mathbf{A}}$ are called, respectively, the *tangent* and the *cotangent space* to the variety X at the point p and denoted, respectively, by $\Theta_{X,p}$ and $\Theta^*_{X,p}$.

Let $\mathbf{B}$ be another local noetherian ring with the maximal ideal $\mathfrak{n}$. A (ring) homomorphism $\varphi : \mathbf{A} \to \mathbf{B}$ is said to be *local* if $\varphi(\mathfrak{m}) \subset \mathfrak{n}$. In this case φ induces a homomorphism of fields $\overline{\varphi} : \mathbf{K} \to \mathbf{L} = \mathbf{B}\mathfrak{n}$ and a homomorphism $d^*\varphi : \Theta^*_{\mathbf{A}} \to \Theta^*_{\mathbf{B}}$. If, moreover, $\overline{\varphi}$ is an isomorphism, it also induces a homomorphism of dual spaces $d\varphi : \Theta_{\mathbf{A}} \to \Theta_{\mathbf{B}}$. The latter is always the case, when $\mathbf{A} = \mathcal{O}_{X,p}$, $\mathbf{B} = \mathcal{O}_{Y,q}$ and $\varphi = f_q^*$ is induced by a morphism $f : Y \to X$ mapping q to p. In this situation $d^*\varphi$ and d^φ are denoted, respectively, by $d_q^* f$ and $d_q f$ and are called, respectively, the *cotangent* and the *tangent mappings* of the morphism f at the point q.

EXAMPLES 4.3.2. (1) Let $\mathfrak{p} \neq \mathfrak{m}$ be a prime ideal of $\mathbf{A}$, $\mathbf{B} = \mathbf{A}_{\mathfrak{p}}$ and $\varphi : \mathbf{A} \to \mathbf{B}$ be the natural homomorphism, mapping a to $a/1$. It is *not local*: if $a \in \mathfrak{m}\mathfrak{p}$, then $\varphi(a) = a/1 \notin \mathfrak{p}\mathbf{B}$ (which is the maximal ideal of $\mathbf{B}$).

(2) On the other hand, if $\varphi : \mathbf{A} \to \mathbf{B}$ is surjective, then $\mathbf{B} \simeq \mathbf{A}/I$ for $I = \operatorname{Ker}\varphi$ and $\mathfrak{n} \simeq \mathfrak{m}/I = \varphi(\mathfrak{m})$. Hence, φ is always local and $\Theta_{\mathbf{B}}^* = \mathfrak{n}/\mathfrak{n}^2 \simeq \mathfrak{m}/(I + \mathfrak{m}^2) \simeq \Theta_{\mathbf{A}}^*/\mathfrak{I}$, where $\mathfrak{I} = (I + \mathfrak{m}^2)/\mathfrak{m}^2 \subseteq \Theta_{\mathbf{A}}^*$. Thus, $d\varphi^*$ is a surjection, so its dual $d\varphi : \Theta_{\mathbf{B}} \to \Theta_{\mathbf{A}}$ is an embedding. (Note that in this situation always $\mathbf{B}/\mathfrak{n} \simeq \mathbf{A}/\mathfrak{m}$.) More precisely, $d\varphi$ induces an isomorphism of $\Theta_{\mathbf{B}}$ onto the subspace $\{\, v \mid \omega(v) = 0 \text{ for all } \omega \in \mathfrak{I} \,\}$ of $\Theta_{\mathbf{A}}$.

We give other interpretations of the tangent space in the case, when $\mathbf{A}$ contains a *subfield of representatives* of $\mathbf{K}$, i.e., a subfield $\mathbf{K}'$ such that $\{\, \lambda + \mathfrak{m} \,\}$ exhaust all residue classes from $\mathbf{K}$. We identify $\mathbf{K}'$ with $\mathbf{K}$ identifying $\lambda + \mathfrak{m}$ with λ. Then $\mathbf{A} = \mathbf{K} \oplus \mathfrak{m}$, so every element $a \in \mathbf{A}$ can be uniquely written in the form $a = a(0) + a'$ with $a(0) \in \mathbf{K}$ and $a' \in \mathfrak{m}$. Denote by da the class of $a' = a - a(0)$ in $\Theta_{\mathbf{A}}^*$. One can easily check the following properties of the mapping $d : \mathbf{A} \to \Theta_{\mathbf{A}}^*$.

PROPOSITION 4.3.3. (1) *$d(a + b) = da + db$;*

(2) *$d(\lambda a) = \lambda da$ for every $\lambda \in \mathbf{K}$;*

(3) *$d(ab) = adb + bda$.*

One calls such a mapping a *derivation* of the ring $\mathbf{A}$ to the $\mathbf{A}$-module $\Theta_{\mathbf{A}}^*$. Note that $a\omega = a(0)\omega$ for all $v \in \Theta_{\mathbf{A}}^*$.

COROLLARY 4.3.4. *In the situation above, there is one-to-one correspondence between $\Theta_{\mathbf{A}}$ and the vector space of all derivations* $\operatorname{Der}(\mathbf{A}, \mathbf{K})$, *which maps $v \in \Theta_{\mathbf{A}}$ to the derivation $D_v : a \mapsto v(da)$.*

PROOF. As $d : \mathbf{A} \to \Theta_{\mathbf{A}}^*$ is a derivation and $v : \Theta_{\mathbf{A}}^* \to \mathbf{K}$ is a linear mapping, D_v is a derivation. On the contrary, let $D : \mathbf{A} \to \mathbf{K}$ be a derivation. Then $D1 = d(1 \cdot 1) = D1 + D1$, whence $D1 = 0$ and $D\lambda = \lambda D1 = 0$ for all $\lambda \in \mathbf{K}$. Hence, D is completely defined by its values on $\mathfrak{m}$. On the other hand, if $a, b \in \mathfrak{m}$, then $D(ab) = aDb + bDa = 0$ as both a and b annihilate $\mathbf{K} = \mathbf{A}/\mathfrak{m}$. So, indeed, $v = D|_{\mathfrak{m}}$ is a mapping $\mathfrak{m}/\mathfrak{m}^2 \to \mathbf{K}$, i.e., an element of $\Theta_{\mathbf{A}}$. Clearly, $D = D_v$. $\square$

In what follows, we identify the elements of $\Theta_{\mathbf{A}}$ with the corresponding derivations $\mathbf{A} \to \mathbf{K}$; in particular, we write $v(a)$ instead of $D_v a$, etc.

If $\mathbf{A} = \mathcal{O}_{X,p}$ for a point p of a variety X, we usually write $d_p a$ or even $d_{X,p} a$ for da, where $a \in \mathbf{A}$, because we often have to consider p as a point of some subvarieties of X or a as an element of another local ring $\mathcal{O}_{X,q}$ too.

One can use Example 4.3.2(2) to describe the tangent (and cotangent) spaces to an algebraic variety X. Certainly, as we are only interested in a neighbourhood of a point p, one may suppose X affine: $X = V(F_1, F_2, \dots, F_r) \subseteq \mathbb{A}^n$. We always suppose that $I(X) = \langle F_1, F_2, \dots, F_r \rangle$. First precise the case of the affine space itself.

Proposition 4.3.5. *For any point* $p = (\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{A}^n$, $\{ d_p x_1, d_p x_2, \dots, d_p x_n \}$ *is a basis of* $\Theta^*_{\mathbb{A}^n,p}$. *If* $\{ D_1, D_2, \dots, D_n \}$ *is the dual basis of* $\Theta_{\mathbb{A},p}$, *then* $D_i F = \partial F/\partial x_i(p)$ *for every* $F \in \mathcal{O}_{\mathbb{A}^n,p}$. (Note that elements from $\mathcal{O}_{\mathbb{A}^n,}$ can be identified with the rational functions $F \in \mathbf{K}(x_1, \dots, x_n)$, which are defined at p, i.e., such that the denominator of F is non-zero at the point p.)

Proof. The ideal $\mathfrak{m}_p \in \mathbf{K}[\mathbf{x}]$ is generated by $x_1 - \lambda_1, \dots, x_n - \lambda_n$. Hence the maximal ideal $\mathfrak{m} \subset \mathcal{O}_{\mathbb{A}^n,p}$ is generated by the same elements. Moreover, it is a *minimal* system of generators, as $\mathrm{e.dim}_p \mathbb{A}^n = \dim \mathbb{A}^n = n$. Hence, there classes in $\Theta^*_{\mathbb{A}^n,p}$, which coincide with $d_p x_i$, form a basis of the cotangent space. Let $\{ D_1, D_2, \dots, D_n \}$ be the dual basis of the tangent space. It means that $D_i(d_p x_j) = \delta_{ij}$ for all i, j. Any rational function F, which is defined at p, can be written as $F(0) + \sum_j \xi_j (x_j - \lambda_i) + F'$, where $F' \in \mathfrak{m}^2$. Moreover, $\xi_j = \partial F/\partial x_j(p)$. Then $D_i F = D_i(\sum_j \xi_j d_p x_j) = \xi_i = \partial F/\partial x_i(p)$. □

In what follows, we often denote the derivation D_i by $\partial/\partial x_i$ or by $\partial/\partial x_i(p)$ if p should be precised.

Let now $X \subseteq \mathbb{A}^n$ be an affine variety, $I(X) = \langle F_1, F_2, \dots, F_r \rangle \in \mathbf{K}[\mathbf{x}]$. Then $\mathcal{O}_{X,p} = \mathcal{O}_{\mathbb{A}_n,p} / \langle F_1, F_2, \dots, F_n \rangle$ (here it means the generators of an $\mathcal{O}_{X,p}$-ideal) and $\Theta^*_{X,p} = \Theta^*_{\mathbb{A}^n,p} / \langle d_p F_1, d_p F_2, \dots, d_p F_r \rangle$. Hence, $\Theta_{X,p}$ coincides with the subspace $\{ D \mid D F_i = 0,\ i = 1, \dots \}$ of $\Theta_{\mathbb{A}^n,p}$. In other words, $D = \sum_j \xi_j \partial/\partial x_j$ belongs to $\Theta_{X,p}$ if and only if $\sum_j \xi_j \partial F_i/\partial x_j(p) = 0$ for all $i = 1, \dots, r$.

Consider now a morphism $G : \mathbb{A}^n \to \mathbb{A}^m$ given by the rule $p \mapsto (G_1(p), \dots, G_m(p))$, where G_i are some polynomials. Let $p \in \mathbb{A}^n$ and $q = G(p) \in \mathbb{A}^m$. Then, for any function $F \in \mathcal{O}_{\mathbb{A}^m,q}$, $G^*(F) = F(G_1, G_2, \dots, G_m)$. Therefore,

$$d_p G(\partial/\partial x_j)(F) = \partial(G^*(F))/\partial x_j(p) = \sum_{i=1}^{m} \partial G_i/\partial x_j(p) \cdot \partial F/\partial y_i(q),$$

so, the linear mapping d_p, with respect to "standard" bases of $\Theta_{\mathbb{A}^n.p}$ and $\Theta_{\mathbb{A}^m,q}$, is given by the value of the Jacoby matrix $\partial G/\partial x(p) = (\partial G_i/\partial x_j(p))$.

If $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ are affine varieties and g is a morphism of X to Y, it is indeed a restriction onto X of some morphism $G : \mathbb{A}^n \to \mathbb{A}^m$. Certainly, the mapping $d_p g$ is also the restriction onto $\Theta_{X,p}$ of the tangent mapping $d_p G$, i.e., it is given by the same Jacoby matrix. One only has to remember that $\Theta_{X,p}$ only consists of *some* linear combinations $\sum_j \xi_j \partial/\partial x_j$ (cf. above). The condition $G(X) \subseteq Y$ guarantees that if such a linear combination belongs to $\Theta_{X,p}$, its image under $d_p G$ belongs to $\Theta_{Y,q}$.

EXERCISE 4.3.6. Let X be an algebraic variety, $p \in X$, $\mathfrak{m} = \mathfrak{m}_{X,p}$ (the maximal ideal of the local ring $\mathcal{O}_{X,p}$) and $\langle a_1, a_2, \dots, a_n \rangle$ be a generating set for $\mathfrak{m}$. Denote by S_d the set of all homogeneous polynomials F of degree d from $\mathbf{K}[x_1, \dots, x_n]$ such that $F(a_1, a_2, \dots, a_n) \in \mathfrak{m}^{d+1}$, and $S = \bigcup_{d=1}^{\infty} S_d$. The affine variety $T_{X,p} = V(S) \subseteq \mathbb{A}^n$ is called the *tangent cone* of X at the point p. (As all polynomials from S are homogeneous, it is a cone indeed.) Prove that:

(1) Another choice of the generating set of $\mathfrak{m}$ gives rise to the isomorphic variety $T_{X,p}$.
(2) If $X \subset \mathbb{A}^n$ is an affine variety, $I = I(X)$, $p = (0, \dots, 0)$, then $T_{X,p} = V(\, F^{(0)} \mid F \in I\,)$, where $F^{(0)}$ denotes the "lowest form" of a polynomial F, i.e., if $F = \sum_{\mathbf{k}} \lambda_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}$ and $d = \min\{\, |\mathbf{k}| \mid \lambda_{\mathbf{k}} \neq 0 \,\}$, then $F^{(0)} = \sum_{|\mathbf{k}|=d} \lambda_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}$. In particular, if X is a hypersurface, i.e., $I(X) = \langle F \rangle$, then $T_{X,p} = V(F^{(0)})$.
(3) A morphism $f : X \to Y$ induces a morphism $T_f : T_{X,p} \to T_{Y,f(p)}$ and if f is an isomorphism, so is T_f.

How does $T_{X,p}$ look like if p is a regular point?

EXERCISES 4.3.7. (1) Let X be one of the following plane curves:
 (a) $y^2 = x^3 + x^2$;
 (b) $y^2 = x^3 + y^3$;
 (c) $x^2 y + x y^2 = x^4$.
 Check that all their points, except of 0, are regular. Find the tangent cones to these curves at 0. Outline the corresponding curves (more precisely, their sets of real points) together with their tangent cones in a neighbourhood of 0.
(2) Let X be the space surface: $y^2 = x^2 z$.
 (a) Find the set X_{sing}.
 (b) For every $p \in X_{\mathrm{sing}}$, find the tangent cone $T_{X,p}$.
 (c) Outline X in a neighbourhood of 0.

4.4. Blowing-up

We are going to consider a procedure, often allowing to "improve" the singularities of an algebraic variety. In what follows, let p be a point of an algebraic variety X, $\mathfrak{m} = \mathfrak{m}_{X,p}$, the maximal ideal of the local ring $\mathcal{O}_{X,p}$, and $\{ t_1, t_2, \dots, t_n \}$ a set of generators of $\mathfrak{m}$. The elements $t_1, t_2, \dots, t_n$ are indeed regular functions on a neighborhood U of p. Moreover, diminishing U, one can suppose that U is affine and the maximal ideal $\{ f \in \mathcal{O}_X(U) \mid f(p) = 0 \}$ is generated by the elements $t_1, t_2, \dots, t_n$, i.e., if $p' \in U$, $p' \neq p$, at least one of the values $t_i(p')$ is non-zero.

Put $U' = U \setminus \{ p \}$ and consider the following subset $\tilde{U}' \subseteq U \times \mathbb{P}^{n-1}$:

$$\tilde{U}' = \{ p' \times (y_1 : \dots : y_n) \mid p' \neq p, \text{ and } t_i(p')y_j = t_j(p')y_i \\ \text{for all } i, j = 1, \dots, n \}$$

(here and later on $y_1, y_2, \dots, y_n$ denotes the homogeneous coordinates on $\mathbb{P}^{n-1}$). Obviously, $\tilde{U}'$ is closed in $U' \times \mathbb{P}^{n-1}$ and the projection pr_U induces an isomorphism $\tilde{U}' \xrightarrow{\sim} U'$, the inverse mapping being $p' \mapsto p' \times (t_1(p') : \dots : t_n(p'))$. Put $\tilde{U} = \overline{\tilde{U}'}$, the closure of $\tilde{U}'$ in $U \times \mathbb{P}^{n-1}$. Then $\tilde{U}'$ is open and dense in $\tilde{U}$. The projection pr_U defines a surjective morphism $\sigma : \tilde{U} \to U$. Put $E = \sigma^{-1}(p)$. It is a closed subvariety in the projective space $\mathbb{P}^{n-1} \simeq p \times \mathbb{P}^{n-1}$.

As $\tilde{U}' \simeq U'$, we can glue $X \setminus \{ p \}$ with $\tilde{U}$ using this isomorphism and Proposition 3.7.4. The surjection σ can also be prolonged onto $\tilde{X}$ and its restriction onto $\tilde{X} \setminus E$ is an isomorphism $\tilde{X} \setminus E \xrightarrow{\sim} X \setminus \{ p \}$. One calls $\sigma : \tilde{X} \to X$ the *blowing-up* of the variety X at the point p. Sometimes the variety $\tilde{X}$ itself is called the blowing-up of X at p. As $\tilde{X} \setminus E$ is open and dense in $\tilde{X}$, σ is a birational mapping with $\mathrm{Dom}(\sigma^{-1}) \supseteq X \setminus \{ p \}$. Moreover, σ is a *closed* mapping: it is so on $\tilde{U}$ as $\mathbb{P}^{n-1}$ is complete and on $\tilde{X} \setminus E$ as it is an isomorphism there. Certainly, neither $\tilde{X}$ nor σ depend on the choice of the neighbourhood U as above. In particular, one can always diminish U (it is often useful and we will profit from this remark).

The subvariety $E \subset \tilde{X}$ is called the *exceptional subvariety* or the *exceptional fibre* of the blowing-up. Sometimes it is useful to note that it can be given locally by one equation. Indeed, consider the intersection $\tilde{U}_i = \tilde{U} \cap U \times \mathbb{A}_i^{n-1}$, where, as usually, $\mathbb{A}_i^{n-1}\mathbb{P}^{n-1}$ is given by the condition $y_i \neq 0$. The affine coordinates on $\mathbb{A}_i^{n-1}$ are $z_j = y_j / y_i$ ($j = 1, \dots, n$, $j \neq i$). The equations for $\tilde{U}'$ in these coordinates are $t_j = z_j t_i$, hence, $E \cap \tilde{U}_i$ is defined (inside $\tilde{U}_i$) by the unique equation $t_i = 0$.

Exercises 4.4.1. Let $\sigma : \tilde{X} \to X$ be a blowing-up at a point p. Prove that:

(1) If X is complete, $\tilde{X}$ is also complete.
(2) If X is projective, $\tilde{X}$ is also projective.
(3) If the point p is singular, $E \neq \mathbb{P}^{n-1}$.

Hint: Take a homogeneous polynomial F of degree k such that $F(t_1, t_2, \dots, t_n) \in \mathfrak{m}^{k+1}$. Suppose that $F = t_1^k + \sum_{i=2}^{k} t_i F_i$ and get a non-trivial equation for $E \cap \mathbb{A}_1^{n-1}$.

Though the blowing-up has been defined using a fixed set of generators of $\mathfrak{m}$, it does not depend on this special set.

PROPOSITION 4.4.2. *The blowing-up does not depend on the choice of generators of* $\mathfrak{m}$. *More precisely, if* $\{ y_1, y_2, \dots, y_m \}$ *is another set of generators of* $\mathfrak{m}$ *and* $\tau : Y \to X$ *is the blowing-up constructed via this choice of generators, there is a unique isomorphism* $\varphi : \tilde{X} \to Y$ *such that* $\sigma = \tau \circ \varphi$.

PROOF. The uniqueness of φ follows from the fact that both σ and τ are birational, i.e., having inverse on an open dense subset of X.

First suppose that both $\{ t_1, t_2, \dots, t_n \}$ and $\{ t'_1, t'_2, \dots, t'_m \}$ are *minimal* sets of generators. Then $m = n$ and $t'_i = \sum_{j=1}^{n} a_{ij} t_i$ for some elements $a_{ij} \in \mathcal{O}_{X,p}$ such that $\det(a_{ij}) \notin \mathfrak{m}$. One may suppose that $a_{ij} \in \mathcal{O}_X(U)$ and $\det(a_{ij})$ is nowhere zero on U, hence, invertible in $\mathcal{O}_X(U)$. Define the automorphism ψ of $U \times \mathbb{P}^{n-1}$ mapping $p' \times (\xi_1 : \dots : \xi_n)$ of $p' \times (\xi'_1 : \dots : \xi'_n)$, where $\xi' = \sum_{j=1}^{n} a_{ij}(p')\xi_i$. One easily checks that its restriction onto $U' \times \mathbb{P}^{n-1}$ maps $\tilde{U}'$ onto $W \subseteq U' \times \mathbb{P}^{n-1}$, where

$$W = \left\{ p' \times (y_1 : \dots : y_n) \,|\, p' \neq p \text{ and } t'_i(p')y_j = t'_j(p')y_i \right. \\ \left. \text{for all } i, j = 1, \dots, n \right\}.$$

As $\tau^{-1}(U)$ is the *closure* of W in $U' \times \mathbb{P}^{n-1}$, ψ induces an isomorphism of $\tilde{U}$ onto $\tau^{-1}(U)$. This isomorphism can obviously be prolonged up to an isomorphism $\varphi : \tilde{X} \to Y$. Its definition guarantees that $\sigma = \tau \circ \varphi$.

Now suppose that the system of generators $\{ t_1, t_2, \dots, t_n \}$ is *not minimal*. Then, up to permutation of indices, $t_n = \sum_{i=1}^{n-1} a_i t_i$ for some $a_i \in \mathcal{O}_{X,p}$. One may again suppose that $a_i \in \mathcal{O}_X(U)$. Then, for every point $p' \times (\xi_1 : \dots : \xi_n) \in \tilde{U}'$, the equality $\xi_n = \sum_{i=1}^{n-1} a_i(p')\xi_i$ holds. Therefore, it holds also for every point $p \times (\xi_1 : \dots : \xi_n)$ from E. Identify $\mathbb{P}^{n-2}$ with the hyperplane of $\mathbb{P}^{n-1}$ given by the equation $y_n = \sum_{i=1}^{n-1} \alpha_i y_i$, where $\alpha_i = a_i(p)$, and consider $y_1, \dots, y_{n-1}$ as homogeneous coordinates on this hyperplane. Then one easily sees that the blowing-up defined via the generators $t_1, t_2, \dots, t_{n-1}$ coincide, under this identification, with $\tilde{X}$. It accomplishes the proof. $\square$

Let Y be a subvariety of X containing p. Then the same elements $t_1, t_2, \dots, t_n$ generate the maximal ideal of $\mathcal{O}_{Y,p}$, so we can use them to construct the blowing-up $\tilde{Y}$ of Y at the point p. Then the construction above immediately implies that $\tilde{Y}$ is indeed a subvariety of $\tilde{X}$ such that $\sigma^{-1}(Y) = \tilde{Y} \cup E$.

In what follows, we suppose that $\{ t_1, t_2, \dots, t_n \}$ is a *minimal* set of generators of $\mathfrak{m}$. Consider some examples. Start with the simplest case.

PROPOSITION 4.4.3. *If p is a regular point of X, then $E = \mathbb{P}^{n-1}$ and every point of E is regular on $\tilde{X}$. In particular, if X is smooth, so is $\tilde{X}$.*

PROOF. As p only belongs to one component of X (cf. Corollaryopenreg), we may suppose X irreducible and $n = \dim X$. Let $q \in \mathbb{P}^{n-1}$. Changing coordinates (which corresponds to the change of generators of $\mathfrak{m}$), one may suppose that $q = (1 : 0 : \cdots : 0)$. Consider the subvariety $Y \subseteq X$ given by the equations $t_i = 0$ ($i = 2, \dots, n$). By Corollary 4.2.8, p is a regular point of Y and $\dim_p Y = 1$. If $p' \times (\xi_1 : \cdots : \xi_n) \in \tilde{Y} \setminus E$, then $t_i(p') = 0$ and $t_1(p') \neq 0$ implies that $\xi_i = 0$ for $i = 2, \dots, n$. Hence, the same is valid for any point of $\tilde{Y} \cap E$, i.e., there is only one point in this intersection, namely, q. Thus $E = \mathbb{P}^{n-1}$.

Put $\tilde{U}_i = \tilde{U} \cap \mathbb{A}^{n-1}_i$, and $\tilde{U}'_i = \tilde{U}_i \setminus E$ where, as usually, $\mathbb{A}^{n-1}_i$ denotes the subset of $\mathbb{P}^{n-1}$ given by the inequality $y_i \neq 0$. The affine coordinates on $\mathbb{A}^{n-1}_i$ are $z_j = y_j / y_i$ ($j = 1, \dots, n,\ j \neq i$). On $\tilde{U}'_i$ $t_i = t_1 z_i$, hence, it is also valid on $\tilde{U}_i$. The point $p \times q$ (as above) belongs to $\tilde{U}_1$ and $z_j(q) = 0$. Any rational function f on $\tilde{U}_1$ can be considered as a rational fraction from $\mathbf{K}(U)(z_2, \dots, z_n)$. In particular, if $f \in \mathcal{O}_{\tilde{U}, p \times q}$, its denominator is non-zero at this point. Such a function can always be written as $f = a + \sum_{j=2}^n z_j f_j$, where $a \in \mathbf{K}(U)$. If $f(p \times q) = 0$, then $a(p) = 0$, whence $a = \sum_{i=1}^n b_i t_i = t_1(b_1 + \sum i = 2^n b_i z_i$. Therefore, $f \in \langle t_1, z_2, \dots, z_n \rangle$, so $\mathfrak{m}_{\tilde{X}, p \times q} = \langle t_1, z_2, \dots, z_n \rangle$. As $n = \dim \tilde{X}$, this point is regular on $\tilde{X}$. $\square$

Suppose now that $X \subset \mathbb{A}^2$ is an affine curve, $I(X) = \langle F \rangle$ and $p = (0, 0)$. Then $\mathfrak{m} = \langle x, y \rangle$ (further, they are the *restrictions* of x and y onto X). Let $F = F_m + F_{m+1} + O(m+2)$, where F_k denotes a form of degree k and $O(m+2)$ stands for a polynomial having no terms of degrees less than $m+2$. (One calls m the *multiplicity* of the point p.) Decompose F_m into a product of linear forms: $F_m = \prod_{i=1}^m (\beta_i x - \alpha_i y)$ for some $\alpha_i, \beta_i \in \mathbf{K}$. We call the points $(\alpha_i : \beta_i)$ of $\mathbb{P}^1$ the *roots* of F_m. They are indeed those points from $\mathbb{P}^1$, for which $F_m(\alpha_i, \beta_i) = 0$. Consider again $\tilde{X}_i = \tilde{X} \cap (X \times \mathbb{A}^1_i)$ ($i = 1, 2$). The coordinate on $\mathbb{A}^1_1$ is $z = y_2 / y_1$ and, for points from $\tilde{X}_1$, $y = tx$. So, the equations of $\tilde{U}_1'$ are:

$$y = zx\,,$$
$$x^m F_m(1,z) + x^{m+1} F_{m+1}(1,z) + x^{m+2} G(x,z)$$

for some polynomial G. As $x \neq 0$ on $\tilde{U}'$, the second equation can be rewritten as

$$\tilde{F}(x,z) = F_m(1,z) + xF_{m+1}(1,z) + x^2 G(x,z) = 0\,. \tag{4.4.1}$$

Hence, (4.4.1) is just the equation of $\tilde{X}_1$ with respect to the coordinates x, z. In particular, $\tilde{X}_1$ is again an affine curve. The intersection $\tilde{X}_1 \cap E$ is given by the equation $x = 0$, whence $F_m(1,z) = 0$. Moreover, given a point $q = (0,\eta)$ from E,

$$\partial\tilde{F}/\partial x(q) = F_{m+1}(1,\eta)\,;$$
$$\partial\tilde{F}/\partial z(q) = \partial F/\partial y(1,\eta)\,.$$

Therefore, this point is regular if and only if either $\partial F/\partial y(1,\eta) \neq 0$ or $F_{m+1}(1, eta) \neq 0$. The former equation just means that η is am ordinary root of $F_m(1,z)$, or, the same, $(1:\eta)$ is an ordinary root of $F_m(x,y)$. Certainly, the same is valid for $\tilde{X}_2$ as well, which gives us the following result.

PROPOSITION 4.4.4. *In the above notations, the points of E are just $p \times (\alpha_i : \beta_i)$ ($i = 1, \dots, m$). Such a point is regular on $\tilde{X}$ if and only if either $(\alpha_i : \beta_i)$ is an ordinary root of F_m or $F_{m+1}(\alpha_i, \beta_i) \neq 0$.*

The point $p = (0.0)$ is called an *ordinary m-tuple point* if F_m has no multiple roots, i.e., all points $(\alpha_i : \beta_i)$ are pairwise different.

COROLLARY 4.4.5. *If p is an ordinary m-tuple point of the curve X, then the exceptional fibre E consists of m different regular points.*

One can note that the equation (4.4.1) is "better" than that of the curve X. Indeed, if $F_m \neq y^m$, the new equation contains z in a smaller degree than m. Hence, the multiplicity of the new points are smaller than m. If $F_m = y^m$, $\tilde{F}$ contains x in a smaller degree than F .his observation implies the following corollary.

COROLLARY 4.4.6. *Let X be a plane curve. There is a sequence of blowing-ups:*

$$X = X_0 \xleftarrow{\sigma_1} X_1 \xleftarrow{\sigma_2} X_2 \dots \xleftarrow{\sigma_k} X_k$$

such that X_k is a smooth curve. Moreover, one can choose for σ_i an arbitrary blowing-up at a singular point of X_{i-1}.

EXAMPLE 4.4.7. One says that a plane curve $X \subset \mathbb{A}^2$ has a *singularity if type* A_n at the origin if $I(X) = \langle F \rangle$, where, under a certain choice of coordinates, $F = y^2 + x^{n+1} + O(n+2)$ ($n > 0$; if $n = 1$ it is just an ordinary double point, or *node*). In this case E consists of a unique point and its equation in the neighbourhood of this point is $z^2 + x^{n-1} + O(n)$. In other words, this new point is a singularity of type A_{n-2} (if $n \le 2$, this point is regular).

EXERCISE 4.4.8. (1) Suppose that $X \subset \mathbb{A}^n$ is a hypersurface, $I(X) = \langle F \rangle$ with $F = F_m + F_{m+1} + O(m+2)$, where F_m and F_{m+1} are homogeneous polynomials of degrees, respectively, m and $m+1$. Prove that $E = PV(F_m)$ and a point $\xi = (\xi_1 : \dots : \xi_n) \in E$ is regular on $\tilde{X}$ if and only if either $\partial F_m/\partial x_i(\xi_1, \dots \xi_n) \neq 0$ for some i or $F_{m+1}(\xi_1, \dots, \xi_n) \neq 0$.

(2) Let $X \subset \mathbb{A}^2$ be an affine curve, $I(X) = \langle F \rangle$. The point p is called a *singularity of type* D_n ($n > 3$) if, under a proper choice of coordinates in $\mathbb{A}^2$, $F = xy^2 - x^{n-1} + O(n)$. Show that in this case $\tilde{X}$ is smooth if $n \le 5$ and has a unique singular point, which is a singularity of type A_{n-5}, if $n > 5$.

(3) Let $X = V(xy^2 - z^2) \subset \mathbb{A}^3$. Show that $\tilde{X}$ contains an affine open subset isomorphic to X (under this isomorphism the point $p \in X$ corresponds to some point of E).

(4) Let $X \subseteq \mathbb{A}^n$ be a *cone*, i.e., $I = I(X)$ be a homogeneous ideal. Prove that $E = PV(I)$ and a point $\xi \in E$ is regular on $\tilde{X}$ if and only if it is regular on E.

(5) Denote by S_d the set of all homogeneous polynomials F of degree d from $\mathbf{K}[x_1, \dots, x_n]$ such that $F(t_1, t_2, \dots, t_n) \in \mathfrak{m}^{d+1}$ and $S = \bigcup_{d=1}^{\infty} S_d$ (cf. Exercise 4.3.6). Prove that $E \simeq PV(S) \subset \mathbb{P}^{n-1}$ (i.e., E is the "projectivization" of the tangent cone to X at p).

4.5. Complete local rings

Every local noetherian ring $\mathbf{A}$ with the maximal ideal $\mathfrak{m}$ can be considered as a *topological ring* with respect to the so called $\mathfrak{m}$-*adic topology.* The base of open sets in this topology is formed by the cosets $a + \mathfrak{m}^k$ ($a \in \mathbf{A}, k \in \mathbb{N}$). One can easily check that they satisfy the properties of a base of topology. Moreover, Artin–Rees Theorem guarantees that this topology is *Hausdorff*: if $a \neq b$, there is k such that $a - b \notin \mathfrak{m}^k$, hence, $(a+\mathfrak{m}^k) \cap (b+\mathfrak{m}^k) = \emptyset$. One can even consider $\mathbf{A}$ as a *metric space.* Namely, put $o(a) = \sup\{\, k \mid a \in \mathfrak{m}^k \,\} \in \mathbb{N} \cup \{\infty\}$ (certainly, $o(a) = \infty$ means that $a = 0$) and define the distance between a and b as $d(a, b) = 2^{-o(a)}$ (putting $2^\infty = 0$). One checks easily that it is indeed a distance generating the above defined topology. This metric is indeed an *ultrametric*, which means, by definition, that $d(a, c) \le \min\{\, d(a, b), d(b, c) \,\}$. In particular, a series $\sum_{k=0}^{\infty} a_k$ with $a_k \in \mathbf{A}$ is a Cauchy series if and only if $o(a_k) \to \infty$ when $k \to \infty$.

Usually, so defined metric space is not complete. For instance, if $\mathbf{A} = \mathcal{O}_{\mathbb{A}^1,0}$, any series $\sum_{k=0}^{\infty} \lambda_k x^k$ (x being the coordinate on $\mathbb{A}^1$) is a Cauchy series, but it converges in $\mathbf{A}$ if and only if the sequence of the coefficients λ_k is *periodic* (as the limit should be a rational function in x). One can check that it is always the case if $\mathbf{A} = \mathcal{O}_{X,p}$ for a point p of an algebraic variety X of positive dimension.

It is often useful to consider the *completion* of the ring $\mathbf{A}$ in $\mathfrak{m}$-adic topology. One can give a pure algebraic description of it using the notion of *inverse limit*. Indeed, consider the factor-rings $\mathbf{A}_k = \mathbf{A}/\mathfrak{m}^k$ and natural surjections $\pi_k : \mathbf{A}_k \to \mathbf{A}_{k-1}$. The *inverse limit* $\hat{\mathbf{A}} = \varprojlim_k \mathbf{A}_k$ is, by definition, the set of all sequences $(a_1, a_2, \dots, a_n, \dots)$, where $a_k \in \mathbf{A}_k$ and $\pi_k(a_k) = a_{k-1}$, with the addition and multiplication defined coordinate-wise. Certainly, any element $a \in \mathbf{A}$ defines such a sequence if we put $a_k = a + \mathfrak{m}^k$. So we get a homomorphism $\mathbf{A} \to \hat{\mathbf{A}}$, which is indeed an embedding (by Artin–Rees Theorem). The ring $\hat{\mathbf{A}}$ is again local: its unique maximal ideal $\hat{\mathfrak{m}}$ consists of all sequences (a_k) with $a_1 \neq 0$ (then $a_k \not\equiv 0 \pmod{\mathfrak{m}}$ for all k, i.e., all a_k are invertible). Moreover, $\hat{\mathfrak{m}}^k$ consists of all sequences with $a_k = 0$, hence, $\hat{\mathfrak{m}}^k \cap \mathbf{A} = \mathfrak{m}^k$, i.e., the $\mathfrak{m}$-adic topology coincides with the restriction on $\mathbf{A}$ of the $\hat{\mathfrak{m}}$-adic one. A sequence $a^{(l)} = (a_k^{(n)})$ of elements of $\hat{\mathbf{A}}$ is a Cauchy sequence if and only if the coordinate $a_k^{(l)}$ stabilizes for every k, i.e., there is a number l_0 such that $a_k^{(l)} = a_k^{(l_0)}$ for all $l > l_0$. Then the element a whose coordinates are these “limit” values, is, obviously, the limit of $a^{(l)}$. Therefore, $\hat{\mathbf{A}}$ is complete. One can see that $\mathbf{A}$ is dense in $\hat{\mathbf{A}}$, so $\hat{\mathbf{A}}$ is the completion of $\mathbf{A}$. Usually, we prefer this description of the $\mathfrak{m}$-adic completion, as it is much easier to deal with. Note that this definition n implies immediately that $\mathbf{A}/\mathfrak{m}^k \simeq \hat{\mathbf{A}}/\hat{\mathfrak{m}}^k$ for all k.

In the case, when $\mathbf{A} = \mathcal{O}_{X,p}$, one denotes the completion $\hat{\mathbf{A}}$ by $\hat{\mathcal{O}}_{X,p}$.

Examples 4.5.1. (1) If $\mathbf{A} = \mathcal{O}_{X,p}$, where p is a regular point, $\mathfrak{m} = \langle t_1, t_2, \dots, t_n \rangle$, where $n = \dim_p X$, the completion $\hat{\mathbf{A}}$ can be identified with the algebra of *formal power series* $\mathbf{K}[[x_1, \dots, x_n]]$. Namely, every series $F = \sum_{d=0}^{\infty} F_d$, where F_d is a homogeneous polynomial of degree k, defines an element (a_k) of $\hat{\mathbf{A}}$ such that $a_k = F|_k(t_1, t_2, \dots, t_n)$, where $F|_k$ denotes $\sum_{d<k} F_d$. On the other hand, Theorem 4.2.6 implies that

$$\begin{aligned}\mathbf{A}/\mathfrak{m}^k &\simeq \mathbf{K}[x_1, \dots, x_n]/\langle x_1, x_2, \dots, x_n \rangle \\ &\simeq \mathbf{K}[[x_1, \dots, x_n]]/\langle x_1, x_2, \dots, x_n \rangle,\end{aligned}$$

i.e., every element from $\hat{\mathbf{A}}$ can be obtained in this way.

(2) Suppose now that $\mathbf{A} = \mathcal{O}_{X,p}$, where $X \subseteq \mathbb{A}^n$ is an affine variety and p is the origin. Then one easily sees that $\hat{\mathbf{A}} \simeq \mathbf{K}[[x_1, \dots, x_n]]/I(X)\mathbf{K}[[x_1, \dots, x_n]]$. It follows again from

the isomorphism

$$\mathbf{K}[x_1,\dots,x_n]/\langle x_1,x_2,\dots,x_n\rangle \simeq \mathbf{K}[[x_1,\dots,x_n]]/\langle x_1,x_2,\dots,x_n\rangle$$

and the fact that $I=\bigcap_{k=1}^{\infty}(I+\mathfrak{m}^k)$ (cf. Corollary 4.2.4).

DEFINITION 4.5.2. Two local noetherian rings $\mathbf{A}$ and $\mathbf{B}$ are said to be *analytically equivalent* if $\hat{\mathbf{A}}\simeq\hat{\mathbf{B}}$. In particular, one says that the varieties X and Y are *analytically equivalent in the neighbourhoods* of the points, respectively, p and q if $\hat{\mathcal{O}}_{X,p}\simeq\hat{\mathcal{O}}_{Y,q}$. In this case we write $(X,p)\mathrel{\widehat{\sim}}(Y,q)$.

EXAMPLE 4.5.3. If the points $p\in X$ and $q\in Y$ are regular and $\dim_p X=\dim_q Y$, then $(X,p)\mathrel{\widehat{\sim}}(Y,q)$.

The following result is of great use both in algebraic geometry and in number theory.

THEOREM 4.5.4 (Hensel's Lemma). *Let $\mathbf{A}$ be a complete local ring with the maximal ideal $\mathfrak{m}$, $F\in\mathbf{A}[x_1,\dots,x_n]$ be a polynomial and $\mathbf{a}=(a_1,a_2,\dots,a_n)$ be an n-tuple of elements of $\mathbf{A}$ such that:*

(1) $F(\mathbf{a})\equiv 0 \pmod{\mathfrak{m}^{2k+1}}$.

(2) $J=\langle \partial F/\partial x_1(\mathbf{a}),\dots,\partial F/\partial x_n(\mathbf{a})\rangle\supseteq\mathfrak{m}^k$.

Then there is an n-tuple $\mathbf{b}=(b_1,b_2,\dots,b_n)$ such that $F(\mathbf{b})=0$ and $\mathbf{b}\equiv\mathbf{a} \pmod{\mathfrak{m}^{k+1}}$, i.e. $b_i\equiv a_i \pmod{\mathfrak{m}^{k+1}}$ for all indices i.

PROOF. We construct recursively a sequence of n-tuples $\mathbf{a}^{(l)}$, for all $l\ge k$, such that:

(1) $\mathbf{b}^{(k)}=\mathbf{a}$.

(2) $\mathbf{b}^{(l+1)}\equiv\mathbf{b}^{(l)} \pmod{\mathfrak{m}^l}$ for every l.

(3) $F(\mathbf{b}^{(l)})\equiv 0 \pmod{\mathfrak{m}^{k+l+1}}$ for every l.

As $\mathbf{A}$ is complete, there is an n-tuple $\mathbf{b}$ such that $\mathbf{b}\equiv\mathbf{b}^{(l)} \pmod{\mathfrak{m}^l}$ for every l. Then, in particular, $\mathbf{b}\equiv\mathbf{a} \pmod{\mathfrak{m}^k}$ and $F(\mathbf{b})\equiv 0 \pmod{\mathfrak{m}^l}$ for every l, whence $F(\mathbf{b})=0$.

Suppose $\mathbf{b}^{(l)}$ constructed. Then $F(\mathbf{b})\in\mathfrak{m}^{k+l+1}\subseteq J\mathfrak{m}^{l+1}$, thus, there is an n-tuple $\mathbf{h}=(h_1,h_2,\dots,h_n)$ such that $h_i\in\mathfrak{m}^{l+1}$ and $F(\mathbf{b}^{(l)})=-\sum_{i=1}^n \partial F/\partial x_i(\mathbf{a})h_i$. Note that $\partial F/\partial x_i(\mathbf{a})\equiv\partial F/\partial x_i(\mathbf{b}^{(l)}) \pmod{\mathfrak{m}^{k+1}}$. Hence, putting $\mathbf{b}^{(l+1)}=\mathbf{b}^{(l)}+\mathbf{h}$, we get:

$$F(\mathbf{b}^{(l+1)})=F(\mathbf{b}^{(l)})+\sum_{i=1}^n \partial F/\partial x_i(\mathbf{b}^{(l)})h_i+\sum_{i,j}c_{ij}h_ih_j\equiv 0 \pmod{\mathfrak{m}^{k+l+2}},$$

as necessary. □

EXAMPLE 4.5.5. We apply this result to the case of *isolated hypersurface singularities.* Namely, let $X\subset\mathbb{A}^n$ be a hypersurface, $I=I(X)=\langle F\rangle$. Suppose that the origin $p=(0,\dots,0)$ is a singular point on X, which means that $F=O(2)$. Denote by F_m the homogeneous part of F of degree m. Moreover, suppose that this singularity is isolated, i.e., there is a neighbourhood $U \ni p$ containing no more singular points. It means that $V(F, \partial F/\partial x_1, \dots, \partial F/\partial x_n) \cap U = \{ p \}$ or, the same (in view of Hilbert Nullstellensatz), the ideal in the local ring $\mathbf{A} = \mathcal{O}_{X,p}$ generated by the images of $\partial F/\partial x_i$ contains some power $\mathfrak{m}^k$ of the maximal ideal $\mathfrak{m}$. Let $t_1, t_2, \dots, t_n$ denote the images of the affine coordinates $x_1, x_2, \dots, x_n$ in $\mathbf{A}$, $\mathbf{t} = (t_1, t_2, \dots, t_n)$. Consider the polynomial $\tilde{F} = \sum_{i=2}^{2k} F_i \in \mathbf{A}[\, x_1, \dots, x_n \,]$. Then $\tilde{F}(\mathbf{t}) \equiv 0 \pmod{\mathfrak{m}^k}$. Moreover,

$$\partial \tilde{F}/\partial x_i(\mathbf{t}) \equiv \partial F/\partial x_i(\mathbf{t}) \pmod{\hat{\mathfrak{m}}^{2k+1}},$$

hence, $\langle\, \partial \tilde{F}/\partial x_1(\mathbf{t}) \,\rangle \supseteq \hat{\mathfrak{m}}^k$ too. By Hensel's Lemma, there are elements $t'_i \in \hat{\mathbf{A}}$ such that $\tilde{F}\,(t'_1, t'_2, \dots, t'_n) = 0$ and $t'_i \equiv t_i \pmod{\hat{\mathfrak{m}}^{k+1}}$. Then $t'_1, t'_2, \dots, t'_n$ generate $\hat{\mathfrak{m}}^k$, so they can also be used for expansion of elements of $\hat{\mathbf{A}}$ into power series. But as $\hat{\mathbf{A}}$ is *complete*, any power series defines an element of $\hat{\mathbf{A}}$. It means that $\hat{\mathbf{A}} \simeq \mathbf{K}[[\, x_1, \dots, x_n \,]]/\langle\, \tilde{F} \,\rangle$. So, $(X,p) \mathrel{\widehat{\sim}} (X',p)$, where $I(X') = \langle\, \tilde{F} \,\rangle$. In other words, considering an isolated hypersurface singularity, one can always omit the terms of the defining relation of big enough degrees (starting from $2k+1$ in the above situation).

COROLLARY 4.5.6. *Suppose that p is a singular point of a hypersurface $X \subset \mathbb{A}^n$ such that, if $I(X) = \langle\, F \,\rangle$, the matrix $(\partial^2 F/\partial x_i \partial x_j)$ is invertible. If* $\operatorname{char} \mathbf{K} \neq 2$, $(X,p) \mathrel{\widehat{\sim}} (C,0)$, *where C is the quadratic affine cone $C = V(\sum_{i=1}^n x_i^2)$.*

PROOF. One can suppose that p is also the origin, i.e., $F = O(2)$. A change of coordinates allows to put $F_2 = \sum_{i=1}^2 x_i^2$. Then $\langle\, \partial F/\partial x_1, \partial F/\partial x_2, \dots, \partial F/\partial x \,\rangle = \mathfrak{m}$ and we can apply Example 4.5.5. □

EXERCISES 4.5.7. In all these exercises X denotes a hypersurface in $\mathbb{A}^n$ and we suppose that $p = (0, \dots, 0) \in X$ is a singular point of X. Let $I(X) = \langle\, F \,\rangle$. Then $F = F_2 + \dots + F_m$, where F_k is homogeneous of degree k. Write $O(m)$ for a polynomial having no terms of degrees less than m.

(1) ("Formal Morse's Lemma"). Let $r = \operatorname{rk} F_2$ (the rank of the matrix of the quadratic form F_2). Prove that $(X,p) \mathrel{\widehat{\sim}} (Y,p)$, where $I(Y) = \langle\, \sum_{i=1}^r x_i^2 + G(x_{r+1}, \dots, x_n) \,\rangle$. (Certainly, $G = O(3)$.)
(2) Suppose that p is a singularity of type A_k, i.e., $n = 2$ and $F = y^2 + x^{k+1} + O(k+2)$. Prove that $(X,p) \mathrel{\widehat{\sim}} (Y,p)$, where $I(Y) = \langle\, y^2 + x^{k+1} \,\rangle$.
(3) Prove that an *ordinary multiple point* of a plane curve is analytically equivalent to its tangent cone.

CHAPTER 5

Intersection theory

This chapter is the shortest one. It only contains the first steps towards the intersection theory. Namely, we consider the intersections of projective varieties in the projective space. The resulting point is certainly Bezout Theorem generalizing the elementary fact that a polynomial (in one variable) has as many roots as its degree; of course, if we calculate them with the "corresponding multiplicities." Indeed, the main problem here is to define well what "corresponding multiplicities" mean.

DEFINITIONS 5.1. (1) A *graded ring* is a ring $\mathbf{A}$ together with a direct decomposition of its additive group: $\mathbf{A} = \bigoplus_{k=0}^{\infty} \mathbf{A}_k$, such that $\mathbf{A}_k\mathbf{A}_l \subseteq \mathbf{A}_{k+l}$ for all k, l.[1]

(2) A *graded module* over a graded ring $\mathbf{A}$ is an $\mathbf{A}$-module M together with a direct decomposition of its additive group: $M = \bigoplus_{k=-\infty}^{+\infty}$, such that $\mathbf{A}_k M_l \subseteq M_{k+l}$.

Elements from $\mathbf{A}_k$ or M_k are called *homogeneous of degree* k. Usually considering elements from a graded ring or module we suppose them homogeneous. For an arbitrary element $u \in M$, its *homogeneous components* are, by definition, such elements $u_k \in M_k$ that $u = \sum_k u_k$. (They are uniquely defined and almost all zero.)

(3) A submodule N of a graded module M (in particular, an ideal of a graded ring itself) is called *homogeneous* if $N = \bigoplus_k (N \cap M_k)$ or, the same, whenever an element a (non-homogeneous!) belongs to N, all its homogeneous components belong to N as well. We always consider such a submodule as a graded module putting $N_k = N \cap M_k$.

(4) For a graded module M, the *shifted* module $M(m)$ is defined as the same module, but with a new grading: $M(m)_k = M_{k+m}$.

EXAMPLE 5.2. The polynomial algebra $\mathbf{K}[\,\mathbf{x}\,] = \mathbf{K}[\,x_0, x_1, \dots, x_n\,]$ can be considered as a graded one if we denote by $\mathbf{K}[\,\mathbf{x}\,]_k$ the set of homogeneous polynomials of degree k (including zero). We always

[1]Sometimes more general notion of graded ring is considered, when the index k runs through a semi-group; in particular, the case $k \in \mathbb{Z}$ often occurs. Evident changes in the definitions can be easily made by a reader.

consider $\mathbf{K}[\mathbf{x}]$ with this grading (though in some questions it can happen useful to endure other grading on it).

If $N \subseteq M$ is a homogeneous submodule, the factor-module M/N can also be considered as a graded one: $M/N = \bigoplus_k M_k/N_k$. In particular, if $I \subseteq \mathbf{A}$ is a homogeneous ideal, the factor-ring $\mathbf{A}/I$ is again a graded ring. If a graded module M is finitely generated, one can always choose a finite generating set of M consisting of homogeneous elements (just taking non-zero homogeneous components of an arbitrary generators). Therefore, there is an index k_0 such that $M_k = 0$ for $k < k_0$ (take the minimal degree of homogeneous generators).

It follows from the definition that $\mathbf{A}_0$ is a subring of $\mathbf{A}$ and all components $\mathbf{A}_k$ as well as all components M_k of a graded $\mathbf{A}$-module M are $\mathbf{A}_0$-modules.

We usually consider the case when $\mathbf{A}$ is indeed a graded $\mathbf{K}$-algebra (then, of course, all $\mathbf{A}_k$ are supposed to be subspaces). Moreover, we mostly deal with such graded algebras that $\mathbf{A}_0 = \mathbf{K}$; they are called *connected graded* $\mathbf{K}$-algebras.

EXAMPLE 5.3. Our main examples are related to projective varieties. If $X \subseteq \mathbb{P}^n$ is a projective variety, the ideal $I(X)$ is a homogeneous ideal in $\mathbf{K}[\mathbf{x}]$. Put $\mathbf{K}^{\mathrm{h}}[X] = \mathbf{K}[\mathbf{x}]/I(X)$ and call $\mathbf{K}^{\mathrm{h}}[X]$ the *graded coordinate algebra* of X. Indeed, it depends not only on X but also on the embedding $X \subseteq \mathbb{P}^n$ (cf. Exercise refex2-7(9)).

The following proposition is quite obvious.

PROPOSITION 5.4. *Suppose that* $\mathbf{A}$ *is a finitely generated graded* $\mathbf{K}$*-algebra,* M *be a finitely generated graded* $\mathbf{A}$*-module. Then* $\dim_{\mathbf{K}} M_k < \infty$ *for every* k.

In this situation the function $h_M(k) = \dim_{\mathbf{K}} M_k$ is called the *Hilbert function* of the module M.

EXAMPLES 5.5. (1) For $M = \mathbf{A} = \mathbf{K}[x_0, x_1, \dots, x_n]$, one has $h_M(k) = \binom{k+n}{n}$. So, it is a polynomial with the leading coefficient $1/n!$.

(2) Let now $M = \mathbf{A} = \mathbf{K}[x_0, x_1, \dots, x_n]/\langle F \rangle$, where F is a homogeneous polynomial of degree m. Then

$$h_M(k) = \begin{cases} \binom{k+n}{n} & \text{if } k < m \\ \binom{k+n}{n} - \binom{k-m+n}{n} & \text{if } k \geq m \end{cases}$$

So, for $k \geq m$, $h_M(k)$ coincides with a polynomial, whose leading coefficient coincides with that of $x^n/n! - (x-m)/n!$, which is $m/(n-1)!$.

We are going to prove that these examples are quite typical. Namely, we say that two functions $f, g : \mathbb{Z} \to \mathbb{Z}$ *coincide for big enough* k if there is k_0 such that $f(k) = g(k)$ for all $k \geq k_0$. We denote by $\mathfrak{s}$ the graded algebra $\mathbf{K}[x_0, x_1, \dots, x_n]$.

THEOREM 5.6 (Hilbert–Serre's Theorem). *Let M be a finitely generated graded $\mathbb{S}$-module. Denote $d(M) = \dim PV(\operatorname{Ann}_{\mathbb{S}} M)$. Then there is a polynomial $H_M(x) \in \mathbb{Q}[x]$ of degree $d = d(M)$ such that $h_M(k) = H_M(k)$ for big enough k. Moreover, the leading coefficient of $H_M(x)$ is $e/d!$ for some positive integer e.*

The polynomial H_M is called the *Hilbert polynomial* of the module M and the integer e is called the *degree* of the module M and denoted $\deg M$. If $M = \mathbb{S}/I(X)$, where $X \subseteq \mathbb{P}^n$ is a projective variety, H_M is called the *Hilbert polynomial* of the variety X and denoted by H_X, while $\deg M$ is called the *degree* of the variety X and denoted by $\deg X$.

The examples above show that $\deg \mathbb{P}^n = 1$, while for a hypersurface $X \subset \mathbb{P}^n$, $\deg X = \deg F$, where $I(X) = \langle F \rangle$. Remind that both Hilbert polynomial and the degree of a projective variety are *not*invariants of this variety itself, but further of its embedding into a projective space. For instance, $\mathbb{P}^1 \simeq C$, where $C \subset \mathbb{P}^2$ is an irreducible conic, but $\deg \mathbb{P}^1 = 1$, while $\deg C = 2$.

REMARK. Let $\sqrt{\operatorname{Ann} M} = \bigcap_{i=1}^s \mathfrak{p}_i$ be the prime decomposition of $\sqrt{\operatorname{Ann} M}$. Then $PV(\operatorname{Ann} M) = \bigcup_{i=1}^s PV(\mathfrak{p}_i)$ is the irreducible decomposition of the variety $PV(\operatorname{Ann} M)$. Hence, $\dim PV(\operatorname{Ann} M) = \max_i \dim PV(\mathfrak{p}_i) = \max_i(n - \operatorname{ht} \mathfrak{p}_i)$ (cf. Theorem 3.5.1 and Proposition 3.5.10). Note that $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_s$ are just the minimal among the prime ideals containing $\operatorname{Ann} M$.

First we establish some properties of polynomials from $\mathbb{Q}[x]$ having integral values in all integral points. We call such polynomials the *numerical polynomials.*

LEMMA 5.7. (1) *If $f \in \mathbb{Q}[x]$ is a numerical polynomial of degree d, there are integers c_i such that*

$$f(x) = \sum_{i=0}^{d} c_i \binom{x+i}{i}.$$

(In particular, the leading coefficient of f is $c_d x^d/d!$ with integral c_d.)

(2) *If $h : \mathbb{N} \to \mathbb{Z}$ is a function such that, for big enough k, the* difference function $\Delta h(k)$ *coincides with a numerical polynomial, then $h(k)$ also coincides, for big enough k, with a numerical polynomial.*

PROOF. We prove both *1* and *2* together using, for *1*, the induction by $d = \deg f$. The claim *1* is trivial for $d = 0$. Now suppose that *1* is true for polynomials of degree $d-1$ and let $\Delta h(k)$ coincide, for $k \geq k_0$, with a numerical polynomial $g(x)$ of degree d. Then, by the induction hypothesis,

$$g(x)=\sum_{i=0}^{d-1} c_i\binom{x+i}{i}$$

for some integers c_i. Put

$$f(x)=\sum_{i=1}^{d} c_{i-1}\binom{x+i}{i}+h(k_0)-\sum_{i=1}^{d} c_{i-1}\binom{k_0+i}{i}.$$

Then $\Delta f(x)=g(x)$ and $f(k_0)=h(k_0)$, hence, $f(k)=h(k)$ for all $k\geq k_0$. $\square$

Proof of Theorem 5.6. We use the induction on $d(M)$. First consider the case $d(M)=-1$ (i.e., $M=\emptyset$) or, the same, $\sqrt{\operatorname{Ann} M}=I_+=\langle x_0,x_1,\dots,x_n\rangle$ (cf. Theorem 2.1.3). Then $I_+^m M=0$ for some m, which evidently implies that $M_k=0$ for big enough k (namely, for $k>m+k_0$, where k_0 is the biggest integer such that M_{k_0} contains elements from a chosen generating set). Thus, $h_M(k)=0$ for big enough k.

Now suppose that the theorem holds for modules N with $d(N)=d(M)-1$. Consider the case, when $M=\mathbb{S}/\mathfrak{p}$ for a prime homogeneous ideal $\mathfrak{p}\neq I_+$. Choose $x_i\notin\mathfrak{p}$. Then the multiplication by x_i is a monomorphism $M(-1)\to M$. (We should write $M(-1)$ here as, if $u\in M_k$, $x_iu\in M_{k+1}$ and $M(-1)_{k+1}=M_k$.) So M contains a submodule $x_iM\simeq M(-1)$. Put $N=M/x_iM$. Then $h_N(k)=h_M(k)-h_{M(-1)}(k)=\Delta h_M(k)$. On the other hand, $\operatorname{Ann} N=\mathfrak{p}+\langle x_i\rangle$, so, by Krull Hauptidealsatz, for any minimal prime ideal $\mathfrak{q}\supseteq\operatorname{Ann} N$, $\operatorname{ht}\mathfrak{q}=\operatorname{ht}\mathfrak{p}+1$, whence $d(N)=d(M)-1$. By the inductive hypothesis, $h_N(k)=H_N(k)$ for big enough k, where $H_N(k)$ is a numerical polynomial of degree $d(N)$, so, by Lemma 5.7, $h_M(k)=H_M(k)$ for big enough k, where $H_M(k)$ is a numerical polynomial of degree $d(M)$.

The rest of the proof relies on the following lemma, which is also useful in many other situations.

Lemma 5.8. *Let* $\mathbf{A}$ *be a graded noetherian ring,* M *be a finitely generated graded* $\mathbf{A}$*-module. There is a finite filtration*

$$M=M_0\supset M_1\supset M_2\supset\ldots\supset M_l=\langle 0\rangle, \tag{5.1}$$

where M_i *are homogeneous submodules and, for every* $i=1,\dots l$, $M_{i-1}/M_i\simeq\mathbf{A}/\mathfrak{p}_i(m_i)$ *for some homogeneous prime ideals* $\mathfrak{p}_i$ *and some integers* m_i.

Such a filtration will further be called a "*good filtration.*"

Having a good filtration in a finitely generated $\mathbb{S}$-module M, we are able to calculate $h_M(k)$ as $\sum_{i=1}^{l} h_{N_i}(k)$, where $N_i=\mathbb{S}/\mathfrak{p}_i(m_i)$. As we have proved above, each summand coincides, for big enough k, with a numerical polynomial $H_i(k)$ of degree $n - \operatorname{ht}\mathfrak{p}_i$. Therefore, $h_M(k)$ coincides, for big enough k, with the numerical polynomial $H_M(k) = \sum_{i=1}^{l} H_i(k)$. Note now that $\operatorname{Ann} M \subseteq \operatorname{Ann} M_{i-1}/M_i = \mathfrak{p}_i$ for each i and $\operatorname{Ann} M \supseteq \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_l$. Hence, a prime ideal $\mathfrak{p}$ contains $\operatorname{Ann} M$ if and only if it contains one of $\mathfrak{p}_i$. Thus, $d(M) = \max_i \{ n - \operatorname{ht}\mathfrak{p}_i \} = \deg H_M(k)$, which accomplishes the proof of the theorem. □

Proof of Lemma 5.8. Consider the annihilators of all non-zero homogeneous elements of M. They are proper homogeneous ideals in $\mathbf{A}$. As $\mathbf{A}$ is noetherian, this set contains a maximal element $I = \operatorname{Ann} v_0$. We show that I is prime. Indeed, let $ab \in I$ but $a \notin I$. Certainly, we can choose a and b homogeneous. Then $av_0 \neq 0$ but $(I + \langle b \rangle)(av_0) = 0$. As I is maximal among annihilators, $b \in I$. Thus, if $v \in M_m$, $\langle v_0 \rangle \simeq \mathbf{A}/I(m)$, i.e., every (non-zero) finitely generated graded $\mathbf{A}$-module M contains a submodule of the shape $\mathbf{A}/\mathfrak{p}(m)$. As M is noetherian, one can choose a maximal submodule $N \subseteq M$ having a good filtration. If $M/N \neq \langle 0 \rangle$, this factor-module has a submodule of the shape $\mathbf{A}/\mathfrak{p}(m)$, so, the preimage of this submodule in M is a bigger submodule $N' \supset N$ having a good filtration, which is impossible. Hence, $N = M$ and the lemma has been proved. □

A good filtration of a module M constructed in Lemma 5.8 is not unique. Nevertheless, if $\mathfrak{p}$ is a *minimal* prime ideal containing $\operatorname{Ann} M$, the multiplicity of $\mathbf{A}/\mathfrak{p}$ as of factor of this filtration is uniquely determined as the following lemma shows.

Lemma 5.9. *Let $M = M_0 \supset M_1 \supset \dots \supset M_l = \{ 0 \}$ be a good filtration of a graded $\mathbf{A}$-module M as in Lemma 5.8 and $\mathfrak{p}$ be a minimal prime ideal containing* $\operatorname{Ann} M$. *Then the number* $\operatorname{mult}_{\mathfrak{p}}(M) = \# \{ i \mid \mathfrak{p}_i = \mathfrak{p} \}$ *does not depend on the choice of a good filtration.*

This number is called the *multiplicity* of $\mathfrak{p}$ in M.

Proof. For any $\mathbf{A}$-module M and any multiplicative subset $S \subseteq \mathbf{A}$, one defines the $\mathbf{A}[S^{-1}]$-module $M[S^{-1}]$ as the set of "formal fractions" $\{ v/s \mid v \in M,\ s \in S \}$ with just the same rules as for the ring of fractions, namely:

$$\frac{v}{s} = \frac{u}{t} \text{ if and only if there is } r \in S \text{ such that } rtv = rsu;$$
$$\frac{v}{s} + \frac{u}{t} = \frac{tv + su}{st};$$
$$\frac{a}{s} \cdot \frac{u}{t} = \frac{au}{st}.$$

(In the last line $a/s \in \mathbf{A}[S^{-1}]$.) One easily check that these rules are indeed consistent and define an $\mathbf{A}[S^{-1}]$-module. Moreover, if $N \subseteq M$ is a submodule, then $N[S^{-1}]$ is a submodule in $M[S^{-1}]$ and $M[S^{-1}]/N[S^{-1}] \simeq M/N[S^{-1}]$. (They say that this procedure, or the "functor" $M \mapsto M[S^{-1}]$ is *exact*.)

We consider the case when $S = \mathbf{A} \setminus \mathfrak{p}$ and write $M_{\mathfrak{p}}$ instead of $M[\,S^{-1}\,]$. Let $N = \mathbf{A}/\mathfrak{q}$ for some prime $\mathfrak{q}$. If $\mathfrak{q} \not\subseteq \mathfrak{p}$, there is $s \in \mathfrak{q}\setminus\mathfrak{p}$, so, for every $v \in \mathfrak{m}$, $sv = 0$ implies that $v/t = 0$ in $N_{\mathfrak{p}}$ for all t, i.e., $N_{\mathfrak{p}} = \{\,0\,\}$. On the contrary, if $N = \mathbf{A}/\mathfrak{p}$, then $N_{\mathfrak{p}} \simeq \mathbf{A}_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$ is the simple $\mathbf{A}_{\mathfrak{p}}$-module.

Now, given a good filtration of $\mathfrak{m}$, we get a filtration $M_{\mathfrak{p}} = M_{0\mathfrak{p}} \supseteq M_{1\mathfrak{p}} \supseteq \ldots \supseteq M_{l\mathfrak{p}} = \{\,0\,\}$ with the factors $(\mathbf{A}/\mathfrak{p}_i)_{\mathfrak{p}}$. But whenever $\mathfrak{p}_i \neq \mathfrak{p}$, one also has $\mathfrak{p}_i \not\subset \mathfrak{p}$ (as $\mathfrak{p}$ is minimal). Hence, the only non-zero factors of the latter filtration are those with $\mathfrak{p}_i = \mathfrak{p}$ and all of them are simple $\mathbf{A}_{\mathfrak{p}}$-modules. Thus, $\operatorname{mult}_{\mathfrak{p}}(M)$ coincides with the *length* of the $\mathbf{A}_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$, which certainly does not depend on the filtration. $\square$

Let now $X, Y \subseteq \mathbb{P}^n$ be projective varieties. One knows that $X \cap Y = PV(I(X) + I(Y))$. Denote by $M(X.Y)$ the factor-module $\mathbb{S}/I(X) + I(Y)$. Then the irreducible components of $X \cap Y$ are of the form $PV(\mathfrak{p})$, where $\mathfrak{p}$ runs through minimal prime ideals containing $I(X) + I(Y) = \operatorname{Ann} M(X.Y)$. For every such component $Z = PV(\mathfrak{p})$ put $\operatorname{mult}(X.Y; Z) = \operatorname{mult}_{\mathfrak{p}}(M(X.Y))$. This number is also called the *multiplicity* of Z in the intersection $X \cap Y$. A good filtration (5.1) of the module $M = M(X.Y)$ gives the equality for the Hilbert polynomial:

$$H_M(x) = \sum_Z \operatorname{mult}(X.Y; Z) H_Z(x)\,,$$

where Z runs through irreducible components of $X \cap Y$. If we are interested in the *degree* of $M(X.Y)$, we only have to consider the components of the biggest degree in this formula, whence

$$\deg(M(X.Y)) = \sum_Z \operatorname{mult}(X.Y; Z) \deg Z\,, \tag{5.2}$$

where Z runs through irreducible components of $X \cap Y$ such that $\dim Z = \dim X \cap Y$.

Example 5.10 (Bezout's Theorem). Consider the case, when Y is a hypersurface of degree m, i.e., $I(Y) = \langle\, F\,\rangle$ with $\deg F = m$. We suppose, moreover, that Y contains no component of X, which means, in view of Hilbert Nullstellensatz, that the image of F in $\mathbb{S}/I(X)$ is non-zero divisor. Hence, we have an exact sequence

$$0 \longrightarrow \mathbb{S}/I(X)(-m) \xrightarrow{F} \mathbb{S}/I(X) \longrightarrow M(X.Y) \longrightarrow 0\,,$$

which gives: $H_M(x) = H_X(x) - H_X(x-m)$, where $M = M(X.Y)$. Hence, the leading coefficient of H_M coincides with that of $ex^d/d! - e(x-m)^d/d!$, where $d = \dim X$, $e = \deg X$. So, $\deg M = em$, which gives, together with (5.2), the following formula, known as "*Bezout's Theorem*":

$$\sum_Z \operatorname{mult}(X.Y; Z) \deg Z = \deg X \deg Y\,, \tag{5.3}$$

where Z runs through all components of the intersection $X \cap Y$ whose dimension is $\dim X - 1$.

Bezout's Theorem becomes especially simple if X and Y are both *plane curves*, i.e., $n = 2$, $I(X) = \langle G \rangle$, $I(Y) = \langle F \rangle$, where F and G have no common divisors. Then, in (5.3), all Z are just points, so, $\deg Z = 1$, whence:

$$\sum_{p \in X \cap Y} \operatorname{mult}(X.Y; p) = \deg X \deg Y .$$

This is the classical Bezout's Theorem for the "number of roots of a system of two non-linear equations". Note that, as often, to get a "good" form of the theorem, we should introduce "infinite points," i.e., to pass from affine to projective spaces, as well as to do some job to prescribe the "correct" multiples to the roots.

EXERCISES 5.11. Define the *multiplicity* in multiple intersections $\operatorname{mult}(X_1.X_2.\dots.X_k; Z)$ and prove analogues of the formula (5.2) and of Bezout Theorem. In particular, for n hypersurfaces $X_1, X_2, \dots, X_n$ in $\mathbb{P}^n$ in "general position" prove that

$$\sum_{p \in \bigcup_{i=1}^n X_i} \operatorname{mult}(X_1.X_2.\dots.X_k; p) = \deg X \deg Y .$$

("General position" means here that $\dim \bigcup_{i=1}^n X_i = 0$.)

Contents