A Primer of Commutative Algebra

James S. Milne

March 18, 2017, v4.02

Abstract

These notes collect the basic results in commutative algebra used in the rest of my notes and books. Although most of the material is standard, the notes include a few results, for example, the affine version of Zariski's main theorem, that are difficult to find in 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 $\mathbb{N} = \{0, 1, 2, \ldots\}$. Throughout, k is a field and k^{al} is an algebraic closure of k.

$X \subset Y$	X is a subset of Y (not necessarily proper).
$X \overset{\text{def}}{=} Y$	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.

Historical Notes

Sometime I'll add these. For the moment, I refer the reader to Bourbaki AC, Historical Note; Matsumura 1986, Introduction; Nagata 1962, Appendix A2.

Acknowledgements

I thank the following for providing corrections and comments for earlier versions of these notes: Amir Džambić, Florian Herzig, Chun Yin Hui, Keenan Kidwell, Leon Lampret, Junyu Lu, Andrew McLennan, Shu Otsuka, Dmitri Panov, Moss Sweedler, Bhupendra Nath Tiwari, Wei Xu.

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

When $A \subset B$ and $x_1, \ldots, x_n \in B$, we let $A[x_1, \ldots, x_n]$ 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. This means that B is a quotient of a polynomial ring $A[X_1, \ldots, X_n]$. An A-algebra B is ***finitely presented*** if it is the quotient of a polynomial ring $A[X_1, \ldots, X_n]$ 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 A a k-algebra. If $1_A \neq 0$, then 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. If $1_A = 0$, then 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 both an integral domain and an algebra over a field k. If A is finite over k, then it 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 every element a of A is algebraic over k, then $k[a]$ is finite over k, and hence contains an inverse of a; again A is a field.

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

Exercises

EXERCISE 1.1. Let k be an infinite field, and let f be a nonzero polynomial in $k[X_1, \ldots, X_n]$. Show that there exist $a_1, \ldots, a_n \in k$ such that $f(a_1, \ldots, a_n) \neq 0$.

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;
- $a \in \mathfrak{a}, r \in A \implies ra \in \mathfrak{a}$.

[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".

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 $S = \{a, b, \ldots\}$, we write $(a, b, \ldots)$ for the ideal it generates.

An ideal is ***principal*** if it is generated by a single element. Such an ideal (a) is proper if and only if a is not a unit. Thus a ring A is a field if and only if $1_A \neq 0$ and the only proper ideal in A is (0).

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 $\mathfrak{a} = (a_1, \ldots, a_m)$ and $\mathfrak{b} = (b_1, \ldots, b_n)$, then $\mathfrak{ab} = (a_1 b_1, \ldots, a_i b_j, \ldots, a_m b_n)$. 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 (regarded as an additive group) forms a ring $A/\mathfrak{a}$, and $a \mapsto a + \mathfrak{a}$ is a homomorphism $\varphi \colon A \to A/\mathfrak{a}$ whose kernel is $\mathfrak{a}$. There is a one-to-one correspondence

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

For 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. When $\mathfrak{p}$ is prime, we write $\kappa(\mathfrak{p})$ for the field of fractions of $A/\mathfrak{p}$.

LEMMA 2.1. *Let $\mathfrak{p}$ be a prime ideal in A.*

(a) *If $\mathfrak{p}$ contains a product of elements of A, then it contains one of the elements.*
(b) *If $\mathfrak{p}$ contains a finite product of ideals, then it contains one of the ideals.*

PROOF. (a) In the integral domain $A/\mathfrak{p}$, a finite product of elements is 0 only if one of its terms is zero.

(b) Suppose that $\mathfrak{p} \supset \mathfrak{a}_1 \cdots \mathfrak{a}_n$. If $\mathfrak{p}$ contains none of the $\mathfrak{a}_i$, then there exist $a_i \in \mathfrak{p} \smallsetminus \mathfrak{a}_i$, $i = 1, \ldots, a_n$. But then $a_1 \cdots a_n \in \mathfrak{p}$, which is a contradiction.

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 nonzero proper ideals (by (2)), and so is a field. Note that

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

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

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

For example, the following are multiplicative subsets:
the multiplicative subset $\{1, f, \ldots, f^r, \ldots\}$ generated by an element f of A;
the complement of a prime ideal (or of a union of prime ideals);
$1+\mathfrak{a} \overset{\text{def}}{=} \{1+a \mid a \in \mathfrak{a}\}$ for any ideal $\mathfrak{a}$ of A.

PROPOSITION 2.2. *Let S be a subset of a ring A and $\mathfrak{a}$ 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 2.3. *Every proper ideal in a ring is contained in a maximal ideal.*

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

An element f of a ring is ***nilpotent*** if $f^r = 0$ for some $r \geq 1$. A ring is ***reduced*** if it has no nonzero nilpotents. The ***radical*** $\mathrm{rad}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ in a ring A is

$$\{f \in A \mid f^r \in \mathfrak{a} \text{ some } r \geq 1\}.$$

An ideal $\mathfrak{a}$ is said to be ***radical*** if it equals its radical. Thus an ideal $\mathfrak{a}$ is radical if and only if $A/\mathfrak{a}$ is reduced. 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 2.4. *Let $\mathfrak{a}$ be an ideal in a ring A.*

(a) The radical of $\mathfrak{a}$ is an ideal.

(b) $\mathrm{rad}(\mathrm{rad}(\mathfrak{a})) = \mathrm{rad}(\mathfrak{a})$.

PROOF. (a) If $f \in \mathrm{rad}(\mathfrak{a})$, 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 4.11 below), but $\mathfrak{a} + \mathfrak{b} = (X^2, Y)$, which contains X^2 but not X.

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

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

For the reverse inclusion, let $f \notin \mathrm{rad}(\mathfrak{a})$. According to Proposition 2.2, there exists a prime ideal containing $\mathfrak{a}$ and disjoint from the multiplicative subset $\{1, f, \ldots\}$. Therefore $f \notin \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$.

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

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

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

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

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

$\Rightarrow$: 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.

$\Leftarrow$: If $1 - ac$ is not a unit, then it lies in some maximal ideal $\mathfrak{m}$ of A (by 2.3). Now $c \notin \mathfrak{m}$, because otherwise $1 = (1 - ac) + ac \in \mathfrak{m}$.

PROPOSITION 2.8 (PRIME AVOIDANCE). *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, $r \geq 1$, be ideals in A with $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ 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 $r > 1$. Suppose that $\mathfrak{a} \subset \bigcup_{1 \leq j \leq r} \mathfrak{p}_j$ and that no $\mathfrak{p}_j$ can be deleted from the union. In particular, $\mathfrak{a} \not\subset \bigcup_{j \neq i} \mathfrak{p}_j$, and so there exists an $a_i \in \mathfrak{a} \smallsetminus \bigcup_{j \neq i} \mathfrak{p}_j$. Then $a_i \in \mathfrak{p}_i$, because otherwise $a_i \in \mathfrak{a} \smallsetminus \bigcup_{1 \leq j \leq r} \mathfrak{p}_j$. Consider

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

I claim that a belongs to no $\mathfrak{p}_i$, which is a contradiction. Because none of the elements $a_1, \ldots, a_{r-1}$ lies in $\mathfrak{p}_r$ and $\mathfrak{p}_r$ is prime, their product does not lie in $\mathfrak{p}_r$ (2.1); but $a_r \in \mathfrak{p}_r$, and so $a \notin \mathfrak{p}_r$. Next consider an ideal $\mathfrak{p}_i$ 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 $a \notin \mathfrak{p}_i$.

ASIDE 2.9. [4]In general, the condition in (2.8) that the ideals $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ be prime is necessary. For example, the ideal (x, y) in $\mathbb{F}_2[x, y]$ is the union of three proper nonprime ideals. However, when A contains an infinite field k, the condition can be dropped. In the above proof, let V be the (finite-dimensional) k-vector space generated by the a_i, and let $V_i = \mathfrak{p}_i \cap V$. Then $V \subset \bigcup_{1 \leq i \leq r} V_i$, but the V_i are proper subspaces of V, and so this is impossible as k is infinite.

Extension and contraction of ideals

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

NOTATION 2.10. 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, $\mathfrak{b}^c = \mathfrak{b} \cap A$.

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

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

2.12. Let $\mathfrak{a}$ be an ideal of A and $\mathfrak{b}$ an ideal of B. Obviously (i) $\mathfrak{a} \subset \mathfrak{a}^{ec}$ and (ii) $\mathfrak{b}^{ce} \subset \mathfrak{b}$. 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:

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

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[5] of the theorem: let $d_1, \ldots, d_n$ be integers, relatively prime in pairs; then for any integers $x_1, \ldots, x_n$, 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 $d = \prod d_i$.

---

[4]Asides can be ignored.

[5]Often credited to Qin Jiushao (1208-1261), one of the greatest mathematicians of his era (NAMS, 2013).

We want to translate this into a statement about 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,

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

but the two ideals need not be equal.

These remarks suggest the following statement.

THEOREM 2.13 (CHINESE REMAINDER THEOREM). *Let $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ be ideals in a ring A. If $\mathfrak{a}_i$ is relatively prime to $\mathfrak{a}_j$ whenever $i \neq j$, then the map*

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

is surjective with kernel $\prod \mathfrak{a}_i$ (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. Moreover, 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 $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$. Thus

$$A/\mathfrak{a}_1\mathfrak{a}_2 \simeq A/\mathfrak{a}_1 \times A/\mathfrak{a}_2.$$

We now use induction to prove the theorem for $n > 2$. For $i \geq 2$, there exist elements $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_i$ such that

$$a_i + b_i = 1.$$

The product $\prod_{i\geq 2}(a_i + b_i)$ lies in $\mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n$ and equals 1, and so

$$\mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n = A.$$

Therefore,

$$\begin{aligned} A/\mathfrak{a}_1 \cdots \mathfrak{a}_n &= A/\mathfrak{a}_1 \cdot (\mathfrak{a}_2 \cdots \mathfrak{a}_n) \\ &\simeq A/\mathfrak{a}_1 \times A/\mathfrak{a}_2 \cdots \mathfrak{a}_n && \text{by the } n = 2 \text{ case} \\ &\simeq A/\mathfrak{a}_1 \times A/\mathfrak{a}_2 \times \cdots \times A/\mathfrak{a}_n && \text{by induction.} \end{aligned}$$

Exercises

EXERCISE 2.14. Let M be an A-module. Define the product of two elements of $A \oplus M$ by

$$(a,m)(a',m') = (aa', am' + a'm).$$

Show that this makes $A \oplus M$ into a ring. Show that the ideals of $A \oplus M$ contained in M are exactly the A-submodules of M.[6]

[6]This construction shows that modules over A and their submodules can be realized as ideals in the ring $A \oplus M$, which is useful for deducing results about modules from results about ideals. Nagata calls this the "principle of idealization" (Nagata 1962, p.2).

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., $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \cdots$ for some m.*
(c) *every nonempty set of ideals in A has a maximal element.*

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

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

(b) $\Rightarrow$ (c): Let Σ be a nonempty set of ideals in A. If Σ has no maximal element, then the axiom of dependent choice[7] shows that there exists a strictly ascending sequence of ideals in Σ, which contradicts (b).

(c) $\Rightarrow$ (a): Let $\mathfrak{a}$ be an ideal in A, 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 $\mathfrak{c} = (a_1, \ldots, a_r)$. If $\mathfrak{c} \neq \mathfrak{a}$, then there exists an element $a \in \mathfrak{a} \smallsetminus \mathfrak{c}$, and $(a_1, \ldots, a_r, a)$ will be a finitely generated ideal in $\mathfrak{a}$ properly containing $\mathfrak{c}$. This contradicts the definition of $\mathfrak{c}$, and so $\mathfrak{c} = \mathfrak{a}$.

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 A be a ring and*

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

an exact sequence of A-modules.

[7] 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 $a_n R a_{n+1}$ 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 $p \in P$. The second condition implies that there exists an $n \in N$ such that $\beta(n) = \beta(p)$. Then $\beta(p-n) = 0$, and so $p-n$ lies in $\alpha M'$, and hence in $\alpha M' \cap P = \alpha M' \cap N \subset N$. Thus $p = (p-n)+n \in N$.

(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 (3.3c).

Hence, every submodule of a finitely generated module over a noetherian ring is finitely generated. This statement is false for nonnoetherian rings, as any non finitely generated ideal in the ring demonstrates.

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 $x \neq 0$.

Let $\mathfrak{a} = \operatorname{ann}(x)$ be maximal among the annihilators of nonzero elements of M. I claim that $\mathfrak{a}$ is prime. 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 among the annihilators of nonzero elements of M, 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 (2.2) 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 a noetherian ring, and let B be a finitely generated A-algebra. We argue by induction on the minimum number of generators for B. As $A[x_1,\ldots,x_n] = A[x_1,\ldots,x_{n-1}][x_n]$, it suffices to prove the theorem for $n = 1$. But then B is a quotient of $A[X]$, and so it suffices to prove that $A[X]$ is noetherian.

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 called 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 $X(cX^{i-1} + \cdots) \in \mathfrak{a}$.

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 $\mathfrak{b} = \mathfrak{a}$. Suppose otherwise, and let f be a polynomial in $\mathfrak{a}$ of least degree i not in $\mathfrak{b}$. Because $\mathfrak{b}(i) = \mathfrak{a}(i)$, there exists a $g \in \mathfrak{b}$ such that $\deg(f - g) < \deg(f) = i$. Now $f - g \in \mathfrak{b}$, and so $f = (f - g) + g \in \mathfrak{b}$.

As A is noetherian, the sequence of ideals

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

becomes constant, say, $\mathfrak{a}(d) = \mathfrak{a}(d+1) = \ldots$ (and $\mathfrak{a}(d)$ contains the leading coefficient of *every* polynomial in $\mathfrak{a}$). For each $i \le d$, there exists a finite generating set $\{c_{i1}, c_{i2}, \ldots\}$ for $\mathfrak{a}(i)$, and for each (i, j), there exists a polynomial $f_{ij} \in \mathfrak{a}$ of degree i with leading coefficient c_{ij}. The ideal $\mathfrak{b}$ of $A[X]$ 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 A is noetherian, every finitely generated A-algebra is finitely presented.*

PROOF. Every finitely generated A-algebra B is of the form $A[X_1,\ldots,X_n]/\mathfrak{a}$ for some n and ideal $\mathfrak{a}$ in $A[X_1,\ldots,X_n]$. Because $A[X_1,\ldots,X_n]$ is noetherian, the ideal $\mathfrak{a}$ is finitely generated, and so B is finitely presented.

In particular, the polynomial ring $k[X_1,\ldots,X_n]$ over a field k is noetherian. This is the original theorem of Hilbert.

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 $\{e_1, \ldots, e_n\}$ for M, $n \geq 1$, and write

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

Then

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

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

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

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

COROLLARY 3.10. *Let A be a local ring with maximal ideal $\mathfrak{m}$ and residue field $k \overset{\text{def}}{=} A/\mathfrak{m}$, and let M be a finitely generated module over A. The action of A on $M/\mathfrak{m}M$ factors through k, and elements $a_1, \ldots, a_n$ of M generate it as an A-module if and only if the elements*

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

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

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

COROLLARY 3.11. *Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$. Elements $a_1, \ldots, a_n$ of $\mathfrak{m}$ generate $\mathfrak{m}$ as an ideal if and only if $a_1 + \mathfrak{m}^2, \ldots, a_n + \mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$ 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 (but see the next remark). 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 $\mathbb{Q} \neq 0$.

REMARK 3.13. Let A be a ring and $\mathfrak{a}$ a nilpotent ideal in A, say $\mathfrak{a}^r = 0$. Let M be an A-module (not necessarily finitely generated). If $M = \mathfrak{a}M$, then $M = \mathfrak{a}M = \cdots = \mathfrak{a}^r M = 0$. Therefore, if N is a submodule of M such that $M = N + \mathfrak{a}M$, then $M = N$ (because $M/N = \mathfrak{a}(M/N)$).

DEFINITION 3.14. Let A be a noetherian ring.

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

$$\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0. \tag{4}$$

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

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 (4) is d). It is sometimes convenient to define the Krull dimension of the zero ring to be -1.

Let A be an integral domain. Then

$$\dim(A) = 0 \iff (0) \text{ is maximal} \iff A \text{ is a field.}$$

The height of a nonzero prime ideal in a principal ideal domain is 1, and so such a ring has Krull dimension 1 (unless it is a field).

We shall see in §21 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).[8]

LEMMA 3.15. *Every set of generators for a finitely generated ideal contains a finite generating set.*

PROOF. Let S be a set of generators for an ideal $\mathfrak{a}$, and suppose that $\mathfrak{a}$ is generated by a finite set $\{a_1,...,a_n\}$. Each a_i lies in the ideal generated by a finite subset S_i of S, and so $\mathfrak{a}$ is generated by the finite subset $\bigcup S_i$ of S.

The lemma applies also to algebras, groups, modules, ... , not just ideals.

THEOREM 3.16 (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,

$$\bigcap\nolimits_{n\geq 1}\mathfrak{a}^n = \mathfrak{a}\cdot\bigcap\nolimits_{n\geq 1}\mathfrak{a}^n. \tag{5}$$

When $\mathfrak{a}$ is contained in all maximal ideals of A, Nakayama's lemma then shows that $\bigcap_{n\geq 1}\mathfrak{a}^n = 0$.

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

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

In other words, $\mathfrak{a}^n$ consists of the elements of A of the form $g(a_1,\ldots,a_r)$ for some homogeneous polynomial $g\in A[X_1,\ldots,X_r]$ of degree n.

Let S_m denote the set of homogeneous polynomials $f(X_1,\ldots,X_r)$ of degree m such that $f(a_1,\ldots,a_r)\in\bigcap_{n\geq 1}\mathfrak{a}^n$, and let $\mathfrak{c}$ be the ideal in $A[X_1,\ldots,X_r]$ generated by $\bigcup_m S_m$. Because $A[X_1,\ldots,X_r]$ is noetherian, $\mathfrak{c}$ is finitely generated, and so $\mathfrak{c}$ is generated by a finite set $\{f_1,\ldots,f_s\}$ of elements of $\bigcup_m S_m$ (3.15). Let $d_i = \deg f_i$, and let $d = \max d_i$.

Let $b\in\bigcap_{n\geq 1}\mathfrak{a}^n$; then $b\in\mathfrak{a}^{d+1}$, and so $b = f(a_1,\ldots,a_r)$ for some homogeneous polynomial f of degree $d+1$. By definition, $f\in S_{d+1}\subset\mathfrak{c}$, and so there exist $g_i\in A[X_1,\ldots,X_r]$ such that

$$f = g_1f_1+\cdots+g_sf_s \quad \text{in } A[X_1,\ldots,X_r].$$

[8] In Nagata 1962, p.203, there is the following example. Let $\mathbb{N} = I_0\sqcup I_1\sqcup\ldots$ be a partition of $\mathbb{N}$ into finite sets with strictly increasing cardinality. Let $A = k[X_0,X_1,\ldots]$ be the polynomial ring in a set of symbols indexed by $\mathbb{N}$, and let $\mathfrak{p}_i$ be the prime ideal in A generated by the X_j 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 $|I_i|$.

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 can choose the g_i to be homogeneous of degree $\deg f - \deg f_i = d + 1 - d_i > 0$. In particular, the constant term of g_i is zero, and so $g_i(a_1, \ldots, a_r) \in \mathfrak{a}$. Now

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

which completes the proof of (5).

The equality (5) can also be proved using primary decompositions — see (19.14).

PROPOSITION 3.17. *In a noetherian ring, every ideal contains a power of its radical; in particular, some power of the nilradical of the ring is zero.*

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

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

has a factor of the form $a_i^{r_i}$ for some i, and so lies in $\mathfrak{a}$. Thus $\mathrm{rad}(\mathfrak{a})^{r_1 + \cdots + r_n} \subset \mathfrak{a}$.

ASIDE 3.18. 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 3.19. The following example shows that the Krull intersection theorem fails for nonnoetherian rings. Let A be the ring of germs[9] 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 $\bigcap_{n \geq 1} \mathfrak{m}^n$ consists of the germs whose derivatives at zero are all zero. In particular, it contains the nonzero function e^{-1/x^2}.

Exercises

EXERCISE 3.20. Consider the subalgebra

$$A = k + k[X, Y]X = k[X, XY, XY^2, \ldots]$$

of $k[X, Y]$. Show that A is not noetherian (hence subrings of noetherian rings need not be noetherian, and subalgebras of finitely generated algebras need not be finitely generated).

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.,

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

[9] A 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 $U \cap U'$.

An integral domain A is called a ***unique factorization domain*** (or a ***factorial 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. The uniqueness condition 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.*

Thus, (a) is a prime ideal if a is irreducible and 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.

COROLLARY 4.2. *Let A be an integral domain. If A is a unique factorization domain, then every prime ideal of height 1 is principal.*

PROOF. Let $\mathfrak{p}$ be a prime ideal of height 1. Then $\mathfrak{p}$ contains a nonzero element, and hence an irreducible element a. We have $\mathfrak{p} \supset (a) \supset (0)$. As (a) is prime and $\mathfrak{p}$ has height 1, we must have $\mathfrak{p} = (a)$.

The converse is true for noetherian integral domains (21.4).

PROPOSITION 4.3. *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. We have to prove the uniqueness of factorizations. Suppose that

$$a_1 \cdots a_m = b_1 \cdots b_n \tag{6}$$

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 (6), 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 4.4. *Let A be an integral domain in which every ascending chain of principal ideals becomes constant (e.g., a noetherian integral domain). Then 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 4.5. *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

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

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

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

Let A be a unique factorization domain. A nonzero polynomial

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

in $A[X]$ is said to be ***primitive*** if the coefficients a_i have no common factor other than units. Every polynomial f in $F[X]$ 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 4.6. *Let A be a unique factorization domain. The product of two primitive polynomials in $A[X]$ is primitive.*

PROOF. Let

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

be primitive polynomials, and let p be a prime element of A. Let a_{i_0} be the first coefficient of f not divisible by p and b_{j_0} the first coefficient of g not divisible by p. Then all the terms in $\sum_{i+j=i_0+j_0} a_i b_j$ are divisible by p, except $a_{i_0} b_{j_0}$, which is not divisible by p. Therefore, p doesn't divide the $(i_0 + j_0)$th-coefficient of fg. We have shown that no prime 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 4.7. *Let A be a unique factorization domain with field of fractions F, and let $f, g \in F[X]$. Then*

$$c(fg) = c(f) \cdot c(g).$$

Hence every factor in $A[X]$ of a primitive polynomial is primitive.

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

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

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

COROLLARY 4.8. *The irreducible elements in $A[X]$ are the irreducible elements c of A and the nonconstant primitive polynomials f such that f is irreducible in $F[X]$.*

PROOF. Obvious from Propositions 4.5 and 4.7.

THEOREM 4.9. *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 (4.7). 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 $A[X]$.

It remains to show that each irreducible element of $A[X]$ is prime (see 4.3). There are two cases (4.8).

Let c 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 $q \in F[X]$. Because f is primitive, $c(q) = c(f)c(q)$, and $c(f)c(q) = c(fq) = c(g) \in A$, and so $q \in A[X]$. Therefore f divides g in $A[X]$.

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

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

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

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

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

THEOREM 4.10. *The ring $k[X_1, \ldots, X_n]$ is a unique factorization domain.*

PROOF. Note that

$$A[X_1,\ldots,X_n] = A[X_1,\ldots,X_{n-1}][X_n]. \tag{7}$$

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

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

The theorem is trivially true when $n=0$, and (7) allows us to deduce it from (4.9) for all n.

COROLLARY 4.11. *A nonzero proper principal ideal (f) in $k[X_1,\ldots,X_n]$ is prime if and only f is irreducible.*

PROOF. Special case of Proposition 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:

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

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

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

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

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

If S contains no zero-divisors, for example, if A is an integral domain and $0\notin S$, then i_S is injective. 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 every other ring homomorphism $\alpha\colon A\to B$ with this property factors uniquely through i_S

$$\begin{tikzcd} A \arrow[r, "i_S"] \arrow[dr, "\alpha"'] & S^{-1}A \arrow[d, dashed, "\exists!"] \\ & B. \end{tikzcd}$$

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

$$\begin{aligned} \tfrac{a}{s} = \tfrac{b}{t} &\implies u(at - bs) = 0 \text{ some } u \in S \\ &\implies \alpha(a)\alpha(t) - \alpha(b)\alpha(s) = 0 \quad \text{because } \alpha(u) \in B^{\times}, \end{aligned}$$

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

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

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

EXAMPLE 5.2. Let $h \in A$. Then $S_h = \{1, h, h^2, \ldots\}$ is a multiplicative subset of A, and we let $A_h = S_h^{-1}A$. Thus every element of A_h can be written in the form a/h^m, $a \in A$, and

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

If h is nilpotent, then $A_h = 0$, and if A is an integral domain with field of fractions F and $h \neq 0$, then A_h is the subring of F of elements 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 $\alpha: A \to B$ be a homomorphism of rings such that $\alpha(h)$ is a unit in B. The homomorphism

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

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.

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

Let S be a multiplicative subset of a ring A and $S^{-1}A$ 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*

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

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 $\bar{S}$ be the image of S in $A/\mathfrak{p}$. Then $(S^{-1}A)/\mathfrak{p}^e \simeq \bar{S}^{-1}(A/\mathfrak{p})$ because $S^{-1}A/\mathfrak{p}^e$ has the correct universal property, and $\bar{S}^{-1}(A/\mathfrak{p})$ is an integral domain because $A/\mathfrak{p}$ is an integral domain and $\bar{S}$ doesn't contain 0. Therefore $\mathfrak{p}^e$ is prime. From (2.12) 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 every multiplicative set S.*

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

Let $\operatorname{spec}(A)$ denote the set of prime ideals in A. Then Proposition 5.4 says that

$$\operatorname{spec}(S^{-1}A) \simeq \{\mathfrak{p} \in \operatorname{spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}.$$

PROPOSITION 5.6. *Let $\varphi \colon A \to B$ 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. Suppose $\mathfrak{p} = \mathfrak{q}^c$ with $\mathfrak{q}$ prime. Then $\mathfrak{p}^{ec} = \mathfrak{q}^{cec} \overset{2.12}{=} \mathfrak{q}^c = \mathfrak{p}$. 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 disjoint from $\mathfrak{p}^e$. It is a multiplicative subset of B, and so there exists a prime ideal $\mathfrak{q}$ in B containing $\mathfrak{p}^e$ and disjoint from $\varphi(S)$ (apply 2.2). 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 $S_{\mathfrak{p}} \overset{\text{def}}{=} A \smallsetminus \mathfrak{p}$ is a multiplicative subset of A, and we let $A_{\mathfrak{p}} = S_{\mathfrak{p}}^{-1}A$. Thus each element of $A_{\mathfrak{p}}$ can be written in the form $\frac{a}{c}$, $c \notin \mathfrak{p}$, and

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

A prime ideal is disjoint from $S_{\mathfrak{p}}$ if and only if it is contained $\mathfrak{p}$, and so

$$\operatorname{spec}(A_{\mathfrak{p}}) \simeq \{\mathfrak{q} \in \operatorname{spec}(A) \mid \mathfrak{q} \subset \mathfrak{p}\}.$$

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*

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

is an isomorphism. Moreover, it induces isomorphisms

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

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

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

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

We consider extension and contraction with respect to $a \mapsto \frac{a}{1} \colon A \to A_{\mathfrak{m}}$. Note that $\mathfrak{n}^n = (\mathfrak{m}^n)^e$, and so the kernel of $A/\mathfrak{m}^n \to A_{\mathfrak{m}}/\mathfrak{n}^n$ is $(\mathfrak{m}^n)^{ec}/\mathfrak{m}^n$. Let $a \in (\mathfrak{m}^n)^{ec}$. Then $\frac{a}{1} = \frac{b}{s}$ with $b \in \mathfrak{m}^n$ and $s \in S$, and so $tsa \in \mathfrak{m}^n$ for some $t \in S$. Therefore $tsa = 0$ in $A/\mathfrak{m}^n$. Every maximal ideal of A containing $\mathfrak{m}$ contains $\operatorname{rad}(\mathfrak{m}^n) = \mathfrak{m}$, and so equals $\mathfrak{m}$. Therefore the only maximal ideal in $A/\mathfrak{m}^n$ is $\mathfrak{m}/\mathfrak{m}^n$. But ts is not in $\mathfrak{m}/\mathfrak{m}^n$, and so it must be a unit in $A/\mathfrak{m}^n$. Therefore $a = 0$ in $A/\mathfrak{m}^n$, which means that $a \in \mathfrak{m}^n$. We deduce that $A/\mathfrak{m}^n \to A_{\mathfrak{m}}/\mathfrak{n}^n$ is injective.

It remains to prove that $A \to A_{\mathfrak{m}}/\mathfrak{n}^n$ is surjective. Let $\frac{a}{s} \in A_{\mathfrak{m}}$, $a \in A$, $s \in A \smallsetminus \mathfrak{m}$. As we just showed, 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

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

On passing to $A_{\mathfrak{m}}$ and multiplying by s^{-1}, we find that

$$\tfrac{ba}{1} = \tfrac{a}{s} - \tfrac{aq}{s}.$$

As $\frac{aq}{s} \in \mathfrak{n}^n$, this shows that $\frac{a}{s}$ mod $\mathfrak{n}^n$ is in the image of $A \to A_{\mathfrak{m}}/\mathfrak{n}^n$.

PROPOSITION 5.9. *In a noetherian ring A, only 0 lies in all powers of all maximal ideals:*

$$\bigcap\{\mathfrak{m}^n \mid \mathfrak{m} \textit{ maximal}, n \in \mathbb{N}\} = \{0\}.$$

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 3.16), 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:

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

It is easily 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 $m \mapsto \frac{m}{1} \colon M \xrightarrow{i_S} S^{-1}M$ 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:*

the elements of S act invertibly on $S^{-1}M$, and every homomorphism $M \to N$ from M to an A-module N on which the elements of S act invertibly factors uniquely through i_S

$$\begin{tikzcd} M \arrow[r, "i_S"] \arrow[dr] & S^{-1}M \arrow[d, dashed, "\exists!"] \\ & N. \end{tikzcd}$$

PROOF. Similar to that of Proposition 5.1.

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

$$\begin{tikzcd} M \arrow[r, "i_S"] \arrow[d, "\alpha"] & S^{-1}M \arrow[d, "S^{-1}\alpha"] \\ N \arrow[r, "i_S"] & S^{-1}N. \end{tikzcd}$$

In other words, $S^{-1}\alpha$ is the unique homomorphism of $S^{-1}A$-modules $S^{-1}M \to S^{-1}N$ such that

$$(S^{-1}\alpha)(\tfrac{m}{s}) = \frac{\alpha(m)}{s}, \quad m \in M,$$

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

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

EXAMPLE 5.12. Let M be an A-module. For $h\in A$, let $M_h=S_h^{-1}M$ where $S_h=\{1,h,h^2,\ldots\}$. Then every element of M_h can be written in the form $\frac{m}{h^r}$, $m\in M$, $r\in\mathbb{N}$, and $\frac{m}{h^r}=\frac{m'}{h^{r'}}$ if and only if $h^N(h^{r'}m-h^rm')=0$ for some $N\in\mathbb{N}$.

PROPOSITION 5.13. *Let M be a finitely generated A-module. If $S^{-1}M=0$, then there exists an $h\in S$ such that $M_h=0$.*

PROOF. To say that $S^{-1}M=0$ means that, for each $x\in M$, there exists an $s_x\in S$ such that $s_xx=0$. Let $x_1,\ldots,x_n$ generate M. Then $h\overset{\text{def}}{=}s_{x_1}\cdots s_{x_n}$ lies in S and has the property that $hM=0$. Therefore $M_h=0$.

PROPOSITION 5.14. *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 2.3), and so it contains 1. Now $m=1m=0$.

COROLLARY 5.15. *An A-module $M=0$ if $M_{\mathfrak{m}}=0$ for all maximal ideals $\mathfrak{m}$.*

PROOF. Immediate consequence of the lemma.

PROPOSITION 5.16. *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 Proposition 5.11. For the sufficiency, let $N=\mathrm{Ker}(\beta)/\mathrm{Im}(\alpha)$. Because the functor $M\rightsquigarrow M_{\mathfrak{m}}$ is exact,

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

If (11) is exact for all $\mathfrak{m}$, then $N_{\mathfrak{m}}=0$ for all $\mathfrak{m}$, and so $N=0$ (by 5.15). But this means that (10) is exact.

COROLLARY 5.17. *A homomorphism $M\to N$ of A-modules is injective (resp. surjective, zero) if and only if $M_{\mathfrak{m}}\to N_{\mathfrak{m}}$ is injective (resp. surjective, zero) for all maximal ideals $\mathfrak{m}$.*

PROOF. Apply the proposition to $0 \to M \to N$ (resp. $M \to N \to 0$, $M \xrightarrow{\mathrm{id}} M \to N$).

PROPOSITION 5.18. *Let $\mathfrak{N}$ be the nilradical of A. For every multiplicative subset S of A, $S^{-1}\mathfrak{N}$ is the nilradical of $S^{-1}A$.*

PROOF. Let $a \in A$ and $s \in S$. If $(\frac{a}{s})^n = 0$, then $ta^n = 0$ for some $t \in S$, and so $\frac{a}{s} = \frac{ta}{ts} \in S^{-1}\mathfrak{N}$. Conversely, if $a \in \mathfrak{N}$, then clearly $\frac{a}{s}$ is in the nilradical of $S^{-1}A$.

COROLLARY 5.19. *A ring A is reduced if and only if $A_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$ in A.*

PROOF. Combine Proposition 5.18 with Corollary 5.15.

EXAMPLE 5.20. Let $\mathfrak{p}$ be a prime ideal in a ring A. When we apply Proposition 5.11 to the exact sequence

$$0 \to \mathfrak{p} \to A \to A/\mathfrak{p} \to 0$$

with $S = S_{\mathfrak{p}}$, we obtain an isomorphism

$$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq \kappa(\mathfrak{p})$$

where $\kappa(\mathfrak{p})$ is the field of fractions of $A/\mathfrak{p}$.

Exercises

EXERCISE 5.21. (Bourbaki AC, II, §2, Exercise 1.) 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 every A-module M, the canonical homomorphism $S^{-1}M \to \widetilde{S}^{-1}M$ is bijective. In particular, $S^{-1}A \simeq \widetilde{S}^{-1}A$.

EXERCISE 5.22. Let $A \to B$ be a homomorphism of rings, and let $\mathfrak{p}$ be a prime ideal of A. Show that the prime ideals of B lying over $\mathfrak{p}$ are in natural one-to-one correspondence with the prime ideals of $B \otimes_A \kappa(\mathfrak{p})$.

EXERCISE 5.23. Show that a ring A is reduced if and only if it can be realized as a subring of a product of fields. (Hint: Consider the map $A \to \prod_{\mathfrak{p}} \kappa(\mathfrak{p})$ where $\mathfrak{p}$ runs over the minimal prime ideals of A.)

6 Integral dependence

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

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

More generally, an element of an A-algebra B is ***integral*** over A if it is integral over the image of A in B. 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 a variant of Cramer's rule. We define the determinant of an $m \times m$ matrix $C = (c_{ij})$ with coefficients c_{ij} in a ring A by the usual formula

$$\det(C) = \sum_{\sigma \in S_m} \operatorname{sign}(\sigma) c_{1\sigma(1)} \cdots c_{m\sigma(m)}.$$

Clearly, $\det(C)$ is linear in each column, and $\det(C) = 0$ if two columns are equal because then each term occurs twice but with opposite signs. If $x_1, \ldots, x_m$ is a solution to the system of linear equations

$$\sum_{j=1}^{m} c_{ij} x_j = 0, \quad i = 1, \ldots, m,$$

with coefficients in a ring A, then

$$\det(C) \cdot x_j = 0, \quad j = 1, \ldots, m, \tag{12}$$

where C is the matrix of coefficients. To prove this, expand out the left hand side of

$$\det \begin{pmatrix} c_{11} & \ldots & c_{1\,j-1} & \sum_i c_{1i} x_i & c_{1\,j+1} & \ldots & c_{1m} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ c_{m1} & \ldots & c_{m\,j-1} & \sum_i c_{mi} x_i & c_{m\,j+1} & \ldots & c_{mm} \end{pmatrix} = 0$$

using the properties of determinants mentioned above.

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 $A[\alpha]$-submodule 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, α, ..., α^{n-1} has the property that $\alpha M \subset M$, and it is faithful because it contains 1.

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

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

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

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 rule (12) 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 $\det(C)$, we obtain an equation

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

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.*

PROOF. We may replace A with its image in B. Suppose that $B = A[\alpha_1, \ldots, \alpha_m]$ and that

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

Every monomial in the α_i 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 (6.2).

$\Rightarrow$: We may replace A with its image in B. Then B is a faithful $A[\alpha]$-module for all $\alpha \in B$ (because $1_B \in B$), 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.

PROPOSITION 6.4. *Consider rings $A \subset B \subset C$. If B is integral over A and C is integral over B, then C is integral over A.*

PROOF. Let $\gamma \in C$. Then

$$\gamma^n + b_1\gamma^{n-1} + \cdots + b_n = 0$$

for some $b_i \in B$. Now $A[b_1, \ldots, b_n]$ is finite over A (see 6.2), and $A[b_1, \ldots, b_n][\gamma]$ is finite over $A[b_1, \ldots, b_n]$, and so it is finite over A. Therefore γ is integral over A by (6.1).

THEOREM 6.5. *Let A be a subring of a ring B. The elements of B integral over A form an A-subalgebra 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 6.6. 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. When A is an integral domain, the integral closure of A in its field of fractions is called the ***integral closure*** of A (tout court).

PROPOSITION 6.7. *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 nonzero $d \in A$ such that $d\alpha$ is integral over A.*

PROOF. By assumption, α satisfies an equation

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

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

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

We can rewrite this as

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

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

COROLLARY 6.8. *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 6.9. 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 6.10. *Every unique factorization domain is integrally closed.*

PROOF. Let A be a unique factorization domain. 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 prime 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 (as A is a unique factorization domain).

Let $F \subset E$ be fields, and let $\alpha \in E$ be algebraic over F. The ***minimum polynomial*** of α over F is the monic polynomial in $F[X]$ of smallest degree having α as a root. Then f is the (unique) monic generator of the kernel of the homomorphism $X \mapsto \alpha \colon F[X] \to F[\alpha]$, and so this map defines an isomorphism $F[X]/(f) \to F[\alpha]$, i.e.,

$$F[x] \simeq F[\alpha], \quad x \leftrightarrow \alpha.$$

A ***conjugate*** of α is an element α' in some field containing F such that $f(\alpha') = 0$. Then f is the minimum polynomial of α' over F, and so there is an isomorphism

$$F[\alpha] \simeq F[\alpha'], \quad \alpha \leftrightarrow \alpha'.$$

PROPOSITION 6.11. *Let A be a normal integral domain and E 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 f be the minimum polynomial of α over F, and let L a field containing F and splitting f. For every conjugate α' of α in L, there is an isomorphism $\sigma\colon F[\alpha] \to F[\alpha']$ sending α to α'. On applying σ to the above equation we obtain an equation

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

demonstrating that α' is integral over A. As the coefficients of f are polynomials in the conjugates of α in L, it follows from Theorem 6.5 that the coefficients of f are integral over A. They lie in F, and A is integrally closed in F, and so they lie in A. This proves the "only if" part of the statement, and the "if" part is obvious.

COROLLARY 6.12. *Let A be a normal integral domain with field of fractions F, and let f be a monic polynomial in $A[X]$. Then every monic factor of f 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 over F. As α is a root of f, it is integral over A, and so g has coefficients in A.

We shall need a more general form of Corollary 6.12.

LEMMA 6.13. *Let A be a ring and B an A-algebra. Let $f, g \in B[T]$ be monic polynomials such that g divides f. If the coefficients of f are integral over A, then so also are those of g.*

PROOF. There exists a ring B' containing B such that f splits in $B'[T]$. This can be constructed in the same as way as the splitting field of a polynomial over a field.[12] The roots of f in B' are integral over the A-subalgebra of B generated by the coefficients of f, and hence over A (see 6.4). As the roots of g are also roots of f, they are integral over A. The coefficients of g are polynomials in its roots, and hence are integral over A (see 6.5).

PROPOSITION 6.14. *Let $A \subset B$ be rings, and let A' be the integral closure of A in B. For every 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

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

[12] If $\deg(f) \leq 1$, we take $B' = B$. Otherwise, let $B_1 = B[T]/(f)$. As f is monic, $\deg(fg) = \deg(f) + \deg(g)$ for any polynomial $g \in B[T]$, and so $(f) \cap B = \{0\}$. Therefore the map $B \to B_1$ is injective. On the other hand, f has a root $b = T \bmod (f)$ in B_1, and so $f = (T - b) f_1$ in $B_1[T]$ with f_1 monic. If $\deg(f_1) > 1$, apply the same argument to it and B_1. Continuing in this fashion, we eventually arrive at the required ring B'.

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

For the converse, let b/s ($b \in B$, $s \in S$) be integral over $S^{-1}A$. 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 $s^n s_1^n \cdots s_n^n$, we find that $s_1 \cdots s_n b \in A'$, and therefore that $b/s = s_1 \cdots s_n b/ss_1 \cdots s_n \in S^{-1}A'$.

COROLLARY 6.15. *Let $A \subset B$ be rings and S 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 6.16. *The following conditions on an integral domain A are equivalent:*
(a) *A is integrally closed;*
(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 (6.15), 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 6.14). If (c) holds, then $A_{\mathfrak{m}} \to (A')_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ in A, which implies that $A \to A'$ is surjective (by 5.17), and so A is integrally closed.

We shall need to use the next statement in the proof of Zariski's main theorem (Chapter 17).

PROPOSITION 6.17. *Every polynomial ring over a normal integral domain is a normal integral domain.*

PROOF. It suffices to prove that if A is a normal integral domain, then $A[T]$ is a normal integral domain. Let F be the field of fractions of A. If an element of the field of fractions $F(T)$ of $A[T]$ is integral over $A[T]$, then it is integral over $F[T]$, and so lies in $F[T]$ (see 6.10). We can now apply the next proposition with $B = F$.

PROPOSITION 6.18. *Let B be an A-algebra. If a polynomial in $B[T]$ is integral over $A[T]$, then each of its coefficients is integral over A.*

PROOF. We may replace A with its image in B. Suppose that $P \in B[T]$ is a root of the polynomial

$$q(X) = X^n + f_1 X^{n-1} + \cdots + f_n, \quad f_i \in A[T].$$

Let r be greater than the degrees of the polynomials $P, f_1, \ldots, f_n$. Let $P_1(T) = P(T) - T^r$, and let

$$q_1(X) \stackrel{\text{def}}{=} q(X + T^r) = X^n + g_1 X^{n-1} + \cdots + g_n, \quad g_i \in A[T].$$

Then P_1 is a root of $q_1(X)$,

$$P_1^n + g_1 P_1^{n-1} + \cdots + g_n = 0,$$

and so

$$g_n = -P_1 \cdot (P_1^{n-1} + g_1 P_1^{n-2} + \cdots + g_{n-1}).$$

The choice of r implies that both P_1 and g_n are monic (as polynomials in T). As g_n has coefficients in A, Lemma 6.13 shows that the coefficients of P_1 are integral over A. This implies that the coefficients of P are integral over A.

Exercises

EXERCISE 6.19. 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.

EXERCISE 6.20. Prove the converse of Proposition 6.18.

EXERCISE 6.21. Let A be an integral domain and A' its integral closure. Show that the integral closure of $A[T]$ is $A'[T]$.

7 The going-up and going-down theorems

The going-up theorem

PROPOSITION 7.1. *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. 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

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

REMARK 7.2. The second part of the proof shows that $A \cap B^{\times} = A^{\times}$.

COROLLARY 7.3. *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 7.4 (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 $\mathfrak{q} = \mathfrak{q}'$.*

In other words, if $B \supset A$ is integral over A, then there is no containment relation between the prime ideals of B lying over a given prime ideal of A.

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 7.3). Now

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

PROPOSITION 7.5. *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 2.3), and let $\mathfrak{q}$ be the inverse image of $\mathfrak{n}$ in B. We claim that $\mathfrak{q} \cap A = \mathfrak{p}$.

The ideal $\mathfrak{n} \cap A_\mathfrak{p}$ is maximal (7.3), but $\mathfrak{p}A_\mathfrak{p}$ is the unique maximal ideal of $A_\mathfrak{p}$, and so $\mathfrak{n} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$. From the commutative diagram

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

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

THEOREM 7.6. *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 $\mathfrak{q}' \cap A = \mathfrak{p}'$:*

$$\begin{array}{ccccc} B & \quad & \mathfrak{q} & \subset & \mathfrak{q}' \\ | & & | & & | \\ A & & \mathfrak{p} & \subset & \mathfrak{p}'. \end{array}$$

PROOF. We have $A/\mathfrak{p} \subset B/\mathfrak{q}$, and $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. According to the (7.5), 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 7.7. *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* $i \leq n$*:*

$$\begin{array}{ccccccccc}
\mathfrak{q}_1 & \subset & \cdots & \subset & \mathfrak{q}_m & \subset & \cdots & \subset & \mathfrak{q}_n \\
| & & & & | & & & & | \\
\mathfrak{p}_1 & \subset & \cdots & \subset & \mathfrak{p}_m & \subset & \cdots & \subset & \mathfrak{p}_n
\end{array}$$

PROOF. Immediate consequence of Corollary 7.6.

Theorem 7.6 and its corollary 7.7 are known as the ***going-up theorem*** (of Cohen and Seidenberg).

ASIDE 7.8. The going-up theorem (7.6) fails for the rings $\mathbb{Z} \subset \mathbb{Z}[X]$: consider the prime ideals $(0) \subset (2)$ of $\mathbb{Z}$, and the prime ideal $\mathfrak{q} = (1+2X)$ of $\mathbb{Z}[X]$; then $\mathfrak{q} \cap \mathbb{Z} = (0)$, but a prime ideal $\mathfrak{q}'$ of $\mathbb{Z}[X]$ containing $\mathfrak{q}$ and such that $\mathfrak{q}' \cap \mathbb{Z} = (2)$ would have to contain $(2, 1+2X) = \mathbb{Z}[X]$ (mo159544).

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, finitely generated as an A-module, such that $bM \subset \mathfrak{a}M$.

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 7.9. *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 $b^n M \subset \mathfrak{a}M$, 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 7.10. *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 Proposition 6.11, 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 7.9).

THEOREM 7.11. *Let $A \subset B$ be integral domains with A normal and B integral over A. Let $\mathfrak{p} \supset \mathfrak{p}'$ be prime ideals in A, and let $\mathfrak{q}$ be a prime ideal in B such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then $\mathfrak{q}$ contains a prime ideal $\mathfrak{q}'$ in B such that $\mathfrak{q}' \cap A = \mathfrak{p}'$:*

$$\begin{array}{ccccc} B & \qquad & \mathfrak{q} & \supset & \mathfrak{q}' \\ \Big| & & \Big| & & \Big| \\ A & & \mathfrak{p} & \supset & \mathfrak{p}'. \end{array}$$

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 (7.9), y is integral over $\mathfrak{p}'$, and so (by 7.10) 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 s is integral over A, and so (by 6.11), 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 7.12. *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:

$$\begin{array}{ccccccccc} \mathfrak{q}_1 & \supset & \cdots & \supset & \mathfrak{q}_m & \supset & \cdots & \supset & \mathfrak{q}_n \\ \Big| & & & & \Big| & & & & \Big| \\ \mathfrak{p}_1 & \supset & \cdots & \supset & \mathfrak{p}_m & \supset & \cdots & \supset & \mathfrak{p}_n \end{array}$$

PROOF. Immediate consequence of the theorem.

Theorem 7.11 and its corollary 7.12 are known as the ***going-down theorem*** (of Cohen and Seidenberg). The going-down theorem also holds for flat A-algebras — see (11.20).

8 Noether's normalization theorem

THEOREM 8.1 (NOETHER NORMALIZATION THEOREM). *Every finitely generated algebra A over a field k contains a polynomial algebra R such that A is a finite R-algebra.*

In other words, there exist elements $y_1,\ldots,y_r$ of A that are algebraically independent over k and such that A is finite over $k[y_1,\ldots,y_r]$.

Let $A=k[x_1,\ldots,x_n]$. If the x_i are algebraically independent, then there is nothing to prove. Otherwise, the next lemma shows that A is finite over a subring $k[x_1',\ldots,x_{n-1}']$. Continuing in this fashion, we arrive at a proof.

LEMMA 8.2. *Let $A=k[x_1,\ldots,x_n]$ be a finitely generated k-algebra, and let $\{x_1,\ldots,x_d\}$ be a maximal algebraically independent subset of $\{x_1,\ldots,x_n\}$. If $n>d$, then there exist an $m\in\mathbb{N}$ such that A is finite over its subalgebra $k[x_1-x_n^m,\ldots,x_d-x_n^{m^d},x_{d+1},\ldots,x_{n-1}]$.*

PROOF. By assumption, the set $\{x_1,\ldots,x_d,x_n\}$ is algebraically dependent, and so there exists a nonzero $f\in k[X_1,\ldots,X_d,T]$ such that

$$f(x_1,\ldots,x_d,x_n)=0. \tag{18}$$

Because the set $\{x_1,\ldots,x_d\}$ is algebraically independent, T occurs in f, and so we can write

$$f(X_1,\ldots,X_d,T)=a_0T^r+a_1T^{r-1}+\cdots+a_r$$

with $a_i\in k[X_1,\ldots,X_d]$, $a_0\neq 0$, and $r>0$.

If $a_0\in k$, then (18) shows that x_n is integral over $k[x_1,\ldots,x_d]$. Hence $x_1,\ldots,x_n$ are integral over $k[x_1,\ldots,x_{n-1}]$, and so A is finite over $k[x_1,\ldots,x_{n-1}]$ (see 6.3). Thus the lemma holds with $m=0$.

If $a_0\notin k$, then we make a change of variables so that it becomes constant. Specifically, for a suitable $m\in\mathbb{N}$, the polynomial

$$g(X_1,\ldots,X_d,T)\stackrel{\text{def}}{=}f(X_1+T^m,X_2+T^{m^2},\ldots,X_d+T^{m^d},T)$$

takes the form

$$g(X_1,\ldots,X_d,T)=c_0T^r+c_1T^{r-1}+\cdots+c_r$$

with $c_0\in k^\times$ (see the next lemma). As

$$g(x_1-x_n^m,\ldots,x_d-x_n^{m^d},x_n)=0, \tag{19}$$

this shows that x_n is integral over $k[x_1-x_n^m,\ldots,x_d-x_n^{m^d}]$. The elements x_i, $i\leq d$, are too, because $x_i=(x_i-x_n^m)+x_n^m$, and so A is finite over $k[x_1-x_n^m,\ldots,x_d-x_n^{m^d},x_{d+1},\ldots,x_{n-1}]$.

LEMMA 8.3. *Let $f\in k[X_1,\ldots,X_d,T]$. For a suitable $m\in\mathbb{N}$,*

$$f(X_1+T^m,X_2+T^{m^2},\ldots,X_d+T^{m^d},T)$$

takes the form $c_0T^r+c_1T^{r-1}+\cdots+c_r$ with $c_0\in k^\times$.

PROOF. Let
$$f(X_1,\dots,X_d,T) = \sum c_{j_1\cdots j_n} X_1^{j_1}\cdots X_d^{j_d} T_n^{j_n}. \tag{20}$$
Let S be the set of $(d+1)$-tuples $(j_1,\dots,j_d,j_n)$ such that $c_{j_1\dots j_n} \neq 0$, and choose m so that $m > \max_i j_i$ for all $(j_1,\dots,j_d) \in S$. Note that
$$\begin{aligned}(X_1+T^m)^{j_1}\cdots(X_d+T^{m^d})^{j_d} T_n^{j_n} \\ = T^{mj_1+m^2j_2+\cdots+m^d j_d+j_n} + \text{terms of lower degree in } T.\end{aligned}$$
When $(j_1,\dots,j_n)$ runs over the elements of S, the exponents
$$mj_1 + m^2 j_2 + \cdots + m^d j_d + j_n \tag{21}$$
are distinct, because they are distinct base-m expansions of natural numbers. Now
$$g(X_1,\dots,X_d,T) = c_0 T_1^N + c_1 T_1^{N-1} + \cdots$$
with $c_0 \in k^\times$ and N equal to the largest value of (21).

REMARK 8.4. When k is infinite, it is possible to prove 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 my Algebraic Geometry notes.

ASIDE 8.5. The map $k[y_1,\dots,y_r] \to A$ in (8.1) is flat if and only if A is Cohen-Macaulay (for example, regular). See (23.10).

Let X be the variety obtained by removing the origin from $\mathbb{C}^2$ and identifying the points $(1,1)$ and $(-1,-1)$. Then $G = \mathbb{Z}/2$ acts on by $(x,y) \mapsto (-x,-y)$ and the quotient is smooth, but X is not Cohen-Macaulay (two planes intersecting in a point is not Cohen-Macaulay). Therefore the quotient map. See mo173538.

9 Direct and inverse limits

Direct limits

DEFINITION 9.1. 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 9.2. Let $(I,\leq)$ be a directed set, and let A be a ring.

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

$$\begin{tikzcd} & & M_k \\ M_i \arrow[rru, "\alpha^i_k"] \arrow[r, "\alpha^i_j"'] & M_j \arrow[ru, "\alpha^j_k"'] & \end{tikzcd}$$

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

$$\begin{tikzcd} & & M \arrow[dd, dashed, "\alpha"] \\ M_i \arrow[rru, bend left, "\alpha^i"] \arrow[r, "\alpha^i_j"] \arrow[rrd, bend right, "\beta^i"'] & M_j \arrow[ru, "\alpha^j"] \arrow[rd, "\beta^j"'] & \\ & & N \end{tikzcd}$$

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 $\alpha^i \colon M_i \to M$ such that $\alpha^i = \alpha^j \circ \alpha_j^i$ for all $i \le j$ 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) if $m_i \in M_i$ maps to zero in M, then it maps to zero in M_j for some $j \ge i$.

CONSTRUCTION

Consider the direct sum $\bigoplus_{i \in I} M_i$ of the modules M_i. Thus, the elements of $\bigoplus_{i \in I} M_i$ are the families $(m_i)_{i \in I}$ with $m_i = 0$ for all but finitely many i. We can identify M_{i_0} with the submodule of $\bigoplus_{i \in I} M_i$ of elements $(m_i)_i$ with $m_i = 0$ for $i \ne i_0$. Then every element of $\bigoplus_{i \in I} M_i$ is a finite sum $\sum_{i \in I} m_i$ with $m_i \in M_i$. Let M be the quotient of $\bigoplus_{i \in I} M_i$ by the A-submodule M' generated by the elements

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

Let $\alpha^i(m_i) = m_i + M'$. Then certainly $\alpha^i = \alpha^j \circ \alpha_j^i$ for all $i \le j$. For every A-module N and A-linear maps $\beta^j \colon M_j \to N$, 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 9.3. *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. An element h of a ring that divides a unit is itself a unit (if $u = hq$, then $1 = h(qu^{-1})$). Therefore, if $h|h'$ in A, say, $h' = hq$, then h becomes a unit in $A_{h'}$, and so (see 5.1) there is a unique homomorphism $A_h \to A_{h'}$ respecting the maps $A \to A_h$ and $A \to A_{h'}$, namely, $\frac{a}{h} \mapsto \frac{ag}{h'}$. In this way, 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 $\frac{a}{h} \mapsto \frac{a}{h} \colon A_h \to S^{-1}A$, and these homomorphisms are compatible with the maps in the direct system (apply 5.1 again). The criterion p. 36 shows that $S^{-1}A$ is the direct limit of the A_h.

EXACTNESS

PROPOSITION 9.4. *The direct limit of a system of exact sequences of modules is exact.*

This means the following: suppose that (M_i, α^i_j), (N_i, β^i_j), and (P_i, γ^i_j) are direct systems with repect to the directed set I, and let

$$(M_i, \alpha^i_j) \xrightarrow{(a_i)} (N_i, \beta^i_j) \xrightarrow{(b_i)} (P_i, \gamma^i_j)$$

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

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

are exact for all i, then the direct limit sequence

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

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 of M_i such that $a_i(m_i) = n_i$. Then (m_i) maps to (n_i). This proves the exactness.

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. In this case, 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 A-module homomorphism

$$(\ldots, m_n, \ldots) \mapsto (\ldots, m_n - \alpha_n(m_{n+1}), \ldots) \colon \prod M_n \to \prod M_n.$$

PROPOSITION 9.5. *For every inverse system (M_n, α_n) and A-module N,*

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

PROOF. This is easy to check directly.

PROPOSITION 9.6. *Every inverse system of exact sequences*

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

gives rise to 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 9.7. *If the maps $\alpha_n : M_{n+1} \to M_n$ are all surjective, then $\varprojlim^1 M_n = 0$.*

PROOF. Let $(m_i) \in \prod_{i\in\mathbb{N}} M_i$. We have show that there exists an infinite sequence $(x_i)_{i\in\mathbb{N}}$, $x_i \in M_i$, such that

$$x_i - \alpha_i(x_{i+1}) = m_i \tag{22}$$

for all $i \in \mathbb{N}$. We consider finite sequences $\{x_0,\ldots,x_n\}$, $x_i \in M_i$, satisfying (22) for $i < n$. For example, $\{0\}$ is such a sequence. Such a sequence $\{x_0,\ldots,x_n\}$ can always be extended: use the surjectivity of α_{n+1} to find an $x_{n+1} \in M_{n+1}$ such that

$$\alpha_n(x_{n+1}) = x_n - m_n.$$

Now the axiom of dependent choice shows that there exists a sequence $(x_i)_{n\in\mathbb{N}}$, $x_i \in M_i$, satisfying (22) for all n.

ASIDE 9.8. Direct (resp. inverse) limits are also called inductive (resp. projective) limits or colimits (resp. limits).

10 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

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

$$\begin{tikzcd} M \times N \arrow[r, "\phi"] \arrow[dr, "\phi'"'] & T \arrow[d, dashed, "\exists!\text{ linear}"] \\ & T'. \end{tikzcd}$$

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

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

is A-bilinear — we have imposed the fewest relations necessary to ensure this. Every element of $M\otimes_A N$ can be written as a finite sum[13]

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

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 every bilinear map $\phi'\colon M\times N\to T'$ defines an A-linear map $A^{(M\times N)}\to T'$, which factors through $A^{(M\times N)}/K$, and gives a commutative triangle.

SYMMETRIC MONOIDAL STRUCTURE

PROPOSITION 10.1. *Let M,N,P be modules over a ring A.*

(a) *(Existence of an identity object) There is a unique isomorphism*

$$\lambda\colon A\otimes M\to M$$

such that $\lambda(a\otimes m)=am$ for all $a\in A$, $m\in M$.

(b) *(Associativity) There is a unique isomorphism*

$$\alpha\colon M\otimes(N\otimes P)\to(M\otimes N)\otimes P$$

such that $\alpha(m\otimes(n\otimes p))=\alpha((m\otimes n)\otimes p)$ for all $m\in M$, $n\in N$, $p\in P$.

[13] "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.

(c) *(Symmetry) There is a unique isomorphism*

$$\gamma\colon M\otimes N\to N\otimes M$$

such that $\gamma(m\otimes n)=n\otimes m$ *for all* $m\in M$, $n\in N$.

PROOF. We prove (b). The uniqueness is obvious because the elements $m\otimes(n\otimes p)$ generate $M\otimes(N\otimes P)$ as an A-module. The map

$$(m,n,p)\mapsto m\otimes(n\otimes p)\colon M\times N\times P\to M\otimes(N\otimes P) \tag{23}$$

is A-trilinear. Let $\beta\colon M\times N\times P\to Q$ be a second A-trilinear map. For a fixed $m\in M$, the map $(n,p)\to\beta(m,n,p)\colon N\times P\to Q$ is A-bilinear, and so it extends uniquely to an A-linear map $\beta_m\colon N\otimes P\to Q$. Now the map $(m,n\otimes p)\mapsto\beta_m(n\otimes p)\colon M\times(N\otimes P)\to Q$ is A-bilinear, and so it extends uniquely to an A-linear map $M\otimes(N\otimes P)\to Q$. This shows that (23) is universal among A-trilinear maps from $M\times N\times P$ to an A-module. Similarly, the A-trilinear map

$$(m,n,p)\mapsto(m\otimes n)\otimes p\colon M\times N\times P\to(M\otimes N)\otimes P$$

is universal, from which the statement follows (see the footnote p.19).

The proofs of (a) and (c) are similar, but easier.

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 $\alpha\colon M\to N$ defines a B-linear map $\beta\colon B\otimes_A M\to N$ such that $b\otimes m\mapsto b\cdot\alpha(m)$, and $\alpha\leftrightarrow\beta$ is an isomorphism:

$$\mathrm{Hom}_{A\text{-linear}}(M,N)\simeq\mathrm{Hom}_{B\text{-linear}}(B\otimes_A M,N). \tag{24}$$

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.

The functor $M\rightsquigarrow M_B\overset{\text{def}}{=}B\otimes_A M$ commutes with taking tensor products:

$$(M\otimes_A N)_B\simeq M_B\otimes_B N_B. \tag{25}$$

To see this, note that

$$\begin{aligned}
M_B\otimes_B N_B &= (B\otimes_A M)\otimes_B(B\otimes_A N) \quad \text{(definition)}\\
&\simeq ((B\otimes_A M)\otimes_B B)\otimes_A N \quad \text{(associativity)}\\
&\simeq (B\otimes_A M)\otimes_A N \quad \text{(obvious)}\\
&\simeq B\otimes_A(M\otimes_A N) \quad \text{(associativity)}\\
&= (M\otimes_A N)_B \quad \text{(definition).}
\end{aligned}$$

BEHAVIOUR WITH RESPECT TO DIRECT LIMITS

PROPOSITION 10.2. *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:

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 $(f,g) \circ j = \beta$,

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr, "f"'] & C \arrow[d, dashed, "(f,g)", "\exists!"'] & B \arrow[l, "j"'] \arrow[dl, "g"] \\ & R & \end{tikzcd}$$

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

$$\mathrm{Hom}(A \otimes_k B, R) \simeq \mathrm{Hom}(A, R) \times \mathrm{Hom}(B, R) \tag{26}$$

(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 10.3. 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 10.4. The ring $k[X_1, \ldots, X_m, X_{m+1}, \ldots, X_{m+n}]$, together with the obvious inclusions

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

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

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

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

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

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

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

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

REMARK 10.5. (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 $TM \to R$.

$$\begin{tikzcd} M \arrow[r] \arrow[dr, "A\text{-linear}"'] & TM \arrow[d, dashed, "\exists! A\text{-algebra}"] \\ & R \end{tikzcd}$$

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^2M 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).

$$\begin{tikzcd} M \arrow[r] \arrow[dr, "A\text{-linear}"'] & \mathrm{Sym}(M) \arrow[d, dashed, "\exists! A\text{-algebra}"] \\ & R \end{tikzcd}$$

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

Exercises

EXERCISE 10.6. Look up "symmetric monoidal category" in the Wikipedia and show that the category of A-modules equipped with the bifunctor $\otimes$ and the maps λ, α, and γ in (10.1) is such a category.

11 Flatness

PROPOSITION 11.1. *Let M be an A-module, and let $0 \to N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \to 0$ be an exact sequence of A-modules. Then the sequence*

$$M \otimes_A N' \xrightarrow{1 \otimes \alpha} M \otimes_A N \xrightarrow{1 \otimes \beta} M \otimes_A N'' \to 0$$

is exact.

PROOF. The surjectivity of $1 \otimes \beta$ is obvious. Let $M \otimes_A N \xrightarrow{\phi} Q$ be the cokernel of $1 \otimes \alpha$. Because

$$(1 \otimes \beta) \circ (1 \otimes \alpha) = 1 \otimes (\beta \circ \alpha) = 0,$$

there is a unique A-linear map $f\colon Q \to M \otimes_A N''$ such that $f \circ \phi = 1 \otimes \beta$. We shall construct an inverse g to f.

Let $m \in M$, and let $n \in N$. If $\beta(n) = 0$, then $n = \alpha(n')$ for some $n' \in N'$; hence $m \otimes n = m \otimes \alpha(n')$, and so $\phi(m \otimes n) = 0$. It follows by linearity that $\phi(m \otimes n_1) = \phi(m \otimes n_2)$ if $\beta(n_1) = \beta(n_2)$, and so the A-bilinear map

$$M \times N \to Q, \quad (m, n) \mapsto \phi(m \otimes n)$$

factors through $M \times N''$. It therefore defines an A-linear map $g\colon M \otimes_A N'' \to Q$. To show that f and g are inverse, it suffices to check that $g \circ f = \mathrm{id}_Q$ on elements of the form $\phi(m \otimes n)$ and that $f \circ g = \mathrm{id}_{M \otimes_A N''}$ on elements of the form $m \otimes \beta(n)$ — both are obvious.

The map $M \otimes_A N' \to M \otimes_A N$ in (11.1) 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 $\mathbb{Z}/m\mathbb{Z}$, only the sequence

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

is exact.

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.[14] In fact, $M \otimes_A M$ may be zero without M being zero. For example,

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

To see this, 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

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

DEFINITION 11.2. 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.

Thus, an A-module M is flat if and only if the functor $M \otimes_A -$ takes short exact sequences to short exact sequences. In other words, M is flat if and only if $M \otimes_A -$ is an exact functor, i.e.,

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

An A-algebra B is said to be ***flat*** if B is flat as an A-module.

EXAMPLE 11.3. The functor $M \otimes_A -$ takes direct sums to direct sums, and direct sums of exact sequences are exact; in particular, direct sums of injective maps are injective. Therefore direct sums of flat modules are flat, and direct summands of flat modules are flat. All free A-modules are flat. Therefore all vector spaces over a field are flat, and nonzero vector spaces are faithfully flat.

[14] 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.

EXAMPLE 11.4. Quotient maps $A \to A/\mathfrak{a}$ are rarely flat. If A is a product, $A = A_1 \times A_2$, then the projection map $A \to A_1$ is obviously flat. When A is noetherian, all flat quotient maps are of this form (Exercise 23.12).

EXAMPLE 11.5. Let $A = k[X]$. Then $M = k[X, X^{-1}]$ is a flat A-module, but $M = k[X]/(X)$ is not flat.

EXAMPLE 11.6. Since tensor products commute with direct limits, and direct limits are of exact sequences are exact, direct limits of flat A-modules are flat. In fact, every flat A-module is a direct limit of free A-modules of finite rank (Lazard, Bull. SMF 97, 81–128, 1969).

PROPOSITION 11.7. *Let P be a faithfully flat A-module. A sequence of A-modules*

$$(N):\quad N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \tag{27}$$

is exact if and only if

$$P \otimes_A (N):\quad P \otimes_A N' \xrightarrow{1\otimes\alpha} P \otimes_A N \xrightarrow{1\otimes\beta} P \otimes_A N'' \tag{28}$$

is exact.

PROOF. Consider the exact sequence

$$N' \xrightarrow{\alpha} \mathrm{Ker}(\beta) \longrightarrow C \longrightarrow 0.$$

As P is flat, the sequence

$$P \otimes_A N' \xrightarrow{1\otimes\alpha} \mathrm{Ker}(1 \otimes \beta) \longrightarrow P \otimes_A C \longrightarrow 0$$

is exact. Now

$$(N) \text{ is exact} \iff C = 0 \iff P \otimes_A C = 0 \iff P \otimes_A (N) \text{ is exact.}$$

REMARK 11.8. There is a converse to the proposition: suppose that

$$(N) \text{ is exact } \Leftrightarrow P \otimes_A (N) \text{ is exact;}$$

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

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

If $P \otimes_A N = 0$, then this sequence becomes exact when tensored with P, and so is itself exact, which implies that $N = 0$. Thus P is *faithfully* flat.

COROLLARY 11.9. *Let $A \to B$ be faithfully flat. An A-module M is flat (resp. faithfully flat) if $M \otimes_A B$ is flat (resp. faithfully flat) as a B-module.*

PROOF. We test with the sequence $(N): N' \to N \to N''$. If $M \otimes_A B$ is flat, then

$$(N) \text{ is exact } \iff B \otimes_A (N) \text{ is exact } \implies ((N) \otimes_A B) \otimes_B (M \otimes_A B) \text{ is exact.}$$

But this last is isomorphic to $((N) \otimes_A M) \otimes_A B$, which is exact if and only if $(N) \otimes_A M$ is exact. Thus M is flat. If $B \otimes_A M$ is faithfully flat, then the argument shows that (N) is exact if and only if $(N) \otimes_A M$ is exact, and so M is faithfully flat.

COROLLARY 11.10. *Let $A \to B$ be faithfully flat, and let M be an A-module. Then M is finitely generated if $B \otimes_A M$ is finitely generated.*

PROOF. Let $1 \otimes m_1, \ldots, 1 \otimes m_r$ generate $B \otimes_A M$, and let N be the submodule of M generated by the m_i. The sequence $N \to M \to N/M \to 0$ remains exact when tensored with B. Now $B \otimes N/M = 0$, and so $N/M = 0$.

PROPOSITION 11.11. *Let $i: A \to B$ be a faithfully flat homomorphism. For every A-module M, the sequence*

$$0 \to M \xrightarrow{d_0} B \otimes_A M \xrightarrow{d_1} B \otimes_A B \otimes_A M \tag{29}$$

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 (29) becomes exact after tensoring in B. But the sequence obtained from (29) by tensoring with B is isomorphic to the sequence (29) 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 11.12. *If $A \to B$ is faithfully flat, then it is injective with image the set of elements on which the maps*

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

agree.

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

PROPOSITION 11.13. *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 every 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 11.14. *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 $a \mapsto \frac{a}{1}\colon A \to S^{-1}A$ is flat.

PROOF. To give an $S^{-1}A$-module is the same as giving an A-module on which the elements of S act invertibly. Therefore $S^{-1}A \otimes_A M$ and $S^{-1}M$ satisfy the same universal property (see §10, especially (24)), 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.

COROLLARY 11.15. *If M is a flat (resp. faithfully flat) A-module, then $S^{-1}M$ is a flat (resp. faithfully flat) $S^{-1}A$-module.*

PROOF. If $N' \to N \to N''$ is an exact sequence of $S^{-1}A$-modules, then it is exact as a sequence of A-modules, and so

$$S^{-1}A \otimes_A M \otimes_A N' \to S^{-1}A \otimes_A M \otimes_A N \to S^{-1}A \otimes_A M \otimes_A N''$$

is exact. But

$$S^{-1}A \otimes_A M \otimes_A N \simeq S^{-1}M \otimes_A N \simeq S^{-1}M \otimes_{S^{-1}A} N,$$

and so $S^{-1}M$ is flat. The proof for faithful flatness is similar.

COROLLARY 11.16. *An A-module M is flat (resp. faithfully flat) if and only if the $A_{\mathfrak{m}}$-module $M_{\mathfrak{m}}$ is flat (resp. faithfully flat) for all maximal ideals $\mathfrak{m}$ in A.*

PROOF. The necessity follows from (11.15). The sufficiency is an immediate consequence of (5.15, 5.16).

PROPOSITION 11.17. *A homomorphism of rings $\varphi\colon A \to B$ 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 (11.14). 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 11.18. *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 $\mathfrak{a} = \mathrm{ann}(x) \overset{\text{def}}{=} \{a \in A \mid ax = 0\}$. Then $\mathfrak{a}$ is an ideal in A, and $M' \overset{\text{def}}{=} Ax \simeq A/\mathfrak{a}$. Moreover, $B \otimes_A M' \simeq B/\varphi(\mathfrak{a}) \cdot B$ and, because $A \to B$ is flat, $B \otimes_A M'$ is a submodule of $B \otimes_A M$. Because $\mathfrak{a}$ is proper, it is contained in a maximal ideal $\mathfrak{m}$ of A, and therefore

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

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

Let $\mathrm{spm}(A)$ denote the set of maximal ideals in A (see Chapter 15). In more geometric terms, the proposition says that a flat homomorphism $\varphi: A \to B$ is faithfully flat if and only if the image of the map $\mathrm{spec}(\varphi): \mathrm{spec}(B) \to \mathrm{spec}(A)$ contains $\mathrm{spm}(A)$. In fact, as we now prove, if φ is flat, then $\mathrm{spec}(B) \to \mathrm{spec}(A)$ is surjective.

PROPOSITION 11.19. *Let $\varphi: A \to B$ be a faithfully flat homomorphism. Every prime ideal $\mathfrak{p}$ of A is of the form $\varphi^{-1}(\mathfrak{q})$ for some prime ideal $\mathfrak{q}$ of B.*

PROOF. The prime ideals of B lying over $\mathfrak{p}$ are in natural one-to-one correspondence with the prime ideals of $B \otimes_A \kappa(\mathfrak{p})$ (5.22). But the ring $B \otimes_A \kappa(\mathfrak{p})$ is nonzero because $A \to B$ is faithfully flat, and so it has a prime (even maximal) ideal.

PROPOSITION 11.20. *Let $A \to B$ be a flat homomorphism. Let $\mathfrak{p}' \subset \mathfrak{p}$ be prime ideals in A, and let $\mathfrak{q}$ be a prime ideal in B such that $\mathfrak{q}^c = \mathfrak{p}$. Then there exists a prime ideal $\mathfrak{q}' \subset \mathfrak{q}$ in B such that $\mathfrak{q}'^c = \mathfrak{p}'$.*

PROOF. Because $A \to B$ is flat, the homomorphism $A_\mathfrak{p} \to B_\mathfrak{q}$ is flat, and because $\mathfrak{p}A_\mathfrak{p} = (\mathfrak{q}B_\mathfrak{q})^c$, it is faithfully flat (11.18). The ideal $\mathfrak{p}'A_\mathfrak{p}$ is prime (5.4), and so there exists a prime ideal of $B_\mathfrak{q}$ lying over $\mathfrak{p}'A_\mathfrak{p}$ (by 11.19). The contraction of this ideal to B is contained in $\mathfrak{q}$ and contracts to $\mathfrak{p}'$ in A.

The proposition says that the going-down theorem (7.11), hence also its corollary (7.12), holds for flat homomorphisms. The going-up theorem fails for flat homomorphisms (7.8).

THEOREM 11.21 (GENERIC FLATNESS). *Let A a noetherian integral domain, and let B be a finitely generated A-algebra. Then for some nonzero elements a of A and b of B, the homomorphism $A_a \to B_b$ is faithfully flat.*

PROOF. Let F be the field of fractions of A. We first assume that $B \subset F \otimes_A B$.

As $F \otimes_A B$ is a finitely generated F-algebra, the Noether normalization theorem (8.1) shows that there exist elements $x_1, \ldots, x_m$ of $F \otimes_A B$ such that $F[x_1, \ldots, x_m]$ is a polynomial ring over F and $F \otimes_A B$ is a finite $F[x_1, \ldots, x_m]$-algebra. After multiplying each x_i by an element of A, we may suppose that it lies in B. Let $b_1, \ldots, b_n$ generate B as an A-algebra. Each b_i satisfies a monic polynomial equation with coefficients in $F[x_1, \ldots, x_m]$. Let $a \in A$ be a common denominator for the coefficients of these polynomials. Then each b_i is integral over A_a. As the b_i generate B_a as an A_a-algebra, this shows that B_a is a finite $A_a[x_1, \ldots, x_m]$-algebra (by 6.2). Therefore, after replacing A with A_a and B with B_a, we may suppose that B is a finite $A[x_1, \ldots, x_m]$-algebra.

$$\begin{tikzcd}
B \arrow[r, "\text{injective}"] & F \otimes_A B \arrow[r] & E \otimes_{A[x_1,\ldots,x_m]} B \\
A[x_1, \ldots, x_m] \arrow[u, "\text{finite}"'] \arrow[r] & F[x_1, \ldots, x_m] \arrow[u, "\text{finite}"'] \arrow[r] & E \stackrel{\text{def}}{=} F(x_1, \ldots, x_n) \arrow[u, "\text{finite}"'] \\
A \arrow[u] \arrow[r] & F. \arrow[u] &
\end{tikzcd}$$

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

$$(c_1, \ldots, c_r) \mapsto \sum c_i b_i \colon A[x_1, \ldots, x_m]_q^r \to B_q \tag{30}$$

is surjective. This map becomes an isomorphism when tensored with E over $A[x_1, \ldots, x_m]_q$, which implies that each element of its kernel is killed by a nonzero element of $A[x_1, \ldots, x_m]_q$ and so is zero (because $A[x_1, \ldots, x_n]_q$ is an integral domain). Hence the map (30) is an isomorphism, and so B_q is free of finite rank over $A[x_1, \ldots, x_m]_q$. Let a be some nonzero coefficient of the polynomial q, and consider the maps

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

The first and third arrows realize their targets as nonzero free modules over their sources, and so are faithfully flat. The middle arrow is flat by (11.14). Let $\mathfrak{m}$ be a maximal ideal in A_a. Then $\mathfrak{m}A_a[x_1, \ldots, x_m]$ does not contain the polynomial q because the coefficient a of q is invertible in A_a. Hence $\mathfrak{m}A_a[x_1, \ldots, x_m]_q$ is a proper ideal of $A_a[x_1, \ldots, x_m]_q$, and so the map $A_a \to A_a[x_1, \ldots, x_m]_q$ is faithfully flat (apply 11.18). This completes the proof when $B \subset F \otimes_A B$.

We now prove the general case. Note that $F \otimes_A B$ is the ring of fractions of B with respect to the multiplicative subset $A \smallsetminus \{0\}$ (see 11.14), 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.

Exercises

EXERCISE 11.22. Let $f_1, \ldots, f_m$ be elements of a ring A. Show that the canonical homomorphism $A \to \prod_i A_{f_i}$ is faithfully flat if and only if $(f_1, \ldots, f_m) = A$. Let $f_1, \ldots, f_m$ satisfy this condition, and let M be an A-module. Deduce from (11.11) that the sequence

$$0 \to M \to \prod_{1 \le i \le m} M_{f_i} \to \prod_{1 \le i,j \le m} M_{f_i f_j}$$

is exact (the first map sends m to (n_i) with n_i equal to the image of m in M_{f_i}, and the second map sends (m_i) to (n_{ij}) with

$$n_{ij} = (\text{image of } m_i \text{ in } M_{f_i f_j}) - (\text{image of } m_j \text{ in } M_{f_i f_j})).$$

EXERCISE 11.23. 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.)

EXERCISE 11.24. Let A be an integrally closed integral domain, and let G be a finite group acting on A by ring homomorphisms. Show that $A^G \overset{\text{def}}{=} \{a \in A \mid ga = a \text{ for all } g \in G\}$ is an integrally closed integral domain.

12 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, finitely generated projective modules are the algebraist's analogue of the differential geometer's vector bundles (see 12.12).

Projective modules

DEFINITION 12.1. An A-module P is ***projective*** if, for each surjective A-linear map $f\colon M \to N$ and A-linear map $g\colon P \to N$, there exists an A-linear map $h\colon P \to M$ (not necessarily unique) such that $f \circ h = g$:

$$\begin{tikzcd} & P \arrow[dl, dashed, "\exists h"'] \arrow[d, "g"] & \\ M \arrow[r, "f"] & N \arrow[r] & 0. \end{tikzcd}$$

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

$$M \rightsquigarrow \mathrm{Hom}(P, M) \qquad (A\text{-linear maps})$$

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 summand is projective. As A itself is projective, this shows that free A-modules are 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

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

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 12.2. 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 12.3. *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. Let $A^n \to M$ be a surjective homomorphism with finitely generated kernel N. We have to show that the kernel N' of every other surjective homomorphism $A^m \to M$ is finitely generated. Consider the diagram:

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] \arrow[d, dashed, "f"] & A^n \arrow[r] \arrow[d, dashed, "g"] & M \arrow[r] \arrow[d, "\mathrm{id}_M"] & 0 \\ 0 \arrow[r] & N' \arrow[r] & A^m \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

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. The image of N in N' is finitely generated, and so N' is an extension of finitely generated modules. Therefore it is finitely generated (3.3(b)).

COROLLARY 12.4. *Let $A \to B$ be faithfully flat, and let M be an A-module. Then M is finitely presented if $B \otimes_A M$ is finitely presented.*

PROOF. From Corollary 11.10 we know that M is finite generated, and so there is a surjective map $\alpha: A^r \to M$ for some $r \in \mathbb{N}$. The kernel of α is finitely generated because it becomes finitely generated when tensored with M. Hence M is finitely presented.

PROPOSITION 12.5. *A finitely generated projective module is finitely presented.*

PROOF. Let M be finitely generated and projective. There exists a surjective homomorphism $A^n \to M$ (because M is finitely generated), whose kernel N is a direct summand of A^n (because M is projective). As N is a quotient of A^n, it is finitely generated.

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

PROOF. (a)⇒(d). Free modules are flat, and direct summands of flat modules are flat (11.3). Therefore, projective modules are flat, and we know (12.5) that finitely generated projective modules are finitely presented.

(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 an $f \in A \smallsetminus \mathfrak{m}$ such that $N'_f = 0 = N_f$ (5.13). Now α becomes an isomorphism when tensored with A_f.

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

(c)⇒(d). Let $B = \prod_{i \in I} A_{f_i}$. Then B is faithfully flat over A (Exercise 11.22), 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 11.9).

(c)⇒(e). This is obvious.

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

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

defines a surjection $A_\mathfrak{p}^r \to M_\mathfrak{p}$ (Nakayama's lemma; note that $\kappa(\mathfrak{p}) \simeq A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$). The cokernel N of α is finitely generated, and so $gN = 0$ for some $g \in A \smallsetminus \mathfrak{p}$. The map α becomes surjective once f has been replaced fg. For every 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 elements f will generate A.

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

LEMMA 12.7. *Let*

$$0 \to N \to F \to M \to 0 \tag{31}$$

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 $f\colon F \to N$ with $f(n_j) = n_j$, $j = 1, \ldots, r$.*

PROOF. (a) Consider

$$\begin{tikzcd}
 & \mathfrak{a} \otimes N \arrow[r] & \mathfrak{a} \otimes F \arrow[r] \arrow[d, "\simeq"] & \mathfrak{a} \otimes M \arrow[d, "\simeq"] \\
0 \arrow[r] & N \cap \mathfrak{a}F \arrow[r] & \mathfrak{a}F \arrow[r] & \mathfrak{a}M
\end{tikzcd}$$

The first row is obtained from (31) by tensoring with $\mathfrak{a}$, and the second row is a subsequence of (31). 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

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

Then

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

has the required property.

We now complete the proof of the theorem.

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

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

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

(d)⇒(b). We may suppose that A itself is local, with maximal ideal $\mathfrak{m}$. Let $x_1,\ \ldots,\ x_r\in M$ be such that their images in $M/\mathfrak{m}M$ form a basis for this over the field $A/\mathfrak{m}$. Then the x_i generate M (by Nakayama's lemma 3.9), and so there exists an exact

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

in which F is free with basis $\{y_1,\ \ldots,\ y_r\}$ and $g(y_i)=x_i$. According to (a) of the lemma, $\mathfrak{m}N=N\cap(\mathfrak{m}F)$, which equals N because $N\subset\mathfrak{m}F$. Therefore N is zero by Nakayama's lemma 3.9.

DEFINITION 12.8. A ring is ***semilocal*** if it has only finitely many maximal ideals.

Let A be a semilocal ring with maximal ideals $\mathfrak{m}_1,\ldots,\mathfrak{m}_n$. Then

$$A/\mathfrak{m}_1\cdots\mathfrak{m}_n\simeq A/\mathfrak{m}_1\times\cdots\times A/\mathfrak{m}_n$$

by the Chinese remainder theorem 2.13. This says that the quotient of A by its Jacobson radical is a finite product of fields.

PROPOSITION 12.9. *A locally free module M of finite constant rank over a semilocal ring A is free*

PROOF. The statement is obvious when A is a finite product of fields, and the general case then follows from the next lemma.

LEMMA 12.10. *Let A be a ring and $\mathfrak{a}$ an ideal of A contained in all maximal ideals. A finitely presented flat A-module M is free if $M/\mathfrak{a}M$ is a free $A/\mathfrak{a}$-module.*

PROOF. Let $e_1,\ldots,e_r$ be elements of M whose images $\bar{e}_1,\ldots,\bar{e}_r$ in $M/\mathfrak{a}M$ form a basis. The map $(a_i)\mapsto\sum a_ie_i\colon A^r\to M$ is surjective by Nakayama's lemma (3.9), and it remains to show that its kernel N is 0. For this, it suffices to show that $\mathfrak{a}N=N$ (by 3.9 again).

Consider the commutative diagram

$$\begin{tikzcd}
 & \mathfrak{a}\otimes N \arrow[r] \arrow[d, "a"] & \mathfrak{a}\otimes A^r \arrow[r] \arrow[d, "b"] & \mathfrak{a}\otimes M \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & N \arrow[r] & A^r \arrow[r] & M \arrow[r] & 0
\end{tikzcd} \qquad a\otimes x\mapsto ax.$$

The rows are exact (see 11.1 for the top row), and the map c is injective because M is flat. Therefore the sequence of cokernels

$$0\to\operatorname{Coker}(a)\to\operatorname{Coker}(b)\to\operatorname{Coker}(c)\to 0$$

is exact by the snake lemma. But $\operatorname{Coker}(a)=N/\mathfrak{a}N$ and the map $\operatorname{Coker}(b)\to\operatorname{Coker}(c)$ is the isomorphism

$$(a_i)\mapsto\sum a_i\bar{e}_i\colon(A/\mathfrak{a})^r\to M/\mathfrak{a}M,$$

and so $N=\mathfrak{a}N$ as required.

EXAMPLE 12.11. (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 $R/\mathfrak{a}$ is finitely generated and flat, but not projective (it is not finitely presented).

ASIDE 12.12. The equivalence of (a) and (c) in the theorem has the following geometric interpretation: for an affine scheme X, the functor $\mathcal{M}\rightsquigarrow\mathcal{M}(X)$ is an equivalence from the category of locally free $\mathcal{O}_X$-modules of finite rank to the category of finitely generated $\mathcal{O}_X(X)$-modules. (See Section 50 of J.-P. Serre, Ann. of Math. (2) 61 (1955), 197–278. This is also where Serre asked whether a finitely generated projective $k[X_1,\ldots,X_n]$-module is necessarily free. That it is was proved (independently) by Quillen and Suslin. For a beautiful exposition of Quillen's proof, see A. Suslin, *Quillen's solution of Serre's problem*. J. K-Theory 11 (2013), 549–552.)

ASIDE 12.13. 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 needed 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 $\mathrm{Hom}_{A\text{-linear}}(M,A)$ of an A-module M is denoted $M^\vee$.

PROPOSITION 12.14. *For all A-modules M, S, T with M finitely generated and projective, the canonical maps*

$$\mathrm{Hom}_{A\text{-linear}}(S, T\otimes_A M) \to \mathrm{Hom}_{A\text{-linear}}(S\otimes_A M^\vee, T) \tag{32}$$
$$T\otimes_A M \to \mathrm{Hom}_{A\text{-linear}}(M^\vee, T) \tag{33}$$
$$M^\vee\otimes T^\vee \to (M\otimes T)^\vee \tag{34}$$
$$M \to M^{\vee\vee} \tag{35}$$

are isomorphisms.

PROOF. The canonical map (32) sends $f\colon S\to T\otimes_A M$ to the map $f'\colon S\otimes_A M^\vee\to T$ such that $f'(s\otimes g)=(T\otimes g)(f(s))$. It becomes the canonical isomorphism

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

when $M=A^n$. It follows that (32) 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 (33) sends $t\otimes m$ to the map $f\mapsto f(m)t$. It is the special case of (32) in which $S=A$.

The canonical map (34) sends $f\otimes g\in M^\vee\otimes T^\vee$ to the map $m\otimes t\mapsto f(m)\otimes g(t)\colon M\otimes T\to A$, and the canonical map (35) sends m to the map $f\mapsto f(m)\colon M^\vee\to A$. 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 $\mathrm{ev}\colon M^\vee\otimes_A M\to A$ denote the evaluation map $f\otimes m\mapsto f(m)$.

LEMMA 12.15. *Let M and N be modules over commutative ring A, and let $e\colon N\otimes_A M\to A$ be an A-linear map. There exists at most one A-linear map $\delta\colon A\to M\otimes_A N$ such that the composites*

$$\begin{array}{ccccc} M & \xrightarrow{\delta\otimes M} & M\otimes N\otimes M & \xrightarrow{M\otimes e} & M\\ N & \xrightarrow{N\otimes\delta} & N\otimes M\otimes N & \xrightarrow{e\otimes N} & N \end{array} \tag{36}$$

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

$$T\otimes_A N\simeq \mathrm{Hom}_{A\text{-linear}}(M,T) \tag{37}$$

for all A-modules T. In particular,

$$(N,e)\simeq(M^\vee,\mathrm{ev}). \tag{38}$$

PROOF. From e we get an A-linear map

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

which allows us to define an A-linear map

$$x\mapsto f_x\colon T\otimes_A N\to\mathrm{Hom}_{A\text{-lin}}(M,T) \tag{39}$$

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

$$f \mapsto (f \otimes N)(\delta(1)): \mathrm{Hom}_{A\text{-lin}}(M,T) \to T \otimes_A N. \tag{40}$$

When the first (resp. the second) composite in (36) is the identity, then (40) is a right (resp. a left) inverse to (39).[15] Therefore, when a map δ exists with the required properties, the map (39) 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 (38), take $T = M$ in (37).

Let $A \to B$ be a ring homomorphism. Let $e: N \otimes_A M \to A$ be an A-linear map. Because the functor $M \rightsquigarrow M_B \overset{\text{def}}{=} B \otimes_A M$ commutes with tensor products (see p.40), $\delta: A \to M \otimes_A N$ satisfies the conditions of (12.15) relative to e, then $\delta_B: B \to M_B \otimes_B N_B$ satisfies the conditions of (12.15) relative to e_B.

PROPOSITION 12.16. *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*

$$\begin{cases} (M \otimes \mathrm{ev}) \circ (\delta \otimes M) = \mathrm{id}_M \\ (M^\vee \otimes \delta) \circ (\mathrm{ev} \otimes M^\vee) = \mathrm{id}_{M^\vee}. \end{cases} \tag{41}$$

PROOF. $\Longleftarrow$: On taking $T = M$ in (37), we see that $M^\vee \otimes_A M \simeq \mathrm{End}(M)$ (A-linear endomorphisms). 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.

$\Longrightarrow$: 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 (41).

[15] 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 (36) 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

$$\begin{tikzcd} & T \otimes_A N \otimes_A M \arrow[r, "T \otimes e"] & T \\ M \arrow[r, "\delta \otimes M"] & M \otimes_A N \otimes_A M \arrow[r, "M \otimes e"] \arrow[u, "f \otimes N \otimes M"] & M. \arrow[u, "f"] \end{tikzcd}$$

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 $f = f_{(f \otimes N)(\delta(1))}$.

Moreover, it is the unique map satisfying (41) — see (12.15). In particular, it is independent of the choice of e_i.

For the general case, we choose a family $(f_i)_{1\leq i\leq m}$ as in (12.6c). In particular, M_{f_i} is a free A_{f_i}-module, and so δ is defined for each module M_{f_i}; the uniqueness assertion in Lemma 12.15 then implies that the δ for the different M_{f_i} patch together to give a δ for M.

In more detail, consider the diagram

$$\begin{tikzcd}
A \arrow[r] & \prod_{1\leq i\leq m} A_{f_i} \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "(\delta_i)"] & \prod_{1\leq i,j\leq m} A_{f_i f_j} \arrow[d] \\
M\otimes M^{\vee} \arrow[r] & \prod_{1\leq i\leq m} (M\otimes M^{\vee})_{f_i} \arrow[r, shift left] \arrow[r, shift right] & \prod_{1\leq i,j\leq m} (M\otimes M^{\vee})_{f_i f_j}.
\end{tikzcd}$$

In the top row, the first arrow sends a to (a_i) with a_i equal to the image of a in A_{f_i}, and the upper arrow (resp. lower arrow) sends (a_i) to $(a_{i,j})$ with $a_{i,j}$ equal to the image of a_i in $A_{f_i f_j}$ (resp. the image of a_j in $A_{f_i f_j}$). The bottom row is obtained from the top row by tensoring with $M\otimes M^{\vee}$. The vertical map (δ_i) is the product of the (unique) maps satisfying (41). The vertical map at right can be described as the extension of scalars of (δ_i) via the upper arrow $\prod_i A_{f_i}\to\prod_{i,j} A_{f_i f_j}$ or the extension of scalars of (δ_i) via the lower arrow — they are the same because they both equal the unique $\prod_{i,j} A_{f_i f_j}$-linear map satisfying the condition (41). As A and M are the submodules of $\prod_i A_{f_i}$ and $\prod_i M_{f_i}$ on which the pairs of arrows agree (Exercise 11.22), the map (δ_i) induces an A-linear $A\to M\otimes M^{\vee}$, which satisfies (41). [This argument becomes more transparent when expressed in terms of sheaves.]

ASIDE 12.17. A module M over a ring A is said to be ***reflexive*** if the canonical map $M\to M^{\vee\vee}$ is an isomorphism. We have seen that for finitely generated modules "projective" implies "reflexive", but the converse is false. In fact, for a finite generated module M over an integrally closed noetherian integral domain A, the following are equivalent (Bourbaki AC, VII, §4, 2):

(a) M is reflexive;

(b) M is torsion-free and equals the intersection of its localizations at the prime ideals of A of height 1;

(c) M is the dual of a finitely generated module.

For noetherian rings of global dimension ≤ 2, for example, for regular local rings of Krull dimension ≤ 2, every finitely generated reflexive module is projective: for 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 12.18. 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 to 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 12.19. 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).

13 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 $p_1, \ldots, p_r$ are monic irreducible polynomials in $k[X]$, then $p_1 \cdots p_r + 1$ is divisible by a monic irreducible polynomial distinct from $p_1, \ldots, p_r$.

THEOREM 13.1 (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

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

If K is not algebraic over k, then at least one x_i, say x_1, is not algebraic over k. Then, $k[x_1]$ is a polynomial ring in one symbol over k, and its field of fractions $k(x_1)$ is a subfield of K. Clearly K is generated as a $k(x_1)$-algebra by $x_2, \ldots, x_r$, and so the induction hypothesis implies that $x_2, \ldots, x_r$ are algebraic over $k(x_1)$. According to Proposition 6.7, there exists a $c \in k[x_1]$ such that $cx_2, \ldots, cx_r$ are integral over $k[x_1]$.

Let $f \in k(x_1)$. Then $f \in K = k[x_1, \ldots, x_r]$ and so, for a sufficiently large N, $c^N f \in k[x_1, cx_2, \ldots, cx_r]$. Therefore $c^N f$ is integral over $k[x_1]$ by (6.5), which implies that $c^N f \in k[x_1]$ because $k[x_1]$ is integrally closed in $k(x_1)$ (6.10). But this contradicts the fact that $k[x_1]$ ($\simeq k[X]$) has infinitely many distinct monic irreducible polynomials that can occur as denominators of elements of $k(x_1)$. Hence K is algebraic over k.

COROLLARY 13.2. *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.

COROLLARY 13.3. *Let $k \subset K \subset A$ be k-algebras with K a field and A finitely generated over k. Then K is algebraic over k.*

PROOF. Let $\mathfrak{m}$ be a maximal ideal in A. Then $\mathfrak{m} \cap K = (0)$, and so $k \subset K \subset A/\mathfrak{m}$. The theorem shows that the field $A/\mathfrak{m}$ is algebraic over k, and hence K is also.

REMARK 13.4. Let A be a finitely generated k-algebra. It follows from (13.2) that the maximal ideals $\mathfrak{m}$ in A are exactly the kernels of k-algebra homomorphisms $\varphi: A \to k^{\mathrm{a}}$. If $\mathfrak{m} = \mathrm{Ker}(\varphi)$, then $\mathfrak{m}$ has residue field k if and only if the image of φ is k. In this way, we get a one-to-one correspondence between the maximal ideals of A with residue field k and the k-algebra homomorphisms from A to k.

ASIDE 13.5. There is a very short proof of Zariski's lemma when k is uncountable. Let $k \subset K$ be fields. If K is finitely generated as a k-algebra, then its dimension as a k-vector space is countable. On the other hand, if $x \in K$ is transcendental over k, then the elements $\frac{1}{x-c}$, $c \in k$, are linearly independent (assume a linear relation, and clear denominators). When k is uncountable, this gives a contradiction.

Alternative proof of Zariski's lemma

The following is a simplification of Swan's simplication[16] of a proof of Munshi.

LEMMA 13.6. *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).

PROPOSITION 13.7. *Let A be an integral domain, and suppose that there exists a maximal ideal $\mathfrak{m}$ in $A[X_1,\ldots,X_n]$ such that $A \cap \mathfrak{m} = (0)$. Then there exists a nonzero $a \in A$ such that A_a is a field and $A[X_1,\ldots,X_n]/\mathfrak{m}$ is a finite extension of A_a.*

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

[16]For a leisurely exposition of Munshi's proof, see May, J. Peter, Munshi's proof of the Nullstellensatz. Amer. Math. Monthly 110 (2003), no. 2, 133–140.

PROOF. 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 $A[X_1,\ldots,X_n]$ as a polynomial ring in $n-1$ symbols over $A[X_i]$ for some fixed i. If $\mathfrak{m} \cap A[X_i] = (0)$, then, by induction, there exists an $f \in A[X_i]$ such that $A[X_i]_f$ is a field, contradicting Lemma 13.6. We conclude that, for each i, there exists a nonzero element

$$a_i X_i^{n_i} + \cdots$$

in $\mathfrak{m} \cap A[X_i]$. 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 $A_{a_1 \cdots a_n}$. This implies that $A_{a_1 \cdots a_n}$ is a field (see 7.1), and K is finite over it because it is integral and finitely generated (6.3).

We now prove Zariski's lemma. Let $\mathfrak{m}$ be a maximal ideal in $k[X_1,\ldots,X_n]$. Then $k \cap \mathfrak{m} = (0)$ because k is a field. According to the proposition, there exists a nonzero $a \in k$ such that $k[X_1,\ldots,X_n]/\mathfrak{m}$ is a finite extension of k_a, but, because k is a field, $k_a = k$.

The Nullstellensatz

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

THEOREM 13.8 (NULLSTELLENSATZ). *Every proper ideal $\mathfrak{a}$ in $k[X_1,\ldots,X_n]$ has a zero in $(k^{\mathrm{al}})^n$, i.e., there exists a point $(a_1,\ldots,a_n) \in (k^{\mathrm{al}})^n$ such that $f(a_1,\ldots,a_n) = 0$ for all $f \in \mathfrak{a}$.*

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

COROLLARY 13.9. *When k is algebraically closed, the maximal ideals in $k[X_1,\ldots,X_n]$ are exactly the ideals $(X_1 - a_1,\ldots,X_n - a_n)$, $(a_1,\ldots,a_n) \in k^n$.*

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

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

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

THEOREM 13.10 (STRONG NULLSTELLENSATZ). *For an ideal $\mathfrak{a}$ in $k[X_1,\ldots,X_n]$, let $Z(\mathfrak{a})$ be the set of zeros of $\mathfrak{a}$ in $(k^{\mathrm{al}})^n$. If a polynomial $h \in k[X_1,\ldots,X_n]$ is zero on $Z(\mathfrak{a})$, then some power of h lies in $\mathfrak{a}$.*

PROOF. [17]We may assume $h \neq 0$. Let $g_1,\ldots,g_m$ generate $\mathfrak{a}$, and consider the system of $m+1$ equations in $n+1$ variables, $X_1,\ldots,X_n,Y$,

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

If $(a_1,\ldots,a_n,b)$ satisfies the first m equations, then $(a_1,\ldots,a_n) \in Z(\mathfrak{a})$; consequently, $h(a_1,\ldots,a_n)=0$, and $(a_1,\ldots,a_n,b)$ doesn't satisfy the last equation. Therefore, the equations are inconsistent, and so, according to the Nullstellensatz (13.8), the ideal

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

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

$$1 = \sum_{i=1}^{m} f_i \cdot g_i + f_{m+1}\cdot(1-Yh). \tag{42}$$

On applying the homomorphism

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

to (42), we obtain the identity

$$1 = \sum\nolimits_i f_i(X_1,\ldots,X_n,h^{-1})\cdot g_i(X_1,\ldots,X_n) \tag{43}$$

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

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

for some N_i. Let N be the largest of the N_i. On multiplying (43) by h^N we obtain an identity

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

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

PROPOSITION 13.11. *The radical of an ideal* $\mathfrak{a}$ *in a finitely generated* k*-algebra* A *is equal to the intersection of the maximal ideals containing it:* $\mathrm{rad}(\mathfrak{a}) = \bigcap_{\mathfrak{m}\supset\mathfrak{a}} \mathfrak{m}$. *In particular, if* A *is reduced, then* $\bigcap_{\mathfrak{m}\text{ maximal}} \mathfrak{m} = 0$.

PROOF. Because of the correspondence between the ideals in a ring and in a quotient of the ring ((2), p. 4), it suffices to prove this for $A = k[X_1,\ldots,X_n]$.

[17]This argument is known as Rabinowitsch's trick (J. L. Rabinowitsch, "Zum Hilbertschen Nullstellensatz", Math. Ann. 102 (1930), p.520). When he emigrated to the United States, Rabinowitsch simplified his name to Rainich. He was a faculty member at the University of Michigan from 1925–1956, where the following story is folklore: Rainich was giving a lecture in which he made use of a clever trick which he said he had discovered. Someone in the audience indignantly interrupted him pointing out that this was the famous Rabinowitsch trick and berating Rainich for claiming to have discovered it. Without a word Rainich turned to the blackboard and wrote RABINOWITSCH. He then began erasing letters. When he was done what remained was RA IN I CH. He then went on with his lecture. See also mo45185.

The inclusion $\operatorname{rad}(\mathfrak{a}) \subset \bigcap_{\mathfrak{m}\supset\mathfrak{a}} \mathfrak{m}$ holds in every ring (because maximal ideals are radical and $\operatorname{rad}(\mathfrak{a})$ is the smallest radical ideal containing $\mathfrak{a}$).

For the reverse inclusion, let h lie in all maximal ideals containing $\mathfrak{a}$, and let $(a_1,\ldots,a_n) \in Z(\mathfrak{a})$. The image of the evaluation map

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

is 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 so also contains h. This shows that $h(a_1,\ldots,a_n) = 0$, and we conclude from the strong Nullstellensatz that $h \in \operatorname{rad}(\mathfrak{a})$.

14 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 14.1. *There are the following relations:*

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

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

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

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

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

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

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

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

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

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).

Idempotents and decompositions of spec(A)

An element e of a ring A is ***idempotent*** if $e^2 = e$. For example, 0 and 1 are both idempotents — they are called the ***trivial idempotents***. Idempotents $e_1, \ldots, e_n$ are ***orthogonal*** if $e_i e_j = 0$ for $i \neq j$. Every sum of orthogonal idempotents is again idempotent. A set $\{e_1, \ldots, e_n\}$ of orthogonal idempotents is ***complete*** if $e_1 + \cdots + e_n = 1$. Every finite set of orthogonal idempotents $\{e_1, \ldots, e_n\}$ can be made into a complete set of orthogonal idempotents by adding the idempotent $e = 1 - (e_1 + \cdots + e_n)$.

LEMMA 14.2. *The topological space* spec(A) *is disconnected if and only if A contains a nontrivial idempotent e, in which case*

$$\operatorname{spec}(A) = D(e) \sqcup D(1-e).$$

PROOF. Let e be a nontrivial idempotent, 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 $D(e)$ and $D(f)$, each of which is open. If $D(e) = \operatorname{spec} A$, then e would be a unit (2.3), 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 (2.5), say $(ab)^m = 0$. Every 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.

Let U be an open and closed subset of spec(A). The proof of the lemma shows that $U = D(e)$ for some idempotent $e \in A$. Let $U' = \operatorname{spec}(A) \smallsetminus U$. The image of e in $\mathcal{O}(U')$ lies in all prime ideals of $\mathcal{O}(U')$; hence is nilpotent; hence is 0. The image $\bar{e}$ of e in $\mathcal{O}(U)$ lies in no prime ideals of $\mathcal{O}(U)$; hence $1 - \bar{e} = 0$; hence $\bar{e} = 1$. As $\operatorname{spec}(A) = U \cup U'$, this shows that e is uniquely determined by U.

PROPOSITION 14.3. *Let $X = \operatorname{spec}(A)$. There are natural one-to-one correspondences between the following objects.*

(a) *Decompositions*

$$X = X_1 \sqcup \ldots \sqcup X_n$$

of X into a finite disjoint union of open subsets.

(b) *Decompositions*

$$A = A_1 \times \cdots \times A_n$$

of A into a finite product of rings ($A_i \subset A$).

(c) *Decompositions*

$$1 = e_1 + \cdots + e_n$$

of 1 into the sum of a complete sets $\{e_1,\ldots,e_n\}$ of orthogonal idempotents in A.

The sets X_i in (a) are connected $\iff$ no ring A_i in (b) has a nontrivial idempotent $\iff$ no idempotent e_i in (c) can be written as a sum of two nontrivial idempotents.

PROOF. (b)↔(c). If $A = A_1 \times \cdots \times A_n$ (direct product of rings), then the elements

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

form a complete set of orthogonal idempotents in A. Conversely, if $\{e_1,\ldots,e_n\}$ is a complete set of orthogonal idempotents in A, then Ae_i becomes a ring[18] with the addition and multiplication induced by that of A, and $A \simeq Ae_1 \times \cdots \times Ae_n$.

(c)↔(a). Let $\{e_1,\ldots,e_n\}$ be a complete set of orthogonal idempotents, and 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

$$\operatorname{spec}(A) = X_1 \sqcup \ldots \sqcup X_n$$

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

$$\operatorname{spec} A = X_1 \sqcup (X_2 \sqcup \ldots \sqcup X_n).$$

From Lemma 14.2 et seq. we know that there exist unique orthogonal idempotents $e_1, e_1' \in A$ such that $e_1 + e_1' = 1$ and

$$X_1 = D(e_1)$$
$$X_2 \sqcup \ldots \sqcup X_n = D(e_1') = \operatorname{spec} Ae_1'.$$

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

(b)↔(a). 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). As $\prod_i A_i/\prod_i \mathfrak{a}_i \simeq \prod_i A/\mathfrak{a}_i$, we see that the prime 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. It follows that $\operatorname{spec}(A) = \bigsqcup_i \operatorname{spec}(A_i)$ (disjoint union of open subsets).

Let spec$(A) = X_1 \sqcup \ldots \sqcup X_n$, and let $1 = e_1 + \cdots + e_n$ be the corresponding decomposition of 1. Then $\mathcal{O}_X(X_i) \simeq \mathcal{O}_X(X)e_i$, and so $\mathcal{O}_X(X) \simeq \prod_i \mathcal{O}_X(X_i)$.

[18]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 $a \mapsto ae_i : A \to Ae_i$ realizes Ae_i as a quotient of A.

Properties of 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 14.4. *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) *Every open covering of V has a finite subcovering.*
(d) *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.*

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

(c) 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 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 $a_1, \ldots, a_m \in A$. Now 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.

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

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). A topological space V having the property in (d) is said to be ***noetherian***. This condition is equivalent to the following: every nonempty set of closed subsets of V has a minimal element. Clearly, noetherian spaces are quasi-compact. Since an open subspace of a noetherian space is again noetherian, it will also be quasi-compact.

DEFINITION 14.5. 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 14.6. *A closed subset W of* $\operatorname{spec}(A)$ *is irreducible if and only if $I(W)$ is prime. 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 $\mathfrak{p}$ in W, and so either $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$; 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 14.1c) and that $\mathfrak{a} \cap \mathfrak{b}$ is radical; hence $I(W) = \mathfrak{a} \cap \mathfrak{b}$ (by 15.3). 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 14.7. Let $f \in k[X_1, \ldots, X_n]$. According to Theorem 4.10, $k[X_1, \ldots, X_n]$ 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 14.8. *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. The V_i are exactly the maximal irreducible subsets of V.*

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 $f: \{1,\ldots,m\} \to \{1,\ldots,n\}$ such that $V_i \subset W_{f(i)}$ for each i. Similarly, there is a function $g: \{1,\ldots,n\} \to \{1,\ldots,m\}$ 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.

Let W be a maximal irreducible subset of V. Then

$$W = (V_1 \cap W) \cup \ldots \cup (V_m \cap W).$$

Each set $V_i \cap W$ is closed in W, and so $W = V_i \cap W$ for some i, i.e., $W \subset V_i$ for some i. Because W is maximal, it equals V_i.

The V_i given uniquely by the proposition are called the ***irreducible components*** of V. In Example 14.7, the $V(f_i)$ are the irreducible components of $V(f)$.

COROLLARY 14.9. *Every radical ideal $\mathfrak{a}$ in a noetherian ring A 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. Every prime ideal of A containing $\mathfrak{a}$ contains some $\mathfrak{p}_i$.*

PROOF. In view of the correspondence between radical (resp. prime) ideals in A and closed (resp. irreducible closed) subsets in $\mathrm{spec}(A)$, this is a restatement of the proposition.

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

COROLLARY 14.10. *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 14.11. (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 proper 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 §19). 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 14.7.

Maps of spectra

Let $\varphi\colon A \to B$ be a homomorphism of rings, and let $\mathfrak{p}$ be a prime ideal of B. Then $B/\mathfrak{p}B$ is an integral domain and the map $A/\varphi^{-1}(\mathfrak{p}) \to B/\mathfrak{p}$ is injective, and so $\varphi^{-1}(\mathfrak{p})$ is a prime ideal in A. Therefore φ defines a map

$$\varphi^a\colon \mathrm{spec}(B) \to \mathrm{spec}(A).$$

This map is continuous because $(\varphi^a)^{-1}(D(f)) = D(\varphi(f))$. In this way, spec becomes a contravariant functor from the category of commutative rings to the category of topological spaces.

DEFINITION 14.12. A subset C of a noetherian topological space X is ***constructible*** if it is a finite union of subsets of the form $U \cap Z$ with U open and Z closed.

The constructible subsets of $\mathbb{A}^n$ are those that can be defined by a finite number of statements of the form

$$f(X_1,\ldots,X_n) = 0$$

combined using only "and", "or", and "not". This explains the name.

PROPOSITION 14.13. *Let C be a constructible set whose closure $\bar{C}$ is irreducible. Then C contains a nonempty open subset of $\bar{C}$.*

PROOF. We are given that $C = \bigcup(U_i \cap Z_i)$ with each U_i open and each Z_i closed. We may assume that each set $U_i \cap Z_i$ in this decomposition is nonempty. Clearly $\bar{C} \subset \bigcup Z_i$, and as $\bar{C}$ is irreducible, it must be contained in one of the Z_i. For this i

$$C \supset U_i \cap Z_i \supset U_i \cap \bar{C} \supset U_i \cap C \supset U_i \cap (U_i \cap Z_i) = U_i \cap Z_i.$$

Thus $U_i \cap Z_i = U_i \cap \bar{C}$ is a nonempty open subset of $\bar{C}$ contained in C.

THEOREM 14.14. *Let A be a noetherian ring, and let $\varphi\colon A \to B$ be a finitely generated A-algebra. The map $\varphi^a\colon \mathrm{spec}(B) \to \mathrm{spec}(A)$ sends constructible sets to constructible sets. In particular, if U is a nonempty open subset of $\mathrm{spec}(B)$, then $\varphi^a(U)$ contains a nonempty open subset of its closure in $\mathrm{spec}(A)$.*

PROOF. The "in particular" statement of the theorem is proved for finitely generated k-algebras in (15.8) below and for noetherian rings in (21.11) below.

We now explain how to deduce the main statement of the theorem from the "in particular" statement. Let $X = \mathrm{spec}(A)$ and $Y = \mathrm{spec}(B)$, and let C be a constructible subset of Y. Let Y_i be the irreducible components of Y. Then $C \cap Y_i$ is constructible in Y_i, and $\varphi^a(Y)$ is the union of the $\varphi^a(C \cap Y_i)$; it is therefore constructible if the $\varphi^a(C \cap Y_i)$ are. Hence we may assume that Y is irreducible. Moreover, C is a finite union of its irreducible components, and these are closed in C; they are therefore constructible. We may therefore assume that C also is irreducible; $\bar{C}$ is then an irreducible closed subvariety of Y.

We shall prove the theorem by induction on the dimension of Y. If $\dim(Y) = 0$, then the statement is obvious because Y is a point. If $\bar{C} \neq Y$, then $\dim(\bar{C}) < \dim(Y)$, and because C is constructible in $\bar{C}$, we see that $\varphi^a(C)$ is constructible (by induction). We may therefore assume that $\bar{C} = Y$. But then $\bar{C}$ contains a nonempty open subset of Y, and so we know that $\varphi^a(C)$ contains an nonempty open subset U of its closure. Replace X with the closure of $\varphi^a(C)$, and write

$$\varphi^a(C) = U \cup \varphi^a(C \cap (\varphi^a)^{-1}(X \smallsetminus U)).$$

Then $(\varphi^a)^{-1}(X \smallsetminus U)$ is a proper closed subset of Y (the complement of $X - U$ is dense in X and φ^a is dominant). As $C \cap (\varphi^a)^{-1}(X \smallsetminus U)$ is constructible in $(\varphi^a)^{-1}(X \smallsetminus U)$, the set $\varphi^a(C \cap (\varphi^a)^{-1}(X \smallsetminus U))$ is constructible in X by induction, which completes the proof.

Let $\mathfrak{p}$ and $\mathfrak{p}'$ be prime ideals in a ring A. If $\mathfrak{p} \subset \mathfrak{p}'$ (i.e., $\mathfrak{p}' \in V(\mathfrak{p})$), then we say that $\mathfrak{p}'$ is a ***specialization*** of $\mathfrak{p}$ and that $\mathfrak{p}$ is a ***generalization*** of $\mathfrak{p}'$.

PROPOSITION 14.15. *Let A be a noetherian ring, and let $X = \mathrm{spec}(A)$. A constructible subset Z of X is closed if it is closed under specialization.*

PROOF. Let W be an irreducible component of $\bar{Z}$, and let $\mathfrak{p} = I(W)$; then $W = V(\mathfrak{p})$, i.e., W consists of the specializations of $\mathfrak{p}$. Then $W \cap Z$ is constructible and it is dense in W, and so it contains a nonempty open subset U of W (14.13). Hence $\mathfrak{p} \in U$ and, because Z is closed under specialization, $W \subset Z$. As Z contains all irreducible components of $\bar{Z}$, it contains Z.

PROPOSITION 14.16. *Let A be a noetherian ring, and let $\varphi\colon A \to B$ be a finitely generated A-algebra. If φ satisfies the going-down theorem, then the map $\varphi^a\colon \mathrm{spec}(B) \to \mathrm{spec}(A)$ is open (i.e., sends open subsets to open subsets).*

PROOF. Let U be an open subset of $\mathrm{spec}(B)$, Then $\varphi^a(U)$ is constructible (14.14), and the going-down theorem says that it is closed under generalization. Therefore $\mathrm{spec}(A) \smallsetminus \varphi^a(U)$ is constructible and closed under specialization, and hence closed.

15 Jacobson rings and max spectra

DEFINITION 15.1. 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 $(0) = \bigcap_{p \text{ prime}}(p)$. 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 15.2. *Every finitely generated algebra over a field is Jacobson.*

PROOF. Apply (13.11).

PROPOSITION 15.3. *In a Jacobson ring, the radical of an ideal is equal to the intersection of the maximal ideals containing it. In particular, an element is nilpotent if it is contained in all maximal ideals.*

[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 $p_1, \ldots, p_s$, and so a is contained in only finitely many prime ideals. Similarly, in a Dedekind domain, a nonzero ideal $\mathfrak{a}$ factors as $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_s^{r_s}$ with the $\mathfrak{p}_i$ prime ideals (cf. 20.7 below), and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the only prime ideals containing $\mathfrak{a}$. On taking $\mathfrak{a} = (a)$, we see that again a is contained in only finitely many prime ideals.

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

ASIDE 15.4. Every ring of finite type over a Jacobson ring is a Jacobson ring (EGA IV, 10.4.6).

Max spectra

Let A be ring. The set $\operatorname{spm}(A)$ of maximal ideals in A acquires a topology in exactly the same way as $\operatorname{spec}(A)$. Namely, the closed sets for the topology are the subsets

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

of $\operatorname{spm}(A)$ with $\mathfrak{a}$ an ideal in A.

Everything in §14 holds, with essentially the same proofs, for the max spectra of *Jacobson* rings. For example, in the proof of (14.2), we used that an element of A is nilpotent if it is contained in all prime ideals. The is true with "maximal" for "prime" provided A is Jacobson.

In particular, for 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 15.5. By definition, $\operatorname{spm}(A)$ is the subspace of $\operatorname{spec}(A)$ consisting of the closed points. When A is Jacobson, the map $U \mapsto U \cap \operatorname{spm}(A)$ is a bijection from the set of open subsets of $\operatorname{spec}(A)$ onto the set of open subsets of $\operatorname{spm}(A)$; therefore $\operatorname{spm}(A)$ and $\operatorname{spec}(A)$ have the same topologies — only the underlying sets differ.

ASIDE 15.6. 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.

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

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

on X. When A is reduced, Proposition 13.11 shows that this realizes A as a ring of k-valued functions on X. Moreover, because (45) 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, $\operatorname{spm}(A)$ is the spectrum of A in the sense of analysis.

The max spectrum of a finitely generated k-algebra

Let k be a field, and let A be a finitely generated k-algebra. For every maximal ideal $\mathfrak{m}$ of A, the field $\kappa(\mathfrak{m}) \stackrel{\text{def}}{=} A/\mathfrak{m}$ is a finitely generated k-algebra, and so $\kappa(\mathfrak{m})$ is finite over k (Zariski's lemma, 13.1). In particular, it equals $\kappa(\mathfrak{m}) = k$ when k is algebraically closed.

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

$$\operatorname{Hom}_{k\text{-alg}}(A, k^{\mathrm{al}}) \to \operatorname{spm}(A). \tag{44}$$

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

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

and so differ by an automorphism[20] of k^{al}. Therefore, the fibres of (44) are exactly the orbits of $\mathrm{Gal}(k^{\mathrm{al}}/k)$. When k is perfect, each extension $k(\mathfrak{m})/k$ is separable, and so each orbit has $[k(\mathfrak{m}){:}k]$ elements, and when k is algebraically closed, the map (44) is a bijection.

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

$$V(\mathfrak{a}) \to \mathrm{spm}(A) \tag{45}$$

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

Maps of max spectra

Let $\varphi\colon A \to B$ be a homomorphism of rings, and let $\mathfrak{p}$ be a prime ideal of B. Then $B/\mathfrak{p}$ is an integral domain and $A/\varphi^{-1}(\mathfrak{p}) \to B/\mathfrak{p}$ is injective, and so $\varphi^{-1}(\mathfrak{p})$ is a prime ideal in A. In this way, spec becomes a functor from rings to topological spaces. Unfortunately, when $\mathfrak{p}$ is maximal, $\varphi^{-1}(\mathfrak{p})$ need not be maximal — consider for example the inclusion map $\mathbb{Z} \to \mathbb{Q}$ and the ideal (0) in $\mathbb{Q}$. Therefore, spm is not a functor on the category of all rings, but it is a functor on the category of finitely generated over a fixed field.

LEMMA 15.7. *Let $\varphi\colon A \to B$ be a homomorphism of k-algebras, and let $\mathfrak{m}$ be a maximal ideal in B. If B is finitely generated over k, then the ideal $\varphi^{-1}(\mathfrak{m})$ is maximal in A.*

PROOF. 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, 13.1). Therefore the image of A in $B/\mathfrak{m}$ is an integral domain finite over k, and hence is a field (see §1). As this image is isomorphic to $A/\varphi^{-1}(\mathfrak{m})$, this shows that the ideal $\varphi^{-1}(\mathfrak{m})$ is maximal in A.

Therefore φ defines a map

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

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

THEOREM 15.8. *Let $\varphi\colon A \to B$ be a homomorphism of finitely generated k-algebras. Let U be a nonempty open subset of $\mathrm{spm}(B)$, and let $\varphi^*(U)^-$ be the closure of its image in $\mathrm{spm}(A)$. Then $\varphi^*(U)$ contains a nonempty open subset of each irreducible component of $\varphi^*(U)^-$.*

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

We first prove the theorem in the case that φ is an injective homomorphism of integral domains. For some $b \neq 0$, $D(b) \subset U$. According to Proposition 15.9 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 $W_1, \ldots, W_r$ are the irreducible components of W, then $\varphi^*(W)^-$ is a union of the sets $\varphi^*(W_i)^-$, and any irreducible component C of $\varphi^*(U)^-$ is contained in one of $\varphi^*(W_i)^-$, say $\varphi^*(W_1)^-$. Let $\mathfrak{q} = I(W_1)$ and let $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$. Because W_1 is irreducible, they are both prime ideals. The homomorphism $\varphi: A \to B$ 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 15.9. *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 15.10. *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 15.9). 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} with the property that every 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 15.11. 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. Atiyah and Macdonald 1969 5.23, p.66).

ASIDE 15.12. Let A be a noetherian ring, and let $\varphi\colon A \to B$ be a finitely generated A-algebra. Then the statement of (15.8) holds for $\varphi^*\colon \mathrm{spm}(B) \to \mathrm{spm}(A)$ with much the same proof.

ASIDE 15.13. Let A be a ring and $\varphi\colon A \to B$ a finitely generated A-algebra. If A is Jacobson, so also is B, and φ induces a map $\mathrm{spm}(B) \to \mathrm{spm}(A)$.

ASIDE 15.14. In general, the map $A \to A[X]$ does not induce a map $\mathrm{spm}(A[X]) \to \mathrm{spm}(A)$. 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.

ASIDE 15.15. There exists a local integral domain A whose prime ideals form a single infinite chain $(0) = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{m}$. The open subscheme $\mathrm{spec}(A) \smallsetminus \{\mathfrak{m}\}$ of $\mathrm{spec}(A)$ has no closed points.

Exercises

EXERCISE 15.16. Let A denote the polynomial ring $\mathbb{Q}[X_1, X_2, \ldots]$ in countably many symbols.

(a) Show that A is not a Jacobson ring (consider the kernel of a surjective homomorphism from A to a countable local domain, e.g., $\mathbb{Q}[X]_{(X)}$).

(b) Show that $(0) = \bigcap\{\mathfrak{m} \mid \mathfrak{m} \text{ a maximal ideal in } A\}$.

See mo151011.

16 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 16.1. *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. Let a be a nonzero element 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, and so A' is a field, and $\mathfrak{p}$ is maximal.

COROLLARY 16.2. *In an artinian ring, the nilradical and the Jacobson radical coincide.*

PROOF. The first is the intersection of the prime ideals (2.5), and the second is the intersection of the maximal ideals (2.6).

PROPOSITION 16.3. *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 16.4. *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 choose an $\mathfrak{a}$ that is 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 16.5. *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 $M_r \overset{\text{def}}{=} \mathfrak{m}_1 \cdots \mathfrak{m}_{r-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_r$ 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 16.6. *A ring is artinian if and only if it is noetherian of dimension zero.*

PROOF. $\Rightarrow$: Let A be an artinian ring. After (16.1), it remains to show that A is noetherian, but according to (16.2), (16.3), and (16.4), some finite product of maximal ideals is zero, and so this follows from Lemma 16.5.

$\Leftarrow$: Let A be a noetherian ring of dimension zero. Because A is noetherian, its radical $\mathfrak{N}$ is a finite intersection of prime ideals (14.9), each of which is maximal because $\dim A = 0$. Hence $\mathfrak{N}$ is a finite intersection of maximal ideals (2.5), and since some power of $\mathfrak{N}$ is zero (3.17), we again have that some finite product of maximal ideals is zero, and so can apply Lemma 16.5.

THEOREM 16.7. *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 (16.6) 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 2.13 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 16.8. *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 16.4); 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 16.9. 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 16.10. Every finitely generated module over a principal Artin ring is a direct sum of cyclic modules (see mo22722).

17 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 17.1. *Let B be a finitely generated k-algebra. A prime ideal $\mathfrak{q}$ of B is an isolated point of spec(B) if and only if $B_{\mathfrak{q}}$ is finite over k.*

PROOF. To say that $\mathfrak{q}$ is an isolated point of spec(B) means that there exists an $f\in B\smallsetminus\mathfrak{q}$ such that spec$(B_f)=\{\mathfrak{q}\}$. Now B_f is noetherian with only one prime ideal, namely, $\mathfrak{m}\overset{\text{def}}{=}\mathfrak{q}B_f$, and so it is artinian (16.6). 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 13.1). 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.

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

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

$$0 \to M \to B \to B_{\mathfrak{q}} \to N \to 0 \tag{46}$$

of B-modules. When we apply the functor $S_{\mathfrak{q}}^{-1}$ to the sequence (46), 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 $f' \overset{\text{def}}{=} f_1 \ldots f_m$ 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 $f \overset{\text{def}}{=} f'f'' \in B \smallsetminus \mathfrak{q}$ has the property that $M_f = 0 = N_f$. When we apply the functor S_f^{-1} to (46), 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.

PROPOSITION 17.2. *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 (16.7)

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

and

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

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 14.3) with $B_{f_i} = B_{\mathfrak{q}_i}$. According to Proposition 17.1, each k-algebra $B_{\mathfrak{q}_i}$ is finite over k, and so B is finite over k.

DEFINITION 17.3. 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 17.4. *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 (17.1) 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 17.5. *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 Proposition 17.2.

EXAMPLE 17.6. 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, $\operatorname{spec}(C \otimes_A \kappa(\mathfrak{p}))$ is discrete for all primes $\mathfrak{p}$ of A, 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 17.7. *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 17.8. *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 7.1), and it is finitely generated as an

$A/\mathfrak{p}$-algebra. Zariski's lemma (13.1) 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 (17.3)).

ASIDE 17.9. 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 17.10. *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 17.11. *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 17.12. *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 (17.11) shows that there exists an A-subalgebra A'' of A', finite over A, which contains $f_1, \ldots, f_n$ 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 17.10, its corollary 17.12, and various global versions of these statements are referred to as Zariski's main theorem.

A variant of Zariski's main theorem

PROPOSITION 17.13. *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 17.13 IMPLIES 17.10

Let A, A', and B be as in the Theorem 17.10. We apply the proposition to $A' \subset B = B$ — Lemma 17.7 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 $b_1, \ldots, b_n$ 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 17.10

We proceed by proving four special cases of Proposition 17.10.

LEMMA 17.14. *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

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

By assumption, $\mathfrak{q}$ is an isolated point in $\operatorname{spec}(k[\bar{x}])$. Consequently, $\bar{x}$ is algebraic over k, because otherwise $k[\bar{x}]$ 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 17.15. *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 every 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 (7.6) 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 (6.17), and the going down theorem (7.11) 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 7.5), 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 7.4 to $B \subset B'$). But, according to the preceding paragraph, $\mathfrak{q}'$ is not minimal, which implies that $\mathfrak{q}$ is not minimal (apply 7.4 again).

LEMMA 17.16. *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 $c = b - Q(x)$,

$$F(x)c = R(x). \tag{47}$$

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 (47) 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 every multiplicative subset S of A,

$$\mathfrak{f}(S^{-1}B/S^{-1}A) = S^{-1}\mathfrak{f}(B/A). \tag{48}$$

LEMMA 17.17. *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 every $u \in \mathfrak{f} \smallsetminus \mathfrak{q}$, we have $A[x]_u = B_u$, and so Lemma 17.8 shows that $A[x]$ is quasi-finite over A at $\mathfrak{r}$.[23] Now Lemma 17.14 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 17.15 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 (7.3) 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 $\mathfrak{f}_{\mathfrak{n}}$. 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 17.16 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 17.10

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.

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

Write $C = A[x_1,\ldots,x_n]$, and let A' be the integral closure of $A[x_1,\ldots,x_{n-1}]$ 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 17.7). From Lemma 17.17 we deduce that $A'_{\mathfrak{p}'} = B_{\mathfrak{p}'}$ with $\mathfrak{p}' = A' \cap \mathfrak{q}$.

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

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

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

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

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, $A[x_1,\ldots,x_{n-1}]$, 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 17.13 and hence of Theorem 17.10.

18 Dimension theory for finitely generated k-algebras

Except in the final subsection, A is an integral domain containing a field k and finitely generated as a k-algebra. 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 $F(A)$ of A (see §9 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 18.1. *For all linear forms $\ell_1,\ldots,\ell_m$ in $X_1,\ldots,X_n$, the quotient ring*

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

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

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

PROOF. This follows from the more precise statement:

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

This is obvious if the forms ℓ_i are $X_1,\ldots,X_r$. In the general case, because $\{X_1,\ldots,X_n\}$ and $\{\ell_1,\ldots,\ell_r,X_{i_1},\ldots,X_{i_{n-r}}\}$ are both bases for the linear forms, each element of one set can be expressed as a linear combination of the elements of the other. Therefore,

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

and so

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

PROPOSITION 18.2. *For every irreducible polynomial f in $k[X_1,\ldots,X_n]$, the quotient ring $k[X_1,\ldots,X_n]/(f)$ has transcendence degree $n-1$.*

PROOF. Let
$$k[x_1,\ldots,x_n]=k[X_1,\ldots,X_n]/(f),\quad x_i=X_i+(f),$$
and let $k(x_1,\ldots,x_n)$ be the field of fractions of $k[x_1,\ldots,x_n]$. Since f is not zero, some X_i, say, X_n, occurs in it. Then X_n occurs in every nonzero multiple of f, and so no nonzero polynomial in $X_1,\ldots,X_{n-1}$ belongs to (f). This means that $x_1,\ldots,x_{n-1}$ are algebraically independent. On the other hand, x_n is algebraic over $k(x_1,\ldots,x_{n-1})$, and so $\{x_1,\ldots,x_{n-1}\}$ is a transcendence basis for $k(x_1,\ldots,x_n)$ over k.

PROPOSITION 18.3. *For every nonzero prime ideal $\mathfrak{p}$ in a k-algebra A,*

$$\operatorname{trdeg}_k(A/\mathfrak{p})<\operatorname{trdeg}_k(A).$$

PROOF. We may suppose that

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

For $f\in A$, let $\bar{f}$ denote the image of f in $A/\mathfrak{p}$, so that $A/\mathfrak{p}=k[\bar{x}_1,\ldots,\bar{x}_n]$. Let $d=\operatorname{trdeg}_k A/\mathfrak{p}$, and number the X_i so that $\bar{x}_1,\ldots,\bar{x}_d$ are algebraically independent (for a proof that this is possible, see 8.9 of my notes Fields and Galois Theory). I shall show that, for any nonzero $f\in\mathfrak{p}$, the $d+1$ elements $x_1,\ldots,x_d,f$ are algebraically independent, which shows that $\operatorname{trdeg}_k A\geq d+1$.

Suppose otherwise. Then there is a nontrivial algebraic relation, which we can write

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

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

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

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

PROPOSITION 18.4. *Let A be a polynomial ring. If $\mathfrak{p}$ is a prime ideal in A such that $\operatorname{trdeg}_k A/\mathfrak{p}=\operatorname{trdeg}_k A-1$, 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

$$\operatorname{tr}\deg_k A/\mathfrak{p} \overset{18.3}{>} \operatorname{tr}\deg_k A/(f) \overset{18.2}{=} \operatorname{tr}\deg_k A - 1,$$

which contradicts the hypothesis.

THEOREM 18.5. *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 18.6. *Let A be an integrally closed integral domain, and let L be a finite extension of the field of fractions K of A. If $\alpha \in L$ is integral over A, then $\operatorname{Nm}_{L/K}\alpha \in A$, and α divides $\operatorname{Nm}_{L/K}\alpha$ in the ring $A[\alpha]$.*

PROOF. Let $X^r + a_{r-1}X^{r-1} + \cdots + a_0$ be the minimum polynomial of α over K. Then r divides the degree n of L/K, and $\operatorname{Nm}_{L/K}(\alpha) = \pm a_0^{\frac{n}{r}}$ (see 5.40 of my notes Fields and Galois Theory). Moreover, a_0 lies in A by (6.11). From the equation

$$0 = \alpha(\alpha^{r-1} + a_{r-1}\alpha^{r-2} + \cdots + a_1) + a_0$$

we see that α divides a_0 in $A[\alpha]$, and therefore it also divides $\operatorname{Nm}_{L/K}\alpha$.

PROOF (OF THEOREM 18.5). Write $\operatorname{rad}(f)$ as an irredundant intersection of prime ideals $\operatorname{rad}(f) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ (see 14.9). 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, $\operatorname{rad}(\frac{f}{1}) = \operatorname{rad}(f)^e = \mathfrak{p}_1^e$. Therefore, after replacing A with A_h, we may suppose that $\operatorname{rad}(f)$ is prime, say, equal to $\mathfrak{p}$.

According to the Noether normalization theorem (8.1), there exist algebraically independent elements $x_1, \ldots, x_d$ in A such that A is a finite $k[x_1, \ldots, x_d]$-algebra. Note that $d = \operatorname{tr}\deg_k A$. According to the lemma, $f_0 \overset{\text{def}}{=} \operatorname{Nm}(f)$ lies in $k[x_1, \ldots, x_d]$, and we shall show that $\mathfrak{p} \cap k[x_1, \ldots, x_d] = \operatorname{rad}(f_0)$. Therefore, the homomorphism

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

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

$$\operatorname{tr}\deg_k A/\mathfrak{p} = \operatorname{tr}\deg_k k[x_1, \ldots, x_d]/\operatorname{rad}(f_0) \overset{18.2}{=} d - 1,$$

as required.

By assumption A is finite (hence integral) over its subring $k[x_1, \ldots, x_d]$. The lemma shows that f divides f_0 in A, and so $f_0 \in (f) \subset \mathfrak{p}$. Hence $(f_0) \subset \mathfrak{p} \cap k[x_1, \ldots, x_d]$, which implies

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

because $\mathfrak{p}$ is radical. For the reverse inclusion, let $g \in \mathfrak{p} \cap k[x_1,\dots,x_d]$. 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 18.7. *Let $\mathfrak{p}$ be a minimal nonzero prime ideal in A; then* $\operatorname{tr}\deg_k(A/\mathfrak{p}) = \operatorname{tr}\deg_k(A) - 1$.

PROOF. Let f be a nonzero element of $\mathfrak{p}$. Then f is not a unit, and $\mathfrak{p}$ is minimal among the prime ideals containing f.

THEOREM 18.8. *The length d of every maximal (i.e., nonrefinable) chain of distinct prime ideals*

$$\mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0 \tag{49}$$

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 Corollary 18.7, 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 18.9. 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 18.10. 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 18.4). 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 18.11. 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 18.12. 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. 15.14).

A short proof that the Krull dimension equals the transcendence degree

The following proof shortens that in Coquand and Lombardi, Amer. Math. Monthly 112 (2005), no. 9, 826–829.

Let A be an arbitrary commutative ring. Let $x \in A$, and let $S_{\{x\}}$ denote the multiplicative subset of A consisting of the elements of the form

$$x^n(1-ax), \quad n \in \mathbb{N}, \quad a \in A.$$

The ***boundary*** $A_{\{x\}}$ of A at x is defined to be the ring of fractions $S_{\{x\}}^{-1}A$.

We write $\dim(A)$ for the Krull dimension of A.

PROPOSITION 18.13. *Let A be a ring and let $n \in \mathbb{N}$. Then*

$$\dim(A) \le n \iff \textit{for all } x \in A,\ \dim(A_{\{x\}}) \le n-1.$$

PROOF. Recall (5.4) that $\operatorname{Spec}(S^{-1}A) \simeq \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}$. We shall need the following statements.

(a) *For every $x \in A$ and maximal ideal $\mathfrak{m} \subset A$, $\mathfrak{m} \cap S_{\{x\}} \neq \emptyset$.* Indeed, if $x \in \mathfrak{m}$, then $x \in \mathfrak{m} \cap S$; otherwise x is invertible modulo $\mathfrak{m}$, and so there exists an $a \in A$ such that $1-ax \in \mathfrak{m}$.

(b) *Let $\mathfrak{m}$ be a maximal ideal, and let $\mathfrak{p}$ be a prime ideal contained in m; for every $x \in \mathfrak{m} \smallsetminus \mathfrak{p}$, we have $\mathfrak{p} \cap S_{\{x\}} = \emptyset$.* Indeed, if $x^n(1-ax) \in \mathfrak{p}$, then $1-ax \in \mathfrak{p}$ (as $x \notin \mathfrak{p}$); hence $1-ax \in \mathfrak{m}$, and so $1 \in \mathfrak{m}$, which is a contradiction.

Statement (a) shows that every chain of prime ideals beginning with a maximal ideal is shortened when passing from A to $A_{\{x\}}$, while statement (b) shows that a maximal chain of length n is shortened only to $n-1$ when x is chosen appropriately. From this, the proposition follows.

PROPOSITION 18.14. *Let $k \subset F \subset E$ be fields. Then*

$$\text{tr deg}_k E = \text{tr deg}_k F + \text{tr deg}_F E.$$

PROOF. More precisely, if B and C are transcendence bases for F/k and E/F respectively, then $B \cup C$ is a transcendence basis for E/k. This is easy to check (see, for example, Jacobson, Lectures in Abstract Algebra III, 1964, Exercise 3, p.156).

PROPOSITION 18.15. *Let A be an integral domain with field of fractions $F(A)$, and let k be a subfield of A. Then*

$$\text{tr deg}_k F(A) \ge \dim(A).$$

PROOF. If $\text{tr deg}_k F(A) = \infty$, there is nothing to prove, and so we assume that $\text{tr deg}_k F(A) = n \in \mathbb{N}$. We argue by induction on n. We can replace k with its algebraic closure in A without changing $\text{tr deg}_k F(A)$. Let $x \in A$. If $x \notin k$, then it is transcendental over k, and so

$$\text{tr deg}_{k(x)} F(A) = n-1$$

by (18.14); since $k(x) \subset A_{\{x\}}$, this implies (by induction) that $\dim(A_{\{x\}}) \le n-1$. If $x \in k$, then $0 = 1 - x^{-1}x \in S_{\{x\}}$, and so $A_{\{x\}} = 0$; again $\dim(A_{\{x\}}) \le n-1$. Now (18.13) shows that $\dim(A) \le n$.

COROLLARY 18.16. *The polynomial ring $k[X_1,\ldots,X_n]$ has Krull dimension n.*

PROOF. The existence of the sequence of prime ideals

$$(X_1,\ldots,X_n) \supset (X_1,\ldots,X_{n-1}) \supset \cdots \supset (X_1) \supset (0)$$

shows that $k[X_1,\ldots,X_n]$ has Krull dimension at least n. Now(18.15) completes the proof.

THEOREM 18.17. *Let A be an integral domain containing a field k and finitely generated as a k-algebra. Then*

$$\text{tr deg}_k F(A) = \dim(A).$$

PROOF. According to the Noether normalization theorem (8.1), A is integral over a polynomial subring $k[x_1,\ldots,x_n]$. Clearly $n =$tr $\deg_k F(A)$. From the going-up theorem (7.7), $\dim(A) \geq \dim(k[x_1,\ldots,x_n]) = n$, and so $\dim(A) = n$ (18.15).

19 Primary decompositions

DEFINITION 19.1. An ideal $\mathfrak{q}$ in A is ***primary*** if it is $\neq A$ 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 every zero-divisor in $A/\mathfrak{q}$ is nilpotent. Therefore, a radical ideal is primary if and only if it is prime, and an ideal (m) in $\mathbb{Z}$ is primary if and only if m is a power of a prime.

PROPOSITION 19.2. *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 $\mathfrak{q}$).*

PROOF. Suppose that $ab \in \text{rad}(\mathfrak{q})$ but $b \notin \text{rad}(\mathfrak{q})$. Some power, say $a^m b^m$, of ab lies xin $\mathfrak{q}$, but $b^m \notin \mathfrak{q}$, and so $(a^m)^n \in \mathfrak{q}$ for some n. Hence, $a \in \text{rad}(\mathfrak{q})$. Therefore $\text{rad}(\mathfrak{q})$ is prime.

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 $a \in \mathfrak{p}$. Therefore $\mathfrak{p} \supset \text{rad}(\mathfrak{q})$.

When $\mathfrak{q}$ is a primary ideal and $\mathfrak{p}$ is its radical, we say that $\mathfrak{q}$ is ***$\mathfrak{p}$-primary.*** Note that this means that if $ab \in \mathfrak{q}$, then either $b \in \mathfrak{q}$ or $a \in \mathfrak{p}$ (or both).

PROPOSITION 19.3. *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 $A/\mathfrak{q}$ is local with maximal ideal $\mathfrak{m}/\mathfrak{q}$. Therefore, every element of $A/\mathfrak{q}$ is either a unit, and hence is not a zero-divisor, or it lies in $\mathfrak{m}/\mathfrak{q}$, and hence is nilpotent.

PROPOSITION 19.4. *Let $\varphi\colon A \to B$ be a homomorphism of rings. If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in B, then $\mathfrak{q}^c \overset{\text{def}}{=} \varphi^{-1}(\mathfrak{q})$ is a $\mathfrak{p}^c$-primary ideal in A.*

PROOF. The map $A/\mathfrak{q}^c \to B/\mathfrak{q}$ is injective, and so every zero-divisor in $A/\mathfrak{q}^c$ is nilpotent. This shows that $\mathfrak{q}^c$ is primary, and it remains to show that $\mathrm{rad}(\mathfrak{q}^c) = \mathfrak{p}^c$. But

$$\mathrm{rad}(\mathfrak{q}^c) \overset{2.11}{=} \mathrm{rad}(\mathfrak{q})^c = \mathfrak{p}^c$$

as claimed.

LEMMA 19.5. *Let $\mathfrak{q}$ and $\mathfrak{p}$ be ideals in A such that*
(a) $\mathfrak{q} \subset \mathfrak{p} \subset \mathrm{rad}(\mathfrak{q})$ *and*
(b) $ab \in \mathfrak{q} \implies a \in \mathfrak{p}$ *or* $b \in \mathfrak{q}$.
Then $\mathfrak{p}$ is a prime ideal and $\mathfrak{q}$ is $\mathfrak{p}$-primary.

PROOF. Clearly $\mathfrak{q}$ is primary, hence $\mathrm{rad}(\mathfrak{q})$-primary, and $\mathrm{rad}(\mathfrak{q})$ is prime. By assumption $\mathfrak{p} \subset \mathrm{rad}(\mathfrak{q})$, and it remains to show that they are equal. Let $a \in \mathrm{rad}(\mathfrak{q})$, and let n be the smallest positive integer such that $a^n \in \mathfrak{q}$. If $n = 1$, then $a \in \mathfrak{q} \subset \mathfrak{p}$; on the other hand, if $n > 1$, then $a^n = aa^{n-1} \in \mathfrak{q}$ and $a^{n-1} \notin \mathfrak{q}$, and so $a \in \mathfrak{p}$ by (b).

PROPOSITION 19.6. *A finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

PROOF. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be $\mathfrak{p}$-primary, and let $\mathfrak{q} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$. We show that the pair of ideals $\mathfrak{q} \subset \mathfrak{p}$ satisfies the conditions of (19.5).

Let $a \in \mathfrak{p}$. Then some power of a, say, a^{n_i}, lies in $\mathfrak{q}_i$, and $a^{\max(n_i)} \in \bigcap \mathfrak{q}_i = \mathfrak{q}$. Therefore $\mathfrak{p} \subset \mathrm{rad}(\mathfrak{q})$.

Let $ab \in \mathfrak{q}$, so $ab \in \mathfrak{q}_i$ all i. If $a \notin \mathfrak{p}$, then $b \in \mathfrak{q}_i$ all i, and so $b \in \mathfrak{q}$.

The ***minimal prime ideals*** of an ideal $\mathfrak{a}$ are the minimal elements of the set of prime ideals containing $\mathfrak{a}$.

DEFINITION 19.7. A ***primary decomposition*** of an ideal $\mathfrak{a}$ is a finite set of primary ideals whose intersection is $\mathfrak{a}$. Such a decomposition S of $\mathfrak{a}$ is ***minimal*** if
(a) the prime ideals $\mathrm{rad}(\mathfrak{q})$, $\mathfrak{q} \in S$, are distinct, and
(b) no element of S can be omitted, i.e., for no $\mathfrak{q} \in S$ does $\mathfrak{q} \supset \bigcap\{\mathfrak{q}' \mid \mathfrak{q}' \in S, \mathfrak{q}' \neq \mathfrak{q}\}$.

If $\mathfrak{a}$ admits a primary decomposition, then it admits a minimal primary decomposition, because Proposition 19.6 can be used to combine primary ideals with the same radical, and any $\mathfrak{q}$ 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 19.8. *Suppose that $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary for $i = 1, \ldots, n$. Then the minimal prime ideals of $\mathfrak{a}$ are the minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.*

PROOF. Let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{a}$. Then $\mathfrak{p}$ is a prime ideal containing $\mathfrak{q}_1 \cdots \mathfrak{q}_n$, and so $\mathfrak{p}$ contains one of the ideals $\mathfrak{q}_i$ (2.1b). Now Proposition 19.2 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 nilradical is a *finite* intersection of prime ideals (which is always the case for noetherian rings, see 14.9).

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 contains $\mathfrak{a}$, and equals A if $x \in \mathfrak{a}$.

LEMMA 19.9. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal and let $x \in A \smallsetminus \mathfrak{q}$. Then $(\mathfrak{q}\colon x)$ is $\mathfrak{p}$-primary.*

PROOF. Let $a \in (\mathfrak{q}\colon x)$; then $ax \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, and so $a \in \mathfrak{p}$. Therefore $\mathfrak{p} \supset (\mathfrak{q}\colon x) \supset \mathfrak{q}$. On taking radicals, we find that $\mathrm{rad}(\mathfrak{q}\colon x) = \mathfrak{p}$.

Let $ab \in (\mathfrak{q}\colon x)$, so that $abx \in \mathfrak{q}$. If $a \notin \mathfrak{p}$, then $bx \in \mathfrak{q}$, and so $b \in (\mathfrak{q}\colon x)$. Therefore, $(\mathfrak{q}\colon x)$ is primary, and hence $\mathfrak{p}$-primary.

THEOREM 19.10. *Let $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ be a minimal primary decomposition of $\mathfrak{a}$, and let $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$. Then*

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \{\mathrm{rad}(\mathfrak{a}\colon x) \mid x \in A, \quad \mathrm{rad}(\mathfrak{a}\colon x) \text{ prime}\}.$$

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

PROOF. For every $a \in A$,

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

and so

$$\mathrm{rad}(\mathfrak{a}\colon a) = \mathrm{rad}\left(\bigcap (\mathfrak{q}_i\colon a)\right) = \bigcap \mathrm{rad}(\mathfrak{q}_i\colon a).$$

Now $\mathrm{rad}(\mathfrak{q}_i\colon a) = \mathfrak{p}_i$ or A according as $a \notin \mathfrak{q}_i$ or $a \in \mathfrak{q}_i$ (19.9), and so

$$\mathrm{rad}(\mathfrak{a}\colon a) = \bigcap_{i \text{ such that } a \notin \mathfrak{q}_i} \mathfrak{p}_i. \tag{50}$$

If $\mathrm{rad}(\mathfrak{a}\colon a)$ is prime, then it contains one of the $\mathfrak{p}_i$ (2.1), and hence equals it, i.e.,

$$\mathrm{rad}(\mathfrak{a}\colon a) \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}.$$

On the other hand, 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 (50) shows that $\mathrm{rad}(\mathfrak{a}\colon a) = \mathfrak{p}_i$.

An ideal $\mathfrak{a}$ is said to be ***irreducible*** if it cannot be expressed as the intersection of two strictly large ideals, i.e., if

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \; (\mathfrak{b}, \mathfrak{c} \text{ ideals}) \implies \mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}.$$

THEOREM 19.11. *In a noetherian ring A, every ideal admits a primary decomposition. More precisely:*

(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) Let S be the set of ideals for which (a) fails. If S is empty, then (a) is true. Otherwise, it contains a maximal element $\mathfrak{a}$. Then $\mathfrak{a}$ itself is not irreducible, and so $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{b}$ and $\mathfrak{c}$ properly containing $\mathfrak{a}$. As $\mathfrak{a}$ is maximal in S, 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

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

becomes constant, say,

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

Let $c \in (b) \cap (a^m)$. Because $c \in (b)$, $ca = 0$, and because $c \in (a^m)$, $c = da^m$ for some $d \in A$. But

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

and so $(b) \cap (a^m) = (0)$. Because $\mathfrak{a}$ is irreducible, the zero ideal in A' is irreducible, and it follows that $a^m = 0$.

A $\mathfrak{p}$-primary ideal $\mathfrak{q}$ in a noetherian ring contains a power of $\mathfrak{p}$ by Proposition 3.17. The next result proves a converse when $\mathfrak{p}$ is maximal.

PROPOSITION 19.12. *Let $\mathfrak{m}$ be a maximal ideal of a noetherian ring. Every 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 19.13. 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 19.14. Let $\mathfrak{a}$ be an ideal in a noetherian ring, and let $\mathfrak{b} = \bigcap_{n\geq 1} \mathfrak{a}^n$. We give another proof that $\mathfrak{a}\mathfrak{b} = \mathfrak{b}$ (see p. 13). Let

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

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

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

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

from which it follows that $\mathfrak{a} \subset \mathfrak{p}_i$. We know that $\mathfrak{p}_i^r \subset \mathfrak{q}_i$ for some r (see 3.17), 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.

Primary decompositions for modules

Let M be a module over a ring A. The statements for modules below can be proved as for ideals, or deduced from them by considering the ring $A \oplus M$ (see 2.14).

For a submodule N of M, let

$$(N{:}M) = \{a \in A \mid aM \subset N\}.$$

It is an ideal in A. Let

$$r_M(N) = \operatorname{rad}((N{:}M)) = \{a \in A \mid a^n M \subset N \text{ for some } n \geq 0\}.$$

An element a of A is a ***zero divisor*** of M if $ax = 0$ for some nonzero $x \in M$, and it is ***nilpotent*** on M if $a^n M = 0$ for some n. A submodule Q of M is ***primary*** if every zero divisor of M/Q is nilpotent on M/Q.

PROPOSITION 19.15. *If Q is a primary submodule of M, then $(Q{:}M)$ is a primary ideal, and so $r_M(Q)$ is a prime ideal $\mathfrak{p}$. We say that Q is **$\mathfrak{p}$-primary** in M.*

For simplicity, we now assume that A is noetherian and that M is finitely generated.

A prime ideal of A is an ***associated prime ideal*** of M if it is the annihilator $\operatorname{ann}(x)$ of an element of M. We write $\operatorname{Ass}(M)$ for the set of associated prime ideals of M.

PROPOSITION 19.16. *A submodule Q of M is primary if and only if $\operatorname{Ass}(M/Q)$ consists of a single element $\mathfrak{p}$, in which case $\mathfrak{p} = r_M(Q)$.*

PROPOSITION 19.17. *A finite intersection of $\mathfrak{p}$-primary submodules is $\mathfrak{p}$-primary.*

A ***primary decomposition*** of a submodule N is a finite set of primary submodules whose intersection is N. A primary decomposition S is ***minimal*** if

(a) the prime ideals $r_M(Q)$, $Q \in S$, are distinct, and
(b) no element of S can be omitted, i.e., for no $Q \in S$ does $Q \supset \bigcap\{Q' \mid Q' \in S,\ Q' \neq Q\}$.

If N admits a primary decomposition, then it admits a minimal primary decomposition, because Proposition 19.17 can be used to combine submodules with the same $\mathfrak{p}$, and any Q that fails (b) can simply be omitted.

A submodule of M is ***irreducible*** it cannot be expressed as the intersection of two strictly larger submodules.

THEOREM 19.18. *Every submodule of M (as above) admits a primary decomposition. More precisely:*

(a) *Every submodule of M can be expressed as a finite intersection of irreducible submodules.*
(b) *Every irreducible submodule in M is primary.*

THEOREM 19.19. *Let N be a submodule of M. Let $N = Q_1 \cap \ldots \cap Q_n$ be a minimal primary decomposition of N, and let $\mathfrak{p}_i = r_M(Q_i)$. Then*

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \operatorname{Ass}(M/N).$$

In particular, the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ is independent of the choice of the minimal primary decomposition. Its elements are called the prime ideals ***belonging*** to N (in M).

20 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) A has exactly one prime element up to associates;
(c) A is local and is not a field.
A ring satisfying these conditions is called a ***discrete valuation ring***.

EXAMPLE 20.1. The ring $\mathbb{Z}_{(p)} \overset{\text{def}}{=} \{\frac{m}{n} \in \mathbb{Q} \mid n \text{ not divisible by } p\}$ 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

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

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

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

Thus, a b for which $\operatorname{ann}(b + (c))$ is maximal, is of the form $v\pi^{m-1}$, and for this choice $\operatorname{ann}(b + (c))$ 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 20.2. *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 $M \overset{\text{def}}{=} A/(c)$. 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 $\mathfrak{a}\pi^{-m-1} \not\subset A$. Then $\mathfrak{a}\pi^{-m} \not\subset \mathfrak{p}$, and so $\mathfrak{a}\pi^{-m} = A$. Hence $\mathfrak{a} = (\pi^m)$.

Dedekind domains

DEFINITION 20.3. 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 20.2 says that a local integral domain is a Dedekind domain if and only if it is a discrete valuation ring.

PROPOSITION 20.4. *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 Proposition 5.4 shows that it holds for $S^{-1}A$. Conditions (a) and (b) follow from the next lemma.

PROPOSITION 20.5. *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 6.15.)

COROLLARY 20.6. *For every nonzero prime ideal $\mathfrak{p}$ in a Dedekind domain A, the localization $A_{\mathfrak{p}}$ is a discrete valuation ring.*

PROOF. We saw in Example 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 20.7. *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 20.8. 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 20.9. *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 $\mathfrak{a}A_{\mathfrak{p}_i} = \mathfrak{p}_i^{r_i} A_{\mathfrak{p}_i}$ and $\mathfrak{a}A_{\mathfrak{p}_i} = \mathfrak{p}_i^{r_i} A_{\mathfrak{p}_i}$

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

(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 20.10. *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 Theorem 20.7, to show that A is principal, it suffices to show that the prime ideals are principal. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be these ideals. Choose an element $x_1 \in \mathfrak{p}_1 \smallsetminus \mathfrak{p}_1^2$. According to the Chinese Remainder Theorem (2.13), 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 20.9).

COROLLARY 20.11. *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 20.12. *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 Corollary 20.11 to $\mathfrak{a} \supset (a)$.

COROLLARY 20.13. *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 20.11) 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 20.14. *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 4.4) 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.

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 20.15. *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.

PROOF. (a) 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 so M is projective (12.6). From a surjective homomorphism $A^r \to M$, we get a homomorphism $M \to A^r$ whose composite with some projection $A^r \to A$ will be nonzero, and hence have image a nonzero 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.

(b) Omitted.

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 20.16 (INVARIANT FACTOR THEOREM). *Let $M \supset N$ be finitely generated torsion-free A-modules of the same rank m. Then there exist elements $e_1, ..., e_m$ of M, fractional ideals $\mathfrak{a}_1, ..., \mathfrak{a}_m$, and integral ideals $\mathfrak{b}_1 \supset \mathfrak{b}_2 \supset ... \supset \mathfrak{b}_m$ such that*

$$M = \mathfrak{a}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m e_m, \quad N = \mathfrak{a}_1 \mathfrak{b}_1 e_1 \oplus \cdots \oplus \mathfrak{a}_m \mathfrak{b}_m e_m.$$

PROOF. Omitted.

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.

ASIDE 20.17. 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.

21 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. 2.10). Recall (5.7) that $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}^e\overset{\text{def}}{=}\mathfrak{p}A_{\mathfrak{p}}$. 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 21.1. *The ideal $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.*

PROOF. According to Proposition 19.3, the ideal $(\mathfrak{p}^e)^n$ is $\mathfrak{p}^e$-primary. Hence (see 19.4), $((\mathfrak{p}^e)^n)^c$ is $(\mathfrak{p}^e)^c$-primary. But $\mathfrak{p}^{ec}=\mathfrak{p}$ (see 5.4), and

$$(((\mathfrak{p}^e)^n)^c\overset{2.11}{=}((\mathfrak{p}^n)^e)^c\overset{\text{def}}{=}\mathfrak{p}^{(n)}. \tag{51}$$

LEMMA 21.2. *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

$$\mathfrak{p}'=\mathfrak{p}'^{ec}\supsetneqq\mathfrak{p}''^c\supset\mathfrak{a}^{ec}\supset\mathfrak{a}$$

contradicts the minimality of $\mathfrak{p}'$.

THEOREM 21.3 (KRULL'S PRINCIPAL IDEAL THEOREM). *Let A be a noetherian ring. For every 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 21.2, $\mathfrak{p}^e$ is a minimal prime ideal of $(b)^e=(\frac{b}{1})$, and Proposition 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 16.6). 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

$$\mathfrak{p}_1^{(s)}+(b)=\mathfrak{p}_1^{(s+1)}+(b)=\mathfrak{p}_1^{(s+2)}+(b)=\cdots. \tag{52}$$

We claim that, for every $m \geq s$,

$$\mathfrak{p}_1^{(m)} \subset (b)\mathfrak{p}_1^{(m)} + \mathfrak{p}_1^{(m+1)}. \tag{53}$$

Let $x \in \mathfrak{p}_1^{(m)}$. Then

$$x \in (b) + \mathfrak{p}_1^{(m)} \overset{(52)}{=} (b) + \mathfrak{p}_1^{(m+1)},$$

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 21.1) 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 every $m \geq s$,

$$\mathfrak{p}_1^{(m)} = \mathfrak{p}_1^{(m+1)}.$$

As $b \in \mathfrak{p}$, (53) 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

$$\bigcap\nolimits_{m \geq s} \mathfrak{p}_1^{(m)} \overset{(51)}{=} \bigcap\nolimits_{m \geq s} ((\mathfrak{p}_1^{e})^m)^c = (\bigcap\nolimits_{m \geq s} (\mathfrak{p}_1^{e})^m)^c \overset{3.16}{=} (0)^c,$$

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 $a \in A \smallsetminus \mathfrak{p}_1 \subset A \smallsetminus \mathfrak{p}_2$, 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.

COROLLARY 21.4. *A noetherian integral domain A is a unique factorization domain if every prime ideal of height 1 is principal.*

PROOF. After Propositions 4.1 and 4.3, it suffices to show that every irreducible element a of A is prime. Let $\mathfrak{p}$ be minimal among the prime ideals containing (a). According to the principal ideal theorem (21.3), $\mathfrak{p}$ has height 1, and so is principal, say $\mathfrak{p} = (b)$. As $(a) \subset (b)$, b divides a, and so $a = b \times$unit. Hence $(a) = (b) = \mathfrak{p}$, and $\mathfrak{p}$ is prime.

In order to extend Theorem 21.7 to non principal ideals, we shall need a lemma.

LEMMA 21.5. *Let $\mathfrak{p}$ be a prime ideal in a noetherian ring A, and let S be a finite set of prime ideals in A, none of which contains $\mathfrak{p}$. If there exists a chain of distinct prime ideals*

$$\mathfrak{p} \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0,$$

then there exists such a chain with $\mathfrak{p}_1$ not contained in any ideal in S.

PROOF. We first prove this in the special case that the chain has length 2. Suppose that $\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_0$ are distinct prime ideals and that $\mathfrak{p}$ is not contained in any prime ideal in S. According to Proposition 2.8, there exists an element

$$a \in \mathfrak{p} \smallsetminus (\mathfrak{p}_0 \cup \bigcup\{\mathfrak{p}' \in S\}).$$

As $\mathfrak{p}$ contains $(a)+\mathfrak{p}_0$, it also contains a minimal prime ideal $\mathfrak{p}_1'$ of $(a)+\mathfrak{p}_0$. Now $\mathfrak{p}_1'/\mathfrak{p}_0$ is a minimal prime ideal of the *principal ideal* $((a)+\mathfrak{p}_0)/\mathfrak{p}_0$ in $A/\mathfrak{p}_0$, and so has height 1, whereas the chain $\mathfrak{p}/\mathfrak{p}_0 \supset \mathfrak{p}_1/\mathfrak{p}_0 \supset \mathfrak{p}_0/\mathfrak{p}_0$ shows that $\mathfrak{p}/\mathfrak{p}_0$ has height at least 2. Therefore $\mathfrak{p} \supset \mathfrak{p}_1' \supset \mathfrak{p}_0$ are distinct primes, and $\mathfrak{p}_1' \notin S$ because it contains a. This completes the proof of the special case.

Now consider the general case. On applying the special case to $\mathfrak{p} \supset \mathfrak{p}_{d-1} \supset \mathfrak{p}_{d-2}$, we see that there exists a chain of distinct prime ideals $\mathfrak{p} \supset \mathfrak{p}_{d-1}' \supset \mathfrak{p}_{d-2}$ such that $\mathfrak{p}_{d-1}'$ is not contained in any ideal in S. Then on applying the special case to $\mathfrak{p}_{d-1}' \supset \mathfrak{p}_{d-2} \supset \mathfrak{p}_{d-1}$, we we see that there exists a chain of distinct prime ideals $\mathfrak{p} \supset \mathfrak{p}_{d-1}' \supset \mathfrak{p}_{d-2}' \supset \mathfrak{p}_{d-2}$ such that $\mathfrak{p}_{d-2}'$ is not contained in any ideal in S. Repeat the argument until the proof is complete.

THEOREM 21.6. *Let A be a noetherian ring. For every proper ideal $\mathfrak{a} = (a_1,\ldots,a_m)$, the height of a minimal prime ideal of $\mathfrak{a}$ is at most m.*

PROOF. For $m=1$, this was just proved. Thus, we may suppose 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 $\mathfrak{p}_1',\ldots,\mathfrak{p}_t'$ be the minimal prime ideals of $(a_2,\ldots,a_m)$. Each $\mathfrak{p}_i'$ has height at most $m-1$. If $\mathfrak{p}$ is contained in one of the $\mathfrak{p}_i'$, it will have height $\leq m-1$, and so we may suppose that it isn't.

Let $\mathfrak{p}$ have height d. We have to show that $d \leq m$. According to the lemma, there exists a chain of distinct prime ideals

$$\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0, \quad d \geq 1,$$

with $\mathfrak{p}_1$ not contained in any $\mathfrak{p}_i'$, and so Proposition 2.8 shows that there exists a

$$b \in \mathfrak{p}_1 \smallsetminus \bigcup_{i=1}^{r} \mathfrak{p}_i'.$$

We next show that $\mathfrak{p}$ is a minimal prime ideal of $(b,a_2,\ldots,a_m)$. Certainly $\mathfrak{p}$ contains a minimal prime ideal $\mathfrak{p}'$ of this ideal. As $\mathfrak{p}' \supset (a_2,\ldots,a_m)$, $\mathfrak{p}$ contains one of the $\mathfrak{p}_i'$s, but, by construction, it cannot equal it. If $\mathfrak{p} \neq \mathfrak{p}'$, then

$$\mathfrak{p} \supset \mathfrak{p}' \supset \mathfrak{p}_i'$$

are distinct ideals, which shows that $\bar{\mathfrak{p}} \stackrel{\text{def}}{=} \mathfrak{p}/(a_2,\ldots,a_m)$ has height at least 2 in $\bar{A} \stackrel{\text{def}}{=} A/(a_2,\ldots,a_m)$. But $\bar{\mathfrak{p}}$ is a minimal ideal in $\bar{A}$ of the principal ideal $(a_1,\ldots,a_n)/(a_2,\ldots,a_n)$, which contradicts Theorem 21.3. Hence $\mathfrak{p}$ is minimal, as claimed.

But now $\mathfrak{p}/(b)$ is a minimal prime ideal of $(b,a_2,\ldots,a_m)$ in $R/(b)$, and so the height of $\mathfrak{p}/(b)$ is at most $m-1$ (by induction). The prime ideals

$$\mathfrak{p}/(b) = \mathfrak{p}_d/(b) \supset \mathfrak{p}_{d-1}/(b) \supset \cdots \supset \mathfrak{p}_1/(b)$$

are distinct, and so $d-1 \leq m-1$. This completes the proof that $d=m$.

The ***height*** of an ideal $\mathfrak{a}$ in a noetherian ring is the minimum height of a prime ideal containing it,

$$\operatorname{ht}(\mathfrak{a}) = \min_{\mathfrak{p} \supset \mathfrak{a},\ \mathfrak{p} \text{ prime}} \operatorname{ht}(\mathfrak{p}).$$

The theorem shows that $\operatorname{ht}(\mathfrak{a})$ is finite.

The following provides a (strong) converse to Theorem 21.6.

THEOREM 21.7. *Let A be a noetherian ring, and let $\mathfrak{a}$ be a proper ideal of A of height r. Then there exist r elements $a_1,\ldots,a_r$ of $\mathfrak{a}$ such that, for each $i \leq r$, $(a_1,\ldots,a_i)$ has height i.*

PROOF. If $r = 0$, then we take the empty set of a_is. Thus, suppose that $r \geq 1$. There are only finitely many prime ideals of height 0, because such an ideal is a minimal prime ideal of (0), and none of these ideals can contain $\mathfrak{a}$ because it has height ≥ 1. Proposition 2.8 shows that there exists an

$$a_1 \in \mathfrak{a} \smallsetminus \bigcup\{\text{prime ideals of height } 0\}.$$

By construction, (a_1) has height at least 1, and so Theorem 21.3 shows it has height exactly 1.

This completes the proof when $r = 1$, and so suppose that $r \geq 2$. There are only finitely many prime ideals of height 1 containing (a_1) because such an ideal is a minimal prime ideal of (a_1), and none of these ideals can contain $\mathfrak{a}$ because it has height ≥ 2. Choose

$$a_2 \in \mathfrak{a} \smallsetminus \bigcup\{\text{prime ideals of height 1 containing } (a_1)\}.$$

By construction, (a_1,a_2) has height at least 2, and so Theorem 21.6 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 21.8. *Every prime ideal of height r in a noetherian ring arises as a minimal prime ideal for an ideal generated by r elements.*

PROOF. According to the theorem, an ideal $\mathfrak{a}$ of height r contains an ideal $(a_1,\ldots,a_r)$ of height r. If $\mathfrak{a}$ is prime, then it is a minimal ideal of $(a_1,\ldots,a_r)$.

COROLLARY 21.9. *Let A be a commutative noetherian ring, and let $\mathfrak{a}$ be an ideal in A that can be generated by n elements. For every prime ideal $\mathfrak{p}$ in A containing $\mathfrak{a}$,*

$$\mathrm{ht}(\mathfrak{p}/\mathfrak{a}) \leq \mathrm{ht}(\mathfrak{p}) \leq \mathrm{ht}(\mathfrak{p}/\mathfrak{a}) + n.$$

PROOF. The first inequality follows immediately from the correspondence between ideals in A and in $A/\mathfrak{a}$.

Denote the quotient map $A \to A' \stackrel{\text{def}}{=} A/\mathfrak{a}$ by $a \mapsto a'$. Let $\mathrm{ht}(\mathfrak{p}/\mathfrak{a}) = d$. Then there exist elements $a_1,\ldots,a_d$ in A such that $\mathfrak{p}/\mathfrak{a}$ is a minimal prime ideal of $(a_1',\ldots,a_d')$. Let $b_1,\ldots,b_n$ generate $\mathfrak{a}$. Then $\mathfrak{p}$ is a minimal prime ideal of $(a_1,\ldots,a_d,b_1,\ldots,b_n)$, and hence has height $\leq d+n$.

We now use dimension theory to prove a stronger version of "generic flatness" (11.21).

THEOREM 21.10 (GENERIC FREENESS). *Let A be a noetherian integral domain, and let B be a finitely generated A-algebra. For every 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 Theorem 11.21 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 (8.1) shows that there exist algebraically independent elements $x_1,\ldots,x_m$ of $F\otimes_A B$ such that $F\otimes_A B$ is a finite $F[x_1,\ldots,x_m]$-algebra. As in the proof of Theorem11.21, there exists a nonzero $a\in A$ such that B_a is a finite $A_a[x_1,\ldots,x_m]$-algebra. Hence M_a is a finitely generated $A_a[x_1,\ldots,x_m]$-module.

As every extension of free modules is free[24], Proposition 3.5 shows that it suffices to prove the theorem for $M_a = A_a[x_1,\ldots,x_m]/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ in $A_a[x_1,\ldots,x_m]$. If $\mathfrak{p}=0$, then M_a is free over A_a (with basis the monomials in the x_i). Otherwise, $F\otimes_A (A_a[x_1,\ldots,x_m]/\mathfrak{p})$ has Krull dimension less than that of $F\otimes_A B$, and so we can apply the induction hypothesis.

COROLLARY 21.11. *Let A be a noetherian ring, and let $\varphi\colon A\to B$ be a finitely generated A-algebra. If U is a nonempty open subset of* $\mathrm{Spec}(B)$, *then $\varphi^a(U)$ contains a nonempty open subset of its closure in* $\mathrm{Spec}(A)$.

PROOF. We may replace A with its image in B, and B with B_f for some f such that $D(f)\subset U$. Then we have to show that the image of $\varphi^a\colon\mathrm{Spec}(B)\to\mathrm{Spec}(A)$ contains a nonempty open subset of $\mathrm{Spec}(A)$. According to (21.10), there exists an $a\in A$ such that B_a is a nonzero free A_a-module. For any prime ideal $\mathfrak{p}$ of A not containing a, $B\otimes_A A/\mathfrak{p}\simeq B_a\otimes_{A_a} A/\mathfrak{p}\neq 0$. As $B\otimes_A A/\mathfrak{p}$ is nonzero, it contains a prime ideal, but the prime ideals in $B\otimes_A A/\mathfrak{p}$ correspond to prime ideals $\mathfrak{q}$ in B such that $\mathfrak{q}\cap A=\mathfrak{p}$. Therefore the image of φ^a contains $D(a)$.

22 Regular local rings

Throughout this section, A is a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field k. The Krull dimension d of A is equal to the height of $\mathfrak{m}$, and

$$\mathrm{ht}(\mathfrak{m}) \overset{(21.6)}{\leq} \text{minimum number of generators of } \mathfrak{m} \overset{(3.11)}{=} \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

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 22.1. *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'.

[24] If M' is a submodule of M such that $M''\overset{\text{def}}{=}M/M'$ is free, then $M\approx M'\oplus M''$.

PROOF. Let $e_1,\ldots,e_n$ be elements of $\mathfrak{m}$ such that $\{e_1',\ldots,e_n'\}$ is a k-linear basis for $\mathfrak{m}'/\mathfrak{m}'^2$. We shall show that $\{e_1,\ldots,e_n,c\}$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$.

As $e_1',\ldots,e_n'$ span $\mathfrak{m}'/\mathfrak{m}'^2$, they generate the ideal $\mathfrak{m}'$ (see 3.11), and so $\mathfrak{m}=(e_1,\ldots,e_n)+(c)$, which implies that $\{e_1,\ldots,e_n,c\}$ spans $\mathfrak{m}/\mathfrak{m}^2$.

Suppose that $a_1,\ldots,a_{n+1}$ are elements of A such that

$$a_1e_1+\cdots+a_ne_n+a_{n+1}c\equiv 0 \bmod \mathfrak{m}^2. \tag{54}$$

Then

$$a_1'e_1'+\cdots+a_n'e_n'\equiv 0 \bmod \mathfrak{m}'^2,$$

and so $a_1',\ldots,a_n'\in\mathfrak{m}'$. It follows that $a_1,\ldots,a_n\in\mathfrak{m}$. Now (54) 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 (54) is the trivial one.

PROPOSITION 22.2. *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, Corollary 21.9 shows that

$$\mathrm{ht}(\mathfrak{m}')\le\mathrm{ht}(\mathfrak{m})\le\mathrm{ht}(\mathfrak{m}')+1.$$

Therefore

$$\dim_k(\mathfrak{m}'/\mathfrak{m}'^2)\ge\mathrm{ht}(\mathfrak{m}')\ge\mathrm{ht}(\mathfrak{m})-1=\dim_k(\mathfrak{m}/\mathfrak{m}^2)-1=\dim_k(\mathfrak{m}'/\mathfrak{m}'^2).$$

Equalities must hold throughout, which proves that A' is regular with dimension $\dim A-1$.

THEOREM 22.3. *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 $b=a^nc$ 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 $b\in\bigcap_n\mathfrak{a}^n\overset{3.16}{=}\{0\}$. 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 (§19) that S is finite. We have shown that $\mathfrak{m}\smallsetminus\mathfrak{m}^2\subset\bigcup\{\mathfrak{p}\mid\mathfrak{p}\in S\}$, and so $\mathfrak{m}\subset\mathfrak{m}^2\cup\bigcup\{\mathfrak{p}\mid\mathfrak{p}\in S\}$. It follows from Proposition 2.8 that either $\mathfrak{m}\subset\mathfrak{m}^2$ (and hence $\mathfrak{m}=0$) or $\mathfrak{m}$ is a minimal prime ideal of A, but both of these statements contradict the assumption that $d\ge 1$.

COROLLARY 22.4. *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 3.17). The ring $A/\mathfrak{m}^r$ is local and artinian, and so $\mathfrak{a} = (t^s) + \mathfrak{m}^r$ for some $s \geq 1$ (by 16.8). This implies that $\mathfrak{a} = (t^s)$ by Nakayama's lemma (3.9).

THEOREM 22.5. *Let A be a regular noetherian local ring.*

(a) *For every 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.

DEFINITION 22.6. Let $(A, \mathfrak{m})$ be a noetherian local ring of dimension d. A ***system of parameters*** of A is a set of elements $\{a_1, \ldots, a_d\}$ such that $(a_1, \ldots, a_d) \supset \mathfrak{m}^n$ for some n. If $(a_1, \ldots, a_d) = \mathfrak{m}$, then $\{a_1, \ldots, a_d\}$ is called a ***regular system of parameters***.

In other words, $\{a_1, \ldots, a_d\}$ is a system of parameters if the ideal $(a_1, \ldots, a_d)$ is $\mathfrak{m}$-primary. A system of parameters always exists, and a regular system of parameters exists if and only if A is regular.

23 Flatness and fibres

Recall that, for a prime ideal $\mathfrak{p}$ in a ring A, the field of fractions of $A/\mathfrak{p}$ is denoted $\kappa(\mathfrak{p})$. For example, for a maximal ideal $\mathfrak{m}$, $\kappa(\mathfrak{m}) = A/\mathfrak{m}$; more generally, $\kappa(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$.

Let $\varphi\colon A \to B$ be a homomorphism of rings. We say that the going-down theorem holds for φ if the statement (7.12) holds with $\mathfrak{q}_i \cap A$ interpreted as $\mathfrak{q}_i^c$:

$$\begin{array}{ccccccccccc}
\mathfrak{q}_1 & \supset & \cdots & \supset & \mathfrak{q}_m & \supset & \cdots & \supset & \mathfrak{q}_n & & \\
| & & & & | & & & & | & & \mathfrak{p}_i = \mathfrak{q}_i^c. \\
\mathfrak{p}_1 & \supset & \cdots & \supset & \mathfrak{p}_m & \supset & \cdots & \supset & \mathfrak{p}_n & &
\end{array}$$

THEOREM 23.1. *Let $\varphi\colon A \to B$ be a homomorphism of noetherian rings. Let $\mathfrak{q}$ be a prime ideal of B, and let $\mathfrak{p} = \mathfrak{q}^c$.*

(a) *We have* $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{p}) + \dim(B_{\mathfrak{q}} \otimes \kappa(\mathfrak{p}))$.

(b) *If the going-down theorem holds for φ, then equality holds in (a).*

PROOF. The statement depends only on the homomorphism of local rings $A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ defined by φ. Thus, we can replace A and B with $A_{\mathfrak{p}}$ and $B_{\mathfrak{q}}$, and $\mathfrak{q}$ and $\mathfrak{p}$ with the maximal ideals $\mathfrak{n} = \mathfrak{q}B_{\mathfrak{q}}$ and $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$. Then the inequality becomes

$$\dim(B) \leq \dim(A) + \dim(B/\mathfrak{m}B).$$

(a) Let $\{a_1, \ldots, a_r\}$ be a system of parameters for A, so that

$$\mathfrak{m}^n \subset (a_1, \ldots, a_r).$$

for some n. Let $b_1,\ldots,b_s$ be elements of B whose images in $B/\mathfrak{m}B$ form a system of parameters for $B/\mathfrak{m}B$, so that

$$\mathfrak{n}^{n'} \subset (b_1,\ldots,b_s) + \mathfrak{m}B$$

for some n'. Now

$$\mathfrak{n}^{n'n} \subset (b_1,\ldots,b_s) + (a_1,\ldots,a_r)B$$

and so $\{a_1,\ldots,a_r,b_1,\ldots b_s\}$ generates an $\mathfrak{n}$-primary ideal in B. Hence

$$\dim(B) \leq r+s = \dim(A) + \dim(B/\mathfrak{m}B).$$

(b) Let $m = \dim(B/\mathfrak{m}B)$, and let

$$\mathfrak{n} = \mathfrak{q}_0 \supset \cdots \supset \mathfrak{q}_m$$

be a chain of distinct prime ideals in B containing $\mathfrak{m}B$. Clearly $\mathfrak{q}_i^c = \mathfrak{m}$ for all i. Let $m' = \dim A$, and let

$$\mathfrak{m} = \mathfrak{p}_0 \supset \cdots \supset \mathfrak{p}_{m'}$$

be a chain of distinct prime ideals in A. By the going-down theorem, there exists a chain of ideals

$$\mathfrak{q}_m \supset \cdots \supset \mathfrak{q}_{m+m'}$$

such that $\mathfrak{q}_{m+i}^c = \mathfrak{p}_i$ for all i. The existence of the chain

$$\mathfrak{q}_0 \supset \cdots \supset \mathfrak{q}_{m+m'}$$

of distinct prime ideals in B shows that $\dim(B) \geq m'+m = \dim A + \dim(B/\mathfrak{m}B)$.

THEOREM 23.2. *The going-down theorem holds for every flat homomorphism $\varphi\colon A \to B$.*

PROOF. Let $\mathfrak{p}' \subset \mathfrak{p}$ be prime ideals in A, and let $\mathfrak{q}$ be a prime ideal in B such that $\mathfrak{q}^c = \mathfrak{p}$. We have to show that there exists a prime ideal $\mathfrak{q}' \subset \mathfrak{q}$ in B such that $\mathfrak{q}'^c = \mathfrak{p}'$. Because φ is flat, $A_\mathfrak{p} \to B_\mathfrak{q}$ is faithfully flat (11.18), and so there exists a prime ideal in $B_\mathfrak{q}$ contracting to $\mathfrak{p}'A_\mathfrak{p}$ in $A_\mathfrak{p}$ (11.19). The contraction of this ideal to B has the required properties. (See also 11.20.)

COROLLARY 23.3. *Let $\varphi\colon A \to B$ be a homomorphism of rings, and let $\mathfrak{q}$ be a prime ideal of B. If φ is flat, then*

$$\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{p}) + \dim(B_\mathfrak{q} \otimes \kappa(\mathfrak{p})), \quad \mathfrak{p} = \mathfrak{q}^c.$$

PROOF. According to the theorem, φ satisfies the going-down theorem, and so we can apply Theorem 23.1.

COROLLARY 23.4. *Let A be a noetherian ring, and let $\varphi\colon A \to B$ be a homomorphism of rings. If φ is flat of finite type, then the map $\varphi^a\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is open.*

PROOF. According to the theorem, φ satisfies the going-down theorem, and so we can apply Proposition 14.16.

Let $\varphi\colon A \to B$ be a homomorphism of rings such that all maximal ideals in A have the same height and similarly for B. If φ is flat and $\mathrm{spm}(\varphi)$ is surjective, then Corollary 23.3 says that

$$\dim(B) = \dim(A) + \dim(B \otimes_A \kappa(\mathfrak{m}))$$

for all maximal ideals of A. In other words, the dimension of the fibre

$$\mathrm{spm}(B) \to \mathrm{spm}(A)$$

over $\mathfrak{m} \in \mathrm{spm}(A)$ is $\dim(\mathrm{spm}(B)) - \dim(\mathrm{spm}(A))$.

Corollary 23.3 has a converse.

THEOREM 23.5. *Let $\varphi\colon A \to B$ be a local homomorphism of noetherian local rings, and let $\mathfrak{m}$ be the maximal ideal of A. If A is regular, B is Cohen-Macaulay, and*

$$\dim(B) = \dim(A) + \dim(B \otimes \kappa(\mathfrak{m})),$$

then φ is flat.

PROOF. Matsumura 1986, 23.1.

We don't define the notion of being Cohen-Macaulay here (see ibid. p.134), but merely list some of its properties.

23.6. A noetherian ring A is Cohen-Macaulay if and only if $A_{\mathfrak{m}}$ is Cohen-Macaulay for every maximal ideal $\mathfrak{m}$ of A (this is part of the definition).

23.7. Zero-dimensional and reduced one-dimensional noetherian rings are Cohen-Macaulay (ibid. p.139).

23.8. Regular noetherian rings are Cohen-Macaulay (ibid. p.137).

23.9. Let $\varphi\colon A \to B$ be a flat local homomorphism of noetherian local rings, and let $\mathfrak{m}$ be the maximal ideal of A. Then B is Cohen-Macaulay if and only if both A and $B \otimes_A \kappa(\mathfrak{m})$ are Cohen-Macaulay (ibid. p.181).

PROPOSITION 23.10. *Let $\varphi\colon A \to B$ be a finite homomorphism noetherian rings with A regular. Then φ is flat if and only if B is Cohen-Macaulay.*

PROOF. Note that $\dim(B/\mathfrak{m}B)$ is zero-dimensional, hence Cohen-Macaulay, for every maximal ideal $\mathfrak{m}$ of A (23.7), and that $\mathrm{ht}(\mathfrak{n}) = \mathrm{ht}(\mathfrak{n}^c)$ for every maximal ideal $\mathfrak{n}$ of B. If φ is flat, then B is Cohen-Macaulay by (23.9). Conversely, if B is Cohen-Macaulay, then φ is flat by (23.5).

ASIDE 23.11. In contrast to the going-down theorem, the going-up theorem fails for flat homomorphisms — it even fails for $\mathbb{Z} \to \mathbb{Z}[X]$ (see 7.8).

Exercises

EXERCISE 23.12. Show that the only flat surjective homomorphisms from a noetherian ring are the projection maps $A_1 \times A_2 \to A_1$.

24 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

$$M/\mathfrak{a}M \leftarrow M/\mathfrak{a}^2 M \leftarrow \cdots \leftarrow M/\mathfrak{a}^n M \leftarrow \cdots$$

whose limit we define to be the $\mathfrak{a}$-adic completion $\hat{M}$ of M:

$$\hat{M} \stackrel{\text{def}}{=} \varprojlim M/\mathfrak{a}^n M.$$

For example, the $\mathfrak{a}$-adic completion of A is

$$\hat{A} \stackrel{\text{def}}{=} \varprojlim_n A/\mathfrak{a}^n.$$

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 24.1. *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 $\hat{M}$ 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 $\hat{M}$ 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 $\bar{m}_n$ denote the constant value. The family $(\bar{m}_n)_{n\in\mathbb{N}}$ depends only on the equivalence class of the Cauchy sequence $(m_n)_{n\in\mathbb{N}}$, and

$$[(m_n)] \mapsto (\bar{m}_n)\colon \hat{M} \to \varprojlim M/M_n$$

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 24.2. *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 $\mathfrak{a}^n M \subset M_n$ for all n. For some n_0, $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$, and so $M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subset \mathfrak{a}^n M$.

LEMMA 24.3 (ARTIN-REES). *If A is noetherian and M is finitely generated, then, for every A-submodule M' of M, the filtration $(M' \cap \mathfrak{a}^n M)_{n\in\mathbb{N}}$ on M' is a stable $\mathfrak{a}$-filtration.*

PROOF. Omitted for the moment.

PROPOSITION 24.4. *For every noetherian ring A and ideal $\mathfrak{a}$, the functor $M \rightsquigarrow \hat{M}$ 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 24.5. *For every ideal $\mathfrak{a}$ in a noetherian ring A and finitely generated A-module M, the homomorphism*

$$a \otimes m \mapsto am : \widehat{A} \otimes_A M \to \widehat{M}$$

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

$$\begin{array}{ccccccccc}
 & & \widehat{A} \otimes_A N & \longrightarrow & \widehat{A}^m & \longrightarrow & \widehat{A} \otimes_A M & \longrightarrow & 0 \\
 & & \downarrow a & & \downarrow \simeq & & \downarrow b & & \\
0 & \longrightarrow & \widehat{N} & \longrightarrow & \widehat{A}^m & \longrightarrow & \widehat{M} & \longrightarrow & 0
\end{array}$$

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 24.6. *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 Propositions 24.4 and 24.5 that $\widehat{A} \otimes_A -$ is exact on finitely generated A-modules, but this implies that it is exact on all A-modules.

ASIDE 24.7. Let $\mathfrak{m}$ be a maximal ideal of a ring A, and let $A \to \widehat{A}$ denote the $\mathfrak{m}$-adic completion of A. Then $A/\mathfrak{m}^n \to \widehat{A}/\widehat{\mathfrak{m}}^n$ is the $\mathfrak{m}$-adic completion of $A/\mathfrak{m}^n$, but $A/\mathfrak{m}^n$ is discrete, and so $A/\mathfrak{m}^n \to \widehat{A}/\widehat{\mathfrak{m}}^n$ is an isomorphism. Similarly, $A_\mathfrak{m}/\mathfrak{m}_m^n \to \widehat{A}_\mathfrak{m}/\widehat{\mathfrak{m}}_\mathfrak{m}^n \simeq \widehat{A}/\widehat{\mathfrak{m}}^n$ is an isomorphism. On combining these statements, we obtain a conceptual proof of Proposition 5.8.

Sections to be added.

25. Henselian rings.
26. Graded rings.
27. Hilbert polynomials.
28. Homological methods.
29. Regular local rings revisited.
30. Connections with geometry.
31. Computational commutative algebra.

A Solutions to the exercises.

1.1. For $n = 1$, use that a nonzero polynomial in one variable has only finitely many roots (which follows from unique factorization, for example). Now suppose $n > 1$, and assume the statement for polynomials in $\leq n-1$ symbols. Write $f = \sum g_i X_n^i$ with each $g_i \in k[X_1,\ldots,X_{n-1}]$. If f is not the zero polynomial, then some g_i is not the zero polynomial, and there exist $(a_1,\ldots,a_{n-1}) \in k^{n-1}$ such that $f(a_1,\ldots,a_{n-1},X_n)$ is not the zero polynomial. Now, by the degree-one case, there exists a b such that $f(a_1,\ldots,a_{n-1},b) \neq 0$.

6.20. Let $f = \sum b_i T^{m-i}$, $b_i \in B$. If the coefficients b_i of f are integral over A, then they are integral over $A[T]$ (as elements of $B[T]$). Certainly T is integral over $A[T]$, and so this implies that $f = \sum b_i T^i$ is integral over A (see 6.5).

11.22. The set $\mathrm{spm}(A_{f_i})$ consists of the maximal ideals in A not containing f_i, and $\mathrm{spm}(\prod_i A_{f_i}) = \coprod_i \mathrm{spm}(A_{f_i})$. Therefore the map $\mathrm{spm}(\prod_i A_{f_i}) \to \mathrm{spm}(A)$ is surjective if and only if $(f_1,\ldots,f_m) = A$. Now apply (11.18). For the second statement, it is only a question of showing that the sequence in (11.11) becomes the sequence in (11.22) when $i\colon A \to B$ is taken to be $A \to \prod_i A_{f_i}$.

15.16. (a) Let B be a countable local domain, and number its elements $b_1, b_2, \ldots$. Consider the homomorphism $A \to B$ sending X_i to b_i. It is surjective, and its kernel is a prime ideal $\mathfrak{p}$ of A. The ideal $\mathfrak{p}$ is not an intersection of maximal ideals because the only maximal ideal of A containing $\mathfrak{p}$ is the inverse image of the maximal ideal in B.

(b) Let f be a nonzero element of A, say, $f = f(X_1,\ldots,X_n)$. Choose $a_1,\ldots,a_n \in \mathbb{Q}$ such that $f(a_1,\ldots,a_n) \neq 0$ (Exercise 1.1). The kernel of the homomorphism $A \to \mathbb{Q}$ sending X_i to a_i for $i \leq n$ and X_i to 0 for $i > n$ is a maximal ideal in A not containing f.

23.12. Consider surjective homomorphism $A \to A/\mathfrak{a}$. The set $V(\mathfrak{a})$ is closed in $\mathrm{spec}(A)$ (by definition of the topology on $\mathrm{spec}(A)$). 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 $V(\mathfrak{b}) = \mathrm{spec}(A_1)$. 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

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

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).

References

Atiyah, M. F. and Macdonald, I. G. 1969. Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont.

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.

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