Commutative algebra draught.

INTEGRALITY. Let $A \subset B$ be two commutative rings. An element $b \in B$ is called *integer* over A if it satisfy the conditions of the lemma below.

Lemma 21.1 *For any two commutative rings $A \subset B$ the following properties of a given $b \in B$ are pairwise equivalent:*

1. $b^m = a_1 b^{m-1} + \cdots + a_{m-1} b + a_0$ *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 faceful*[1] *A-submodule* $M \subset B$ *such that* $bM \subset M$*.*

Proof. The implications (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) are trivial. So, we have to deduce (1) from (3). Let $\{e_1, e_2, \dots, e_m\}$ generate M over A and an 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. The Laplace identity $\det X \cdot E = \widehat{X} \cdot X$ implies that $(\det X)M \subset \operatorname{im} \varkappa$. Now, let a multiplication by b be presented by a matrix Y, that is, $(be_1, be_2, \dots, be_m) = (e_1, e_2, \dots, e_m) \cdot Y$. Then the zero operator $M \longrightarrow 0$ can be presented by a matrix $b \cdot E - Y$. Hence, a multiplication by $\det(b \cdot E - Y)$ annihilates M. Since M is faceful, $\det(b \cdot E - Y) = 0$. This is a polynomial equation in b with the coefficients in A and the leading term b^n as required in (1). $\square$

A set of all $b \in B$ that are integer over A is called *an integer closure* of A in B. If each $b \in B$ is integer over A, then B is called *an integer extension* of A or *an integer* A-algebra.

Lemma 21.2 *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 $p^m = x_1 p^{m-1} + \cdots + x_1 p + x_0$, $q^n = y_1 q^{n-1} + \cdots + y_1 q + y_0$ 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 faceful (it contains 1) and goes to itself under the multiplication by both $p+q$ and pq. Similarly, if $c^r = z_1 c^{r-1} + \cdots + z_1 c + z_0$ and all z_ν are integer over A, then a multiplication by c preserves a faceful A-module spanned by a sufficient number of products $c^i z_1^{j_1} z_2^{j_2} \cdots z_r^{j_r}$. $\square$

Corollary 21.3 *Let $B \supset A$ is 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}. $\square$

ALGEBRAICITY. 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 $f \in k[x]$. Usually, such b is called rather *algebraic* than *integer*. We write $k[b]$ for a k-linear span of $\{b^n\}_{n \geqslant 0}$; $k[b] \subset B$ is the minimal k-subalgebra containing 1 and b. Clearly, $k[b] = \operatorname{im}(\mathrm{ev}_b) = k[x]/\ker(\mathrm{ev}_b)$, where $\mathrm{ev}_b : k[x] \xrightarrow{f(x) \mapsto f(b)} B$ is *an evaluation homomorphism*. So, b is algebraic $\Longleftrightarrow$ $k[b]$ is finite dimensional $\Longleftrightarrow$ $k[b]$ is a field[2].

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 $k[x_1, \dots, x_m] \overset{\pi}{\twoheadrightarrow} B$. Images $b_i = \pi(x_i) \in B$ are called *algebra generators* for B over k.

Lemma 21.4 *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 $\{b_1, b_2, \dots, b_m\}$. The basic case $m = 1$, $B = k[b]$ was already discussed in the previous section, so we can use the induction over m. If $k[b_m]$ is a field, then B is algebraic over $k[b_m]$ and $k[b_m]$ is algebraic over k by the inductive assumption. Hence, B is algebraic over k, because of Lemma 21.2. So, we have only to show that b_m must be algebraic over k. If b_m is not algebraic, then an evaluation $\mathrm{ev}_{b_m} : k[x] \xrightarrow{x \mapsto b_m} B$ is injective and a k-linear span $k(b_m)$ of $\{b_m^i\}_{i \in \mathbb{Z}}$ is identified with the field $k(x)$ by sending $x \longmapsto b_m$. By the inductive assumption, B is algebraic over $k(b_m)$, that is, each of $b_1, b_2, \dots, b_{m-1}$ satisfies a polynomial equation with coefficients in $k(b_m)$.

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

[2] the last equivalence follows from Corollary 21.3 and a trivial remark that $k[b] \simeq k[x]$ is not a field as soon as $\ker(\mathrm{ev}_b) = 0$

We can suppose (multiplying by appropriate polynomials in b_m) that all these equations have polynomial coefficients and the same leading coefficient, say, $p(b_m) \in k[b_m]$. So, B is integer over a subalgebra F generated by b_m and $q = 1/p(b_m)$ over k. By Corollary 21.3, F is a field. Let $g(b_m, q) \in F$ with $g \in k[x_1, x_2]$ be inverse to $1+q$. We write a rational function $g(x\,,\,1/p(x)) \in k(x)$ as $h(x)/p^k(x)$, where $h \in k[x]$ is coprime with $p \in k[x]$, and multiply both sides of $(1 + 1/p(b_m))\,h(b_m)/p^k(b_m) = 1$ by $p^{k+1}(b_m)$. So, b_m satisfy the 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. $\square$

<u>NOETHERIAN RINGS.</u> We say that an ideal $I \subset A$ *is generated* by a set $\{f_\nu\} \subset I$ if each $g \in I$ can be written as a finite linear combination $h_1 f_{\nu_1} + h_2 f_{\nu_2} + \cdots + h_s f_{\nu_s}$ with $h_i \in A$. We write $(f_1, f_2, \ldots, f_m)$ for the ideal generated by a finite set $\{f_1, f_2, \ldots, f_m\}$. A commutative ring A is called *Noetherian* if it satisfies the lemma below.

<u>Lemma 21.5</u> *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) implies (2). To deduce (3) from (2), take a finite set of generators for the ideal $I = \bigcup_\nu I_\nu$; since they belong to some I_n, we have $I_\nu = I_n = I \quad \forall\, \nu \geqslant n$. Finally, (1) follows from (3) applied to the chain $I_\nabla = (f_1, f_2, \ldots, f_n)$, where f_i are chosen from $\{f_\nu\}$ in such a way that $f_\nu \notin (f_1, f_2, \ldots, f_{\nu-1})$. $\square$

<u>Theorem 21.6</u> (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 $a_1, a_2, \ldots, a_s \in A$ coming from $f_1, f_2, \ldots, f_s \in I$ and let $\max_\nu(\deg f_\nu) = m$. So, a leading term of any polynomial of degree $\geqslant m$ can be killed by adding an appropriate combination of f_ν. Hence, I is generated by $f_1, f_2, \ldots, f_s$ and $I_1, I_2, \ldots, I_{m-1}$, which are finitely generated. $\square$

<u>Corollary 21.7</u> *A polynomial ring $A[x_1, \ldots, x_n]$ over a Noetherian ring A is Noetherian as well.* $\square$

<u>Corollary 21.8</u> *Any finitely generated k-algebra is Noetherian for any field k.*

Proof. A polynomial algebra $k[x_1, \ldots, x_n]$ is Noetherian by the previous corollary. Since a preimage of an ideal under a ring homomorphism is an ideal, a factor ring of a Noetherian ring is Noetherian as well by the third property in Lemma 21.5. $\square$

<u>HILBERT'S NULLSTELLENSATZ.</u> For any ideal $I \subset k[x_1, \ldots, x_n]$ we write $V(I) \subset \mathbb{A}^n$ for an affine algebraic subset given by polynomial equations $f(x) = 0$ with $f \in I$.

<u>Theorem 21.9</u> (week Nullstellensatz). *If k is algebraically closed, then $V(I) = \varnothing \iff 1 \in I$.*

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 $I \subset k[x_1, \ldots, x_n]$. We can 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 and 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 $K = k[x_1, \ldots, x_n]/I$ is a field. Hence, any element of K is algebraic over $k \subset K$ by Lemma 21.4. Since k is algebraically closed, this means that any polynomial is (mod I)-congruent to some constant. Let $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$ be the constants presenting the basic linear forms $x_1, x_2, \ldots, x_n$ (mod I). Then any polynomial $f \in k[x_1, \ldots, x_n]$ is (mod I) congruent to $f(\vartheta_1, \vartheta_2, \ldots, \vartheta_n) \in k$. In particular, $f(\vartheta_1, \vartheta_2, \ldots, \vartheta_n) = 0$ for any $f \in I$ as required. $\square$

For any affine algebraic subset $V \subset \mathbb{A}^n$ we write $I(V)$ for a set of all polynomials $f \in k[x_1, \ldots, x_n]$ vanishing along V. Clearly, $I(V)$ is an ideal and $I(V(I)) \supset I$ for any I. In general, this inclusion is proper. For example, if $I = (x^2) \in \mathbb{C}[x]$, then $V(I) = \{0\} \subset \mathbb{A}^1(\mathbb{C})$ and $I(V(I)) = (x)$.

<u>Theorem 21.10</u> (strong Nullstellensatz). *If k is algebraically closed, then $f \in I(V(I)) \iff f^k \in I$ for some $k \in \mathbb{N}$.*

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 $(t,\, x_1, x_2, \ldots, x_n)$. If $f \in k[x_1, \ldots, x_n] \subset k[t,\, x_1, x_2, \ldots, x_n]$ vanishes along $V(I)$, then an ideal $J \subset k[t,\, x_1, x_2, \ldots, x_n]$ generated by I and a polynomial $g(t, x) = 1 - t\,f(x)$ has an empty zero set $V(J)$, because of $g(x, t) \equiv 1$ on $V(I)$. So, $1 \in J$, that is, there are some $q_0, q_1, \ldots, q_s \subset k[t,\, x_1, x_2, \ldots, x_n]$ and $f_1, f_2, \ldots, f_s \subset I$ such that $q_0(x,t)(1 - tf(x)) + q_1(t,x)f_1(x) + \cdots + q_s(x,t)f_s(x) = 1$. A homomorphism $k[t,\, x_1, x_2, \ldots, x_n] \longrightarrow k(x_1, x_2, \ldots, x_n)$ sending $t \longmapsto 1/f(x)$, $x_\nu \longmapsto x_\nu$ takes this equality to

$$q_1(1/f(x)\,,\,x)\,f_1(x) + \cdots + q_s(1/f(x)\,,\,x)\,f_s(x) = 1\,.$$

Since I is proper, some of $q_\nu(1/f(x), x)$ should have nontrivial denominators. So, a multiplication by appropriate power f^k leads to a required expression $\widetilde{q}_1(x)\,f_1(x) + \cdots + \widetilde{q}_s(x)\,f_s(x) = f^k(x)$ with $\widetilde{q}_\nu \in k[x_1, \ldots, x_n]$. $\square$