A Primer of Commutative Algebra

James S. Milne

May 2, 2013, v3.00

Abstract

These notes collect the basic results in commutative algebra used in the rest of my notes and books.

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 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).

Prerequisites

A knowledge of the algebra usually taught in advanced undergraduate or first-year graduate courses.

References

A reference to monnnn is to question nnnn on mathoverflow.net.

Acknowledgements

I thank the following for providing corrections and comments for earlier versions of these notes: Florian Herzig, Chun Yin Hui, Keenan Kidwell, Leon Lampret, Andrew McLennan, Shu Otsuka, Bhupendra Nath Tiwari.

[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.

[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.

1 Rings and algebras

A ring is an ***integral domain*** if it is not the zero ring and if $ab = 0$ in the ring implies that $a = 0$ or $b = 0$.

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 $i_B: A \to B$. A ***homomorphism*** of A-algebras $B \to C$ is a homomorphism of rings $\varphi: B \to C$ such that $\varphi(i_B(a)) = i_C(a)$ for all $a \in A$.

Elements $x_1, \dots, x_n$ 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 $A[X_1, \dots, X_n] \to B$ acting as i_B on A and sending X_i to x_i is surjective.

When $A \subset B$ and $x_1, \dots, x_n \in B$, we let $A[x_1, \dots, x_n]$ denote the A-subalgebra of B generated by the x_i.

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, i.e, if B is a quotient of a polynomial ring $A[X_1, \dots, X_n]$. An A-algebra B is ***finitely presented*** if it is the quotient of a polynomial ring $k[X_1, \dots, X_n]$ by a *finitely generated* ideal.

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 integral domain and an algebra over a field k. If A is finite over k (more generally, if every element of A is algebraic over k), then A is a field. To see this, let a be a nonzero element of A. Because A is an integral domain, the k-linear map $x \mapsto ax: A \to A$ is injective, and hence is surjective if A is finite, which shows that a has an inverse. More generally, if a is algebraic over k, then $k[a]$ is 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 $e_1, \dots, e_n$ are ***orthogonal*** if $e_i e_j = 0$ for $i \neq j$. Every sum of orthogonal idempotents is again idempotent. A set $\{e_1, \dots, e_n\}$ of orthogonal idempotents is ***complete*** if $e_1 + \cdots + e_n = 1$. Every set of orthogonal idempotents $\{e_1, \dots, e_n\}$ 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

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

[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".

form a complete set of orthogonal idempotents in A. Conversely, if $\{e_1,\dots,e_n\}$ 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;
- $a \in \mathfrak{a}, r \in A \implies ra \in \mathfrak{a}$.

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 $\sum r_i s_i$ with $r_i \in A$, $s_i \in S$. The ideal generated by the empty set is the zero ideal $\{0\}$. When $S = \{a,b,\dots\}$, we write $(a,b,\dots)$ 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 if 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 $\sum a_i b_i$ with $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$, and if $\mathfrak{a} = (a_1,\dots,a_m)$ and $\mathfrak{b} = (b_1,\dots,b_n)$, then $\mathfrak{ab} = (a_1b_1,\dots,a_ib_j,\dots,a_mb_n)$. 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 every 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

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

For an 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

$$ab = 0 \implies a = 0 \text{ or } b = 0,$$

i.e., $A/\mathfrak{p}$ is an integral domain. In particular, the zero ideal is prime if and only if the ring 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.). When $\mathfrak{p}$ is prime, we write $\kappa(\mathfrak{p})$ for the field of fractions of $A/\mathfrak{p}$.

[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.

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 $\{1, f, \dots, f^r, \dots\}$ generated by an element f of A;
the complement of a prime ideal (or of a union of prime ideals);
$1 + \mathfrak{a} \stackrel{\text{def}}{=} \{1 + a \mid a \in \mathfrak{a}\}$ 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 every 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.

Now 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 S contains an element in $\mathfrak{c} + (b)$, say,

$$f = c + ab, \quad c \in \mathfrak{c}, \quad a \in A.$$

Similarly, if b' is not in $\mathfrak{c}$, then S contains an element

$$f' = c' + a'b, \quad c' \in \mathfrak{c}, \quad a' \in A.$$

Now

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

which contradicts

$$ff' \in S.$$

Therefore, at least one of b or b' is in $\mathfrak{c}$, which is therefore prime. □

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

PROOF. Apply the proposition with $S = \{1\}$. □

The ***radical*** $\operatorname{rad}(\mathfrak{a})$ 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) between ideals of A and ideals of $A/\mathfrak{a}$, 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 2.3. *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 $f \in \mathrm{rad}(\mathfrak{a})$, then clearly $af \in \mathrm{rad}(\mathfrak{a})$ for all $a \in A$. Suppose that $a, b \in \mathrm{rad}(\mathfrak{a})$, 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. In fact, it 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 4.10 below), but $\mathfrak{a} + \mathfrak{b} = (X^2, Y)$, which contains X^2 but not X.

PROPOSITION 2.4. *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 $\mathfrak{a}$.

For the reverse inclusion, let $f \notin \mathrm{rad}(\mathfrak{a})$. 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 2.5. 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 2.6. *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 2.7 (PRIME AVOIDANCE). *Let $\mathfrak{p}_1,\dots,\mathfrak{p}_r$, $r\geq 1$, be ideals in A with $\mathfrak{p}_2,\dots,\mathfrak{p}_r$ prime. If an ideal $\mathfrak{a}$ is not contained in any of the $\mathfrak{p}_i$, then it is not contained in their union.*

PROOF. When $r=1$, there is nothing to prove, and so we may assume that $r>1$ and (inductively) that the statement is true for $r-1$. Then $\mathfrak{a}$ is not contained in the union of the ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_{i-1},\mathfrak{p}_{i+1},\dots,\mathfrak{p}_r$, and so there exists an $a_i\in\mathfrak{a}\smallsetminus\bigcup_{j\neq i}\mathfrak{p}_j$. If some a_i does not lie in $\mathfrak{p}_i$, then that $a_i\in\mathfrak{a}\smallsetminus\bigcup_{1\leq i\leq r}\mathfrak{p}_i$, and the proof is complete. Thus suppose that every $a_i\in\mathfrak{p}_i$, and consider

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

I claim that a belongs to no $\mathfrak{p}_i$. Because $\mathfrak{p}_r$ is prime and none of the elements $a_1,\dots,a_{r-1}$ lies in $\mathfrak{p}_r$, their product does not lie in $\mathfrak{p}_r$; as $a_r\in\mathfrak{p}_r$, we see that $a\notin\mathfrak{p}_r$. 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 $a\notin\mathfrak{p}_i$. This completes the proof. □

ASIDE 2.8. In general, the condition in (2.7) that the ideals $\mathfrak{p}_2,\dots,\mathfrak{p}_r$ be prime is necessary: the ideal (x,y) in $\mathbb{F}_2[x,y]$ is the union of three smaller nonprime ideals. However, when A contains an infinite field, the condition can be dropped (see mo108594, Mohan).

Extension and contraction of ideals

Let $\varphi\colon A\to B$ 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):

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

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:

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

Note that, for every 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 $d_1,\dots,d_n$ be integers, relatively prime in pairs; then for any integers $x_1,\dots,x_n$, 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 $\mathfrak{a}_1,\dots,\mathfrak{a}_n$ be ideals in a ring A. If $\mathfrak{a}_i$ is relatively prime to $\mathfrak{a}_j$ whenever $i \neq j$, then the map*

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

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

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 $a_1x_2 + a_2x_1$ 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 $(x_1 \bmod \mathfrak{a}_1, \dots, x_n \bmod \mathfrak{a}_n)$, which shows that (3) is surjective.

The kernel of the map is $\bigcap \mathfrak{a}_i$, and so 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

$$c = a_1c + a_2c \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$$

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

$$\mathfrak{a}_1 \cdot \left(\prod\nolimits_{i\geq 2} \mathfrak{a}_i\right) = \mathfrak{a}_1 \cap \left(\prod\nolimits_{i\geq 2} \mathfrak{a}_i\right)$$

by the $n = 2$ case. Now $\mathfrak{a}_1 \cdot \left(\prod_{i\geq 2} \mathfrak{a}_i\right) = \prod_{i\geq 1} \mathfrak{a}_i$ and $\mathfrak{a}_1 \cap \left(\prod_{i\geq 2} \mathfrak{a}_i\right) = \mathfrak{a}_1 \cap \left(\bigcap_{i\geq 2} \mathfrak{a}_i\right) = \bigcap_{i\geq 1} \mathfrak{a}_i$, 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 $\{a_1, \dots, a_n\}$ 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. If Σ has no maximal element, then the axiom of dependent choice[5] shows that there exists a strictly ascending sequence of ideals in Σ, which contradicts (b).

(c) $\Rightarrow$ (a): Let $\mathfrak{a}$ be an ideal, and let Σ be the set of finitely generated ideals contained in $\mathfrak{a}$. Then Σ is nonempty because it contains the zero ideal, and so it contains a maximal element $\mathfrak{c} = (a_1, \dots, a_r)$. If $\mathfrak{c} \neq \mathfrak{a}$, then there exists an element $a \in \mathfrak{a} \smallsetminus \mathfrak{c}$, and $(a_1, \dots, a_r, a)$ 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 (3.6) that this is, in fact, true for every 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 every 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*

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

be an exact sequence of A-modules.

[5] This says: Let R be a binary relation on a nonempty set X, and suppose that, for each a in X, there exists a b such that aRb; then there exists a sequence $(a_n)_{n\in\mathbb{N}}$ of elements of X such that a_nRa_{n+1} for all n. It is strictly stronger than the axiom of countable choice but weaker than the axiom of choice. See the Wikipedia (axiom of dependent choice).

(a) *If $N \subset P$ are submodules of M such that $\alpha(M') \cap N = \alpha(M') \cap P$ and $\beta(N) = \beta(P)$, then $N = P$.*
(b) *If M' and M'' are finitely generated, so also is M.*
(c) *M is noetherian if and only if M' and M'' are both noetherian.*

PROOF. (a) Let $x \in P$. The second condition implies that there exists a $y \in N$ such that $\beta(y) = \beta(x)$. Now $\beta(x-y) = 0$, and so $x - y \in \alpha M' \cap P = \alpha M' \cap N$. Thus $x = (x-y) + y \in N$.

(b) Let S' be a finite set of generators for M, and let S'' be a finite subset of M such that $\beta S''$ generates M''. The submodule N of M generated by $\alpha S' \cup S''$ is such that $\alpha M' \cap N = \alpha M'$ and $\beta N = M''$. Therefore (a) shows that $N = M$.

(c) $\Rightarrow$: An ascending chain of submodules of M' or of M'' gives rise to an ascending chain in M, and therefore becomes constant.

$\Leftarrow$: Consider an ascending chain of submodules of M. As M'' is Noetherian, the image of the chain in M'' becomes constant, and as M' is Noetherian, the intersection of the chain with $\alpha M'$ becomes constant. Now the (a) shows that the chain itself becomes constant. □

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.

PROPOSITION 3.4. *Every finitely generated module over a noetherian ring is noetherian.*

PROOF. Let M be a module over a noetherian ring A. 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. Clearly M contains a submodule N generated by $n-1$ elements such that the quotient M/N is generated by a single element, and so 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*** of an element x of M is

$$\operatorname{ann}(x) \stackrel{\text{def}}{=} \{a \in A \mid ax = 0\}.$$

It is an ideal in A, which is proper if $x \neq 0$. I claim that every ideal $\mathfrak{a}$ that is maximal among the annihilators of nonzero elements of A is prime. Let $\mathfrak{a} = \operatorname{ann}(x)$, 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 every $x \in M$, the submodule Ax of M is isomorphic to $A/\operatorname{ann}(x)$. If M is nonzero, then there exists a nonzero x such that $\operatorname{ann}(x)$ is maximal, and so M contains a submodule $M_1 = Ax$ isomorphic to $A/\mathfrak{p}_1$ with $\mathfrak{p}_1$ prime. 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). □

ASIDE 3.6. The proofs of (2.1) and (3.5) are two 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 and Reyes, J. Algebra 319 (2008), no. 7, 3006–3027.

THEOREM 3.7 (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 $A[X_1,\dots,X_n]$. Note that

$$A[X_1,\dots,X_n] = A[X_1,\dots,X_{n-1}][X_n]. \tag{4}$$

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

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

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 $\mathfrak{a}(i)$ 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 $\mathfrak{a}(i)$ is obviously an ideal in A, and $\mathfrak{a}(i-1) \subset \mathfrak{a}(i)$ because, if $cX^{i-1} + \cdots \in \mathfrak{a}$, then so also does $X(cX^{i-1} + \cdots)$.

Let $\mathfrak{b}$ be an ideal of $A[X]$ contained in $\mathfrak{a}$. Then $\mathfrak{b}(i) \subset \mathfrak{a}(i)$, and if equality holds for all i, then $\mathfrak{b} = \mathfrak{a}$. Indeed, let f be a polynomial of degree i in $\mathfrak{a}$. Because $\mathfrak{b}(i) = \mathfrak{a}(i)$, there exists a $g \in \mathfrak{b}$ such that $\deg(f-g) < \deg f$. On repeating this argument with $f-g$, we eventually find that $f \in \mathfrak{b}$.

As A is noetherian, the sequence of ideals

$$\mathfrak{a}(1) \subset \mathfrak{a}(2) \subset \cdots \subset \mathfrak{a}(i) \subset \cdots$$

eventually becomes constant, say, $\mathfrak{a}(d) = \mathfrak{a}(d+1) = \dots$ (and then $\mathfrak{a}(d)$ contains the leading coefficients of *all* polynomials in $\mathfrak{a}$). For each $i \leq d$, choose a finite generating set $\{c_{i1}, c_{i2}, \dots\}$ for $\mathfrak{a}(i)$, and for each (i,j), choose a polynomial $f_{ij} \in \mathfrak{a}$ of degree i with leading coefficient c_{ij}. The ideal $\mathfrak{b}$ generated by the f_{ij} is contained in $\mathfrak{a}$ and has the property that $\mathfrak{b}(i) = \mathfrak{a}(i)$ for all i. Therefore $\mathfrak{b} = \mathfrak{a}$, and $\mathfrak{a}$ is finitely generated. □

COROLLARY 3.8. *When R is noetherian, every finitely generated R-algebra is finitely presented.*

PROOF. Obvious. □

NAKAYAMA'S LEMMA 3.9. *Let A be a ring, let $\mathfrak{a}$ be an ideal in A, and let M be an A-module. Assume that $\mathfrak{a}$ is contained in all maximal ideals of A and that M is finitely generated.*

(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 that $M \neq 0$. Choose a minimal set of generators $\{e_1, \dots, e_n\}$ 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 $e_2, \dots, e_n$ 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 (2.5) 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 3.10. *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 $a_1, \dots, a_n$ of M generate it as an A-module if and only if the elements*

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

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

PROOF. If $a_1, \dots, a_n$ generate M, then it is obvious that their images generate the vector space $M/\mathfrak{m}M$. Conversely, suppose that $a_1 + \mathfrak{m}M, \dots, a_n + \mathfrak{m}M$ span $M/\mathfrak{m}M$, and let N be the submodule of M generated by $a_1, \dots, a_n$. 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 3.11. *Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Elements $a_1, \dots, a_n$ of $\mathfrak{m}$ generate $\mathfrak{m}$ as an ideal if and only if $a_1 + \mathfrak{m}^2, \dots, a_n + \mathfrak{m}^2$ span $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over $A/\mathfrak{m}$. 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 3.12. 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 consider the $\mathbb{Z}_{(p)}$-module $\mathbb{Q}$. Then $\mathbb{Z}_{(p)}$ is a local ring with maximal ideal (p) (see §5 below) and $\mathbb{Q} = p\mathbb{Q}$ but $\mathbb{Q} \neq 0$.

DEFINITION 3.13. Let A be a noetherian ring.

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

$$\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0. \tag{5}$$

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

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 (5) is d). For example, the integral domains of dimension 0 are the fields. The height of a 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 §19 that the height of every prime ideal in a noetherian ring is finite. However, the Krull dimension of the ring may be infinite, because it may contain a sequence of prime ideals whose heights tend to infinity (Krull 1938).[6]

LEMMA 3.14. *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 $\mathfrak{a}$, and let $\mathfrak{a}'$ be maximal among the ideals generated by finite subsets of S. Then $\mathfrak{a}'$ contains every element of S (otherwise it wouldn't be maximal), and so equals $\mathfrak{a}$. □

THEOREM 3.15 (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 *every* ideal $\mathfrak{a}$ in a noetherian ring,

$$\bigcap\nolimits_{n\geq 1}\mathfrak{a}^n = \mathfrak{a}\cdot\bigcap\nolimits_{n\geq 1}\mathfrak{a}^n. \tag{6}$$

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

Let $a_1,\dots,a_r$ 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 $g(a_1,\dots,a_r)$ for some homogeneous polynomial $g(X_1,\dots,X_r)\in A[X_1,\dots,X_r]$ of degree n.

Let S_m denote the set of homogeneous polynomials f of degree m such that $f(a_1,\dots,a_r)\in\bigcap_{n\geq 1}\mathfrak{a}^n$, and let $\mathfrak{c}$ be the ideal in $A[X_1,\dots,X_r]$ generated by $\bigcup_m S_m$. Because $A[X_1,\dots,X_r]$ is noetherian, $\mathfrak{c}$ is finitely generated, and so $\mathfrak{c}$ is generated by a finite set $\{f_1,\dots,f_s\}$ of elements of $\bigcup_m S_m$. 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 $b=f(a_1,\dots,a_r)$ for some homogeneous polynomial f of degree $d+1$. By definition, $f\in S_{d+1}\subset\mathfrak{c}$, and so

$$f = g_1f_1+\cdots+g_sf_s$$

for some $g_i\in A[X_1,\dots,X_n]$. 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 $g_i(a_1,\dots,a_r)\in\mathfrak{a}$. Now

$$b=f(a_1,\dots,a_r)=\sum\nolimits_i g_i(a_1,\dots,a_r)\cdot f_i(a_1,\dots,a_r)\in\mathfrak{a}\cdot\bigcap\nolimits_n\mathfrak{a}^n,$$

which completes the proof of (6). □

[6] In Nagata 1962, p.203, there is the following example. Let $\mathbb{N}=I_0\sqcup I_1\sqcup\dots$ be a partition of $\mathbb{N}$ into finite sets with strictly increasing cardinality. Let $A=k[X_0,X_1,\dots]$ be the polynomial ring in a countably infinite number of symbols, and let $\mathfrak{p}_i$ be the prime ideal in A generated by the X_j's with j in I_i. Let S be the multiplicative set $A\smallsetminus\bigcup\mathfrak{p}_i$. Then $S^{-1}A$ is noetherian and regular, and the prime ideal $S^{-1}\mathfrak{p}_i$ has height $|I_i|$.

The equality (6) can also be proved using primary decompositions — see (17.15).

PROPOSITION 3.16. *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 $a_1,\dots,a_n$ generate $\operatorname{rad}(\mathfrak{a})$. For each i, some power of a_i, say $a_i^{r_i}$, lies in $\mathfrak{a}$. Then every term of the expansion of

$$(c_1a_1+\cdots+c_na_n)^{r_1+\cdots+r_n},\quad c_i\in A,$$

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

ASIDE 3.17. In a noetherian ring, every ideal is finitely generated, but there is little that one can say in general about the number of generators required. For example, in $k[X]$ every ideal is generated by a single element, but in $k[X,Y]$ the ideal $(X,Y)^n$ requires at least $n+1$ generators.

ASIDE 3.18. The following example shows that the Krull intersection theorem fails for nonnoetherian rings. Let A be the ring of germs of C^∞ functions at 0 on the real line. Then A is a local ring with maximal ideal $\mathfrak{m}$ equal to the set of germs zero at 0, and $\bigcap_{n\ge1}\mathfrak{m}^n$ consists of the germs whose derivatives at zero are all zero. It therefore contains e^{-1/x^2}. [Every germ of a function at 0 is represented by a function f on an open neighbourhood U of 0; two pairs (f,U) and (f',U') represent the same germ if and only if f and f' agree on some neighbourhood of 0 in $U\cap U'$.]

4 Unique factorization

Let A be an integral domain. An element a of A is said to be ***irreducible*** if it is neither zero nor a unit and 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 it is neither zero nor a unit and (a) is a prime ideal, i.e.,

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

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. In more detail, the uniqueness means that if

$$a=\prod\nolimits_{i\in I}a_i=\prod\nolimits_{j\in J}b_j$$

with each a_i and 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. We have shown that a is irreducible.

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

PROPOSITION 4.2. *Let A be an integral domain in which every nonzero nonunit element is a finite product of irreducible elements. If every irreducible element of A is prime, then A is a unique factorization domain.*

PROOF. Suppose that

$$a_1 \cdots a_m = b_1 \cdots b_n \tag{7}$$

with the a_i and b_i irreducible elements in A. As a_1 is prime, it divides one of the b_i, which we may suppose to be b_1, say $b_1 = a_1 u$. As b_1 is irreducible, u is a unit. On cancelling a_1 from both sides of (7), we obtain the equality

$$a_2 \cdots a_m = (ub_2)b_3 \cdots b_n.$$

Continuing in this fashion, we find that the two factorizations are the same up to units and the order of the factors. □

PROPOSITION 4.3. *Let A be an integral domain in which every ascending chain of principal ideals becomes constant (e.g., a noetherian integral domain). Then every every nonzero nonunit element in A is a finite product of irreducible elements.*

PROOF. The hypothesis implies that every nonempty set of principal ideals has a maximal element (cf. the proof of 3.1). Assume that A has nonfactorable elements, and let (a) be maximal among the ideals generated by such elements. Then a is not itself irreducible, and so $a = bc$ with neither b nor c units. Now (b) and (c) both properly contain (a), and so b and c are both factorable, which contradicts the nonfactorability of a. □

PROPOSITION 4.4. *Let A be a unique factorization domain with field of fractions F. If an element f of $A[X]$ factors into the product of two nonconstant polynomials in $F[X]$, then it factors into the product of two nonconstant polynomials in $A[X]$.*

In other words, if f is not the product of two nonconstant polynomials in $A[X]$, then it is irreducible in $F[X]$.

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

$$(cd/p)f = g_2h_1 \text{ in } A[X].$$

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

$$f = a_0 + a_1X + \cdots + a_mX^m$$

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

PROPOSITION 4.5. *The product of two primitive polynomials is primitive.*

PROOF. Let

$$f = a_0 + a_1X + \cdots + a_mX^m$$
$$g = b_0 + b_1X + \cdots + b_nX^n,$$

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 $\sum_{i+j=i_0+j_0} a_ib_j$ 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. □

Each of the last two propositions is referred to as ***Gauss's lemma*** (Gauss proved them with $A = \mathbb{Z}$).

PROPOSITION 4.6. *Let A be a unique factorization domain with field of fractions F. For polynomials $f, g \in F[X]$, $c(fg) = c(f) \cdot c(g)$; 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

$$fg = c(f)c(g)f_1g_1$$

with f_1g_1 primitive, and so $c(fg) = c(f)c(g)$. □

COROLLARY 4.7. *The irreducible elements in $A[X]$ are the irreducible elements a of A and the nonconstant primitive polynomials f such that f is irreducible in $F[X]$.*

PROOF. Obvious from (4.4) and (4.6). □

THEOREM 4.8. *If A is a unique factorization domain, then so also is $A[X]$.*

PROOF. Let $f \in A[X]$, and write $f = c(f)f_1$. Then $c(f)$ is a product of irreducible elements in A. If f_1 is not irreducible, then it can be written as a product of two polynomials of lower degree, which are necessarily primitive (4.6). Continuing in this fashion, we find that f_1 is a product of irreducible primitive polynomials, and hence that f is a product of irreducible elements in $A[X]$.

According to Proposition 4.2, in order prove that $A[X]$ is a unique factorization domain, it remains to show that each irreducible element of $A[X]$ is prime.

Let a be an irreducible element of A. If a divides the product gh of $g,h \in A[X]$, then it divides $c(gh) = c(g)c(h)$. As a is prime, it divides $c(g)$ or $c(h)$, and hence also g or h.

Let f be a nonconstant primitive polynomial in $A[X]$ such that f is irreducible in $F[X]$. If f divides the product gh of $g,h \in A[X]$, then it divides g or h in $F[X]$. Suppose the first, and write $fq = g$ with $q \in F[X]$. Then $c(q) = c(f)c(q) = c(fq) = c(g) \in A$, and so $q \in A[X]$. Therefore f divides g in $A[X]$. □

Let k be a field. A ***monomial*** in $X_1,\dots,X_n$ 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 $f(X_1,\dots,X_n)$ is the largest total degree of a monomial occurring in f with nonzero coefficient. Since

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

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

THEOREM 4.9. *The ring $k[X_1,\dots,X_n]$ is a unique factorization domain.*

PROOF. This is trivially true when $n = 0$, and an induction argument using (4), p.11, proves it for all n. □

COROLLARY 4.10. *A nonzero proper principal ideal (f) in $k[X_1,\dots,X_n]$ is prime if and only f is irreducible.*

PROOF. Special case of (4.1). □

5 Rings of fractions

Recall that a multiplicative subset of a ring is a nonempty subset closed under the formation of finite products. In particular, it contains 1 (the empty product).

Let S be a multiplicative subset of a ring A. 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 $a \mapsto \frac{a}{1}: A \xrightarrow{i_S} S^{-1}A$ whose kernel is

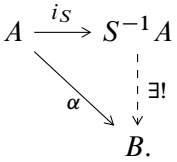
$$\{a \in A \mid sa = 0 \text{ for some } s \in S\}.$$

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

A homomorphism $A \to B$ factors through $A \xrightarrow{i_S} S^{-1}A$ if and only if the image of S in B consists of units. More formally:

PROPOSITION 5.1. *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 $\alpha: A \to B$ with this property factors uniquely through i_S



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

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

and so

$$\beta(\tfrac{a}{s}) = \alpha(a)\alpha(s)^{-1}. \tag{8}$$

This shows that there can be at most one β such that $\beta \circ i_S = \alpha$. We define β by the formula (8). 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.[7]

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 $t \in T$.

[7] 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 $\alpha: A_1 \to A_2$ such that $\alpha \circ i_1 = i_2$ (universal property of A_1, i_1); similarly, there exists a unique homomorphism $\alpha': A_2 \to A_1$ 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 $\alpha' \circ i_2 = i_1$).

EXAMPLE 5.2. Let $h \in A$. Then $S_h = \{1, h, h^2, \dots\}$ 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 that can be written in the form a/h^m, $a \in A$, $m \in \mathbb{N}$.

PROPOSITION 5.3. *For every 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

$$A[x] \stackrel{\text{def}}{=} A[X]/(1-hX),$$

$1 = hx$, 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

$$\textstyle\sum_i a_i X^i \mapsto \sum_i \alpha(a_i)\alpha(h)^{-i}\colon A[X] \to B$$

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 every 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 proposition shows, some is retained.

PROPOSITION 5.4. *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 $i_S\colon A \to S^{-1}A$. 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 map $\mathfrak{p} \mapsto \mathfrak{p}^e$ 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 $\overline{S}$ be the image of S in $A/\mathfrak{p}$. Then $(S^{-1}A)/\mathfrak{p}^e \simeq \overline{S}^{-1}(A/\mathfrak{p})$ because $S^{-1}A/\mathfrak{p}^e$ has the correct universal property, and $\overline{S}^{-1}(A/\mathfrak{p})$ is an integral domain because $A/\mathfrak{p}$ is an integral domain and $\overline{S}$ doesn't contain 0. Therefore $\mathfrak{p}^e$ is prime. From (2.11) 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 5.5. *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 $(\mathfrak{b}^c)^e = \mathfrak{b}$. □

PROPOSITION 5.6. *Let $\varphi: A \to B$ be a ring homomorphism. A prime ideal $\mathfrak{p}$ of A is the contraction of a prime ideal in B if and only if $\mathfrak{p} = \mathfrak{p}^{ec}$.*

PROOF. If $\mathfrak{p} = \mathfrak{q}^c$, then $\mathfrak{p}^{ec} = \mathfrak{q}^{cec} \overset{2.11}{=} \mathfrak{q}^c = \mathfrak{p}$. Conversely, suppose that $\mathfrak{p} = \mathfrak{p}^{ec}$, and let $S = A \smallsetminus \mathfrak{p}$. Let $s \in S$; if $\varphi(s) \in \mathfrak{p}^e$, then $s \in \mathfrak{p}^{ec} = \mathfrak{p}$, contradicting the definition of S. Therefore $\varphi(S)$ is a multiplicative subset of B disjoint from $\mathfrak{p}^e$, and so there exists a prime ideal $\mathfrak{q}$ in B containing $\mathfrak{p}^e$ and disjoint from $\varphi(S)$ (apply 2.1). Now $\varphi^{-1}(\mathfrak{q})$ contains $\mathfrak{p}$ and is disjoint from S, and so it equals $\mathfrak{p}$. □

EXAMPLE 5.7. 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

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

According to (5.4), 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 5.8. *Let $\mathfrak{m}$ be a maximal ideal of a ring A, and let $\mathfrak{n} = \mathfrak{m}A_{\mathfrak{m}}$ be the maximal ideal of $A_{\mathfrak{m}}$. For all n, the map*

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

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 $r \leq n$.

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 $(\mathfrak{m}^n)^{ec} \subset \mathfrak{m}^n$, 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 $\frac{a}{s} \in A_{\mathfrak{m}}$, $a \in A$, $s \in A \smallsetminus \mathfrak{m}$. The only maximal ideal of A containing $\mathfrak{m}^n$ is $\mathfrak{m}$, and so no maximal ideal contains both s and $\mathfrak{m}^n$. Therefore $(s) + \mathfrak{m}^n = A$, and so $sb + q = 1$ for some $b \in A$ and $q \in \mathfrak{m}^n$. Hence

$$s(ba) = a(1-q). \tag{9}$$

Because s is invertible in $A_{\mathfrak{m}}/\mathfrak{n}^n$, $\frac{a}{s}$ is the *unique* element of this ring such that $s\frac{a}{s} = a$. But (9) shows that the image of ba in $A_{\mathfrak{m}}$ also has this property and therefore equals $\frac{a}{s}$. □

PROPOSITION 5.9. *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 its annihilator $\{b \mid ba = 0\}$ is a proper ideal in A, 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 3.15), which implies that $a \notin \mathfrak{m}^n$ (by 5.8). □

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

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

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

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

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

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

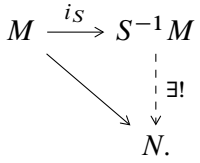
and a homomorphism $m \mapsto \frac{m}{1} : M \xrightarrow{i_S} S^{-1}M$ of A-modules whose kernel is

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

A homomorphism $M \to N$ of A-modules factors through $M \to S^{-1}M$ if and only if every element of S acts invertibly on N. More formally:

PROPOSITION 5.10. *The pair $(S^{-1}M, i_S)$ has the following universal property:*

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



PROOF. Similar to that of Proposition 5.1. □

In particular, for any homomorphism $\alpha: M \to N$ of A-modules, there is a unique homomorphism $S^{-1}\alpha: S^{-1}M \to S^{-1}N$ 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 from A-modules to $S^{-1}A$-modules.

PROPOSITION 5.11. *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

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

PROPOSITION 5.12. *Let M be an A-module. The canonical map*

$$M \to \prod\{M_{\mathfrak{m}} \mid \mathfrak{m} \text{ a maximal ideal in } A\}$$

is injective.

PROOF. Let $m \in M$ map to zero in all $M_{\mathfrak{m}}$. The annilator $\mathfrak{a} = \{a \in A \mid am = 0\}$ of m is an ideal in A. Because m maps to zero $M_{\mathfrak{m}}$, there exists an $s \in A \smallsetminus \mathfrak{m}$ such that $sm = 0$. Therefore $\mathfrak{a}$ is not contained in $\mathfrak{m}$. Since this is true for all maximal ideals $\mathfrak{m}$, $\mathfrak{a} = A$ (by 2.2), and so it contains 1. Now $m = 1m = 0$. □

COROLLARY 5.13. *The A-module $M = 0$ if $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$.*

PROOF. Immediate consequence of the lemma. □

PROPOSITION 5.14. *A sequence*

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \tag{10}$$

is exact if and only if

$$M'_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} M_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} M''_{\mathfrak{m}} \tag{11}$$

is exact for all maximal ideals $\mathfrak{m}$.

PROOF. The necessity is a special case of (5.11). For the sufficiency, let $N = \operatorname{Ker}(\beta)/\operatorname{Im}(\alpha)$. Because the functor $M \rightsquigarrow M_{\mathfrak{m}}$ is exact,

$$N_{\mathfrak{m}} = \operatorname{Ker}(\beta_{\mathfrak{m}})/\operatorname{Im}(\alpha_{\mathfrak{m}}).$$

If (11) is exact for all $\mathfrak{m}$, then $N_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$, and so $N = 0$ (by 5.13). But this means that (10) is exact. □

COROLLARY 5.15. *A homomorphism $M \to N$ of A-modules is injective (resp. surjective) if and only if $M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective) for all maximal ideals $\mathfrak{m}$.*

PROOF. Apply the proposition to $0 \to M \to N$ (resp. $M \to N \to 0$). □

EXAMPLE 5.16. Let M be an A-module. For $h \in A$, let $M_h = S_h^{-1}M$ where $S_h = \{1, h, h^2, \dots\}$. 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 $N \in \mathbb{N}$.

EXERCISE 5.17. A multiplicative subset S of a ring A is said to be *saturated* if

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

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

6 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[8] polynomial with coefficients in A, i.e., if it satisfies an equation

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

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 rule. As usually stated in linear algebra courses, this says that, if $x_1, \dots, x_m$ is a solution to the system of linear equations

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

then

$$x_j = \frac{\det(C_j)}{\det(C)}, \tag{12}$$

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

where $C = (c_{ij})$ 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 rewrites (12) in the form

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

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

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

using standard properties of determinants.

PROPOSITION 6.1. *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*[9] *$A[\alpha]$-submodule M of B that is finitely generated as an A-module.*

PROOF. $\Rightarrow$: Suppose that

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

Then the A-submodule M of B generated by $1, \alpha, ..., \alpha^{n-1}$ 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 $\{e_1, \dots, e_n\}$ 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

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

PROPOSITION 6.2. *An A-algebra B is finite if it is generated as an A-algebra by a finite number of elements, each of which is integral over A.*

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

PROOF. Suppose that $B = A[\alpha_1, \dots, \alpha_m]$ and that

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

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 $\alpha_1^{r_1} \cdots \alpha_m^{r_m}$, $1 \le r_i < n_i$. □

COROLLARY 6.3. *An A-algebra B is finite if and only if it is finitely generated and integral over A.*

PROOF. $\Leftarrow$: Immediate consequence of the proposition.

$\Rightarrow$: As an A-module, B is faithful (because $a \cdot 1_B = a$), and so (6.1) shows 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 6.4. *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 (6.1) shows that $\alpha \pm \beta$ and $\alpha\beta$ are integral over A. □

DEFINITION 6.5. 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 6.6. *Let A be an integral domain with field of fractions F, and let E be a field containing F. If $\alpha \in E$ 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 $a_1 d, \dots, a_m d^m \in A$, this shows that $d\alpha$ is integral over A. □

COROLLARY 6.7. *Let A be an integral domain and let E be an algebraic extension of the field of fractions of A. Then E is the field of fractions of the integral closure of A in E.*

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

DEFINITION 6.8. An integral domain A is is said to be ***integrally closed*** or ***normal*** 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 6.9. *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. □

Let $F \subset E$ be fields, and let $\alpha \in E$ be algebraic over F. The ***minimum polynomial*** of α over F is the unique element of smallest degree in the set of monic polynomials in $F[X]$ having α as a root. If f is the minimum polynomial of α, then the homomorphism $X \mapsto \alpha: F[X] \to F[\alpha]$ defines an isomorphism $F[X]/(f) \to F[\alpha]$, i.e., $F[x] \simeq F[\alpha]$, $x \leftrightarrow \alpha$.

PROPOSITION 6.10. *Let A be a normal integral domain, and let E be a finite extension of the field of fractions F of A. An element of E is integral over A if and only if its minimum polynomial 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 (see above)

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

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. As the coefficients of f are polynomials in the conjugates of α, it follows from (6.4) 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 6.11. *Let A be a normal 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 of α, which, being also a root of f, is integral over A. Therefore g has coefficients in A. □

PROPOSITION 6.12. *Let $A \subset B$ be rings, and let A' be the integral closure of A in B. For any multiplicative subset S of A, $S^{-1}A'$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

PROOF. Let $b/s \in S^{-1}A'$ with $b \in A'$ and $s \in S$. Then

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

for some $a_i \in A$, and so

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0.$$

Therefore b/s is integral over $S^{-1}A$. This shows that $S^{-1}A'$ is contained in the integral closure of $S^{-1}B$.

For the converse, let b/s be integral over $S^{-1}A$ with $b \in B$ and $s \in S$. Then

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s_1}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s_n} = 0.$$

for some $a_i \in A$ and $s_i \in S$. On multiplying this equation by $s^n s_1 \cdots s_n$, we find that $s_1 \cdots s_n b \in A'$, and therefore that $b/s = s_1 \cdots s_n b / s s_1 \cdots s_n \in S^{-1}A'$. □

COROLLARY 6.13. *Let $A \subset B$ be rings, and let S be a multiplicative subset of A. If A is integrally closed in B, then $S^{-1}A$ is integrally closed in $S^{-1}B$.*

PROOF. Special case of the proposition in which $A' = A$. □

PROPOSITION 6.14. *The following conditions on an integral domain A are equivalent:*

(a) *A is an integral domain;*
(b) *$A_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p}$;*
(c) *$A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m}$.*

PROOF. The implication (a)⇒(b) follows from (6.13), and (b)⇒(c) is obvious. For (c)⇒(a), let A' be the integral closure of A in its field of fractions F. Then $(A')_{\mathfrak{m}}$ is the integral closure of $A_{\mathfrak{m}}$ in F (by 6.12). If (c) holds, then $A_m \to (A')_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$, which implies that $A \to A'$ is surjective (by 5.15), and so A is integrally closed. □

PROPOSITION 6.15. *If A is a normal integral domain, so also is the polynomial ring $A[X]$.*

PROOF. Omitted for the present. □

The going-up theorem

PROPOSITION 6.16. *Let $A \subset B$ be integral domains, with B integral over A. Then B is a field if and only if A is a field.*

PROOF. Suppose that A is a field, and let b be a nonzero element of B. Then

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

for some $a_i \in A$, and we may suppose that n is the minimum degree of such a relation. Then, as B is an integral domain, $a_n \neq 0$, and the equation

$$b \cdot (b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) a_n^{-1} = -1$$

shows that b has an inverse in B.

Conversely, suppose that B is a field, and let a be a nonzero element of A. Then a has an inverse a^{-1} in B, and

$$a^{-n} + a_1 a^{-(n-1)} + \cdots + a_n = 0$$

for some $a_i \in A$. On multiplying through by a^{n-1}, we find that

$$a^{-1} + a_1 + a_2 a \cdots + a_n a^{n-1} = 0,$$

and so

$$a^{-1} = -(a_1 + a_2 a \cdots + a_n a^{n-1}) \in A.$$

□

COROLLARY 6.17. *Let $A \subset B$ be rings with B integral over A. Let $\mathfrak{q}$ be a prime ideal of B, and let $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

PROOF. Apply the proposition to $A/\mathfrak{p} \subset B/\mathfrak{q}$. □

COROLLARY 6.18 (INCOMPARABILITY). *Let $A \subset B$ be rings with B integral over A, and let $\mathfrak{q} \subset \mathfrak{q}'$ be prime ideals of B. If $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$, then $\mathfrak{q} = \mathfrak{q}'$.*

PROOF. Let $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Then $A_\mathfrak{p} \subset B_\mathfrak{p}$, and $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. The ideals $\mathfrak{q}B_\mathfrak{p} \subset \mathfrak{q}'B_\mathfrak{p}$ are both prime ideals of $B_\mathfrak{p}$ lying over $\mathfrak{p}A_\mathfrak{p}$, which is maximal, and so $\mathfrak{q}B_\mathfrak{p} = \mathfrak{q}'B_\mathfrak{p}$ (by 6.17). Now

$$\mathfrak{q} \overset{5.4}{=} (\mathfrak{q}B_\mathfrak{p})^c = \left(\mathfrak{q}'B_\mathfrak{p}\right)^c \overset{5.4}{=} \mathfrak{q}'.$$

□

THEOREM 6.19. *Let $A \subset B$ be rings with B integral over A, and let $\mathfrak{p}$ be a prime ideal of A. Then there exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{p} = \mathfrak{q} \cap A$.*

PROOF. We have $A_\mathfrak{p} \subset B_\mathfrak{p}$, and $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. Let $\mathfrak{n}$ be a maximal ideal in $B_\mathfrak{p}$ (which exists by 2.2). Then $\mathfrak{n} \cap A_\mathfrak{p}$ is maximal (6.17). But $\mathfrak{p}A_\mathfrak{p}$ is the unique maximal ideal of $A_\mathfrak{p}$, and so $\mathfrak{n} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. Let $\mathfrak{q}$ be the inverse image of $\mathfrak{n}$ in B. Then $\mathfrak{q} \cap A$ is the inverse image of $\mathfrak{p}A_\mathfrak{p}$ in A, because the diagram

$$\begin{array}{ccc} B & \longrightarrow & B_\mathfrak{p} \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_\mathfrak{p} \end{array}$$

commutes. But the inverse image of $\mathfrak{p}A_\mathfrak{p}$ in A is $\mathfrak{p}$ (as $\mathfrak{p}^{ec} = \mathfrak{p}$; see 5.4). Therefore $\mathfrak{q} \cap A = \mathfrak{p}$. □

COROLLARY 6.20. *Let $A \subset B$ be rings with B integral over A. Let $\mathfrak{p} \subset \mathfrak{p}'$ be prime ideals of A, and let $\mathfrak{q}$ be a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then there exists a prime ideal $\mathfrak{q}'$ of B containing $\mathfrak{q}$ and such that $\mathfrak{q}' \cap A = \mathfrak{p}'$.*

PROOF. We have $A/\mathfrak{p} \subset B/\mathfrak{q}$, and $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. According to the theorem, there exists a prime ideal $\mathfrak{q}''$ in $B/\mathfrak{q}$ such that $\mathfrak{q}'' \cap (A/\mathfrak{p}) = \mathfrak{p}'/\mathfrak{p}$. The inverse image $\mathfrak{q}'$ of $\mathfrak{q}''$ in B has the required properties. □

COROLLARY 6.21. *Let $A \subset B$ be rings with B integral over A, and let $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be prime ideals in A. Let*

$$\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m \quad (m < n) \tag{13}$$

be prime ideals in B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \leq m$. Then (13) can be extended to a chain of prime ideals

$$\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$$

such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all $i \leq n$.

PROOF. Immediate consequence of Corollary 6.20. □

Theorem 6.19 and its corollaries are referred to as the ***going-up theorem*** (of Cohen and Seidenberg).

The going-down theorem

Before proving the going-down theorem, we need to extend some of the definitions and results from earlier in this section.

Let $A \subset B$ be rings, and let $\mathfrak{a}$ be an ideal of A. An element b of B is said to be ***integral*** over $\mathfrak{a}$ if it satisfies an equation

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \tag{14}$$

with the $a_i \in \mathfrak{a}$. The set of elements of B integral over $\mathfrak{a}$ is called the ***integral closure*** of $\mathfrak{a}$ in B. The proof of Proposition 6.1 shows that $b \in B$ is integral over $\mathfrak{a}$ if there exists a faithful $A[b]$-submodule M of B such that $bM \subset \mathfrak{a}M$ and M is finitely generated as an A-module.

Note that if b^m is integral over $\mathfrak{a}$, so also is b (the equation (14) for b^m can be read as a similar equation for b).

LEMMA 6.22. *Let A' be the integral closure of A in B. Then the integral closure of $\mathfrak{a}$ in B is the radical of $\mathfrak{a}A'$.*

PROOF. Let $b \in B$ be integral over $\mathfrak{a}$. From (14) we see that $b \in A'$ and that $b^n \in \mathfrak{a}A'$, and so b is in the radical of $\mathfrak{a}A'$.

Conversely, let b be in the radical of $\mathfrak{a}A'$, so that

$$b^m = \sum\nolimits_i a_i x_i, \quad \text{some } m > 0, \quad a_i \in \mathfrak{a}, \quad x_i \in A'.$$

As each x_i is integral over A, $M \overset{\text{def}}{=} A[x_1, \ldots, x_n]$ is a finite A-algebra (see 6.2). As $b^n M \subset M$, we see that b^n is integral over $\mathfrak{a}$, which implies that b is integral over $\mathfrak{a}$. □

In particular, the integral closure of $\mathfrak{a}$ in B is an ideal in A', and so it is closed under the formation of sums and (nonempty) products.

PROPOSITION 6.23. *Let A be a normal integral domain, and let E extension of the field of fractions F of A. If an element of E is integral over an ideal $\mathfrak{a}$ in A, then its minimum polynomial over F has coefficients in the radical of $\mathfrak{a}$.*

PROOF. Let α be integral over $\mathfrak{a}$, so that

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

for some $n > 0$ and $a_i \in \mathfrak{a}$. As in the proof of (6.10), the conjugates of α satisfy the same equation as α, and so are also integral over $\mathfrak{a}$. The coefficients of the minimum polynomial of α over F are polynomials without constant term in its conjugates, and so they are also integral over $\mathfrak{a}$. As these coefficients lie in F, they lie in the integral closure of $\mathfrak{a}$ in F, which is the radical of $\mathfrak{a}$ (by 6.22). □

THEOREM 6.24. *Let $A \subset B$ be integral domains with A normal and B integral over A. Let $\mathfrak{p}' \subset \mathfrak{p}$ be prime ideals in A, and let $\mathfrak{q}$ be a prime ideal in B such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then there exists a prime ideal $\mathfrak{q}' \subset \mathfrak{q}$ in B such that $\mathfrak{q}' \cap A = \mathfrak{p}'$.*

PROOF. The prime ideals of B contained in $\mathfrak{q}$ are the contractions of prime ideals in $B_{\mathfrak{q}}$ (see 5.4), and so we have show to that $\mathfrak{p}'$ is the contraction of a prime ideal of $B_{\mathfrak{q}}$, or, equivalently (see 5.6), that

$$A \cap (\mathfrak{p}'B_{\mathfrak{q}}) = \mathfrak{p}'.$$

Let $b \in \mathfrak{p}'B_{\mathfrak{q}}$. Then $b = y/s$ with $y \in \mathfrak{p}'B$ and $s \in B \smallsetminus \mathfrak{q}$. By (6.22), y is integral over $\mathfrak{p}'$, and so (by 6.23) the minimum equation

$$y^m + a_1 y^{m-1} + \cdots + a_m = 0 \tag{15}$$

of y over the field of fractions F of A has coefficients $a_i \in \mathfrak{p}'$.

Suppose that $b \in A \cap \mathfrak{p}'B_{\mathfrak{q}}$. Then $b^{-1} \in F$, and so, on replacing y with bs in (15) and dividing through by b^m, we obtain the minimum equation for s over F:

$$s^m + (a_1/b)s^{m-1} + \cdots + (a_m/b^m) = 0. \tag{16}$$

But b is integral over A, and so (by 6.10), each coefficient $a_i/b^i \in A$. Suppose that $b \notin \mathfrak{p}'$. The coefficients $a_i/b^i \in \mathfrak{p}'$, and so (16) shows that $s^m \in \mathfrak{p}'B \subset \mathfrak{p}B \subset \mathfrak{q}$, and so $s \in \mathfrak{q}$, which contradicts its definition. Hence $b \in \mathfrak{p}'$, and so $A \cap \mathfrak{p}'B_{\mathfrak{q}} = \mathfrak{p}'$ as required. □

COROLLARY 6.25. *Let $A \subset B$ be integral domains with A normal and B integral over A. Let $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$ be prime ideals in B, and let*

$$\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m \quad (m < n) \tag{17}$$

be prime ideals in B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all i. Then (17) can be extended to a chain of prime ideals

$$\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_n$$

such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all i.

PROOF. Immediate consequence of the theorem. □

Theorem 6.24 and its corollary are referred to as the ***going-down theorem*** (of Cohen and Seidenberg).

The Noether normalization theorem

THEOREM 6.26 (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 $y_1,\dots,y_r$ of A such that A is a finitely generated $k[y_1,\dots,y_r]$-module and $y_1,\dots,y_r$ are algebraically independent[10] 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 $n\ge 1$ and that the statement is true for k-algebras generated by $n-1$ (or fewer) elements.

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

$$f = c_0T_1^N + c_1T_1^{N-1} + \cdots + c_N,\quad c_i\in k[T_2,\dots,T_n],\quad c_0\ne 0.$$

If $c_0\in k$, then the equation

$$0 = f(x_1,\dots,x_n) = c_0x_1^N + c_1(x_2,\dots,x_n)x_1^{N-1} + \cdots + c_N(x_2,\dots,x_n)$$

shows that x_1 is integral over $k[x_2,\dots,x_n]$. By induction, there exist algebraically independent elements $y_1,\dots,y_r$ such that $k[x_2,\dots,x_n]$ is finite over $k[y_1,\dots,y_r]$. It follows that A is finite over $k[y_1,\dots,y_r]$ (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

$$x_1' = x_1, x_2' = x_2 - x_1^{m^2},\dots,x_n' = x_n - x_1^{m^n}.$$

Then

$$k[x_1',\dots,x_n'] = k[x_1,\dots,x_n] = A$$

because each $x_i'\in k[x_1,\dots,x_n]$ and, conversely, each

$$x_i\in k[x_1,x_2',\dots,x_n'] = k[x_1',\dots,x_n'].$$

When we let

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

then

$$g(x_1',\dots,x_n') = f(x_1',x_2'+x_1'^{m^2},\dots,x_n'+x_1'^{m^n}) = 0.$$

I claim that, if m is chosen sufficiently large, then

$$g(T_1,\dots,T_n) = c_0'T_1^N + c_1'T_1^{N-1} + \cdots + c_N',$$

with $c_i'\in k[T_2,\dots,T_n]$ and $c_0'\in k^\times$, and so the previous argument applies.

[10] Recall that this means that the homomorphism of k-algebras $k[X_1,\dots,X_r]\to k[y_1,\dots,y_r]$ sending X_i to y_i is an isomorphism, or, equivalently, that

$$P(y_1,\dots,y_r)=0,\quad P\in k[X_1,\dots,X_r]\implies P=0.$$

To prove the claim, let

$$f(T_1,\dots,T_n) = \sum c_{j_1\cdots j_n} T_1^{j_1}\cdots T_n^{j_n}.$$

Choose m so large that the numbers

$$j_1 + m^2 j_2 + \cdots + m^n j_n, \tag{18}$$

are distinct when $(j_1,\dots,j_n)$ runs over the n-tuples with $c_{j_1,\dots,j_n} \neq 0$. Then

$$f(T_1, T_2 + T_1^{m^2},\dots,T_n + T_1^{m^n}) = cT_1^N + c_1 T_1^{N-1} + \cdots$$

with $c \in k \smallsetminus \{0\}$ and N equal to the largest value of (18). □

REMARK 6.27. When k is infinite, there is a simpler proof of a somewhat stronger result: let $A = k[x_1,\dots,x_n]$; then there exist algebraically independent elements $f_1,\dots,f_r$ that are *linear combinations* of the x_i such that A is finite over $k[f_1,\dots,f_r]$ (see 8.13 of my algebraic geometry notes).

EXERCISE 6.28. A ring A is said to be ***normal*** if $A_{\mathfrak{p}}$ is a normal integral domain for all prime ideals $\mathfrak{p}$ in A. Show that a noetherian ring is normal if and only if it is a finite product of normal integral domains.

7 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 7.1. *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 7.2. *In an artinian ring, the nilradical and the Jacobson radical coincide.*

PROOF. The first is the intersection of the prime ideals (2.4), and the second is the intersection of the maximal ideals (2.5). □

PROPOSITION 7.3. *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 7.4. *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 that $\mathfrak{N}^n \neq 0$. 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 7.5. *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 that $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$ 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 7.6. *A ring is artinian if and only if it is noetherian of dimension zero.*

PROOF. $\Rightarrow$: Let A be an artinian ring. After (7.1), it remains to show that A is noetherian, but according to (7.2), (7.3), and (7.4), 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 (17.11), 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 (2.4), and since some power of $\mathfrak{N}$ is zero (3.16), we again have that some finite product of maximal ideals is zero, and so can apply the lemma. □

THEOREM 7.7. *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 (7.6) 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 7.8. *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 7.4); 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 7.9. 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).

ASIDE 7.10. Every finitely generated module over a principal Artin ring is a direct sum of cyclic modules (see mo22722).

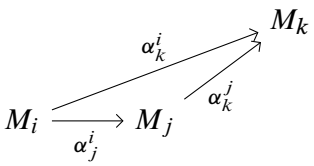
8 Direct and inverse limits

Direct limits

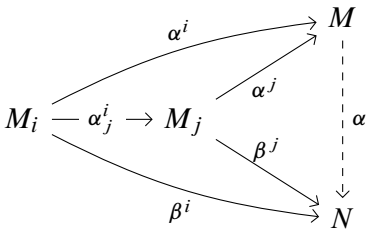
DEFINITION 8.1. A partial ordering $\leq$ on a set I is said to be ***directed***, and the pair $(I, \leq)$ is called a ***directed set***, if for all $i, j \in I$ there exists a $k \in I$ such that $i, j \leq k$.

DEFINITION 8.2. 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 $(\alpha_j^i : M_i \to M_j)_{i \leq j}$ of A-linear maps such that $\alpha_i^i = \mathrm{id}_{M_i}$ and $\alpha_k^j \circ \alpha_j^i = \alpha_k^i$ all $i \leq j \leq k$.



An A-module M together with a family $(\alpha^i : M_i \to M)_{i \in I}$ of A-linear maps satisfying $\alpha^i = \alpha^j \circ \alpha_j^i$ all $i \leq j$ is said to be a ***direct limit*** of the system $((M_i), (\alpha_j^i))$ 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 $\beta^i = \beta^j \circ \alpha_j^i$ all $i \leq j$, 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 $\varinjlim(M_i, \alpha_i^j)$, or just $\varinjlim M_i$.

CRITERION

An A-module M together with A-linear maps $\alpha^i : M_i \to M$ such that $\alpha^i = \alpha^j \circ \alpha_j^i$ for all $i \leq j$ is the direct limit of a system (M_i, α_i^j) 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 $j \geq i$.

CONSTRUCTION

Let

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

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

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

Let $\alpha^i(m_i) = m_i + M'$. Then certainly $\alpha^i = \alpha^j \circ \alpha_j^i$ for all $i \leq j$. For every 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 8.3. *For every 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 5.1), and these homomorphisms are compatible with the maps in the direct system. Now apply the criterion p. 34 to see that $S^{-1}A$ is the direct limit of the A_h. □

EXACTNESS

PROPOSITION 8.4. *The direct limit of a system of exact sequences of modules is exact.*

This means the following: suppose that (M_i, α_j^i), (N_i, β_j^i), and (P_i, γ_j^i) are direct systems with repect to the directed set I, and let

$$0 \to (M_i, \alpha_j^i) \xrightarrow{(a_i)} (N_i, \beta_j^i) \xrightarrow{(b_i)} (P_i, \gamma_j^i) \to 0$$

be a sequence of maps of direct systems; if the sequences

$$0 \to M_i \xrightarrow{a_i} N_i \xrightarrow{b_i} P_i \to 0$$

are exact for all i, then the direct limit sequence

$$0 \to \varinjlim M_i \xrightarrow{\varinjlim a_i} \varinjlim N_i \xrightarrow{\varinjlim b_i} \varinjlim P_i \to 0$$

is exact.

PROOF. Let $(n_i) \in \varinjlim N_i$. If $(b_i(n_i)) = 0$, then there exists an i_0 such that $b_i(n_i) = 0$ for all $i \geq i_0$. Let $m_i = 0$ unless $i \geq i_0$, in which case we let m_i be the unique element such that $a_i(m_i) = n_i$. Then (m_i) maps to (n_i). This proves exactness at $\varinjlim N_i$, and the proof of exactness at the other terms is obvious. □

Inverse limits

Inverse limits are the same as direct limits except that the directions of the arrows is reversed. Thus, formally, the theory of inverse limits is the same as that of inverse limits. However, in concrete categories, they behave very differently. For example, the inverse limit of a system of exact sequences of modules need not be exact.

We shall consider inverse limits only in the case that the indexing set if $\mathbb{N}$ with its usual ordering. Thus, an inverse system of A-modules is nothing more than a sequence of modules and A-homomorphisms

$$M_0 \xleftarrow{\alpha_0} M_1 \xleftarrow{\alpha_1} \cdots \xleftarrow{\alpha_{n-1}} M_n \xleftarrow{\alpha_n} \cdots .$$

A homomorphism $(M_n,\alpha_n) \to (N_n,\beta_n)$ of inverse systems is a sequence of A-homomorphisms $\gamma_n\colon M_n \to N_n$ such that $\beta_n \circ \gamma_{n+1} = \gamma_n \circ \alpha_n$ for all $n \in \mathbb{N}$.

Given an inverse system (M_n,α_n) of A-modules, we define $\varprojlim M_n$ and $\varprojlim^1 M_n$ to be the kernel and cokernel of the map

$$(m_n)_{n\in\mathbb{N}} \mapsto (m_n - \alpha_n(m_{n+1}))\colon \prod M_n \to \prod M_n.$$

PROPOSITION 8.5. *For any inverse system (M_n,α_n) and A-module N,*

$$\operatorname{Hom}(\varprojlim M_n, N) \simeq \varprojlim \operatorname{Hom}(M_n, N).$$

PROOF. Obvious. □

PROPOSITION 8.6. *For any inverse system of exact sequence*

$$0 \to (M_n,\alpha_n) \to (N_n,\beta_n) \to (P_n,\gamma_n) \to 0,$$

there is an exact sequence

$$0 \to \varprojlim M_n \to \varprojlim N_n \to \varprojlim P_n \to \varprojlim{}^1 M_n \to \varprojlim{}^1 N_n \to \varprojlim{}^1 P_n \to 0.$$

PROOF. The sequence

$$0 \to \prod M_n \to \prod N_n \to \prod P_n \to 0$$

is exact, and so this follows from the snake lemma. □

COROLLARY 8.7. *If the maps $\alpha_n\colon M_{n+1} \to M_n$ are all surjective, then the sequence*

$$0 \to \varprojlim M_n \to \varprojlim N_n \to \varprojlim P_n \to 0$$

is exact.

PROOF. The hypothesis implies that $\varprojlim^1 M_n = 0$ (axiom of determined choice). □

ASIDE 8.8. Direct (resp. inverse) limits are also called inductive (resp. projective) limits or colimits (resp. limits).

9 Tensor Products

Tensor products of modules

Let A be a ring, and let M, N, and P be A-modules. A map $\phi: M \times N \to P$ 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.

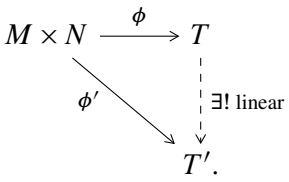
An A-module T together with an A-bilinear map

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

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

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

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

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

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 $\phi' : M \times N \to T'$ 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. Let M be an A-module and N a B-module; an A-linear map $\alpha : M \to N$ defines a B-linear map $\beta : B \otimes_A M \to N$ such that $b \otimes m \mapsto b \cdot \alpha(m)$, and $\alpha \leftrightarrow \beta$ is an isomorphism:

$$\mathrm{Hom}_{A\text{-linear}}(M,N) \simeq \mathrm{Hom}_{B\text{-linear}}(B \otimes_A M, N). \tag{19}$$

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 9.1. *Direct limits commute with tensor products:*

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

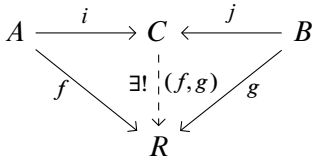
Proof. Using the universal properties of direct limits and tensor products, one sees easily that $\varinjlim(M_i \otimes_A N_j)$ has the universal property to be the tensor product of $\varinjlim M_i$ and $\varinjlim N_j$. □

Tensor products of algebras

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

[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.

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



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

$$\mathrm{Hom}(A \otimes_k B, R) \simeq \mathrm{Hom}(A,R) \times \mathrm{Hom}(B,R) \tag{20}$$

(k-algebra homomorphisms).

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

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

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

EXAMPLE 9.2. 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 $c \otimes a \mapsto ca: k \otimes_k A \to A$ is an isomorphism.

EXAMPLE 9.3. The ring $k[X_1, \dots, X_m, X_{m+1}, \dots, X_{m+n}]$, together with the obvious inclusions

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

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

$$\mathrm{Hom}(k[X_1, \dots, X_{m+n}], R) \to \mathrm{Hom}(k[X_1, \dots], R) \times \mathrm{Hom}(k[X_{m+1}, \dots], R)$$

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

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

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

REMARK 9.4. (a) Let $k \hookrightarrow k'$ be a homomorphism of rings. Then

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

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

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

(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

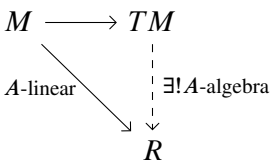
$$TM = \bigoplus\nolimits_{r \geq 0} T^r M.$$

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: every 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 $x_1, \dots, x_n$, 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

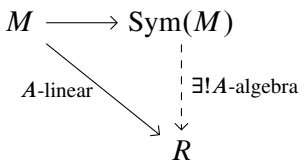
The ***symmetric algebra*** $\mathrm{Sym}(M)$ of an A-module M is the quotient of TM by the ideal generated by all elements of $T^2 M$ of the form

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

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: every 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 $x_1, \dots, x_n$, 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).

10 Flatness

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

$$0 \to N' \to N \to N'' \to 0 \tag{21}$$

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

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{x \mapsto mx = 0} \mathbb{Z}/m\mathbb{Z} \xrightarrow{x \mapsto x} \mathbb{Z}/m\mathbb{Z} \to 0.$$

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] In fact, $M \otimes_A M$ may be zero without M being zero, for example,[13]

$$\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0.$$

DEFINITION 10.1. 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 ***flat*** (resp. ***faithfully flat***) when B is flat (resp. faithfully flat) as an A-module.

[12] It was once customary in certain circles to require a ring to have an identity element $1 \neq 0$ (see, for example, Northcott 1953, p.3). However, without the zero ring, tensor products don't always exist. Bourbaki's first example of a ring is the zero ring.

[13] Let $x, y \in \mathbb{Q}/\mathbb{Z}$; then $nx = 0$ for some $n \in \mathbb{Z}$, and $y = ny'$ for some $y' \in \mathbb{Q}/\mathbb{Z}$; now

$$x \otimes y = x \otimes ny' = nx \otimes y' = 0 \otimes y' = 0.$$

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

$$0 \to M \otimes_A N' \to M \otimes_A N \to M \otimes_A N'' \to 0 \tag{22}$$

is exact whenever (21) is exact. An A-algebra B is said to be ***flat*** if B is flat as an A-module.

EXAMPLE 10.2. 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. In fact, every module over a product of fields (even an infinite product) is flat.

EXAMPLE 10.3. Quotient maps $A \to A/\mathfrak{a}$ are rarely flat. If A is a product, $A = A_1 \times A_2$, then the quotient map $A \twoheadrightarrow A_1$ is obviously flat. When A is noetherian, all flat quotient maps are of this form.[14]

PROPOSITION 10.4. *Let $A \to B$ be a faithfully flat homomorphism of rings. A sequence of A-modules*

$$0 \to N' \to N \to N'' \to 0 \tag{23}$$

is exact if

$$0 \to B \otimes_A N' \to B \otimes_A N \to B \otimes_A N'' \to 0 \tag{24}$$

is exact.

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 10.5. There is a converse to the proposition: suppose that

$$(23) \text{ is exact } \Leftrightarrow (24) \text{ is exact;}$$

then $A \to B$ is faithfully flat. The implication "$\Rightarrow$" 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 10.6. *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.*

[14] The set $V(\mathfrak{a})$ is closed in $\operatorname{spec}(A)$ (by definition of the topology on $\operatorname{spec}(A)$). If $A \to A/\mathfrak{a}$ is flat, then $V(\mathfrak{a})$ is also open. Therefore $A = A_1 \times A_2$ and $\mathfrak{a}$ is of the form $\mathfrak{b} \times A_2$ with $\mathfrak{b}$ an ideal in A_1 such that $V(\mathfrak{b}) = \operatorname{spec}(A_1)$. On tensoring

$$0 \to \mathfrak{b} \times A_2 \to A_1 \times A_2 \to A_1/\mathfrak{b} \to 0$$

with $A_1/\mathfrak{b}$ we get an exact sequence

$$0 \to \mathfrak{b}/\mathfrak{b}^2 \to A_1/\mathfrak{b} \xrightarrow{\text{id}} A_1/\mathfrak{b} \to 0.$$

Therefore $\mathfrak{b} = \mathfrak{b}^2$, but $\mathfrak{b}$ is contained in all prime ideals of A_1, and so this implies that $\mathfrak{b} = 0$ (Nakayama's lemma, 3.9).

PROOF. Assume that $M_B \stackrel{\text{def}}{=} B \otimes_A N$ 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 (10.4) 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 10.7. *Let $i: A \to B$ be a faithfully flat homomorphism. For every A-module M, the sequence*

$$0 \to M \xrightarrow{d_0} B \otimes_A M \xrightarrow{d_1} B \otimes_A B \otimes_A M \tag{25}$$

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 $f: B \to A$ such that $f \circ i = \mathrm{id}_A$, and define

$$\begin{aligned} &k_0: B \otimes_A M \to M, && k_0(b \otimes m) = f(b)m \\ &k_1: B \otimes_A B \otimes_A M \to B \otimes_A M, && k_1(b \otimes b' \otimes m) = f(b)b' \otimes m. \end{aligned}$$

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 (25) becomes exact after tensoring in B. But the sequence obtained from (25) by tensoring with B is isomorphic to the sequence (25) for the homomorphism of rings $b \mapsto 1 \otimes b: B \to B \otimes_A B$ 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 10.8. *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 10.9. *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 10.10. *For every multiplicative subset S of a ring A and A-module M,*

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

The homomorphism $a \mapsto \frac{a}{1}: A \to S^{-1}A$ 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 §9, especially (19)), which proves the first statement. As $M \rightsquigarrow S^{-1}M$ is exact (5.11), so also is $M \rightsquigarrow S^{-1}A \otimes_A M$, which proves the second statement. □

PROPOSITION 10.11. *A homomorphism of rings $\varphi: A \to B$ is flat if $A_{\varphi^{-1}(\mathfrak{n})} \to B_{\mathfrak{n}}$ is flat for all maximal ideals $\mathfrak{n}$ in B.*

PROOF. Let $N' \to N$ be an injective homomorphism of A-modules, and let $\mathfrak{n}$ be a maximal ideal of B. Then $\mathfrak{p} = \varphi^{-1}(\mathfrak{n})$ is a prime ideal in A, and $A_{\mathfrak{p}} \otimes_A (N' \to N)$ is injective (10.10). Therefore, the map

$$B_{\mathfrak{n}} \otimes_A (N' \to N) \simeq B_{\mathfrak{n}} \otimes_{A_{\mathfrak{p}}} (A_{\mathfrak{p}} \otimes_A (N' \to N))$$

is injective, and so the kernel M of $B \otimes_A (N' \to N)$ has the property that $M_{\mathfrak{n}} = 0$. Let $x \in M$, and let $\mathfrak{a} = \{b \in B \mid bx = 0\}$. For each maximal ideal $\mathfrak{n}$ of B, x maps to zero in $M_{\mathfrak{n}}$, and so $\mathfrak{a}$ contains an element not in $\mathfrak{n}$. Hence $\mathfrak{a} = B$, and so $x = 0$. □

PROPOSITION 10.12. *The following conditions on a flat homomorphism $\varphi: A \to B$ 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) $\Rightarrow$ (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 $\mathfrak{a} = \operatorname{ann}(x) \stackrel{\text{def}}{=} \{a \in A \mid ax = 0\}$. Then $\mathfrak{a}$ is an ideal in A, and $M' \stackrel{\text{def}}{=} Ax \simeq A/\mathfrak{a}$. 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 $B \otimes_A M \supset B \otimes_A M' \neq 0$. □

In more geometric terms, the proposition says that a homomorphism $\varphi: A \to B$ is faithfully flat if it is flat and the map $\operatorname{spm} B \to \operatorname{spm} A$ is surjective.

THEOREM 10.13 (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 (6.26) shows that there exist elements $x_1, \dots, x_m$ of $F \otimes_A B$ such that $F[x_1, \dots, x_m]$ is a polynomial ring over F and $F \otimes_A B$ is a finite $F[x_1, \dots, x_m]$-algebra. After multiplying each x_i by an element of A, we may suppose that it lies in B. Let $b_1, \dots, b_n$ generate B as an A-algebra. Each b_i satisfies a monic polynomial equation with coefficients in $F[x_1, \dots, x_m]$. 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 $A_a[x_1, \dots, x_m]$-algebra (by 6.2). Therefore, after replacing A with A_a and B with B_a, we may suppose that B is a finite $A[x_1, \dots, x_m]$-algebra.

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

Let $E = F(x_1, \dots, x_m)$ be the field of fractions of $A[x_1, \dots, x_m]$, and let $b_1, \dots, b_r$ be elements of B that form a basis for $E \otimes_{A[x_1,\dots,x_m]} B$ as an E-vector space. Each element of B can be expressed as 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 $A[x_1, \dots, x_m]$-module. Then $b_1, \dots, b_r$ generate B_q as an $A[x_1, \dots, x_m]_q$-module. In other words, the map

$$(c_1, \dots, c_r) \mapsto \textstyle\sum c_i b_i : A[x_1, \dots, x_m]_q^r \to B_q \tag{26}$$

is surjective. This map becomes an isomorphism when tensored with E over $A[x_1, \dots, x_m]_q$, which implies that each element of its kernel is killed by a nonzero element of $A[x_1, \dots, x_m]_q$ and so is zero (because $A[x_1, \dots, x_n]_q$ is an integral domain). Hence the map (26) is an isomorphism, and so B_q is free of finite rank over $A[x_1, \dots, x_m]_q$. Let a be some nonzero coefficient of the polynomial q, and consider the maps

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

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 (10.10). Let $\mathfrak{m}$ be a maximal ideal in A_a. Then $\mathfrak{m}A_a[x_1, \dots, x_m]$ does not contain the polynomial q because the coefficient a of q is invertible in A_a. Hence $\mathfrak{m}A_a[x_1, \dots, x_m]_q$ is a proper ideal of $A_a[x_1, \dots, x_m]_q$, and so the map $A_a \to A_a[x_1, \dots, x_m]_q$ is faithfully flat (apply 10.12). This completes the proof. □

REMARK 10.14. The theorem holds for every 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 10.10), 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 3.7), 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.

EXERCISE 10.15. Let (A_i, α^i_j) be a direct system of rings, and let (M_i, β^i_j) be a direct system of abelian groups with the same indexing set. Suppose that each M_i has the structure of an A_i-module, and that the diagrams

$$\begin{array}{ccc} A_i \times M_i & \longrightarrow & M_i \\ \downarrow{\scriptstyle \alpha^i_j \times \beta^i_j} & & \downarrow{\scriptstyle \beta^i_j} \\ A_j \times M_j & \longrightarrow & M_j \end{array}$$

commute for all $i \le j$. Let $A = \varinjlim A_i$ and $M = \varinjlim M_i$.

(a) Show that M has a unique structure of an A-module for which the diagrams

$$\begin{array}{ccc} A_i \times M_i & \longrightarrow & M_i \\ \downarrow{\scriptstyle \alpha^i \times \beta^i} & & \downarrow{\scriptstyle \beta^i} \\ A \times M & \longrightarrow & M \end{array}$$

commute for all i.

(b) Show that M is flat as an A-module if each M_i is flat as an A_i-module.

(Bourbaki AC, I, §2, Prop. 9.)

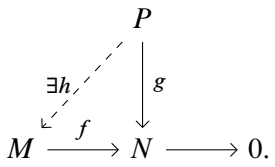
11 Finitely generated projective modules

In many situations, the correct generalization of "finite-dimensional vector space" is not "finitely generated module" but "finitely generated projective module". From a different perspective, they are the algebraists analogue of the differential geometers vector bundle. Throughout this section, A is a commutative ring.

Projective modules

DEFINITION 11.1. 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 $f \circ h = g$:



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 $h\colon P \to F$ 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 11.2. 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 $(a_i) \mapsto \sum_{i\in I} a_i e_i\colon A^I \to M$. 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 11.3. *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 N, and we wish to show that the kernel N' of $A^m \to M$ is finitely generated. Consider the diagram:

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

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

$$N \xrightarrow{f} N' \to A^m/gA^n \to 0,$$

either from the snake lemma or by a direct diagram chase. As N and A^m/gA^n are both finitely generated, so also is N' (by 3.3(b)). □

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 11.4. *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 and M is finitely presented, 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[15] 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 $f_i \in T$.

[15] 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 $s \overset{\text{def}}{=} s_{x_1} \cdots s_{x_n}$ lies in S and has the property that $sN = 0$. Therefore, $N_s = 0$.

(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 10.6).

(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

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

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 11.5. *Let*

$$0 \to N \to F \to M \to 0 \tag{27}$$

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

(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 $n = \sum_{i\in I} a_i y_i$ of F lies in N, then there exist $n_i \in N$ such that $n = \sum_{i\in I} a_i n_i$.*

(c) *Assume that M is flat and F is free. For every finite set $\{n_1, \ldots, n_r\}$ of elements of N, there exists an A-linear map $f: F \to N$ with $f(n_j) = n_j,\ j = 1, \ldots, r$.*

PROOF. (a) Consider

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

The first row is obtained from (27) by tensoring with $\mathfrak{a}$, and the second row is a subsequence of (27). 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 $n = \sum a_i n_i$.

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

$$n_1 = \textstyle\sum_{i\in I_0} a_i y_i$$

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

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

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

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

Then

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

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 $x_1,\ \dots,\ x_r \in M$ 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 $\{y_1,\ \dots,\ y_r\}$ 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.

EXAMPLE 11.6. (a) When regarded as a $\mathbb{Z}$-module, $\mathbb{Q}$ is flat but not projective (it is not finitely generated, much less finitely presented, and so this doesn't contradict the theorem).

(b) Let R be a product of copies of $\mathbb{F}_2$ indexed by $\mathbb{N}$, and let $\mathfrak{a}$ be the ideal in R consisting of the elements $(a_n)_{n\in\mathbb{N}}$ such that a_n is nonzero for only finitely many values of n (so $\mathfrak{a}$ is a direct *sum* of copies of $\mathbb{F}_2$ indexed by $\mathbb{N}$). The R-module R/I is finitely generated and flat, but not projective (it is not finitely presented, and so this doesn't contradict the theorem).

ASIDE 11.7. An A-module M is finitely generated and projective if and only if $\mathrm{Hom}(M, \cdot)$ commutes with arbitrary set-indexed direct sums (check; cf Keller 1998, 6.3).

ASIDE 11.8. 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 modules that are not finitely generated 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 11.9. *For any A-modules M, S, T with M finitely generated and projective, the canonical maps*

$$\mathrm{Hom}_{A\text{-}lin}(S, T \otimes_A M) \to \mathrm{Hom}_{A\text{-}lin}(S \otimes_A M^\vee, T) \tag{28}$$

$$T \otimes_A M \to \mathrm{Hom}_{A\text{-}lin}(M^\vee, T) \tag{29}$$

$$M^\vee \otimes T^\vee \to (M \otimes T)^\vee \tag{30}$$

$$M \to M^{\vee\vee} \tag{31}$$

are isomorphisms.

PROOF. The canonical map (28) 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 (28) 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 (29) sends $t \otimes m$ to the map $f \mapsto f(m)t$. It is the special case of (28) in which $S = A$.

The canonical map (30) 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 (31) sends m to the map $f \mapsto f(m): M^\vee \to A$. Again, it is obviously an isomorphism if one of M or T is free of finite rank, and hence also if one is a direct summand of such a module. □

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

LEMMA 11.10. *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*

$$\begin{array}{ccccc} M & \xrightarrow{\delta \otimes M} & M \otimes N \otimes M & \xrightarrow{M \otimes e} & M \\ N & \xrightarrow{N \otimes \delta} & N \otimes M \otimes N & \xrightarrow{e \otimes N} & N \end{array} \tag{32}$$

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

$$T \otimes_A N \simeq \mathrm{Hom}_{A\text{-}lin}(M, T) \tag{33}$$

for all A-modules T. In particular,

$$(N, e) \simeq (M^\vee, \mathrm{ev}). \tag{34}$$

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

$$x \mapsto f_x: T \otimes_A N \to \mathrm{Hom}_{A\text{-lin}}(M, T) \tag{35}$$

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

$$f \mapsto (f \otimes N)(\delta(1)): \mathrm{Hom}_{A\text{-lin}}(M, T) \to T \otimes_A N. \tag{36}$$

When the first (resp. the second) composite in (32) is the identity, then (36) is a right (resp. a left) inverse to (35).[16] Therefore, when a map δ exists with the required properties, the map (35) 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 sends $\delta(a)$ to the endomorphism $x \mapsto ax$ of M. This proves that δ is unique.

To get (34), take $T = M$ in (33). □

PROPOSITION 11.11. *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 (11.4c). Then δ is defined for each module M_{f_i}, and the uniqueness assertion in Lemma 11.10 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 (33), 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. □

ASIDE 11.12. 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):

---

[16] 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 (32) 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 $f = f_{(f \otimes N)(\delta(1))}$.

(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 every 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 11.13. 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.

SUMMARY 11.14. Here is a summary of the assumptions under which the canonical morphisms of A-modules below are isomorphisms. If P is finitely generated projective:

$$P \xrightarrow{\simeq} P^{\vee\vee}$$

A module P is finitely generated projective if and only if the following canonical map is an isomorphism

$$P^\vee \otimes P \xrightarrow{\simeq} \mathrm{End}(P).$$

If P or P' is finitely generated projective:

$$P^\vee \otimes P' \xrightarrow{\simeq} \mathrm{Hom}(P, P').$$

If both P and P' or both P and M or both P' and M' are finitely generated projective

$$\mathrm{Hom}(P, M) \otimes \mathrm{Hom}(P', M') \xrightarrow{\simeq} \mathrm{Hom}(P \otimes P', M \otimes M').$$

In particular, for P or P' finitely generated projective

$$P^\vee \otimes P'^\vee \xrightarrow{\simeq} (P \otimes P')^\vee.$$

(Georges Elencwajg on mathoverflow.net).

12 Zariski's lemma and 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 is obvious, because the polynomials $X - a$, $a \in k$, are distinct and irreducible. When k is finite, we can adapt Euclid's argument: if $p_1, \dots, p_r$ are monic irreducible polynomials in $k[X]$, then $p_1 \cdots p_r + 1$ is divisible by a monic irreducible polynomial distinct from $p_1, \dots, p_r$.

THEOREM 12.1 (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 it 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

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

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 $x_2, \dots, x_r$, and so the induction hypothesis implies that $x_2, \dots, x_r$ are algebraic over $k(x_1)$. According to Proposition 6.6, there exists a $c \in k[x_1]$ such that $cx_2, \dots, cx_r$ are integral over $k[x_1]$. Let $f \in K$. For a sufficiently large N, $c^N f \in k[x_1, cx_2, \dots, cx_r]$, and so $c^N f$ is integral over $k[x_1]$ by 6.4. 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 $k(x_1)$. □

COROLLARY 12.2. *Let A be a finitely generated k-algebra. Every maximal ideal in A is the kernel of a homomorphism from A into a finite field extension of k.*

PROOF. Indeed, $A/\mathfrak{m}$ itself is a finite field extension of k. □

Alternative proof of Zariski's lemma

The following is a simplification of Swan's simplication of a proof of Munshi — see Swan.

LEMMA 12.3. *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 $f \notin A$, and we can 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 in $A[X]$, which is absurd (it has degree ≥ 1). □

LEMMA 12.4. *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 $a_1, \dots, a_n \in A$ 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 12.5. *Let A be an integral domain, and suppose that there exists a maximal ideal $\mathfrak{m}$ in $A[X_1, \dots, X_n]$ such that $A \cap \mathfrak{m} = (0)$. Then there exists a nonzero element a in A such that A_a is a field and $A[X_1, \dots, X_n]/\mathfrak{m}$ 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 $K = A[X_1,\dots,X_n]/\mathfrak{m}$, and so the statement makes sense.

We argue by induction on n. When $n = 0$, the hypothesis is that (0) is a maximal ideal in A; hence A is a field, and the statement is trivial. Therefore, suppose that $n \geq 1$, and regard $A[X_1,\dots,X_n]$ 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 12.3. 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 12.4, $A_{a_1 \cdots a_n}$ is a field, and K is finite over it because it is integral (algebraic) and finitely generated. □

We now prove Zariski's lemma. Write $K = k[X_1,\dots,X_n]/\mathfrak{m}$. 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 12.6 (NULLSTELLENSATZ). *Every proper ideal $\mathfrak{a}$ in $k[X_1,\dots,X_n]$ has a zero in $(k^{\mathrm{al}})^n$, i.e., there exists a point $(a_1,\dots,a_n) \in (k^{\mathrm{al}})^n$ such that $f(a_1,\dots,a_n) = 0$ for all $f \in \mathfrak{a}$.*

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

COROLLARY 12.7. *When k is algebraically closed, the maximal ideals in $k[X_1,\dots,X_n]$ are exactly the ideals $(X_1-a_1,\dots,X_n-a_n)$, $(a_1,\dots,a_n) \in k^n$.*

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

$$f \in \mathfrak{m} \implies f \in (X_1-a_1,\dots,X_n-a_n),$$

and so $\mathfrak{m} = (X_1-a_1,\dots,X_n-a_n)$. □

THEOREM 12.8 (STRONG NULLSTELLENSATZ). *For an ideal $\mathfrak{a}$ in $k[X_1,\dots,X_n]$, let $Z(\mathfrak{a})$ be the set of zeros of $\mathfrak{a}$ in $(k^{\mathrm{al}})^n$. If a polynomial $h \in k[X_1,\dots,X_n]$ is zero on $Z(\mathfrak{a})$, then some power of h lies in $\mathfrak{a}$.*

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

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

If $(a_1,\dots,a_n,b)$ satisfies the first m equations, then $(a_1,\dots,a_n)\in Z(\mathfrak{a})$; consequently, $h(a_1,\dots,a_n)=0$, and $(a_1,\dots,a_n,b)$ doesn't satisfy the last equation. Therefore, the equations are inconsistent, and so, according to the Nullstellensatz (12.6), the ideal

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

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

$$1=\sum_{i=1}^{m} f_i\cdot g_i+f_{m+1}\cdot(1-Yh). \tag{37}$$

On applying the homomorphism

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

to (37), we obtain the identity

$$1=\textstyle\sum_i f_i(X_1,\dots,X_n,h^{-1})\cdot g_i(X_1,\dots,X_n) \tag{38}$$

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

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

for some N_i. Let N be the largest of the N_i. On multiplying (38) by h^N we obtain an identity

$$h^N=\textstyle\sum_i(\text{polynomial in } X_1,\dots,X_n)\cdot g_i(X_1,\dots,X_n),$$

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

PROPOSITION 12.9. *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:* $\operatorname{rad}(\mathfrak{a})=\bigcap_{\mathfrak{m}\supset\mathfrak{a}}\mathfrak{m}$. *In particular, if A is reduced, then* $\bigcap_{\mathfrak{m}\ \text{maximal}}\mathfrak{m}=0$.

PROOF. Because of the correspondence (2), p. 4, it suffices to prove this for $A=k[X_1,\dots,X_n]$.

The inclusion $\operatorname{rad}(\mathfrak{a})\subset\bigcap_{\mathfrak{m}\supset\mathfrak{a}}\mathfrak{m}$ holds in any ring (because maximal ideals are radical and $\operatorname{rad}(\mathfrak{a})$ is the smallest radical ideal containing $\mathfrak{a}$). Let $\mathfrak{a}$ be an ideal in $k[X_1,\dots,X_n]$, and let $h\in\bigcap_{\mathfrak{m}\supset\mathfrak{a}}\mathfrak{m}$. For any $(a_1,\dots,a_n)\in Z(\mathfrak{a})$, the evaluation map

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

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 $h(a_1,\dots,a_n)=0$, and we conclude from the strong Nullstellensatz that $h\in\operatorname{rad}(\mathfrak{a})$. □

13 The spectrum of a ring

Definition

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

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

PROPOSITION 13.1. *There are the following relations:*

(a) $\mathfrak{a} \subset \mathfrak{b} \implies V(\mathfrak{a}) \supset V(\mathfrak{b})$;
(b) $V(0) = V$; $V(A) = \emptyset$;
(c) $V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$;
(d) $V(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} V(\mathfrak{a}_i)$ *for every family of ideals* $(\mathfrak{a}_i)_{i \in I}$.

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

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

For the reverse inclusions, observe that if $\mathfrak{p} \notin V(\mathfrak{a}) \cup V(\mathfrak{b})$, then there exist an $f \in \mathfrak{a} \smallsetminus \mathfrak{p}$ and a $g \in \mathfrak{b} \smallsetminus \mathfrak{p}$; but then $fg \in \mathfrak{ab} \smallsetminus \mathfrak{p}$, and so $\mathfrak{p} \notin V(\mathfrak{ab})$. 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 $\operatorname{spec}(A)$ denote the set of prime ideals in A endowed with its Zariski topology.

For $h \in A$, let

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

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

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

and so the sets $D(h)$ form a base for the topology on V. Note that

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

For every element h of A, $\operatorname{spec}(A_h) \simeq D(h)$ (see 5.4), and for every ideal $\mathfrak{a}$ in A, $\operatorname{spec}(A)/\mathfrak{a} \simeq V(\mathfrak{a})$ (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.8). 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 $\operatorname{spec}(A) = \bigsqcup_i \operatorname{spec}(A_i)$ (disjoint union of open subsets).

Idempotents and connected components

Let A be a ring. In §1, we saw that complete sets of orthogonal idempotents in A correspond to decompositions of A into a finite product of rings. We now see that they also correspond to decompositions of spec A into a finite disjoint union of open subsets.

LEMMA 13.2. *The space* spec A *is disconnected if and only if A contains a nontrivial idempotent.*

PROOF. Let e be a nontrivial nilpotent, and let $f = 1-e$. For a prime ideal $\mathfrak{p}$, the map $A \to A/\mathfrak{p}$ must send exactly one of e or f to a nonzero element. This shows that spec A is a disjoint union of the sets[17] $D(e)$ and $D(f)$, each of which is open. If $D(e) = \operatorname{spec} A$, then e would be a unit (2.2), and hence can be cancelled from $ee = e$ to give $e = 1$. Therefore $D(e) \neq \operatorname{spec} A$, and similarly, $D(f) \neq \operatorname{spec} A$.

Conversely, suppose that spec A is disconnected, say, the disjoint union of two nonempty closed subsets $V(\mathfrak{a})$ and $V(\mathfrak{b})$. Because the union is disjoint, no prime ideal contains both $\mathfrak{a}$ and $\mathfrak{b}$, and so $\mathfrak{a}+\mathfrak{b} = A$. Thus $a+b = 1$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. As $ab \in \mathfrak{a}\cap\mathfrak{b}$, all prime ideals contain ab, which is therefore nilpotent (2.4), say $(ab)^m = 0$. Any prime ideal containing a^m contains a; similarly, any prime ideal containing b^m contains b; thus no prime ideal contains both a^m and b^m, which shows that $(a^m, b^m) = A$. Therefore, $1 = ra^m + sb^m$ for some $r, s \in A$. Now

$$\begin{aligned}(ra^m)(sb^m) &= rs(ab)^m = 0,\\ (ra^m)^2 &= (ra^m)(1-sb^m) = ra^m,\\ (sb^m)^2 &= sb^m\\ ra^m + sb^m &= 1,\end{aligned}$$

and so $\{ra^m, sb^m\}$ is a complete set of orthogonal idempotents. Clearly $V(\mathfrak{a}) \subset V(ra^m)$ and $V(\mathfrak{b}) \subset V(sb^m)$. As $V(ra^m)\cap V(sb^m) = \emptyset$, we see that $V(\mathfrak{a}) = V(ra^m)$ and $V(\mathfrak{b}) = V(sb^m)$, and so each of ra^m and sb^m is a nontrivial idempotent. □

PROPOSITION 13.3. *Let $\{e_1, \dots, e_n\}$ be a complete set of orthogonal idempotents in A. Then*

$$\operatorname{spec} A = D(e_1) \sqcup \dots \sqcup D(e_n)$$

is a decomposition of spec A *into a disjoint union of open subsets. Moreover, every such decomposition arises in this way.*

PROOF. Let $\mathfrak{p}$ be a prime ideal in A. Because $A/\mathfrak{p}$ is an integral domain, exactly one of the e_i's maps to 1 in $A/\mathfrak{p}$ and the remainder map to zero. This proves that spec A is the disjoint union of the sets $D(e_i)$.

Now consider a decomposition

$$\operatorname{spec} A = U_1 \sqcup \dots \sqcup U_n$$

each U_i open. We use induction on n to show that it arises from a complete set of orthogonal idempotents. When $n = 1$, there is nothing to prove, and when $n \geq 2$, we write

$$\operatorname{spec} A = U_1 \sqcup (U_2 \sqcup \dots \sqcup U_n).$$

[17] The set $D(e)$ consists of the prime ideals of A *not* containing e, and $V(\mathfrak{a})$ consists of all prime ideals containing $\mathfrak{a}$.

The proof of the lemma shows that there exist orthogonal idempotents $e_1, e_1' \in A$ such that $e_1 + e_1' = 1$ and

$$U_1 = D(e_1)$$
$$U_2 \sqcup \ldots \sqcup U_n = D(e_1') = \operatorname{spec} Ae_1'.$$

By induction, there exist orthogonal idempotents $e_2, \ldots, e_n$ in Ae_1' such that $e_2 + \cdots + e_n = e_1'$ and $U_i = D(e_i)$ for $i = 2, \ldots, n$. Now $\{e_1, \ldots, e_n\}$ is a complete set of orthogonal idempotents in A such that $U_i = D(e_i)$ for all i. □

The topological space spec(A)

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

$$S \subset A, \qquad V(S) = \{\mathfrak{p} \in \operatorname{spec}(A) \mid S \subset \mathfrak{p}\},$$
$$W \subset \operatorname{spec}(A), \qquad I(W) = \bigcap\nolimits_{\mathfrak{p} \in W} \mathfrak{p}.$$

Thus $V(S)$ is a closed subset of spec(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 spec(A) containing W); in particular, $VI(W) = W$ if W is closed.

PROPOSITION 13.4. *Let V be a closed subset of* spec(A).

(a) *There is an order-inverting one-to-one correspondence $W \leftrightarrow I(W)$ between the closed subsets of* spec(A) *and the radical ideals in A.*
(b) *The closed points of V are exactly the maximal ideals in V.*
(c) *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.*
(d) *If A is noetherian, every open covering of V has a finite subcovering.*

PROOF. (a) and (b) are obvious.

(c) 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., $V_m = V_{m+1}$.

(d) 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 $U_{i_0} \subsetneq U_{i_0} \cup U_{i_1}$. If $U_{i_0} \cup U_{i_1} \neq V$, then there exists an $i_2 \in I$ etc.. Because of (c), 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 ***quasi-compact*** (by Bourbaki at least; others call it compact, but Bourbaki requires a compact space to be Hausdorff). The proof of (d) shows that every noetherian space is quasi-compact. Since an open subspace of a noetherian space is again noetherian, it will also be quasi-compact.[18]

[18] In fact, spec(A) is always quasi-compact. To see this, let $(U_i)_{i \in I}$ be an open covering of spec(A). On covering each U_i with basic open subsets, we get a covering $(D(h_j))_{j \in J}$ of spec(A) by basic open subsets. Because $\operatorname{spec}(A) = \bigcup_j D(h_j)$, the ideal generated by the h_j is A, and so $1 = a_1 h_{j_1} + \cdots + a_m h_{j_m}$ for some $a_1, \ldots, a_m \in A$. Therefore $\operatorname{spec}(A) = \bigcup_{1 \le l \le m} D(h_{j_l})$, and it follows that spec(A) is covered by finitely many of the sets U_i.

DEFINITION 13.5. 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 13.6. *A closed subset W of* $\operatorname{specm}(A)$ *is irreducible if and only if it is irreducible. In particular, the spectrum of a ring A is irreducible if and only if the nilradical of A is prime.*

PROOF. $\Rightarrow$: Let W be an irreducible closed subset of $\operatorname{spec}(A)$, and suppose that $fg \in I(W)$. 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 that $W = V(\mathfrak{a}) \cup V(\mathfrak{b})$ 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 13.1c) and that $\mathfrak{a} \cap \mathfrak{b}$ is radical; hence $I(W) = \mathfrak{a} \cap \mathfrak{b}$ (by 14.2). 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 spectrum of a 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 13.7. Let $f \in k[X_1, \ldots, X_n]$. According to Theorem 4.9, $k[X_1, \ldots, X_n]$ 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 that f factors as

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

Then

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

PROPOSITION 13.8. *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 13.7, the $V(f_i)$ are the irreducible components of $V(f)$.

COROLLARY 13.9. *A radical ideal $\mathfrak{a}$ in a noetherian 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 $\mathfrak{p}_i = I(V_i)$. □

In particular, a noetherian ring has only finitely many minimal prime ideals, and their intersection is the radical of the ring.

COROLLARY 13.10. *A noetherian topological space has only finitely many connected components (each of which is open).*

PROOF. Each connected component is closed, hence noetherian, and so is a finite union of its irreducible components. Each of these is an irreducible component of the whole space, and so there can be only finitely many. □

REMARK 13.11. (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 $\mathrm{spec}(A)$ 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 §17). 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 13.7.

14 Jacobson rings and max spectra

DEFINITION 14.1. 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 $(0) = \bigcap_{p=2,3,5,\dots}(p)$. A principal ideal domain (more generally, a Dedekind domain) is Jacobson if it has infinitely many maximal ideals.[19] A local ring is Jacobson if and only if its maximal ideal is its only prime ideal. Proposition 12.9 shows that every finitely generated algebra over a field is Jacobson.

PROPOSITION 14.2. *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 2.4 says that the radical of an ideal is an intersection of prime ideals, and so this follows from the definition of a Jacobson ring. □

In a Jacobson ring A, there are natural one-to-one correspondences between

- ◇ the decompositions of $\operatorname{spm}(A)$ into a finite disjoint union of open subspaces,
- ◇ the decompositions of A into a finite direct products of rings, and
- ◇ the complete sets of orthogonal idempotents in A.

ASIDE 14.3. 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 $\operatorname{specm}(B) \to \operatorname{specm}(A)$.

ASIDE 14.4. The spectrum $\operatorname{spec}(A)$ 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 $\operatorname{specm}(A)$ is the subspace of $\operatorname{spec}(A)$ consisting of the closed points. When A is Jacobson, the map $U \mapsto U \cap \operatorname{specm}(A)$ is a bijection from the set of open subsets of $\operatorname{spec}(A)$ onto the set of open subsets of $\operatorname{specm}(A)$; therefore $\operatorname{specm}(A)$ and $\operatorname{spec}(A)$ have the same topologies — only the underlying sets differ.

ASIDE 14.5. 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 $X = \operatorname{specm}(A)$. An element f of A defines a k-valued function

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

on X. When A is reduced, Proposition 12.9 shows that this realizes A as a ring of k-valued functions on X. Moreover, because (40) 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, $\operatorname{specm}(A)$ is the spectrum of A in the sense of analysis.

[19] 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 $p_1, \dots, p_s$, 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. 18.7 below), and $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ 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.

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 $k(\mathfrak{m}) \stackrel{\text{def}}{=} A/\mathfrak{m}$ is a finitely generated k-algebra, and so $k(\mathfrak{m})$ is finite over k (Zariski's lemma, 12.1). 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 $A \to k^{\text{al}}$ 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

$$\text{Hom}_{k\text{-alg}}(A, k^{\text{al}}) \to \text{specm}(A). \tag{39}$$

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

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

and so differ by an automorphism[20] of k^{al}. Therefore, the fibres of (39) are exactly the orbits of $\text{Gal}(k^{\text{al}}/k)$. 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 (39) is a bijection.

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

$$Z(\mathfrak{a}) \to \text{specm}(A) \tag{40}$$

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

Maps of max spectra

Let $\varphi: A \to B$ 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, 12.1). 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

$$\varphi^*: \text{specm}(B) \to \text{specm}(A), \quad \mathfrak{m} \mapsto \varphi^{-1}(\mathfrak{m}),$$

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

THEOREM 14.6. *Let $\varphi: A \to B$ be a homomorphism of finitely generated k-algebras. Let U be a nonempty open subset of* specm(B)*, and let $\varphi^*(U)^-$ be the closure of its image in* specm(A)*. Then $\varphi^*(U)$ contains a nonempty open subset of each irreducible component of $\varphi^*(U)^-$.*

[20] 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}.

PROOF. Let $W = \operatorname{specm}(B)$ and $V = \operatorname{specm}(A)$, 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 14.7 below, there exists a nonzero element $a \in A$ such that every homomorphim $\alpha: A \to k^{\mathrm{al}}$ such that $\alpha(a) \neq 0$ extends to a homomorphism $\beta: B \to k^{\mathrm{al}}$ 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 $W_1, \dots, W_r$ 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 $\varphi: A \to B$ induces an injective homomorphism $\overline{\varphi}: A/\mathfrak{p} \to B/\mathfrak{q}$, and $\overline{\varphi}^*$ can be identified with the restriction of φ^* to W_1. From the first case, we know that $\overline{\varphi}^*(U \cap W_1)$ 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 14.7. *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 $\alpha: A \to \Omega$ from A into an algebraically closed field Ω such that $\alpha(a) \neq 0$ can be extended to a homomorphism $\beta: B \to \Omega$ such that $\beta(b) \neq 0$.*

We first need a lemma.

LEMMA 14.8. *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 $\alpha(\mathfrak{a})$,[21] 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.

[21] 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.

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 that $n < m$. If $m = 1$, such a $g(T)$ can't exist, and so we may suppose that $m > 1$ 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 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 14.7). 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 $\alpha: A[t_1, \ldots, t_{n-1}] \to \Omega$ such that $\alpha(b_{n-1}) \neq 0$ extends to a homomorphism $\beta: B \to \Omega$ 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 $\alpha: A \to \Omega$ 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 $\beta: B \to \Omega$ by the lemma, and $\beta(u(t) \cdot b) = \beta(c) \neq 0$, and so $\beta(b) \neq 0$. □

REMARK 14.9. 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 (cf. AM 5.23, p.66).

ASIDE 14.10. In general, the map $A \to A[X]$ does not induce a map $\operatorname{spm}(A[X]) \to \operatorname{spm}(A)$. Consider for example a discrete valuation ring A with maximal ideal (π) (e.g., $\mathbb{Z}_{(p)}$ with maximal ideal (p)). The ideal $(\pi X - 1)$ is maximal, because $A[X]/(\pi X - 1)$ is the field of fractions of A (by 5.3), but $(\pi X - 1) \cap A = (0)$, which is not maximal.

15 Quasi-finite algebras and Zariski's main theorem.

In this section we prove a fundamental theorem of Zariski.[22] Throughout, k is a field and A is a commutative ring.

Quasi-finite algebras

PROPOSITION 15.1. *Let B be a finite generated k-algebra. A prime ideal $\mathfrak{q}$ of B is an isolated point of $\operatorname{spec}(B)$ if and only if $B_{\mathfrak{q}}$ is finite over k.*

PROOF. To say that $\mathfrak{q}$ is an isolated point of $\operatorname{spec}(B)$ means that there exists an $f \in B \smallsetminus \mathfrak{q}$ such that $\operatorname{spec}(B_f) = \{\mathfrak{q}\}$. Now B_f is noetherian with only one prime ideal, namely, $\mathfrak{m} \stackrel{\text{def}}{=} \mathfrak{q}B_f$, and so it is artinian (7.6). The quotient $B_f/\mathfrak{m}$ is a field which is finitely generated as a k-algebra, and hence is finite over k (Zariski's lemma 12.1). Because B_f is artinian,

$$B_f \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots$$

can be refined to a finite filtration whose quotients are one-dimensional vector spaces over $B_f/\mathfrak{m}$. Therefore B_f is a finite k-algebra. As $f \notin \mathfrak{q}$, we have $B_{\mathfrak{q}} = (B_f)_{\mathfrak{q}}$, which equals B_f because B_f is local. Therefore $B_{\mathfrak{q}}$ is also a finite k-algebra.

For the converse, suppose that $B_{\mathfrak{q}}$ is finite over k, and consider the exact seqence

$$0 \to M \to B \to B_{\mathfrak{q}} \to N \to 0 \tag{41}$$

of B-modules. When we apply the functor $S_{\mathfrak{q}}^{-1}$ to (41), it remains exact (5.11), but the middle arrow becomes an isomorphism, and so $M_{\mathfrak{q}} = 0 = N_{\mathfrak{q}}$. Because B is noetherian, the B-module M is finitely generated, with generators $e_1, \ldots, e_m$ say. As $M_{\mathfrak{q}} = 0$, there exists, for each i, an $f_i \in B \smallsetminus \mathfrak{q}$ such that $f_i e_i = 0$. Now $f' \stackrel{\text{def}}{=} f_1 \ldots f_m$ has the property that $f'M = 0$, and so $M_{f'} = 0$.

Because $B_{\mathfrak{q}}$ is a finite k-algebra, N is finitely generated as a k-module, and therefore also as a B-module. As for M, there exists an $f'' \in B \smallsetminus \mathfrak{q}$ such that $M_{f''} = 0$. Now $f \stackrel{\text{def}}{=} f'f'' \in B \smallsetminus \mathfrak{q}$ has the property that $M_f = 0 = N_f$. When we apply the functor S_f^{-1} to (41), we obtain an isomorphism $B_f \simeq B_{\mathfrak{q}}$, and so $\operatorname{spec}(B_f) = \operatorname{spec}(B_{\mathfrak{q}}) = \{\mathfrak{q}\}$, which shows that $\mathfrak{q}$ is an isolated point. □

[22] Our exposition of the proof follows those in Raynaud 1970 and in Hochster's course notes from Winter, 2010.

PROPOSITION 15.2. *Let B be a finitely generated k-algebra. The space* $\operatorname{spec}(B)$ *is discrete if and only if B is a finite k-algebra.*

PROOF. If B is finite over k, then it is artinian and so (7.7)

$$B = \prod\{B_{\mathfrak{m}} \mid \mathfrak{m} \text{ maximal}\} \quad \text{(finite product)},$$

and

$$\operatorname{spec}(B) = \bigsqcup_{\mathfrak{m}} \operatorname{spec}(B_{\mathfrak{m}}) = \bigsqcup_{\mathfrak{m}} \{\mathfrak{m}\} \quad \text{(disjoint union of open subsets)}.$$

Therefore each point is isolated in $\operatorname{spec}(B)$.

Conversely, if $\operatorname{spec}(B)$ is discrete then it is a finite disjoint union,

$$\operatorname{spec}(B) = \bigsqcup_{1 \le i \le n} \operatorname{spec}(B_{f_i}), \quad f_i \in B,$$

with $\operatorname{spec}(B_{f_i}) = \{\mathfrak{q}_i\}$. Hence $B = \prod_{1 \le i \le n} B_{f_i}$ (by 13.3) with $B_{f_i} = B_{\mathfrak{q}_i}$. According to Proposition (15.1), each k-algebra $B_{\mathfrak{q}_i}$ is finite over k, and so B is finite over k. □

DEFINITION 15.3. Let B be a finitely generated A-algebra.

(a) Let $\mathfrak{q}$ be a prime ideal of B, and let $\mathfrak{p} = \mathfrak{q}^c$. The ring B is said to be ***quasi-finite over A at*** $\mathfrak{q}$ if $B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}$ is a finite $\kappa(\mathfrak{p})$-algebra.

(b) The ring B is said to be ***quasi-finite*** over A if it is quasi-finite over A at all the prime ideals of B.

PROPOSITION 15.4. *Let B be a finitely generated A-algebra. Let $\mathfrak{q}$ be a prime ideal of B, and let $\mathfrak{p} = \mathfrak{q}^c$. Then B is quasi-finite over A at $\mathfrak{q}$ if and only if $\mathfrak{q}$ is an isolated point of* $\operatorname{spec}(B \otimes_A \kappa(\mathfrak{p}))$.

PROOF. As

$$B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}} \simeq (B/\mathfrak{p}B)_{\mathfrak{q}/\mathfrak{p}} \simeq (B \otimes_A \kappa(\mathfrak{p}))_{\mathfrak{q}/\mathfrak{p}},$$

this is an immediate consequence of (15.1) applied to the $\kappa(\mathfrak{p})$-algebra $B \otimes_A \kappa(\mathfrak{p})$. □

The prime ideals of $B/\mathfrak{p}B$ correspond to the prime ideals of B whose contraction to A contains $\mathfrak{p}$, and the prime ideals of $B \otimes_A \kappa(\mathfrak{p})$ correspond to the prime ideals of B whose contraction to A is $\mathfrak{p}$. To say that B is quasi-finite over A at $\mathfrak{q}$ means that $\mathfrak{q}$ is both maximal and minimal among the prime ideals lying over $\mathfrak{p}$ (i.e., that each point of $\operatorname{spec}(B \otimes_A \kappa(\mathfrak{p}))$ is closed).

PROPOSITION 15.5. *A finitely generated A-algebra B is quasi-finite over A if and only if, for all prime ideals $\mathfrak{p}$ of A, $B \otimes_A \kappa(\mathfrak{p})$ is finite over $\kappa(\mathfrak{p})$.*

PROOF. Immediate consequence of (15.2). □

EXAMPLE 15.6. Let C be a finitely generated A-algebra. If C is finite over A, then $C \otimes_A \kappa(\mathfrak{p})$ is finite over $\kappa(\mathfrak{p})$ for all prime ideals $\mathfrak{p}$ of A, and so C is quasi-finite over A. In particular, $\operatorname{spec}(C)$ is discrete, and so if B is a finitely generated C-algebra such that the map $\operatorname{spec}(B) \to \operatorname{spec}(C)$ is an open immersion, then B is also quasi-finite over A. Zariski's main theorem says that all quasi-finite A-algebras arise in this way.

The next two lemmas will be used in the proof of Zariski's main theorem.

LEMMA 15.7. *Let $A \to C \to B$ be homomorphisms of rings such that the composite $A \to B$ is of finite type, and let $\mathfrak{q}$ be a prime ideal of B. If B is quasi-finite over A at $\mathfrak{q}$, then it is quasi-finite over C at $\mathfrak{q}$.*

PROOF. Let $\mathfrak{p}_A$ and $\mathfrak{p}_C$ be the inverse images of $\mathfrak{q}$ in A and C respectively. Then $\operatorname{spec}(B \otimes_C \kappa(\mathfrak{p}_C))$ is subspace of $\operatorname{spec}(B \otimes_A \kappa(\mathfrak{p}_A))$, and so if $\mathfrak{q}$ is an isolated point in the second space, then it is an isolated point in the first space. □

LEMMA 15.8. *Let $A \subset C \subset B$ be rings. Let $\mathfrak{q}$ be a prime ideal of B, and let $\mathfrak{r} = \mathfrak{q} \cap C$ and $\mathfrak{p} = \mathfrak{q} \cap A$.*

(a) *If $\mathfrak{q}$ is minimal among the primes lying over $\mathfrak{p}$ and there exists a $u \in C \smallsetminus \mathfrak{q}$ such that $C_u = B_u$, then $\mathfrak{r}$ is minimal among the primes lying over $\mathfrak{p}$.*
(b) *If B is integral over a finitely generated A-subalgebra B_0 and $\mathfrak{q}$ is maximal among the prime ideals lying over $\mathfrak{p}$, then $\mathfrak{r}$ is maximal among the prime ideals lying over $\mathfrak{p}$.*
(c) *Assume that B is integral over a finitely generated A-subalgebra B_0, and that there exists a $u \in C \smallsetminus \mathfrak{q}$ such that $C_u = B_u$. If B is quasi-finite over A at $\mathfrak{q}$, then C is quasi-finite over A at $\mathfrak{r}$.*

PROOF. (a) If $\mathfrak{r}'$ is a prime ideal of C lying over $\mathfrak{p}$ and strictly contained in $\mathfrak{r}$, then by extending $\mathfrak{r}'$ to $C_u = B_u$ and then contracting the result to B, we obtain a prime ideal $\mathfrak{q}'$ of B lying over $\mathfrak{p}$ and strictly contained in $\mathfrak{q}$.

(b) We may replace A, C, and B with their localizations at $\mathfrak{p}$, and so assume that A is local with maximal ideal $\mathfrak{p}$. Then

$$A/\mathfrak{p} \subset C/\mathfrak{r} \subset B/\mathfrak{q}$$

and we also have

$$A/\mathfrak{p} \subset B_0/\mathfrak{r}' \subset B/\mathfrak{r}$$

where $\mathfrak{r}' = \mathfrak{q} \cap B_0$. As $\mathfrak{q}$ is maximal among the prime ideals lying over $\mathfrak{p}$, $B/\mathfrak{q}$ is a field. As $B/\mathfrak{q}$ is integral over $B_0/\mathfrak{r}'$, the latter is also a field (see 6.16), and it is finitely generated as an $A/\mathfrak{p}$-algebra. Zariski's lemma (12.1) now shows that $B_0/\mathfrak{r}'$ is a finite algebraic extension of $A/\mathfrak{p}$, and so $B/\mathfrak{q}$ is an algebraic extension of $A/\mathfrak{p}$. It follows that $C/\mathfrak{r}$ is a field, and so $\mathfrak{r}$ is maximal among the prime ideals in C over $\mathfrak{p}$.

(c) Combine (a) and (b) (with the remark following (15.3)). □

ASIDE 15.9. Geometrically, to say that $A \to B$ is quasi-finite means that the map $\operatorname{Spec} B \to \operatorname{Spec} A$ has finite fibres. The condition that $A \to B$ be finite is much stronger: it not only requires that $\operatorname{Spec} B \to \operatorname{Spec} A$ have finite fibres but also that it be universally closed. See, for example, my notes on algebraic geometry.

Statement of Zariski's main theorem

THEOREM 15.10. *Let B be a finitely generated A-algebra, and let A' be the integral closure of A in B. Then B is quasi-finite over A at a prime ideal $\mathfrak{q}$ if and only if $A'_f \simeq B_f$ for some $f \in A' \smallsetminus \mathfrak{q}$.*

The sufficiency is obvious; the proof of the necessity will occupy the rest of this section. First, we list some consequences.

COROLLARY 15.11. *Let B be a finitely generated A-algebra. The set of prime ideals of B at which B is quasi-finite over A is open in* $\operatorname{spec}(B)$.

PROOF. Let $\mathfrak{q}$ be a prime ideal of B such that B is quasi-finite over A at $\mathfrak{q}$. The theorem shows that there exists an $f \in A' \smallsetminus \mathfrak{q}$ such that $A'_f \simeq B_f$. Write A' as the union of the finitely generated A-subalgebras A_i of A' containing f:

$$A' = \bigcup\nolimits_i A_i .$$

Because A' is integral over A, each A_i is finite over A (see 6.3). We have

$$B_f \simeq A'_f = \bigcup\nolimits_i A_{if} .$$

Because B_f is a finitely generated A-algebra, $B_f = A_{if}$ for all sufficiently large A_i. As the A_i are finite over A, B_f is quasi-finite over A, and $\operatorname{spec}(B_f)$ is an open neighbourhood of $\mathfrak{q}$ consisting of quasi-finite points. □

COROLLARY 15.12. *Let B be a finitely generated A-algebra, quasi-finite over A, and let A' be the integral closure of A in B. Then*

(a) *the map* $\operatorname{Spec} B \to \operatorname{Spec} A'$ *is an open immersion, and*
(b) *there exists an A-subalgebra A'' of A', finite over A, such that* $\operatorname{Spec} B \to \operatorname{Spec} A''$ *is an open immersion.*

PROOF. (a) Because B is quasi-finite over A at every point of $\operatorname{spec}(B)$, the theorem implies that there exist $f_i \in A'$ such that the open sets $\operatorname{spec}(B_{f_i})$ cover $\operatorname{spec}(B)$ and $A'_{f_i} \simeq B_{f_i}$ for all i. As $\operatorname{spec}(B)$ quasi-compact, finitely many sets $\operatorname{spec}(B_{f_i})$ suffice to cover $\operatorname{spec}(B)$, and it follows that $\operatorname{spec}(B) \to \operatorname{spec}(A')$ is an open immersion.

(b) We have seen that $\operatorname{spec}(B) = \bigcup_{1\le i\le n} \operatorname{spec}(B_{f_i})$ for certain $f_i \in A'$ such that $A'_{f_i} \simeq B_{f_i}$. The argument in the proof of (15.11) shows that there exists an A-subalgebra A'' of A', finite over A, which contains $f_1, \dots, f_n$ and is such that $B_{f_i} \simeq A''_{f_i}$ for all i. Now the map $\operatorname{spec}(B) \to \operatorname{spec}(A'')$ is an open immersion. □

Theorem 15.10, its corollary 15.12, and various global versions of these statements are referred to as Zariski's main theorem.

A variant of Zariski's main theorem

PROPOSITION 15.13. *Let $A \subset C \subset B$ be rings such that A integrally closed in B, C is finitely generated over A, and B is finite over C. If B is quasi-finite over A at a prime ideal $\mathfrak{q}$, then $B_{\mathfrak{p}} = A_{\mathfrak{p}}$ with $\mathfrak{p} = \mathfrak{q} \cap A$.*

PROOF THAT 15.13 IMPLIES 15.10

Let A, A', and B be as in the Theorem 15.10. We apply the proposition to $A' \subset B = B$ — Lemma 15.7 shows that the ring B is quasi-finite over A' at $\mathfrak{q}$. The proposition shows that $B_{\mathfrak{p}'} = A'_{\mathfrak{p}'}$ with $\mathfrak{p}' = \mathfrak{q} \cap A'$. Let $b_1, \dots, b_n$ generate B as an A'-algebra, and let b'_i denote the image of b_i in $B_{\mathfrak{p}'} = A'_{\mathfrak{p}'}$. Then $b'_i = a_i/f$ for some $a_i \in A'$ and $f \in A' \smallsetminus \mathfrak{p}'$. The b'_i are in the image of the map $A'_f \to B_f$, which is therefore surjective. But $A'_f \to B_f$ is injective because $A \subset B$, and so the map is an isomorphism. This completes the proof of the theorem.

Proof of Proposition 15.10

We proceed by proving four special cases of Proposition 15.10.

LEMMA 15.14. *Let $A \subset A[x] = B$ be rings such that A is integrally closed in B. If B is quasi-finite over A at a prime ideal $\mathfrak{q}$, then $B_{\mathfrak{p}} = A_{\mathfrak{p}}$ with $\mathfrak{p} = \mathfrak{q} \cap A$.*

PROOF. The hypotheses remain true when we invert the elements of $S \smallsetminus \mathfrak{p}$ to obtain $A_{\mathfrak{p}} \subset A_{\mathfrak{p}}[x] = B_{\mathfrak{p}}$. Thus, we may suppose that A is local with maximal ideal $\mathfrak{p}$, and we have to prove that $B = A$. As A is integrally closed in B and $B = A[x]$, it suffices to show that x is integral over A.

Let $k = A/\mathfrak{p}$ and consider the k-algebra

$$k[\overline{x}] \stackrel{\text{def}}{=} A[x] \otimes_A k = B \otimes_A \kappa(\mathfrak{p}).$$

By assumption, $\mathfrak{q}$ is an isolated point in $\operatorname{spec}(k[\overline{x}])$. Consequently, $\overline{x}$ is algebraic over k, because otherwise $k[\overline{x}]$ would be a polynomial ring over k, and its spectrum would have no isolated points. Therefore there exists a polynomial $F \in A[X]$ with nonconstant image in $k[X]$ such that $F(x) \in \mathfrak{p}A[x]$. Now $F - F(x)$ is a polynomial in $A[X]$ that vanishes on x and has at least one coefficient not in $\mathfrak{p}$. Choose such a polynomial H of minimum degree m, and write it

$$H(X) = a_m X^m + \cdots + a_0.$$

The equation $a^{m-1}H(x) = 0$ can be written

$$(a_m x)^m + a_{m-1}(a_m x)^{m-1} + \cdots + a_0 a_m^{m-1} = 0.$$

It shows that $a_m x$ is integral over A, and so lies in A. Now the polynomial

$$(a_m x + a_{m-1})X^{m-1} + \cdots + a_0$$

lies in $A[X]$ and vanishes on x. As it has degree $< m$, all of its coefficients must lie in $\mathfrak{p}$. In particular, $a_m x + a_{m-1} \in \mathfrak{p}$. If a_m is a unit, then x is integral over A, as required. Otherwise, $a_m \in \mathfrak{p}$ and a_{m-1} is a unit (because otherwise all coefficients of H lie in $\mathfrak{p}$); hence $a_{m-1} \in \mathfrak{p}B$, which is contradiction because $\mathfrak{p}B \subset \mathfrak{q}$. □

LEMMA 15.15. *Let B be an integral domain containing a polynomial ring $A[X]$ and integral over it. Then B is not quasi-finite over A at any prime ideal $\mathfrak{q}$.*

PROOF. Let $\mathfrak{q}$ be a prime ideal of B, and let $\mathfrak{p} = \mathfrak{q} \cap A$. If B is quasi-finite over A at $\mathfrak{q}$, then $\mathfrak{q}$ is both maximal and minimal among the prime ideals lying over $\mathfrak{p}$. We shall assume that $\mathfrak{q}$ is maximal and prove that it can't then be minimal.

Suppose first that A is integrally closed, and let $\mathfrak{r} = \mathfrak{q} \cap A[X]$. If $\mathfrak{r}$ were not maximal among the prime ideals of $A[X]$ lying over $\mathfrak{p}$, then the going-up theorem (6.20) would imply that $\mathfrak{q}$ is not either. Therefore $\mathfrak{r}$ is maximal among the prime over $\mathfrak{p}$, and it follows that its image $\overline{\mathfrak{r}}$ in $\kappa(\mathfrak{p})[X]$ is maximal. In particular, $\overline{\mathfrak{r}} \neq 0$, and so $\mathfrak{r}$ strictly contains the prime ideal $\mathfrak{p}A[X]$ in $A[X]$. As A is integrally closed, $A[X]$ is also (6.15), and the going down theorem (6.24) shows that $\mathfrak{q}$ strictly contains a prime ideal lying over $\mathfrak{p}A[X]$. Therefore, $\mathfrak{q}$ is not minimal among the prime ideals lying over $\mathfrak{p}$.

In the general case, we let B' denote the integral closure of B in its field of fractions. Then B' contains the integral closure A' of A, and is integral over $A'[T]$. Let $\mathfrak{q}'$ be a prime

ideal of B' lying over $\mathfrak{q}$ (which exists by 6.19), and let $\mathfrak{p}' = \mathfrak{q}' \cap A'$. As $\mathfrak{q}$ is maximal among the primes lying over $\mathfrak{p}$, $\mathfrak{q}'$ is maximal among those lying over $\mathfrak{p}'$ (apply 6.18 to $B \subset B'$). But, according to the preceding paragraph, $\mathfrak{q}'$ is not minimal, which implies that $\mathfrak{q}$ is not minimal (apply 6.18 again). □

LEMMA 15.16. *Let $A \subset A[x] \subset B$ be rings such that B is integral over $A[x]$ and A is integrally closed in B. If there exists a monic polynomial $F \in A[X]$ such that $F(x)B \subset A[x]$, then $A[x] = B$.*

PROOF. Let $b \in B$ be arbitrary. By assumption $F(x)b \in A[x]$, and so $F(x)b = G(x)$ for some polynomial G in $A[X]$. As F is monic, we can divide F into G to get

$$G = QF + R, \quad \deg R < \deg F, \quad Q, R \in A[X].$$

Now

$$F(x)b = G(x) = Q(x)F(x) + R(x).$$

For $c = b - Q(x)$,

$$F(x)c = R(x). \tag{42}$$

To show that $b \in A[x]$, it suffices to show that $c \in A$, and for this it suffices to show that c is integral over A.

Let A' be the image of A in B_c. As $\deg R < \deg F$, the equality (42) shows that $x/1$, as an element of B_c, is integral over the subring A'_c. As B is integral over $A[x]$, this implies that B_c is integral over A'_c. In particular, $c/1$ is integral over A'_c, and so it satisfies an equation whose coefficients we can assume to have a common denominator c^M:

$$(c/1)^m + \frac{a_1}{c^M}(c/1)^{m-1} + \cdots + \frac{a_m}{c^M} = 0, \quad a_i \in A,$$

(equality in B_c). Therefore

$$c^{M+m} + a_1 c^{m-1} + \cdots + a_m$$

is an element of B whose image in B_c is zero, and so is killed by a power of c. This shows that c is integral over A, as required. □

Let B be a finite A-algebra. The ***conductor*** of B in A is

$$\mathfrak{f}(B/A) = \{a \in A \mid aB \subset A\}.$$

This is an ideal of both A and B. In fact, it is the largest ideal in A that is also an ideal in B, because every element a of such an ideal has the property that $aB \subset A$. For any multiplicative subset S of A,

$$\mathfrak{f}(S^{-1}B/S^{-1}A) = S^{-1}\mathfrak{f}(B/A). \tag{43}$$

LEMMA 15.17. *Let $A \subset A[x] \subset B$ be rings such that B is finite over $A[x]$ and A is integrally closed in B. If B is quasi-finite over A at a prime ideal $\mathfrak{q}$, then $B_{\mathfrak{p}} = A_{\mathfrak{p}}$ with $\mathfrak{p} = \mathfrak{q} \cap A$.*

PROOF. Let $\mathfrak{f} = \mathfrak{f}(B/A[x])$, so

$$\mathfrak{f} = \{\alpha \in A[x] \mid \alpha B \subset A[x]\}.$$

We first consider the case that $\mathfrak{f} \not\subset \mathfrak{q}$. Let $\mathfrak{r} = \mathfrak{q} \cap A[x]$. For any $u \in \mathfrak{f} \smallsetminus \mathfrak{q}$, we have $A[x]_u = B_u$, and so Lemma 15.8 shows that $A[x]$ is quasi-finite over A at $\mathfrak{r}$.[23] Now Lemma 15.14 shows that $A[x]_{\mathfrak{p}} = A_{\mathfrak{p}}$. But B is finite over $A[x]$, and therefore $B_{\mathfrak{p}}$ is finite over $A[x]_{\mathfrak{p}} = A_{\mathfrak{p}}$. As A is integrally closed in B, $A_{\mathfrak{p}}$ is integrally closed in $B_{\mathfrak{p}}$, and therefore $A_{\mathfrak{p}} = B_{\mathfrak{p}}$, as required.

It remains to consider the case $\mathfrak{f} \subset \mathfrak{q}$. We choose a prime ideal $\mathfrak{n} \subset \mathfrak{q}$ of B minimal among those containing $\mathfrak{f}$. Let t denote the image of x in the ring $B/\mathfrak{n}$, and let $\mathfrak{m} = \mathfrak{n} \cap A$. Now

$$A/\mathfrak{m} \subset (A/\mathfrak{m})[t] \subset B/\mathfrak{n},$$

and $B/\mathfrak{n}$ is integral over $(A/\mathfrak{m})[t]$. As B is quasi-finite over A at $\mathfrak{q}$, the quotient $B/\mathfrak{n}$ is quasi-finite over $A/\mathfrak{m}$ at $\mathfrak{q}/\mathfrak{n}$. Now Lemma 15.15 implies that t is algebraic over $A/\mathfrak{m}$. We shall complete the proof by obtaining a contradiction, which will show that this case doesn't occur.

After making an extension of scalars $A \to A_{\mathfrak{m}}$, we may assume that A is a local ring with maximal ideal $\mathfrak{m}$. Let $\mathfrak{n}' = \mathfrak{n} \cap A[x]$. Because t is algebraic over $A/\mathfrak{m}$, the integral domain $A[x]/\mathfrak{n}'$ is a finite $A/\mathfrak{m}$-algebra, and hence a field (see §1). Therefore, $\mathfrak{n}'$ is maximal in $A[x]$, and it follows from (6.17) that $\mathfrak{n}$ is maximal in B. Thus $B/\mathfrak{n}$ is a field.

Because t is algebraic over $A/\mathfrak{m}$, there exists a monic polynomial F in $A[X]$ such that $F(x) \in \mathfrak{n}$. But $\mathfrak{n}$ is minimal among the prime ideals of B containing $\mathfrak{f}$, and so $\mathfrak{n}B_{\mathfrak{n}}$ is minimal among the prime ideals of $B_{\mathfrak{n}}$ containing $\mathfrak{f}_n$. In fact, $\mathfrak{n}B_{\mathfrak{n}}$ is the only prime ideal containing $\mathfrak{f}_{\mathfrak{n}}$, and so $\mathfrak{n}B_{\mathfrak{n}}$ is the radical of $\mathfrak{f}_{\mathfrak{n}}$. Therefore, there exists an integer $r > 0$ such that $(F(x))^r \in \mathfrak{f}_{\mathfrak{n}}$, and a $y \in B \smallsetminus \mathfrak{n}$ such that $yF(x)^r \in \mathfrak{f}$.

We therefore have $yF(x)^r B \subset A[x]$. On applying Lemma 15.16 with $A \subset A[x] \subset B'$, $B' = A[x][yB]$, and $F' = F^r$, we deduce that $B' = A[x]$ and therefore that $yB \subset A[x]$. Hence $y \in \mathfrak{f} \subset \mathfrak{n}$, which contradicts the definition of y. □

PROOF OF PROPOSITION 15.10

We use induction on the number n of generators of the A-algebra C. If $n = 0$, then B is integral over A, and so $B = A$. Assume that $n > 0$ and that the proposition has been proved when C is generated by $n-1$ elements.

Write $C = A[x_1, \dots, x_n]$, and let A' be the integral closure of $A[x_1, \dots, x_{n-1}]$ in B. Then

$$A' \subset A'[x_n] \subset B,$$

and B is finite over $A'[x_n]$. The ring B is finite over $A'[x_n]$ and it is quasi-finite over A at $\mathfrak{q}$, and so B is quasi-finite over A' at $\mathfrak{q}$ (by 15.7). From Lemma 15.17 we deduce that $A'_{\mathfrak{p}'} = B_{\mathfrak{p}'}$ with $\mathfrak{p}' = A' \cap \mathfrak{q}$.

As A' is integral over $A[x_1, \dots, x_{n-1}]$, it is a union of its finite subalgebras,

$$A' = \bigcup\nolimits_i A'_i, \quad A'_i \text{ finite over } A[x_1, \dots, x_{n-1}].$$

Let $\mathfrak{p}'_i = \mathfrak{q} \cap A'_i = \mathfrak{p}' \cap A'_i$. As B is finitely generated over $A[x_1, \dots, x_{n-1}]$, the canonical homomorphism

$$(A'_i)_{\mathfrak{p}'_i} \to B_{\mathfrak{p}'_i}$$

[23] Here we follow Hochster. Raynaud simply states that $A[x]$ is quasi-finite over A at $\mathfrak{r}$.

is an isomorphism for all sufficiently large i. For such an i, we have a fortiori that

$$(A_i')_{\mathfrak{p}_i'} \simeq B_{\mathfrak{q}},$$

and so A_i' is quasi-finite over A at $\mathfrak{p}_i'$. On applying the induction hypothesis to A, $A[x_1,\dots,x_{n-1}]$, and A_i', we deduce that

$$A_{\mathfrak{p}} \simeq (A_i')_{\mathfrak{p}} \simeq (A_i')_{\mathfrak{p}_i'},$$

and consequently that $A_{\mathfrak{p}} \simeq B_{\mathfrak{p}}$. This completes the proof of Proposition 15.13 and hence of Theorem 15.10.

16 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 16.1. *For any linear forms $\ell_1,\dots,\ell_m$ in $X_1,\dots,X_n$, the quotient ring*

$$k[X_1,\dots,X_n]/(\ell_1,\dots,\ell_m)$$

is an integral domain of transcendence degree equal to the dimension of the subspace of k^n defined by the equations

$$\ell_i = 0, \quad i = 1,\dots,m.$$

PROOF. This follows from the more precise statement:

> Let $\mathfrak{c}$ be an ideal in $k[X_1,\dots,X_n]$ generated by linearly independent linear forms $\ell_1,\dots,\ell_r$, and let $X_{i_1},\dots,X_{i_{n-r}}$ be such that
>
> $$\{\ell_1,\dots,\ell_r,X_{i_1},\dots,X_{i_{n-r}}\}$$
>
> is a basis for the linear forms in $X_1,\dots,X_n$. Then
>
> $$k[X_1,\dots,X_n]/\mathfrak{c} \simeq k[X_{i_1},\dots,X_{i_{n-r}}].$$

This is obvious if the forms ℓ_i are $X_1,\dots,X_r$. In the general case, because $\{X_1,\dots,X_n\}$ and $\{\ell_1,\dots,\ell_r,X_{i_1},\dots,X_{i_{n-r}}\}$ 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,

$$k[X_1,\dots,X_n] = k[\ell_1,\dots,\ell_r,X_{i_1},\dots,X_{i_{n-r}}],$$

and so

$$\begin{aligned} k[X_1,\dots,X_n]/\mathfrak{c} &= k[\ell_1,\dots,\ell_r,X_{i_1},\dots,X_{i_{n-r}}]/\mathfrak{c} \\ &\simeq k[X_{i_1},\dots,X_{i_{n-r}}]. \end{aligned}$$

□

PROPOSITION 16.2. *For any irreducible polynomial f in $k[X_1,\dots,X_n]$, the quotient ring $k[X_1,\dots,X_n]/(f)$ has transcendence degree $n-1$.*

PROOF. Let

$$k[x_1,\dots,x_n] = k[X_1,\dots,X_n]/(f), \quad x_i = X_i + (f),$$

and let $k(x_1,\dots,x_n)$ be the field of fractions of $k[x_1,\dots,x_n]$. 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 $X_1,\dots,X_{n-1}$ belongs to (f). This means that $x_1,\dots,x_{n-1}$ are algebraically independent. On the other hand, x_n is algebraic over $k(x_1,\dots,x_{n-1})$, and so $\{x_1,\dots,x_{n-1}\}$ is a transcendence basis for $k(x_1,\dots,x_n)$ over k. □

PROPOSITION 16.3. *For every 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 that

$$A = k[X_1,\dots,X_n]/\mathfrak{a} = k[x_1,\dots,x_n].$$

For $f \in A$, let $\bar{f}$ denote the image of f in $A/\mathfrak{p}$, so that $A/\mathfrak{p} = k[\bar{x}_1,\dots,\bar{x}_n]$. Let $d = \operatorname{tr.deg}_k A/\mathfrak{p}$, and number the X_i so that $\bar{x}_1,\dots,\bar{x}_d$ 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 $x_1,\dots,x_d, f$ 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

$$a_0(x_1,\dots,x_d)f^m + a_1(x_1,\dots,x_d)f^{m-1} + \cdots + a_m(x_1,\dots,x_d) = 0,$$

with $a_i \in k[X_1,\dots,X_d]$ and $a_0 \neq 0$. Because A is an integral domain, we can cancel a power of f if necessary to make $a_m(x_1,\dots,x_d)$ nonzero. On applying the homomorphism $A \to A/\mathfrak{p}$ to the above equality, we find that

$$a_m(\bar{x}_1,\dots,\bar{x}_d) = 0,$$

which contradicts the algebraic independence of $\bar{x}_1,\dots,\bar{x}_d$. □

PROPOSITION 16.4. *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

$$\operatorname{tr.deg}_k A/\mathfrak{p} \overset{16.3}{>} \operatorname{tr.deg}_k A/(f) \overset{16.2}{=} \operatorname{tr.deg}_k A - 1,$$

which contradicts the hypothesis. □

THEOREM 16.5. *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 16.6. *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 $\mathrm{Nm}_{L/K}\alpha \in A$, and α divides $\mathrm{Nm}_{L/K}\alpha$ 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 $\mathrm{Nm}_{L/K}(\alpha) = \pm a_0^{\frac{n}{r}}$ (see 5.40 of my notes Fields and Galois Theory). Moreover, a_0 lies in A by (6.10). 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 $\mathrm{Nm}_{L/K}\alpha$. □

PROOF (OF THEOREM 16.5). Write $\mathrm{rad}(f)$ as an irredundant intersection of prime ideals $\mathrm{rad}(f) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ (see 13.9). 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, $\mathrm{rad}(\frac{f}{1}) = \mathrm{rad}(f)^e = \mathfrak{p}_1^e$. Therefore, after replacing A with A_h, we may suppose that $\mathrm{rad}(f)$ is prime, say, equal to $\mathfrak{p}$.

According to the Noether normalization theorem (6.26), 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 $d = \mathrm{tr.deg}_k A$. According to the lemma, $f_0 \overset{\text{def}}{=} \mathrm{Nm}(f)$ lies in $k[x_1, \ldots, x_d]$, and we shall show that $\mathfrak{p} \cap k[x_1, \ldots, x_d] = \mathrm{rad}(f_0)$. Therefore, the homomorphism

$$k[x_1, \ldots, x_d]/\mathrm{rad}(f_0) \to A/\mathfrak{p}$$

is injective. As it is also finite, this implies that

$$\mathrm{tr.deg}_k A/\mathfrak{p} = \mathrm{tr.deg}_k k[x_1, \ldots, x_d]/\mathrm{rad}(f_0) \overset{16.2}{=} d - 1,$$

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

$$\mathrm{rad}(f_0) \subset \mathfrak{p} \cap k[x_1, \ldots, x_d]$$

because $\mathfrak{p}$ is radical. For the reverse inclusion, let $g \in \mathfrak{p} \cap k[x_1, \ldots, x_d]$. Then $g \in \mathrm{rad}(f)$, and so $g^m = fh$ for some $h \in A$, $m \in \mathbb{N}$. Taking norms, we find that

$$g^{me} = \mathrm{Nm}(fh) = f_0 \cdot \mathrm{Nm}(h) \in (f_0),$$

where e is the degree of the extension of the fields of fractions, which proves the claim. □

COROLLARY 16.7. *Let $\mathfrak{p}$ be a minimal nonzero prime ideal in A; then $\mathrm{tr.deg}_k(A/\mathfrak{p}) = \mathrm{tr.deg}_k(A) - 1$.*

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 16.8. *The length d of any maximal (i.e., nonrefinable) chain of distinct prime ideals*

$$\mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0 \tag{44}$$

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 (16.7), 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 16.9. 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 16.10. 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 16.4). 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 16.11. 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 $x_1, \dots, x_m$ is an algebraically independent set of elements of A such that A is a finite $k[x_1, \dots, x_m]$-algebra, then $\dim A = m$.

REMARK 16.12. Let A be a discrete valuation ring A with maximal ideal (π). Then $A[X]$ is a noetherian integral domain of Krull dimension 2, and $(\pi X - 1)$ is a maximal ideal in $A[X]$ of height 1 (cf. 14.10).

17 Primary decompositions

In this section, A is an arbitrary commutative ring.

DEFINITION 17.1. 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 17.2. *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 that $ab \in \text{rad}(\mathfrak{q})$ but $b \notin \text{rad}(\mathfrak{q})$. Then some power, say $a^n b^n$, of ab lies in $\mathfrak{q}$, but $b^n \notin \mathfrak{q}$, and so $a \in \text{rad}(\mathfrak{q})$. This shows that $\text{rad}(\mathfrak{q})$ is primary, and hence prime (because it is radical).

Let $\mathfrak{p}$ be a second prime ideal containing $\mathfrak{q}$, and let $a \in \text{rad}(\mathfrak{q})$. 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 17.3. *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 17.4. *Let $\varphi: A \to B$ 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 $\text{rad}(\mathfrak{q}^c)$-primary. But (see 2.10), $\text{rad}(\mathfrak{q}^c) = \text{rad}(\mathfrak{q})^c = \mathfrak{p}^c$, as claimed. □

LEMMA 17.5. *Let $\mathfrak{q}$ and $\mathfrak{p}$ be a pair of ideals in A such that $\mathfrak{q} \subset \mathfrak{p} \subset \text{rad}(\mathfrak{q})$ and*

$$ab \in \mathfrak{q} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{q}. \tag{45}$$

Then $\mathfrak{p}$ is a prime ideal and $\mathfrak{q}$ is $\mathfrak{p}$-primary.

PROOF. Clearly $\mathfrak{q}$ is primary, hence $\text{rad}(\mathfrak{q})$-primary, and $\text{rad}(\mathfrak{q})$ is prime. By assumption $\mathfrak{p} \subset \text{rad}(\mathfrak{q})$, and it remains to show that they are equal. Let $a \in \text{rad}(\mathfrak{q})$, 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 (45). □

PROPOSITION 17.6. *A finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

PROOF. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ be $\mathfrak{p}$-primary, and let $\mathfrak{q} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$. We show that the pair of ideals $\mathfrak{q} \subset \mathfrak{p}$ satisfies the conditions of (17.5).

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 $\mathfrak{p} \subset \text{rad}(\mathfrak{q})$.

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 17.7. 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 $\text{rad}(\mathfrak{q})$, $\mathfrak{q} \in S$, 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 17.6 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 17.8. *Suppose that* $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *where* $\mathfrak{q}_i$ *is* $\mathfrak{p}_i$*-primary for* $i = 1, \dots, n$*. Then the minimal prime ideals of* $\mathfrak{a}$ *are the minimal elements of the set* $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$*.*

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 (17.2) 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 17.9. *Let* $\mathfrak{q}$ *be a* $\mathfrak{p}$*-primary ideal and let* $x \in A \smallsetminus \mathfrak{q}$*. Then* $(\mathfrak{q}:x)$ *is* $\mathfrak{p}$*-primary (and hence* $\operatorname{rad}(\mathfrak{q}:x) = \mathfrak{p}$*).*

PROOF. For any $a \in (\mathfrak{q}:x)$, we know that $ax \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, and so $a \in \mathfrak{p}$. Hence $(\mathfrak{q}:x) \subset \mathfrak{p}$. On taking radicals, we find that $\operatorname{rad}(\mathfrak{q}:x) = \mathfrak{p}$. Let $ab \in (\mathfrak{q}:x)$. 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, $b \in (\mathfrak{q}:x)$ as required. □

THEOREM 17.10. *Let* $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ *be a minimal primary decomposition of* $\mathfrak{a}$*, and let* $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$*. Then*

$$\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \{\operatorname{rad}(\mathfrak{a}:x) \mid x \in A, \quad \operatorname{rad}(\mathfrak{a}:x) \text{ prime}\}.$$

In particular, the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ *is independent of the choice of the minimal primary decomposition.*

PROOF. For any $a \in A$,

$$(\mathfrak{a}:a) = (\textstyle\bigcap \mathfrak{q}_i : a) = \bigcap (\mathfrak{q}_i : a),$$

and so

$$\operatorname{rad}(\mathfrak{a}:a) = \operatorname{rad} \textstyle\bigcap (\mathfrak{q}_i:a) \overset{(17.9)}{=} \bigcap_{a \notin \mathfrak{q}_i} \mathfrak{p}_i. \tag{46}$$

If $\operatorname{rad}(\mathfrak{a}:a)$ is prime, then it equals one of the $\mathfrak{p}_i$ (otherwise, for each i there exists an $a_i \in \mathfrak{p}_i \smallsetminus \mathfrak{p}$, 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 $a \in \bigcap_{j \neq i} \mathfrak{q}_j \smallsetminus \mathfrak{q}_i$ because the decomposition is minimal, and (46) shows that $\operatorname{rad}(\mathfrak{a}:a) = \mathfrak{p}_i$. □

THEOREM 17.11. *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 17.12. *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 that (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 $A' \stackrel{\text{def}}{=} A/\mathfrak{a}$. 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

$$((0):a) \subset ((0):a^2) \subset \cdots$$

becomes constant, say, $((0):a^m) = ((0):a^{m+1})) = \cdots$. 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

$$(da^m)a = 0 \Rightarrow d \in (0:a^{m+1}) = (0:a^m) \Rightarrow c = 0.$$

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 3.16. The next result proves a converse when $\mathfrak{p}$ is maximal.

PROPOSITION 17.13. *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 17.14. 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 17.15. 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 $\mathfrak{ab} = \mathfrak{b}$ (see p. 13). Let

$$\mathfrak{ab} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_s, \quad \operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i,$$

be a minimal primary decomposition of $\mathfrak{ab}$. We shall show that $\mathfrak{b} \subset \mathfrak{ab}$ by showing that $\mathfrak{b} \subset \mathfrak{q}_i$ for each i.

If there exists a $b \in \mathfrak{b} \smallsetminus \mathfrak{q}_i$, then

$$\mathfrak{a}b \subset \mathfrak{ab} \subset \mathfrak{q}_i,$$

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 3.16), 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.

NOTES. In a future version, I'll explain the geometric significance of these statements. Also, I'll include the statements for modules, and explain how to deduce them from the statements for rings by a trick of Nagata. (When M is an A-module, $A \oplus M$ can be made into a ring by setting the product of any two elements of M equal to zero.). See also mo3910.

18 Dedekind domains

Discrete valuation rings

It follows from the elementary theory of principal ideal domains that the following conditions on a principal ideal domain A are equivalent:

(a) A has exactly one nonzero prime ideal;
(b) up to associates, A has exactly one prime element;
(c) A is local and is not a field.

A ring satisfying these conditions is called a ***discrete valuation ring***.

EXAMPLE 18.1. The ring $\mathbb{Z}_{(p)} \stackrel{\text{def}}{=} \{\frac{m}{n} \in \mathbb{Q} \mid n \text{ not divisible by } p\}$ is a discrete valuation ring with (p) as its unique nonzero prime ideal. The units in $\mathbb{Z}_{(p)}$ are the nonzero elements m/n with neither m nor n divisible by p, and the prime elements are those of the form unit$\times p$.

In a discrete valuation ring A with prime element π, nonzero elements of A can be expressed uniquely as $u\pi^m$ with u a unit and $m \geq 0$ (and $m > 0$ unless the element is a unit). Every nonzero ideal in A is of the form (π^m) for a unique $m \in \mathbb{N}$. Thus, if $\mathfrak{a}$ is an ideal in A and $\mathfrak{p}$ denotes the (unique) maximal ideal of A, then $\mathfrak{a} = \mathfrak{p}^m$ for a well-defined integer $m \geq 0$.

Recall that, for an A-module M and an $m \in M$, the annihilator of m

$$\text{ann}(m) = \{a \in A \mid am = 0\}.$$

It is an ideal in A, which is proper if $m \neq 0$. Suppose that A is a discrete valuation ring, and let c be a nonzero element of A. Let $M = A/(c)$. What is the annihilator of a nonzero element $b + (c)$ of M? Fix a prime element π of A, and let $c = u\pi^m$, $b = v\pi^n$ with u and v units. Then $n < m$ (else $b + (c) = 0$ in M), and

$$\text{ann}(b + (c)) = (\pi^{m-n}).$$

Thus, a b for which $\text{ann}(b + (c))$ is maximal, is of the form $v\pi^{m-1}$, and for this choice $\text{ann}(b + (c))$ is a prime ideal generated by $\frac{c}{b}$. We shall exploit these observations in the proof of the next proposition, which gives a criterion for a ring to be a discrete valuation ring.

PROPOSITION 18.2. *An integral domain A is a discrete valuation ring if and only if*

(a) *A is Noetherian,*
(b) *A is integrally closed, and*
(c) *A has exactly one nonzero prime ideal.*

PROOF. The necessity of the three conditions is obvious, and so let A be an integral domain satisfying (a), (b), and (c). We have to show that every ideal in A is principal. As a first step, we prove that the nonzero prime ideal is principal. Note that (c) implies that A is a local ring.

Choose an element $c \in A$, $c \neq 0$, $c \neq$ unit, and consider the A-module $M \stackrel{\text{def}}{=} A/(c)$. For each nonzero element m of M,

$$\operatorname{ann}(m) = \{a \in A \mid am = 0\}$$

is a proper ideal in A. Because A is Noetherian, we can choose an m so that $\operatorname{ann}(m)$ is maximal among these ideals. Write $m = b + (c)$ and $\mathfrak{p} = \operatorname{ann}(b + (c))$. Note that $c \in \mathfrak{p}$, and so $\mathfrak{p} \neq 0$, and that

$$\mathfrak{p} = \{a \in A \mid c|ab\}.$$

I claim that $\mathfrak{p}$ is prime. If not there exist elements $x, y \in A$ such that $xy \in \mathfrak{p}$ but neither x nor $y \in \mathfrak{p}$. Then $yb + (c)$ is a nonzero element of M because $y \notin \mathfrak{p}$. Consider $\operatorname{ann}(yb + (c))$. Obviously it contains $\mathfrak{p}$ and it contains x, but this contradicts the maximality of $\mathfrak{p}$ among ideals of the form $\operatorname{ann}(m)$. Hence $\mathfrak{p}$ is prime.

I claim that $\frac{b}{c} \notin A$. Otherwise $b = c \cdot \frac{b}{c} \in (c)$, and $m = 0$ (in M).

I claim that $\frac{c}{b} \in A$, and $\mathfrak{p} = (\frac{c}{b})$. By definition, $\mathfrak{p}b \subset (c)$, and so $\mathfrak{p} \cdot \frac{b}{c} \subset A$, and it is an ideal in A. If $\mathfrak{p} \cdot \frac{b}{c} \subset \mathfrak{p}$, then $\frac{b}{c}$ is integral over A (by 6.1, since $\mathfrak{p}$ is finitely generated), and so $\frac{b}{c} \in A$ (because of condition (b)), but we know $\frac{b}{c} \notin A$. Thus $\mathfrak{p} \cdot \frac{b}{c} = A$ (by (c)), and this implies that $\mathfrak{p} = (\frac{c}{b})$.

Let $\pi = \frac{c}{b}$, so that $\mathfrak{p} = (\pi)$. Let $\mathfrak{a}$ be a proper ideal of A, and consider the sequence

$$\mathfrak{a} \subset \mathfrak{a}\pi^{-1} \subset \mathfrak{a}\pi^{-2} \subset \cdots.$$

If $\mathfrak{a}\pi^{-r} = \mathfrak{a}\pi^{-r-1}$ for some r, then $\pi^{-1}(\mathfrak{a}\pi^{-r}) = \mathfrak{a}\pi^{-r}$, and π^{-1} is integral over A (by 6.1), and so lies in A — this is impossible (π is not a unit in A). Therefore the sequence is strictly increasing, and (again because A is Noetherian) it can't be contained in A. Let m be the smallest integer such that $\mathfrak{a}\pi^{-m} \subset A$ but $\mathfrak{a}\pi^{-m-1} \not\subseteq A$. Then $\mathfrak{a}\pi^{-m} \not\subseteq \mathfrak{p}$, and so $\mathfrak{a}\pi^{-m} = A$. Hence $\mathfrak{a} = (\pi^m)$. □

Dedekind domains

DEFINITION 18.3. A ***Dedekind domain*** is an integral domain A, not equal to a field, such that

(a) A is Noetherian,
(b) A is integrally closed, and
(c) every nonzero prime ideal is maximal (i.e., A has Krull dimension 1).

Thus Proposition 18.2 says that a local integral domain is a Dedekind domain if and only if it is a discrete valuation ring.

PROPOSITION 18.4. *Let A be a Dedekind domain, and let S be a multiplicative subset of A. Then $S^{-1}A$ is either a Dedekind domain or a field.*

PROOF. Condition (c) says that there is no containment relation between nonzero prime ideals of A. If this condition holds for A, then (5.4) shows that it holds for $S^{-1}A$. Conditions (a) and (b) follow from the next lemma. □

PROPOSITION 18.5. *Let A be an integral domain, and let S be a multiplicative subset of A.*

(a) *If A is Noetherian, then so also is $S^{-1}A$.*
(b) *If A is integrally closed, then so also is $S^{-1}A$.*

PROOF. (a) Let $\mathfrak{a}$ be an ideal in $S^{-1}A$. Then $\mathfrak{a} = S^{-1}(\mathfrak{a} \cap A)$ (see 5.4), and so $\mathfrak{a}$ is generated by any (finite) set of generators for $\mathfrak{a} \cap A$.

(b) Let α be an element of the field of fractions of A (= field of fractions of $S^{-1}A$) that is integral over $S^{-1}A$. Then

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

For each i, there exists an $s_i \in S$ such that $s_i a_i \in A$. Set $s = s_1 \cdots s_m \in S$, and multiply through the equation by s^m :

$$(s\alpha)^m + sa_1(s\alpha)^{m-1} + \cdots + s^m a_m = 0.$$

This equation shows that $s\alpha$ is integral over A, and so lies in A. Hence $\alpha = (s\alpha)/s \in S^{-1}A$. (See also 6.13.) □

COROLLARY 18.6. *For any nonzero prime ideal $\mathfrak{p}$ in a Dedekind domain A, the localization $A_\mathfrak{p}$ is a discrete valuation ring.*

PROOF. We saw in (5.7) that $A_\mathfrak{p}$ is local, and the proposition implies that it is Dedekind. □

The main result concerning Dedekind domains is the following.

THEOREM 18.7. *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. The primary ideals in a Dedekind domain are exactly the powers of prime ideals, and so this follows from the preceding section. (For an elementary proof, see my notes on algebraic number theory.) □

REMARK 18.8. Note that

$$r_i > 0 \iff \mathfrak{a}A_{\mathfrak{p}_i} \neq A_{\mathfrak{p}_i} \iff \mathfrak{a} \subset \mathfrak{p}_i.$$

COROLLARY 18.9. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in A; then*

$$\mathfrak{a} \subset \mathfrak{b} \iff \mathfrak{a}A_\mathfrak{p} \subset \mathfrak{b}A_\mathfrak{p}$$

for all nonzero prime ideals $\mathfrak{p}$ of A. In particular, $\mathfrak{a} = \mathfrak{b}$ if and only if $\mathfrak{a}A_\mathfrak{p} = \mathfrak{b}A_\mathfrak{p}$ for all $\mathfrak{p}$.

PROOF. The necessity is obvious. For the sufficiency, factor $\mathfrak{a}$ and $\mathfrak{b}$

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}, \quad \mathfrak{b} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}, \quad r_i, s_i \geq 0.$$

Then

$$\mathfrak{a}A_{\mathfrak{p}_i} \subset \mathfrak{b}A_{\mathfrak{p}_i} \iff r_i \geq s_i,$$

(recall that $A_{\mathfrak{p}_i}$ is a discrete valuation ring) and $r_i \geq s_i$ all i implies $\mathfrak{a} \subset \mathfrak{b}$. □

COROLLARY 18.10. *Let A be an integral domain with only finitely many prime ideals; then A is a Dedekind domain if and only if it is a principal ideal domain.*

PROOF. Assume A is a Dedekind domain. After (18.7), to show that A is principal, it suffices to show that the prime ideals are principal. Let $\mathfrak{p}_1,\dots,\mathfrak{p}_m$ be these ideals. Choose an element $x_1 \in \mathfrak{p}_1 \smallsetminus \mathfrak{p}_1^2$. According to the Chinese Remainder Theorem (2.12), there is an element $x \in A$ such that

$$x \equiv x_1 \mod \mathfrak{p}_1^2, \quad x \equiv 1 \mod \mathfrak{p}_i, \quad i \neq 1.$$

Now the ideals $\mathfrak{p}_1$ and (x) generate the same ideals in $A_{\mathfrak{p}_i}$ for all i, and so they are equal in A (by 18.9). □

COROLLARY 18.11. *Let $\mathfrak{a} \supset \mathfrak{b} \neq 0$ be two ideals in a Dedekind domain; then $\mathfrak{a} = \mathfrak{b} + (a)$ for some $a \in A$.*

PROOF. Let $\mathfrak{b} = \mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_m^{r_m}$ and $\mathfrak{a} = \mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_m^{s_m}$ with $r_i, s_j \geq 0$. Because $\mathfrak{b} \subset \mathfrak{a}$, $s_i \leq r_i$ for all i. For $1 \leq i \leq m$, choose an $x_i \in A$ such that $x_i \in \mathfrak{p}_i^{s_i}$, $x_i \notin \mathfrak{p}_i^{s_i+1}$. By the Chinese Remainder Theorem, there is an $a \in A$ such that

$$a \equiv x_i \mod \mathfrak{p}_i^{r_i}, \text{ for all } i.$$

Now one sees that $\mathfrak{b} + (a) = \mathfrak{a}$ by looking at the ideals they generate in $A_{\mathfrak{p}}$ for all $\mathfrak{p}$. □

COROLLARY 18.12. *Let $\mathfrak{a}$ be an ideal in a Dedekind domain, and let a be any nonzero element of $\mathfrak{a}$; then there exists a $b \in \mathfrak{a}$ such that $\mathfrak{a} = (a,b)$.*

PROOF. Apply (18.11) to $\mathfrak{a} \supset (a)$. □

COROLLARY 18.13. *Let $\mathfrak{a}$ be a nonzero ideal in a Dedekind domain; then there exists a nonzero ideal $\mathfrak{a}^*$ in A such that $\mathfrak{a}\mathfrak{a}^*$ is principal. Moreover, $\mathfrak{a}^*$ can be chosen to be relatively prime to any particular ideal $\mathfrak{c}$, and it can be chosen so that $\mathfrak{a}\mathfrak{a}^* = (a)$ with a any particular element of $\mathfrak{a}$ (but not both).*

PROOF. Let $a \in \mathfrak{a}$, $a \neq 0$; then $\mathfrak{a} \supset (a)$, and so we have

$$(a) = \mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_m^{r_m} \text{ and } \mathfrak{a} = \mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_m^{s_m}, \quad s_i \leq r_i.$$

If $\mathfrak{a}^* = \mathfrak{p}_1^{r_1-s_1}\cdots\mathfrak{p}_m^{r_m-s_m}$, then $\mathfrak{a}\mathfrak{a}^* = (a)$.

We now show that $\mathfrak{a}^*$ can be chosen to be prime to $\mathfrak{c}$. We have $\mathfrak{a} \supset \mathfrak{a}\mathfrak{c}$, and so (by 18.11) there exists an $a \in \mathfrak{a}$ such that $\mathfrak{a} = \mathfrak{a}\mathfrak{c} + (a)$. As $\mathfrak{a} \supset (a)$, we have $(a) = \mathfrak{a}\cdot\mathfrak{a}^*$ for some ideal $\mathfrak{a}^*$ (by the above argument); now, $\mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{a}^* = \mathfrak{a}$, and so $\mathfrak{c} + \mathfrak{a}^* = A$. (Otherwise $\mathfrak{c} + \mathfrak{a}^* \subset \mathfrak{p}$ some prime ideal, and $\mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{a}^* = \mathfrak{a}(\mathfrak{c} + \mathfrak{a}^*) \subset \mathfrak{a}\mathfrak{p} \neq \mathfrak{a}$.) □

In basic graduate algebra courses, it is shown that

$$A \text{ a principal ideal domain} \Rightarrow A \text{ is a unique factorization domain.}$$

The converse is false because, for example, $k[X,Y]$ is a unique factorization domain in which the ideal (X,Y) is not principal, but it is true for Dedekind domains.

PROPOSITION 18.14. *A Dedekind domain that is a unique factorization domain is a principal ideal domain.*

PROOF. In a unique factorization domain, an irreducible element π can divide a product bc only if π divides b or c (write $bc = \pi q$ and express each of b, c, and q as a product of irreducible elements). This means that (π) is a prime ideal.

Now let A be a Dedekind domain with unique factorization. It suffices to show that each nonzero prime ideal $\mathfrak{p}$ of A is principal. Let a be a nonzero element of $\mathfrak{p}$. Then a factors into a product of irreducible elements (see 4.3) and, because $\mathfrak{p}$ is prime, it will contain one of these irreducible factors π. Now $\mathfrak{p} \supset (\pi) \supset (0)$, and, because (π) is a nonzero prime ideal, it is maximal, and so equals $\mathfrak{p}$. □

Modules over Dedekind domains (sketch).

The structure theorem for finitely generated modules over principal ideal domains has an interesting extension to modules over Dedekind domains. Throughout this subsection, A is a Dedekind domain.

First, note that a finitely generated torsion-free A-module M need not be free. For example, every fractional ideal is finitely generated and torsion-free but it is free if and only if it is principal. Thus the best we can hope for is the following.

THEOREM 18.15. *Let A be a Dedekind domain.*

(a) *Every finitely generated torsion-free A-module M is isomorphic to a direct sum of fractional ideals,*
$$M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m.$$

(b) *Two finitely generated torsion-free A-modules $M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ and $N \approx \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_n$ are isomorphic if and only if $m = n$ and $\prod \mathfrak{a}_i \equiv \prod \mathfrak{b}_i$ modulo principal ideals.*

Hence,
$$M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m \approx A \oplus \cdots \oplus A \oplus \mathfrak{a}_1 \cdots \mathfrak{a}_m.$$

Moreover, two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A are isomorphic as A-modules if and only if they define the same element of the class group of A.

The ***rank*** of a module M over an integral domain R is the dimension of $K \otimes_R M$ as a K-vector space, where K is the field of fractions of R. Clearly the rank of $M \approx \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ is m.

These remarks show that the set of isomorphism classes of finitely generated torsion-free A-modules of rank 1 can be identified with the class group of A. Multiplication of elements in $\mathrm{Cl}(A)$ corresponds to the formation of tensor product of modules. The Grothendieck group of the category of finitely generated A-modules is $\mathrm{Cl}(A) \oplus \mathbb{Z}$.

THEOREM 18.16 (INVARIANT FACTOR THEOREM). *Let $M \supset N$ be finitely generated torsion-free A-modules of the same rank m. Then there exist elements $e_1, \ldots, e_m$ of M, fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$, and integral ideals $\mathfrak{b}_1 \supset \mathfrak{b}_2 \supset \ldots \supset \mathfrak{b}_m$ such that*
$$M = \mathfrak{a}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m e_m, \quad N = \mathfrak{a}_1\mathfrak{b}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m\mathfrak{b}_m e_m.$$

The ideals $\mathfrak{b}_1$, $\mathfrak{b}_2$, ..., $\mathfrak{b}_m$ are uniquely determined by the pair $M \supset N$, and are called the ***invariant factors*** of N in M.

The last theorem also yields a description of finitely generated torsion A-modules.

NOTES. We sketch a proof of (18.15a). Let A be a Dedekind domain, and let M be finitely generated torsion-free A-module. Then $A_\mathfrak{p} \otimes M$ is free, hence projective, for every nonzero prime ideal $\mathfrak{p}$ in A (because $A_\mathfrak{p}$ is principal ideal domain), and this implies that M is projective. Therefore there is a nonzero homomorphism $M \to A$, whose image is an ideal $\mathfrak{a}$ in A. As $\mathfrak{a}$ is projective, there exists a section to the map $M \twoheadrightarrow \mathfrak{a}$, and so $M \approx \mathfrak{a} \oplus M_1$ for some submodule M_1 of M. Now M_1 is projective because it is a direct summand of a projective module, and so we can repeat the argument with M_1. This process ends because M is noetherian.

NOTES. The Jordan-Hölder and Krull-Schmidt theorems fail for finitely generated projective modules over non-principal Dedekind domains. For example, suppose that A has a nonprincipal ideal $\mathfrak{a}$ of order 2 in the class group. Then $\mathfrak{a} \oplus \mathfrak{a} \approx A \oplus A$, contradicting both theorems.

19 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 (5.7) that $A_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}^e \stackrel{\text{def}}{=} \mathfrak{p}A_\mathfrak{p}$. The ideal

$$\left(\mathfrak{p}^n\right)^{ec} = \{a \in A \mid sa \in \mathfrak{p}^n \text{ for some } s \in S\}$$

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 5.8).

LEMMA 19.1. *The ideal $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.*

PROOF. According to Proposition 17.3, the ideal $(\mathfrak{p}^e)^n$ is $\mathfrak{p}^e$-primary. Hence (see 17.4), $((\mathfrak{p}^e)^n)^c$ is $(\mathfrak{p}^e)^c$-primary. But $\mathfrak{p}^{ec} = \mathfrak{p}$ (see 5.4), and

$$(((\mathfrak{p}^e)^n)^c \stackrel{2.10}{=} ((\mathfrak{p}^n)^e)^c \stackrel{\text{def}}{=} \mathfrak{p}^{(n)}. \tag{47}$$

LEMMA 19.2. *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 (5.4), $\mathfrak{p}' = \mathfrak{p}'^{ec}$ and $\mathfrak{p}''^c \neq \mathfrak{p}'^{ec}$, and so

$$\mathfrak{p}' = \mathfrak{p}'^{ec} \supsetneq \mathfrak{p}''^c \supset \mathfrak{a}^{ec} \supset \mathfrak{a}$$

contradicts the minimality of $\mathfrak{p}'$. □

THEOREM 19.3 (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 19.2, $\mathfrak{p}^e$ is a minimal prime ideal of $(b)^e = (\frac{b}{1})$, and (5.4) 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 7.6). 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

$$\mathfrak{p}_1^{(s)}+(b) = \mathfrak{p}_1^{(s+1)}+(b) = \mathfrak{p}_1^{(s+2)}+(b) = \cdots. \tag{48}$$

We claim that, for any $m \geq s$,

$$\mathfrak{p}_1^{(m)} \subset (b)\mathfrak{p}_1^{(m)} + \mathfrak{p}_1^{(m+1)}. \tag{49}$$

Let $x \in \mathfrak{p}_1^{(m)}$. Then

$$x \in (b)+\mathfrak{p}_1^{(m)} \overset{(48)}{=} (b)+\mathfrak{p}_1^{(m+1)},$$

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 19.1) 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 $b \in \mathfrak{p}$, (49) 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 (3.9).

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

$$\bigcap\nolimits_{m\geq s} \mathfrak{p}_1^{(m)} \overset{(47)}{=} \bigcap\nolimits_{m\geq s} ((\mathfrak{p}_1^e)^m)^c = (\bigcap\nolimits_{m\geq s} (\mathfrak{p}_1^e)^m)^c \overset{3.15}{=} (0)^c,$$

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 19.6 to non principal ideals, we shall need a lemma.

LEMMA 19.4. *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 2.7, 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 19.5. *Let A be a noetherian ring. For any proper ideal $\mathfrak{a} = (a_1,\dots,a_m)$, 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 that $m \geq 2$ 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 $\mathfrak{p}_1',\dots,\mathfrak{p}_t'$ be the minimal prime ideals of $(a_2,\dots,a_m)$. 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 2.7 shows that there exists a

$$b \in \mathfrak{p}_1 \smallsetminus \textstyle\bigcup_{i=1}^r \mathfrak{p}_i'.$$

We next show that $\mathfrak{p}$ is a minimal prime ideal of $(b,a_2,\dots,a_m)$. Certainly $\mathfrak{p}$ contains a minimal prime ideal $\mathfrak{p}'$ of this ideal. As $\mathfrak{p}' \supset (a_2,\dots,a_m)$, $\mathfrak{p}$ 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 $\overline{\mathfrak{p}} \stackrel{\text{def}}{=} \mathfrak{p}/(a_2,\dots,a_m)$ has height at least 2 in $\overline{A} \stackrel{\text{def}}{=} A/(a_2,\dots,a_m)$. But $\overline{\mathfrak{p}}$ is a minimal ideal in $\overline{A}$ of the principal ideal $(a_1,\dots,a_n)/(a_2,\dots,a_n)$, which contradicts Theorem 19.3. Hence $\mathfrak{p}$ is minimal, as claimed.

But now $\mathfrak{p}/(b)$ is a minimal prime ideal of $(b,a_2,\dots,a_m)$ 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 19.5.

THEOREM 19.6. *Let A be a noetherian ring, and let $\mathfrak{a}$ be a proper ideal of A of height r. Then there exist r elements $a_1,\dots,a_r$ of $\mathfrak{a}$ such that, for each $i \le r$, $(a_1,\dots,a_i)$ has height i.*

PROOF. If $r = 0$, then we take the empty set of a_is. Thus, suppose that $r \ge 1$. 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 2.7 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 19.3 shows it has height exactly 1.

This completes the proof when $r = 1$, and so suppose that $r \ge 2$. 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

$$a_2 \in \mathfrak{a} \smallsetminus \bigcup\{\text{prime ideals of height } 1 \text{ containing } (a_1)\}.$$

By construction, (a_1,a_2) has height at least 2, and so Theorem 19.5 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 19.7. *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 $(a_1,\dots,a_r)$ of height r. If $\mathfrak{a}$ is prime, then it is a minimal ideal of $(a_1,\dots,a_r)$. □

COROLLARY 19.8. *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 $\mathfrak{a}$,*

$$\operatorname{ht}(\mathfrak{p}/\mathfrak{a}) \le \operatorname{ht}(\mathfrak{p}) \le \operatorname{ht}(\mathfrak{p}/\mathfrak{a}) + n.$$

PROOF. The first inequality follows immediately from the correspondence between ideals in A and in $A/\mathfrak{a}$.

Denote the quotient map $A \to A' \overset{\text{def}}{=} A/\mathfrak{a}$ by $a \mapsto a'$. Let $\operatorname{ht}(\mathfrak{p}/\mathfrak{a}) = d$. Then there exist elements $a_1,\dots,a_d$ in A such that $\mathfrak{p}/\mathfrak{a}$ is a minimal prime ideal of $(a_1',\dots,a_d')$. Let $b_1,\dots,b_n$ generate $\mathfrak{a}$. Then $\mathfrak{p}$ is a minimal prime ideal of $(a_1,\dots,a_d,b_1,\dots,b_n)$, and hence has height $\le d+n$. □

We now use dimension theory to prove a stronger version of "generic flatness" (10.13).

THEOREM 19.9 (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 (10.14) 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 theorem (6.26) shows that there exist algebraically independent elements $x_1, \dots, x_m$ of $F \otimes_A B$ such that $F \otimes_A B$ is a finite $F[x_1, \dots, x_m]$-algebra. As in the proof of (10.13), there exists a nonzero $a \in A$ such that B_a is a finite $A_a[x_1, \dots, x_m]$-algebra. Hence M_a is a finitely generated $A_a[x_1, \dots, x_m]$-module.

As any extension of free modules is free[24], Proposition 3.5 shows that it suffices to prove the theorem for $M_a = A_a[x_1, \dots, x_m]/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ in $A_a[x_1, \dots, x_m]$. If $\mathfrak{p} = 0$, then M_a is free over A_a (with basis the monomials in the x_i). Otherwise, $F \otimes_A (A_a[x_1, \dots, x_m]/\mathfrak{p})$ has Krull dimension less than that of $F \otimes_A B$, and so we can apply the induction hypothesis. □

20 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

$$\operatorname{ht}(\mathfrak{m}) \overset{(19.5)}{\leq} \text{minimum number of generators of } \mathfrak{m} \overset{(3.11)}{=} \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

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.

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 20.1. *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 $e_1, \dots, e_n$ be elements of $\mathfrak{m}$ such that $\{e'_1, \dots, e'_n\}$ is a k-linear basis for $\mathfrak{m}'/\mathfrak{m}'^2$. We shall show that $\{e_1, \dots, e_n, c\}$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$.

As $e'_1, \dots, e'_n$ span $\mathfrak{m}'/\mathfrak{m}'^2$, they generate the ideal $\mathfrak{m}'$ (see 3.11), and so $\mathfrak{m} = (e_1, \dots, e_n) + (c)$, which implies that $\{e_1, \dots, e_n, c\}$ spans $\mathfrak{m}/\mathfrak{m}^2$.

Suppose that $a_1, \dots, a_{n+1}$ are elements of A such that

$$a_1e_1 + \cdots + a_ne_n + a_{n+1}c \equiv 0 \bmod \mathfrak{m}^2. \tag{50}$$

[24] If M' is a submodule of M such that $M'' \overset{\text{def}}{=} M/M'$ is free, then $M \approx M' \oplus M''$.

Then

$$a'_1e'_1 + \cdots + a'_ne'_n \equiv 0 \bmod \mathfrak{m}'^2,$$

and so $a'_1, \dots, a'_n \in \mathfrak{m}'$. It follows that $a_1, \dots, a_n \in \mathfrak{m}$. Now (50) 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 (50) is the trivial one. □

PROPOSITION 20.2. *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, (19.8) shows that

$$\operatorname{ht}(\mathfrak{m}') \le \operatorname{ht}(\mathfrak{m}) \le \operatorname{ht}(\mathfrak{m}') + 1.$$

Therefore

$$\dim_k(\mathfrak{m}'/\mathfrak{m}'^2) \ge \operatorname{ht}(\mathfrak{m}') \ge \operatorname{ht}(\mathfrak{m}) - 1 = \dim_k(\mathfrak{m}/\mathfrak{m}^2) - 1 = \dim_k(\mathfrak{m}'/\mathfrak{m}'^2).$$

Equalities must hold throughout, which proves that A' is regular with dimension $\dim A - 1$. □

THEOREM 20.3. *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 that $b \in \mathfrak{a}^n = (a^n)$ for some $n \ge 1$. 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 $b \in \bigcap_n \mathfrak{a}^n \overset{3.15}{=} \{0\}$. Therefore $\mathfrak{p} = \{0\}$, and so A is an integral domain.

We now assume $d \ge 1$, 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 (§17) 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 2.7 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 $d \ge 1$. □

COROLLARY 20.4. *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 3.16). The ring $A/\mathfrak{m}^r$ is local and artinian, and so $\mathfrak{a} = (t^s) + \mathfrak{m}^r$ for some $s \ge 1$ (by 7.8). This implies that $\mathfrak{a} = (t^s)$ by Nakayama's lemma (3.9). □

THEOREM 20.5. *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. Omitted for the moment. □

The best proof uses homological methods. See May, RegularLocal.pdf or Matsumura 1986 19.3, 20.3.

21 Completions

Let A be a ring and $\mathfrak{a}$ an ideal in A. For any A-module, we get an inverse system of quotient maps

$$M/\mathfrak{a}M \leftarrow M/\mathfrak{a}^2M \leftarrow \cdots \leftarrow M/\mathfrak{a}^nM \leftarrow \cdots$$

whose limit we define to be the $\mathfrak{a}$-adic completion $\widehat{M}$ of M:

$$\widehat{M} \stackrel{\text{def}}{=} \varprojlim M/\mathfrak{a}^nM.$$

For example, the $\mathfrak{a}$-adic completion of A is

$$\widehat{A} \stackrel{\text{def}}{=} \varprojlim_n A/\mathfrak{a}^n.$$

We now explain why this is called the completion. Let M be an A-module. A filtration on M is a sequence of submodules

$$M = M_0 \supset \cdots \supset M_n \supset \cdots.$$

LEMMA 21.1. *Let $(M_n)_{n\in\mathbb{N}}$ be a filtration on an A-module M. There is a unique topology on M such that, for each $x \in M$, the set $\{x + M_n \mid n \in \mathbb{N}\}$ is a fundamental system of neighbourhoods for x. The completion $\widehat{M}$ of M relative to this topology is canonically isomorphic to $\varprojlim M/M_n$.*

PROOF. The first statement is obvious. For the second, recall that $\widehat{M}$ consists of the equivalence classes of Cauchy sequences in M. Let $(m_n)_{n\in\mathbb{N}}$ be a Cauchy sequence. For each n, the image of m_i in M/M_n becomes constant for large i — let $\overline{m}_n$ denote the constant value. The family $(\overline{m}_n)_{n\in\mathbb{N}}$ depends only on the equivalence class of the Cauchy sequence $(m_n)_{n\in\mathbb{N}}$, and

$$[(m_n)] \mapsto (\overline{m}_n)\colon \widehat{M} \to \varprojlim M/M_n$$

is an isomorphism. □

Let A be a ring and let $\mathfrak{a}$ be an ideal in A. A filtration $(M_n)_{n\in\mathbb{N}}$ on an A-module M is an $\mathfrak{a}$-filtration if $\mathfrak{a}M_n \subset M_{n+1}$ for all n. An $\mathfrak{a}$-filtration is stable if $\mathfrak{a}M_n = M_{n+1}$ for all sufficiently large n.

LEMMA 21.2. *Any two stable $\mathfrak{a}$-filtrations on an A-module M define the same topology on M.*

PROOF. It suffices to show that a stable $\mathfrak{a}$-filtration $(M_n)_{n\in\mathbb{N}}$ defines the $\mathfrak{a}$-adic topology on M. As $\mathfrak{a}M_n \subset M_{n+1}$ for all n, we have that $\mathfrak{a}^nM \subset M_n$ for all n. For some n_0, $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$, and so $M_{n+n_0} = \mathfrak{a}^nM_{n_0} \subset \mathfrak{a}^nM$. □

LEMMA 21.3 (ARTIN-REES). *If A is noetherian and M is finitely generated, then, for any A-submodule M' of M, the filtration $(M' \cap \mathfrak{a}^nM)_{n\in\mathbb{N}}$ on M' is a stable $\mathfrak{a}$-filtration.*

PROOF. Omitted for the moment. □

PROPOSITION 21.4. *For every noetherian ring A and ideal $\mathfrak{a}$, the functor $M \rightsquigarrow \widehat{M}$ is exact on finitely generated A-modules.*

PROOF. Let

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

be an exact sequence of A-modules. For each n, the sequence

$$0 \to M' \cap \mathfrak{a}^n M \to \mathfrak{a}^n M \to \mathfrak{a}^n M'' \to 0$$

is exact, and so

$$0 \to M'/(M' \cap \mathfrak{a}^n M) \to M/\mathfrak{a}^n M \to M''/\mathfrak{a}^n M'' \to 0$$

is exact. On passing to the inverse limit, we obtain an exact sequence

$$0 \to \varprojlim_n M'/(M' \cap \mathfrak{a}^n M) \to \widehat{M} \to \widehat{M}'' \to 0,$$

but the last three lemmas show that $\varprojlim_n M'/(M' \cap \mathfrak{a}^n M)$ is the $\mathfrak{a}$-adic completion of M'. □

PROPOSITION 21.5. *For every ideal $\mathfrak{a}$ in a noetherian ring A and finitely generated A-module M, the homomorphism*

$$a \otimes m \mapsto am \colon \widehat{A} \otimes_A M \to \widehat{M}$$

is an isomorphism.

PROOF. In other words, when A is noetherian, the functors $M \rightsquigarrow \widehat{A} \otimes M$ and $M \rightsquigarrow \widehat{M}$ agree on finitely generated A-modules M. This is obvious for $M = A$, and it follows for finitely generated free A-module because both functors take finite direct sums to direct sums. Choose a surjective homomorphism $A^m \to M$, and let N be its kernel. The exact sequence

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

gives rise to a exact commutative diagram

$$\begin{array}{ccccccccc} & & \widehat{A} \otimes_A N & \longrightarrow & \widehat{A}^m & \longrightarrow & \widehat{A} \otimes_A M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \simeq} & & \downarrow{\scriptstyle b} & & \\ 0 & \longrightarrow & \widehat{N} & \longrightarrow & \widehat{A}^m & \longrightarrow & \widehat{M} & \longrightarrow & 0 \end{array}$$

Because the middle vertical arrow is an isomorphism, the arrow b is surjective. But M is arbitrary, and so the arrow a is also surjective, which implies that the arrow b is an isomorphism. □

PROPOSITION 21.6. *For every noetherian ring A and ideal $\mathfrak{a}$, the $\mathfrak{a}$-adic completion $\widehat{A}$ of A is a flat A-algebra.*

PROOF. It follows from (21.4) and (21.5) that $\widehat{A} \otimes_A -$ is exact on finitely generated A-modules, but this implies that it is exact on all A-modules. □

References

BOURBAKI, N. AC. Algèbre Commutative. Éléments de mathématique. Hermann; Masson, Paris. 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.

RAYNAUD, M. 1970. Anneaux locaux henséliens. Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, Berlin.

Index