Commutative algebra draught

NOETHERIAN RINGS. We write $(f_1, f_2, \dots, f_m)$ for the ideal $\{g_1 f_1 + g_2 f_2 + \dots + g_m f_m \mid g_\nu \in A\}$ spanned (as A-module) by $\{f_1, f_2, \dots, f_m\} \subset A$. A commutative ring A is called *Noetherian*, if it satisfies the next lemma:

Lemma 1.1. *The following properties of a commutative ring A are mutually equivalent*

1) *any set of elements f_ν contains some finite subset that generates the same ideal as the initial set;*
2) *any ideal admits a finite set of generators;*
3) *for any infinite chain of embedded ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ there exists $n \in \mathbb{N}$ such that $I_\nu = I_n \quad \forall\, \nu \geqslant n$.*

Proof. Clearly, (1) $\Rightarrow$ (2). To deduce (3) from (2), take a finite set of generators for the ideal $I = \bigcup I_\nu$; since they belong to some I_n, we have $I_\nu = I_n = I \ \forall\ \nu \geqslant n$. Finally, (1) follows from (3) applied to the chain $I_n = (f_1, f_2, \dots, f_n)$, where f_i are chosen from $\{f_\nu\}$ in order to have $f_\nu \notin (f_1, f_2, \dots, f_{\nu-1})$. □

Theorem 1.2. (Hilbert's base theorem). *If A is Noetherian, then $A[x]$ is Noetherian too.*

Proof. Let $I \subset A[x]$ be an ideal. We write $L_d \subset A$ for a set of leading coefficients of all degree d polynomials in I. Clearly, each L_d and $L_\infty \stackrel{\text{def}}{=} \bigcup_d L_d$ are ideals in A. Let L_∞ be generated by $a_1, a_2, \dots, a_s \in A$ coming from $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{s_\infty}^{(\infty)} \in I$ and let $\max_\nu(\deg f_\nu) = m$. Similarly, write $f_1^{(k)}, f_2^{(k)}, \dots, f_{s_k}^{(k)}$ for the polynomials whose leading coefficients span the ideal L_k for $0 \leqslant k \leqslant m-1$. To finish the proof, make: □

Exercice 1.3. Show that I is spanned by $s_0 + \dots + s_{m-1} + s_\infty$ polynomials $f_\nu^{(\mu)}$ just constructed.

Corollary 1.4. *A polynomial ring $A[x_1, x_2, \dots, x_n]$ over a Noetherian ring A is Noetherian as well.* □

Corollary 1.5. *Any finitely generated k-algebra is Noetherian for any field k.*

Proof. A polynomial algebra $k[x_1, x_2, \dots, x_n]$ is Noetherian by the previous corollary. Any its factor algebra A is Noetherian as well: full preimage of any ideal $I \subset A$ under the factorizing morphism $k[x_1, x_2, \dots, x_n] \twoheadrightarrow A$ is an ideal in $k[x_1, x_2, \dots, x_n]$, i. e. admits a finite set of generators, whose classes span I over A, certainly. □

INTEGRALITY. Let $A \subset B$ be two commutative rings. An element $b \in B$ is called *integer* over A, if it satisfies the conditions from Lemma 1.6 below. If all $b \in B$ are integer over A, then B is called an *integer extension* of A or an *integer A-algebra*.

Lemma 1.6. *The following properties of an element $b \in B$ are pairwise equivalent:*

1) *$b^m = a_1 b^{m-1} + \dots + a_{m-1} b + a_0$ for some $m \in \mathbb{N}$ and some $a_1, a_2, \dots, a_m \in A$;*
2) *A-module spanned by all nonnegative powers $\{b^i\}_{i \geqslant 0}$ admits a finite set of generators;*
3) *there exist a finitely generated faithful[1] A-submodule $M \subset B$ such that $bM \subset M$.*

Proof. The implications (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) are trivial. To deduce (1) from (3), let $\{e_1, e_2, \dots, e_m\}$ generate M over A and let the multiplication $M \xrightarrow{m \mapsto bm} M$ be presented by a matrix Y, i. e. write $(be_1, be_2, \dots, be_m) = (e_1, e_2, \dots, e_m) \cdot Y$.

Note that if A-linear map $M \xrightarrow{\varkappa} M$ takes $(e_1, e_2, \dots, e_m) \longmapsto (e_1, e_2, \dots, e_m) \cdot X$, where X is a square matrix with entries in A, then there is an inclusion $(\det X) \cdot M \subset \operatorname{im} \varkappa$, which follows from the Laplace identity $\det X \cdot \mathrm{Id} = \widehat{X} \cdot X$ applied to $(e_1, e_2, \dots, e_m)$.

In our case the zero operator $M \xrightarrow{\varkappa} 0$ can be presented by the matrix $X = b \cdot \mathrm{Id} - Y$. So, the multiplication by $\det(b \cdot \mathrm{Id} - Y)$ annihilates M. Since M is faithful, $\det(b \cdot \mathrm{Id} - Y) = 0$. This is a polynomial equation on b with the coefficients in A and the leading term b^n as required in (1). □

Example 1.7: Integer algebraic numbers. Let $K \supset \mathbb{Q}$ be a finite dimensional[2] field extension; then elements $z \in K$ are called *algebraic numbers*. Such a number z is integer over $\mathbb{Z}$ iff there are some $\vartheta_1, \vartheta_2, \dots, \vartheta_m \in K$ such that the multiplication by z sends their $\mathbb{Q}$-linear span to itself and is presented there by a matrix whose entries belong to $\mathbb{Z}$.

Example 1.8: Invariants of a finite group action. Let a finite group $\mathfrak{G}$ act on a k-algebra B via k-algebra automorphisms $B \xrightarrow{g} B$, $g \in \mathfrak{G}$, and let $A = B^{\mathfrak{G}} = \{a \in B \mid ga = a \ \ \forall\, g \in \mathfrak{G}\}$ be the subalgebra of $\mathfrak{G}$-invariants. Then B is an integer extension of A. Indeed, if $b_1, b_2, \dots, b_s \in B$ form a $\mathfrak{G}$-orbit of any given $b = b_1 \in B$, then the polynomial $\beta(t) = \prod (t - b_i)$ is monic[3], lies in $A[t]$, and annihilates b.

[1] A-module M is called *faithful*, if $aM = 0$ implies $a = 0$ for $a \in A$

[2] as a vector space over $\mathbb{Q}$

[3] a polynomial is called *monic* or *unitary*, if its leading coefficient equals 1

INTEGER CLOSURES. A set of all $b \in B$ that are integer over a subring $A \subset B$ is called *an integer closure* of A in B. If this closure coincides with A, then A is called *integrally closed* in B.

Lemma 1.9. *The integer closure of A is a subring in B (in particular, ab is integer for any $a \in A$ as soon as b is integer). If $C \supset B$ is an other commutative ring and $c \in C$ is integer over an integer closure of A in B, then c is integer over A as well (in particular, any integer B-algebra is an integer A-algebra as soon as B is an integer A-algebra).*

Proof. If $p^m = x_{m-1}\, p^{m-1} + \cdots + x_1\, p + x_0$, $q^n = y_{n-1}\, q^{n-1} + \cdots + y_1\, q + y_0$ for $p, q \in B$, $x_\nu, y_\mu \in A$, then A-module spanned by $p^i q^j$ with $0 \leqslant i \leqslant (m-1)$, $0 \leqslant j \leqslant (n-1)$ is faithful (it contains 1) and goes to itself under the multiplication by both $p+q$ and pq. Similarly, if $c^r = z_{r-1}\, c^{r-1} + \cdots + z_1\, c + z_0$ and all z_ν are integer over A, then a multiplication by c preserves a faithful A-module spanned by a sufficient number of products $c^i z_1^{j_1} z_2^{j_2} \cdots z_r^{j_r}$. □

Corollary 1.10. [4] *For any two commutative rings $A \subset B$ let $f(x), g(x) \in B[x]$ be two monic polynomials. Then all coefficients of $h(x) = f(x)g(x)$ are integer over A iff all coefficients of both $f(x)$, $g(x)$ are integer over A.*

Proof. There exists[5] a ring $C \supset B$ such that $f(x) = \prod(t - \alpha_\nu)$ and $g(x) = \prod(t - \beta_\mu)$ in $C[x]$ for some $\alpha_\nu, \beta_\mu \in C$. By Lemma 1.9, all coefficients of $h(x) = \prod(t - \alpha_\nu) \prod(t - \beta_\mu)$ are integer over $A \iff$ all α_ν, β_μ are integer over $A \iff$ all coefficients of $f(x)$ and $g(x)$ are integer over A. □

Lemma 1.11. *Let $B \supset A$ be integer over A. If B is a field, then A is a field. Vise versa, if A is a field and there are no zero divisors in B, then B is a field.*

Proof. If B is a field integer over A, then any non zero $a \in A$ has an inverse $a^{-1} \in B$, which satisfy an equation $a^{-m} = \alpha_1\, a^{1-m} + \cdots + \alpha_{m-1}\, a^{-1} + \alpha_0$ with $\alpha_\nu \in A$. We multiply the both sides by a^{m-1} and get $a^{-1} = \alpha_1 + \cdots + \alpha_{m-1}\, a^{m-2} + \alpha_0\, a^{m-1} \in A$. Conversely, if A is a field and B is an integer A-algebra, then all non negative integer powers b^i of any $b \in B$ form a finite dimensional vector space V over A. If $b \neq 0$ and there are no zero divisors in B, then $x \longmapsto bx$ is an injective linear operator on V, that is, an isomorphism. A preimage of $1 \in V$ is b^{-1}. □

Example 1.12: algebraic elements and minimal polynomials. If $A = k$ is a field and $B \supset k$ is a k-algebra, then $b \in B$ is integer over k iff b satisfy a polynomial equation $f(b) = 0$ for some $f \in k[x]$. Traditionally, such b is called *algebraic* over k rather than *integer*. We write $k[b]$ for a k-linear span of nonnegative integer powers $\{b^n\}_{n \geqslant 0}$ and $k(b)$ for a k-linear span of all integer powers $\{b^n\}_{n \in \mathbb{Z}}$ (if such exist in B). Clearly, $k[b] \subset B$ is the minimal k-subalgebra containing 1 and b; in other terms, $k[b] = \operatorname{im}(\mathrm{ev}_b) = k[x]/\ker(\mathrm{ev}_b)$, where $\mathrm{ev}_b : k[x] \xrightarrow{f(x) \mapsto f(b)} B$ is *an evaluation homomorphism*. If b is algebraic, then $\ker(\mathrm{ev}_b) = (f) \stackrel{\text{def}}{=} f \cdot k[x]$ for some $0 \neq f \in k[x]$, because $k[x]$ is a principal ideal domain. This f is fixed uniquely as a monic polynomial of lowest degree such that $f(b) = 0$; it is called *the minimal polynomial* of b over k. Note that $k[b]$ is a $\deg(f)$-dimensional vector space over k with a basis $1, b, b^2, \ldots, b^{\deg(f)-1}$. If B does not have zero divisors, then $k[b]$ is a field by Lemma 1.11; in particular, the minimal polynomial of b is irreducible in this case. If b is not algebraic, then $\ker(\mathrm{ev}_b) = 0$ and $k[b] \simeq k[x]$ is a polynomial ring. In particular, it is an infinite dimensional vector space over k and it is not a field. This phenomenon will be generalized in Lemma 1.17 below.

Lemma 1.13. *Let $k = Q(A)$ be the fraction field for a commutative ring A without zero divisors, B be any k-algebra, and $b \in B$ be algebraic over k with minimal polynomial $f \in k[x]$. If b is integer over A, then all coefficients of f are integer over A.*

Proof. Since b is integer, $g(q) = 0$ for some monic $g \in A[x]$. Then $g = fh$ in $k[x]$ for some monic $h \in k[x]$ and all the coefficients of g, h are integer over A by Corollary 1.10. □

NORMAL RINGS. A commutative ring A without zero divisors is called *normal*, if there are no $b \in Q(A) \setminus A$ integer over A. Certainly, any field is normal.

Exercice 1.14. Show that the ring $\mathbb{Z}$ is normal.

HINT. A polynomial $a_0 t^m + a_1 t^{m-1} + \cdots + a_{m-1} t + a_m \in \mathbb{Z}[t]$ annihilates a fraction $p/q \in \mathbb{Q}$ with coprime $p, q \in \mathbb{Z}$ only if $q | a_0$ and $p | a_m$

Corollary 1.15. *Let A be a normal ring and $f \in A[x]$ be factorized in $Q(A)[x]$ as $f = g\,h$. If both g, h are monic, then necessarily $g, h \in A[x]$.*

Proof. Indeed, all the coefficients of g, h are integer over A by Corollary 1.10. □

Corollary 1.16. *Let A be normal ring with the fraction field $k = Q(A)$ and B be any k-algebra. Then $b \in B$ is integer over A iff it is algebraic over k and its minimal polynomial (over k) lies in $A[x]$.*

Proof. This follows immediately from Lemma 1.13. □

[4] it is known as Gauss - Kronecker - Dedekind lemma

[5] For any commutative ring A and any monic non constant $f(x) \in A[x]$ there exists a commutative ring $C \supset A$ such that $f(x) = \prod(x - c_\nu)$ in $C[x]$ for some $c_\nu \in C$. It is constructed inductively as follows. Consider a factor ring $B = A[x]/(f)$ (which contains A as the congruence classes of constants) and put $b \stackrel{\text{def}}{=} x \pmod f \in B$. Then $f(b) = 0$ in $B[x]$. Hence the residue after dividing $f(x)$ by $(x - b)$ in $B[x]$ vanishes and we get the factorization $f(x) = (x - b)h(x)$ with $h(x) \in B[x]$. Now repeat the procedure for h, B instead of f, A e. t. c.

FINITELY GENERATED COMMUTATIVE k-ALGEBRAS. Let k be any field. A commutative k-algebra B is called *finitely generated*, if there is a k-algebra epimorphism $k[x_1, x_2, \dots, x_m] \xrightarrow{\pi} B$. Images $b_i = \pi(x_i) \in B$ are called *algebra generators* for B over k.

Lemma 1.17. *A finitely generated k-algebra B is a field only if each $b \in B$ is algebraic over k.*

Proof. Let B be generated by $\{b_1, b_2, \dots, b_m\}$. We use induction over m. The base case: $m = 1$, $B = k[b]$, was considered in Example 1.12. Let $m > 1$. If b_m is algebraic over k, then $k[b_m]$ is a field and B is algebraic over $k[b_m]$ by the inductive assumption. Hence, by Lemma 1.9, B is algebraic over k as well.

So, we only have to show that b_m *must* be algebraic over k. Suppose the contrary: let b_m be not algebraic, that is $k(b_m)$ be isomorphic to the field $k(x)$, of rational functions in 1 variable, via sending $b_m \longmapsto x$. Then, by the inductive assumption, B is algebraic over $k(b_m)$ and each of $b_1, b_2, \dots, b_{m-1}$ satisfies a polynomial equation with coefficients in $k(b_m)$. Multiplying these equations by appropriate polynomials in b_m, we can put their coefficients into $k[b_m]$ and make all their leading coefficients to be equal to the same polynomial, which we denote by $p(b_m) \in k[b_m]$.

Now, B is integer over the subalgebra $F \subset B$ generated over k by b_m and $q = 1/p(b_m)$. By Lemma 1.11, F is a field. So, there exists a polynomial $g \in k[x_1, x_2]$ such that $g(b_m, q)$ is inverse to $1 + q$ in F. Let us write the rational function $g(x\,,\, 1/p(x)) \in k(x)$ as $h(x)/p^k(x)$, where $h \in k[x]$ is coprime to $p \in k[x]$. Multiplying the both sides of

$$\left(1 + \frac{1}{p(b_m)}\right) \frac{h(b_m)}{p^k(b_m)} = 1$$

by $p^{k+1}(b_m)$, we get for b_m a polynomial equation $h(b_m)\,(p(b_m)+1) = p^{k+1}(b_m)$, which is nontrivial, because $h(x)(1+p(x))$ is not divisible by $p(x)$. Hence, b_m should be algebraic over k. □

HILBERT'S NULLSTELLENSATZ. Let us write $V(I) = \{a \in \mathbb{A}_n \mid f(a) = 0 \quad \forall\, f \in I\ \} \subset \mathbb{A}^n$ for affine algebraic variety defined by a system of polynomial equations[6] $I \subset k[x_1, x_2, \dots, x_n]$. Vise versa, for any subset $V \subset \mathbb{A}^n$ we write $I(V) = \{f \in k[x_1, x_2, \dots, x_n] \mid f|_V \equiv 0\}$ for a set of all polynomials vanishing along V. Clearly, $I(V)$ is always an ideal and $I(V(I)) \supset I$ for any ideal I. In general, then last inclusion is proper. For example, if $I = (x^2) \in \mathbb{C}[x]$, then $V(I) = \{0\} \subset \mathbb{A}^1(\mathbb{C})$ and $I(V(I)) = (x)$.

Theorem 1.18. (week Nullstellensatz). *If k is algebraically closed, then $V(I) = \varnothing \iff 1 \in I$ for an ideal I.*

Proof. We only have to find a point $p \in \mathbb{A}_n$ such that $f(p) = 0$ for any polynomial f from a given proper ideal $I \subset k[x_1, x_2, \dots, x_n]$. Moreover, it is enough to suppose that I is *maximal*, that is, any $f \notin I$ is invertible modulo I. Indeed, otherwise an ideal J generated by f and I would be proper and strictly larger than I, i. e. we could replace I by J; a finite chain of such replacements leads to some maximal ideal. As soon as I is maximal, the factor algebra $K = k[x_1, x_2, \dots, x_n]/I$ is a field. Hence, any element of K is algebraic over $k \subset K$ by Lemma 1.17. Since k is algebraically closed, this means that any polynomial is (mod I)-congruent to some constant. Let $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ be the constants presenting the basic linear forms $x_1, x_2, \dots, x_n \pmod I$. Then any polynomial $f \in k[x_1, x_2, \dots, x_n]$ is (mod I) congruent to $f(\vartheta_1, \vartheta_2, \dots, \vartheta_n) \in k$. In particular, $f(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = 0$ for any $f \in I$ as required. □

Corollary 1.19. (strong Nullstellensatz). *Under conditions of Theorem 1.18, $f \in I(V(I)) \iff \exists\, k \in \mathbb{N} : f^k \in I$.*

Proof. Only the implication '$\Rightarrow$' for *nonempty* $V(I) \subset \mathbb{A}^n$ is nontrivial. To prove it, we identify $\mathbb{A}^n$ with the hyperplane $t = 0$ in $\mathbb{A}^{n+1}$ coordinated by $(t,\ x_1, x_2, \dots, x_n\ )$. If $f \in k[x_1, x_2, \dots, x_n] \subset k[t,\ x_1, x_2, \dots, x_n\ ]$ vanishes along $V(I)$, then an ideal $J \subset k[t,\ x_1, x_2, \dots, x_n\ ]$ spanned by I and a polynomial $g(t, x) = 1 - t\,f(x)$ has empty zero set $V(J) \subset \mathbb{A}^{n+1}$, because of $g(x, t) \equiv 1$ on $V(I)$. So, $1 \in J$, i. e. $\exists\quad q_0, q_1, \dots, q_s\ \subset k[t,\ x_1, x_2, \dots, x_n\ ],\quad f_1, f_2, \dots, f_s\ \subset I$: $q_0(x,t)(1-tf(x)) + q_1(t,x)f_1(x) + \dots + q_s(x,t)f_s(x) = 1$. Then a homomorphism $k[t,\ x_1, x_2, \dots, x_n] \longrightarrow k(x_1, x_2, \dots, x_n)$ sending $t \longmapsto 1/f(x)$, $x_\nu \longmapsto x_\nu$ takes this equality to $q_1(1/f(x)\,,\, x)\, f_1(x) + \dots + q_s(1/f(x)\,,\, x)\, f_s(x) = 1$. Since I is proper, some of $q_\nu(1/f(x), x)$ should have nontrivial denominators. Hence, multiplication by appropriate power f^k leads to an expression we are looking for: $\widetilde{q}_1(x)\, f_1(x) + \dots + \widetilde{q}_s(x)\, f_s(x) = f^k(x)$, where $\widetilde{q}_\nu \in k[x_1, x_2, \dots, x_n]$. □

[6] certainly, we can always extend I to an ideal spanned by I — this does not effect on $V(I)$