A Primer of Commutative Algebra

James S. Milne

April 27, 2010, v2.21

Abstract

These notes prove the basic theorems in commutative algebra required for algebraic geometry and algebraic groups. They assume only a knowledge of the algebra usually taught in advanced undergraduate or first-year graduate courses.

Available at `www.jmilne.org/math/`.

Contents

NOTATIONS AND CONVENTIONS

Our convention is that rings have identity elements,[1] and homomorphisms of rings respect the identity elements. A *unit* of a ring is an element admitting an inverse. The units of a

[1]An element e of a ring A is an *identity element* if $ea = a = ae$ for all elements a of the ring. It is usually denoted 1_A or just 1. Some authors call this a unit element, but then an element can be a unit without being a unit element. Worse, a unit need not be the unit.

ring A form a group, which we denote by[2] $A^\times$. Throughout "ring" means "commutative ring". Following Bourbaki, we let $\mathbb{N} = \{0,1,2,\ldots\}$. For a field k, k^{al} denotes an algebraic closure of k.

$X \subset Y$	X is a subset of Y (not necessarily proper).
$X \stackrel{\text{def}}{=} Y$	X is defined to be Y, or equals Y by definition.
$X \approx Y$	X is isomorphic to Y.
$X \simeq Y$	X and Y are canonically isomorphic (or there is a given or unique isomorphism).

ACKNOWLEDGEMENTS

I thank the following for providing corrections and comments for earlier versions of these notes: Keenan Kidwell, Andrew McLennan, Shu Otsuka.

1 Rings and algebras

Let A be a ring. A *subring* of A is a subset that contains 1_A and is closed under addition, multiplication, and the formation of negatives. An *A-algebra* is a ring B together with a homomorphism $i_B \colon A \to B$. A *homomorphism* of A-algebras $B \to C$ is a homomorphism of rings $\varphi \colon B \to C$ such that $\varphi(i_B(a)) = i_C(a)$ for all $a \in A$.

Elements $x_1, \ldots, x_n$ of an A-algebra B are said to *generate* it if every element of B can be expressed as a polynomial in the x_i with coefficients in $i_B(A)$, i.e., if the homomorphism of A-algebras $A[X_1,\ldots,X_n] \to B$ acting as i_B on A and sending X_i to x_i is surjective. We then write $B = (i_B A)[x_1,\ldots,x_n]$.

A ring homomorphism $A \to B$ is of *finite type*, and B is a *finitely generated* A-algebra, if B is generated by a finite set of elements as an A-algebra.

A ring homomorphism $A \to B$ is *finite*, and B is a *finite*[3] A-algebra, if B is finitely generated as an A-module. If $A \to B$ and $B \to C$ are finite ring homomorphisms, then so also is their composite $A \to C$.

Let k be a field, and let A be a k-algebra. When $1_A \neq 0$, the map $k \to A$ is injective, and we can identify k with its image, i.e., we can regard k as a subring of A. When $1_A = 0$, the ring A is the zero ring $\{0\}$.

Let $A[X]$ be the ring of polynomials in the symbol X with coefficients in A. If A is an integral domain, then $\deg(fg) = \deg(f) + \deg(g)$, and so $A[X]$ is also an integral domain; moreover, $A[X]^\times = A^\times$.

Let A be an algebra over a field k. If A is an integral domain and finite as a k-algebra, then it is a field because, for each nonzero $a \in A$, the k-linear map $x \mapsto ax \colon A \to A$ is injective, and hence is surjective, which shows that a has an inverse. If A is an integral domain and each element of A is algebraic over k, then for each $a \in A$, $k[a]$ is an integral domain finite over k, and hence contains an inverse of a; again A is a field.

PRODUCTS AND IDEMPOTENTS

An element e of a ring A is *idempotent* if $e^2 = e$. For example, 0 and 1 are both idempotents — they are called the *trivial idempotents*. Idempotents $e_1, \ldots, e_n$ are *orthogonal* if $e_i e_j = 0$

[2]This notation differs from that of Bourbaki, who writes $A^\times$ for the multiplicative monoid $A \smallsetminus \{0\}$ and A^* for the group of units. We shall rarely need the former, and $*$ is overused.

[3]This is Bourbaki's terminology (AC V §1, 1). Finite homomorphisms of rings correspond to finite maps of varieties and schemes. Some other authors say "module-finite".

for $i \neq j$. Any sum of orthogonal idempotents is again idempotent. A set $\{e_1,\ldots,e_n\}$ of orthogonal idempotents is *complete* if $e_1+\cdots+e_n=1$. Any set of orthogonal idempotents $\{e_1,\ldots,e_n\}$ can be made into a complete set of orthogonal idempotents by adding the idempotent $e=1-(e_1+\cdots+e_n)$.

If $A=A_1\times\cdots\times A_n$ (direct product of rings), then the elements

$$e_i=(0,\ldots,\overset{i}{1},\ldots,0),\quad 1\leq i\leq n,$$

form a complete set of orthogonal idempotents in A. Conversely, if $\{e_1,\ldots,e_n\}$ is a complete set of orthogonal idempotents in A, then Ae_i becomes a ring[4] with the addition and multiplication induced by that of A, and $A\simeq Ae_1\times\cdots\times Ae_n$.

2 Ideals

Let A be a ring. An *ideal* $\mathfrak{a}$ in A is a subset such that

◇ $\mathfrak{a}$ is a subgroup of A regarded as a group under addition;

◇ $a\in\mathfrak{a},\ r\in A\Rightarrow ra\in\mathfrak{a}$.

The *ideal generated by a subset* S of A is the intersection of all ideals $\mathfrak{a}$ containing S — it is easy to verify that this is in fact an ideal, and that it consists of all finite sums of the form $\sum r_is_i$ with $r_i\in A$, $s_i\in S$. The ideal generated by the empty set is the zero ideal $\{0\}$. When $S=\{a,b,\ldots\}$, we write $(a,b,\ldots)$ for the ideal it generates.

An ideal is *principal* if it is generated by a single element. Such an ideal (a) is proper if and only a is not a unit. Thus a ring A is a field if and only if $1_A\neq 0$ and A contains no nonzero proper ideals.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in A. The set $\{a+b\mid a\in\mathfrak{a},\ b\in\mathfrak{b}\}$ is an ideal, denoted $\mathfrak{a}+\mathfrak{b}$. The ideal generated by $\{ab\mid a\in\mathfrak{a},\ b\in\mathfrak{b}\}$ is denoted by $\mathfrak{ab}$. Clearly $\mathfrak{ab}$ consists of all finite sums $\sum a_ib_i$ with $a_i\in\mathfrak{a}$ and $b_i\in\mathfrak{b}$, and if $\mathfrak{a}=(a_1,\ldots,a_m)$ and $\mathfrak{b}=(b_1,\ldots,b_n)$, then $\mathfrak{ab}=(a_1b_1,\ldots,a_ib_j,\ldots,a_mb_n)$. Note that $\mathfrak{ab}\subset\mathfrak{a}A=\mathfrak{a}$ and $\mathfrak{ab}\subset A\mathfrak{b}=\mathfrak{b}$, and so

$$\mathfrak{ab}\subset\mathfrak{a}\cap\mathfrak{b}. \tag{1}$$

The kernel of a homomorphism $A\to B$ is an ideal in A. Conversely, for any ideal $\mathfrak{a}$ in a ring A, the set of cosets of $\mathfrak{a}$ in A forms a ring $A/\mathfrak{a}$, and $a\mapsto a+\mathfrak{a}$ is a homomorphism $\varphi\colon A\to A/\mathfrak{a}$ whose kernel is $\mathfrak{a}$. There is a one-to-one correspondence

$$\{\text{ideals of } A \text{ containing } \mathfrak{a}\}\ \underset{\varphi^{-1}(\mathfrak{b})\leftarrow\!\shortmid\,\mathfrak{b}}{\overset{\mathfrak{b}\mapsto\varphi(\mathfrak{b})}{\longleftrightarrow}}\ \{\text{ideals of } A/\mathfrak{a}\}. \tag{2}$$

For any ideal $\mathfrak{b}$ of A, $\varphi^{-1}\varphi(\mathfrak{b})=\mathfrak{a}+\mathfrak{b}$.

The ideals of $A\times B$ are all of the form $\mathfrak{a}\times\mathfrak{b}$ with $\mathfrak{a}$ and $\mathfrak{b}$ ideals in A and B. To see this, note that if $\mathfrak{c}$ is an ideal in $A\times B$ and $(a,b)\in\mathfrak{c}$, then $(a,0)=(1,0)(a,b)\in\mathfrak{c}$ and $(0,b)=(0,1)(a,b)\in\mathfrak{c}$. Therefore, $\mathfrak{c}=\mathfrak{a}\times\mathfrak{b}$ with

$$\mathfrak{a}=\{a\mid(a,0)\in\mathfrak{c}\},\quad \mathfrak{b}=\{b\mid(0,b)\in\mathfrak{c}\}.$$

An ideal $\mathfrak{p}$ in A is *prime* if $\mathfrak{p}\neq A$ and $ab\in\mathfrak{p}\Rightarrow a\in\mathfrak{p}$ or $b\in\mathfrak{p}$. Thus $\mathfrak{p}$ is prime if and only if the quotient ring $A/\mathfrak{p}$ is nonzero and has the property that

$$ab=0,\quad b\neq 0\Rightarrow a=0,$$

[4]But Ae_i is not a subring of A if $n\neq 1$ because its identity element is $e_i\neq 1_A$. However, the map $a\mapsto ae_i\colon A\to Ae_i$ realizes Ae_i as a quotient of A.

i.e., $A/\mathfrak{p}$ is an integral domain. Note that if $\mathfrak{p}$ is prime and $a_1 \cdots a_n \in \mathfrak{p}$, then at least one of the $a_i \in \mathfrak{p}$ (because either $a_1 \in \mathfrak{p}$ or $a_2 \cdots a_n \in \mathfrak{p}$; if the latter, then either $a_2 \in \mathfrak{p}$ or $a_3 \cdots a_n \in \mathfrak{p}$; etc.).

An ideal $\mathfrak{m}$ in A is *maximal* if it is a maximal element of the set of proper ideals in A. Therefore an ideal $\mathfrak{m}$ is maximal if and only if the quotient ring $A/\mathfrak{m}$ is nonzero and has no proper nonzero ideals (by (2)), and so is a field. Note that

$$\mathfrak{m} \text{ maximal } \implies \mathfrak{m} \text{ prime.}$$

A *multiplicative subset* of a ring A is a subset S with the property:

$$1 \in S, \quad a,b \in S \implies ab \in S.$$

For example, the following are multiplicative subsets:

the multiplicative subset $\{1, f, \ldots, f^r, \ldots\}$ generated by an element f of A;

the complement of a prime ideal (or of a union of prime ideals);

$1 + \mathfrak{a} \overset{\text{def}}{=} \{1 + a \mid a \in \mathfrak{a}\}$ for any ideal $\mathfrak{a}$ of A.

PROPOSITION 2.1. *Let S be a subset of a ring A, and let $\mathfrak{a}$ be an ideal disjoint from S. The set of ideals in A containing $\mathfrak{a}$ and disjoint from S contains maximal elements (i.e., an element not properly contained in any other ideal in the set). If S is multiplicative, then any such maximal element is prime.*

PROOF. The set Σ of ideals containing $\mathfrak{a}$ and disjoint from S is nonempty (it contains $\mathfrak{a}$). If A is noetherian (see §3 below), Σ automatically contains maximal elements. Otherwise, we apply Zorn's lemma. Let $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \cdots$ be a chain of ideals in Σ, and let $\mathfrak{b} = \bigcup \mathfrak{b}_i$. Then $\mathfrak{b} \in \Sigma$, because otherwise some element of S lies in $\mathfrak{b}$, and hence in some $\mathfrak{b}_i$, which contradicts the definition of Σ. Therefore $\mathfrak{b}$ is an upper bound for the chain. As every chain in Σ has an upper bound, Zorn's lemma implies that Σ has a maximal element.

Assume that S is a multiplicative subset of A, and let $\mathfrak{c}$ be maximal in Σ. Let $bb' \in \mathfrak{c}$. If b is not in $\mathfrak{c}$, then $\mathfrak{c} + (b)$ properly contains $\mathfrak{c}$, and so it is not in Σ. Therefore there exist an $f \in S \cap (\mathfrak{c} + (b))$, say, $f = c + ab$ with $c \in \mathfrak{c}$. Similarly, if b' is not in $\mathfrak{c}$, then there exists an $f' \in S$ such that $f = c' + a'b'$ with $c' \in \mathfrak{c}$. Now

$$ff' = cc' + abc' + a'b'c + aa'bb' \in \mathfrak{c},$$

which contradicts

$$ff' \in S. \qquad \square$$

COROLLARY 2.2. *Every proper ideal in a ring is contained in a maximal ideal.*

PROOF. For a proper ideal $\mathfrak{a}$ of A, apply the proposition with $S = \{1\}$. □

ASIDE 2.3. The proof of (2.1) is one of many in commutative algebra in which an ideal, maximal with respect to some property, is shown to be prime. For a general examination of this phenomenon, see Lam, T. Y. and Reyes, Manuel L., A prime ideal principle in commutative algebra. J. Algebra 319 (2008), no. 7, 3006–3027.

The *radical* $\mathrm{rad}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ is

$$\{f \in A \mid f^r \in \mathfrak{a}, \text{ some } r \in \mathbb{N}, r > 0\}.$$

An ideal $\mathfrak{a}$ is said to be *radical* if it equals its radical. Thus $\mathfrak{a}$ is radical if and only if the quotient ring $A/\mathfrak{a}$ is *reduced*, i.e., without nonzero *nilpotent* elements (elements some power of which is zero). Since integral domains are reduced, prime ideals (*a fortiori* maximal ideals) are radical. The radical of (0) consists of the nilpotent elements of A — it is called the *nilradical* of A.

If $\mathfrak{b} \leftrightarrow \mathfrak{b}'$ under the one-to-one correspondence (2), then $A/\mathfrak{b} \simeq (A/\mathfrak{a})/\mathfrak{b}'$, and so $\mathfrak{b}$ is prime (resp. maximal, radical) if and only if $\mathfrak{b}'$ is prime (resp. maximal, radical).

PROPOSITION 2.4. *Let $\mathfrak{a}$ be an ideal in a ring A.*
(a) The radical of $\mathfrak{a}$ is an ideal.
(b) $\mathrm{rad}(\mathrm{rad}(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$.

PROOF. (a) If $a \in \mathrm{rad}(\mathfrak{a})$, then clearly $fa \in \mathrm{rad}(\mathfrak{a})$ for all $f \in A$. Suppose $a, b \in \mathrm{rad}(\mathfrak{a})$, with say $a^r \in \mathfrak{a}$ and $b^s \in \mathfrak{a}$. When we expand $(a+b)^{r+s}$ using the binomial theorem, we find that every term has a factor a^r or b^s, and so lies in $\mathfrak{a}$.

(b) If $a^r \in \mathrm{rad}(\mathfrak{a})$, then $a^{rs} = (a^r)^s \in \mathfrak{a}$ for some $s > 0$, and so $a \in \mathrm{rad}(\mathfrak{a})$. □

Note that (b) of the proposition shows that $\mathrm{rad}(\mathfrak{a})$ is radical, and so is the smallest radical ideal containing $\mathfrak{a}$.

If $\mathfrak{a}$ and $\mathfrak{b}$ are radical, then $\mathfrak{a} \cap \mathfrak{b}$ is radical, but $\mathfrak{a} + \mathfrak{b}$ need not be: consider, for example, $\mathfrak{a} = (X^2 - Y)$ and $\mathfrak{b} = (X^2 + Y)$; they are both prime ideals in $k[X, Y]$ (by 4.7 below), but $\mathfrak{a} + \mathfrak{b} = (X^2, Y)$, which contains X^2 but not X.

PROPOSITION 2.5. *The radical of an ideal is equal to the intersection of the prime ideals containing it. In particular, the nilradical of a ring A is equal to the intersection of the prime ideals of A.*

PROOF. If $\mathfrak{a} = A$, then the set of prime ideals containing it is empty, and so the intersection is A. Thus we may suppose that $\mathfrak{a}$ is a proper ideal of A. Then $\mathrm{rad}(\mathfrak{a}) \subset \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$ because prime ideals are radical and $\mathrm{rad}(\mathfrak{a})$ is the smallest radical ideal containing $\mathfrak{a}$.

Conversely, suppose that $f \notin \mathrm{rad}(\mathfrak{a})$. According to Proposition 2.1, there exists a prime ideal containing $\mathfrak{a}$ and disjoint from the multiplicative subset $\{1, f, \ldots\}$. Therefore $f \notin \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. □

DEFINITION 2.6. The *Jacobson radical* $\mathfrak{J}$ of a ring is the intersection of the maximal ideals of the ring:

$$\mathfrak{J}(A) = \bigcap \{\mathfrak{m} \mid \mathfrak{m} \text{ maximal in } A\}.$$

A ring A is *local* if it has exactly one maximal ideal. For such a ring, the Jacobson radical is $\mathfrak{m}$.

PROPOSITION 2.7. *An element c of A is in the Jacobson radical of A if and only if $1 - ac$ is a unit for all $a \in A$.*

PROOF. We prove the contrapositive: there exists a maximal ideal $\mathfrak{m}$ such that $c \notin \mathfrak{m}$ if and only if there exists an $a \in A$ such that $1-ac$ is not a unit.

$\Leftarrow$: As $1-ac$ is not a unit, it lies in some maximal ideal $\mathfrak{m}$ of A (by 2.2). Then $c \notin \mathfrak{m}$, because otherwise $1=(1-ac)+ac \in \mathfrak{m}$.

$\Rightarrow$: Suppose that c is not in the maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}+(c)=A$, and so $1=m+ac$ for some $m \in \mathfrak{m}$ and $a \in A$. Now $1-ac \in \mathfrak{m}$, and so it is not a unit. □

PROPOSITION 2.8. *Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$, $r \geq 1$, be ideals in A with $\mathfrak{p}_2,\ldots,\mathfrak{p}_r$ prime, and let $\mathfrak{a}$ be an ideal in A. Then*

$$\mathfrak{a} \subset \bigcup\nolimits_{1\leq i\leq r} \mathfrak{p}_i \implies \mathfrak{a} \subset \mathfrak{p}_i \text{ for some } i.$$

PROOF. We prove the contrapositive:

> if the ideal $\mathfrak{a}$ in not contained in any of the ideals $\mathfrak{p}_i$, then it is not contained in their union.

For $r=1$, there is nothing to prove, and so we may assume that $r>1$ and (inductively) that the statement is true for $r-1$. As $\mathfrak{a}$ is not contained in any of the ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$, for each i, there exists an a_i in $\mathfrak{a}$ not in the union of the ideals $\mathfrak{p}_1,\ldots,\mathfrak{p}_{i-1},\mathfrak{p}_{i+1},\ldots,\mathfrak{p}_r$. If there exists an i such that a_i does not lie in $\mathfrak{p}_i$, then that $a_i \in \mathfrak{a} \smallsetminus \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$, and the proof is complete. Thus suppose that every $a_i \in \mathfrak{p}_i$, and consider

$$a = a_1 \cdots a_{r-1} + a_r.$$

Because $\mathfrak{p}_r$ is prime and none of the elements $a_1,\ldots,a_{r-1}$ lies in $\mathfrak{p}_r$, their product does not lie in $\mathfrak{p}_r$; however, $a_r \in \mathfrak{p}_r$, and so $a \notin \mathfrak{p}_r$. Next consider a prime $\mathfrak{p}_i$ with $i \leq r-1$. In this case $a_1 \cdots a_{r-1} \in \mathfrak{p}_i$ because the product involves a_i, but $a_r \notin \mathfrak{p}_i$, and so again $a \notin \mathfrak{p}_i$. Now $a \in \mathfrak{a} \smallsetminus \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_r$, and so $\mathfrak{a}$ is not contained in the union of the $\mathfrak{p}_i$. □

EXTENSION AND CONTRACTION OF IDEALS

Let $\varphi: A \to B$ be a homomorphism of rings.

NOTATION 2.9. For an ideal $\mathfrak{b}$ of B, $\varphi^{-1}(\mathfrak{b})$ is an ideal in A, called the *contraction* of $\mathfrak{b}$ to A, which is often denoted $\mathfrak{b}^c$. For an ideal $\mathfrak{a}$ of A, the ideal in B generated by $\varphi(\mathfrak{a})$ is called the *extension* of $\mathfrak{a}$ to B, and is often denoted $\mathfrak{a}^e$. When φ is surjective, $\varphi(\mathfrak{a})$ is already an ideal, and when A is a subring of B, $\mathfrak{b}^c = \mathfrak{b} \cap A$.

2.10. There are the following equalities ($\mathfrak{a},\mathfrak{a}'$ ideals in A; $\mathfrak{b},\mathfrak{b}'$ ideals in B):

$$(\mathfrak{a}+\mathfrak{a}')^e = \mathfrak{a}^e + \mathfrak{a}'^e, \quad (\mathfrak{a}\mathfrak{a}')^e = \mathfrak{a}^e\mathfrak{a}'^e, \quad (\mathfrak{b}\cap\mathfrak{b}')^c = \mathfrak{b}^c \cap \mathfrak{b}'^c, \quad \mathrm{rad}(\mathfrak{b})^c = \mathrm{rad}(\mathfrak{b}^c).$$

2.11. Obviously (i) $\mathfrak{a} \subset \mathfrak{a}^{ec}$ and (ii) $\mathfrak{b}^{ce} \subset \mathfrak{b}$ ($\mathfrak{a}$ an ideal of A; $\mathfrak{b}$ an ideal of B). On applying e to (i), we find that $\mathfrak{a}^e \subset \mathfrak{a}^{ece}$, and (ii) with $\mathfrak{b}$ replaced by $\mathfrak{a}^e$ shows that $\mathfrak{a}^{ece} \subset \mathfrak{a}^e$; therefore $\mathfrak{a}^e = \mathfrak{a}^{ece}$. Similarly, $\mathfrak{b}^{cec} = \mathfrak{b}^c$. It follows that extension and contraction define inverse bijections between the set of contracted ideals in A and the set of extended ideals in B:

$$\{\mathfrak{b}^c \subset A \mid \mathfrak{b} \text{ an ideal in } B\} \underset{c}{\overset{e}{\rightleftharpoons}} \{\mathfrak{a}^e \subset B \mid \mathfrak{a} \text{ an ideal in } A\}$$

Note that, for any ideal $\mathfrak{b}$ in B, the map $A/\mathfrak{b}^c \to B/\mathfrak{b}$ is injective, and so $\mathfrak{b}^c$ is prime (resp. radical) if $\mathfrak{b}$ is prime (resp. radical).

THE CHINESE REMAINDER THEOREM

Recall the classical form of the theorem: let $d_1,...,d_n$ be integers, relatively prime in pairs; then for any integers $x_1,...,x_n$, the congruences

$$x \equiv x_i \bmod d_i$$

have a simultaneous solution $x \in \mathbb{Z}$; moreover, if x is one solution, then the other solutions are the integers of the form $x + md$ with $m \in \mathbb{Z}$ and $d = \prod d_i$.

We want to translate this in terms of ideals. Integers m and n are relatively prime if and only if $(m,n) = \mathbb{Z}$, i.e., if and only if $(m) + (n) = \mathbb{Z}$. This suggests defining ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a ring A to be *relatively prime* (or *coprime*) if $\mathfrak{a} + \mathfrak{b} = A$.

If $m_1,...,m_k$ are integers, then $\bigcap(m_i) = (m)$ where m is the least common multiple of the m_i. Thus $\bigcap(m_i) \supset (\prod m_i)$, which equals $\prod(m_i)$. If the m_i are relatively prime in pairs, then $m = \prod m_i$, and so we have $\bigcap(m_i) = \prod(m_i)$. Note that in general,

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n \subset \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap ... \cap \mathfrak{a}_n,$$

but the two ideals need not be equal.

These remarks suggest the following statement.

THEOREM 2.12 (CHINESE REMAINDER THEOREM). *Let $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ be ideals in a ring A. If $\mathfrak{a}_i$ is relatively prime to $\mathfrak{a}_j$ whenever $i \neq j$, then the map*

$$a \mapsto (\ldots, a + \mathfrak{a}_i, \ldots) \colon A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n \tag{3}$$

is surjective with kernel $\prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$.

PROOF. Suppose first that $n = 2$. As $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, there exist $a_i \in \mathfrak{a}_i$ such that $a_1 + a_2 = 1$. Then $a_1 x_2 + a_2 x_1$ maps to $(x_1 \bmod \mathfrak{a}_1, x_2 \bmod \mathfrak{a}_2)$, which shows that (3) is surjective.

For each i, there exist elements $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_i$ such that

$$a_i + b_i = 1, \text{ all } i \geq 2.$$

The product $\prod_{i\geq 2}(a_i + b_i) = 1$, and lies in $\mathfrak{a}_1 + \prod_{i \geq 2} \mathfrak{a}_i$, and so

$$\mathfrak{a}_1 + \prod_{i\geq 2} \mathfrak{a}_i = A.$$

We can now apply the theorem in the case $n = 2$ to obtain an element y_1 of A such that

$$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \prod_{i\geq 2} \mathfrak{a}_i.$$

These conditions imply

$$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \mathfrak{a}_j, \text{ all } j > 1.$$

Similarly, there exist elements $y_2,...,y_n$ such that

$$y_i \equiv 1 \bmod \mathfrak{a}_i, \quad y_i \equiv 0 \bmod \mathfrak{a}_j \text{ for } j \neq i.$$

The element $x = \sum x_i y_i$ maps to $(x_1 \bmod \mathfrak{a}_1, \ldots, x_n \bmod \mathfrak{a}_n)$, which shows that (3) is surjective.

It remains to prove that $\bigcap \mathfrak{a}_i = \prod \mathfrak{a}_i$. Obviously $\prod \mathfrak{a}_i \subset \bigcap \mathfrak{a}_i$. Suppose first that $n = 2$, and let $a_1 + a_2 = 1$, as before. For $c \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, we have

$$c = a_1 c + a_2 c \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$$

which proves that $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1 \mathfrak{a}_2$. We complete the proof by induction. This allows us to assume that $\prod_{i \geq 2} \mathfrak{a}_i = \bigcap_{i \geq 2} \mathfrak{a}_i$. We showed above that $\mathfrak{a}_1$ and $\prod_{i \geq 2} \mathfrak{a}_i$ are relatively prime, and so

$$\mathfrak{a}_1 \cdot (\prod_{i \geq 2} \mathfrak{a}_i) = \mathfrak{a}_1 \cap (\prod_{i \geq 2} \mathfrak{a}_i)$$

by the $n = 2$ case. Now $\mathfrak{a}_1 \cdot (\prod_{i \geq 2} \mathfrak{a}_i) = \prod_{i \geq 1} \mathfrak{a}_i$ and $\mathfrak{a}_1 \cap (\prod_{i \geq 2} \mathfrak{a}_i) = \mathfrak{a}_1 \cap (\bigcap_{i \geq 2} \mathfrak{a}_i) = \bigcap_{i \geq 1} \mathfrak{a}_i$, which completes the proof. □

3 Noetherian rings

PROPOSITION 3.1. *The following three conditions on a ring A are equivalent:*

(a) *every ideal in A is finitely generated;*
(b) *every ascending chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ eventually becomes constant, i.e., for some m, $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \cdots$.*
(c) *every nonempty set of ideals in A has a maximal element.*

PROOF. (a) $\Rightarrow$ (b): If $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ is an ascending chain, then $\mathfrak{a} = \bigcup \mathfrak{a}_i$ is an ideal, and hence has a finite set $\{a_1, \ldots, a_n\}$ of generators. For some m, all the a_i belong $\mathfrak{a}_m$, and then

$$\mathfrak{a}_m = \mathfrak{a}_{m+1} = \cdots = \mathfrak{a}.$$

(b) $\Rightarrow$ (c): Let Σ be a nonempty set of ideals in A. Then (b) certainly implies that every ascending chain of ideals in Σ has an upper bound in Σ, and so (a mild form of) Zorn's lemma shows that Σ has a maximal element.

(c) $\Rightarrow$ (a): Let $\mathfrak{a}$ be an ideal, and let Σ be the set of finitely generated ideals contained in $\mathfrak{a}$. Then S is nonempty because it contains the zero ideal, and so it contains a maximal element $\mathfrak{c} = (a_1, \ldots, a_r)$. If $\mathfrak{c} \neq \mathfrak{a}$, then there exists an element $a \in \mathfrak{a} \setminus \mathfrak{c}$, and $(a_1, \ldots, a_r, a)$ will be a finitely generated ideal in $\mathfrak{a}$ properly containing $\mathfrak{c}$. This contradicts the definition of $\mathfrak{c}$. □

A ring A is *noetherian* if it satisfies the equivalent conditions of the proposition. For example, fields and principal ideal domains are noetherian. On applying (c) to the set of all proper ideals containing a fixed proper ideal, we see that every proper ideal in a noetherian ring is contained in a maximal ideal. We saw in (2.3) that this is, in fact, true for any ring, but the proof for non-noetherian rings requires Zorn's lemma.

A quotient $A/\mathfrak{a}$ of a noetherian ring A is noetherian, because the ideals in $A/\mathfrak{a}$ are all of the form $\mathfrak{b}/\mathfrak{a}$ with $\mathfrak{b}$ an ideal in A, and any set of generators for $\mathfrak{b}$ generates $\mathfrak{b}/\mathfrak{a}$.

PROPOSITION 3.2. *Let A be a ring. The following conditions on an A-module M are equivalent:*

(a) *every submodule of M is finitely generated (in particular, M is finitely generated);*
(b) *every ascending chain of submodules $M_1 \subset M_2 \subset \cdots$ eventually becomes constant.*
(c) *every nonempty set of submodules of M has a maximal element.*

PROOF. Essentially the same as that of (3.1). □

An A-module M is *noetherian* if it satisfies the equivalent conditions of the proposition. Let ${}_AA$ denote A regarded as a left A-module. Then the submodules of ${}_AA$ are exactly the ideals in A, and so ${}_AA$ is noetherian (as an A-module) if and only if A is noetherian (as a ring).

PROPOSITION 3.3. *Let M be an A-module, and let N be a submodule of M. The module M is noetherian if and only both N and M/N are noetherian.*

PROOF. $\Rightarrow$: An ascending chain of submodules in N or in M/N gives rise to an ascending chain in M, and therefore becomes constant.

$\Leftarrow$: I claim that if $M' \subset M''$ are submodules of M such that $M' \cap N = M'' \cap N$ and M' and M'' have the same image in M/N, then $M' = M''$. To see this, let $x \in M''$; the second condition implies that there exists a $y \in M'$ with the same image as x in M/N, i.e., such that $x - y \in N$. Then $x - y \in M'' \cap N \subset M'$, and so $x \in M'$.

Now consider an ascending chain of submodules of M. If M/N is Noetherian, the image of the chain in M/N becomes stationary, and if N is Noetherian, the intersection of the chain with N becomes stationary. Now the claim shows that the chain itself becomes stationary. □

More generally, consider an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of A-modules. The module M is noetherian if and only if M' and M'' are both noetherian. For example, a direct sum

$$M = M_1 \oplus M_2$$

of A-modules is noetherian if and only if M_1 and M_2 are both noetherian (because $0 \to M_1 \to M \to M_2 \to 0$ is exact).

PROPOSITION 3.4. *Let A be a noetherian ring. Then every finitely generated A-module is noetherian.*

PROOF. If M is generated by a single element, then $M \approx A/\mathfrak{a}$ for some ideal $\mathfrak{a}$ in A, and the statement is obvious. We argue by induction on the minimum number n of generators of M. Since M contains a submodule N generated by $n-1$ elements such that the quotient M/N is generated by a single element, the statement follows from (3.3). □

PROPOSITION 3.5. *Every finitely generated module M over a noetherian ring A contains a finite chain of submodules $M \supset M_r \supset \cdots \supset M_1 \supset 0$ such that each quotient M_i/M_{i-1} is isomorphic to $A/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$.*

PROOF. The annihilator $\operatorname{ann}(x)$ of an element x of M is $\{a \in A \mid ax = 0\}$. It is an ideal in A, which is proper if $x \neq 0$. I claim that any ideal $\mathfrak{a}$ that is maximal among the annihilators of nonzero elements of A is prime. Suppose that $\mathfrak{a} = \operatorname{ann}(x)$, and let $ab \in \mathfrak{a}$, so that $abx = 0$. Then $\mathfrak{a} \subset (a) + \mathfrak{a} \subset \operatorname{ann}(bx)$. If $b \notin \mathfrak{a}$, then $bx \neq 0$, and so $\mathfrak{a} = \operatorname{ann}(bx)$ by maximality, which implies that $a \in \mathfrak{a}$.

We now prove the proposition. Note that, for any $x \in M$, the submodule Ax of M is isomorphic to $A/\operatorname{ann}(x)$. Therefore, if M is nonzero, then it contains a submodule M_1

isomorphic to $A/\mathfrak{p}_1$ for some prime ideal $\mathfrak{p}_1$. Similarly, M/M_1 contains a submodule M_2/M_1 isomorphic $A/\mathfrak{p}_2$ for some prime ideal $\mathfrak{p}_2$, and so on. The chain $0 \subset M_1 \subset M_2 \subset \cdots$ terminates because M is noetherian (by 3.4). □

THEOREM 3.6 (HILBERT BASIS THEOREM). *Every finitely generated algebra over a noetherian ring is noetherian.*

PROOF. Let A be noetherian. Since every finitely generated A-algebra is a quotient of a polynomial algebra, it suffices to prove the theorem for $A[X_1,\ldots,X_n]$. Note that

$$A[X_1,\ldots,X_n] = A[X_1,\ldots,X_{n-1}][X_n]. \tag{1}$$

This simply says that every polynomial f in n symbols $X_1,\ldots,X_n$ can be expressed uniquely as a polynomial in X_n with coefficients in $k[X_1,\ldots,X_{n-1}]$,

$$f(X_1,\ldots,X_n) = a_0(X_1,\ldots,X_{n-1})X_n^r + \cdots + a_r(X_1,\ldots,X_{n-1}).$$

Thus an induction argument shows that it suffices to prove the theorem for $A[X]$.

Recall that for a polynomial

$$f(X) = c_0X^r + c_1X^{r-1} + \cdots + c_r, \quad c_i \in A, \quad c_0 \neq 0,$$

c_0 is the *leading coefficient* of f.

Let $\mathfrak{a}$ be an ideal in $A[X]$, and let $\mathfrak{c}_i$ be the set of elements of A that occur as the leading coefficient of a polynomial in $\mathfrak{a}$ of degree i (we also include 0). Then $\mathfrak{c}_i$ is obviously an ideal in A, and $\mathfrak{c}_{i-1} \subset \mathfrak{c}_i$ because, if $cX^{i-1} + \cdots \in \mathfrak{a}$, then so also does $X(cX^{i-1} + \cdots) = cX^i + \cdots$. As A is noetherian, the sequence of ideals

$$\mathfrak{c}_1 \subset \mathfrak{c}_2 \subset \cdots \subset \mathfrak{c}_i \subset \cdots$$

eventually becomes constant, say, $\mathfrak{c}_d = \mathfrak{c}_{d+1} = \ldots$ (and then $\mathfrak{c}_d$ contains the leading coefficients of *all* polynomials in $\mathfrak{a}$).

For each $i \leq d$, choose a finite generating set $\{c_{i1}, c_{i2}, \ldots\}$ for $\mathfrak{c}_i$, and for each (i,j), choose a polynomial $f_{ij} \in \mathfrak{a}$ of degree i with leading coefficient c_{ij}. We shall show that the f_{ij}'s generate $\mathfrak{a}$.

Let $f \in \mathfrak{a}$; we have to show that $f \in (f_{ij})$. Suppose first that f has degree $s \geq d$. Then $f = cX^s + \cdots$ with $c \in \mathfrak{c}_d$, and so

$$c = \sum\nolimits_j a_j c_{dj}, \quad \text{some } a_j \in A.$$

Now

$$f - \sum\nolimits_j a_j f_{dj} X^{s-d}$$

is either zero and $f \in (f_{ij})$, or it has degree $< \deg(f)$. In the second case, we repeat the argument, until we obtain a polynomial f of degree $s < d$ that differs from the original polynomial by an element of (f_{ij}). By a similar argument, we then construct elements $a_j \in A$ such that

$$f - \sum\nolimits_j a_j f_{sj}$$

is either zero or has degree $< \deg(f)$. In the second case, we repeat the argument, until we obtain zero. □

NAKAYAMA'S LEMMA 3.7. *Let $\mathfrak{a}$ be an ideal in a ring A contained in all maximal ideals of A, and let M be a finitely generated A-module.*

(a) *If $M = \mathfrak{a}M$, then $M = 0$.*

(b) *If N is a submodule of M such that $M = N + \mathfrak{a}M$, then $M = N$.*

PROOF. (a) Suppose $M \neq 0$. Choose a minimal set of generators $\{e_1, \ldots, e_n\}$ for M, $n \geq 1$, and write

$$e_1 = a_1 e_1 + \cdots + a_n e_n, \quad a_i \in \mathfrak{a}.$$

Then

$$(1 - a_1)e_1 = a_2 e_2 + \cdots + a_n e_n$$

and, as $1 - a_1$ lies in no maximal ideal, it is a unit. Therefore $e_2, \ldots, e_n$ generate M, which contradicts the minimality of the original set.

(b) The hypothesis implies that $M/N = \mathfrak{a}(M/N)$, and so $M/N = 0$. □

Recall (2.6) that the Jacobson radical $\mathfrak{J}$ of A is the intersection of the maximal ideals of A, and so the condition on $\mathfrak{a}$ is that $\mathfrak{a} \subset \mathfrak{J}$. In particular, the lemma holds with $\mathfrak{a} = \mathfrak{J}$; for example, when A is a local ring, it holds with $\mathfrak{a}$ the maximal ideal in A.

COROLLARY 3.8. *Let A be a local ring with maximal ideal $\mathfrak{m}$ and residue field $k \stackrel{\text{def}}{=} A/\mathfrak{m}$, and let M be a finitely generated module over A. The action of A on $M/\mathfrak{m}M$ factors through k, and elements $a_1, \ldots, a_n$ of M generate it as an A-module if and only if*

$$a_1 + \mathfrak{m}M, \ldots, a_n + \mathfrak{m}M$$

span $M/\mathfrak{m}M$ as k-vector space.

PROOF. If $a_1, \ldots, a_n$ generate M, then it is obvious that their images generate the vector space $M/\mathfrak{m}M$. Conversely, suppose that $a_1 + \mathfrak{m}M, \ldots, a_n + \mathfrak{m}M$ span $M/\mathfrak{m}M$, and let N be the submodule of M generated by $a_1, \ldots, a_n$. The composite $N \to M \to M/\mathfrak{m}M$ is surjective, and so $M = N + \mathfrak{m}M$. Now Nakayama's lemma shows that $M = N$. □

COROLLARY 3.9. *Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Elements $a_1, \ldots, a_n$ of $\mathfrak{m}$ generate $\mathfrak{m}$ as an ideal if and only if $a_1 + \mathfrak{m}^2, \ldots, a_n + \mathfrak{m}^2$ span $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $k \stackrel{\text{def}}{=} A/\mathfrak{m}$. In particular, the minimum number of generators for the maximal ideal is equal to the dimension of the vector space $\mathfrak{m}/\mathfrak{m}^2$.*

PROOF. Because A is noetherian, $\mathfrak{m}$ is finitely generated, and we can apply the preceding corollary with $M = \mathfrak{m}$. □

EXAMPLE 3.10. Nakayama's lemma may fail if M is not finitely generated. For example, let $\mathbb{Z}_{(p)} = \{\frac{m}{n} \mid p \text{ does not divide } n\}$ and let $M = \mathbb{Q}$. Then $\mathbb{Z}_{(p)}$ is a local ring with maximal ideal (p) (see §6 below) and $M = pM$ but $M \neq 0$.

DEFINITION 3.11. Let A be a noetherian ring.

(a) The *height* $\text{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ in A is the greatest length d of a chain of distinct prime ideals

$$\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0. \tag{2}$$

(b) The *(Krull) dimension* of A is $\sup\{\text{ht}(\mathfrak{p}) \mid \mathfrak{p} \subset A, \quad \mathfrak{p} \text{ prime}\}$.

Thus, the Krull dimension of a ring A is the supremum of the lengths of chains of prime ideals in A (the length of a chain is the number of gaps, so the length of (2) is d). For example, a field has Krull dimension 0, and conversely an integral domain of Krull dimension 0 is a field. The height of every nonzero prime ideal in a principal ideal domain is 1, and so such a ring has Krull dimension 1 (provided it is not a field). It is sometimes convenient to define the Krull dimension of the zero ring to be -1.

We shall see in §16 that the height of any prime ideal in a noetherian ring is finite. However, the Krull dimension of the ring may be infinite, because it may contain a sequence $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots$ of prime ideals such that $\mathrm{ht}(\mathfrak{p}_i)$ tends to infinity (see Krull 1938 or Nagata 1962, p.203, for examples).

LEMMA 3.12. *In a noetherian ring, every set of generators for an ideal contains a finite generating set.*

PROOF. Let S be a set of generators for an ideal $\mathfrak{a}$ in a noetherian ring A. An ideal maximal in the set of ideals generated by finite subsets of S must contain every element of S (otherwise it wouldn't be maximal), and so equals $\mathfrak{a}$. □

THEOREM 3.13 (KRULL INTERSECTION THEOREM). *Let $\mathfrak{a}$ be an ideal in a noetherian ring A. If $\mathfrak{a}$ is contained in all maximal ideals of A, then $\bigcap_{n\geq 1}\mathfrak{a}^n = \{0\}$.*

PROOF. We shall show that, for *any* ideal $\mathfrak{a}$ in a noetherian ring,

$$\bigcap_{n\geq 1}\mathfrak{a}^n = \mathfrak{a}\cdot\bigcap_{n\geq 1}\mathfrak{a}^n. \tag{3}$$

When $\mathfrak{a}$ is contained in all maximal ideals of A, Nakayama's lemma shows that $\bigcap_{n\geq 1}\mathfrak{a}^n$ is zero.

Let $a_1,\ldots,a_r$ generate $\mathfrak{a}$. Then $\mathfrak{a}^n$ consists of finite sums

$$\sum_{i_1+\cdots+i_r=n} c_{i_1\cdots i_r}a_1^{i_1}\cdots a_r^{i_r}, \quad c_{i_1\cdots i_r}\in A.$$

In other words, $\mathfrak{a}^n$ consists of the elements of A of the form $g(a_1,\ldots,a_r)$ for some homogeneous polynomial $g(X_1,\ldots,X_r)\in A[X_1,\ldots,X_r]$ of degree n. Let S_m be the set of homogeneous polynomials f of degree m such that $f(a_1,\ldots,a_r)\in\bigcap_{n\geq 1}\mathfrak{a}^n$, and let $\mathfrak{c}$ be the ideal in $A[X_1,\ldots,X_r]$ generated by all the S_m. According to the lemma, there exists a finite set $\{f_1,\ldots,f_s\}$ of elements of $\bigcup_m S_m$ that generates $\mathfrak{c}$. Let $d_i = \deg f_i$, and let $d = \max d_i$.

Let $b\in\bigcap_{n\geq 1}\mathfrak{a}^n$; then $b\in\mathfrak{a}^{d+1}$, and so $b = f(a_1,\ldots,a_r)$ for some homogeneous polynomial f of degree $d+1$. By definition, $f\in S_{d+1}\subset\mathfrak{a}$, and so

$$f = g_1 f_1 + \cdots + g_s f_s$$

for some $g_i\in A[X_1,\ldots,X_n]$. As f and the f_i are homogeneous, we can omit from each g_i all terms not of degree $\deg f - \deg f_i$, since these terms cancel out. In other words, we may choose the g_i to be homogeneous of degree $\deg f - \deg f_i = d+1-d_i > 0$. In particular, the constant term of g_i is zero, and so $g_i(a_1,\ldots,a_r)\in\mathfrak{a}$. Now

$$b = f(a_1,\ldots,a_r) = \sum_i g_i(a_1,\ldots,a_r)\cdot f_i(a_1,\ldots,a_r)\in\mathfrak{a}\cdot\bigcap_n\mathfrak{a}^n,$$

which completes the proof of (3). □

The equality (3) can also be proved using primary decompositions — see (14.15).

PROPOSITION 3.14. *In a noetherian ring, every ideal contains a power of its radical; in particular, some power of the nilradical of the ring is zero.*

PROOF. Let $a_1, \ldots, a_n$ generate $\mathrm{rad}(\mathfrak{a})$. For each i, some power of a_i, say $a_i^{r_i}$, lies in $\mathfrak{a}$. Then every term of the expansion of

$$(c_1 a_1 + \cdots + c_n a_n)^{r_1 + \cdots + r_n}, \quad c_i \in A,$$

has a factor of the form $a_i^{r_i}$ for some i, and so lies in $\mathfrak{a}$. □

4 Unique factorization

Let A be an integral domain, and let a be an element of A that is neither zero nor a unit. Then a is said to be *irreducible* if it admits only trivial factorizations, i.e.,

$$a = bc \implies b \text{ or } c \text{ is a unit.}$$

The element a is said to be *prime* if (a) is a prime ideal, i.e.,

$$a|bc \implies a|b \text{ or } a|c.$$

An integral domain A is called a *unique factorization domain* if every nonzero nonunit a in A can be written as a finite product of irreducible elements in exactly one way up to units and the order of the factors, i.e., $a = \prod_{i \in I} a_i$ with each a_i irreducible, and if $a = \prod_{j \in J} b_j$ with each b_j irreducible, then there exists a bijection $i \mapsto j(i) \colon I \to J$ such that $b_{j(i)} = a_i \times \text{unit}$ for each i. Every principal ideal domain is a unique factorization domain (proved in most algebra courses).

PROPOSITION 4.1. *Let A be an integral domain, and let a be an element of A that is neither zero nor a unit. If a is prime, then a is irreducible, and the converse holds when A is a unique factorization domain.*

PROOF. Assume that a is prime. If $a = bc$, then a divides bc and so a divides b or c. Suppose the first, and write $b = aq$. Now $a = bc = aqc$, which implies that $qc = 1$ because A is an integral domain, and so c is a unit. Therefore a is irreducible.

For the converse, assume that a is irreducible and that A is a unique factorization domain. If $a|bc$, then

$$bc = aq, \text{ some } q \in A.$$

On writing each of b, c, and q as a product of irreducible elements, and using the uniqueness of factorizations, we see that a differs from one of the irreducible factors of b or c by a unit. Therefore a divides b or c. □

GAUSS'S LEMMA 4.2. *Let A be a unique factorization domain with field of fractions F. If $f(X) \in A[X]$ factors into the product of two nonconstant polynomials in $F[X]$, then it factors into the product of two nonconstant polynomials in $A[X]$.*

PROOF. Let $f = gh$ in $F[X]$. For suitable $c, d \in A$, the polynomials $g_1 = cg$ and $h_1 = dh$ have coefficients in A, and so we have a factorization

$$cdf = g_1 h_1 \text{ in } A[X].$$

If an irreducible element p of A divides cd, then, looking modulo (p), we see that

$$0 = \overline{g_1} \cdot \overline{h_1} \text{ in } (A/(p))[X].$$

According to Proposition 4.1, the ideal (p) is prime, and so $(A/(p))[X]$ is an integral domain. Therefore, p divides all the coefficients of at least one of the polynomials g_1, h_1, say g_1, so that $g_1 = pg_2$ for some $g_2 \in A[X]$. Thus, we have a factorization

$$(cd/p) f = g_2 h_1 \text{ in } A[X].$$

Continuing in this fashion, we can remove all the irreducible factors of cd, and so obtain a factorization of f in $A[X]$. □

The proof shows that every factorization $f = gh$ in $F[X]$ of an element f of $A[X]$ gives a factorization $f = (cg)(c^{-1}h)$ in $A[X]$ for a suitable $c \in F$.

Let A be a unique factorization domain. A nonzero polynomial

$$f = a_0 + a_1 X + \cdots + a_m X^m$$

in $A[X]$ is said to be *primitive* if the coefficients a_i have no common factor other than units. Every polynomial f in $A[X]$ can be written $f = c(f) \cdot f_1$ with $c(f) \in A$ and f_1 primitive. The element $c(f)$, well-defined up to multiplication by a unit, is called the *content* of f.

LEMMA 4.3. *The product of two primitive polynomials is primitive.*

PROOF. Let

$$f = a_0 + a_1 X + \cdots + a_m X^m$$
$$g = b_0 + b_1 X + \cdots + b_n X^n,$$

be primitive polynomials, and let p be an irreducible element of A. Let a_{i_0} be the first coefficient of f not divisible by p and b_{j_0} the first coefficient of g not divisible by p. Then all the terms in $\sum_{i+j=i_0+j_0} a_i b_j$ are divisible by p, except $a_{i_0} b_{j_0}$, which is not divisible by p. Therefore, p doesn't divide the $(i_0 + j_0)$th-coefficient of fg. We have shown that no irreducible element of A divides all the coefficients of fg, which must therefore be primitive. □

LEMMA 4.4. *For polynomials $f, g \in A[X]$, $c(fg) = c(f) \cdot c(g)$; hence every factor in $A[X]$ of a primitive polynomial is primitive.*

PROOF. Let $f = c(f) f_1$ and $g = c(g) g_1$ with f_1 and g_1 primitive. Then

$$fg = c(f) c(g) f_1 g_1$$

with $f_1 g_1$ primitive, and so $c(fg) = c(f) c(g)$. □

PROPOSITION 4.5. *If A is a unique factorization domain, then so also is $A[X]$.*

PROOF. From the factorization $f = c(f)f_1$, we see that the irreducible elements of $A[X]$ are to be found among the constant polynomials and the primitive polynomials, but a constant polynomial a is irreducible if and only if a is an irreducible element of A (obvious) and a primitive polynomial is irreducible if and only if it has no primitive factor of lower degree (by 4.4). From this it is clear that every nonzero nonunit f in $A[X]$ is a product of irreducible elements.

Let

$$f = c_1 \cdots c_m f_1 \cdots f_n = d_1 \cdots d_r g_1 \cdots g_s$$

be two factorizations of an element f of $A[X]$ into irreducible elements with the c_i, d_j constants and the f_i, g_j primitive polynomials. Then

$$c(f) = c_1 \cdots c_m = d_1 \cdots d_r \text{ (up to units in } A).$$

From this it follows that:

(a) $m = r$ and the c_i's differ from the d_i's only by units and ordering, and

(b) $f_1 \cdots f_n = g_1 \cdots g_s$ (up to units in A). Gauss's lemma shows that the f_i, g_j are irreducible polynomials in $F[X]$ and, on using that $F[X]$ is a unique factorization domain, we see that $n = s$ and that the f_i's differ from the g_i's only by units in F and by their ordering. But if $f_i = \frac{a}{b} g_j$ with a and b nonzero elements of A, then $bf_i = ag_j$. As f_i and g_j are primitive, this implies that $b = a$ (up to a unit in A), and hence that $\frac{a}{b}$ is a unit in A. □

Let k be a field. A *monomial* in $X_1, \ldots, X_n$ is an expression of the form

$$X_1^{a_1} \cdots X_n^{a_n}, \quad a_j \in \mathbb{N}.$$

The *total degree* of the monomial is $\sum a_i$. The *degree*, $\deg(f)$, of a nonzero polynomial $f(X_1, \ldots, X_n)$ is the largest total degree of a monomial occurring in f with nonzero coefficient. Since

$$\deg(fg) = \deg(f) + \deg(g),$$

$k[X_1, \ldots, X_n]$ is an integral domain and $k[X_1, \ldots, X_n]^\times = k^\times$. Therefore, an element f of $k[X_1, \ldots, X_n]$ is irreducible if it is nonconstant and $f = gh \implies g$ or h is constant.

THEOREM 4.6. *The ring $k[X_1, \ldots, X_n]$ is a unique factorization domain.*

PROOF. This is trivially true when $n = 0$, and an induction argument using (1), p.10, proves it for all n. □

COROLLARY 4.7. *A nonzero proper principal ideal (f) in $k[X_1, \ldots, X_n]$ is prime if and only f is irreducible.*

PROOF. Special case of (4.1). □

5 Integrality

Let A be a subring of a ring B. An element α of B is said to be *integral* over A if it is a root of a monic[5] polynomial with coefficients in A, i.e., if it satisfies an equation

$$\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$

[5]A polynomial is *monic* if its leading coefficient is 1, i.e., $f(X) = X^n +$ terms of degree less than n.

If every element of B is integral over A, then B is said to be *integral* over A.

In the next proof, we shall need to apply Cramer's formula. As usually stated in linear algebra courses, this says that, if $x_1,\ldots,x_m$ is a solution to the system of linear equations

$$\sum_{j=1}^{m} c_{ij}x_j = d_i,\quad i=1,\ldots,m,$$

then

$$x_j = \frac{\det(C_j)}{\det(C)},\quad \text{where } C=(c_{ij}) \text{ and}$$

$$C_j = \begin{pmatrix} c_{11} & \cdots & c_{1,j-1} & d_1 & c_{1,j+1} & \cdots & c_{1m} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ c_{m1} & \cdots & c_{m,j-1} & d_m & c_{m,j+1} & \cdots & c_{mm} \end{pmatrix}.$$

When one restates the formula as

$$\det(C)\cdot x_j = \det(C_j)$$

it becomes true over any ring (whether or not $\det(C)$ is a unit). The proof is elementary—expand out the right hand side of

$$\det C_j = \det\begin{pmatrix} c_{11} & \ldots & c_{1\,j-1} & \sum c_{1j}x_j & c_{1\,j+1} & \ldots & c_{1m} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ c_{m1} & \ldots & c_{m\,j-1} & \sum c_{mj}x_j & c_{m\,j+1} & \ldots & c_{mm} \end{pmatrix}$$

using standard properties of determinants.

PROPOSITION 5.1. *Let A be a subring of a ring B. An element α of B is integral over A if and only if there exists a faithful*[6] *$A[\alpha]$-submodule M of B that is finitely generated as an A-module.*

PROOF. $\Rightarrow$: Suppose

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0,\quad a_i\in A.$$

Then the A-submodule M of B generated by 1, α, ..., α^{n-1} has the property that $\alpha M\subset M$, and it is faithful because it contains 1.

$\Leftarrow$: Let M be an A-module in B with a finite set $\{e_1,\ldots,e_n\}$ of generators such that $\alpha M\subset M$ and M is faithful as an $A[\alpha]$-module. Then, for each i,

$$\alpha e_i = \sum a_{ij}e_j,\ \text{some } a_{ij}\in A.$$

We can rewrite this system of equations as

$$\begin{aligned} (\alpha - a_{11})e_1 - a_{12}e_2 - a_{13}e_3 - \cdots &= 0\\ -a_{21}e_1 + (\alpha - a_{22})e_2 - a_{23}e_3 - \cdots &= 0\\ \cdots &= 0. \end{aligned}$$

Let C be the matrix of coefficients on the left-hand side. Then Cramer's formula tells us that $\det(C)\cdot e_i = 0$ for all i. As M is faithful and the e_i generate M, this implies that $\det(C)=0$. On expanding out the determinant, we obtain an equation

$$\alpha^n + c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_n = 0,\quad c_i\in A.$$

□

[6] An A-module M is *faithful* if $aM=0$, $a\in A$, implies $a=0$.

PROPOSITION 5.2. *An A-algebra B is finite if and only if it is finitely generated and integral over A.*

PROOF. $\Leftarrow$: Suppose $B = A[\alpha_1,\ldots,\alpha_m]$ and that

$$\alpha_i^{n_i} + a_{i1}\alpha_i^{n_i-1} + \cdots + a_{in_i} = 0, \quad a_{ij} \in A, \quad i = 1,\ldots,m.$$

Any monomial in the α_i's divisible by some $\alpha_i^{n_i}$ is equal (in B) to a linear combination of monomials of lower degree. Therefore, B is generated as an A-module by the monomials $\alpha_1^{r_1}\cdots\alpha_m^{r_m}$, $1 \le r_i < n_i$.

$\Rightarrow$: As an A-module, B is faithful (because $a \cdot 1_B = a$), and so (5.1) show that every element of B is integral over A. As B is finitely generated as an A-module, it is certainly finitely generated as an A-algebra. □

The proof shows that, if an A-algebra B is generated by a finite number of elements each of which is integral over A, then it is finitely generated as an A-module.

THEOREM 5.3. *Let A be a subring of a ring B. The elements of B integral over A form a subring of B.*

PROOF. Let α and β be two elements of B integral over A. As just noted, $A[\alpha,\beta]$ is finitely generated as an A-module. It is stable under multiplication by $\alpha \pm \beta$ and $\alpha\beta$ and it is faithful as an $A[\alpha \pm \beta]$-module and as an $A[\alpha\beta]$-module (because it contains 1_A). Therefore (5.1) shows that $\alpha \pm \beta$ and $\alpha\beta$ are integral over A. □

DEFINITION 5.4. Let A be a subring of the ring B. The *integral closure* of A in B is the subring of B consisting of the elements integral over A.

PROPOSITION 5.5. *Let A be an integral domain with field of fractions F, and let L be a field containing F. If $\alpha \in L$ is algebraic over F, then there exists a $d \in A$ such that $d\alpha$ is integral over A.*

PROOF. By assumption, α satisfies an equation

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0, \quad a_i \in F.$$

Let d be a common denominator for the a_i, so that $da_i \in A$ for all i, and multiply through the equation by d^m:

$$d^m\alpha^m + a_1 d^m \alpha^{m-1} + \cdots + a_m d^m = 0.$$

We can rewrite this as

$$(d\alpha)^m + a_1 d (d\alpha)^{m-1} + \cdots + a_m d^m = 0.$$

As $a_1 d,\ldots,a_m d^m \in A$, this shows that $d\alpha$ is integral over A. □

COROLLARY 5.6. *Let A be an integral domain and let L be an algebraic extension of the field of fractions of A. Then L is the field of fractions of the integral closure of A in L.*

PROOF. In fact, the proposition shows that every element of L is a quotient β/d with β integral over A and $d \in A$. □

DEFINITION 5.7. An integral domain A is *integrally closed* if it is equal to its integral closure in its field of fractions F, i.e., if

$$\alpha \in F, \quad \alpha \text{ integral over } A \implies \alpha \in A.$$

PROPOSITION 5.8. *Every unique factorization domain is integrally closed.*

PROOF. An element of the field of fractions of A not in A can be written a/b with $a, b \in A$ and b divisible by some irreducible element p not dividing a. If a/b is integral over A, then it satisfies an equation

$$(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$

On multiplying through by b^n, we obtain the equation

$$a^n + a_1 a^{n-1} b + \cdots + a_n b^n = 0.$$

The element p then divides every term on the left except a^n, and hence must divide a^n. Since it doesn't divide a, this is a contradiction. □

PROPOSITION 5.9. *Let A be an integrally closed integral domain, and let L be a finite extension of the field of fractions F of A. An element of L is integral over A if and only if its minimum polynomial*[7] *over F has coefficients in A.*

PROOF. Let α be integral over A, so that

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0, \quad \text{some } a_i \in A, \quad m > 0.$$

Let α' be a conjugate of α, i.e., a root of the minimum polynomial $f(X)$ of α over F in some field containing L. Then there is an F-isomorphism[8]

$$\sigma\colon F[\alpha] \to F[\alpha'], \quad \sigma(\alpha) = \alpha'$$

On applying σ to the above equation we obtain the equation

$$\alpha'^m + a_1\alpha'^{m-1} + \cdots + a_m = 0,$$

which shows that α' is integral over A. Hence all the conjugates of α are integral over A, and it follows from (5.3) that the coefficients of $f(X)$ are integral over A. They lie in F, and A is integrally closed, and so they lie in A. This proves the "only if" part of the statement, and the "if" part is obvious. □

COROLLARY 5.10. *Let A be an integrally closed integral domain with field of fractions F, and let $f(X)$ be a monic polynomial in $A[X]$. Then every monic factor of $f(X)$ in $F[X]$ has coefficients in A.*

PROOF. It suffices to prove this for an irreducible monic factor g of f in $F[X]$. Let α be a root of g in some extension field of F. Then g is the minimum polynomial α, which, being also a root of f, is integral. Therefore g has coefficients in A. □

---

[7] Most authors write "minimal polynomial" but the polynomial in question is in fact minimum (smallest element in the set of monic polynomials having α as a root).

[8] Recall that the homomorphism $X \mapsto \alpha\colon F[X] \to F[\alpha]$ defines an isomorphism $F[X]/(f) \to F[\alpha]$.

THEOREM 5.11 (NOETHER NORMALIZATION THEOREM). *Every finitely generated algebra A over a field k contains a polynomial algebra R such that A is a finite R-algebra.*

In other words, there exist elements $y_1, \ldots, y_r$ of A such that A is a finitely generated $k[y_1, \ldots, y_r]$-module and $y_1, \ldots, y_r$ are algebraically independent[9] over k.

PROOF. We use induction on the minimum number n of generators of A as a k-algebra. If $n = 0$, there is nothing to prove, and so we may suppose that $n \geq 1$ and that the statement is true for k-algebras generated by $n-1$ (or fewer) elements.

Let $A = k[x_1, \ldots, x_n]$. If the x_i are algebraically independent, then there is nothing to prove, and so we may suppose that there exists a nonconstant polynomial $f(T_1, \ldots, T_n)$ such that $f(x_1, \ldots, x_n) = 0$. Some T_i occurs in f, say T_1, and we can write

$$f = c_0 T_1^N + c_1 T_1^{N-1} + \cdots + c_N, \quad c_i \in k[T_2, \ldots, T_n], \quad c_0 \neq 0.$$

If $c_0 \in k$, then the equation

$$0 = f(x_1, \ldots, x_n) = c_0 x_1^N + c_1(x_2, \ldots, x_n) x_1^{N-1} + \cdots + c_N(x_2, \ldots, x_n)$$

shows that x_1 is integral over $k[x_2, \ldots, x_n]$. By induction, there exist algebraically independent elements $y_1, \ldots, y_r$ such that $k[x_2, \ldots, x_n]$ is finite over $k[y_1, \ldots, y_r]$. It follows that A is finite over $k[y_1, \ldots, y_r]$ (a composite of finite ring homorphisms is finite).

If $c_0 \notin k$, then we choose different generators for A. Fix an integer $m > 0$, and let

$$y_1 = x_1, y_2 = x_2 - x_1^{m^2}, \ldots, y_r = x_r - x_1^{m^r}.$$

Then

$$k[y_1, \ldots, y_n] = k[x_1, \ldots, x_n] = A$$

because each $y_i \in k[x_1, \ldots, x_n]$ and, conversely, each $x_i \in k[x_1, y_2, \ldots, y_n] = k[y_1, \ldots, y_n]$. Moreover,

$$f(y_1, y_2 + y_1^{m^2}, \ldots, y_r + y_1^{m^r}) = 0.$$

In other words, when we let

$$g(T_1, \ldots, T_n) = f(T_1, T_2 + T_1^{m^2}, \ldots, T_r + T_1^{m^r}) \in k[T_1, \ldots, T_n],$$

$g(y_1, \ldots, y_n) = 0$. I claim that, if m is chosen sufficiently large, then

$$g(T_1, \ldots, T_n) = c_0' T_1^N + c_1' T_1^{N-1} + \cdots + c_N', \quad c_i' \in k[T_2, \ldots, T_r], \quad c_0' \neq 0$$

with $c_0' \in k$, and so the previous argument applies.

To prove the claim, let

$$f(T_1, \ldots, T_r) = \sum c_{j_1 \cdots j_r} T_1^{j_1} \cdots T_r^{j_r}.$$

[9]Recall that this means that the homomorphism of k-algebras $k[X_1, \ldots, X_n] \to k[y_1, \ldots, y_n]$ sending X_i to y_i is an isomorphism, or, equivalently, that if

$$P(y_1, \ldots, y_n) = 0, \quad P(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n],$$

then $P = 0$.

Choose m so large that the numbers

$$j_1 + m^2 j_2 + \cdots + m^r j_r, \tag{1}$$

are distinct when $(j_1, \ldots, j_r)$ runs over the r-tuples with $c_{j_1,\ldots,j_r} \neq 0$. Then

$$f(T_1, T_2 + T_1^{m^2}, \ldots, T_r + T_1^{m^r}) = cT_1^N + c_1 T_1^{N-1} + \cdots$$

with $c \in k \smallsetminus \{0\}$ and N equal to the largest value of (1). □

REMARK 5.12. When k is infinite, there is a simpler proof of a somewhat stronger result: let $A = k[x_1, \ldots, x_n]$; then there exist algebraically independent elements $f_1, \ldots, f_r$ that are *linear combinations* of the x_i such that A is finite over $k[f_1, \ldots, f_r]$ (see 8.13 of my algebraic geometry notes).

6 Rings of fractions

Recall that a multiplicative subset of a ring is a nonempty subset closed under the formation of finite products.

Let S be a multiplicative subset of A, and define an equivalence relation on $A \times S$ by

$$(a,s) \sim (b,t) \iff u(at - bs) = 0 \text{ for some } u \in S.$$

Write $\frac{a}{s}$ for the equivalence class containing (a,s), and define addition and multiplication of equivalence classes according to the rules:

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

It is easily checked these do not depend on the choices of representatives for the equivalence classes, and that we obtain in this way a ring

$$S^{-1}A = \{\tfrac{a}{s} \mid a \in A, s \in S\}$$

and a ring homomorphism $a \mapsto \frac{a}{1} \colon A \xrightarrow{i_S} S^{-1}A$ whose kernel is

$$\{a \in A \mid sa = 0 \text{ for some } s \in S\}.$$

If S contains no zero-divisors, for example, if A is an integral domain and $0 \notin S$, then $i_S \colon A \to S^{-1}A$ is injective. At the opposite extreme, if $0 \in S$, then $S^{-1}A$ is the zero ring.

PROPOSITION 6.1. *The pair $(S^{-1}A, i_S)$ has the following universal property:*

every element of S maps to a unit in $S^{-1}A$, and any other ring homomorphism $A \to B$ with this property factors uniquely through i_S

$$\begin{array}{ccc} A & \xrightarrow{i_S} & S^{-1}A \\ & \searrow & \downarrow{\scriptstyle \exists!} \\ & & B. \end{array}$$

PROOF. Let $\alpha \colon A \to B$ be a homomorphism, and let $\beta \colon S^{-1}A \to B$ be a homomorphism such that $\beta \circ i_S = \alpha$. Then

$$\frac{s}{1}\frac{a}{s} = \frac{a}{1} \implies \beta(\tfrac{s}{1})\beta(\tfrac{a}{s}) = \beta(\tfrac{a}{1}),$$

and so

$$\beta(\tfrac{a}{s}) = \alpha(a)\alpha(s)^{-1}. \tag{1}$$

This shows that there can be at most one β such that $\beta \circ i_S = \alpha$. When α maps the elements of S to units in B, we define β by the formula (1). Then

$$\tfrac{a}{s} = \tfrac{b}{t} \implies u(at - bs) = 0 \text{ some } u \in S \overset{\alpha(u)\in B^\times}{\implies} \alpha(a)\alpha(t) - \alpha(b)\alpha(s) = 0,$$

which shows that β is well-defined, and it is easy to check that it is a homomorphism. □

As usual, this universal property determines the pair $(S^{-1}A, i_S)$ uniquely up to a unique isomorphism.[10]

When A is an integral domain and $S = A \smallsetminus \{0\}$, the ring $S^{-1}A$ is the field of fractions F of A. In this case, for any other multiplicative subset T of A not containing 0, the ring $T^{-1}A$ can be identified with the subring of F consisting of the fractions $\frac{a}{t}$ with $a \in A$ and $t \in T$.

EXAMPLE 6.2. Let $h \in A$. Then $S_h = \{1, h, h^2, \ldots\}$ is a multiplicative subset of A, and we let $A_h = S_h^{-1}A$. Thus every element of A_h can be written in the form a/h^m, $a \in A$, and

$$\tfrac{a}{h^m} = \tfrac{b}{h^n} \iff h^N(ah^n - bh^m) = 0, \quad \text{some } N.$$

If h is nilpotent, then $A_h = 0$, and if A is an integral domain with field of fractions F and $h \neq 0$, then A_h is the subring of F of elements of the form a/h^m, $a \in A$, $m \in \mathbb{N}$.

PROPOSITION 6.3. *For any ring A and $h \in A$, the map $\sum a_i X^i \mapsto \sum \frac{a_i}{h^i}$ defines an isomorphism*

$$A[X]/(1 - hX) \to A_h.$$

PROOF. If $h = 0$, both rings are zero, and so we may assume $h \neq 0$. In the ring $A[x] = A[X]/(1 - hX)$, $1 = hx$, and so h is a unit. Let $\alpha\colon A \to B$ be a homomorphism of rings such that $\alpha(h)$ is a unit in B. The homomorphism $\sum a_i X^i \mapsto \sum \alpha(a_i)\alpha(h)^{-i}\colon A[X] \to B$ factors through $A[x]$ because $1 - hX \mapsto 1 - \alpha(h)\alpha(h)^{-1} = 0$, and this is the unique extension of α to $A[x]$. Therefore $A[x]$ has the same universal property as A_h, and so the two are (uniquely) isomorphic by an A-algebra isomorphism that makes h^{-1} correspond to x. □

Let S be a multiplicative subset of a ring A, and let $S^{-1}A$ be the corresponding ring of fractions. For any ideal $\mathfrak{a}$ in A, the ideal generated by the image of $\mathfrak{a}$ in $S^{-1}A$ is

$$S^{-1}\mathfrak{a} = \{\tfrac{a}{s} \mid a \in \mathfrak{a}, \quad s \in S\}.$$

If $\mathfrak{a}$ contains an element of S, then $S^{-1}\mathfrak{a}$ contains 1, and so is the whole ring. Thus some of the ideal structure of A is lost in the passage to $S^{-1}A$, but, as the next lemma shows, some is retained.

[10]Recall the proof: let (A_1, i_1) and (A_2, i_2) have the universal property in the proposition; because every element of S maps to a unit in A_2, there exists a unique homomorphism $\alpha\colon A_1 \to A_2$ such that $\alpha \circ i_1 = i_2$ (universal property of A_1, i_1); similarly, there exists a unique homomorphism $\alpha'\colon A_2 \to A_1$ such that $\alpha' \circ i_2 = i_1$; now

$$\alpha' \circ \alpha \circ i_1 = \alpha' \circ i_2 = i_1 = \mathrm{id}_{A_1} \circ i_1,$$

and so $\alpha' \circ \alpha = \mathrm{id}_{A_1}$ (universal property of A_1, i_1); similarly, $\alpha \circ \alpha' = \mathrm{id}_{A_2}$, and so α and α' are inverse isomorphisms (and they are uniquely determined by the conditions $\alpha \circ i_1 = i_2$ and $\alpha' \circ i_2 = i_1$).

PROPOSITION 6.4. *Let S be a multiplicative subset of the ring A, and consider extension $\mathfrak{a} \mapsto \mathfrak{a}^e = S^{-1}\mathfrak{a}$ and contraction $\mathfrak{a} \mapsto \mathfrak{a}^c = \{a \in A \mid \frac{a}{1} \in \mathfrak{a}\}$ of ideals with respect to the homomorphism $A \to S^{-1}A$. Then*

$$\mathfrak{a}^{ce} = \mathfrak{a} \qquad \text{for all ideals of } S^{-1}A$$
$$\mathfrak{a}^{ec} = \mathfrak{a} \qquad \text{if } \mathfrak{a} \text{ is a prime ideal of } A \text{ disjoint from } S.$$

Moreover, the $\mathfrak{p} \mapsto \mathfrak{p}^e$ is a bijection from the set of prime ideals of A disjoint from S onto the set of all prime ideals of $S^{-1}A$; the inverse map is $\mathfrak{p} \mapsto \mathfrak{p}^c$.

PROOF. Let $\mathfrak{a}$ be an ideal in $S^{-1}A$. Certainly $\mathfrak{a}^{ce} \subset \mathfrak{a}$. For the reverse inclusion, let $b \in \mathfrak{a}$. We can write $b = \frac{a}{s}$ with $a \in A$, $s \in S$. Then $\frac{a}{1} = s(\frac{a}{s}) \in \mathfrak{a}$, and so $a \in \mathfrak{a}^c$. Thus $b = \frac{a}{s} \in \mathfrak{a}^{ce}$, and so $\mathfrak{a} \subset \mathfrak{a}^{ce}$.

Let $\mathfrak{p}$ be a prime ideal of A disjoint from S. Clearly $\mathfrak{p}^{ec} \supset \mathfrak{p}$. For the reverse inclusion, let $a \in \mathfrak{p}^{ec}$ so that $\frac{a}{1} = \frac{a'}{s}$ for some $a' \in \mathfrak{p}$, $s \in S$. Then $t(as - a') = 0$ for some $t \in S$, and so $ast \in \mathfrak{p}$. Because $st \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime, this implies that $a \in \mathfrak{p}$, and so $\mathfrak{p}^{ec} \subset \mathfrak{p}$.

Let $\mathfrak{p}$ be a prime ideal of A disjoint from S, and let $\bar{S}$ be the image of S in $A/\mathfrak{p}$. Then $(S^{-1}A)/\mathfrak{p}^e \simeq \bar{S}^{-1}(A/\mathfrak{p})$ because $S^{-1}A/\mathfrak{p}^e$ has the correct universal property, and $\bar{S}^{-1}(A/\mathfrak{p})$ is an integral domain because $A/\mathfrak{p}$ is an integral domain and $\bar{S}$ doesn't contain 0. Therefore $\mathfrak{p}^e$ is prime. From §2 we know that $\mathfrak{p}^c$ is prime if $\mathfrak{p}$ is, and so $\mathfrak{p} \mapsto \mathfrak{p}^e$ and $\mathfrak{p} \mapsto \mathfrak{p}^c$ are inverse bijections on the two sets. □

COROLLARY 6.5. *If A is noetherian, then so also is $S^{-1}A$ for any multiplicative set S.*

PROOF. As $\mathfrak{b}^c$ is finitely generated, so also is $(\mathfrak{b}^c)^e = \mathfrak{b}$. □

EXAMPLE 6.6. Let $\mathfrak{p}$ be a prime ideal in A. Then $S_\mathfrak{p} = A \smallsetminus \mathfrak{p}$ is a multiplicative subset of A, and we let $A_\mathfrak{p} = S_\mathfrak{p}^{-1}A$. Thus each element of $A_\mathfrak{p}$ can be written in the form $\frac{a}{c}$, $c \notin \mathfrak{p}$, and

$$\tfrac{a}{c} = \tfrac{b}{d} \iff s(ad - bc) = 0, \text{ some } s \notin \mathfrak{p}.$$

According to (6.4), the prime ideals of $A_\mathfrak{p}$ correspond to the prime ideals of A disjoint from $A \smallsetminus \mathfrak{p}$, i.e., contained in $\mathfrak{p}$. Therefore, $A_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{m} = \mathfrak{p}^e = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}$.

PROPOSITION 6.7. *Let $\mathfrak{m}$ be a maximal ideal of a noetherian ring A, and let $\mathfrak{n} = \mathfrak{m}A_\mathfrak{m}$ be the maximal ideal of $A_\mathfrak{m}$. For all n, the map*

$$a + \mathfrak{m}^n \mapsto a + \mathfrak{n}^n \colon A/\mathfrak{m}^n \to A_\mathfrak{m}/\mathfrak{n}^n$$

is an isomorphism. Moreover, it induces isomorphisms

$$\mathfrak{m}^r/\mathfrak{m}^n \to \mathfrak{n}^r/\mathfrak{n}^n$$

for all pairs (r, n) with $r \le n$.

PROOF. The second statement follows from the first, because of the exact commutative diagram ($r < n$):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{m}^r/\mathfrak{m}^n & \longrightarrow & A/\mathfrak{m}^n & \longrightarrow & A/\mathfrak{m}^r & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow\simeq & & \downarrow\simeq & & \\
0 & \longrightarrow & \mathfrak{n}^r/\mathfrak{n}^n & \longrightarrow & A_\mathfrak{m}/\mathfrak{n}^n & \longrightarrow & A_\mathfrak{m}/\mathfrak{n}^r & \longrightarrow & 0.
\end{array}$$

We consider extension and contraction with respect to $a \mapsto \frac{a}{1}: A \to A_{\mathfrak{m}}$. In order to show that the map $A/\mathfrak{m}^n \to A_{\mathfrak{m}}/\mathfrak{n}^n$ is injective, we have to show that $(\mathfrak{m}^n)^{ec} = \mathfrak{m}^n$. If $a \in (\mathfrak{m}^n)^{ec}$, then $\frac{a}{1} = \frac{b}{s}$ with $b \in \mathfrak{m}^n$ and $s \in S$. Then $s'sa \in \mathfrak{m}^n$ for some $s' \in S$, and so $s'sa = 0$ in $A/\mathfrak{m}^n$. The only maximal ideal containing $\mathfrak{m}^n$ is $\mathfrak{m}$, and so the only maximal ideal in $A/\mathfrak{m}^n$ is $\mathfrak{m}/\mathfrak{m}^n$. As $s's$ is not in $\mathfrak{m}/\mathfrak{m}^n$, it must be a unit in $A/\mathfrak{m}^n$, and so $a = 0$ in $A/\mathfrak{m}^n$, i.e., $a \in \mathfrak{m}^n$. We have shown that $(\mathfrak{m}^n)^{ec} \subset \mathfrak{m}$, and the reverse inclusion is always true.

We now prove that $A/\mathfrak{m}^n \to A_{\mathfrak{m}}/\mathfrak{n}^n$ is surjective. Let $\frac{a}{s} \in A_{\mathfrak{m}}$, $a \in A$, $s \in A \setminus \mathfrak{m}$. The only maximal ideal of A containing $\mathfrak{m}^n$ is $\mathfrak{m}$, and so no maximal ideal contains both s and $\mathfrak{m}^n$; it follows that $(s) + \mathfrak{m}^n = A$. Therefore, there exist $b \in A$ and $q \in \mathfrak{m}^n$ such that $sb + q = 1$. Because s is invertible in $A_{\mathfrak{m}}/\mathfrak{n}^n$, $\frac{a}{s}$ is the *unique* element of this ring such that $s\frac{a}{s} = a$. As $s(ba) = a(1-q)$, the image of ba in $A_{\mathfrak{m}}$ also has this property and therefore equals $\frac{a}{s}$. □

PROPOSITION 6.8. *In a noetherian ring, only* 0 *lies in all powers of all maximal ideals.*

PROOF. Let a be an element of a noetherian ring A. If $a \neq 0$, then $\mathrm{ann}(a) = \{b \mid ba = 0\}$ is a proper ideal, and so it is contained in some maximal ideal $\mathfrak{m}$. Then $\frac{a}{1}$ is nonzero in $A_{\mathfrak{m}}$, and so $\frac{a}{1} \notin (\mathfrak{m}A_{\mathfrak{m}})^n$ for some n (by the Krull intersection theorem 3.13), which implies that $a \notin \mathfrak{m}^n$ (by 6.7). □

MODULES OF FRACTIONS

Let S be a multiplicative subset of the ring A, and let M be an A-module. Define an equivalence relation on $M \times S$ by

$$(m,s) \sim (n,t) \iff u(mt - ns) = 0 \text{ for some } u \in S.$$

Write $\frac{m}{s}$ for the equivalence class containing (m,s), and define addition and multiplication of equivalence classes by the rules:

$$\frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st}, \quad \frac{a}{s}\frac{m}{t} = \frac{am}{st}, \quad m,n \in M, \quad s,t \in S, \quad a \in A.$$

It is easily y to show that these definitions do not depend on the choices of representatives for the equivalence classes, and that we obtain in this way an $S^{-1}A$-module

$$S^{-1}M = \{\tfrac{m}{s} \mid m \in M, s \in S\}$$

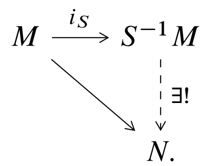
and a homomorphism $m \mapsto \frac{m}{1}: M \xrightarrow{i_S} S^{-1}M$ of A-modules whose kernel is

$$\{a \in M \mid sa = 0 \text{ for some } s \in S\}.$$

EXAMPLE 6.9. Let M be an A-module. For $h \in A$, let $M_h = S_h^{-1}M$ where $S_h = \{1, h, h^2, \ldots\}$. Then every element of M_h can be written in the form $\frac{m}{h^r}$, $m \in M$, $r \in \mathbb{N}$, and $\frac{m}{h^r} = \frac{m'}{h^{r'}}$ if and only if $h^N(h^{r'}m - h^r m') = 0$ for some $N \in \mathbb{N}$.

PROPOSITION 6.10. *The pair* $(S^{-1}M, i_S)$ *has the following universal property:*

every element of S acts invertibly on $S^{-1}M$, and any other homomorphism $M \to N$ of A-modules such that the elements of S act invertibly on N factors uniquely through i_S



PROOF. Similar to that of Proposition 6.1. □

In particular, for any homomorphism $\alpha\colon M \to N$ of A-modules, there is a unique homomorphism $S^{-1}\alpha\colon S^{-1}M \to S^{-1}N$ such that $S^{-1}\alpha \circ i_S = i_S \circ \alpha$:

$$\begin{array}{ccc} M & \xrightarrow{i_S} & S^{-1}M \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle S^{-1}\alpha} \\ N & \xrightarrow{i_S} & S^{-1}N. \end{array}$$

In this way, $M \rightsquigarrow S^{-1}M$ becomes a functor.

PROPOSITION 6.11. *The functor $M \rightsquigarrow S^{-1}M$ is exact. In other words, if the sequence of A-modules*

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$$

is exact, then so also is the sequence of $S^{-1}A$-modules

$$S^{-1}M' \xrightarrow{S^{-1}\alpha} S^{-1}M \xrightarrow{S^{-1}\beta} S^{-1}M''.$$

PROOF. Because $\beta \circ \alpha = 0$, we have $0 = S^{-1}(\beta \circ \alpha) = S^{-1}\beta \circ S^{-1}\alpha$. Therefore $\mathrm{Im}(S^{-1}\alpha) \subset \mathrm{Ker}(S^{-1}\beta)$. For the reverse inclusion, let $\frac{m}{s} \in \mathrm{Ker}(S^{-1}\beta)$ where $m \in M$ and $s \in S$. Then $\frac{\beta(m)}{s} = 0$ and so, for some $t \in S$, we have $t\beta(m) = 0$. Then $\beta(tm) = 0$, and so $tm = \alpha(m')$ for some $m' \in M'$. Now

$$\frac{m}{s} = \frac{tm}{ts} = \frac{\alpha(m')}{ts} \in \mathrm{Im}(S^{-1}\alpha).$$ □

EXERCISE 6.12. A multiplicative subset S of a ring A is said to be *saturated* if

$$ab \in S \Rightarrow a \text{ and } b \in S.$$

(a) Show that the saturated multiplicative subsets of A are exactly the subsets S such that $A \smallsetminus S$ is a union of prime ideals.
(b) Let S be a multiplicative subset of A, and let $\tilde{S}$ be the set of $a \in A$ such that $ab \in S$ for some $b \in A$. Show that $\tilde{S}$ is a saturated multiplicative subset of A (hence it is the smallest such subset containing S), and that $A \smallsetminus \tilde{S}$ is the union of the prime ideals of A not meeting S. Show that for any A-module M, the canonical homomorphism $S^{-1}M \to \tilde{S}^{-1}M$ is bijective. (Cf. Bourbaki AC, II §2, Exercises 1,2.)

7 Direct limits

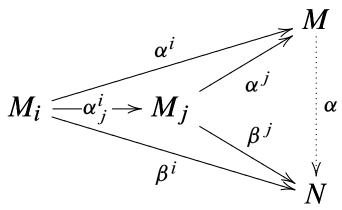
DEFINITION 7.1. A partial ordering $\leq$ on a set I is said to be *directed*, and the pair $(I, \leq)$ is called a *directed set*, if for all $i, j \in I$ there exists a $k \in I$ such that $i, j \leq k$.

DEFINITION 7.2. Let $(I, \leq)$ be a directed set, and let A be a ring.

A *direct system* of A-modules indexed by $(I, \leq)$ is a family $(M_i)_{i \in I}$ of A-modules together with a family $(\alpha^i_j\colon M_i \to M_j)_{i \leq j}$ of A-linear maps such that $\alpha^i_i = \mathrm{id}_{M_i}$ and $\alpha^j_k \circ \alpha^i_j = \alpha^i_k$ all $i \leq j \leq k$.

$$\begin{array}{ccccc} & & & & M_k \\ & & {\scriptstyle \alpha^i_k} \nearrow & & \nearrow {\scriptstyle \alpha^j_k} \\ M_i & & \xrightarrow[\alpha^i_j]{} & & M_j \end{array}$$

An A-module M together with a family $(\alpha^i: M_i \to M)_{i\in I}$ of A-linear maps satisfying $\alpha^i = \alpha^j \circ \alpha^i_j$ all $i \le j$ is said to be a *direct limit* of the system $((M_i), (\alpha^i_j))$ if it has the following universal property: for any other A-module N and family $(\beta^i: M_i \to N)$ of A-linear maps such that $\beta^i = \beta^j \circ \alpha^i_j$ all $i \le j$, there exists a unique morphism $\alpha: M \to N$ such that $\alpha \circ \alpha^i = \beta^i$ for all i.



As usual, the universal property determines the direct limit (if it exists) uniquely up to a unique isomorphism. We denote it $\varinjlim(M_i, \alpha^j_i)$, or just $\varinjlim M_i$.

CRITERION

An A-module M together with A-linear maps $\alpha^i: M_i \to M$ is the direct limit of a system (M_i, α^j_i) if and only if

(a) $M = \bigcup_{i\in I} \alpha^i(M_i)$, and

(b) $m_i \in M_i$ maps to zero in M if and only if it maps to zero in M_j for some $j \ge i$.

CONSTRUCTION

Let

$$M = \bigoplus_{i\in I} M_i / M'$$

where M' is the A-submodule generated by the elements

$$m_i - \alpha^i_j(m_i) \quad \text{all } i < j,\ m_i \in M_i.$$

Let $\alpha^i(m_i) = m_i + M'$. Then certainly $\alpha^i = \alpha^j \circ \alpha^i_j$ for all $i \le j$. For any A-module N and A-linear maps $\beta^j: M_j \to N$, there is a unique map

$$\bigoplus_{i\in I} M_i \to N,$$

namely, $\sum m_i \mapsto \sum \beta^i(m_i)$, sending m_i to $\beta^i(m_i)$, and this map factors through M and is the unique A-linear map with the required properties.

Direct limits of A-algebras, etc., are defined similarly.

AN EXAMPLE

PROPOSITION 7.3. *For any multiplicative subset S of a ring A, $S^{-1}A \simeq \varinjlim A_h$, where h runs over the elements of S (partially ordered by division).*

PROOF. When $h|h'$, say, $h' = hg$, there is a unique homomorphism $A_h \to A_{h'}$ respecting the maps $A \to A_h$ and $A \to A_{h'}$, namely, $\frac{a}{h} \mapsto \frac{ag}{h'}$, and so the rings A_h form a direct system indexed by the set S. When $h \in S$, the homomorphism $A \to S^{-1}A$ extends uniquely to a homomorphism $\frac{a}{h} \mapsto \frac{a}{h}: A_h \to S^{-1}A$ (see 6.1), and these homomorphisms are compatible with the maps in the direct system. Now apply the criterion p.25 to see that $S^{-1}A$ is the direct limit of the A_h. □

8 Tensor Products

TENSOR PRODUCTS OF MODULES

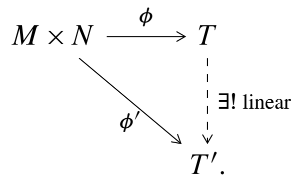
Let A be a ring, and let M, N, and P be A-modules. A map $\phi\colon M\times N\to P$ of A-modules is said to be *A-bilinear* if

$$\begin{aligned}
\phi(x+x',y)&=\phi(x,y)+\phi(x',y), && x,x'\in M,\quad y\in N\\
\phi(x,y+y')&=\phi(x,y)+\phi(x,y'), && x\in M,\quad y,y'\in N\\
\phi(ax,y)&=a\phi(x,y), && a\in A,\quad x\in M,\quad y\in N\\
\phi(x,ay)&=a\phi(x,y), && a\in A,\quad x\in M,\quad y\in N,
\end{aligned}$$

i.e., if ϕ is A-linear in each variable.

An A-module T together with an A-bilinear map

$$\phi\colon M\times N\to T$$



is called the *tensor product* of M and N over A if it has the following universal property: every A-bilinear map

$$\phi'\colon M\times N\to T'$$

factors uniquely through ϕ.

As usual, the universal property determines the tensor product uniquely up to a unique isomorphism. We write it $M\otimes_A N$. Note that

$$\mathrm{Hom}_{A\text{-bilinear}}(M\times N,T)\simeq \mathrm{Hom}_{A\text{-linear}}(M\otimes_A N,T).$$

Construction

Let M and N be A-modules, and let $A^{(M\times N)}$ be the free A-module with basis $M\times N$. Thus each element $A^{(M\times N)}$ can be expressed uniquely as a finite sum

$$\sum a_i(x_i,y_i),\quad a_i\in A,\quad x_i\in M,\quad y_i\in N.$$

Let P be the submodule of $A^{(M\times N)}$ generated by the following elements

$$\begin{aligned}
(x+x',y)-(x,y)-(x',y), &\quad x,x'\in M,\quad y\in N\\
(x,y+y')-(x,y)-(x,y'), &\quad x\in M,\quad y,y'\in N\\
(ax,y)-a(x,y), &\quad a\in A,\quad x\in M,\quad y\in N\\
(x,ay)-a(x,y), &\quad a\in A,\quad x\in M,\quad y\in N,
\end{aligned}$$

and define

$$M\otimes_A N=A^{(M\times N)}/P.$$

Write $x\otimes y$ for the class of (x,y) in $M\otimes_A N$. Then

$$(x,y)\mapsto x\otimes y\colon M\times N\to M\otimes_A N$$

is A-bilinear — we have imposed the fewest relations necessary to ensure this. Every element of $M \otimes_A N$ can be written as a finite sum[11]

$$\sum a_i(x_i \otimes y_i), \quad a_i \in A, \quad x_i \in M, \quad y_i \in N,$$

and all relations among these symbols are generated by the following relations

$$\begin{aligned}(x+x')\otimes y &= x\otimes y + x'\otimes y\\ x\otimes(y+y') &= x\otimes y + x\otimes y'\\ a(x\otimes y) &= (ax)\otimes y = x\otimes ay.\end{aligned}$$

The pair $(M \otimes_A N, (x,y) \mapsto x \otimes y)$ has the correct universal property because any bilinear map $\phi' \colon M \times N \to T'$ defines an A-linear map $A^{(M\times N)} \to T'$, which factors through $A^{(M\times N)}/K$, and gives a commutative triangle.

Extension of scalars

Let A be a commutative ring and let B be an A-algebra (not necessarily commutative) such that the image of $A \to B$ lies in the centre of B. Then $M \rightsquigarrow B \otimes_A M$ is a functor from left A-modules to left B-modules, which has the following universal property:

$$\operatorname{Hom}_{A\text{-linear}}(M,N) \simeq \operatorname{Hom}_{B\text{-linear}}(B \otimes_A M, N), \quad N \text{ a } B\text{-module}. \tag{1}$$

If $(e_\alpha)_{\alpha\in I}$ is a family of generators (resp. basis) for M as an A-module, then $(1 \otimes e_\alpha)_{\alpha \in I}$ is a family of generators (resp. basis) for $B \otimes_A M$ as a B-module.

Behaviour with respect to direct limits

PROPOSITION 8.1. *Direct limits commute with tensor products:*

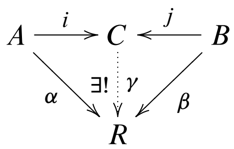
$$\varinjlim_{i\in I} M_i \otimes_A \varinjlim_{j\in J} N_j \simeq \varinjlim_{(i,j)\in I\times J} M_i \otimes_A N_j.$$

PROOF. Using the universal properties of direct limits and tensor products, one sees easily that $\varinjlim(M_i \otimes_A N_j)$ has the universal property to be the tensor product of $\varinjlim M_i$ and $\varinjlim N_j$. □

TENSOR PRODUCTS OF ALGEBRAS

Let k be a ring, and let A and B be k-algebras. A k-algebra C together with homomorphisms $i \colon A \to C$ and $j \colon B \to C$ is called the *tensor product* of A and B if it has the following universal property:

for every pair of homomorphisms (of k-algebras) $\alpha \colon A \to R$ and $\beta \colon B \to R$, there exists a unique homomorphism $\gamma \colon C \to R$ such that $\gamma \circ i = \alpha$ and $\gamma \circ j = \beta$,



If it exists, the tensor product, is uniquely determined up to a unique isomorphism by this property. We write it $A \otimes_k B$. Note that the universal property says that

$$\operatorname{Hom}_{k\text{-algebra}}(A \otimes_k B, R) \simeq \operatorname{Hom}_{k\text{-algebra}}(A,R) \times \operatorname{Hom}_{k\text{-algebra}}(B,R). \tag{2}$$

[11]"An element of the tensor product of two vector spaces is not necessarily a tensor product of two vectors, but sometimes a sum of such. This might be considered a mathematical shenanigan but if you start with the state vectors of two quantum systems it exactly corresponds to the notorious notion of entanglement which so displeased Einstein." Georges Elencwajg on mathoverflow.net.

Construction

Regard A and B as k-modules, and form the tensor product $A\otimes_k B$. There is a multiplication map $A\otimes_k B\times A\otimes_k B\to A\otimes_k B$ for which

$$(a\otimes b)(a'\otimes b')=aa'\otimes bb',\quad \text{all } a,a'\in A,\quad b,b'\in B.$$

This makes $A\otimes_k B$ into a ring, and the homomorphism

$$c\mapsto c(1\otimes 1)=c\otimes 1=1\otimes c$$

makes it into a k-algebra. The maps

$$a\mapsto a\otimes 1\colon A\to A\otimes_k B \text{ and } b\mapsto 1\otimes b\colon B\to A\otimes_k B$$

are homomorphisms, and they make $A\otimes_k B$ into the tensor product of A and B in the above sense.

EXAMPLE 8.2. The algebra A, together with the maps

$$k\longrightarrow A\xleftarrow{\mathrm{id}_A}A,$$

is $k\otimes_k A$ (because it has the correct universal property). In terms of the constructive definition of tensor products, the map $c\otimes a\mapsto ca\colon k\otimes_k A\to A$ is an isomorphism.

EXAMPLE 8.3. The ring $k[X_1,\ldots,X_m,X_{m+1},\ldots,X_{m+n}]$, together with the obvious inclusions

$$k[X_1,\ldots,X_m]\quad\hookrightarrow\quad k[X_1,\ldots,X_{m+n}]\quad\hookleftarrow\quad k[X_{m+1},\ldots,X_{m+n}]$$

is the tensor product of the k-algebras $k[X_1,\ldots,X_m]$ and $k[X_{m+1},\ldots,X_{m+n}]$. To verify this we only have to check that, for every k-algebra R, the map

$$\mathrm{Hom}_{k\text{-alg}}(k[X_1,\ldots,X_{m+n}],R)\to\mathrm{Hom}_{k\text{-alg}}(k[X_1,\ldots],R)\times\mathrm{Hom}_{k\text{-alg}}(k[X_{m+1},\ldots],R)$$

induced by the inclusions is a bijection. But this map can be identified with the bijection

$$R^{m+n}\to R^m\times R^n.$$

In terms of the constructive definition of tensor products, the map

$$k[X_1,\ldots,X_m]\otimes_k k[X_{m+1},\ldots,X_{m+n}]\to k[X_1,\ldots,X_{m+n}]$$

sending $f\otimes g$ to fg is an isomorphism.

REMARK 8.4. (a) Let $k\hookrightarrow k'$ be a homomorphism of rings. Then

$$k'\otimes_k k[X_1,\ldots,X_n]\simeq k'[1\otimes X_1,\ldots,1\otimes X_n]\simeq k'[X_1,\ldots,X_n].$$

If $A=k[X_1,\ldots,X_n]/(g_1,\ldots,g_m)$, then

$$k'\otimes_k A\simeq k'[X_1,\ldots,X_n]/(g_1,\ldots,g_m).$$

(b) If A and B are algebras of k-valued functions on sets S and T respectively, then the definition

$$(f\otimes g)(x,y)=f(x)g(y),\quad f\in A,\ g\in B,\ x\in S,\ y\in T,$$

realizes $A\otimes_k B$ as an algebra of k-valued functions on $S\times T$.

THE TENSOR ALGEBRA OF A MODULE

Let M be a module over a ring A. For each $A \geq 0$, set

$$T^r M = M \otimes_A \cdots \otimes_A M \qquad (r \text{ factors}),$$

so that $T^0 M = A$ and $T^1 M = M$, and define

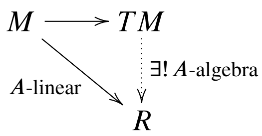
$$TM = \bigoplus\nolimits_{r \geq 0} T^r M.$$

This can be made into a noncommutative A-algebra, called the *tensor algebra* of M, by requiring that the multiplication map

$$T^r M \times T^s M \to T^{r+s} M$$

send $(m_1 \otimes \cdots \otimes m_r, m_{r+1} \otimes \cdots \otimes m_{r+s})$ to $m_1 \otimes \cdots \otimes m_{r+s}$.

The pair $(TM, M \to TM)$ has the following universal property: any A-linear map from M to an A-algebra R (not necessarily commutative) extends uniquely to an A-algebra homomorphism $TM \to R$.



If M is a free A-module with basis $x_1, \ldots, x_n$, then TM is the (noncommutative) polynomial ring over A in the noncommuting symbols x_i (because this A-algebra has the same universal property as TM).

THE SYMMETRIC ALGEBRA OF A MODULE

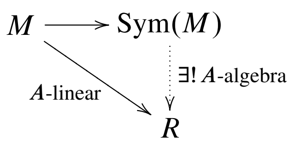
The *symmetric algebra* $\mathrm{Sym}(M)$ of an A-module M is the quotient of TM by the ideal generated by all elements of $T^2 M$ of the form

$$m \otimes n - n \otimes m, \quad m, n \in M.$$

It is a graded algebra $\mathrm{Sym}(M) = \bigoplus_{r \geq 0} \mathrm{Sym}^r(M)$ with $\mathrm{Sym}^r(M)$ equal to the quotient of $M^{\otimes r}$ by the A-submodule generated by all elements of the form

$$m_1 \otimes \cdots \otimes m_r - m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(r)}, \quad m_i \in M, \quad \sigma \in B_r \text{ (symmetric group).}$$

The pair $(\mathrm{Sym}(M), M \to \mathrm{Sym}(M))$ has the following universal property: any A-linear map $M \to R$ from M to a commutative A-algebra R extends uniquely to an A-algebra homomorphism $\mathrm{Sym}(M) \to R$ (because it extends to an A-algebra homomorphism $TM \to R$, which factors through $\mathrm{Sym}(M)$ because R is commutative).



If M is a free A-module with basis $x_1, \ldots, x_n$, then $\mathrm{Sym}(M)$ is the polynomial ring over A in the (commuting) symbols x_i (because this A-algebra has the same universal property as TM).

9 Flatness

Let M be an A-module. If the sequence of A-modules

$$0 \to N' \to N \to N'' \to 0 \tag{1}$$

is exact, then the sequence

$$M \otimes_A N' \to M \otimes_A N \to M \otimes_A N'' \to 0$$

is exact, but $M \otimes_A N' \to M \otimes_A N$ need not be injective. For example, when we tensor the exact sequence of $\mathbb{Z}$-modules

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

with $\mathbb{Z}/m\mathbb{Z}$, we get the sequence

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{m=0} \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \to 0.$$

Moreover, $M \otimes_A N$ may be zero even when neither M nor N is nonzero. For example,

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$$

because it is killed by both 2 and 3.[12]

DEFINITION 9.1. An A-module M is *flat* if

$$N' \to N \text{ injective } \implies M \otimes_A N' \to M \otimes_A N \text{ injective.}$$

It is *faithfully flat* if, in addition,

$$M \otimes_A N = 0 \implies N = 0.$$

A homomorphism of rings $A \to B$ is said to be (*faithfully*) *flat* when B is (faithfully) flat as an A-module.

Thus, an A-module M is flat if and only if $M \otimes_A -$ is an exact functor, i.e.,

$$0 \to M \otimes_A N' \to M \otimes_A N \to M \otimes_A N'' \to 0 \tag{2}$$

is exact whenever (1) is exact.

The functor $M \otimes -$ takes direct sums to direct sums, and therefore split-exact sequences to split-exact sequences. Therefore, all vector spaces over a field are flat, and nonzero vector spaces are faithfully flat.

PROPOSITION 9.2. *Let $A \to B$ be a faithfully flat homomorphism of rings. A sequence of A-modules*

$$0 \to N' \to N \to N'' \to 0 \tag{3}$$

is exact if

$$0 \to B \otimes_A N' \to B \otimes_A N \to B \otimes_A N'' \to 0 \tag{4}$$

is exact.

[12] It was once customary to require a ring to have an identity element $1 \neq 0$ (see, for example, Northcott 1953, p.3). However, the example shows that tensor products do not always exist in the category of such objects, .

PROOF. Let N_0 be the kernel of $N' \to N$. Because $A \to B$ is flat, $B \otimes_A N_0$ is the kernel of $B \otimes_A N' \to B \otimes_A N$, which is zero by assumption; because $A \to B$ is *faithfully* flat, this implies that $N_0 = 0$. We have proved the exactness at N', and the proof of the exactness elsewhere is similar. □

REMARK 9.3. There is a converse to the proposition: suppose that

$$(3) \text{ is exact } \Leftrightarrow (4) \text{ is exact;}$$

then $A \to B$ is faithfully flat. The implication "⇒" shows that $A \to B$ is flat. Now let N be an A-module, and consider the sequence

$$0 \to 0 \to N \to 0 \to 0.$$

If $B \otimes_A N = 0$, then this sequence becomes exact when tensored with B, and so is itself exact, which implies that $N = 0$. This shows that $A \to B$ is *faithfully* flat.

COROLLARY 9.4. *Let $A \to B$ be faithfully flat. An A-module M is flat (resp. faithfully flat) if $B \otimes_A M$ is flat (resp. faithfully flat) as a B-module.*

PROOF. Assume that $M_B \overset{\text{def}}{=} B \otimes_A N$ is flat, and let $N' \to N$ be an injective map of A-modules. We have that

$$B \otimes_A (M \otimes_A N' \to M \otimes_A N) \simeq M_B \otimes_B (N'_B \to N_B),$$

and the map at right is injective because $A \to B$ is flat and M_B is flat. Now (9.2) shows that $M \otimes_A N' \to M \otimes_A N$ is injective. Thus M is flat.

Assume that M_B is faithfully flat, and let N be an A-module. If $M \otimes_A N = 0$, then $M_B \otimes_B N_B$ is zero because it is isomorphic to $(M \otimes_A N)_B$. Now $N_B = 0$ because M_B is faithfully flat, and so $N = 0$ because $A \to B$ is faithfully flat. □

PROPOSITION 9.5. *Let $i\colon A \to B$ be a faithfully flat homomorphism. For any A-module M, the sequence*

$$0 \to M \xrightarrow{d_0} B \otimes_A M \xrightarrow{d_1} B \otimes_A B \otimes_A M \tag{5}$$

with

$$\begin{cases} d_0(m) &= 1 \otimes m, \\ d_1(b \otimes m) &= 1 \otimes b \otimes m - b \otimes 1 \otimes m \end{cases}$$

is exact.

PROOF. Assume first that there exists an A-linear section to $A \to B$, i.e., an A-linear map $f\colon B \to A$ such that $f \circ i = \mathrm{id}_A$, and define

$$k_0\colon B \otimes_A M \to M, \qquad k_0(b \otimes m) = f(b)m$$
$$k_1\colon B \otimes_A B \otimes_A M \to B \otimes_A M, \qquad k_1(b \otimes b' \otimes m) = f(b)b' \otimes m.$$

Then $k_0 d_0 = \mathrm{id}_M$, which shows that d_0 is injective. Moreover,

$$k_1 \circ d_1 + d_0 \circ k_0 = \mathrm{id}_{B \otimes_A M}$$

which shows that, if $d_1(x) = 0$, then $x = d_0(k_0(x))$, as required.

We now consider the general case. Because $A \to B$ is faithfully flat, it suffices to prove that the sequence (5) becomes exact after tensoring in B. But the sequence obtained from (5) by tensoring with B is isomorphic to the sequence (5) for the homomorphism of rings $B \mapsto 1 \otimes B \colon B \to B \otimes_A B$ and the B-module $B \otimes_A M$, because, for example,

$$B \otimes_A (B \otimes_A M) \simeq (B \otimes_A B) \otimes_B (B \otimes_A M).$$

Now $B \to B \otimes_A B$ has an B-linear section, namely, $f(B \otimes B') = BB'$, and so we can apply the first part. □

COROLLARY 9.6. *If $A \to B$ is faithfully flat, then it is injective with image the set of elements on which the maps*

$$\begin{cases} b & \mapsto & 1 \otimes b \\ b & \mapsto & b \otimes 1 \end{cases} : B \to B \otimes_A B$$

agree.

PROOF. This is the special case $M = A$ of the Proposition. □

PROPOSITION 9.7. *Let $A \to A'$ be a homomorphism of rings. If $A \to B$ is flat (or faithfully flat), then so also is $A' \to B \otimes_A A'$.*

PROOF. For any A'-module M,

$$(B \otimes_A A') \otimes_{A'} M \simeq B \otimes_A (A' \otimes_{A'} M) \simeq B \otimes_A M,$$

from which the statement follows. □

PROPOSITION 9.8. *For any multiplicative subset S of a ring A and A-module M,*

$$S^{-1} A \otimes_A M \simeq S^{-1} M.$$

The homomorphism $a \mapsto \frac{a}{1} \colon A \to S^{-1} A$ is flat.

PROOF. To give an $S^{-1}A$-module is the same as giving an A-module on which the elements of S act invertibly. Therefore $S^{-1} A \otimes_A M$ and $S^{-1} M$ satisfy the same universal property (see §8, especially (1)), which proves the first statement. As $M \rightsquigarrow S^{-1} M$ is exact (6.11), so also is $M \rightsquigarrow S^{-1} A \otimes_A M$, which proves the second statement. □

PROPOSITION 9.9. *The following conditions on a flat homomorphism $\varphi \colon A \to B$ are equivalent:*

(a) *φ is faithfully flat;*
(b) *for every maximal ideal $\mathfrak{m}$ of A, the ideal $\varphi(\mathfrak{m})B \neq B$;*
(c) *every maximal ideal $\mathfrak{m}$ of A is of the form $\varphi^{-1}(\mathfrak{n})$ for some maximal ideal $\mathfrak{n}$ of B.*

PROOF. (a) ⇒ (b): Let $\mathfrak{m}$ be a maximal ideal of A, and let $M = A/\mathfrak{m}$; then

$$B \otimes_A M \simeq B/\varphi(\mathfrak{m})B.$$

As $B \otimes_A M \neq 0$, we see that $\varphi(\mathfrak{m})B \neq B$.

(b) $\Rightarrow$ (c): If $\varphi(\mathfrak{m})B \neq B$, then $\varphi(\mathfrak{m})$ is contained in a maximal ideal $\mathfrak{n}$ of B. Now $\varphi^{-1}(\mathfrak{n})$ is a proper ideal in A containing $\mathfrak{m}$, and hence equals $\mathfrak{m}$.

(c) $\Rightarrow$ (a): Let M be a nonzero A-module. Let x be a nonzero element of M, and let $\mathfrak{a} = \mathrm{ann}(x) \overset{\text{def}}{=} \{a \in A \mid ax = 0\}$. Then $\mathfrak{a}$ is an ideal in A, and $M' \overset{\text{def}}{=} Ax \simeq A/\mathfrak{a}$. Moreover, $B \otimes_A M' \simeq B/\varphi(\mathfrak{a}) \cdot B$ and, because $A \to B$ is flat, $B \otimes_A M'$ is a submodule of $B \otimes_A M$. Because $\mathfrak{a}$ is proper, it is contained in a maximal ideal $\mathfrak{m}$ of A, and therefore

$$\varphi(\mathfrak{a}) \subset \varphi(\mathfrak{m}) \subset \mathfrak{n}$$

for some maximal ideal $\mathfrak{n}$ of A. Hence $\varphi(\mathfrak{a}) \cdot B \subset \mathfrak{n} \neq B$, and so $B \otimes_A M \supset B \otimes_A M' \neq 0$. □

THEOREM 9.10 (GENERIC FLATNESS). *Let A an integral domain with field of fractions F, and let B be a finitely generated A-algebra contained in $F \otimes_A B$. Then for some nonzero elements a of A and b of B, the homomorphism $A_a \to B_b$ is faithfully flat.*

PROOF. As $F \otimes_A B$ is a finitely generated F-algebra, the Noether normalization theorem (5.11) shows that there exist elements $x_1, \ldots, x_m$ of $F \otimes_A B$ such that $F[x_1, \ldots, x_m]$ is a polynomial ring over F and $F \otimes_A B$ is a finite $F[x_1, \ldots, x_m]$-algebra. After multiplying each x_i by an element of A, we may suppose that it lies in B. Let $b_1, \ldots, b_n$ generate B as an A-algebra. Each b_i satisfies a monic polynomial equation with coefficients in $F[x_1, \ldots, x_m]$. Let $a \in A$ be a common denominator for the coefficients of these polynomials. Then each b_i is integral over A_a. As the b_i generate B_a as an A_a-algebra, this shows that B_a is a finite $A_a[x_1, \ldots, x_m]$-algebra (by 5.2). Therefore, after replacing A with A_a and B with B_a, we may suppose that B is a finite $A[x_1, \ldots, x_m]$-algebra.

$$\begin{array}{ccccc}
B & \xrightarrow{\text{injective}} & F \otimes_A B & \longrightarrow & E \otimes_{A[x_1,\ldots,x_m]} B \\
\uparrow{\scriptstyle\text{finite}} & & \uparrow{\scriptstyle\text{finite}} & & \uparrow{\scriptstyle\text{finite}} \\
A[x_1, \ldots, x_m] & \longrightarrow & F[x_1, \ldots, x_m] & \longrightarrow & E \overset{\text{def}}{=} F(x_1, \ldots, x_n) \\
\uparrow & & \uparrow & & \\
A & \longrightarrow & F & &
\end{array}$$

Let $E = F(x_1, \ldots, x_m)$ be the field of fractions of $A[x_1, \ldots, x_m]$, and let $b_1, \ldots, b_r$ be elements of B that form a basis for $E \otimes_{A[x_1,\ldots,x_m]} B$ as an E-vector space. Each element of B can be expressed a linear combination of the b_i with coefficients in E. Let q be a common denominator for the coefficients arising from a set of generators for B as an $A[x_1, \ldots, x_m]$-module. Then $b_1, \ldots, b_r$ generate B_q as an $A[x_1, \ldots, x_m]_q$-module. In other words, the map

$$(c_1, \ldots, c_r) \mapsto \sum c_i b_i \colon A[x_1, \ldots, x_m]_q^r \to B_q \qquad (6)$$

is surjective. This map becomes an isomorphism when tensored with E over $A[x_1, \ldots, x_m]_q$, which implies that each element of its kernel is killed by a nonzero element of $A[x_1, \ldots, x_m]_q$ and so is zero (because $A[x_1, \ldots, x_n]_q$ is an integral domain). Hence the map (6) is an isomorphism, and so B_q is free of finite rank over $A[x_1, \ldots, x_m]_q$. Let a be some nonzero coefficient of the polynomial q, and consider the maps

$$A_a \to A_a[x_1, \ldots, x_m] \to A_a[x_1, \ldots, x_m]_q \to B_{aq}.$$

The first and third arrows realize their targets as nonzero free modules over their sources, and so are faithfully flat. The middle arrow is flat by (9.8). Let $\mathfrak{m}$ be a maximal ideal in A_a.

Then $\mathfrak{m}A_a[x_1,\ldots,x_m]$ does not contain the polynomial q because the coefficient a of q is invertible in A_a. Hence $\mathfrak{m}A_a[x_1,\ldots,x_m]_q$ is a proper ideal of $A_a[x_1,\ldots,x_m]_q$, and so the map $A_a \to A_a[x_1,\ldots,x_m]_q$ is faithfully flat (apply 9.9). This completes the proof. □

REMARK 9.11. The theorem holds for any finitely generated B-algebra, i.e., without the requirement that $B \subset F \otimes_A B$. To see this, note that $F \otimes_A B$ is the ring of fractions of B with respect to the multiplicative subset $A \smallsetminus \{0\}$ (see 9.8), and so the kernel of $B \to F \otimes_A B$ is the ideal

$$\mathfrak{n} = \{b \in B \mid ab = 0 \text{ for some nonzero } a \in A\}.$$

This is finitely generated (Hilbert basis theorem 3.6), and so there exists a nonzero $c \in A$ such that $cb = 0$ for *all* $b \in \mathfrak{n}$. I claim that the homomorphism $B_c \to F \otimes_{A_c} B_c$ is injective. If $\frac{b}{c^r}$ lies in its kernel, then $\frac{a}{c^s}\frac{b}{c^r} = 0$ in B_c for some nonzero $\frac{a}{c^s} \in A_c$, and so $c^N ab = 0$ in B for some N; therefore $b \in \mathfrak{n}$, and so $cb = 0$, which implies that $\frac{b}{c^r} = 0$ already in B_c. Therefore, after replacing A, B, and M with A_c, B_c, and M_c, we may suppose that the map $B \to F \otimes_A B$ is injective. On identifying B with its image, we arrive at the situation of the theorem.

10 Finitely generated projective modules

In many situations, the correct generalization of "finite-dimensional vector space" is not "finitely generated module" but "finitely generated projective module". Throughout this section, A is a commutative ring.

PROJECTIVE MODULES

DEFINITION 10.1. An A-module P is *projective* if, for each surjective A-linear map $f: M \to N$ and A-linear map $g: P \to N$, there exists an A-linear map $h: P \to M$ (not necessarily unique) such that $f \circ h = g$:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow^{\exists h} & \downarrow g & & \\ M & \xrightarrow{f} & N & \longrightarrow & 0. \end{array}$$

In other words, P is projective if every map from P onto a quotient of a module M lifts to a map to M. Equivalently, P is projective if the functor $M \rightsquigarrow \mathrm{Hom}_{A\text{-lin}}(P, M)$ is exact.

As

$$\mathrm{Hom}(\textstyle\bigoplus_i P_i, M) \simeq \bigoplus_i \mathrm{Hom}(P_i, M)$$

we see that a direct sum of A-modules is projective if and only if each direct summand is projective. As A itself is projective, this shows that every free A-module is projective and every direct summand of a free module is projective. Conversely, let P be a projective module, and write it as a quotient of a free module,

$$F \xrightarrow{f} P \longrightarrow 0;$$

because P is projective, there exists an A-linear map $h: P \to F$ such that $f \circ h = \mathrm{id}_P$; then

$$F \approx \mathrm{Im}(h) \oplus \mathrm{Ker}(f) \approx P \oplus \mathrm{Ker}(f),$$

and so P is a direct summand of F. We conclude: the projective A-modules are exactly the direct summands of free A-modules.

FINITELY PRESENTED MODULES

DEFINITION 10.2. An A-module M is *finitely presented* if there exists an exact sequence $A^m \to A^n \to M \to 0$, some $m, n \in \mathbb{N}$.

A finite family $(e_i)_{i \in I}$ of generators for an A-module M defines a homomorphism $(a_i) \mapsto \sum_{i \in I} a_i e_i : A^I \to M$. The elements of the kernel of this homomorphism are called the *relations* between the generators. Thus, M is finitely presented if it admits a finite family of generators whose module of relations is finitely generated. Obviously

$$\text{finitely presented} \Rightarrow \text{finitely generated},$$

and the converse is true when A is noetherian (by 3.4).

PROPOSITION 10.3. *If M is finitely presented, then the kernel of every surjective homomorphism $A^m \to M$, $m \in \mathbb{N}$, is finitely generated.*

In other words, if M is finitely presented, then the module of relations for *every* finite generating set is finitely generated.

PROOF. We are given that there exists a surjective homomorphism $A^n \to M$ with finitely generated kernel R, and we wish to show that the kernel R' of $A^m \to M$ is finitely generated. Consider the diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R & \longrightarrow & A^n & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow f & & \downarrow g & & \downarrow \mathrm{id}_M & & \\
0 & \longrightarrow & R' & \longrightarrow & A^m & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

The map g exists because A^n is projective, and it induces the map f. From the diagram, we get an exact sequence

$$R \xrightarrow{g} R' \to A^m/gA^n \to 0,$$

either from the snake lemma or by a direct diagram chase. As R and A^m/gA^n are both finitely generated, so also is R'. □

If M is finitely generated and projective, then the kernel of $A^n \to M$ is a direct summand (hence quotient) of A^n, and so is finitely generated. Therefore M is finitely presented.

Finitely generated projective modules

According to the above discussion, the finitely generated projective modules are exactly the direct summands of free A-modules of finite rank.

THEOREM 10.4. *The following conditions on an A-module are equivalent:*

(a) *M is finitely generated and projective;*
(b) *M is finitely presented and $M_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$ of A;*
(c) *there exists a finite family $(f_i)_{i\in I}$ of elements of A generating the ideal A and such that, for all $i \in I$, the A_{f_i}-module M_{f_i} is free of finite rank;*
(d) *M is finitely presented and flat.*

Moreover, when A is an integral domain, they are equivalent to:

(e) $\dim_{k(\mathfrak{p})}(M \otimes_A k(\mathfrak{p}))$ *is the same for all prime ideals $\mathfrak{p}$ of A (here $k(\mathfrak{p})$ denotes the field of fractions of $A/\mathfrak{p}$).*

PROOF. (a)⇒(d). As tensor products commute with direct sums, every free module is flat and every direct summand of a flat module is flat. Therefore, every projective module M is flat, and we saw above that such a module is finitely presented if it is finitely generated.

(b)⇒(c). Let $\mathfrak{m}$ be a maximal ideal of A, and let $x_1, \ldots, x_r$ be elements of M whose images in $M_{\mathfrak{m}}$ form a basis for $M_{\mathfrak{m}}$ over $A_{\mathfrak{m}}$. The kernel N' and cokernel N of the homomorphism

$$\alpha\colon A^r \to M, \quad g(a_1, \ldots, a_r) = \sum a_i x_i,$$

are both finitely generated, and $N'_{\mathfrak{m}} = 0 = N_{\mathfrak{m}}$. Therefore, there exists[13] an $f \in A \smallsetminus \mathfrak{m}$ such that $N'_f = 0 = N_f$. Now α becomes an isomorphism when tensored with A_f.

The set T of elements f arising in this way is contained in no maximal ideal, and so generates the ideal A. Therefore, $1 = \sum_{i\in I} a_i f_i$ for certain $a_i \in A$ and $f_i \in T$.

(c)⇒(d). Let $B = \prod_{i\in I} A_{f_i}$. Then B is faithfully flat over A, and $B \otimes_A M = \prod M_{f_i}$, which is clearly a flat B-module. It follows that M is a flat A-module (apply 9.4).

(c)⇒(e). This is obvious.

(e)⇒(c). Fix a prime ideal $\mathfrak{p}$ of A. For some $f \notin \mathfrak{p}$, there exist elements $x_1, \ldots, x_r$ of M_f whose images in $M \otimes_A k(\mathfrak{p})$ form a basis. Then the map

$$\alpha\colon A_f^r \to M_f,\ \alpha(a_1, \ldots, a_r) = \sum a_i x_i,$$

defines a surjection $A_{\mathfrak{p}}^r \to M_{\mathfrak{p}}$ (Nakayama's lemma; note that $k(\mathfrak{p}) \simeq A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$). Because the cokernel of α is finitely generated, the map α itself will be surjective once f has been replaced by a multiple. For any prime ideal $\mathfrak{q}$ of A_f, the map $k(\mathfrak{q})^r \to M \otimes_A k(\mathfrak{q})$ defined by α is surjective, and hence is an isomorphism because $\dim(M \otimes_A k(\mathfrak{q})) = r$. Thus $\mathrm{Ker}(\alpha) \subset \mathfrak{q}A_f^r$ for every $\mathfrak{q}$, which implies that it is zero as A_f is reduced. Therefore M_f is free. As in the proof of (b), a finite set of such f's will generate A. □

To prove the remaining implications, (d)⇒(a),(b) we shall need the following lemma.

LEMMA 10.5. *Let*

$$0 \to N \to F \to M \to 0 \tag{1}$$

be an exact sequence of A-modules with N a submodule of F.

[13] To say that $S^{-1}N = 0$ means that, for each $x \in N$, there exists an $s_x \in S$ such that $s_x x = 0$. If $x_1, \ldots, x_n$ generate N, then $s \stackrel{\text{def}}{=} s_{x_1} \cdots s_{x_n}$ lies in S and has the property that $sN = 0$. Therefore, $N_s = 0$.

(a) *If M and F are flat over A, then $N\cap\mathfrak{a}F=\mathfrak{a}N$ (inside F) for all ideals $\mathfrak{a}$ of A.*
(b) *Assume that F is free with basis $(y_i)_{i\in I}$ and that M is flat. If the element $n=\sum_{i\in I}a_iy_i$ of F lies in N, then there exist $n_i\in N$ such that $n=\sum_{i\in I}a_in_i$.*
(c) *Assume that M is flat and F is free. For any finite set $\{n_1,\ \ldots,\ n_r\}$ of elements of N, there exists an A-linear map $f\colon F\to N$ with $f(n_j)=n_j,\ j=1,\ldots,r$.*

PROOF. (a) Consider

$$\begin{array}{ccccccc} & & \mathfrak{a}\otimes N & \longrightarrow & \mathfrak{a}\otimes F & \longrightarrow & \mathfrak{a}\otimes M \\ & & & & \downarrow\simeq & & \downarrow\simeq \\ 0 & \longrightarrow & N\cap\mathfrak{a}F & \longrightarrow & \mathfrak{a}F & \longrightarrow & \mathfrak{a}M \end{array}$$

The first row is obtained from (1) by tensoring with $\mathfrak{a}$, and the second row is a subsequence of (1). Both rows are exact. On tensoring $\mathfrak{a}\to A$ with F we get a map $\mathfrak{a}\otimes F\to F$, which is injective because F is flat. Therefore $\mathfrak{a}\otimes F\to\mathfrak{a}F$ is an isomorphism. Similarly, $\mathfrak{a}\otimes M\to\mathfrak{a}M$ is an isomorphism. From the diagram we get a surjective map $\mathfrak{a}\otimes N\to N\cap\mathfrak{a}F$, and so the image of $\mathfrak{a}\otimes N$ in $\mathfrak{a}F$ is $N\cap\mathfrak{a}F$. But this image is $\mathfrak{a}N$.

(b) Let $\mathfrak{a}$ be the ideal generated by the a_i. Then $n\in N\cap\mathfrak{a}F=\mathfrak{a}N$, and so there are $n_i\in N$ such that $n=\sum a_in_i$.

(c) We use induction on r. Assume first that $r=1$, and write

$$n_1=\textstyle\sum_{i\in I_0}a_iy_i$$

where $(y_i)_{i\in I}$ is a basis for F and I_0 is a finite subset of I. Then

$$n_1=\textstyle\sum_{i\in I_0}a_in_i'$$

for some $n_i'\in N$ (by (b)), and f may be taken to be the map such that $f(y_i)=n_i'$ for $i\in I_0$ and $f(y_i)=0$ otherwise. Now suppose that $r>1$, and that there are maps $f_1,\ f_2:F\to N$ such that $f_1(n_1)=n_1$ and

$$f_2(n_i-f_1(n_i))=n_i-f_1(n_i),\quad i=2,\ \ldots\ r.$$

Then

$$f\colon F\to N,\quad f=f_1+f_2-f_2\circ f_1$$

has the required property. □

We now complete the proof of the theorem.

(d)⇒(a). Because M is finitely presented, there is an exact sequence

$$0\to N\to F\to M\to 0$$

in which F is free and N and F are both finitely generated. Because M is flat, (c) of the lemma shows that this sequence splits, and so M is projective.

(d)⇒(b). We may suppose that A itself is local, with maximal ideal $\mathfrak{m}$. Let $x_1,\ \ldots,\ x_r\in M$ be such that their images in $M/\mathfrak{m}M$ form a basis for this over the field $A/\mathfrak{m}$. Then the x_i generate M (by Nakayama's lemma), and so there exists an exact

$$0\to N\to F\xrightarrow{g}M\to 0$$

in which F is free with basis $\{y_1,\ \ldots,\ y_r\}$ and $g(y_i)=x_i$. According to (a) of the lemma, $\mathfrak{m}N=N\cap(\mathfrak{m}F)$, which equals N because $N\subset\mathfrak{m}F$. Therefore N is zero by Nakayama's lemma.

ASIDE 10.6. Nonfree projective finitely generated modules are common: for example, the ideals in a Dedekind domain are projective and finitely generated, but they are free only if principal. The situation with nonfinitely generated modulies is quite different: if A is a noetherian ring with no nontrivial idempotents, then every nonfinitely generated projective A-module is free (Bass, Hyman. Big projective modules are free. Illinois J. Math. 7 1963, 24–31, Corollary 4.5). The condition on the idempotents is necessary because, for a ring $A \times B$, the module $A^{(I)} \times B^{(J)}$ is not free when the sets I and J have different cardinalities.

DUALS

The dual $\mathrm{Hom}_{A\text{-lin}}(M, A)$ of an A-module M is denoted $M^\vee$.

PROPOSITION 10.7. *For any A-modules M, S, T with M finitely generated and projective, the canonical maps*

$$\mathrm{Hom}_{A\text{-}lin}(S, T \otimes_A M) \to \mathrm{Hom}_{A\text{-}lin}(S \otimes_A M^\vee, T) \tag{2}$$

$$M^\vee \otimes T^\vee \to (M \otimes T)^\vee \tag{3}$$

$$M \to M^{\vee\vee} \tag{4}$$

are isomorphisms.

PROOF. The canonical map (2) sends $f: S \to T \otimes_A M$ to the map $f': S \otimes_A M^\vee \to T$ such that $f'(s \otimes g) = (T \otimes g)(f(s))$. It becomes the canonical isomorphism

$$\mathrm{Hom}_{A\text{-lin}}(S, T^n) \to \mathrm{Hom}_{A\text{-lin}}(S^n, T)$$

when $M = A^n$. It follows that (2) is an isomorphism whenever M is a direct summand of a finitely generated free module, i.e., whenever M is finitely generated and projective.

The canonical map (3) sends $f \otimes g \in M^\vee \otimes T^\vee$ to the map $m \otimes t \mapsto f(m) \otimes g(t): M \otimes T \to A$, and the canonical map (4) sends m to the map $f \mapsto f(m): M^\vee \to A$. Again, they are obviously isomorphisms for A^n, and hence for direct summands of A^n. □

We let $\mathrm{ev}: M^\vee \otimes_A M \to A$ denote the evaluation map $f \otimes m \mapsto f(m)$.

LEMMA 10.8. *Let M and N be modules over commutative ring A, and let $e: N \otimes_A M \to A$ be an A-linear map. There exists at most one A-linear map $\delta: A \to M \otimes_A N$ such that the composites*

$$\begin{array}{ccccc} M & \xrightarrow{\delta \otimes M} & M \otimes N \otimes M & \xrightarrow{M \otimes e} & M \\ N & \xrightarrow{N \otimes \delta} & N \otimes M \otimes N & \xrightarrow{e \otimes N} & N \end{array} \tag{5}$$

are the identity maps on M and N respectively. When such a map exists,

$$T \otimes_A N \simeq \mathrm{Hom}_{A\text{-}lin}(M, T) \tag{6}$$

for all A-modules T. In particular,

$$(N, e) \simeq (M^\vee, \mathrm{ev}). \tag{7}$$

PROOF. From e we get an A-linear map

$$T \otimes e: T \otimes_A N \otimes_A M \to T,$$

which allows us to define an A-linear map

$$x \mapsto f_x : T \otimes_A N \to \mathrm{Hom}_{A\text{-lin}}(M, T) \tag{8}$$

by setting

$$f_x(m) = (T \otimes e)(x \otimes m), \quad x \in T \otimes_A N, m \in M.$$

An A-linear map $f: M \to T$ defines a map $f \otimes N: M \otimes_A N \to T \otimes_A N$, and so a map $\delta: A \to M \otimes_A N$ defines an A-linear map

$$f \mapsto (f \otimes N)(\delta(1)) : \mathrm{Hom}_{A\text{-lin}}(M, T) \to T \otimes_A N. \tag{9}$$

When the first (resp. the second) composite in (5) is the identity, then (9) is a right (resp. a left) inverse to (8).[14] Therefore, when a map δ exists with the required properties, the map (8) defined by e is an isomorphism. In particular, e defines an isomorphism

$$x \mapsto f_x : M \otimes_A N \to \mathrm{Hom}_{A\text{-lin}}(M, M),$$

which one checks sends $\delta(a)$ to the endomorphism $x \mapsto ax$ of M. This proves that δ is unique.

To get (7), take $T = M$ in (6). □

PROPOSITION 10.9. *An A-module M is finitely generated and projective if and only if there exists an A-linear map $\delta: A \to M \otimes M^\vee$ such that*

$$(M \otimes \mathrm{ev}) \circ (\delta \otimes M) = \mathrm{id}_M \text{ and}$$
$$(M^\vee \otimes \delta) \circ (\mathrm{ev} \otimes M^\vee) = \mathrm{id}_{M^\vee}.$$

PROOF. $\Longrightarrow$: Suppose first that M is free with finite basis $(e_i)_{i \in I}$, and let $(e'_i)_{i \in I}$ be the dual basis of $M^\vee$. The linear map $\delta: A \to M \otimes M^\vee$, $1 \mapsto \Sigma e_i \otimes e'_i$, satisfies the conditions. Let $(f_i)_{i \in I}$ be as in (10.4c). Then δ is defined for each module M_{f_i}, and the uniqueness assertion in Lemma 10.8 implies that the δ's for the different M_{f_i}'s patch together to give a δ for M.

$\Longleftarrow$: On taking $T = M$ in (6), we see that $M^\vee \otimes_A M \simeq \mathrm{End}_{A\text{-lin}}(M)$. If $\sum_{i \in I} f_i \otimes m_i$ corresponds to id_M, so that $\sum_{i \in I} f_i(m) m_i = m$ for all $m \in M$, then

$$M \xrightarrow{m \mapsto (f_i(m))} A^I \xrightarrow{(a_i) \mapsto \sum a_i m_i} M$$

is a factorization of id_M. Therefore M is a direct summand of a free module of finite rank. □

[14] Assume δ satisfies the condition in the statement of the lemma.

Let $x \in T \otimes_A N$; by definition, $(f_x \otimes N)(\delta(1)) = (T \otimes e \otimes N)(x \otimes \delta(1))$. On tensoring the second sequence in (5) with T, we obtain maps

$$T \otimes_A N \simeq T \otimes_A N \otimes_A A \xrightarrow{T \otimes N \otimes \delta} T \otimes_A N \otimes_A M \otimes_A N \xrightarrow{T \otimes e \otimes N} T \otimes_A N$$

whose composite is the identity map on $T \otimes_A N$. As $x = x \otimes 1$ maps to $x \otimes \delta(1)$ under $T \otimes N \otimes \delta$, this shows that $(f_x \otimes N)(\delta(1)) = x$.

Let $f \in \mathrm{Hom}_{A\text{-lin}}(M, T)$, and consider the commutative diagram

$$\begin{array}{ccccc} & & T \otimes_A N \otimes_A M & \xrightarrow{T \otimes e} & T \\ & & \uparrow{\scriptstyle f \otimes N \otimes M} & & \uparrow{\scriptstyle f} \\ M & \xrightarrow{\delta \otimes M} & M \otimes_A N \otimes_A M & \xrightarrow{M \otimes e} & M, \end{array}$$

For $m \in M$, the two images of $\delta(1) \otimes m$ in T are $f(m)$ and $f_{(f \otimes N)(\delta(1))}(m)$, and so $f = f_{(f \otimes N)(\delta(1))}$.

ASIDE 10.10. A module M over a ring A is said to be *reflexive* if the canonical map $M \to M^{\vee\vee}$ is an isomorphism. We have seen that for finitely generated modules "projective" implies "reflexive", but the converse is false. In fact, for a finite generated module M over an integrally closed noetherian integral domain A, the following are equivalent (Bourbaki AC, VII §4, 2):

(a) M is reflexive;
(b) M is torsion-free and equals the intersection of its localizations at the prime ideals of A of height 1;
(c) M is the dual of a finitely generated module.

For noetherian rings of global dimension ≤ 2, for example, for regular local rings of Krull dimension ≤ 2, every finitely generated reflexive module is projective: for any finitely generated module M over a noetherian ring A, there exists an exact sequence

$$A^m \to A^n \to M \to 0$$

with $m, n \in \mathbb{N}$; on taking duals and forming the cokernel, we get an exact sequence

$$0 \to M^\vee \to A^n \to A^m \to N \to 0;$$

if A has global dimension ≤ 2, then $M^\vee$ is projective, and if M is reflexive, then $M \simeq (M^\vee)^\vee$.

ASIDE 10.11. For a finitely generated torsion-free module M over an integrally closed noetherian integral domain A, there exists a free submodule L of M such that M/L is isomorphic an ideal $\mathfrak{a}$ in A (Bourbaki AC, VII, §4, Thm 6). When A is Dedekind, every ideal is projective, and so $M \simeq L \oplus \mathfrak{a}$. In particular, M is projective. Therefore, the finitely generated projective modules over a Dedekind domain are exactly the finitely generated torsion-free modules.

11 The Hilbert Nullstellensatz

ZARISKI'S LEMMA

In proving Zariski's lemma, we shall need to use that the ring $k[X]$ contains infinitely many distinct monic irreducible polynomials. When k is infinite, this obvious, because the polynomials $X - a$, $a \in k$, are distinct and irreducible. When k is finite, we can adapt Euclid's argument: if $p_1, \ldots, p_r$ are monic irreducible polynomials in $k[X]$, then $p_1 \cdots p_r + 1$ is divisible by a monic irreducible polynomial distinct from $p_1, \ldots, p_r$.

THEOREM 11.1 (ZARISKI'S LEMMA). *Let $k \subset K$ be fields. If K is finitely generated as a k-algebra, then it is algebraic over k (hence finite over k, and K equals k if k is algebraically closed).*

PROOF. We shall prove this by induction on r, the smallest number of elements required to generate K as a k-algebra. The case $r = 0$ being trivial, we may suppose that

$$K = k[x_1, \ldots, x_r] \text{ with } r \geq 1.$$

If K is not algebraic over k, then at least one x_i, say x_1, is not algebraic over k. Then, $k[x_1]$ is a polynomial ring in one symbol over k, and its field of fractions $k(x_1)$ is a subfield of K. Clearly K is generated as a $k(x_1)$-algebra by $x_2, \ldots, x_r$, and so the induction hypothesis implies that $x_2, \ldots, x_r$ are algebraic over $k(x_1)$. Proposition 5.5 shows that there exists a $c \in k[x_1]$ such that $cx_2, \ldots, cx_r$ are integral over $k[x_1]$. Let $f \in K$. For a sufficiently large N, $c^N f \in k[x_1, cx_2, \ldots, cx_r]$, and so $c^N f$ is integral over $k[x_1]$ by 5.3. When we apply this statement to an element f of $k(x_1)$, it shows that $c^N f \in k[x_1]$ because $k[x_1]$ is integrally closed. Therefore, $k(x_1) = \bigcup_N c^{-N} k[x_1]$, but this is absurd, because $k[x_1]$ ($\simeq k[X]$) has infinitely many distinct monic irreducible polynomials that can occur as denominators of elements of $k(x_1)$. □

ALTERNATIVE PROOF OF ZARISKI'S LEMMA [15]

LEMMA 11.2. *For an integral domain A, there does not exist an $f \in A[X]$ such that $A[X]_f$ is a field.*

PROOF. Suppose, on the contrary, that $A[X]_f$ is a field. Then $\deg f > 0$, and so $f - 1 \notin A$. Write $(f-1)^{-1} = g/f^n$ with $g \in A[X]$ and $n \geq 1$. Then

$$(f-1)g = f^n = (1 + (f-1))^n = 1 + (f-1)h$$

with $h \in A[X]$, and so $(f-1)(g-h) = 1$. Hence $f - 1$ is a unit, which is absurd. □

LEMMA 11.3. *Consider rings $A \subset B$. If B is integral over A, then $A \cap B^{\times} = A^{\times}$. In particular, if B is a field, then so also is A.*

PROOF. Let a be an element of A that becomes a unit in B, say, $ab = 1$ with $b \in B$. There exist $a_1, \ldots, a_n \in A$ such that $b^n + a_1 b^{n-1} + \cdots + a_n = 0$. On multiplying through by a^{n-1}, we find that $b = -a_1 - \cdots - a_n a^{n-1} \in A$, and so $a \in A^{\times}$. □

PROPOSITION 11.4. *Let A be an integral domain, and suppose that there exists a maximal ideal $\mathfrak{m}$ in $A[X_1, \ldots, X_n]$ such that $A \cap \mathfrak{m} = (0)$. Then there exists a nonzero element a in A such that A_a is a field and $A[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite extension of A_a.*

PROOF. Note that the condition $A \cap \mathfrak{m} = (0)$ implies that A (hence also A_a) is a subring of the field $K = A[X_1, \ldots, X_n]/\mathfrak{m}$, and so the statement makes sense.

We argue by induction on n. When $n = 0$, A is a field, and the statement is trivial. Therefore, suppose that $n \geq 1$, and regard $A[X_1, \ldots, X_n]$ as a polynomial ring in $n-1$ symbols over $A[X_i]$. Then $\mathfrak{m} \cap A[X_i] \neq (0)$ because otherwise the induction hypothesis would contradict Lemma 11.2. Let $a_i X_i^{n_i} + \cdots$ be a nonzero element of $\mathfrak{m} \cap A[X_i]$. The image x_i of X_i in K satisfies the equation

$$a_i x_i^n + \cdots = 0,$$

and so K is integral over its subring $A_{a_1 \cdots a_n}$. By Lemma 11.3, $A_{a_1 \cdots a_n}$ is a field, and K is finite over it because it is integral (algebraic) and finitely generated. □

We now prove Zariski's lemma. Write $K = k[X_1, \ldots, X_n]/\mathfrak{m}$. According to the proposition, K is a finite extension of k_a for some nonzero $a \in k$, but because k is a field $k_a = k$.

THE NULLSTELLENSATZ

Recall that k^{al} denotes an algebraic closure of the field k.

THEOREM 11.5 (NULLSTELLENSATZ). *Every proper ideal $\mathfrak{a}$ in $k[X_1, \ldots, X_n]$ has a zero in $(k^{\mathrm{al}})^n \stackrel{\mathrm{def}}{=} k^{\mathrm{al}} \times \cdots \times k^{\mathrm{al}}$, i.e., there exists a point $(a_1, \ldots, a_n) \in (k^{\mathrm{al}})^n$ such that $f(a_1, \ldots, a_n) = 0$ for all $f \in \mathfrak{a}$.*

PROOF. We have to show that there exists a k-algebra homomorphism $k[X_1, \ldots, X_n] \to k^{\mathrm{al}}$ containing $\mathfrak{a}$ in its kernel. Let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{a}$. Then $k[X_1, \ldots, X_n]/\mathfrak{m}$ is a field, which is algebraic over k by Zariski's lemma, and so there exists a k-algebra homomorphism $k[X_1, \ldots, X_n]/\mathfrak{m} \to k^{\mathrm{al}}$. The composite of this with the quotient map $k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/\mathfrak{m}$ contains $\mathfrak{a}$ in its kernel. □

[15] A simplification of Swan's simplication of a proof of Munshi — see `www.math.uchicago.edu/~swan/`.

COROLLARY 11.6. *When k is algebraically closed, the maximal ideals in $k[X_1,\ldots,X_n]$ are exactly the ideals $(X_1-a_1,\ldots,X_n-a_n)$, $(a_1,\ldots,a_n)\in k^n$.*

PROOF. Clearly, $k[X_1,\ldots,X_n]/(X_1-a_1,\ldots,X_n-a_n)\simeq k$, and so $(X_1-a_1,\ldots,X_n-a_n)$ is maximal. Conversely, because k is algebraically closed, a proper ideal $\mathfrak{a}$ has a zero $(a_1,\ldots,a_n)$ in k^n. Let $f\in k[X_1,\ldots,X_n]$; when we write f as a polynomial in $X_1-a_1,\ldots,X_n-a_n$, its constant term is $f(a_1,\ldots,a_n)$. Therefore, if $f\in\mathfrak{a}$, then $f\in(X_1-a_1,\ldots,X-a_n)$. □

THEOREM 11.7 (STRONG NULLSTELLENSATZ). *For an ideal $\mathfrak{a}$ in $k[X_1,\ldots,X_n]$, let $Z(\mathfrak{a})$ be the set of zeros of $\mathfrak{a}$ in $(k^{\mathrm{al}})^n$. If a polynomial $h\in k[X_1,\ldots,X_n]$ is zero on $Z(\mathfrak{a})$, then some power of h lies in $\mathfrak{a}$.*

PROOF. We may assume $h\neq 0$. Let $g_1,\ldots,g_m$ generate $\mathfrak{a}$, and consider the system of $m+1$ equations in $n+1$ variables, $X_1,\ldots,X_n,Y$,

$$\begin{cases} g_i(X_1,\ldots,X_n) &= 0, \quad i=1,\ldots,m \\ 1-Yh(X_1,\ldots,X_n) &= 0. \end{cases}$$

If $(a_1,\ldots,a_n,b)$ satisfies the first m equations, then $(a_1,\ldots,a_n)\in Z(\mathfrak{a})$; consequently, $h(a_1,\ldots,a_n)=0$, and $(a_1,\ldots,a_n,b)$ doesn't satisfy the last equation. Therefore, the equations are inconsistent, and so, according to the Nullstellensatz (11.5), the ideal

$$(g_1,\ldots,g_m,1-Yh)=k[X_1,\ldots,X_n,Y]$$

and there exist $f_i\in k[X_1,\ldots,X_n,Y]$ such that

$$1=\sum_{i=1}^{m} f_i\cdot g_i+f_{m+1}\cdot(1-Yh).$$

On applying the homomorphism

$$\begin{cases} X_i\mapsto X_i \\ Y\mapsto h^{-1} \end{cases} :k[X_1,\ldots,X_n,Y]\to k(X_1,\ldots,X_n)$$

to the above equality, we obtain the identity

$$1=\sum\nolimits_i f_i(X_1,\ldots,X_n,h^{-1})\cdot g_i(X_1,\ldots,X_n) \tag{1}$$

in $k(X_1,\ldots,X_n)$. Clearly

$$f_i(X_1,\ldots,X_n,h^{-1})=\frac{\text{polynomial in } X_1,\ldots,X_n}{h^{N_i}}$$

for some N_i. Let N be the largest of the N_i. On multiplying (1) by h^N we obtain an identity

$$h^N=\sum\nolimits_i (\text{polynomial in } X_1,\ldots,X_n)\cdot g_i(X_1,\ldots,X_n),$$

which shows that $h^N\in\mathfrak{a}$. □

PROPOSITION 11.8. *The radical of an ideal $\mathfrak{a}$ in a finitely generated k-algebra A is equal to the intersection of the maximal ideals containing it:* $\mathrm{rad}(\mathfrak{a})=\bigcap_{\mathfrak{m}\supset\mathfrak{a}}\mathfrak{m}$. *In particular, if A is reduced, then $\bigcap_{\mathfrak{m}\ \mathit{maximal}}\mathfrak{m}=0$.*

PROOF. Because of the correspondence (2), p.3, it suffices to prove this for $A = k[X_1, \ldots, X_n]$.

Let $\mathfrak{a}$ be an ideal in $k[X_1, \ldots, X_n]$. Because $\mathrm{rad}(\mathfrak{a})$ is the smallest radical ideal containing $\mathfrak{a}$ and maximal ideals are radical $\mathrm{rad}(\mathfrak{a}) \subset \bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$. Conversely, suppose h is contained in all maximal ideals containing $\mathfrak{a}$, and let $(a_1, \ldots, a_n) \in Z(\mathfrak{a})$. The evaluation map

$$f \mapsto f(a_1, \ldots, a_n) : k[X_1, \ldots, X_n] \to k^{\mathrm{al}}$$

has image a subring of k^{al} which is algebraic over k, and hence is a field (see §1). Therefore, the kernel of the map is a maximal ideal, which contains $\mathfrak{a}$, and therefore also contains h. This shows that $h(a_1, \ldots, a_n) = 0$, and we conclude from the strong Nullstellensatz that $h \in \mathrm{rad}(\mathfrak{a})$. □

12 The max spectrum of a ring

Let A be a ring, and let V be the set of maximal ideals in A. For an ideal $\mathfrak{a}$ in A, let

$$V(\mathfrak{a}) = \{\mathfrak{m} \in V \mid \mathfrak{m} \supset \mathfrak{a}\}.$$

PROPOSITION 12.1. *There are the following relations:*

(a) $\mathfrak{a} \subset \mathfrak{b} \implies V(\mathfrak{a}) \supset V(\mathfrak{b})$;

(b) $V(0) = V$; $\quad V(A) = \emptyset$;

(c) $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;

(d) $V(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} V(\mathfrak{a}_i)$ *for any family of ideals* $(\mathfrak{a}_i)_{i \in I}$.

PROOF. The first two statements are obvious. For (c), note that

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{b} \implies V(\mathfrak{a}\mathfrak{b}) \supset V(\mathfrak{a} \cap \mathfrak{b}) \supset V(\mathfrak{a}) \cup V(\mathfrak{b}).$$

For the reverse inclusions, observe that if $\mathfrak{m} \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$, then there exist an $f \in \mathfrak{a} \smallsetminus \mathfrak{m}$ and a $g \in \mathfrak{b} \smallsetminus \mathfrak{m}$; but then $fg \in \mathfrak{a}\mathfrak{b} \smallsetminus \mathfrak{m}$, and so $\mathfrak{m} \notin V(\mathfrak{a}\mathfrak{b})$. For (d) recall that, by definition, $\sum \mathfrak{a}_i$ consists of all finite sums of the form $\sum f_i$, $f_i \in \mathfrak{a}_i$. Thus (d) is obvious. □

Statements (b), (c), and (d) show that the sets $V(\mathfrak{a})$ satisfy the axioms to be the closed subsets for a topology on V: both the whole space and the empty set are closed; a finite union of closed sets is closed; an arbitrary intersection of closed sets is closed. This topology is called the *Zariski topology* on V. We let $\mathrm{spm}(A)$ denote the set of maximal ideals in A endowed with its Zariski topology.

For $h \in A$, let

$$D(h) = \{\mathfrak{m} \in V \mid h \notin \mathfrak{m}\}.$$

Then $D(h)$ is open in V, being the complement of $V((h))$. If S is a set of generators for an ideal $\mathfrak{a}$, then

$$V \smallsetminus V(\mathfrak{a}) = \bigcup_{h \in S} D(h),$$

and so the sets $D(h)$ form a base for the topology on V. Note that, because maximal ideals are prime,

$$D(h_1 \cdots h_n) = D(h_1) \cap \cdots \cap D(h_n).$$

For any element h of A, $\mathrm{spm}(A_h) \simeq D(h)$ (see 6.4), and for any ideal $\mathfrak{a}$ in A, $\mathrm{spm}(A)/\mathfrak{a} \simeq V(\mathfrak{a})$ (isomorphisms of topological spaces).

The ideals in a finite product of rings $A = A_1 \times \cdots \times A_n$ are all of the form $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_n$ with $\mathfrak{a}_i$ an ideal in A_i (cf. p.7). The prime (resp. maximal) ideals are those of the form

$$A_1 \times \cdots \times A_{i-1} \times \mathfrak{a}_i \times A_{i+1} \times \cdots \times A_n$$

with $\mathfrak{a}_i$ prime (resp. maximal). It follows that $\mathrm{spm}(A) = \bigsqcup_i \mathrm{spm}(A_i)$ (disjoint union of open subsets).

THE MAX SPECTRUM OF A FINITELY GENERATED k-ALGEBRA

Let k be a field, and let A be a finitely generated k-algebra. For any maximal ideal $\mathfrak{m}$ of A, the field $k(\mathfrak{m}) \overset{\text{def}}{=} A/\mathfrak{m}$ is a finitely generated k-algebra, and so $k(\mathfrak{m})$ is finite over k (Zariski's lemma, 11.1). In particular, it equals $k(\mathfrak{m}) = k$ when k is algebraically closed.

Now fix an algebraic closure k^{al}. The image of any k-algebra homomorphism $A \to k^{\mathrm{al}}$ is a subring of k^{al} which is an integral domain algebraic over k and therefore a field (see §1). Hence the kernel of the homomorphism is a maximal ideal in A. In this way, we get a surjective map

$$\mathrm{Hom}_{k\text{-alg}}(A, k^{\mathrm{al}}) \to \mathrm{spm}(A). \quad (1)$$

Two homomorphisms $A \to k^{\mathrm{al}}$ with the same kernel $\mathfrak{m}$ factor as

$$A \to k(\mathfrak{m}) \to k^{\mathrm{al}},$$

and so differ by an automorphism[16] of k^{al}. Therefore, the fibres of (1) are exactly the orbits of $\mathrm{Gal}(k^{\mathrm{al}}/k)$. When k is perfect, each extension $k(\mathfrak{m})/k$ is separable, and so each orbit has $[k(\mathfrak{m}){:}k]$ elements, and when k is algebraically closed, the map (1) is a bijection.

Set $A = k[X_1, \ldots, X_n]/\mathfrak{a}$. Then to give a homomorphism $A \to k^{\mathrm{al}}$ is the same as giving an n-tuple $(a_1, \ldots, a_n)$ of elements of k^{al} (the images of the X_i) such that $f(a_1, \ldots, a_n) = 0$ for all $f \in \mathfrak{a}$, i.e., an element of the zero-set $Z(\mathfrak{a})$ of $\mathfrak{a}$. The homomorphism corresponding to $(a_1, \ldots, a_n)$ maps $k(\mathfrak{m})$ isomorphically onto the subfield of k^{al} generated by the a_i's. Therefore, we have a canonical surjection

$$Z(\mathfrak{a}) \to \mathrm{spm}(A) \quad (2)$$

whose fibres are the orbits of $\mathrm{Gal}(k^{\mathrm{al}}/k)$. When the field k is perfect, each orbit has $[k[a_1, \ldots, a_n] : k]$-elements, and when k is algebraically closed, $Z(\mathfrak{a}) \simeq \mathrm{spm}(A)$.

ASIDE 12.2. Let $k = \mathbb{R}$ or $\mathbb{C}$. Let X be a set and let A be a k-algebra of k-valued functions on X. In analysis, X is called the *spectrum* of A if, for each k-algebra homomorphism $\varphi\colon A \to k$, there exists a unique $x \in X$ such that $\varphi(f) = f(x)$ for all $f \in A$, and every x arises from a φ (cf. Cartier 2007, 3.3.1, footnote).

Let A be a finitely generated algebra over an arbitrary algebraically closed field k, and let $X = \mathrm{spm}(A)$. An element f of A defines a k-valued function

$$\mathfrak{m} \mapsto f \mod \mathfrak{m}$$

on X. When A is reduced, Proposition 11.8 shows that this realizes A as a ring of k-valued functions on X. Moreover, because (2) is an isomorphism in this case, for each k-algebra homomorphism $\varphi\colon A \to k$, there exists a unique $x \in X$ such that $\varphi(f) = f(x)$ for all $f \in A$. In particular, when $k = \mathbb{C}$ and A is reduced, $\mathrm{spm}(A)$ is the spectrum of A in the sense of analysis.

[16]Let f and g be two k-homomorphisms from a finite field extension k' of k into k^{al}. We consider the set of pairs (K, α) in which α is a k-homomorphism from a subfield K of k^{al} containing $f(k')$ into k^{al} such that $\alpha \circ f = g$. The set is nonempty, and Zorn's lemma can be applied to show that it has a maximal element (K', α'). For such an element K' will be algebraically closed, and hence equal to k^{al}.

JACOBSON RINGS

DEFINITION 12.3. A ring A is *Jacobson* if every prime ideal in A is an intersection of maximal ideals.

A field is Jacobson. The ring $\mathbb{Z}$ is Jacobson because every nonzero prime ideal is maximal and $(0) = \bigcap_{p=2,3,5,\ldots}(p)$. A principal ideal domain (more generally, a Dedekind domain) is Jacobson if it has infinitely many maximal ideals.[17] A local ring is Jacobson if and only if its maximal ideal is its only prime ideal. Proposition 11.8 shows that every finitely generated algebra over a field is Jacobson.

PROPOSITION 12.4. *The radical of an ideal in a Jacobson ring is equal to the intersection of the maximal ideals containing it. (Therefore, the radical ideals are precisely the intersections of maximal ideals.)*

PROOF. Proposition 2.5 says that the radical of an ideal is an intersection of prime ideals, and so this follows from the definition of a Jacobson ring. □

ASIDE 12.5. Any ring of finite type over a Jacobson ring is a Jacobson ring (EGA IV 10.4.6). Moreover, if B is of finite type over A and A is Jacobson, then the map $A \to B$ defines a continuous map $\mathrm{spm}(B) \to \mathrm{spm}(A)$.

THE TOPOLOGICAL SPACE $\mathrm{spm}(A)$

We study more closely the Zariski topology on $\mathrm{spm}(A)$. For each subset S of A, let $V(S)$ denote the set of maximal ideals containing S, and for each subset W of $\mathrm{spm}(A)$, let $I(W)$ denote the intersection of the maximal ideals in W:

$$S \subset A, \qquad V(S) = \{\mathfrak{m} \in \mathrm{spm}(A) \mid S \subset \mathfrak{m}\},$$
$$W \subset \mathrm{spm}(A), \qquad I(W) = \bigcap\nolimits_{\mathfrak{m} \in W} \mathfrak{m}.$$

Thus $V(S)$ is a closed subset of $\mathrm{spm}(A)$ and $I(W)$ is a radical ideal in A. If $V(\mathfrak{a}) \supset W$, then $\mathfrak{a} \subset I(W)$, and so $V(\mathfrak{a}) \supset VI(W)$. Therefore $VI(W)$ is the closure of W (smallest closed subset of $\mathrm{spm}(A)$ containing W); in particular, $VI(W) = W$ if W is closed.

PROPOSITION 12.6. *Let V be a closed subset of* $\mathrm{spm}(A)$.

(a) The points of V are closed for the Zariski topology.

(b) If A is noetherien, then every ascending chain of open subsets $U_1 \subset U_2 \subset \cdots$ of V eventually becomes constant; equivalently, every descending chain of closed subsets of V eventually becomes constant.

(c) If A is noetherian, every open covering of V has a finite subcovering.

PROOF. (a) Clearly $\{\mathfrak{m}\} = V(\mathfrak{m})$, and so it is closed.

(b) We prove the second statement. A sequence $V_1 \supset V_2 \supset \cdots$ of closed subsets of V gives rise to a sequence of ideals $I(V_1) \subset I(V_2) \subset \ldots$, which eventually becomes constant. If $I(V_m) = I(V_{m+1})$, then $VI(V_m) = VI(V_{m+1})$, i.e., $V_m = V_{m+1}$.

[17] In a principal ideal domain, a nonzero element a factors as $a = up_1^{r_1} \cdots p_s^{r_s}$ with u a unit and the p_i prime. The only prime divisors of a are $p_1, \ldots, p_s$, and so a is contained in only finitely many prime ideals. Similarly, in a Dedekind domain, a nonzero ideal $\mathfrak{a}$ factors as $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$ with the $\mathfrak{p}_i$ prime ideals (cf. 14.17 below), and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the only prime ideals containing $\mathfrak{a}$. On taking $\mathfrak{a} = (a)$, we see that again a is contained in only finitely many prime ideals.

(c) Let $V = \bigcup_{i \in I} U_i$ with each U_i open. Choose an $i_0 \in I$; if $U_{i_0} \neq V$, then there exists an $i_1 \in I$ such that $U_{i_0} \subsetneqq U_{i_0} \cup U_{i_1}$. If $U_{i_0} \cup U_{i_1} \neq V$, then there exists an $i_2 \in I$ etc.. Because of (b), this process must eventually stop. □

A topological space V having the property (b) is said to be *noetherian*. This condition is equivalent to the following: every nonempty set of closed subsets of V has a minimal element. A topological space V having property (c) is said to be *quasicompact* (by Bourbaki at least; others call it compact, but Bourbaki requires a compact space to be Hausdorff). The proof of (c) shows that every noetherian space is quasicompact. Since an open subspace of a noetherian space is again noetherian, it will also be quasicompact.

DEFINITION 12.7. A nonempty topological space is said to be *irreducible* if it is not the union of two proper closed subsets. Equivalent conditions: any two nonempty open subsets have a nonempty intersection; every nonempty open subset is dense.

If an irreducible space W is a finite union of closed subsets, $W = W_1 \cup \ldots \cup W_r$, then $W = W_1$ or $W_2 \cup \ldots \cup W_r$; if the latter, then $W = W_2$ or $W_3 \cup \ldots \cup W_r$, etc.. Continuing in this fashion, we find that $W = W_i$ for some i.

The notion of irreducibility is not useful for Hausdorff topological spaces, because the only irreducible Hausdorff spaces are those consisting of a single point — two points would have disjoint open neighbourhoods.

PROPOSITION 12.8. *Let W be a closed subset of* $\operatorname{spm}(A)$. *If W is irreducible, then $I(W)$ is prime; the converse is true if A is a Jacobson ring. In particular, the max spectrum of a Jacobson ring A is irreducible if and only if the nilradical of A is prime.*

PROOF. $\Rightarrow$: Let W be an irreducible closed subset of $\operatorname{spm}(A)$, and suppose $fg \in I(W)$. Then fg lies in each $\mathfrak{m}$ in W, and so either $f \in \mathfrak{m}$ or $g \in \mathfrak{m}$; hence $W \subset V(f) \cup V(g)$, and so

$$W = (W \cap V(f)) \cup (W \cap V(g)).$$

As W is irreducible, one of these sets, say $W \cap V(f)$, must equal W. But then $f \in I(W)$. We have shown that $I(W)$ is prime.

$\Leftarrow$: Assume $I(W)$ is prime, and suppose $W = V(\mathfrak{a}) \cup V(\mathfrak{b})$ with $\mathfrak{a}$ and $\mathfrak{b}$ radical ideals — we have to show that W equals $V(\mathfrak{a})$ or $V(\mathfrak{b})$. Recall that $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$ (see 12.1c) and that $\mathfrak{a} \cap \mathfrak{b}$ is radical; hence $I(W) = \mathfrak{a} \cap \mathfrak{b}$ (by 12.4). If $W \neq V(\mathfrak{a})$, then there exists an $f \in \mathfrak{a} \smallsetminus I(W)$. For all $g \in \mathfrak{b}$,

$$fg \in \mathfrak{a} \cap \mathfrak{b} = I(W).$$

Because $I(W)$ is prime, this implies that $\mathfrak{b} \subset I(W)$; therefore $W \subset V(\mathfrak{b})$. □

Thus, in the max spectrum of a Jacobson ring, there are one-to-one correspondences

$$\begin{aligned} \text{radical ideals} &\leftrightarrow \text{closed subsets} \\ \text{prime ideals} &\leftrightarrow \text{irreducible closed subsets} \\ \text{maximal ideals} &\leftrightarrow \text{one-point sets.} \end{aligned}$$

EXAMPLE 12.9. Let $f \in k[X_1,\ldots,X_n]$. According to Theorem 4.6, $k[X_1,\ldots,X_n]$ is a unique factorization domain, and so (f) is a prime ideal if and only if f is irreducible (4.1). Thus

$$V(f) \text{ is irreducible} \iff f \text{ is irreducible.}$$

On the other hand, suppose f factors,

$$f = \prod f_i^{m_i}, \quad f_i \text{ distinct irreducible polynomials.}$$

Then

$$\begin{aligned} (f) &= \bigcap (f_i^{m_i}), \quad (f_i^{m_i}) \text{ distinct ideals,} \\ \mathrm{rad}((f)) &= \bigcap (f_i), \quad (f_i) \text{ distinct prime ideals,} \\ V(f) &= \bigcup V(f_i), \quad V(f_i) \text{ distinct irreducible algebraic sets.} \end{aligned}$$

PROPOSITION 12.10. *Let V be a noetherian topological space. Then V is a finite union of irreducible closed subsets, $V = V_1 \cup \ldots \cup V_m$. If the decomposition is irredundant in the sense that there are no inclusions among the V_i, then the V_i are uniquely determined up to order.*

PROOF. Suppose that V can not be written as a *finite* union of irreducible closed subsets. Then, because V is noetherian, there will be a closed subset W of V that is minimal among those that cannot be written in this way. But W itself cannot be irreducible, and so $W = W_1 \cup W_2$, with each W_i a proper closed subset of W. Because W is minimal, both W_1 and W_2 can be expressed as finite unions of irreducible closed subsets, but then so can W. We have arrived at a contradiction.

Suppose that

$$V = V_1 \cup \ldots \cup V_m = W_1 \cup \ldots \cup W_n$$

are two irredundant decompositions. Then $V_i = \bigcup_j (V_i \cap W_j)$, and so, because V_i is irreducible, $V_i = V_i \cap W_j$ for some j. Consequently, there exists a function $f\colon \{1,\ldots,m\} \to \{1,\ldots,n\}$ such that $V_i \subset W_{f(i)}$ for each i. Similarly, there is a function $g\colon \{1,\ldots,n\} \to \{1,\ldots,m\}$ such that $W_j \subset V_{g(j)}$ for each j. Since $V_i \subset W_{f(i)} \subset V_{gf(i)}$, we must have $gf(i) = i$ and $V_i = W_{f(i)}$; similarly $fg = \mathrm{id}$. Thus f and g are bijections, and the decompositions differ only in the numbering of the sets. □

The V_i given uniquely by the proposition are called the *irreducible components* of V. They are the maximal closed irreducible subsets of V. In Example 12.9, the $V(f_i)$ are the irreducible components of $V(f)$.

COROLLARY 12.11. *A radical ideal $\mathfrak{a}$ in a noetherian Jacobson ring is a finite intersection of prime ideals, $\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$; if there are no inclusions among the $\mathfrak{p}_i$, then the $\mathfrak{p}_i$ are uniquely determined up to order.*

PROOF. Write $V(\mathfrak{a})$ as a union of its irreducible components, $V(\mathfrak{a}) = \bigcup V_i$, and take $\mathfrak{p}_i = I(V_i)$. □

REMARK 12.12. (a) An irreducible topological space is connected, but a connected topological space need not be irreducible. For example, $Z(X_1X_2)$ is the union of the coordinate axes in k^2, which is connected but not irreducible. A closed subset V of $\mathrm{spm}(A)$ is not connected if and only if there exist ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{a}\cap\mathfrak{b} = I(V)$ and $\mathfrak{a}+\mathfrak{b} = A$.

(b) A Hausdorff space is noetherian if and only if it is finite, in which case its irreducible components are the one-point sets.

(c) In a noetherian ring, every proper ideal $\mathfrak{a}$ has a decomposition into primary ideals: $\mathfrak{a} = \bigcap \mathfrak{q}_i$ (see §14). For radical ideals, this becomes a simpler decomposition into prime ideals, as in the corollary. For an ideal (f) in $k[X_1,\ldots,X_n]$ with $f = \prod f_i^{m_i}$, it is the decomposition $(f) = \bigcap (f_i^{m_i})$ noted in Example 12.9.

MAPS OF MAX SPECTRA

Let $\varphi\colon A \to B$ be a homomorphism of finitely generated k-algebras (k a field). Because B is finitely generated over k, its quotient $B/\mathfrak{m}$ by any maximal ideal $\mathfrak{m}$ is a finite field extension of k (Zariski's lemma, 11.1). Therefore the image of A in $B/\mathfrak{m}$ is an integral domain finite over k, and hence is a field (see §1). Since this image is isomorphic to $A/\varphi^{-1}(\mathfrak{m})$, this shows that the ideal $\varphi^{-1}(\mathfrak{m})$ is maximal in A. Therefore φ defines a map

$$\varphi^*\colon \mathrm{spm}(B) \to \mathrm{spm}(A), \quad \mathfrak{m} \mapsto \varphi^{-1}(\mathfrak{m}),$$

which is continuous because $(\varphi^*)^{-1}(D(f)) = D(\varphi(f))$. In this way, spm becomes a functor from finitely generated k-algebras to topological spaces.

THEOREM 12.13. *Let $\varphi\colon A \to B$ be a homomorphism of finitely generated k-algebras. Let U be a nonempty open subset of* $\mathrm{spm}(B)$, *and let $\varphi^*(U)^-$ be the closure of its image in* $\mathrm{spm}(A)$. *Then $\varphi^*(U)$ contains a nonempty open subset of each irreducible component of $\varphi^*(U)^-$.*

PROOF. Let $W = \mathrm{spm}(B)$ and $V = \mathrm{spm}(A)$, so that φ^* is a continuous map $W \to V$.

We first prove the theorem in the case that φ is an injective homomorphism of integral domains. For some $b \neq 0$, $D(b) \subset U$. According to Proposition 12.14 below, there exists a nonzero element $a \in A$ such that every homomorphim $\alpha\colon A \to k^{\mathrm{al}}$ such that $\alpha(a) \neq 0$ extends to a homomorphism $\beta\colon B \to k^{\mathrm{al}}$ such that $\beta(b) \neq 0$. Let $\mathfrak{m} \in D(a)$, and choose α to be a homomorphism $A \to k^{\mathrm{al}}$ with kernel $\mathfrak{m}$. The kernel of β is a maximal ideal $\mathfrak{n} \in D(b)$ such that $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$, and so $D(a) \subset \varphi^*(D(b))$.

We now prove the general case. If $W_1,\ldots,W_r$ are the irreducible components of W, then $\varphi^*(W)^-$ is a union of the sets $\varphi^*(W_i)^-$, and any irreducible component C of $\varphi^*(U)^-$ is contained in one of $\varphi^*(W_i)^-$, say $\varphi^*(W_1)^-$. Let $\mathfrak{q} = I(W_1)$ and let $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. Because W_1 is irreducible, they are both prime ideals. The homomorphism $\varphi\colon A \to B$ induces an injective homomorphism $\bar\varphi\colon A/\mathfrak{p} \to B/\mathfrak{q}$, and $\bar\varphi^*$ can be identified with the restriction of φ^* to W_1. From the first case, we know that $\bar\varphi^*(U \cap W_1)$ contains a nonempty open subset of C, which implies that $\varphi^*(U)$ does also. □

In the next two statements, A and B are arbitrary commutative rings — they need not be k-algebras.

PROPOSITION 12.14. *Let $A \subset B$ be integral domains with B finitely generated as an algebra over A, and let b be a nonzero element of B. Then there exists an element $a \neq 0$ in A with the following property: every homomorphism $\alpha\colon A \to \Omega$ from A into an algebraically closed field Ω such that $\alpha(a) \neq 0$ can be extended to a homomorphism $\beta\colon B \to \Omega$ such that $\beta(b) \neq 0$.*

We first need a lemma.

LEMMA 12.15. *Let $B \supset A$ be integral domains, and assume $B = A[t] = A[T]/\mathfrak{a}$. Let $\mathfrak{c} \subset A$ be the ideal of leading coefficients of the polynomials in $\mathfrak{a}$. Then every homomorphism $\alpha: A \to \Omega$ from A into an algebraically closed field Ω such that $\alpha(\mathfrak{c}) \neq 0$ can be extended to a homomorphism of B into Ω.*

PROOF. If $\mathfrak{a} = 0$, then $\mathfrak{c} = 0$, and every α extends. Thus we may assume $\mathfrak{a} \neq 0$. Let α be a homomorphism $A \to \Omega$ such that $\alpha(\mathfrak{c}) \neq 0$. Then there exist polynomials $a_m T^m + \cdots + a_0$ in $\mathfrak{a}$ such that $\alpha(a_m) \neq 0$, and we choose one, denoted f, of minimum degree. Because $B \neq 0$, the polynomial f is nonconstant.

Extend α to a homomorphism $A[T] \to \Omega[T]$, again denoted α, by sending T to T, and consider the subset $\alpha(\mathfrak{a})$ of $\Omega[T]$.

FIRST CASE: $\alpha(\mathfrak{a})$ DOES NOT CONTAIN A NONZERO CONSTANT. If the Ω-subspace of $\Omega[T]$ spanned by $\alpha(\mathfrak{a})$ contained 1, then so also would $\alpha(\mathfrak{a})$,[18] contrary to hypothesis. Because

$$T \cdot \sum c_i \alpha(g_i) = \sum c_i \alpha(g_i T), \quad c_i \in \Omega, \quad g_i \in \mathfrak{a},$$

this Ω-subspace an ideal, which we have shown to be proper, and so it has a zero c in Ω. The composite of the homomorphisms

$$A[T] \xrightarrow{\alpha} \Omega[T] \longrightarrow \Omega, \qquad T \mapsto T \mapsto c,$$

factors through $A[T]/\mathfrak{a} = B$ and extends α.

SECOND CASE: $\alpha(\mathfrak{a})$ CONTAINS A NONZERO CONSTANT. This means that $\mathfrak{a}$ contains a polynomial

$$g(T) = b_n T^n + \cdots + b_0 \quad \text{such that} \quad \alpha(b_0) \neq 0, \quad \alpha(b_1) = \alpha(b_2) = \cdots = 0.$$

On dividing $f(T)$ into $g(T)$ we obtain an equation

$$a_m^d g(T) = q(T) f(T) + r(T), \quad d \in \mathbb{N}, \quad q, r \in A[T], \quad \deg r < m.$$

When we apply α, this becomes

$$\alpha(a_m)^d \alpha(b_0) = \alpha(q)\alpha(f) + \alpha(r).$$

Because $\alpha(f)$ has degree $m > 0$, we must have $\alpha(q) = 0$, and so $\alpha(r)$ is a nonzero constant. After replacing $g(T)$ with $r(T)$, we may suppose $n < m$. If $m = 1$, such a $g(T)$ can't exist, and so we may suppose $m > 1$ and (by induction) that the lemma holds for smaller values of m.

For $h(T) = c_r T^r + c_{r-1} T^{r-1} + \cdots + c_0$, let $h'(T) = c_r + \cdots + c_0 T^r$. Then the A-module generated by the polynomials $T^s h'(T)$, $s \geq 0$, $h \in \mathfrak{a}$, is an ideal $\mathfrak{a}'$ in $A[T]$. Moreover, $\mathfrak{a}'$ contains a nonzero constant if and only if $\mathfrak{a}$ contains a nonzero polynomial cT^r, which implies $t = 0$ and $A = B$ (since B is an integral domain).

When $\mathfrak{a}'$ does not contain a nonzero constant, we set $B' = A[T]/\mathfrak{a}' = A[t']$. Then $\mathfrak{a}'$ contains the polynomial $g' = b_n + \cdots + b_0 T^n$, and $\alpha(b_0) \neq 0$. Because $\deg g' < m$, the

[18] Use that, if a system of linear equation with coefficients in a field k has a solution in some larger field, then it has a solution in k.

induction hypothesis implies that α extends to a homomorphism $B' \to \Omega$. Therefore, there exists a $c \in \Omega$ such that, for all $h(T) = c_r T^r + c_{r-1} T^{r-1} + \cdots + c_0 \in \mathfrak{a}$,

$$h'(c) = \alpha(c_r) + \alpha(c_{r-1})c + \cdots + c_0 c^r = 0.$$

On taking $h = g$, we see that $c = 0$, and on taking $h = f$, we obtain the contradiction $\alpha(a_m) = 0$. □

PROOF (OF 12.14) Suppose that we know the proposition in the case that B is generated by a single element, and write $B = A[t_1, \ldots, t_n]$. Then there exists an element b_{n-1} such that any homomorphism $\alpha\colon A[t_1, \ldots, t_{n-1}] \to \Omega$ such that $\alpha(b_{n-1}) \neq 0$ extends to a homomorphism $\beta\colon B \to \Omega$ such that $\beta(b) \neq 0$. Continuing in this fashion (with b_{n-1} for b), we eventually obtain an element $a \in A$ with the required property.

Thus we may assume $B = A[t]$. Let $\mathfrak{a}$ be the kernel of the homomorphism $T \mapsto t$, $A[T] \to A[t]$.

Case (i). The ideal $\mathfrak{a} = (0)$. Write

$$b = f(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_n, \quad a_i \in A,$$

and take $a = a_0$. If $\alpha\colon A \to \Omega$ is such that $\alpha(a_0) \neq 0$, then there exists a $c \in \Omega$ such that $f(c) \neq 0$, and we can take β to be the homomorphism $\sum d_i t^i \mapsto \sum \alpha(d_i) c^i$.

Case (ii). The ideal $\mathfrak{a} \neq (0)$. Let $f(T) = a_m T^m + \cdots + a_0$, $a_m \neq 0$, be an element of $\mathfrak{a}$ of minimum degree. Let $h(T) \in A[T]$ represent b. Since $b \neq 0$, $h \notin \mathfrak{a}$. Because f is irreducible over the field of fractions of A, it and h are coprime over that field. In other words, there exist $u, v \in A[T]$ and a nonzero $c \in A$ such that

$$uh + vf = c.$$

It follows now that ca_m satisfies our requirements, for if $\alpha(ca_m) \neq 0$, then α can be extended to $\beta\colon B \to \Omega$ by the lemma, and $\beta(u(t) \cdot b) = \beta(c) \neq 0$, and so $\beta(b) \neq 0$. □

REMARK 12.16. In case (ii) of the last proof, both b and b^{-1} are algebraic over A, and so there exist equations

$$a_0 b^m + \cdots + a_m = 0, \quad a_i \in A, \quad a_0 \neq 0;$$

$$a_0' b^{-n} + \cdots + a_n' = 0, \quad a_i' \in A, \quad a_0' \neq 0.$$

One can show that $a = a_0 a_0'$ has the property required by the proposition.

ASIDE 12.17. The spectrum $\mathrm{spec}(A)$ of a ring A is the set of prime ideals in A endowed with the topology for which the closed subsets are those of the form

$$V(\mathfrak{a}) = \{\mathfrak{p} \mid \mathfrak{p} \supset \mathfrak{a}\}, \quad \mathfrak{a} \text{ an ideal in } A.$$

Thus $\mathrm{spm}(A)$ is the subspace of $\mathrm{spec}(A)$ consisting of the closed points. When A is Jacobson, the map $U \mapsto U \cap \mathrm{spm}(A)$ is a bijection from the set of open subsets of $\mathrm{spec}(A)$ onto the set of open subsets of $\mathrm{spm}(A)$; therefore $\mathrm{spm}(A)$ and $\mathrm{spec}(A)$ have the same topologies — only the underlying sets differ.

13 Dimension theory for finitely generated k-algebras

Throughout this section, A is both a finitely generated algebra over field k and an integral domain. We define the transcendence degree of A over k, $\operatorname{tr}\deg_k A$, to be the transcendence degree over k of the field of fractions of A (see §8 of my notes Fields and Galois Theory). Thus A has transcendence degree d if it contains an algebraically independent set of d elements, but no larger set (ibid. 8.12).

PROPOSITION 13.1. *For any linear forms $\ell_1,\ldots,\ell_m$ in $X_1,\ldots,X_n$, the quotient ring*

$$k[X_1,\ldots,X_n]/(\ell_1,\ldots,\ell_m)$$

is an integral domain of transcendence degree equal to the dimension of the subspace of k^n defined by the equations

$$\ell_i = 0, \quad i = 1,\ldots,m.$$

PROOF. This follows from the more precise statement:

> Let $\mathfrak{c}$ be an ideal in $k[X_1,\ldots,X_n]$ generated by linearly independent linear forms $\ell_1,\ldots,\ell_r$, and let $X_{i_1},\ldots,X_{i_{n-r}}$ be such that
>
> $$\{\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}\}$$
>
> is a basis for the linear forms in $X_1,\ldots,X_n$. Then
>
> $$k[X_1,\ldots,X_n]/\mathfrak{c} \simeq k[X_{i_1},\ldots,X_{i_{n-r}}].$$

This is obvious if the forms ℓ_i are $X_1,\ldots,X_r$. In the general case, because $\{X_1,\ldots,X_n\}$ and $\{\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}\}$ are both bases for the linear forms, each element of one set can be expressed as a linear combination of the elements of the other. Therefore,

$$k[X_1,\ldots,X_n] = k[\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}],$$

and so

$$\begin{aligned} k[X_1,\ldots,X_n]/\mathfrak{c} &= k[\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}]/\mathfrak{c} \\ &\simeq k[X_{i_1},\ldots,X_{i_{n-r}}]. \end{aligned}$$

□

PROPOSITION 13.2. *For any irreducible polynomial f in $k[X_1,\ldots,X_n]$, the quotient ring $k[X_1,\ldots,X_n]/(f)$ has transcendence degree $n-1$.*

PROOF. Let

$$k[x_1,\ldots,x_n] = k[X_1,\ldots,X_n]/(f), \quad x_i = X_i + (f),$$

and let $k(x_1,\ldots,x_n)$ be the field of fractions of $k[x_1,\ldots,x_n]$. Since f is not zero, some X_i, say, X_n, occurs in it. Then X_n occurs in every nonzero multiple of f, and so no nonzero polynomial in $X_1,\ldots,X_{n-1}$ belongs to (f). This means that $x_1,\ldots,x_{n-1}$ are algebraically independent. On the other hand, x_n is algebraic over $k(x_1,\ldots,x_{n-1})$, and so $\{x_1,\ldots,x_{n-1}\}$ is a transcendence basis for $k(x_1,\ldots,x_n)$ over k. □

PROPOSITION 13.3. *For any nonzero prime ideal* $\mathfrak{p}$ *in a* k*-algebra* A,

$$\operatorname{tr deg}_k(A/\mathfrak{p}) < \operatorname{tr deg}_k(A).$$

PROOF. We may suppose

$$A = k[X_1,\ldots,X_n]/\mathfrak{a} = k[x_1,\ldots,x_n].$$

For $f \in A$, let $\bar{f}$ denote the image of f in $A/\mathfrak{p}$, so that $A/\mathfrak{p} = k[\bar{x}_1,\ldots,\bar{x}_n]$. Let $d = \operatorname{tr deg}_k A/\mathfrak{p}$, and number the X_i so that $\bar{x}_1,\ldots,\bar{x}_d$ are algebraically independent (for a proof that this is possible, see 8.9 of my notes Fields and Galois Theory). I shall show that, for any nonzero $f \in \mathfrak{p}$, the $d+1$ elements $x_1,\ldots,x_d, f$ are algebraically independent, which shows that $\operatorname{tr deg}_k A \geq d+1$.

Suppose otherwise. Then there is a nontrivial algebraic relation, which we can write

$$a_0(x_1,\ldots,x_d)f^m + a_1(x_1,\ldots,x_d)f^{m-1} + \cdots + a_m(x_1,\ldots,x_d) = 0,$$

with $a_i \in k[X_1,\ldots,X_d]$ and $a_0 \neq 0$. Because A is an integral domain, we can cancel a power of f if necessary to make $a_m(x_1,\ldots,x_d)$ nonzero. On applying the homomorphism $A \to A/\mathfrak{p}$ to the above equality, we find that

$$a_m(\bar{x}_1,\ldots,\bar{x}_d) = 0,$$

which contradicts the algebraic independence of $\bar{x}_1,\ldots,\bar{x}_d$. □

PROPOSITION 13.4. *Let* A *be a unique factorization domain. If* $\mathfrak{p}$ *is a prime ideal in* A *such that* $\operatorname{tr deg}_k A/\mathfrak{p} = \operatorname{tr deg}_k A - 1$, *then* $\mathfrak{p} = (f)$ *for some* $f \in A$.

PROOF. The ideal $\mathfrak{p}$ is nonzero because otherwise A and $A/\mathfrak{p}$ would have the same transcendence degree. Therefore $\mathfrak{p}$ contains a nonzero polynomial, and even an irreducible polynomial f, because it is prime. According to (4.1), the ideal (f) is prime. If $(f) \neq \mathfrak{p}$, then

$$\operatorname{tr deg}_k A/\mathfrak{p} \overset{13.3}{>} \operatorname{tr deg}_k A/(f) \overset{13.2}{=} \operatorname{tr deg}_k A - 1,$$

which contradicts the hypothesis. □

THEOREM 13.5. *Let* $f \in A$ *be neither zero nor a unit, and let* $\mathfrak{p}$ *be a prime ideal that is minimal among those containing* (f); *then*

$$\operatorname{tr deg}_k A/\mathfrak{p} = \operatorname{tr deg}_k A - 1.$$

We first need a lemma.

LEMMA 13.6. *Let* A *be an integrally closed integral domain, and let* L *be a finite extension of the field of fractions* K *of* A. *If* $\alpha \in L$ *is integral over* A, *then* $\operatorname{Nm}_{L/K}\alpha \in A$, *and* α *divides* $\operatorname{Nm}_{L/K}\alpha$ *in the ring* $A[\alpha]$.

PROOF. Let $X^r + a_{r-1}X^{r-1} + \cdots + a_0$ be the minimum polynomial of α over K. Then r divides the degree n of L/K, and $\operatorname{Nm}_{L/K}(\alpha) = \pm a_0^{\frac{n}{r}}$ (see 5.40 of my notes Fields and Galois Theory). Moreover, a_0 lies in A by (5.9). From the equation

$$0 = \alpha(\alpha^{r-1} + a_{r-1}\alpha^{r-2} + \cdots + a_1) + a_0$$

we see that α divides a_0 in $A[\alpha]$, and therefore it also divides $\operatorname{Nm}_{L/K}\alpha$. □

PROOF (OF THEOREM 13.5). Write $\operatorname{rad}(f)$ as an irredundant intersection of prime ideals $\operatorname{rad}(f) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ (see 12.11). Then $V(\mathfrak{a}) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_r)$ is the decomposition of $V(\mathfrak{a})$ into its irreducible components. There exists an $\mathfrak{m}_0 \in V(\mathfrak{p}_1) \smallsetminus \bigcup_{i\geq 2} V(\mathfrak{p}_i)$ and an open neighbourhood $D(h)$ of $\mathfrak{m}_0$ disjoint from $\bigcup_{i\geq 2} V(\mathfrak{p}_i)$. The ring A_h (resp. $A_h/S^{-1}\mathfrak{p}$) is an integral domain with the same transcendance degree as A (resp. $A/\mathfrak{p}$) — in fact, with the same field of fractions. In A_h, $\operatorname{rad}(\frac{f}{1}) = \operatorname{rad}(f)^e = \mathfrak{p}_1^e$. Therefore, after replacing A with A_h, we may suppose that $\operatorname{rad}(f)$ is prime, say, equal to $\mathfrak{p}$.

According to the Noether normalization theorem (5.11), there exist algebraically independent elements $x_1, \ldots, x_d$ in A such that A is a finite $k[x_1, \ldots, x_d]$-algebra. Note that $d = \operatorname{tr}\deg_k A$. According to the lemma, $f_0 \overset{\text{def}}{=} \operatorname{Nm}(f)$ lies in $k[x_1, \ldots, x_d]$, and we shall show that $\mathfrak{p} \cap k[x_1, \ldots, x_d] = \operatorname{rad}(f_0)$. Therefore, the homomorphism

$$k[x_1, \ldots, x_d]/\operatorname{rad}(f_0) \to A/\mathfrak{p}$$

is injective. As it is also finite, this implies that

$$\operatorname{tr}\deg_k A/\mathfrak{p} = \operatorname{tr}\deg_k k[x_1, \ldots, x_d]/\operatorname{rad}(f_0) \overset{13.2}{=} d - 1,$$

as required.

By assumption A is finite (hence integral) over its subring $k[x_1, \ldots, x_d]$. The lemma shows that f divides f_0 in A, and so $f_0 \in (f) \subset \mathfrak{p}$. Hence $(f_0) \subset \mathfrak{p} \cap k[x_1, \ldots, x_d]$, which implies

$$\operatorname{rad}(f_0) \subset \mathfrak{p} \cap k[x_1, \ldots, x_d]$$

because $\mathfrak{p}$ is radical. For the reverse inclusion, let $g \in \mathfrak{p} \cap k[x_1, \ldots, x_d]$. Then $g \in \operatorname{rad}(f)$, and so $g^m = fh$ for some $h \in A$, $m \in \mathbb{N}$. Taking norms, we find that

$$g^{me} = \operatorname{Nm}(fh) = f_0 \cdot \operatorname{Nm}(h) \in (f_0),$$

where e is the degree of the extension of the fields of fractions, which proves the claim. □

COROLLARY 13.7. *Let $\mathfrak{p}$ be a minimal nonzero prime ideal in A; then* $\operatorname{tr}\deg_k (A/\mathfrak{p}) = \operatorname{tr}\deg_k (A) - 1$.

PROOF. Let f be a nonzero element of $\mathfrak{p}$. Then f is not a unit, and $\mathfrak{p}$ is minimal among the prime ideals containing f. □

THEOREM 13.8. *The length d of any maximal (i.e., nonrefinable) chain of distinct prime ideals*

$$\mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0 \qquad (1)$$

in A is $\operatorname{tr}\deg_k (A)$. *In particular, every maximal ideal of A has height* $\operatorname{tr}\deg_k (A)$, *and so the Krull dimension of A is equal to* $\operatorname{tr}\deg_k (A)$.

PROOF. From (13.7), we find that

$$\operatorname{tr}\deg_k(A) = \operatorname{tr}\deg_k(A/\mathfrak{p}_1) + 1 = \cdots = \operatorname{tr}\deg_k(A/\mathfrak{p}_d) + d.$$

But $\mathfrak{p}_d$ is maximal, and so $A/\mathfrak{p}_d$ is a finite field extension of k. In particular, $\operatorname{tr}\deg_k(A/\mathfrak{p}_d) = 0$. □

EXAMPLE 13.9. Let $f(X,Y)$ and $g(X,Y)$ be nonconstant polynomials with no common factor. Then $k[X,Y]/(f)$ has Krull dimension 1, and so $k[X,Y]/(f,g)$ has dimension zero.

EXAMPLE 13.10. We classify the prime ideals $\mathfrak{p}$ in $A = k[X,Y]$. If $A/\mathfrak{p}$ has dimension 2, then $\mathfrak{p} = (0)$. If $A/\mathfrak{p}$ has dimension 1, then $\mathfrak{p} = (f)$ for some irreducible polynomial f of A (by 13.4). Finally, if $A/\mathfrak{p}$ has dimension zero, then $\mathfrak{p}$ is maximal. Thus, when k is algebraically closed, the prime ideals in $k[X,Y]$ are exactly the ideals (0), (f) (with f irreducible), and $(X-a, Y-b)$ (with $a,b \in k$).

REMARK 13.11. Let A be a finitely generated k-algebra (not necessarily an integral domain). Every maximal chain of prime ideals in A ending in fixed prime ideal $\mathfrak{p}$ has length $\operatorname{tr deg}_k(A/\mathfrak{p})$, and so the Krull dimension of A is $\max(\operatorname{tr deg}_k(A/\mathfrak{p}))$ where $\mathfrak{p}$ runs over the minimal prime ideals of A. In the next section, we show that a noetherian ring has only finitely many minimal prime ideals, and so the Krull dimension of A is finite.

If $x_1, \ldots, x_m$ is an algebraically independent set of elements of A such that A is a finite $k[x_1, \ldots, x_m]$-algebra, then $\dim A = m$.

14 Primary decompositions

In this section, A is an arbitrary commutative ring.

DEFINITION 14.1. An ideal $\mathfrak{q}$ in A is *primary* if it is proper and

$$ab \in \mathfrak{q},\, b \notin \mathfrak{q} \implies a^n \in \mathfrak{q} \text{ for some } n \geq 1.$$

Thus, a proper ideal $\mathfrak{q}$ in A is primary if and only if all zero-divisors in $A/\mathfrak{q}$ are nilpotent. A radical ideal is primary if and only if it is prime. An ideal (m) in $\mathbb{Z}$ is primary if and only if m is a power of a prime.

PROPOSITION 14.2. *The radical of a primary ideal $\mathfrak{q}$ is a prime ideal containing $\mathfrak{q}$, and it is contained in every other prime ideal containing $\mathfrak{q}$ (i.e., it is the smallest prime ideal containing $\mathfrak{p}$).*

PROOF. Suppose $ab \in \operatorname{rad}(\mathfrak{q})$ but $b \notin \operatorname{rad}(\mathfrak{q})$. Then some power, say $a^n b^n$, of ab lies in $\mathfrak{q}$, but $b^n \notin \mathfrak{q}$, and so $a \in \operatorname{rad}(\mathfrak{q})$. The shows that $\operatorname{rad}(\mathfrak{q})$ is primary, and hence prime (because it is radical).

Let $\mathfrak{p}$ be a second prime ideal containing $\mathfrak{q}$, and let $a \in \operatorname{rad}(\mathfrak{q})$. For some n, $a^n \in \mathfrak{q} \subset \mathfrak{p}$, which implies that $a \in \mathfrak{p}$. □

When $\mathfrak{q}$ is a primary ideal and $\mathfrak{p}$ is its radical, we say that $\mathfrak{q}$ is $\mathfrak{p}$-*primary.*

PROPOSITION 14.3. *Every ideal $\mathfrak{q}$ whose radical is a maximal ideal $\mathfrak{m}$ is primary (in fact, $\mathfrak{m}$-primary); in particular, every power of a maximal ideal $\mathfrak{m}$ is $\mathfrak{m}$-primary.*

PROOF. Every prime ideal containing $\mathfrak{q}$ contains its radical $\mathfrak{m}$, and therefore equals $\mathfrak{m}$. This shows that $A/\mathfrak{a}$ is local with maximal ideal $\mathfrak{m}/\mathfrak{a}$. Therefore, every element of $A/\mathfrak{a}$ is either a unit, and hence is not a zero-divisor, or it lies in $\mathfrak{m}/\mathfrak{a}$, and hence is nilpotent. □

PROPOSITION 14.4. *Let $\varphi\colon A \to B$ be a homomorphism of rings. If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in B, then $\mathfrak{q}^c \overset{\text{def}}{=} \varphi^{-1}(\mathfrak{q})$ is a $\mathfrak{p}^c$-primary ideal in A.*

PROOF. The map $A/\mathfrak{q}^c \to B/\mathfrak{q}$ is injective, and so every zero-divisor in $A/\mathfrak{q}^c$ is nilpotent. This shows that $\mathfrak{q}^c$ is primary, and therefore $\mathrm{rad}(\mathfrak{q}^c)$-primary. But (see 2.10), $\mathrm{rad}(\mathfrak{q}^c) = \mathrm{rad}(\mathfrak{q})^c = \mathfrak{p}^c$, as claimed. □

LEMMA 14.5. *Let $\mathfrak{q}$ and $\mathfrak{p}$ be a pair of ideals in A such that $\mathfrak{q} \subset \mathfrak{p} \subset \mathrm{rad}(\mathfrak{q})$ and*

$$ab \in \mathfrak{q} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{q}. \tag{1}$$

Then $\mathfrak{p}$ is a prime ideal and $\mathfrak{q}$ is $\mathfrak{p}$-primary.

PROOF. Clearly $\mathfrak{q}$ is primary, hence $\mathrm{rad}(\mathfrak{q})$-primary, and $\mathrm{rad}(\mathfrak{q})$ is prime. By assumption $\mathfrak{p} \subset \mathrm{rad}(\mathfrak{q})$, and it remains to show that they are equal. Let $a \in \mathrm{rad}(\mathfrak{q})$, and let n be the smallest positive integer such that $a^n \in \mathfrak{q}$. If $n = 1$, then $a \in \mathfrak{q} \subset \mathfrak{p}$; on the other hand, if $n > 1$, then $a^n = aa^{n-1} \in \mathfrak{q}$ and $a^{n-1} \notin \mathfrak{q}$, and so $a \in \mathfrak{p}$ by (1). □

PROPOSITION 14.6. *A finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

PROOF. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ be $\mathfrak{p}$-primary, and let $\mathfrak{q} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$. We show that the pair of ideals $\mathfrak{q} \subset \mathfrak{p}$ satisfies the conditions of (14.5).

Let $a \in \mathfrak{p}$; since some power of a belongs to each $\mathfrak{q}_i$, a sufficiently high power of it will belong to all of them, and so $\mathfrak{p} \subset \mathrm{rad}(\mathfrak{q})$.

Let $ab \in \mathfrak{q}$ but $a \notin \mathfrak{p}$. Then $ab \in \mathfrak{q}_i$ but $a \notin \mathfrak{p}$, and so $b \in \mathfrak{q}_i$. Since this is true for all i, we have that $b \in \mathfrak{q}$. □

The *minimal prime ideals* of an ideal $\mathfrak{a}$ are the minimal elements of the set of prime ideals containing $\mathfrak{a}$.

DEFINITION 14.7. A *primary decomposition* of an ideal $\mathfrak{a}$ is a finite set of primary ideals whose intersection is $\mathfrak{a}$. A primary decomposition S of $\mathfrak{a}$ is *minimal* if

(a) the prime ideals $\mathrm{rad}(\mathfrak{q})$, $\mathfrak{q} \in S$, are distinct, and
(b) no element of S can be omitted, i.e., for no $\mathfrak{q}_0 \in S$ is $\mathfrak{q}_0 \subset \bigcap\{\mathfrak{q} \mid \mathfrak{q} \in S, \mathfrak{q} \neq \mathfrak{q}_0\}$.

If $\mathfrak{a}$ admits a primary decomposition, then it admits a minimal primary decomposition, because Proposition 14.6 can be used to combine primary ideals with the same radical, and any $\mathfrak{q}_i$ that fails (b) can simply be omitted. The prime ideals occurring as the radical of an ideal in a minimal primary decomposition of $\mathfrak{a}$ are said to *belong to* $\mathfrak{a}$.

PROPOSITION 14.8. *Suppose $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary for $i = 1, \ldots, n$. Then the minimal prime ideals of $\mathfrak{a}$ are the minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.*

PROOF. Let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{a}$, and let $\mathfrak{q}_i'$ be the image of $\mathfrak{q}_i$ in the integral domain $A/\mathfrak{p}$. Then $\mathfrak{p}$ contains $\mathfrak{q}_1 \cdots \mathfrak{q}_n$, and so $\mathfrak{q}_1' \cdots \mathfrak{q}_n' = 0$. This implies that, for some i, $\mathfrak{q}_i' = 0$, and so $\mathfrak{p}$ contains $\mathfrak{q}_i$. Now (14.2) shows that $\mathfrak{p}$ contains $\mathfrak{p}_i$. □

In particular, if $\mathfrak{a}$ admits a primary decomposition, then it has only finitely many minimal prime ideals, and so its radical is a *finite* intersection of prime ideals.

For an ideal $\mathfrak{a}$ in A and an element $x \in A$, we let

$$(\mathfrak{a}{:}x) = \{a \in A \mid ax \in \mathfrak{a}\}.$$

It is again an ideal in A, which equals A if $x \in \mathfrak{a}$.

LEMMA 14.9. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal and let $x \in A \setminus \mathfrak{q}$. Then $(\mathfrak{q}\colon x)$ is $\mathfrak{p}$-primary (and hence $\mathrm{rad}(\mathfrak{q}\colon x) = \mathfrak{p}$).*

PROOF. For any $a \in (\mathfrak{q}\colon x)$, we know that $ax \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, and so $a \in \mathfrak{p}$. Hence $(\mathfrak{q}\colon x) \subset \mathfrak{p}$. On taking radicals, we find that $\mathrm{rad}(\mathfrak{q}\colon x) = \mathfrak{p}$. Let $ab \in (\mathfrak{q}\colon x)$. Then $xab \in \mathfrak{q}$, and so either $a \in \mathfrak{p}$ or $xb \in \mathfrak{q}$ (because $\mathfrak{q}$ is $\mathfrak{p}$-primary); in the second case, $b \in (\mathfrak{q}\colon x)$ as required. □

THEOREM 14.10. *Let $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ be a minimal primary decomposition of $\mathfrak{a}$, and let $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$. Then*

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \{\mathrm{rad}(\mathfrak{a}\colon x) \mid x \in A, \quad \mathrm{rad}(\mathfrak{a}\colon x) \text{ prime}\}.$$

In particular, the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ is independent of the choice of the minimal primary decomposition.

PROOF. For any $a \in A$,

$$(\mathfrak{a}\colon a) = (\textstyle\bigcap \mathfrak{q}_i\colon a) = \bigcap (\mathfrak{q}_i\colon a),$$

and so

$$\mathrm{rad}(\mathfrak{a}\colon a) = \mathrm{rad} \textstyle\bigcap (\mathfrak{q}_i\colon a) \overset{(14.9)}{=} \bigcap_{a \notin \mathfrak{q}_i} \mathfrak{p}_i. \tag{2}$$

If $\mathrm{rad}(\mathfrak{a}\colon a)$ is prime, then it equals one of the $\mathfrak{p}_i$ (otherwise, for each i there exists an $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$, and $a_1 \cdots a_n \in \bigcap_{a \notin \mathfrak{q}_i} \mathfrak{p}_i$ but not $\mathfrak{p}$, which is a contradiction). Hence RHS$\supset$LHS. For each i, there exists an $a \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$ because the decomposition is minimal, and (2) shows that $\mathrm{rad}(\mathfrak{a}\colon a) = \mathfrak{p}_i$. □

THEOREM 14.11. *In a noetherian ring, every ideal admits a primary decomposition.*

The theorem is a consequence of the following more precise statement, but first we need a definition: an ideal $\mathfrak{a}$ is said to be *irreducible* if

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \ (\mathfrak{b}, \mathfrak{c} \text{ ideals}) \implies \mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}.$$

PROPOSITION 14.12. *Let A be a noetherian ring.*

(a) *Every ideal in A can be expressed as a finite intersection of irreducible ideals.*
(b) *Every irreducible ideal in A is primary.*

PROOF. (a) Suppose (a) fails, and let $\mathfrak{a}$ be maximal among the ideals for which it fails. Then, in particular, $\mathfrak{a}$ itself is not irreducible, and so $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{b}$ and $\mathfrak{c}$ properly containing $\mathfrak{a}$. Because $\mathfrak{a}$ is maximal, both $\mathfrak{b}$ and $\mathfrak{c}$ can be expressed as finite intersections of irreducible ideals, but then so can $\mathfrak{a}$.

(b) Let $\mathfrak{a}$ be irreducible in A, and consider the quotient ring $A' \overset{\text{def}}{=} A/\mathfrak{a}$. Let a be a zero-divisor in A', say $ab = 0$ with $b \neq 0$. We have to show that a is nilpotent. As A' is noetherian, the chain of ideals

$$((0)\colon a) \subset ((0)\colon a^2) \subset \cdots$$

becomes constant, say, $((0)\colon a^m) = ((0)\colon a^{m+1})) = \cdots$. Let $c \in (a^m) \cap (b)$. Then $c \in (b)$ implies $ca = 0$, and $c \in (a^m)$ implies that $c = da^m$ for some $d \in A$. Now

$$(da^m)a = 0 \Rightarrow d \in (0\colon a^{m+1}) = (0\colon a^m) \Rightarrow c = 0.$$

Hence $(a^m) \cap (b) = (0)$. Because $\mathfrak{a}$ is irreducible, so also is the zero ideal in A', and it follows that $a^m = 0$. □

A $\mathfrak{p}$-primary ideal $\mathfrak{a}$ in a noetherian ring contains a power of $\mathfrak{p}$ by Proposition 3.14. The next result proves a converse when $\mathfrak{p}$ is maximal.

PROPOSITION 14.13. *Let $\mathfrak{m}$ be a maximal ideal of a noetherian ring. Any proper ideal $\mathfrak{a}$ of A that contains a power of a maximal ideal $\mathfrak{m}$ is $\mathfrak{m}$-primary.*

PROOF. Suppose that $\mathfrak{m}^r \subset \mathfrak{a}$, and let $\mathfrak{p}$ be a prime ideal belonging to $\mathfrak{a}$. Then $\mathfrak{m}^r \subset \mathfrak{a} \subset \mathfrak{p}$, so that $\mathfrak{m} \subset \mathfrak{p}$, which implies that $\mathfrak{m} = \mathfrak{p}$. Thus $\mathfrak{m}$ is the only prime ideal belonging to $\mathfrak{a}$, which means that $\mathfrak{a}$ is $\mathfrak{m}$-primary. □

EXAMPLE 14.14. We give an example of a power of a prime ideal $\mathfrak{p}$ that is not $\mathfrak{p}$-primary. Let

$$A = k[X,Y,Z]/(Y^2 - XZ) = k[x,y,z].$$

The ideal (X,Y) in $k[X,Y,Z]$ is prime and contains $(Y^2 - XZ)$, and so the ideal $\mathfrak{p} = (x,y)$ in A is prime. Now $xz = y^2 \in \mathfrak{p}^2$, but one checks easily that $x \notin \mathfrak{p}^2$ and $z \notin \mathfrak{p}$, and so $\mathfrak{p}^2$ is not $\mathfrak{p}$-primary.

REMARK 14.15. Let $\mathfrak{a}$ be an ideal in a noetherian ring, and let $\mathfrak{b} = \bigcap_{n \geq 1} \mathfrak{a}^n$. We give another proof that $\mathfrak{a}\mathfrak{b} = \mathfrak{b}$ (see p.12). Let

$$\mathfrak{a}\mathfrak{b} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s, \quad \mathrm{rad}(\mathfrak{q}_i) = \mathfrak{p}_i,$$

be a minimal primary decomposition of $\mathfrak{a}\mathfrak{b}$. We shall show that $\mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$ by showing that $\mathfrak{b} \subset \mathfrak{q}_i$ for each i.

If there exists a $b \in \mathfrak{b} \setminus \mathfrak{q}_i$, then

$$\mathfrak{a}b \subset \mathfrak{a}\mathfrak{b} \subset \mathfrak{q}_i,$$

from which it follows that $\mathfrak{a} \subset \mathfrak{p}_i$. We know that $\mathfrak{p}_i^r \subset \mathfrak{q}_i$ for some r (see 3.14), and so

$$\mathfrak{b} = \bigcap \mathfrak{a}^n \subset \mathfrak{a}^r \subset \mathfrak{p}_i^r \subset \mathfrak{q}_i,$$

which is a contradiction. This completes the proof.

DEFINITION 14.16. A *Dedekind domain* is a noetherian integrally closed integral domain of dimension 1.

THEOREM 14.17. *Every proper nonzero ideal $\mathfrak{a}$ in a Dedekind domain can be written in the form*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$$

with the $\mathfrak{p}_i$ distinct prime ideals and the $r_i > 0$; the ideals $\mathfrak{p}_i$ are exactly the prime ideals containing $\mathfrak{a}$, and the exponents r_i are uniquely determined.

PROOF. For the proof, which is quite elementary, see Chapter 3 of my notes Algebraic Number Theory. □

15 Artinian rings

A ring A is *artinian* if every descending chain of ideals $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ in A eventually becomes constant; equivalently, if every nonempty set of ideals has a minimal element. Similarly, a module M over a ring A is *artinian* if every descending chain of submodules $N_1 \supset N_2 \supset \cdots$ in M eventually becomes constant.

PROPOSITION 15.1. *An artinian ring has Krull dimension zero; in other words, every prime ideal is maximal.*

PROOF. Let $\mathfrak{p}$ be a prime ideal of an artinian ring A, and let $A' = A/\mathfrak{p}$. Then A' is an artinian integral domain. For any nonzero element a of A', the chain $(a) \supset (a^2) \supset \cdots$ eventually becomes constant, and so $a^n = a^{n+1}b$ for some $b \in A'$ and $n \geq 1$. We can cancel a^n to obtain $1 = ab$. Thus a is a unit, A' is a field, and $\mathfrak{p}$ is maximal. □

COROLLARY 15.2. *In an artinian ring, the nilradical and the Jacobson radical coincide.*

PROOF. The first is the intersection of the prime ideals (2.5), and the second is the intersection of the maximal ideals (2.6). □

PROPOSITION 15.3. *An artinian ring has only finitely many maximal ideals.*

PROOF. Let $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ be minimal among finite intersections of maximal ideals in an artinian ring, and let $\mathfrak{m}$ be another maximal ideal in the ring. If $\mathfrak{m}$ is not equal to one of the $\mathfrak{m}_i$, then, for each i, there exists an $a_i \in \mathfrak{m}_i \smallsetminus \mathfrak{m}$. Now $a_1 \cdots a_n$ lies in $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ but not in $\mathfrak{m}$ (because $\mathfrak{m}$ is prime), contradicting the minimality of $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$. □

PROPOSITION 15.4. *In an artinian ring, some power of the nilradical is zero.*

PROOF. Let $\mathfrak{N}$ be the nilradical of the artinian ring A. The chain $\mathfrak{N} \supset \mathfrak{N}^2 \supset \cdots$ eventually becomes constant, and so $\mathfrak{N}^n = \mathfrak{N}^{n+1} = \cdots$ for some $n \geq 1$. Suppose $\mathfrak{N}^n \neq 0$. Then there exist ideals $\mathfrak{a}$ such that $\mathfrak{a} \cdot \mathfrak{N}^n \neq 0$, for example $\mathfrak{N}$, and we may suppose that $\mathfrak{a}$ has been chosen to be minimal among such ideals. There exists an $a \in \mathfrak{a}$ such that $a \cdot \mathfrak{N}^n \neq 0$, and so $\mathfrak{a} = (a)$ (by minimality). Now $(a\mathfrak{N}^n)\mathfrak{N}^n = a\mathfrak{N}^{2n} = a\mathfrak{N}^n \neq 0$ and $a\mathfrak{N}^n \subset (a)$, and so $a\mathfrak{N}^n = (a)$ (by minimality again). Hence $a = ax$ for some $x \in \mathfrak{N}^n$. Now $a = ax = ax^2 = \cdots = a0 = 0$ because $x \in \mathfrak{N}$. This contradicts the definition of a, and so $\mathfrak{N}^n = 0$. □

LEMMA 15.5. *Let A be a ring in which some finite product of maximal ideals is zero. Then A is artinian if and only if it is noetherian.*

PROOF. Suppose $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$ with the $\mathfrak{m}_i$ maximal ideals (not necessarily distinct), and consider

$$A \supset \mathfrak{m}_1 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_{r-1} \supset \mathfrak{m}_1 \cdots \mathfrak{m}_r \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_n = 0.$$

The action of A on the quotient $M_r \stackrel{\text{def}}{=} \mathfrak{m}_1 \cdots \mathfrak{m}_{r-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_r$ factors through the field $A/\mathfrak{m}_r$, and the subspaces of the vector space M_r are in one-to-one correspondence with the ideals of A contained between $\mathfrak{m}_1 \cdots \mathfrak{m}_{r-1}$ and $\mathfrak{m}_1 \cdots \mathfrak{m}_r$. If A is either artinian or noetherian, then M_r satisfies a chain condition on subspaces and so it is finite-dimensional as a vector space and both artinian and noetherian as an A-module. Now repeated applications of Proposition 3.3 (resp. its analogue for artinian modules) show that if A is artinian (resp. noetherian), then it is noetherian (resp. artinian) as an A-module, and hence as a ring. □

THEOREM 15.6. *A ring is artinian if and only if it is noetherian of dimension zero.*

PROOF. $\Rightarrow$: Let A be an artinian ring. After (15.1), it remains to show that A is noetherian, but according to (15.2), (15.3), and (15.4), some finite product of maximal ideals is zero, and so this follows from the lemma.

$\Leftarrow$: Let A be a noetherian ring of dimension zero. The zero ideal admits a primary decomposition (14.11), and so A has only finitely many minimal prime ideals, which are all maximal because $\dim A = 0$. Hence $\mathfrak{N}$ is a finite intersection of maximal ideals (2.5), and since some power of $\mathfrak{N}$ is zero (3.14), we again have that some finite product of maximal ideals is zero, and so can apply the lemma. □

THEOREM 15.7. *Every artinian ring is (uniquely) a product of local artinian rings.*

PROOF. Let A be artinian, and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be the distinct maximal ideals in A. We saw in the proof of (15.6) that some product $\mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r} = 0$. For $i \neq j$, the ideal $\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j}$ is not contained in any maximal ideal, and so equals A. Now the Chinese remainder theorem 2.12 shows that

$$A \simeq A/\mathfrak{m}_1^{n_1} \times \cdots \times A/\mathfrak{m}_r^{n_r},$$

and each ring $A/\mathfrak{m}_i^{n_i}$ is obviously local. □

PROPOSITION 15.8. *Let A be a local artinian ring with maximal ideal $\mathfrak{m}$. If $\mathfrak{m}$ is principal, so also is every ideal in A; in fact, if $\mathfrak{m} = (t)$, then every ideal is of the form (t^r) for some $r \geq 0$.*

PROOF. Because $\mathfrak{m}$ is the Jacobson radical of A, some power of $\mathfrak{m}$ is zero (by 15.4); in particular, $(0) = (t^r)$ for some r. Let $\mathfrak{a}$ be a nonzero ideal in A. There exists an integer $r \geq 0$ such that $\mathfrak{a} \subset \mathfrak{m}^r$ but $\mathfrak{a} \not\subset \mathfrak{m}^{r+1}$. Therefore there exists an element a of $\mathfrak{a}$ such that $a = ct^r$ for some $c \in A$ but $a \notin (t^{r+1})$. The second condition implies that $c \notin \mathfrak{m}$, and so it is a unit; therefore $\mathfrak{a} = (a)$. □

EXAMPLE 15.9. The ring $A = k[X_1, X_2, X_3, \ldots]/(X_1, X_2^2, X_3^3, \ldots)$ has only a single prime ideal, namely, $(x_1, x_2, x_3, \ldots)$, and so has dimension zero. However, it is not noetherian (hence not artinian).

16 Dimension theory for noetherian rings

Let A be a noetherian ring and let $\mathfrak{p}$ be a prime ideal in A. Let $A_\mathfrak{p} = S^{-1}A$ where $S = A \smallsetminus \mathfrak{p}$. We begin by studying extension and contraction of ideals with respect to the homomorphism $A \to A_\mathfrak{p}$ (cf. 2.9). Recall (6.6) that $A_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}^e \stackrel{\text{def}}{=} \mathfrak{p}A_\mathfrak{p}$. The ideal

$$(\mathfrak{p}^n)^{ec} = \{a \in A \mid sa \in \mathfrak{p}^n \text{ for some } s \in S\}$$

is called the nth *symbolic power* of $\mathfrak{p}$, and is denoted $\mathfrak{p}^{(n)}$. If $\mathfrak{m}$ is maximal, then $\mathfrak{m}^{(n)} = \mathfrak{m}^n$ (see 6.7).

LEMMA 16.1. *The ideal $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.*

PROOF. According to Proposition 14.3, the ideal $(\mathfrak{p}^e)^n$ is $\mathfrak{p}^e$-primary. Hence (see 14.4), $((\mathfrak{p}^e)^n)^c$ is $(\mathfrak{p}^e)^c$-primary. But $\mathfrak{p}^{ec} = \mathfrak{p}$ (see 6.4), and

$$(((\mathfrak{p}^e)^n)^c \overset{2.10}{=} ((\mathfrak{p}^n)^e)^c \overset{\text{def}}{=} \mathfrak{p}^{(n)}. \tag{1}$$

□

LEMMA 16.2. *Consider ideals* $\mathfrak{a} \subset \mathfrak{p}' \subset \mathfrak{p}$ *with* $\mathfrak{p}'$ *prime. If* $\mathfrak{p}'$ *is a minimal prime ideal of* $\mathfrak{a}$, *then* $\mathfrak{p}'^e$ *is a minimal prime ideal of* $\mathfrak{a}^e$ *(extension relative to* $A \to A_\mathfrak{p}$*).*

PROOF. If not, there exists a prime ideal $\mathfrak{p}'' \neq \mathfrak{p}'^e$ such that $\mathfrak{p}'^e \supset \mathfrak{p}'' \supset \mathfrak{a}^e$. Now, by (6.4), $\mathfrak{p}' = \mathfrak{p}'^{ec}$ and $\mathfrak{p}''^c \neq \mathfrak{p}'^{ec}$, and so

$$\mathfrak{p}' = \mathfrak{p}'^{ec} \supsetneqq \mathfrak{p}''^c \supset \mathfrak{a}^{ec} \supset \mathfrak{a}$$

contradicts the minimality of $\mathfrak{p}'$. □

THEOREM 16.3 (KRULL'S PRINCIPAL IDEAL THEOREM). *Let A be a noetherian ring. For any nonunit* $b \in A$, *the height of a minimal prime ideal* $\mathfrak{p}$ *of* (b) *is at most one.*

PROOF. Consider $A \to A_\mathfrak{p}$. According to Lemma 16.2, $\mathfrak{p}^e$ is a minimal prime ideal of $(b)^e = (\frac{b}{1})$, and (6.4) shows that the theorem for $A_\mathfrak{p} \supset \mathfrak{p}^e \supset (\frac{b}{1})$ implies it for $A \supset \mathfrak{p} \supset (b)$. Therefore, we may replace A with $A_\mathfrak{p}$, and so assume that A is a noetherian local ring with maximal ideal $\mathfrak{p}$.

Suppose that $\mathfrak{p}$ properly contains a prime ideal $\mathfrak{p}_1$: we have to show that $\mathfrak{p}_1 \supset \mathfrak{p}_2 \implies \mathfrak{p}_1 = \mathfrak{p}_2$.

Let $\mathfrak{p}_1^{(r)}$ be the rth symbolic power of $\mathfrak{p}_1$. The only prime ideal of the ring $A/(b)$ is $\mathfrak{p}/(b)$, and so $A/(b)$ is artinian (apply 15.6). Therefore the descending chain of ideals

$$\left(\mathfrak{p}_1^{(1)} + (b)\right)/(b) \supset \left(\mathfrak{p}_1^{(2)} + (b)\right)/(b) \supset \left(\mathfrak{p}_1^{(3)} + (b)\right)/(b) \supset \cdots$$

eventually becomes constant: there exists an s such that

$$\mathfrak{p}_1^{(s)} + (b) = \mathfrak{p}_1^{(s+1)} + (b) = \mathfrak{p}_1^{(s+2)} + (b) = \cdots. \tag{2}$$

We claim that, for any $m \geq s$,

$$\mathfrak{p}_1^{(m)} \subset (b)\mathfrak{p}_1^{(m)} + \mathfrak{p}_1^{(m+1)}. \tag{3}$$

Let $x \in \mathfrak{p}_1^{(m)}$. Then

$$x \in (b) + \mathfrak{p}_1^{(m)} \overset{(2)}{=} (b) + \mathfrak{p}_1^{(m+1)},$$

and so $x = ab + x'$ with $a \in A$ and $x' \in \mathfrak{p}_1^{(m+1)}$. As $\mathfrak{p}_1^{(m)}$ is $\mathfrak{p}_1$-primary (see 16.1) and $ab = x - x' \in \mathfrak{p}_1^{(m)}$ but $b \notin \mathfrak{p}_1$, we have that $a \in \mathfrak{p}_1^{(m)}$. Now $x = ab + x' \in (b)\mathfrak{p}_1^{(m)} + \mathfrak{p}_1^{(m+1)}$ as claimed.

We next show that, for any $m \geq s$,

$$\mathfrak{p}_1^{(m)} = \mathfrak{p}_1^{(m+1)}.$$

As $b \in \mathfrak{p}$, (3) shows that $\mathfrak{p}_1^{(m)}/\mathfrak{p}_1^{(m+1)} = \mathfrak{p} \cdot \left(\mathfrak{p}_1^{(m)}/\mathfrak{p}_1^{(m+1)}\right)$, and so $\mathfrak{p}_1^{(m)}/\mathfrak{p}_1^{(m+1)} = 0$ by Nakayama's lemma (3.7).

Now
$$\mathfrak{p}_1^s \subset \mathfrak{p}_1^{(s)} = \mathfrak{p}_1^{(s+1)} = \mathfrak{p}_1^{(s+2)} = \cdots$$
and so $\mathfrak{p}_1^s \subset \bigcap_{m\geq s} \mathfrak{p}_1^{(m)}$. Note that
$$\bigcap\nolimits_{m\geq s} \mathfrak{p}_1^{(m)} \overset{(1)}{=} \bigcap\nolimits_{m\geq s} ((\mathfrak{p}_1^e)^m)^c = (\bigcap\nolimits_{m\geq s} (\mathfrak{p}_1^e)^m)^c \overset{3.13}{=} (0)^c,$$
and so for any $x \in \mathfrak{p}_1^s$, there exists an $a \in A \smallsetminus \mathfrak{p}_1$ such that $ax = 0$. Let $x \in \mathfrak{p}_1$; then $ax^s = 0$ for some $a \in A \smallsetminus \mathfrak{p}_1 \supset A \smallsetminus \mathfrak{p}_2$, and so $x \in \mathfrak{p}_2$ (because $\mathfrak{p}_2$ is prime). We have shown that $\mathfrak{p}_1 = \mathfrak{p}_2$, as required. □

In order to extend Theorem 16.6 to non principal ideals, we shall need a lemma.

LEMMA 16.4. *Let $\mathfrak{p}$ be a prime ideal in a noetherian ring A, and let S be a finite set of prime ideals in A, none of which contains $\mathfrak{p}$. If there exists a chain of distinct prime ideals*
$$\mathfrak{p} \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0,$$
then there exists such a chain with $\mathfrak{p}_1$ not contained in any ideal in S.

PROOF. We first prove this in the special case that the chain has length 2. Suppose that $\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_0$ are distinct prime ideals and that $\mathfrak{p}$ is not contained in any prime ideal in S. According to Proposition 2.8, there exists an element
$$a \in \mathfrak{p} \smallsetminus (\mathfrak{p}_0 \cup \bigcup\{\mathfrak{p}' \in S\}).$$
As $\mathfrak{p}$ contains $(a) + \mathfrak{p}_0$, it also contains a minimal prime ideal $\mathfrak{p}_1'$ of $(a) + \mathfrak{p}_0$. Now $\mathfrak{p}_1'/\mathfrak{p}_0$ is a minimal prime ideal of the *principal ideal* $((a) + \mathfrak{p}_0)/\mathfrak{p}_0$ in $A/\mathfrak{p}_0$, and so has height 1, whereas the chain $\mathfrak{p}/\mathfrak{p}_0 \supset \mathfrak{p}_1/\mathfrak{p}_0 \supset \mathfrak{p}_0/\mathfrak{p}_0$ shows that $\mathfrak{p}/\mathfrak{p}_0$ has height at least 2. Therefore $\mathfrak{p} \supset \mathfrak{p}_1' \supset \mathfrak{p}_0$ are distinct primes, and $\mathfrak{p}_1' \notin S$ because it contains a. This completes the proof of the special case.

Now consider the general case. On applying the special case to $\mathfrak{p} \supset \mathfrak{p}_{d-1} \supset \mathfrak{p}_{d-2}$, we see that there exists a chain of distinct prime ideals $\mathfrak{p} \supset \mathfrak{p}_{d-1}' \supset \mathfrak{p}_{d-2}$ such that $\mathfrak{p}_{d-1}'$ is not contained in any ideal in S. Then on applying the special case to $\mathfrak{p}_{d-1}' \supset \mathfrak{p}_{d-2} \supset \mathfrak{p}_{d-1}$, we we see that there exists a chain of distinct prime ideals $\mathfrak{p} \supset \mathfrak{p}_{d-1}' \supset \mathfrak{p}_{d-2}' \supset \mathfrak{p}_{d-2}$ such that $\mathfrak{p}_{d-2}'$ is not contained in any ideal in S. Repeat the argument until the proof is complete. □

THEOREM 16.5. *Let A be a noetherian ring. For any proper ideal $\mathfrak{a} = (a_1, \ldots, a_m)$, the height of a minimal prime ideal of $\mathfrak{a}$ is at most m.*

PROOF. For $m = 1$, this was just proved. Thus, we may suppose $m \geq 2$ and that the theorem has been proved for ideals generated by $m-1$ elements. Let $\mathfrak{p}$ be a minimal prime ideal of $\mathfrak{a}$, and let $\mathfrak{p}_1', \ldots, \mathfrak{p}_t'$ be the minimal prime ideals of $(a_2, \ldots, a_m)$. Each $\mathfrak{p}_i'$ has height at most $m-1$. If $\mathfrak{p}$ is contained in one of the $\mathfrak{p}_i'$, it will have height $\leq m-1$, and so we may suppose that it isn't.

Let $\mathfrak{p}$ have height d. We have to show that $d \leq m$. According to the lemma, there exists a chain of distinct prime ideals
$$\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0, \quad d \geq 1,$$

with $\mathfrak{p}_1$ not contained in any $\mathfrak{p}_i'$, and so Proposition 2.8 shows that there exists a

$$b \in \mathfrak{p}_1 \smallsetminus \bigcup_{i=1}^r \mathfrak{p}_i'.$$

We next show that $\mathfrak{p}$ is a minimal prime ideal of $(b, a_2, \ldots, a_m)$. Certainly $\mathfrak{p}$ contains a minimal prime ideal $\mathfrak{p}'$ of this ideal. As $\mathfrak{p}' \supset (a_2, \ldots, a_m)$, $\mathfrak{p}$ contains one of the $\mathfrak{p}_i'$s, but, by construction, it cannot equal it. If $\mathfrak{p} \neq \mathfrak{p}'$, then

$$\mathfrak{p} \supset \mathfrak{p}' \supset \mathfrak{p}_i$$

are distinct ideals, which shows that $\bar{\mathfrak{p}} \overset{\text{def}}{=} \mathfrak{p}/(a_2, \ldots, a_m)$ has height at least 2 in $\bar{A} \overset{\text{def}}{=} A/(a_2, \ldots, a_m)$. But $\bar{\mathfrak{p}}$ is a minimal ideal in $\bar{A}$ of the principal ideal $(a_1, \ldots, a_n)/(a_2, \ldots, a_n)$, which contradicts Theorem 16.3. Hence $\mathfrak{p}$ is minimal, as claimed.

But now $\mathfrak{p}/(b)$ is a minimal prime ideal of $(b, a_2, \ldots, a_m)$ in $R/(b)$, and so the height of $\mathfrak{p}/(b)$ is at most $m-1$ (by induction). The prime ideals

$$\mathfrak{p}/(b) = \mathfrak{p}_d/(b) \supset \mathfrak{p}_{d-1}/(b) \supset \cdots \supset \mathfrak{p}_1/(b)$$

are distinct, and so $d - 1 \leq m - 1$. This completes the proof that $d = m$. □

The *height* of an ideal $\mathfrak{a}$ in a noetherian ring is the minimum height of a prime ideal containing it,

$$\operatorname{ht}(\mathfrak{a}) = \min_{\mathfrak{p} \supset \mathfrak{a},\ \mathfrak{p} \text{ prime}} \operatorname{ht}(\mathfrak{p}).$$

The theorem shows that $\operatorname{ht}(\mathfrak{a})$ is finite.

The following provides a (strong) converse to Theorem 16.5.

THEOREM 16.6. *Let A be a noetherian ring, and let $\mathfrak{a}$ be a proper ideal of A of height r. Then there exist r elements $a_1, \ldots, a_r$ of $\mathfrak{a}$ such that, for each $i \leq r$, $(a_1, \ldots, a_i)$ has height i.*

PROOF. If $r = 0$, then we take the empty set of a_is. Thus, suppose $r \geq 1$. There are only finitely many prime ideals of height 0, because such an ideal is a minimal prime ideal of (0), and none of these ideals can contain $\mathfrak{a}$ because it has height ≥ 1. Proposition 2.8 shows that there exists an

$$a_1 \in \mathfrak{a} \smallsetminus \bigcup\{\text{prime ideals of height } 0\}.$$

By construction, (a_1) has height at least 1, and so Theorem 16.3 shows it has height exactly 1.

This completes the proof when $r = 1$, and so suppose that $r \geq 2$. There are only finitely many prime ideals of height 1 containing (a_1) because such an ideal is a minimal prime ideal of (a_1), and none of these ideals can contain $\mathfrak{a}$ because it has height ≥ 2. Choose

$$a_2 \in \mathfrak{a} \smallsetminus \bigcup\{\text{prime ideals of height 1 containing } (a_1)\}.$$

By construction, (a_1, a_2) has height at least 2, and so Theorem 16.5 shows that it has height exactly 2.

This completes the proof when $r = 2$, and when $r > 2$ we can continue in this fashion until it is complete.

COROLLARY 16.7. *Every prime ideal of height r in a noetherian ring arises as a minimal prime ideal for an ideal generated by r elements.*

PROOF. According to the theorem, an ideal $\mathfrak{a}$ of height r contains an ideal $(a_1,\ldots,a_r)$ of height r. If $\mathfrak{a}$ is prime, then it is a minimal ideal of $(a_1,\ldots,a_r)$. □

COROLLARY 16.8. *Let A be a commutative noetherian ring, and let $\mathfrak{a}$ be an ideal in A that can be generated by n elements. For any prime ideal $\mathfrak{p}$ in A containing $\mathfrak{a}$,*

$$\mathrm{ht}(\mathfrak{p}/\mathfrak{a}) \leq \mathrm{ht}(\mathfrak{p}) \leq \mathrm{ht}(\mathfrak{p}/\mathfrak{a}) + n.$$

PROOF. The first inequality follows immediately from the correspondence between ideals in A and in $A/\mathfrak{a}$.

Denote the quotient map $A \to A' \stackrel{\text{def}}{=} A/\mathfrak{a}$ by $a \mapsto a'$. Let $\mathrm{ht}(\mathfrak{p}/\mathfrak{a}) = d$. Then there exist elements $a_1,\ldots,a_d$ in A such that $\mathfrak{p}/\mathfrak{a}$ is a minimal prime ideal of $(a'_1,\ldots,a'_d)$. Let $b_1,\ldots,b_n$ generate $\mathfrak{a}$. Then $\mathfrak{p}$ is a minimal prime ideal of $(a_1,\ldots,a_d,b_1,\ldots,b_n)$, and hence has height $\leq d+n$. □

We now use dimension theory to prove a stronger version of "generic flatness" (9.10).

THEOREM 16.9 (GENERIC FREENESS). *Let A be a noetherian integral domain, and let B be a finitely generated A-algebra. For any finitely generated B-module M, there exists a nonzero element a of A such that M_a is a free A_a-module.*

PROOF. Let F be the field of fractions of A. We prove the theorem by induction on the Krull dimension of $F \otimes_A B$, starting with the case of Krull dimension -1. Recall that this means that $F \otimes_A B = 0$, and so $a1_B = 0$ for some nonzero $a \in A$. Then $M_a = 0$, and so the theorem is trivially true (M_a is the free A_a-module generated by the empty set).

In the general case, an argument as in (9.11) shows that, after replacing A, B, and M with A_a, B_a, and M_a for a suitable $a \in A$, we may suppose that the map $B \to F \otimes_A B$ is injective — we identify B with its image. The Noether normalization shows that there exist algebraically independent elements $x_1,\ldots,x_m$ of $F \otimes_A B$ such that $F \otimes_A B$ is a finite $F[x_1,\ldots,x_m]$-algebra. As in the proof of (9.10), there exists a nonzero $a \in A$ such that B_a is a finite $A_a[x_1,\ldots,x_m]$-algebra. Hence M_a is a finitely generated $A_a[x_1,\ldots,x_m]$-module.

As any extension of free modules is free[19], Proposition 3.5 shows that it suffices to prove the theorem for $M_a = A_a[x_1,\ldots,x_m]/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ in $A_a[x_1,\ldots,x_m]$. If $\mathfrak{p} = 0$, then M_a is free over A_a (with basis the monomials in the x_i). Otherwise, $F \otimes_A (A_a[x_1,\ldots,x_m]/\mathfrak{p})$ has Krull dimension less than that of $F \otimes_A B$, and so we can apply the induction hypothesis. □

17 Regular local rings

Throughout this section, A is a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field k. The Krull dimension d of A is equal to the height of $\mathfrak{m}$, and

$$\mathrm{ht}(\mathfrak{m}) \stackrel{(16.5)}{\leq} \text{minimum number of generators of } \mathfrak{m} \stackrel{(3.9)}{=} \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

When equality holds, the ring A is said to be *regular*. In other words, $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq d$, and equality holds exactly when the ring is regular.

[19] If M' is a submodule of M such that $M'' \stackrel{\text{def}}{=} M/M'$ is free, then $M \approx M' \oplus M''$.

For example, when A has dimension zero, it is regular if and only if its maximal ideal can be generated by the empty set, and so is zero. This means that A is a field; in particular, it is an integral domain. The main result of this section is that all regular rings are integral domains.

LEMMA 17.1. *Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$, and let $c \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$. Denote the quotient map $A \to A' \overset{\text{def}}{=} A/(c)$ by $a \mapsto a'$. Then*

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k \mathfrak{m}'/\mathfrak{m}'^2 + 1$$

where $\mathfrak{m}' \overset{\text{def}}{=} \mathfrak{m}/(c)$ is the maximal ideal of A'.

PROOF. Let $e_1, \ldots, e_n$ be elements of $\mathfrak{m}$ such that $\{e'_1, \ldots, e'_n\}$ is a k-linear basis for $\mathfrak{m}'/\mathfrak{m}'^2$. We shall show that $\{e_1, \ldots, e_n, c\}$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$.

As $e'_1, \ldots, e'_n$ span $\mathfrak{m}'/\mathfrak{m}'^2$, they generate the ideal $\mathfrak{m}'$ (see 3.9), and so $\mathfrak{m} = (e_1, \ldots, e_n) + (c)$, which implies that $\{e_1, \ldots, e_n, c\}$ spans $\mathfrak{m}/\mathfrak{m}^2$.

Suppose that $a_1, \ldots, a_{n+1}$ are elements of A such that

$$a_1 e_1 + \cdots + a_n e_n + a_{n+1} c \equiv 0 \bmod \mathfrak{m}^2. \tag{1}$$

Then

$$a'_1 e'_1 + \cdots + a'_n e'_n \equiv 0 \bmod \mathfrak{m}'^2,$$

and so $a'_1, \ldots, a'_n \in \mathfrak{m}'$. It follows that $a_1, \ldots, a_n \in \mathfrak{m}$. Now (1) shows that $a_{n+1} c \in \mathfrak{m}^2$. If $a_{n+1} \notin \mathfrak{m}$, then it is a unit in A, and $c \in \mathfrak{m}^2$, which contradicts its definition. Therefore, $a_{n+1} \in \mathfrak{m}$, and the relation (1) is the trivial one. □

PROPOSITION 17.2. *If A is regular, then so also is $A/(a)$ for any $a \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$; moreover, $\dim A = \dim A/(a) + 1$.*

PROOF. With the usual notations, (16.8) shows that

$$\operatorname{ht}(\mathfrak{m}') \leq \operatorname{ht}(\mathfrak{m}) \leq \operatorname{ht}(\mathfrak{m}') + 1.$$

Therefore

$$\dim_k(\mathfrak{m}'/\mathfrak{m}'^2) \geq \operatorname{ht}(\mathfrak{m}') \geq \operatorname{ht}(\mathfrak{m}) - 1 = \dim_k(\mathfrak{m}/\mathfrak{m}^2) - 1 = \dim_k(\mathfrak{m}'/\mathfrak{m}'^2).$$

Equalities must hold throughout, which proves that A' is regular with dimension $\dim A - 1$. □

THEOREM 17.3. *Every regular noetherian local ring is an integral domain.*

PROOF. Let A be a regular local ring of dimension d. We have already noted that the statement is true when $d = 0$.

We next prove that A is an integral domain if it contains distinct ideals $\mathfrak{a} \supset \mathfrak{p}$ with $\mathfrak{a} = (a)$ principal and $\mathfrak{p}$ prime. Let $b \in \mathfrak{p}$, and suppose $b \in \mathfrak{a}^n = (a^n)$ for some $n \geq 1$. Then $b = a^n c$ for some $c \in A$. As a is not in the prime ideal $\mathfrak{p}$, we must have that $c \in \mathfrak{p} \subset \mathfrak{a}$, and so $b \in \mathfrak{a}^{n+1}$. Continuing in this fashion, we see that $b \in \bigcap_n \mathfrak{a}^n \overset{3.13}{=} \{0\}$. Therefore $\mathfrak{p} = \{0\}$, and so A is an integral domain.

We now assume $d \geq 1$, and proceed by induction on d. Let $a \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$. As $A/(a)$ is regular of dimension $d - 1$, it is an integral domain, and so (a) is a prime ideal. If it has height 1, then the last paragraph shows that A is an integral domain. Thus, we may suppose that, for all $a \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$, the prime ideal (a) has height 0, and so is a minimal prime ideal of A. Let S be the set of all minimal prime ideals of A — recall (§14) that S is finite. We have shown that $\mathfrak{m} \smallsetminus \mathfrak{m}^2 \subset \bigcup\{\mathfrak{p} \mid \mathfrak{p} \in S\}$, and so $\mathfrak{m} \subset \mathfrak{m}^2 \cup \bigcup\{\mathfrak{p} \mid \mathfrak{p} \in S\}$. It follows from Proposition 2.8 that either $\mathfrak{m} \subset \mathfrak{m}^2$ (and hence $\mathfrak{m} = 0$) or $\mathfrak{m}$ is a minimal prime ideal of A, but both of these statements contradict the assumption that $d \geq 1$. □

COROLLARY 17.4. *A regular noetherian local ring of dimension* 1 *is a principal ideal domain (with a single nonzero prime ideal).*

PROOF. Let A be a regular local ring of dimension 1 with maximal ideal $\mathfrak{m}$,and let $\mathfrak{a}$ be a nonzero proper ideal in A. The conditions imply that $\mathfrak{m}$ is principal, say $\mathfrak{m} = (t)$. The radical of $\mathfrak{a}$ is $\mathfrak{m}$ because $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{a}$, and so $\mathfrak{a} \supset \mathfrak{m}^r$ for some r (by 3.14). The ring $A/\mathfrak{m}^r$ is local and artinian, and so $\mathfrak{a} = (t^s) + \mathfrak{m}^r$ for some $s \geq 1$ (by 15.8). This implies that $\mathfrak{a} = (t^s)$ by Nakayama's lemma (3.7). □

THEOREM 17.5. *Let A be a regular noetherian local ring.*

(a) *For any prime ideal $\mathfrak{p}$ in A, the ring $A_\mathfrak{p}$ is regular.*
(b) *The ring A is a unique factorization domain (hence is integrally closed).*

PROOF. The best proofs use homological algebra, and are (at present) beyond this primer. For an account of the theorems in the same spirit as this primer, see `http://www.math.uchicago.edu/~may/MISC/RegularLocal.pdf`. See also Matsumura 1986 19.3, 20.3.□

18 Connections with geometry

Throughout this section, k is a field.

AFFINE k-ALGEBRAS

Let A be a finitely generated k-algebra. Recall (11.8) that the nilradical of A is equal to the intersection of the maximal ideals of A.

PROPOSITION 18.1. *Let A be a finitely generated k-algebra over a perfect field k. If A is reduced, then so also is $K \otimes_k A$ for every field $K \supset k$.*

PROOF. Let (e_i) be a basis for K as a k-vector space, and suppose $\alpha = \sum e_i \otimes a_i$ is a nonzero nilpotent element in $K \otimes_k A$. Because A is reduced, there exists a maximal ideal $\mathfrak{m}$ in A such that some a_i do not belong to $\mathfrak{m}$. The image $\bar{\alpha}$ of α in $K \otimes_k (A/\mathfrak{m})$ is a nonzero nilpotent, but $A/\mathfrak{m}$ is a finite separable field extension of k, and so this is impossible.[20] □

When k is not perfect, Proposition 18.1 fails, because then k has characteristic $p \neq 0$ and it contains an element a that is not a pth power. The polynomial $X^p - a$ is irreducible in $k[X]$, but $X^p - a = (X - \alpha)^p$ in $k^{\mathrm{al}}[X]$. Therefore, $A = k[X]/(X^p - a)$ is a field, but $k^{\mathrm{al}} \otimes_k A = k^{\mathrm{al}}[X]/(X - \alpha)^p$ is not reduced.

[20] Every finite separable field extension of k is of the form $k[X]/(f(X))$ with $f(X)$ separable and therefore without repeated factors in any extension field of k; hence $K \otimes_k k[X]/(f(X)) \simeq K[X]/(f(X))$ is a product of fields.

DEFINITION 18.2. An *affine* k-algebra is a finitely generated k-algebra A such that $k^{\mathrm{al}} \otimes_k A$ is reduced.

Let A be a finitely generated k-algebra. If A is affine, then $K \otimes_k A$ is reduced for every finite extension K of k, because a k-homomorphism $K \to k^{\mathrm{al}}$ defines an injective homomorphism $K \otimes_k A \to k^{\mathrm{al}} \otimes_k A$. Conversely, if A is reduced and k is perfect, then (18.1) shows that A is affine.

PROPOSITION 18.3. *If A is an affine k-algebra and B is a reduced k-algebra, then $A \otimes_k B$ is reduced.*

PROOF. Let (e_i) be a basis for A as a k-vector space, and suppose $\alpha = \sum e_i \otimes b_i$ is a nonzero nilpotent element of $A \otimes_k B$. Let B' be the k-subalgebra of B generated by the (finitely many) nonzero b_i. Because B' is reduced, there exists a maximal ideal $\mathfrak{m}$ in B' such that some b_i do not belong to $\mathfrak{m}$. Then the image $\bar{\alpha}$ of α in $A \otimes_k (B'/\mathfrak{m})$ is a nonzero nilpotent, but $B'/\mathfrak{m}$ is a finite field extension of k (Zariski's lemma, 11.1), and so this is impossible. □

COROLLARY 18.4. *If A and B are affine k-algebras, then so also is $A \otimes_k B$.*

PROOF. By definition, $k^{\mathrm{al}} \otimes_k A$ is reduced, and $k^{\mathrm{al}} \otimes_k (A \otimes_k B) \simeq (k^{\mathrm{al}} \otimes_k A) \otimes_k B$, which is reduced by (18.2). □

LOCALLY RINGED SPACES

Let V be a topological space, and let k be a k-algebra. A *presheaf* $\mathcal{O}$ of k-algebras on V assigns to each open subset U of V a k-algebra $\mathcal{O}(U)$ and to each inclusion $U' \subset U$ a "restriction" map

$$f \mapsto f|U' : \mathcal{O}(U) \to \mathcal{O}(U');$$

when $U = U'$ the restriction map is required to be the identity map, and if

$$U'' \subset U' \subset U,$$

then the composite of the restriction maps

$$\mathcal{O}(U) \to \mathcal{O}(U') \to \mathcal{O}(U'')$$

is required to be the restriction map $\mathcal{O}(U) \to \mathcal{O}(U'')$. In other words, a presheaf is a contravariant functor to the category of k-algebras from the category whose objects are the open subsets of V and whose morphisms are the inclusions. A *homomorphism of presheaves* $\alpha : \mathcal{O} \to \mathcal{O}'$ is a family of homomorphisms of k-algebras

$$\alpha(U) : \mathcal{O}(U) \to \mathcal{O}'(U)$$

commuting with the restriction maps, i.e., a natural transformation.

A presheaf $\mathcal{O}$ is a *sheaf* if for every open covering $\{U_i\}$ of an open subset U of V and family of elements $f_i \in \mathcal{O}(U_i)$ agreeing on overlaps (that is, such that $f_i|U_i \cap U_j = f_j|U_i \cap U_j$ for all i, j), there is a unique element $f \in \mathcal{O}(U)$ such that $f_i = f|U_i$ for all i.[21] A *homomorphism of sheaves* on V is a homomorphism of presheaves.

[21] This condition implies that $\mathcal{O}(\emptyset) = 0$.

For $v \in V$, the *stalk* of a sheaf $\mathcal{O}$ (or presheaf) at v is

$$\mathcal{O}_v = \varinjlim \mathcal{O}(U) \quad \text{(limit over open neighbourhoods of } v).$$

In other words, it is the set of equivalence classes of pairs (U, f) with U an open neighbourhood of v and $f \in \mathcal{O}(U)$; two pairs (U, f) and (U', f') are equivalent if $f|U'' = f|U''$ for some open neighbourhood U'' of v contained in $U \cap U'$.

A *ringed space* is a pair $(V, \mathcal{O})$ consisting of topological space V together with a sheaf of rings. If the stalk $\mathcal{O}_v$ of $\mathcal{O}$ at v is a local ring for all $v \in V$, then $(V, \mathcal{O})$ is called a *locally ringed space*.

A *morphism* $(V, \mathcal{O}) \to (V', \mathcal{O}')$ *of ringed spaces* is a pair (φ, ψ) with φ a continuous map $V \to V'$ and ψ a family of maps

$$\psi(U') : \mathcal{O}'(U') \to \mathcal{O}(\varphi^{-1}(U')), \quad U' \text{ open in } V',$$

commuting with the restriction maps. Such a pair defines homomorphism of rings $\psi_v : \mathcal{O}'_{\varphi(v)} \to \mathcal{O}_v$ for all $v \in V$. A *morphism of locally ringed spaces* is a morphism of ringed space such that ψ_v is a local homomorphism for all v.

Let $\mathcal{B}$ be a base for the topology on V that is closed under finite intersections. A sheaf on $\mathcal{B}$ can be defined in the obvious way, and such a sheaf $\mathcal{O}$ extends to a sheaf $\mathcal{O}'$ on V: for any open subset U of V, define $\mathcal{O}'(U)$ to be the set of families

$$(f_{U'})_{U' \subset U, U' \in \mathcal{B}}, \quad f_{U'} \in \mathcal{O}(U'),$$

agreeing on overlaps. Then $\mathcal{O}'$ is a sheaf of k-algebras on V, and there is a canonical isomorphism $\mathcal{O} \to \mathcal{O}'|\mathcal{B}$.

AFFINE ALGEBRAIC SPACES AND VARIETIES

Let A be a finitely generated k-algebra, and let $V = \mathrm{spm}(A)$. Recall (§12) that the set of principal open subsets of V

$$\mathcal{B} = \{D(f) \mid f \in A\}$$

is a base for the topology on V. Moreover, $\mathcal{B}$ is closed under finite intersections because

$$D(f_1 \cdots f_r) = D(f_1) \cap \ldots \cap D(f_r).$$

For a principal open subset D of V, define $\mathcal{O}_A(D) = S_D^{-1} A$ where S_D is the multiplicative subset $A \smallsetminus \bigcup_{\mathfrak{p} \in D} \mathfrak{p}$. If $D = D(f)$, then S_D is the smallest saturated multiplicative subset containing f, and so $\mathcal{O}_A(D) \simeq A_f$ (see 6.12). If $D \supset D'$, then $S_D \subset S_{D'}$, and so there is a canonical "restriction" homomorphism $\mathcal{O}_A(D) \to \mathcal{O}_A(D')$. These restriction maps make $D \rightsquigarrow \mathcal{O}_A(D)$ into a functor on $\mathcal{B}$ satisfying the sheaf condition: for any covering $D = \bigcup_{i \in I} D_i$ of a $D \in \mathcal{B}$ by $D_i \in \mathcal{B}$ and family of elements $f_i \in \mathcal{O}_A(D_i)$ agreeing on overlaps, there is a unique element $f \in \mathcal{O}_A(D)$ such that $f_i = f|D_i$ for all i.

For an open subset U of V, define $\mathcal{O}_A(U)$ to be the set of families $(f_D)_D$ agreeing on overlaps; here D runs over the principal open sets $D \subset U$. Clearly $U \rightsquigarrow \mathcal{O}_A(U)$ is a functor on the open subsets of V, and it is not difficult to check that it is a sheaf. Moreover, in the definition of $\mathcal{O}_A(U)$, instead of taking *all* principal open subsets of U, it suffices to take a covering collection. In particular, if $U = D(f)$, then

$$\mathcal{O}_A(U) \simeq \mathcal{O}_A(D(f)) \simeq A_f.$$

In summary:

PROPOSITION 18.5. *There exists an essentially unique sheaf $\mathcal{O}_A$ of k-algebras on $V = \mathrm{spm}(A)$ such that*

(a) *for all basic open subsets $D = D(f)$ of V,*

$$\mathcal{O}(D) = S_D^{-1}A \simeq A_f,$$

(b) *for all inclusions $D' \subset D$ of basic open subsets, the restriction map $\mathcal{O}(D) \to \mathcal{O}(D')$ is the canonical map $S_D^{-1}A \to S_{D'}^{-1}A$.*

We write $\mathrm{Spm}(A)$ for $\mathrm{spm}(A)$ endowed with this sheaf of k-algebras.

PROPOSITION 18.6. *For every $\mathfrak{m} \in \mathrm{spm}(A)$, the stalk $\mathcal{O}_\mathfrak{m}$ is canonically isomorphic to $\mathcal{O}_\mathfrak{m}$.*

PROOF. Apply (7.3). □

Thus $\mathrm{Spm}(A)$ is a locally ringed space. An *affine algebraic space* is topological space V together with a sheaf of k-algebras $\mathcal{O}$ such that $(V, \mathcal{O})$ is isomorphic to $\mathrm{Spm}(A)$ for some finitely generated k-algebra A. A *regular map* of affine algebraic spaces is morphism of locally ringed spaces.

EXAMPLE 18.7. Affine n-space $\mathbb{A}^n = \mathrm{Spm}(k[X_1, \ldots, X_n])$. To give a regular map $V \to \mathbb{A}^1$ is the same as giving a homomorphism of k-algebras $k[X] \to \mathcal{O}(V)$, i.e., an element of $\mathcal{O}(V)$. For this reason, $\mathcal{O}(V)$ is often called the *ring* (or *k-algebra*) *of regular functions* on V.

PROPOSITION 18.8. *For any affine algebraic space $(V, \mathcal{O}_V)$ and locally ringed space $(W, \mathcal{O}_W)$, the canonical map*

$$\mathrm{Hom}(V, W) \to \mathrm{Hom}_{k\text{-alg}}(\mathcal{O}_W(W), \mathcal{O}_V(V))$$

is an isomorphism.

PROOF. Exercise for the reader. □

An affine algebraic space V defines a functor

$$R \rightsquigarrow V(R) \stackrel{\text{def}}{=} \mathrm{Hom}_{k\text{-alg}}(\mathcal{O}(V), R). \tag{1}$$

from k-algebras to sets. For example, $\mathbb{A}^n(R) \simeq R^n$ for all k-algebras R.

An *affine algebraic variety* is an affine algebraic space V such that $\mathcal{O}_V(V)$ is an affine algebra.

TANGENT SPACES; NONSINGULAR POINTS; REGULAR POINTS

Let $k[\varepsilon]$ be the ring of dual numbers (so $\varepsilon^2 = 0$). For an affine algebraic space V over k, the map $\varepsilon \mapsto 0 \colon k[\varepsilon] \to k$ defines a map

$$V(k[\varepsilon]) \to V(k).$$

For any $a \in V(k)$, we define the *tangent space* to V at a, $\mathrm{Tgt}_a(V)$, to be the inverse image of a under this map.

PROPOSITION 18.9. *There is a canonical isomorphism*

$$\mathrm{Tgt}_a(V) \simeq \mathrm{Hom}_{k\text{-}lin}(\mathfrak{m}_a/\mathfrak{m}_a^2, k).$$

This follows from the next two lemmas.

Let $V = V(\mathfrak{a}) \subset k^n$, and assume that the origin o lies on V. Let $\mathfrak{a}_\ell$ be the ideal generated by the linear terms f_ℓ of the $f \in \mathfrak{a}$. By definition, $T_o(V) = V(\mathfrak{a}_\ell)$. Let $A_\ell = k[X_1,\ldots,X_n]/\mathfrak{a}_\ell$, and let $\mathfrak{m}$ be the maximal ideal in $k[V]$ consisting of the functions zero at o; thus $\mathfrak{m} = (x_1,\ldots,x_n)$.

LEMMA 18.10. *There is a canonical isomorphism*

$$\mathrm{Hom}_{k\text{-}lin}(\mathfrak{m}/\mathfrak{m}^2, k) \xrightarrow{\simeq} \mathrm{Hom}_{k\text{-}alg}(A_\ell, k).$$

PROOF. Let $\mathfrak{n} = (X_1,\ldots,X_n)$ be the maximal ideal at the origin in $k[X_1,\ldots,X_n]$. Then $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathfrak{n}/(\mathfrak{n}^2 + \mathfrak{a})$, and as $f - f_\ell \in \mathfrak{n}^2$ for every $f \in \mathfrak{a}$, it follows that $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathfrak{n}/(\mathfrak{n}^2 + \mathfrak{a}_\ell)$. Let $f_{1,\ell},\ldots,f_{r,\ell}$ be a basis for the vector space $\mathfrak{a}_\ell$. From linear algebra we know that there are $n-r$ linear forms $X_{i_1},\ldots,X_{i_{n-r}}$ forming with the $f_{i,\ell}$ a basis for the linear forms on k^n. Then $X_{i_1} + \mathfrak{m}^2,\ldots,X_{i_{n-r}} + \mathfrak{m}^2$ form a basis for $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space, and the lemma shows that $A_\ell \simeq k[X_{i_1}\ldots,X_{i_{n-r}}]$. A homomorphism $\alpha\colon A_\ell \to k$ of k-algebras is determined by its values $\alpha(X_{i_1}),\ldots,\alpha(X_{i_{n-r}})$, and they can be arbitrarily given. Since the k-linear maps $\mathfrak{m}/\mathfrak{m}^2 \to k$ have a similar description, the first isomorphism is now obvious. □

LEMMA 18.11. *There is a canonical isomorphism*

$$\mathrm{Hom}_{k\text{-}alg}(A_\ell, k) \xrightarrow{\simeq} T_o(V).$$

PROOF. To give a k-algebra homomorphism $A_\ell \to k$ is the same as to give an element $(a_1,\ldots,a_n) \in k^n$ such that $f(a_1,\ldots,a_n) = 0$ for all $f \in A_\ell$, which is the same as to give an element of $T_P(V)$. □

REMARK 18.12. Let $V = \mathrm{Spm}\, k[X_1,\ldots,X_n]/(f_1,\ldots,f_m)$, and let $(a_1,\ldots,a_n) \in V(k)$. Then $\mathrm{Tgt}_a(V)$ is canonically isomorphic to the subspace of k^n defined by the equations

$$\left.\frac{\partial f_i}{\partial X_1}\right|_a X_1 + \cdots + \left.\frac{\partial f_i}{\partial X_n}\right|_a X_n, \quad i = 1,\ldots,m.$$

When a is the origin, this is a restatement of (18.11), and the general case can be deduced from this case by a translation.

The *dimension* of an affine algebraic space V is the Krull dimension of $\mathcal{O}(V)$. If V is irreducible, then $\mathcal{O}(V)/\mathfrak{N}$ is an integral domain, and the dimension of V is equal to the transcendence degree over k of the field of fractions of $\mathcal{O}(V)/\mathfrak{N}$; moreover, all maximal ideals have height $\dim V$ (13.11).

PROPOSITION 18.13. *Let V be an affine algebraic space over k, and let $a \in V(k)$. Then* $\dim \mathrm{Tgt}_a(V) \geq \dim V$, *and equality holds if and only if $\mathcal{O}(V)_{\mathfrak{m}_a}$ is regular.*

PROOF. Let $\mathfrak{n}$ be the maximal ideal of the local ring $A = \mathcal{O}(V)_{\mathfrak{m}_a}$. Then $A/\mathfrak{n} = k$, and $\dim_k \mathfrak{n}/\mathfrak{n}^2 \geq \mathrm{ht}(\mathfrak{n})$, with equality if and only if A is regular. As $\mathfrak{m}_a/\mathfrak{m}_a^2 \simeq \mathfrak{n}/\mathfrak{n}^2$ (6.7), Proposition 18.9 implies that $\dim \mathrm{Tgt}_a(V) = \dim_k \mathfrak{n}/\mathfrak{n}^2$, from which the statement follows. □

An $a \in V(k)$ is *nonsingular* if $\dim \mathrm{Tgt}_a(V) = \dim V$; otherwise it is *singular*. An affine algebraic space V is *regular* if all of its local rings $\mathcal{O}(V)_{\mathfrak{m}}$ are regular, and it is *smooth* if $V_{k^{\mathrm{al}}}$ is regular. Thus an algebraic space over an algebraically closed field is smooth if and only if all $a \in V(k)$ are nonsingular. A smooth algebraic space is regular, but the converse is false. For example, let k' be a finite inseparable extension of k, and let V be a smooth algebraic space over k'; when we regard V is an algebraic space over k, it is regular, but not smooth.

PROPOSITION 18.14. *A smooth affine algebraic space V is a regular affine algebraic variety; in particular, $\mathcal{O}(V)$ is an integral domain. Conversely, if k is perfect, then every regular affine algebraic space over k is smooth.*

PROOF. Let $A = \mathcal{O}(V)$. If V is smooth, then all the local the local rings of $k^{\mathrm{al}} \otimes_k A$ are regular; in particular, they are integral domains (17.3). This implies that $k^{\mathrm{al}} \otimes_k A$ is reduced, because it implies that the annihilator of any nilpotent element is not contained in any maximal ideal, and so is the whole ring. Therefore A is an affine algebra, and so V is an affine algebraic variety. Let $\mathfrak{m}$ be a maximal ideal in A, and let $\mathfrak{n} = \mathfrak{m}(k^{\mathrm{al}} \otimes_k A)$. Then $\mathfrak{n}$ is a maximal ideal of $k^{\mathrm{al}} \otimes_k A$, and

$$\mathfrak{n}/\mathfrak{n}^2 \simeq k^{\mathrm{al}} \otimes (\mathfrak{m}/\mathfrak{m}^2),$$

and so $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim_{k^{\mathrm{al}}}(\mathfrak{n}/\mathfrak{n}^2)$. This implies that $A_{\mathfrak{m}}$ is regular. In particular, $A_{\mathfrak{m}}$ is an integral domain for all maximal ideals of A, which implies that A is integral domain, because it implies that the annihilator of any zero-divisor is not contained in any maximal ideal. Conversely, if V is regular, A is an integral domain, and hence an affine k-algebra if k is perfect. □

PROPOSITION 18.15. *Let V be an irreducible affine algebraic space over an algebraically closed field k, and identify V with $V(k)$. The set of nonsingular points of V is open, and it is nonempty if V is an algebraic variety.*

PROOF. We may suppose $V = \mathrm{Spm}\, k[X_1,\ldots,X_n]/(f_1,\ldots,f_m)$. Let $d = \dim V$. According to Remark 18.12, the set of singular points of V is the zero-set of the ideal generated by the $(n-d)\times(n-d)$ minors of the matrix

$$\mathrm{Jac}(f_1,\ldots,f_m)(a) = \begin{pmatrix} \frac{\partial f_1}{\partial X_1}(a) & \cdots & \frac{\partial f_1}{\partial X_n}(a) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial X_1}(a) & \cdots & \frac{\partial f_m}{\partial X_n}(a) \end{pmatrix},$$

which is closed. Therefore the set of nonsingular points is open.

Now suppose that V is an algebraic variety. The next two lemmas allow us to suppose that $V = k[X_1,\ldots,X_n]/(f)$ where f is a nonconstant irreducible polynomial. Then $\dim V = n-1$, and so we have to show that the equations

$$f = 0, \quad \frac{\partial f}{\partial X_1} = 0, \quad \cdots \quad , \frac{\partial f}{\partial X_n} = 0$$

have no common zero. If $\frac{\partial f}{\partial X_1}$ is identically zero on $V(f)$, then f divides it. But $\frac{\partial f}{\partial X_1}$ has degree less than that of f and f is irreducible, and so this implies that $\frac{\partial f}{\partial X_1} = 0$. Therefore f is a polynomial in $X_2,\ldots,X_n$ (characteristic zero) or $X_1^p, X_2,\ldots,X_n$ (characteristic p). Continuing in this fashion, we find that either f is constant (characteristic zero) or a pth power (characteristic p), which contradict the hypothesis. □

Let V be an irreducible affine algebraic variety. Then $\mathcal{O}(V)$ is an integral domain, and we let $k(V)$ denote its field of fractions. Two irreducible affine algebraic varieties V and W are said to be *birationally equivalent* if $k(V) \approx k(W)$.

LEMMA 18.16. *Two irreducible varieties V and W are birationally equivalent if and only if there are open subsets U and U' of V and W respectively such that $U \approx U'$.*

PROOF. Assume that V and W are birationally equivalent. We may suppose that $A = \mathcal{O}(V)$ and $B = \mathcal{O}(W)$ have a common field of fractions K. Write $B = k[x_1, \ldots, x_n]$. Then $x_i = a_i/b_i$, $a_i, b_i \in A$, and $B \subset A_{b_1 \ldots b_r}$. Since $\mathrm{Spm}(A_{b_1 \ldots b_r})$ is a basic open subvariety of V, we may replace A with $A_{b_1 \ldots b_r}$, and suppose that $B \subset A$. The same argument shows that there exists a $d \in B \subset A$ such $A \subset B_d$. Now

$$B \subset A \subset B_d \Longrightarrow B_d \subset A_d \subset (B_d)_d = B_d,$$

and so $A_d = B_d$. This shows that the open subvarieties $D(b) \subset V$ and $D(b) \subset W$ are isomorphic. This proves the "only if" part, and the "if" part is obvious. □

LEMMA 18.17. *Every irreducible algebraic variety of dimension d is birationally equivalent to a hypersurface in $\mathbb{A}^{d+1}$.*

PROOF. Let V be an irreducible variety of dimension d. According to 8.21 of my notes Fields and Galois Theory, there exist algebraically independent elements $x_1, \ldots, x_d \in k(V)$ such that $k(V)$ is finite and separable over $k(x_1, \ldots, x_d)$. By the primitive element theorem (ibid. 5.1), $k(V) = k(x_1, \ldots, x_d, x_{d+1})$ for some x_{d+1}. Let $f \in k[X_1, \ldots, X_{d+1}]$ be an irreducible polynomial satisfied by the x_i, and let H be the hypersurface $f = 0$. Then $k(V) \approx k(H)$. □

ALGEBRAIC SCHEMES, SPACES, AND VARIETIES

An algebraic space over k is a locally ringed space that admits a finite open covering by affine algebraic spaces. An algebraic variety over k is a locally ringed space $(X, \mathcal{O}_X)$ that admits a finite open covering by affine algebraic spaces and satisfies the following separation condition: for every pair $\varphi_1, \varphi_2 \colon Z \to X$ of locally ringed space with Z and affine algebraic variety, the subset of Z on which φ_1 and φ_2 agree is closed.

Let $(X, \mathcal{O}_X)$ be an algebraic scheme over k, i.e., a scheme of finite type over k, and let X' be the subset of X obtained by omitting all the nonclosed points. Then $(X', \mathcal{O}_X|X')$ is an algebraic space over k. Conversely, let $(X, \mathcal{O}_X)$ be an algebraic space over k; for each open subset U of X, let U' be the set of irreducible closed subsets of U, and regard U' as a subset of X' in the obvious way; then $(X', \mathcal{O}_{X'})$ where $\mathcal{O}_{X'}(U') = \mathcal{O}_X(U)$ is an algebraic scheme over k.

References

BOURBAKI, N. AC. Algèbre Commutative. Elements of Mathematics. Masson, Hermann. Chap. I–IV Masson 1985; Chap. V–VII Hermann 1975; Chap. VIII-IX Masson 1983; Chap. X Masson 1998.

CARTIER, P. 2007. A primer of Hopf algebras, pp. 537–615. *In* Frontiers in number theory, physics, and geometry. II. Springer, Berlin. Preprint available at IHES.

KRULL, W. 1938. Dimensionstheorie in stellenringen. *J. Reine Angew. Math.* 179:204–226.

MATSUMURA, H. 1986. Commutative ring theory, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge.

NAGATA, M. 1962. Local rings. Interscience Tracts in Pure and Applied Mathematics, No. 13. Interscience Publishers, New York-London.

NORTHCOTT, D. G. 1953. Ideal theory. Cambridge Tracts in Mathematics and Mathematical Physics, No. 42. Cambridge, at the University Press.

Index