§6 Commutative algebra draught

Everywhere in §6, the term «ring» means by default a commutative ring with unit. All ring homomorphisms are assumed to map the unit to the unit.

6.1 Noetherian rings. Every subset M in a commutative ring K generates an ideal $(M) \subset K$ formed by all finite sums $b_1a_1 + b_2a_2 + \cdots + b_ma_m$, where $a_1, a_2, \ldots, a_m \in M$, $b_1, b_2, \ldots, b_m \in K$, $m \in \mathbb{N}$. Every ideal $I \subset K$ is generated by some subset $M \subset K$, e.g., by $M = I$. An ideal $I \subset M$ is said to be *finitely generated* if it admits a finite set of generators, that is, if it can be written as $I = (a_1, a_2, \ldots, a_k) = \{b_1a_1 + b_2a_2 + \cdots + b_ka_k \mid b_i \in K\}$ for some $a_1, a_2, \ldots, a_k \in I$.

LEMMA 6.1
The following properties of a commutative ring K are equivalent:

1) Every subset $M \subset K$ contains some finite collection of elements $a_1, a_2, \ldots, a_k \in M$ such that $(M) = (a_1, a_2, \ldots, a_k)$.

2) Every ideal $I \subset K$ is finitely generated.

3) For every infinite chain of increasing ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ in K there exists $n \in \mathbb{N}$ such that $I_\nu = I_n$ for all $\nu \geqslant n$.

PROOF. Clearly, (1) ⇒ (2). To deduce (3) from (2), write $I = \bigcup I_\nu$ for the union of all ideals in the chain. Then I is an ideal as well. By (2), I is generated by some finite set of its elements. All these elements belong to some I_n. Therefore, $I_n = I = I_\nu$ for all $\nu \geqslant n$. To deduce (1) from (3), we construct inductively a chain of strictly increasing ideals $I_n = (a_1, a_2, \ldots, a_n)$ starting from an arbitrary $a_1 \in M$. While $I_k \neq (M)$, we choose any element $a_{k+1} \in M \smallsetminus I_k$ and put $I_{k+1} = (a_{k+1} \cup I_k)$. Since $I_k \subsetneq I_{k+1}$ in each step, by (3) this procedure has to stop after a finite number of steps. At that moment, we obtain $I_m = (a_1, a_2, \ldots, a_m) = (M)$. □

DEFINITION 6.1
A commutative ring K is called to be *Noetherian* if it satisfies the conditions from Lemma 6.1. Note that every field is Noetherian.

THEOREM 6.1 (HILBERT'S BASIS THEOREM)
For every Noetherian commutative ring K the polynomial ring $K[x]$ is Noetherian as well.

PROOF. Consider an arbitrary ideal $I \subset K[x]$ and write $L_d \subset K$ for the set of leading coefficients of all polynomials of degree $\leqslant d$ in I including the zero polynomial. Also we write $L_\infty = \cup_d L_d$ for the set of all leading coefficients of all polynomials in I.

EXERCISE 6.1. Verify that all of the L_d and L_∞ are the ideals in K.

Since K is Noetherian, all ideals L_d and L_∞ are finitely generated. For all d (including $d = \infty$), write $f_1^{(d)}, f_2^{(d)}, \ldots, f_{m_d}^{(d)} \in K[x]$ for those polynomials whose leading coefficients span the ideal $L_d \subset K$. Let $D = \max \deg f_i^{(\infty)}$. We claim that polynomials f_i^{∞} and $f_j^{(d)}$ for $d < D$ generate I. Let us show first that each polynomial $g \in I$ is congruent modulo $f_1^{(\infty)}, f_2^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)}$ to some polynomial of degree less than D. Since the leading coefficient of g lies in L_∞, it can be written as $\sum \lambda_i a_i$, where $\lambda_i \in K$ and a_i is the leading coefficient of $f_i^{(\infty)}$. As long as $\deg g \geqslant D$ all differences $m_i = \deg g - \deg f_i^{(\infty)}$ are nonnegative, and we can form the polynomial $h = g - \sum \lambda_i \cdot f_i^{(\infty)}(x) \cdot x_i^{m_i}$, which is congruent

to g modulo I and has $\deg h < \deg g$. We replace g by h and repeat the procedure while $\deg h \geqslant D$. When we come to a polynomial $h \equiv g \pmod{I}$ such that $\deg h < D$, the leading coefficient of h falls into some L_d with $d < D$, and we can cancel the leading terms of h by subtracting appropriate combinations of polynomials $f_j^{(d)}$ for $0 \leqslant d < D$ until we get $h = 0$. □

COROLLARY 6.1
For every Noetherian commutative ring K, the ring $K[x_1, x_2, \dots, x_n]$ is Noetherian. □

EXERCISE 6.2. For every Noetherian commutative ring K show that the ring $K[\![x_1, x_2, \dots, x_n]\!]$ of formal power series in $x_1, x_2, \dots, x_n$ with coefficients in K is Noetherian as well.

COROLLARY 6.2
Every infinite system of polynomial equations with coefficients in a Noetherian commutative ring K is equivalent to some finite subsystem.

PROOF. Since $K[x_1, x_2, \dots, x_n]$ is Noetherian, among the right hand sides of a polynomial equation system $f_\nu(x_1, x_2, \dots, x_n) = 0$ there is some finite collection $f_1, f_2, \dots, f_m$ that generates the same ideal as all the f_ν. This means that every $f_\nu = g_1 f_1 + g_2 f_2 + \cdots + g_m f_m$ for some $g_i \in K[x_1, x_2, \dots, x_n]$. Hence, every equation $f_\nu = 0$ follows from $f_1 = f_2 = \cdots = f_m = 0$. □

EXERCISE 6.3. Show that all quotient rings of a Noetherian ring are Noetherian.

CAUTION 6.1. A subring of a Noetherian ring is not necessary Noetherian. For example, the ring $\mathbb{C}[\![z]\!]$ is Noetherian by Exercise 6.2. However, the subring $\mathcal{H} \subset \mathbb{C}[\![z]\!]$ of holomorphic functions[1] $f : \mathbb{C} \to \mathbb{C}$ is not Noetherian, because there exist a sequence of holomorphic functions $f_n : \mathbb{C} \to \mathbb{C}$ such that for all $n \in \mathbb{N}$, $f_n(z) = 0$ exactly for $z \in \mathbb{Z} \setminus [-n, n]$ and therefore, $I_n = (f_1, f_2, \dots, f_n)$ form an infinite chain of strictly increasing ideals.

EXERCISE 6.4. Construct such a sequence $(f_n)_{n\in\mathbb{N}}$ explicitly.

6.2 Integral elements. An *extension of rings* is a pair $A \subset B$, where A is a subring of a ring B and both rings have common unit. Given such a ring extension $A \subset B$, an element $b \in B$ is called *integral* over A if it satisfies the conditions of the following lemma.

LEMMA 6.2 (CHARACTERIZATION OF INTEGRAL ELEMENTS)
The following properties of an element $b \in B$ in a ring extension $A \subset B$ are equivalent:

(1) $b^m = a_1 b^{m-1} + \cdots + a_{m-1} b + a_m$ for some $m \in \mathbb{N}$ and $a_1, a_2, \dots, a_m \in A$.

(2) The A-linear span of all nonnegative integer powers b^m is a finitely generated A-module.

(3) There exists a finitely generated A-module $M \subset B$ such that $bM \subset M$ and $b'M \neq 0$ for all nonzero $b' \in B$.

PROOF. The implications (1) ⇒ (2) ⇒ (3) are obvious. Let us show that (3) ⇒ (1). Fix some $e_1, e_2, \dots, e_m$ spanning M over A. Then $(be_1, be_2, \dots, be_m) = (e_1, e_2, \dots, e_m) \cdot Y$ for some matrix

[1] That is, power series converging everywhere in $\mathbb{C}$.

$Y \in \mathrm{Mat}_m(A)$ and therefore, $(e_1, e_2, \dots, e_m) \cdot (bE - Y) = 0$. It follows from the matrix identity[1] $\det X \cdot E = X \cdot X^\vee$, where X is a square matrix over a commutative ring, E is the identity matrix of the same size, and $X^\vee$ is the adjunct matrix[2] of X, that the image of multiplication by $\det X$ lies in the linear span of the columns of the matrix X. For $X = (bE - Y) \in \mathrm{Mat}_m(B)$, this means that $\det(bE - Y) \cdot M$ is contained in the B-linear span of vectors $(e_1, e_2, \dots, e_m) \cdot (bE - Y)$, which is zero. The last property in (3) forces $\det(bE - Y) = 0$. Since all elements of Y lie in A, the latter equality can be rewritten in the form appearing in (1). □

DEFINITION 6.2
Let $A \subset B$ be an extension of rings. The set of all elements $b \in B$ integral over A is called the *integral closure* of A in B. If it coincides with A, then A is said to be *integrally closed* in B. If all elements of B are integral over A, then the extension $A \subset B$ is called an *integral* ring extension, and we say that B is *integral* over A.

EXAMPLE 6.1 ($\mathbb{Z}$ IS INTEGRALLY CLOSED IN $\mathbb{Q}$)
Let $A = \mathbb{Z}$, $B = \mathbb{Q}$. If a fraction $p/q \in \mathbb{Q}$ with coprime $p, q \in \mathbb{Z}$ satisfies a monic polynomial equation

$$\frac{p^m}{q^m} = a_1 \frac{p^{m-1}}{q^{m-1}} + \cdots + a_{m-1}\frac{p}{q} + a_m$$

with $a_i \in \mathbb{Z}$, then $p^m = a_1 q p^{m-1} + \cdots + a_{m-1} q^{m-1} p + a_m q^m$ is divisible by q. Since p, q are coprime, we conclude that $q = \pm 1$. Hence, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

EXAMPLE 6.2 (INVARIANTS OF A FINITE GROUP)
Let a finite group G act on a ring B by ring automorphisms, and $B^G \stackrel{\text{def}}{=} \{ a \in B \mid ga = a \ \forall g \in G \}$ be the subring of *G-invariants*. Then B is integral over B^G. Indeed, write $b_1, b_2, \dots, b_n$ for the G-orbit of an arbitrary element $b = b_1 \in B$. Then b is a root of the monic polynomial

$$f(t) = \prod (t - b_i) \in B^G[t]$$

as required in the first property of Lemma 6.2.

PROPOSITION 6.1
Let $A \subset B$ be an extension of rings, and $\overline{A}_B \subset B$ the integral closure of A in B. Then $\overline{A}_B$ is a subring of B, and for any ring extension $C \supset B$, every element $c \in C$ integral over $\overline{A}_B$ is integral over A as well.

PROOF. If elements $p, q \in B$ satisfy the monic polynomial equations

$$p^m = x_1 p^{m-1} + \cdots + x_{m-1} p + x_m$$
$$q^n = y_1 q^{n-1} + \cdots + y_{n-1} q + y_n$$

for some $x_\nu, y_\mu \in A$, then the products $p^i q^j$ with $0 \leqslant i < m - 1$, $0 \leqslant j < n - 1$ span a finitely generated A-module, containing the unit and mapped to itself by the multiplication by p and by q.

[1] This is $n = 1$ case of the Laplace identity $\mathcal{X}_n \cdot \mathcal{X}_n^\vee = \det X \cdot E$ from the Example 4.4 on p. 47.

[2] That is, transposed to the matrix of algebraic complements $(-1)^{i+j} x_{\hat{i}\hat{j}}$ to the elements x_{ij} of matrix X, see Example 4.4 on p. 47.

Therefore, it satisfies the condition (3) from Lemma 6.2 for both $b = p + q$ and $b = pq$. Similarly, if the monic polynomial equations

$$\begin{aligned} c^r &= z_1\, c^{r-1} + \cdots + z_{r-1}\, c + z_r \\ z_k^{m_k} &= a_{k,1}\, z^{m_k-1} + \cdots + a_{k,m_k-1}\, z_k + a_{k,m_k} \quad 1 \leqslant k \leqslant r, \end{aligned}$$

hold for some $c \in C$, $z_1, z_2, \ldots, z_r \in \overline{A}_B$, and $a_{k,\ell} \in A$, then the A-linear span of products

$$c^i z_1^{j_1} z_2^{j_2} \cdots z_r^{j_r}, \quad 0 \leqslant i < r-1,\ 0 \leqslant j_k < m_k - 1,$$

contains the unit and goes to itself under the multiplication by c. Thus, c is integral over A. □

PROPOSITION 6.2 (GAUSS – KRONECKER – DEDEKIND LEMMA)
Let $A \subset B$ be an extension of rings, and $f, g \in B[x]$ monic polynomials of positive degree. Then all coefficients of the product fg are integral over A if and only if all coefficients of the polynomials f, g are integral A.

PROOF. Let $C \supset B$ be an extension of rings such that the polynomials f, g are completely factorisable in $C[x]$ as $f(x) = \prod(x - \alpha_\nu)$ and $g(x) = \prod(x - \beta_\mu)$ for some $\alpha_\nu, \beta_\mu \in C$. Then their product $h(x) = f(x)g(x) = \prod(x - \alpha_\nu)\prod(x - \beta_\mu)$ is also completely factorisable.

EXERCISE 6.5. Given a finite set of monic polynomials of positive degree in $B[x]$, prove that there is an extension of rings $B \subset C$ such that all polynomials become completely factorisable in $C[x]$.

If all coefficients of h are integral over A, then all the roots $\alpha_\nu, \beta_\mu \in C$ are integral over $\overline{A}_C$ and therefore integral over A by Proposition 6.1. Since integral elements form a ring, all coefficients of both f, g, which are the symmetric functions of α_ν, β_μ, are also integral over A. The same arguments work in the opposite direction as well. □

PROPOSITION 6.3
Let $A \subset B$ be an integral extension of rings. If B is a field, then A is a field too. Conversely, if A is a field and B has no zero divisors, then B is a field.

PROOF. Let B be an integral field over A. Then, for any nonzero $a \in A$, the inverse element $a^{-1} \in B$ satisfies a monic polynomial equation $a^{-m} = \alpha_1\, a^{1-m} + \cdots + \alpha_{m-1}\, a^{-1} + \alpha_m$ for some $\alpha_\nu \in A$. Multiplication of the both sides by a^{m-1} shows that $a^{-1} = \alpha_1 + \alpha_2 a + \cdots + \alpha_m\, a^{m-1} \in A$.

Conversely, if B is an integral algebra over a field A, then for every $b \in B$, the A-linear span of all nonnegative integer powers b^m is a vector space V of finite dimension over A. If $b \neq 0$, the linear endomorphism $b : V \to V$, $x \mapsto bx$, is injective, because B has no zero divisors. This forces it to be bijective. The preimage of the unit $1 \in V$ is b^{-1}. □

6.3 Normal rings. A commutative ring A without zero divisors is called *normal* if A is integrally closed in its field of fractions Q_A. In particular, every field is normal. The same arguments as in Example 6.1 show that every unique factorization domain A is normal. Indeed, a polynomial $a_0 t^m + a_1 t^{m-1} + \cdots + a_{m-1} t + a_m \in A[t]$ annihilates a fraction $p/q \in Q_A$ with $(p, q) = 1$ only if $q \mid a_0$ and $p \mid a_m$. Therefore, $a_0 = 1$ forces $q = 1$. As a consequence, the polynomial rings over a unique factorization domain are normal. For normal rings, Proposition 6.2 leads to the following classical claim going back to Gauss.

COROLLARY 6.3 (GAUSS LEMMA II)
Let A be a normal ring, Q_A its field of fractions, and $f \in A[x]$ a monic polynomial. If $f = gh$ in $Q_A[x]$ for some monic polynomials g, h, then $f, g \in A[x]$. □

COROLLARY 6.4
Under the conditions of Corollary 6.3, let $B \supset Q_A$ be a ring extending Q_A. If an element $b \in B$ is integral over A, then the minimal polynomial[1] of b over Q_A lies in $A[x]$.

PROOF. Since b is integral over A, there exists a monic polynomial $f \in A[x]$ such that $f(b) = 0$. The minimal polynomial of b over Q_A divides f in $Q_A[x]$, and the quotient is also monic. It remains to apply Corollary 6.3. □

6.4 Algebraic elements. Let B be a commutative algebra with unit over an arbitrary field $\Bbbk$. Given an element $b \in B$, we write $\Bbbk[b] \subset B$ for the smallest $\Bbbk$-subalgebra containing 1 and b. It coincides with the image of evaluation map

$$\mathrm{ev}_b \ : \ \Bbbk[x] \to B\,, \quad f \mapsto f(b)\,. \tag{6-1}$$

Recall that b is said to be *transcendental* over $\Bbbk$ if $\ker \mathrm{ev}_b = 0$. In this case, $\Bbbk[b] \simeq \Bbbk[x]$ is infinite-dimensional as a vector space over $\Bbbk$ and is not a field. If $\ker \mathrm{ev}_b \neq 0$, that is, $f(b) = 0$ for some nonzero polynomial $f \in \Bbbk[x]$, the element b is *algebraic*. In this case, $\ker(\mathrm{ev}_b) = (\mu_b)$ is the principal ideal in $\Bbbk[x]$ generated by the minimal polynomial of b over $\Bbbk$, and $\Bbbk[b] = \Bbbk[x]/(\mu_b)$ has dimension $\deg \mu_b$ as a vector space over $\Bbbk$. This dimension is called the *degree* of b over $\Bbbk$ and denoted by $\deg_{\Bbbk}(b)$. Note that the algebraicity of b over $\Bbbk$ means the same as the integrality, and in this case, every element in $\Bbbk[b]$ is algebraic, and the algebra $\Bbbk[b]$ is a field if and only if it has no zero divisors. This certainly holds if B has no zero divisors. On the other side, $\Bbbk[b]$ has no zero divisors if and only if the minimal polynomial μ_b is irreducible in $\Bbbk[x]$.

6.5 Finitely generated algebras over a field. A commutative $\Bbbk$-algebra B with unit is said to be *finitely generated* if there are some elements $b_1, b_2, \dots, b_m \in B$ such that the evaluation map $\mathrm{ev}_{b_1,b_2,\dots,b_m} : \Bbbk[x_1, x_2, \dots, x_m] \to B$, $x_i \mapsto b_i$ for $i = 1, 2, \dots, m$, is surjective. In this case, $B = \Bbbk[x_1, x_2, \dots, x_m]/I$, where the ideal $I = \ker \mathrm{ev}_{b_1,b_2,\dots,b_m}$ consist of all *polynomial relations* between the *generators*[2] $b_1, b_2, \dots, b_m$ of the algebra B. It follows from the Corollary 6.1 and Exercise 6.3 on p. 72 that all finitely generated commutative $\Bbbk$-algebras are Noetherian, and the ideal of polynomial relations between any set of generators for such an algebra is finitely generated.

THEOREM 6.2
If a finitely generated commutative $\Bbbk$-algebra B is a field, then every element of B is algebraic over $\Bbbk$.

PROOF. Let elements $b_1, b_2, \dots, b_m$ generate B as an algebra over $\Bbbk$. We proceed by induction on m. The case $m = 1$, $B = \Bbbk[b]$, was already considered in n° 6.4. Let $m > 1$. If b_m is algebraic over $\Bbbk$, then $\Bbbk[b_m]$ is a field. By induction, B is algebraic over $\Bbbk[b_m]$, and Proposition 6.1 forces B to be algebraic over $\Bbbk$ as well. Thus, it is enough to check that b_m actually is algebraic over $\Bbbk$.

[1] That is, the monic polynomial $\mu_b \in Q_A[x]$ of minimal positive degree such that $\mu_b(b) = 0$.

[2] Generators of an algebra should be not confused with generators of a module. If elements $e_1, e_2, \dots, e_m$ span a ring B over a subring $A \subset B$ as a module, this means that B consists of finite A-liner combinations of these elements e_i, whereas if $b_1, b_2, \dots, b_m$ span B as an A-algebra, then B is formed by finite linear combinations of various monomials $b_1^{s_1} b_2^{s_2} \dots b_m^{s_m}$.

Assume the contrary. Then the evaluation map (6-1) is injective for $b = b_m$, and is uniquely extended to an embedding of fields $\Bbbk(x) \hookrightarrow B$ by the universal property of the quotient field. Write $\Bbbk(b_m) \subset B$ for the image of this embedding. This is the smallest subfield in B containing b_m. By induction, B is algebraic over $\Bbbk(b_m)$. Therefore, every generator b_i, $1 \leqslant i \leqslant m-1$, is a root of some polynomial with coefficients in $\Bbbk(b_m)$. Multiplying this polynomial by an appropriate polynomial in b_m allows us to assume that all $(m-1)$ polynomials annihilating the generators $b_1, b_2, \dots, b_{m-1}$ have coefficients in $\Bbbk[b_m]$ and share the same leading coefficient, which we denote by $p(b_m) \in \Bbbk[b_m]$. Thus, the field B is integral over the subalgebra $F = \Bbbk[b_m, 1/p(b_m)] \subset B$ spanned over $\Bbbk$ by the elements b_m and $1/p(b_m)$. By the Proposition 6.3, F is a field. This forces p to be of positive degree, because otherwise $F = \Bbbk[b_m]$ is not a field. Now we claim that the element $1+p(b_m)$ has no inverse in F. Indeed, in the contrary case, there exists a polynomial $g \in \Bbbk[x_1, x_2]$ such that $g(b_m, 1/p(b_m)) \cdot (1 + p(b_m)) = 1$. Write the rational function $g(x, 1/p(x))$ as $h(x)/p^k(x)$, where $h \in \Bbbk[x]$ is not divisible by p in $\Bbbk[x]$. Then we get the polynomial relation $h(b_m)\cdot(p(b_m)+1) = p^k(b_m)$ on b_m. It is nontrivial, because the left hand side has positive degree and is not divisible by $p(x)$ in $\Bbbk[x]$. Contradiction. □

COROLLARY 6.5
Let a field $\mathbb{F}$ be finitely generated as an algebra over a subfield $\Bbbk \subset \mathbb{F}$. Then $\mathbb{F}$ has finite dimension as a vector space over $\Bbbk$.

PROOF. If $\mathbb{F}$ is generated as a $\Bbbk$-algebra by algebraic elements $b_1, b_2, \dots, b_m$, then the monomials $b_1^{s_1} b_2^{s_2} \dots b_m^{s_m}$ with $0 \leqslant s_i < \deg_{\Bbbk} b_i$ linearly span $\mathbb{F}$ over $\Bbbk$. □

6.6 Transcendence generators. Everywhere in this section we write A for a finitely generated $\Bbbk$-algebra without zero divisors, and Q_A for its field of fractions. Given a collection of elements $a_1, a_2, \dots, a_m \in A$, we write $\Bbbk(a_1, a_2, \dots, a_m) \subset Q_A$ for the smallest subfield containing all these elements.

Elements $a_1, a_2, \dots, a_m \in A$ are called *algebraically independent* if the evaluation map

$$\mathrm{ev}_{(a_1,a_2,\dots,a_m)} : \Bbbk[x_1, x_2, \dots, x_m] \to A,\ x_i \mapsto a_i,\ 1 \leqslant i \leqslant m,$$

is injective, that is, there are no polynomial relations between $a_1, a_2, \dots, a_m$. In this case the evaluation map is uniquely extended to the isomorphism of fields

$$\Bbbk(x_1, x_2, \dots, x_m) \xrightarrow{\sim} \Bbbk(a_1, a_2, \dots, a_m) \subset Q_A,$$

which maps a rational function of $(x_1, x_2, \dots, x_m)$ to its value at $(a_1, a_2, \dots, a_m)$.

Elements $a_1, a_2, \dots, a_m \in A$ are called *transcendence generators* of A over $\Bbbk$, if any element of A is algebraic over $\Bbbk(a_1, a_2, \dots, a_m)$. In this case the whole field Q_A is also algebraic over $\Bbbk(a_1, a_2, \dots, a_m)$, because the integer closure of $\Bbbk(a_1, a_2, \dots, a_m)$ in Q_A is a field by Proposition 6.3, and Q_A is contained in any field containing A by the universal property of the field of fractions.

An algebraically independent collection $a_1, a_2, \dots, a_m$ of transcendence generators of A over $\Bbbk$ is called a *transcendence basis* of A over $\Bbbk$. Since any proper subset of a transcendence basis is algebraically independent, the transcendence bases can be equivalently characterized as the minimal with respect to inclusions collections of transcendence generators, or as the maximal algebraically independent collections.

Similarly to the bases of vector spaces, any two transcendence bases of A have the same cardinality, and the proof is based on the same Exchange Lemma.

LEMMA 6.3 (EXCHANGE LEMMA)
Let elements $a_1, a_2, \dots, a_m$ be transcendence generators of A over $\Bbbk$, and let $b_1, b_2, \dots, b_n \in A$ be algebraically independent over $\Bbbk$. Then $n \leqslant m$, and after appropriate renumbering of the a_i and replacing the first n of them by $b_1, b_2, \dots, b_n$, the resulting elements $b_1, b_2, \dots, b_n, a_{n+1}, \dots, a_m$ are transcendence generators of A as well.

PROOF. Since b_1 is algebraic over $\Bbbk(a_1, a_2, \dots, a_m)$, there is a polynomial relation

$$f(b_1, a_1, a_2, \dots, a_m) = 0\,, \quad f \in \Bbbk[x_1, x_2, \dots, x_{m+1}]\,.$$

Since b_1 is transcendental over $\Bbbk$, this relation contains some a_i. After appropriate renumbering, we can assume that $i = 1$. Then a_1 and therefore all of Q_A is algebraic over $\Bbbk(b_1, a_2, \dots, a_m)$. Assume by induction that $b_1, \dots, b_k, a_{k+1}, \dots, a_m$ are transcendence generators of A over $\Bbbk$ for $k < n$. Since b_{k+1} is algebraic over $\Bbbk\left(b_1, \dots, b_k, a_{k+1}, \dots, a_m\right)$, there is a polynomial relation

$$f\left(b_1, \dots, b_k, b_{k+1}, a_{k+1}, \dots, a_m\right) = 0\,, \quad f \in \Bbbk[x_1, x_2, \dots, x_{m+1}]\,.$$

It must contain some a_{k+i}, because of algebraic independence of $b_1, b_2, \dots, b_n$ over $\Bbbk$. Hence, $m > k$ and after renumbering of the remaining elements a_i, we can assume that a_{k+1} is algebraic over $\Bbbk\left(b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_m\right)$. Therefore, all of the Q_A is algebraic over this field too. This completes the induction step. □

COROLLARY 6.6
Let A be a finitely generated commutative $\Bbbk$-algebra without zero divisors. Then all transcendence bases of A over $\Bbbk$ have the same cardinality, any system of transcendence generators of A over $\Bbbk$ contains some transcendence basis, and every algebraically independent collection of elements in A can be included in a transcendence basis. □

DEFINITION 6.3
The cardinality of a transcendence basis of a finitely generated commutative $\Bbbk$-algebra A without zero divisors is called the *transcendence degree* of A and denoted $\operatorname{tr\,deg}_{\Bbbk} A$.

EXAMPLE 6.3
Let $A \subset \Bbbk(t)$ be a $\Bbbk$-subalgebra different from $\Bbbk$. Then $\operatorname{tr\,deg}_{\Bbbk} A = 1$. Indeed, for every

$$\psi = f(t)/g(t) \in A \smallsetminus \Bbbk\,,$$

the element t satisfies the algebraic equation $\psi \cdot g(x) - f(x) = 0$ with the coefficients in $\Bbbk(\psi)$. This forces the whole of $\Bbbk(t)$ to be algebraic over $\Bbbk(\psi) \subset \mathbb{Q}_A$ and ψ to be transcendental over $\Bbbk$, because otherwise, t would be algebraic over $\Bbbk$. Thus, any $\psi \in A \smallsetminus \Bbbk$ is a transcendence basis for both A and $\Bbbk(t)$.

6.7 Systems of polynomial equations. Any system of polynomial equations

$$f_\nu(x_1, x_2, \dots, x_n) = 0\,, \quad f_\nu \in \Bbbk[x_1, x_2, \dots, x_n]\,, \tag{6-2}$$

can be extended to a system whose left hand sides form the ideal $J \subset \Bbbk[x_1, x_2, \dots, x_n]$ spanned by the polynomials f_ν from (6-2). The extended infinite system has the same set of solutions in the affine space $\mathbb{A}^n = \operatorname{Aff}(\Bbbk^n)$ as the original system, because the equalities $f_\nu = 0$ imply the equalities $\sum_\nu g_\nu f_\nu = 0$ for all $g_\nu \in \Bbbk[x_1, x_2, \dots, x_n]$. Since the polynomial ring is Noetherian, the

system $f = 0$, $f \in J$, is equivalent to a finite subsystem consisting of equations whose left hand sides generate J. Moreover, by the Lemma 6.1 on p. 71, this finite set of generators can be chosen among the original polynomials f_ν from (6-2). Thus, every (even infinite) system of polynomial equations is always equivalent, on the one hand, to some finite subsystem, and on the other hand, to a system of equations $f = 0$, where f runs through some ideal in $\Bbbk[x_1, x_2, \dots, x_n]$.

Given an ideal $J \subset \Bbbk[x_1, x_2, \dots, x_n]$, its zero set $V(J) \stackrel{\text{def}}{=} \{a \in \mathbb{A}^n \mid f(a) = 0 \ \ \forall f \in J\}$ is called an *affine algebraic variety* determined by J. Note that $V(J)$ may be empty. This happens, for example, if $J = (1) = \Bbbk[x_1, x_2, \dots, x_n]$ contains the equation $1 = 0$.

Associated with an arbitrary subset $\Phi \subset \mathbb{A}^n$ is the ideal

$$I(\Phi) \stackrel{\text{def}}{=} \{ f \in \Bbbk[x_1, x_2, \dots, x_n] \,|\, f(p) = 0 \text{ for all } p \in \Phi \},$$

called the *ideal of* Φ. Its zero set $V(I(\Phi))$ is the smallest affine algebraic variety containing Φ. For every ideal $J \subset \Bbbk[x_1, x_2, \dots, x_n]$ there is the tautological inclusion $J \subset I(V(J))$. In general, it is proper. Say, for $n = 1$, the ideal $J = (x^2) \subset \Bbbk[x]$ determines the variety $V(x^2) = \{0\} \subset \mathbb{A}^1$ whose ideal is $I(V(x^2)) = (x) \supsetneq (x^2)$.

THEOREM 6.3 (HILBERT'S NULLSTELLENSATZ)
Let $\Bbbk$ be an algebraically closed field, $J \subset \Bbbk[x_1, x_2, \dots, x_n]$ an ideal, $\sqrt{J} \stackrel{\text{def}}{=} \{f \mid \exists\, m \in \mathbb{N} : f^m \in J\}$ the *radical* of J. Then $I(V(J)) = \sqrt{J}$ (the *strong Nullstellensatz*). In particular, $V(J) = \varnothing$ if and only if $1 \in J$ (the *week Nullstellensatz*).

PROOF. Let us prove the week Nullstellensatz first. It is enough to show that for any proper ideal $J \subset \Bbbk[x_1, x_2, \dots, x_n]$, there exists a point $p \in \mathbb{A}^n$ such that $f(p) = 0$ for all $f \in J$. Without loss of generality the ideal J can replaced by a *maximal* proper ideal $\mathfrak{m} \supset J$.

EXERCISE 6.6. Convince yourself that an ideal $\mathfrak{m}$ in a commutative ring K is maximal among the proper ideals of K partially ordered by inclusions if and only if the quotient ring $K/\mathfrak{m}$ is a field.

Thus, we can assume that the quotient ring $\Bbbk[x_1, x_2, \dots, x_n]/\mathfrak{m}$ is a field. Since it is finitely generated as a $\Bbbk$-algebra, the Theorem 6.2 forces every element $\vartheta \in \Bbbk[x_1, x_2, \dots, x_n]/\mathfrak{m}$ to be algebraic over $\Bbbk$, that is, to satisfy an equation $\mu(\vartheta) = 0$ for a monic irreducible polynomial $\mu \in \Bbbk[t]$. Since $\Bbbk$ is algebraically closed, the polynomial μ has to be linear, and therefore, $\vartheta \in \Bbbk$. In other words, every polynomial is congruent modulo $\mathfrak{m}$ to a constant. Write $p_i \in \Bbbk$ for the constant congruent to x_i. Then the factorization homomorphism $\Bbbk[x_1, x_2, \dots, x_n] \to \Bbbk[x_1, x_2, \dots, x_n]/\mathfrak{m} \simeq \Bbbk$ maps every polynomial $f(x_1, x_2, \dots, x_n)$ to the class of constant $f(p_1, p_2, \dots, p_n) \in \Bbbk$. Since all $f \in \mathfrak{m}$ are mapped to zero, they all vanish at $p = (p_1, p_2, \dots, p_n) \in \mathbb{A}^n$, as desired.

The strong Nullstellensatz is trivial for $V(J) = \varnothing$. Assume that $V(J) \neq \varnothing$, that is, $J \neq (1)$. Consider $\mathbb{A}^n$ as the hyperplane $t = 0$ in the affine space $\mathbb{A}^{n+1}$ with the coordinates

$$(t, x_1, x_2, \dots, x_n).$$

If a polynomial $f \in \Bbbk[x_1, x_2, \dots, x_n] \subset \Bbbk[t, x_1, x_2, \dots, x_n]$ vanishes everywhere on the cylinder $V(J) \subset \mathbb{A}^{n+1}$, then the polynomial $g(t, x) = 1 - t\,f(x)$ equals 1 at every point of $V(J)$. Therefore, the ideal spanned in $\Bbbk[t, x_1, x_2, \dots, x_n]$ by J and $g(t, x)$ has the empty zero set in $\mathbb{A}^{n+1}$. By the week Nullstellensatz, this ideal contains 1, i.e., there exist $q_0, q_1, \dots, q_s \in \Bbbk[t, x_1, x_2, \dots, x_n]$ and $f_1, f_2, \dots, f_s \in J$ such that $q_0(x, t) \cdot \big(1 - tf(x)\big) + q_1(t, x) \cdot f_1(x) + \cdots + q_s(x, t) \cdot f_s(x) = 1$. The

homomorphism $\Bbbk[t, x_1, x_2, \dots, x_n] \to \Bbbk(x_1, x_2, \dots, x_n)$ acting on the variables as $t \mapsto 1/f(x)$, $x_\nu \mapsto x_\nu$ for $1 \leqslant \nu \leqslant n$, maps this equality to the equality

$$q_1\big(1/f(x), x\big) \cdot f_1(x) + \cdots + q_s\big(1/f(x), x\big) \cdot f_s(x) = 1\,. \tag{6-3}$$

in the field $\Bbbk(x_1, x_2, \dots, x_n)$. Since $1 \notin J$, some $q_\nu\big(1/f(x), x\big)$ have nontrivial denominators. All these denominators are canceled via multiplication by f^m for some $m \in \mathbb{N}$. Multiplying both sides by this f^m leads to the required equality $f^m(x) = \widetilde{q}_1(x) \cdot f_1(x) + \cdots + \widetilde{q}_s(x) \cdot f_s(x)$ with $\widetilde{q}_\nu \in \Bbbk[x_1, x_2, \dots, x_n]$. □

6.8 Resultants. Given a system of homogeneous polynomial equations

$$\begin{cases} f_1(x_0, x_1, \dots, x_n) = 0 \\ f_2(x_0, x_1, \dots, x_n) = 0 \\ \qquad \dots\dots\dots\dots\dots\dots \\ f_m(x_0, x_1, \dots, x_n) = 0\,, \end{cases} \tag{6-4}$$

where every $f_i \in \Bbbk[x_0, x_1, \dots, x_n]$ is homogeneous of degree d_i, the set of its solutions, considered up to proportionality, is the intersection of m projective hypersurfaces $S_i = V(f_i) \subset \mathbb{P}(V)$, where $V = \Bbbk^{n+1}$. The projective hypersurfaces of degree d in $\mathbb{P}(V)$ can be viewed as points of the projective space $\mathbb{P}(S^d V^*)$. All collections of hypersurfaces $(S_1, S_2, \dots, S_m)$ of given degrees $d_1, d_2, \dots, d_m$ with nonempty intersection $\bigcap_i S_i \neq \varnothing$ form the figure

$$\mathcal{R}(n+1;\, d_1, d_2, \dots, d_m) \subset \mathbb{P}(S^{d_1}V^*) \times \mathbb{P}(S^{d_2}V^*) \times \cdots \times \mathbb{P}(S^{d_m}V^*)\,, \tag{6-5}$$

called the *resultant variety* of the homogeneous system (6-4). When $m = n+1$ and all $d_i = 1$, the system (6-4) becomes the system of linear equations $Ax = 0$ with the square matrix $A = \big(a_{ij}\big)$. It has a nonzero solution if and only if $\det\big(a_{ij}\big) = 0$. Thus, in this simplest case, the resultant variety is a projective variety determined by one multilinear equation of total degree $n+1$ on the coefficients $a_{i,j}$. We are going to check that the resultant variety (6-5) can always be described by a system of polynomial equations in the coefficients of the polynomials f_i. This system is called a *resultant system*. It depends only on the number of variables and the collection of degrees $d_1, d_2, \dots, d_m$. Every resultant equation is homogeneous in the coefficients of each polynomial.

Write $J = (f_1, f_2, \dots, f_m) \subset \Bbbk[x_0, x_1, \dots, x_n]$ for the ideal spanned by the polynomials (6-4). If $V(J)$ is exhausted by the origin, then every coordinate linear form x_i vanishes on $V(J)$, and therefore, all $x_i^m \in J$ for some $m \in \mathbb{N}$ by the strong Nullstellensatz. This forces J to contain all homogeneous polynomials of degree $d > (m-1)(n+1)$. Conversely, if $J \supset S^d V^*$ for all $d \gg 0$, then the system (6-4) implies the equations $x_0^d = x_1^d = \cdots = x_n^d = 0$, and therefore, has only the zero solution. For any $d \in \mathbb{N}$, the intersection $J \cap S^d V^*$ coincides with the image of $\Bbbk$-linear map

$$\mu_d : S^{d-d_1}V^* \oplus S^{d-d_2}V^* \oplus \cdots \oplus S^{d-d_m}V^* \xrightarrow{(g_0, g_1, \dots, g_n) \mapsto \sum g_\nu f_\nu} S^d\,. \tag{6-6}$$

The matrix of this map in the standard monomial bases consists of zeros and the coefficients of polynomials f_ν. For $d \gg 0$, the dimension of the left hand side in (6-6) grows as

$$\sum_{\nu=1}^{m} \binom{n+d-d_\nu}{n} \sim \frac{m}{n!}\, d^n$$

and becomes greater that the dimension of the right hand side, which grows as

$$\binom{n+d}{n} \sim \frac{1}{n!}\, d^n .$$

Thus, for every $d \gg 0$, the condition $S^d V^* \not\subset J$, that is, the non-surjectivity of the map (6-6), means that the rank of the matrix of μ_d is not maximal. This is equivalent to the vanishing of all minors of the maximal degree in the matrix. Thus, the resultant variety is the zero set of all these minors written for all d such that the dimension of the left hand side of (6-6) is not less than that of the right han side. Since the polynomial ring is Noetherian, this huge system of equations is equivalent to some finite subsystem. If the ideal of the resultant variety (6-5) is not principal, such a system of resultants is not unique in general.

EXAMPLE 6.4 (RESULTANT OF TWO BINARY FORMS)
Let the ground field $\Bbbk$ be algebraically closed. Then every homogeneous binary form of degree d

$$f(t_0, t_1) = a_0\, t_1^d + a_1\, t_0\, t_1^{d-1} + a_2\, t_0^2\, t_1^{d-2} + \cdots + a_{d-1}\, t_0^{d-1}\, t_1 + a_d\, t_0^d$$

has d roots $\alpha_1, \alpha_2, \ldots, \alpha_d$, $\alpha_i = (\alpha_i' : \alpha_i'')$, on $\mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ and is factorized as

$$f(t_0, t_1) = \prod_{i=0}^{d} (\alpha_i'' t_0 - \alpha_i' t_1) = \prod_{i=0}^{d} \det \begin{pmatrix} t_0 & t_1 \\ \alpha_i' & \alpha_i'' \end{pmatrix}$$

The coefficients of f are expressed as the homogeneous polynomials in the roots by means of the *homogeneous Viète's formulas*: $a_k = (-1)^{d-k} \sigma_k(\alpha', \alpha'')$, where

$$\sigma_k(\alpha', \alpha'') = \sum_{\#I = k} \Bigl(\prod_{i \in I} \alpha_i' \cdot \prod_{j \notin I} \alpha_j'' \Bigr)$$

and I runs through the strictly increasing sequences of k indexes. In particular, a_k is bihomogeneous of bidegree $(k, d-k)$ in (α', α''). Let us fix two degrees $r, s \in \mathbb{N}$ and consider the polynomial ring $\Bbbk[\alpha', \alpha'', \beta', \beta'']$ in four collections of variables

$$\begin{aligned} \alpha' &= (\alpha_1', \alpha_2', \ldots, \alpha_s') \quad & \alpha'' &= (\alpha_1'', \alpha_2'', \ldots, \alpha_s'') \\ \beta' &= (\beta_1', \beta_2', \ldots, \beta_r') \quad & \beta'' &= (\beta_1'', \beta_2'', \ldots, \beta_r'') . \end{aligned}$$

Within this ring, consider the product

$$R \stackrel{\text{def}}{=} \prod_{i,j} \Bigl(\alpha_i' \beta_j'' - \alpha_i'' \beta_j' \Bigr) = \prod_{j=1}^{s} f(\beta_j) = (-1)^{rs} \prod_{i=1}^{r} g(\alpha_i) .$$

The polynomial R is bihomogeneous of bidigree (rs, rs) in (α, β). It is evaluated to zero at the roots α, β of binary forms $f(t_0, t_1) = \sum_{i=0}^{s} a_i\, t_0^i\, t_1^{n-i}$, $g(t_0, t_1) = \sum_{j=0}^{r} b_j\, t_0^j\, t_1^{m-j}$ if and only if these forms have a common root in $\mathbb{P}_1$. Let us show that R is expressed as a polynomial R_{fg} in the coefficients $a_i = (-1)^{n-i} \sigma_i(\alpha', \alpha'')$, $b_j = (-1)^{m-j} \sigma_j(\beta', \beta'')$ of f, g by the following *Sylvester*

formula

$$R_{fg} = \det \underbrace{\left(\begin{array}{ccccccccc} a_0 & a_1 & \cdots & \cdots & a_s & & & & \\ & a_0 & a_1 & \cdots & \cdots & a_s & & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & & \\ & & & a_0 & a_1 & \cdots & \cdots & a_s & \\ b_0 & b_1 & \cdots & \cdots & b_r & & & & \\ & b_0 & b_1 & \cdots & \cdots & b_r & & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & & \\ & & & b_0 & b_1 & \cdots & \cdots & b_r & \end{array} \right)}_{r+s} \begin{matrix} \} r \\ \\ \\ \\ \} s \\ \\ \\ \\ \end{matrix} \tag{6-7}$$

where the matrix in the right hand side is transposed to the matrix of the linear map (6-6) written for $n = 1$, $m = 2$, and $d = s + r - 1$ in the standard monomial bases, when it turns to

$$\mu_{s+r-1} : S^{r-1}V^* \oplus S^{s-1}V^* \to S^{s+r-1}V^*, \quad (h_1, h_2) \mapsto fh_1 + gh_2, \quad \dim V = 2,$$

and the both sides are of equal dimension $r + s$.

EXERCISE 6.7. Verify this carefully.

Write $S = S(\alpha', \alpha'', \beta', \beta'') \in \Bbbk[\alpha', \alpha'', \beta', \beta'']$ for the Sylvester determinant from the right hand side of (6-7), and put $D_{ij} = \alpha'_i\beta''_j - \alpha''_i\beta'_j$. For every point $(\alpha, \beta) \in V(D_{ij})$, we have the equality $(\alpha''_i t_0 - \alpha'_i t_1) = (\beta''_i t_0 - \beta'_i t_1)$ up to a constant factor, and this linear form divides $f(t)$, $g(t)$, and all polynomials $f(t)h_1(t) + g(t)h_2(t)$ in $\Bbbk[t_0, t_1]$. Hence, $\operatorname{im}\mu_{r+s-1} \neq S^{r+s-1}V^*$, and therefore, $S(\alpha, \beta) = 0$. Thus, S vanishes identically on $V(D_{ij})$. By the strong Nullstellensatz, some power of S is divisible by D_{ij}. Since D_{ij} is irreducible and the polynomial ring $\Bbbk[\alpha', \alpha'', \beta', \beta'']$ is factorial, D_{ij} divides S, and therefore, S is divisible by the product R_{fg} of all D_{ij}. Comparison of the degrees and coefficients of the lexicographically maximal monomials in S and R_{fg} shows that these two polynomials must be equal.

We conclude that the resultant variety (6-5) for a pair of binary forms f, g of degrees s, r is the hypersurface[1] in $\mathbb{P}_s \times \mathbb{P}_r$ determined by one equation $R_{fg} = 0$ on the coefficients of f, g. The polynomial $R_{f,g}$ is called the *resultant* of f, g. For $t_0 = 1$, $t_1 = x$, it is specialized to the resultant $R_{f_{\text{aff}},g_{\text{aff}}}$ of two non-homogeneous polynomials $f_{\text{aff}}(x) = f(1, x)$, $g_{\text{aff}}(x) = g(1, x)$ in one variable x. Under the assumption that[2] $a_0 b_0 \neq 0$, the resultant $R_{f_{\text{aff}},g_{\text{aff}}}$ vanishes if and only if the polynomials f_{aff}, g_{aff} have a common root in $\Bbbk$.

[1] In Example 9.1 on p. 112, we will see that the same holds for any system of homogeneous polynomial equations in which the number of equations equals the number of unknowns.

[2] It says that both binary forms f, g do not vanish at the point $(0 : 1)$, the infinity of the affine chart U_0 in which the coordinate x is defined.

Comments to some exercises

EXRC. 6.1. Let polynomials $f(x), g(x) \in I$ have degrees $m \geqslant n$ and leading coefficients a, b. Then $a + b$ equals either zero or the leading coefficient of polynomial $f(x) + x^{m-n} \cdot g(x) \in I$ of degree m. Similarly, for every $\alpha \in K$ the product αa either is zero or equals the leading coefficient of polynomial $\alpha f(x) \in I$ of degree m.

EXRC. 6.2. Repeat the arguments proving Theorem 6.1 on p. 71 but cancel non-zero monomials of the lowest degree instead of the leading.

EXRC. 6.3. Let $\pi : A \twoheadrightarrow B$ be the quotient epimorphism. The complete preimage $\pi^{-1}(I)$ of every ideal $I \subset B$ is an ideal in A, and therefore, it is generated by a finite set of element. Their images under π generate I.

EXRC. 6.4. Begin with $f_0 = z \sin(2\pi i z)$.

EXRC. 6.5. It is enough to construct such extension for just one monic irreducible polynomial $f \in B[x]$ of positive degree. If $\deg f = 1$, put $C = B$. Then use induction on $\deg f$. The quotient ring $D = B[x]/(f)$ contains B as the subring formed by residue classes of the constants. Write $\vartheta \in D$ for the residue class of x. Then $f(\vartheta) = 0$ and therefore, f is divisible by $(x - \vartheta)$ in $D[x]$, that is, becomes a product of irreducible monic polynomials of smaller degree in $D[x]$.

EXRC. 6.6. An element $a \in K \setminus \mathfrak{m}$ is invertible in $K/\mathfrak{m}$ if and only if $1 \in (a, \mathfrak{m})$.