A Primer of Commutative Algebra

James S. Milne

January 1, 2009, v1.00

Abstract

These notes prove the fundamental theorems in commutative algebra required for algebraic geometry, algebraic groups, and algebraic number theory.

The reader is assumed to have taken an advanced undergraduate or first-year graduate course in algebra.

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

Contents

NOTATIONS AND CONVENTIONS

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

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

ring A form a group, which we denote $A^\times$.[2] Throughout "ring" means "commutative ring". Following Bourbaki, we let $\mathbb{N} = \{0, 1, 2, \ldots\}$.

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

1 Algebras

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

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

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

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

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

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

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

2 Ideals

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

- $\mathfrak{a}$ is a subgroup of A regarded as a group under addition;
- $a \in \mathfrak{a}, r \in A \Rightarrow ra \in \mathfrak{a}$.

The ***ideal generated by a subset*** S of A is the intersection of all ideals $\mathfrak{a}$ containing A — 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 $S = \{s_1, s_2, \ldots\}$, we write $(s_1, s_2, \ldots)$ for the ideal it generates.

[2] This notation differs from Bourbaki's, who writes $A^\times$ for the multiplicative monoid $A \smallsetminus \{0\}$ and A^* for the group of units. We shall never need the former, and * is overused.

[3] The term "module-finite" is also used.

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

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

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

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

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

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

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 $A/\mathfrak{p}$ is nonzero and has the property that

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

i.e., $A/\mathfrak{p}$ is an integral domain.

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

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

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

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

An ideal $\mathfrak{a}$ is said to be ***radical*** if it equals its radical, i.e., if $f^r \in \mathfrak{a} \implies f \in \mathfrak{a}$. Equivalently, $\mathfrak{a}$ is radical if and only if $A/\mathfrak{a}$ is a ***reduced ring***, i.e., a ring without nonzero ***nilpotent*** elements (elements some power of which is zero). Since integral domains are reduced, prime ideals (*a fortiori* maximal ideals) are radical.

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

PROPOSITION 2.1. *Let $\mathfrak{a}$ be an ideal in a ring A.*

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

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

PROOF. (a) If $a \in \operatorname{rad}(\mathfrak{a})$, then clearly $fa \in \operatorname{rad}(\mathfrak{a})$ for all $f \in A$. Suppose $a, b \in \operatorname{rad}(\mathfrak{a})$, 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 $a^r \in \operatorname{rad}(\mathfrak{a})$, then $a^{rs} = (a^r)^s \in \mathfrak{a}$ for some s. □

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

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

PROPOSITION 2.2. *The radical of an ideal is equal to the intersection of the prime ideals containing it.*

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. As prime ideals are radical, $\mathrm{rad}(\mathfrak{a})$ is contained in every prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$, and so $\mathrm{rad}(\mathfrak{a})\subset\bigcap_{\mathfrak{p}\supset\mathfrak{a}}\mathfrak{p}$.

Conversely, suppose that $f\notin\mathrm{rad}(\mathfrak{a})$, and let S be the set of ideals in A containing $\mathfrak{a}$ but no power of f. Then S is nonempty, because $(0)\in S$. Suppose S contains a maximal element $\mathfrak{c}$, and let $bb'\in\mathfrak{c}$. If neither b nor b' is in $\mathfrak{c}$, then $\mathfrak{c}+(b)$ and $\mathfrak{c}+(b')$ properly contain $\mathfrak{c}$, and so do not lie in S. Therefore

$$f^r=c+ab,\quad f^r=c'+a'b' \text{ some } r,r'\geq 1,\ c,c'\in\mathfrak{c},\ a,a'\in A.$$

Hence

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

which is a contradiction. Therefore $\mathfrak{c}$ is prime, and so $f\notin\bigcap_{\mathfrak{p}\supset\mathfrak{a}}\mathfrak{p}$.

It remains to show that S always contains a maximal element. If A is noetherian (see §3 below), this is automatic. Otherwise, we apply Zorn's lemma to S. Let $\mathfrak{b}_1\subset\mathfrak{b}_2\subset\cdots$ be a chain of ideals in S, and let $\mathfrak{b}=\bigcup\mathfrak{b}_i$. Then $\mathfrak{b}\in S$, because otherwise some power of f lies in $\mathfrak{b}$, and hence in some $\mathfrak{b}_i$, which contradicts the definition of S. Therefore $\mathfrak{b}$ is an upper bound for the chain. As every chain in S has an upper bound, Zorn's lemma shows that S has a maximal element. □

REMARK 2.3. The argument in the last paragraph of the proof applied to the set S of ideals containing $\mathfrak{a}$ but not 1 shows that every proper ideal of A is contained in a maximal ideal.

DEFINITION 2.4. The ***Jacobson radical*** $\mathfrak{J}$ of a ring is the intersection of the maximal ideals of the ring:

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

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

PROPOSITION 2.5. *An element c of A is in the Jacobson radical of A if and only if $1-ac$ is a unit for all $a\in A$.*

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

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

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

PROPOSITION 2.6. *Let S be a nonempty finite set of ideals in A, at most one of which is not prime. Any ideal contained in the union of the ideals in S is contained in at least one of the ideals.*

PROOF. We prove the contrapositive:

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

For $|S| = 1$, there is nothing to prove, and so we assume that $|S| = r + 1 > 1$ and (inductively) that the statement is true for r. We can list the elements of S as $\mathfrak{p}_1, \dots, \mathfrak{p}_{r+1}$ with $\mathfrak{p}_{r+1}$ prime. As $\mathfrak{a}$ is not contained in any of the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_{r+1}$, by induction, for each i, there exists an a_i in $\mathfrak{a}$ not in the union of the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_{i-1}, \mathfrak{p}_{i+1}, \dots, \mathfrak{p}_{r+1}$. If some a_i does not lie in $\mathfrak{p}_i$, then that $a_i \in \mathfrak{a} \setminus \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_{r+1}$, and the proof is complete. Thus assume that every $a_i \in \mathfrak{p}_i$, and consider

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

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

EXTENSION AND CONTRACTION OF IDEALS

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

NOTATION 2.7. For any 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 any ideal $\mathfrak{a}$ of A, the ideal $\varphi(\mathfrak{a})B$ 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, $\mathfrak{b}^c = \mathfrak{b} \cap A$.

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

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

2.9. There are the following relations ($\mathfrak{a}$ an ideal of A; $\mathfrak{b}$ an ideal of B):

$$\mathfrak{a} \subset \mathfrak{a}^{ec}, \quad \mathfrak{b}^{ce} \subset \mathfrak{b}, \quad \mathfrak{a}^e \subset \mathfrak{a}^{ece}, \quad \mathfrak{b}^{cec} \subset \mathfrak{b}^c.$$

Therefore, extension and contraction define inverse bijections between the set of contracted ideals in A and the set of extended ideals in B:

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

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

THE CHINESE REMAINDER THEOREM

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

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

THEOREM 2.10 (CHINESE REMAINDER THEOREM). *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals in a ring A. If $\mathfrak{a}_i$ is coprime to $\mathfrak{a}_j$ (i.e., $\mathfrak{a}_i + \mathfrak{a}_j = A$) whenever $i \neq j$, then the map*

$$A \to A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n \tag{3}$$

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

PROOF. Suppose first that $n = 2$. As $\mathfrak{a}_1 + \mathfrak{a}_2 = A$, there exist $a_i \in \mathfrak{a}_i$ such that $a_1 + a_2 = 1$. Then $a_1x_2 + a_2x_1$ maps to $(x_1 \bmod \mathfrak{a}_1, x_2 \bmod \mathfrak{a}_2)$, which shows that (3) is surjective.

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

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

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

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

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

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

These conditions imply

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

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

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

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

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

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

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

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

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

3 Noetherian rings

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

(a) *every ideal in A is finitely generated;*
(b) *every ascending chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ eventually becomes constant, i.e., for some m, $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \cdots$.*
(c) *every nonempty set of ideals in A has a maximal element (i.e., an element not properly contained in any other ideal in the set).*

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

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

(b) $\Rightarrow$ (c): Let S be a nonempty set of ideals in A. Let $\mathfrak{a}_1 \in S$; if $\mathfrak{a}_1$ is not maximal in S, then there exists an ideal $\mathfrak{a}_2$ in S properly containing $\mathfrak{a}_1$. Similarly, if $\mathfrak{a}_2$ is not maximal in S, then there exists an ideal $\mathfrak{a}_3$ in S properly containing $\mathfrak{a}_2$, etc.. In this way, we obtain an ascending chain of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots$ in S that will eventually terminate in an ideal that is maximal in S.

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

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

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

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

(a) *every submodule of M is finitely generated;*
(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. Note that a ring A is noetherian if and only if it is noetherian as an A-module (because the submodules of A are exactly the ideals in A).

PROPOSITION 3.3. *Let*

$$0 \to M' \xrightarrow{i} M \xrightarrow{q} M'' \to 0$$

be an exact sequence of A-modules. The module M is noetherian if and only if M' and M'' are both noetherian.

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

$\Leftarrow$: That ascending chains of submodules of M eventually become constant follows from the statement:

> Submodules $N' \subset N$ of M are equal if $q(N') = q(N)$ and $i^{-1}(N') = i^{-1}(N)$.

To prove this, let $x \in N$; because $q(N') = q(N)$, there exists an $x' \in N'$ such that $q(x) = q(x')$; now $q(x-x') = 0$, and so there exists $y \in M'$ such that $i(y) = x-x'$. As $i(y) \in N$, we have $y \in i^{-1}(N) = i^{-1}(N')$, and so $i(y) \in N'$. Therefore $x = x' + i(y) \in N'$. □

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

PROOF. As such a module is a quotient of A^r for some r, it suffice to show that A^r is noetherian, but this can be proved by induction on r using the exact sequences

$$0 \to A^{r-1} \xrightarrow{i} A^r \xrightarrow{q} A \to 0 \qquad \begin{cases} i(a_1,\dots,a_{r-1}) = (a_1,\dots,a_{r-1},0) \\ q(a_1,\dots,a_r) = a_r. \end{cases}$$

□

THEOREM 3.5 (HILBERT BASIS THEOREM). *If A is noetherian, then so also is every finitely generated A-algebra.*

In particular, a polynomial ring $A[X_1,\dots,X_n]$ over a noetherian ring is noetherian.

PROOF. As $A[x_1,\dots,x_n] = A[x_1,\dots,x_{n-1}][x_n]$, an induction argument shows that it suffices to prove the theorem for an A-algebra generated by a single element. But such an A-algebra is a quotient of the polynomial algebra $A[X]$, and so it suffices to show 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 the ***leading coefficient*** of f.

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

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

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

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

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

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

Now

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

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

$$f - \sum_j a_j f_{sj}$$

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

PROPOSITION 3.6 (NAKAYAMA'S LEMMA). *Let A be a noetherian ring, let $\mathfrak{a}$ be an ideal in A contained in all maximal ideals of A, and let M be a finitely generated A-module.*

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

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

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

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

Then

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

and, as $1 - a_1$ is a unit (see 2.5), $e_2, \dots, e_n$ generate M. This contradicts the minimality of the set.

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

Now let A be a local noetherian ring with maximal ideal $\mathfrak{m}$. When we regard $\mathfrak{m}$ as an A-module, the action of A on $\mathfrak{m}/\mathfrak{m}^2$ factors through $k \stackrel{\text{def}}{=} A/\mathfrak{m}$.

COROLLARY 3.7. *The elements $a_1, \dots, a_n$ of $\mathfrak{m}$ generate $\mathfrak{m}$ as an ideal if and only if their residues modulo $\mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$ as a vector space over k. 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. If $a_1, \dots, a_n$ generate the ideal $\mathfrak{m}$, it is obvious that their residues generate the vector space $\mathfrak{m}/\mathfrak{m}^2$. Conversely, suppose that their residues generate $\mathfrak{m}/\mathfrak{m}^2$, so that $\mathfrak{m} = (a_1, \dots, a_n) + \mathfrak{m}^2$. Since A is noetherian and (hence) $\mathfrak{m}$ is finitely generated, Nakayama's lemma, applied with $\mathfrak{a} = \mathfrak{m}$, $M = \mathfrak{m}$, and $N = (a_1, \dots, a_n)$, shows that $\mathfrak{m} = (a_1, \dots, a_n)$. □

DEFINITION 3.8. Let A be a noetherian ring.

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

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

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

Thus, the Krull dimension of a ring A is the supremum of the lengths of chains of prime ideals in A (the length of a chain is the number of gaps, so the length of (4) is d). For example, a field has Krull dimension 0, and conversely an integral domain of Krull dimension 0 is a field. The height of every nonzero prime ideal in a principal ideal domain is 1, and so such a ring has Krull dimension 1 (provided it is not a field).

We shall see in §15 that the height of any prime ideal in a noetherian ring is finite. However, the Krull dimension of the ring may be infinite, because it may contain a sequence $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \dots$ of prime ideals such that $\operatorname{ht}(\mathfrak{p}_i)$ tends to infinity (see Krull 1938 or Nagata 1962).

LEMMA 3.9. *In a noetherian ring, every set of generators for an ideal contains a finite generating set.*

PROOF. Let $\mathfrak{a}$ be an ideal in a noetherian ring A, and let S be a set of generators for $\mathfrak{a}$. Because A is noetherian, $\mathfrak{a}$ admits a finite generating set, say, $\mathfrak{a} = (a_1, \dots, a_n)$. Each a_i lies in the ideal generated by a finite subset S_i of S, and $\bigcup_{i=1,\dots,n} S_i$ is finite and generates $\mathfrak{a}$. □

THEOREM 3.10 (KRULL INTERSECTION THEOREM). *Let $\mathfrak{a}$ be an ideal in a noetherian ring A. If $\mathfrak{a}$ is contained in all maximal ideals of A, then $\bigcap_{n\geq 1} \mathfrak{a}^n = \{0\}$.*

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

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

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

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

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

for some $g_i \in A$. 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. Thus, we may choose the g_i to be homogeneous of degree $\deg f - \deg f_i = d + 1 - d_i > 0$. Then

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

which completes the proof of (5). □

The equality (5) can also be proved using primary decompositions — see §13.

PROPOSITION 3.11. *In a noetherian ring, every ideal contains a power of its radical; in particular, some power of the radical of the ring is zero.*

PROOF. Let $a_1, \dots, a_n$ 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

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

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

4 Unique factorization

Let A be an integral domain. An element a of A is ***irreducible*** if it is not zero, not a unit, and admits only trivial factorizations, i.e., those in which one of the factors is a unit. If every nonzero nonunit 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, then A is called a ***unique factorization domain***. In such a ring, an irreducible element a can divide a product bc only if it divides b or c (write $bc = aq$ and express b, c, q as products of irreducible elements). Every principal ideal domain, for example, the polynomial ring $k[X]$ over a field k, is a unique factorization domain.

PROPOSITION 4.1. *Let (a) be a nonzero proper principal ideal in an integral domain A. If (a) is a prime ideal, then a is irreducible, and the converse holds when A is a unique factorization domain.*

PROOF. Assume (a) is prime. Because (a) is neither (0) nor A, a is neither zero nor a unit. If $a = bc$, then $bc \in (a)$, which, because (a) is prime, implies that b or c is in (a), say $b = aq$. Now $a = bc = aqc$, which implies that $qc = 1$, and that c is a unit.

For the converse, assume that a is irreducible. If $bc \in (a)$, then $a|bc$, which (as we noted above) implies that $a|b$ or $a|c$, i.e., that b or $c \in (a)$. □

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

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

$$cdf = g_1h_1 \text{ in } A[X].$$

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

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

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

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

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

Let A be a unique factorization domain. A nonzero polynomial

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

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

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

PROOF. Let

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

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

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

PROOF. Let $f = c(f)f_1$ and $g = c(g)g_1$ with f_1 and g_1 primitive. Then $fg = c(f)c(g)f_1g_1$ with f_1g_1 primitive, and so $c(fg) = c(f)c(g)$. □

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

PROOF. We first show that every element f of $A[X]$ is a product of irreducible elements. From the factorization $f = c(f)f_1$ with f_1 primitive, we see that it suffices to do this for f primitive. If f is not irreducible in $A[X]$, then it factors as $f = gh$ with g, h primitive polynomials in $A[X]$ of lower degree. Continuing in this fashion, we obtain the required factorization.

From the factorization $f = c(f)f_1$, we see that the irreducible elements of $A[X]$ are to be found among the constant polynomials and the primitive polynomials.

Let

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

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

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

and, on using that A is a unique factorization domain, we see that $m = r$ and the c_is differ from the d_is only by units and ordering. Hence,

$$f_1 \cdots f_n = g_1 \cdots g_s \text{ (up to units in } A).$$

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

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

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

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

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

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

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

PROOF. Note that $k[X_1, \dots, X_n] = k[X_1, \dots, X_{n-1}][X_n]$: this simply says that every polynomial f in n variables $X_1, \dots, X_n$ can be expressed uniquely as a polynomial in X_n with coefficients in $k[X_1, \dots, X_{n-1}]$,

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

Since $k[X_1]$ is a unique factorization domain, the theorem follows by induction from Proposition 4.5. □

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

PROOF. Special case of (4.1). □

5 Integrality

Let A be a subring of a ring B. An element α of B is said to be ***integral*** over A if it is a root of a monic[4] polynomial with coefficients in A, i.e., if it satisfies an equation

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

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

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

then

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

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

where $C = (c_{ij})$ and C_j is obtained from C by replacing the elements of the jth column with the d_is. When one restates the equation as

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

it becomes true over any ring (whether or not $\det(C)$ is invertible). The proof is elementary—essentially it is what you wind up with when you eliminate the other variables (try it for $m = 2$). Alternatively, expand out

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

using standard properties of determinants.

PROPOSITION 5.1. *Let A be a subring of a ring B. An element α of B is integral over A if and only if there exists a faithful[5] finitely generated A-submodule M of B such that $\alpha M \subset M$ (in fact, we can take M to be $A[\alpha]$, the A-subalgebra generated by α).*

PROOF. $\Rightarrow$: Suppose

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

Then the A-submodule M of B generated by $1, \alpha, ..., \alpha^{n-1}$ has the property that $\alpha M \subset M$.

$\Leftarrow$: Let M be a nonzero A-module in B such that $\alpha M \subset M$, and let $v_1, \dots, v_n$ be a finite set of generators for M. Then, for each i,

$$\alpha v_i = \sum a_{ij}v_j, \text{ some } a_{ij} \in A.$$

We can rewrite this system of equations as

$$\begin{aligned} (\alpha - a_{11})v_1 - a_{12}v_2 - a_{13}v_3 - \cdots &= 0 \\ -a_{21}v_1 + (\alpha - a_{22})v_2 - a_{23}v_3 - \cdots &= 0 \\ \cdots &= 0. \end{aligned}$$

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

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

PROPOSITION 5.2. *An A-algebra B is finite if and only if it is finitely generated and integral over A (i.e., every element of B is integral over A).*

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

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

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

$\Rightarrow$: As an A-module, B is faithful (because $a \cdot 1_B = a$), and so (5.1) implies 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. $\square$

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

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

PROOF. Let α and β be two elements of B integral over A. Then $A[\alpha,\beta]$ is a faithful finitely generated A-submodule of B, which is stable under multiplication by $\alpha \pm \beta$ and $\alpha\beta$. According to (5.1), this implies that $\alpha \pm \beta$ and $\alpha\beta$ are integral over A. □

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

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

PROOF. By assumption, α satisfies an equation

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

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

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

We can rewrite this as

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

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

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

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

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

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

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

PROOF. Let a/b, $a, b \in A$, be integral over A. If $a/b \notin A$, then there is an irreducible element p of A dividing b but not a. As a/b is integral over A, it satisfies an equation

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

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

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

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

PROPOSITION 5.9. *Let A be an integrally closed integral domain, and let L be a finite extension of the field of fractions F of A. An element α of L 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

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

Let α' be a conjugate of α, i.e., a root of the minimum polynomial $f(X)$ of α over F in some algebraic closure of L. Then there is an F-isomorphism[6]

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

On applying σ to the above equation we obtain the equation

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

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

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

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

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

In other words, there exist elements $f_1, \dots, f_r$ of A such that A is a finite $k[f_1, \dots, f_r]$-algebra and $f_1, \dots, f_r$ are algebraically independent over k.

PROOF. We may suppose that

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

Let $f_1, \dots, f_n$ be elements of $k[X_1, \dots, X_n]$ such that $k[X_1, \dots, X_n]$ is a finite $k[f_1, \dots, f_n]$-algebra (e.g., $x_1, \dots, x_n$), and let $\bar{f}_i$ be the image of f_i in A. We may suppose that the f_i have been numbered so that $\bar{f}_1, \dots, \bar{f}_r$ are nonzero but $\bar{f}_{r+1} = \cdots = \bar{f}_n = 0$. Then A is a finite $k[\bar{f}_1, \dots, \bar{f}_r]$-algebra, and we shall show that, if $\bar{f}_1, \dots, \bar{f}_r$ are not algebraically independent, then it is possible to replace $\{f_1, \dots, f_n\}$ with a similar set having fewer nonzero images in A. By repeating the argument, we will eventually arrive at an n-tuple whose nonzero images in A are algebraically independent.

If $\bar{f}_1, \dots, \bar{f}_r$ are algebraically dependent, then there exists a nonzero polynomial

$$P = \sum c_{j_1 \cdots j_r} X_1^{j_1} \cdots X_r^{j_r} \in k[X_1, \dots, X_r]$$

[6]Recall that the homomorphism $X \mapsto \alpha\colon F[X] \to F[\alpha]$ defines an isomorphism $F[X]/(f) \to F[\alpha]$, where f is the minimum polynomial of α.

such that

$$w_1 \stackrel{\text{def}}{=} P(f_1, \dots, f_r) \in \mathfrak{a}.$$

For $i = 2, \dots, r$, set $w_i = f_i - f_1^{m^i}$ for some positive integer m. On expanding out

$$w_1 = P(f_1, f_1^{m^2} + w_2, \dots, f_1^{m^r} + w_r),$$

we obtain an equality

$$w_1 = \sum c_{j_1 \cdots j_r} (f_1^{j_1 + m^2 j_2 + \cdots + m^r j_r} + \text{terms of lower degree in } f_1).$$

When m is chosen sufficiently large, the exponents

$$j_1 + m^2 j_2 + \cdots + m^r j_r$$

will be distinct — let N be the largest of them. Then the last equality can be rearranged to express f_1^N as a polynomial $c_0 + c_1 f_1 + \cdots + c_{N-1} f_1^{N-1}$ with $c_i \in k[w_1, \dots, w_r]$. It follows that

$$k[f_1, \dots, f_n] \subset \sum\nolimits_{i=0}^{N-1} k[w_1, \dots, w_r, f_{r+1}, \dots, f_n] \cdot f_1^i.$$

Therefore the elements $w_1, \dots, w_r, f_{r+1}, \dots, f_n$ have the property that $k[X_1, \dots, X_n]$ is a finite $k[w_1, \dots, w_r, f_{r+1}, \dots, f_n]$-algebra, but, because $w_1 \in \mathfrak{a}$, at most $r - 1 < r$ of them have nonzero image in A. □

6 Rings of fractions

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

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

In other words, it is a nonempty subset closed under the formation of finite products.

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

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

Write $\frac{a}{s}$ for the equivalence class containing (a, s), and define addition and multiplication in the obvious way:

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

It is easy to show that these are well defined, i.e., do not depend on the choices of representatives for the equivalence classes, and that we obtain in this way a ring

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

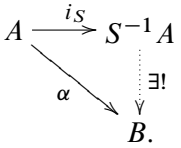
and a ring homomorphism $a \mapsto \frac{a}{1} : A \xrightarrow{i_S} S^{-1}A$, whose kernel is

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

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

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

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



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

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

and so

$$\beta(\tfrac{a}{s}) = \alpha(a)\alpha(s)^{-1}. \tag{6}$$

This shows that there can be at most one such homomorphism β. Define β by the formula (6). Then

$$\tfrac{a}{c} = \tfrac{b}{d} \implies s(ad - bc) = 0 \text{ some } s \in S,$$

which implies that $\alpha(a)\alpha(d) - \alpha(b)\alpha(c) = 0$ because $\alpha(s)$ is a unit in B. This 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 $(S^{-1}A, i)$ uniquely up to a unique isomorphism.[7]

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

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

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

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

EXAMPLE 6.3. Let $\mathfrak{p}$ be a prime ideal in A. Then $S_\mathfrak{p} = A \setminus \mathfrak{p}$ 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

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

The subset $\mathfrak{m} = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}$ is a maximal ideal in $A_\mathfrak{p}$, and it is the only maximal ideal, i.e., $A_\mathfrak{p}$ is a local ring. To see this, first check $\mathfrak{m}$ is an ideal. Next, if $\mathfrak{m} = A_\mathfrak{p}$, then $1 \in \mathfrak{m}$; but if $1 = \frac{a}{s}$ for some $a \in \mathfrak{p}$ and $s \notin \mathfrak{p}$, then $u(s - a) = 0$ some $u \notin \mathfrak{p}$, and so $ua = us \notin \mathfrak{p}$, which contradicts $a \in \mathfrak{p}$. Finally, $\mathfrak{m}$ is maximal because every element of $A_\mathfrak{p}$ not in $\mathfrak{m}$ is a unit.

When A is an integral domain with field of fractions F, $A_\mathfrak{p}$ is the subring of F of elements of the form $\frac{a}{s}$, $a \in A$, $s \notin \mathfrak{p}$.

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

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

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

PROPOSITION 6.4. *For any ring A and $h \in A$, the map $\sum a_i X^i \mapsto \sum \frac{a_i}{h^i}$ defines an isomorphism*

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

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

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

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

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

PROPOSITION 6.5. *Let S be a multiplicative subset of the ring A. The map $\mathfrak{p} \mapsto \mathfrak{p}^e \stackrel{\text{def}}{=} S^{-1}\mathfrak{p}$ is a bijection from the set of prime ideals of A disjoint from S onto the set of all prime ideals of $S^{-1}A$, with inverse $\mathfrak{p} \mapsto \mathfrak{p}^e \stackrel{\text{def}}{=} \{a \in A \mid \frac{a}{1} \in \mathfrak{p}\}$. In particular, $\mathfrak{p}^{ec} = \mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of A disjoint from S, and $\mathfrak{p}^{ce} = \mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of $S^{-1}A$ (in fact, $\mathfrak{b}^{ce} = \mathfrak{b}$ for all ideals $\mathfrak{b}$ of $S^{-1}A$).*

PROOF. For an ideal $\mathfrak{a}$ of A, let $\mathfrak{a}^e = S^{-1}\mathfrak{a}$, and for an ideal $\mathfrak{b}$ of $S^{-1}A$, let $\mathfrak{b}^c$ be the inverse image of $\mathfrak{b}$ in A, so $\mathfrak{b}^c = \{a \in A \mid \frac{a}{1} \in \mathfrak{b}\}$.

For an ideal $\mathfrak{b}$ of $S^{-1}A$, certainly, $\mathfrak{b} \supset \mathfrak{b}^{ce}$. Conversely, if $\frac{a}{s} \in \mathfrak{b}$, $a \in A$, $s \in S$, then $\frac{a}{1} \in \mathfrak{b}$, and so $a \in \mathfrak{b}^c$. Thus $\frac{a}{s} \in \mathfrak{b}^{ce}$, and so $\mathfrak{b} = \mathfrak{b}^{ce}$.

For an ideal $\mathfrak{a}$ of A, certainly $\mathfrak{a} \subset \mathfrak{a}^{ec}$. Conversely, if $a \in \mathfrak{a}^{ec}$, then $\frac{a}{1} \in \mathfrak{a}^e$, and so $\frac{a}{1} = \frac{a'}{s}$ for some $a' \in \mathfrak{a}$, $s \in S$. Thus, $t(as - a') = 0$ for some $t \in S$, and so $ast \in \mathfrak{a}$. If $\mathfrak{a}$ is a prime ideal disjoint from S, this implies that $a \in \mathfrak{a}$: for such an ideal, $\mathfrak{a} = \mathfrak{a}^{ec}$.

For any ideal $\mathfrak{b}$ of $S^{-1}A$, $A/\mathfrak{b}^c \hookrightarrow S^{-1}A/\mathfrak{b}$, and so $\mathfrak{b}^c$ is prime if $\mathfrak{b}$ is.

Let $\mathfrak{a}$ be an ideal of A, and let $\bar{S}$ be the image of S in $A/\mathfrak{a}$. Then $S^{-1}A/\mathfrak{a}^e \simeq \bar{S}^{-1}(A/\mathfrak{a})$, which is a subring of the field of fractions of $A/\mathfrak{a}$ if $\mathfrak{a}$ is a prime ideal disjoint from S, and so $\mathfrak{a}^e$ is prime in this case. □

COROLLARY 6.6. *If A is noetherian, then so also is $S^{-1}A$ for any multiplicative set S.*

PROOF. We saw in the above proof that, $\mathfrak{b} = \mathfrak{b}^{ce}$ for any ideal $\mathfrak{b}$ of $S^{-1}A$. As $\mathfrak{b}^c$ is finitely generated, so also is $(\mathfrak{b}^c)^e = \mathfrak{b}$. □

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

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

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

Let $S = A \setminus \mathfrak{m}$, so that $A_{\mathfrak{m}} = S^{-1}A$, and let $i\colon A \to A_{\mathfrak{m}}$ be the map $a \mapsto \frac{a}{1}$. In order to show that the map $A/\mathfrak{m}^n \to A_{\mathfrak{n}}/\mathfrak{n}^n$ is injective, we have to show that $i^{-1}(\mathfrak{n}^m) = \mathfrak{m}^m$. But $\mathfrak{n}^m = \mathfrak{m}^n A_{\mathfrak{m}} = S^{-1}\mathfrak{m}^m$, and so we have to show that $\mathfrak{m}^m = i^{-1}(S^{-1}\mathfrak{m}^m)$. If $a \in i^{-1}(S^{-1}\mathfrak{m}^m)$, then $\frac{a}{1} = \frac{b}{s}$ with $b \in \mathfrak{m}^m$ and $s \in S$. Then $s'sa \in \mathfrak{m}^m$ for some $s' \in S$, and so $s'sa = 0$ in $A/\mathfrak{m}^m$. The only maximal ideal containing $\mathfrak{m}^m$ is $\mathfrak{m}$ (because $\mathfrak{m}' \supset \mathfrak{m}^m \implies \mathfrak{m}' \supset \mathfrak{m}$), and so the only maximal ideal in $A/\mathfrak{m}^m$ is $\mathfrak{m}/\mathfrak{m}^m$. As $s's$ is not in $\mathfrak{m}/\mathfrak{m}^m$, it must be a unit in $A/\mathfrak{m}^m$, and as $s'sa = 0$ in $A/\mathfrak{m}^m$, a must be 0 in $A/\mathfrak{m}^m$, i.e., $a \in \mathfrak{m}^m$.

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

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

PROOF. Let a be an element of a noetherian ring A. If $a \neq 0$, then $\{b \mid ba = 0\}$ is a proper ideal, and so it is contained in some maximal ideal $\mathfrak{m}$. Then $\frac{a}{1}$ is nonzero in $A_{\mathfrak{m}}$, and so $\frac{a}{1} \notin (\mathfrak{m}A_{\mathfrak{m}})^n$ for some n (by the Krull intersection theorem 3.10), which implies that $a \notin \mathfrak{m}^n$ (by 6.7). □

MODULES OF FRACTIONS

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

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

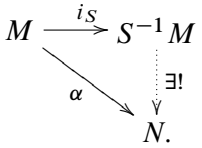
Write $\frac{m}{s}$ for the equivalence class containing (m,s), and define an addition and multiplication in the obvious way:

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

It is easy to show that these are well defined, i.e., do not depend on the choices of representatives for the equivalence classes, and that we obtain in this way an $S^{-1}A$-module $S^{-1}M = \{\frac{m}{s} \mid m \in M, s \in S\}$ and a homomorphism $m \mapsto \frac{m}{1}\colon M \xrightarrow{i_S} S^{-1}M$ of A-modules whose kernel is

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

PROPOSITION 6.9. *The pair $(S^{-1}M, i_S)$ has the following universal property: every element of S acts invertibly on $S^{-1}M$, and any other homomorphism $\alpha: M \to N$ of A-modules with this property factors uniquely through i_S,*



PROOF. Similar to that of Proposition 6.1. □

PROPOSITION 6.10. *The functor $M \rightsquigarrow S^{-1}M$ is exact.*

In other words, if the sequence of A-modules

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

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

$$S^{-1}M' \to S^{-1}M \to S^{-1}M''.$$

The proof is an easy exercise, which we leave to the reader.

7 Direct limits

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

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

(a) An ***direct system*** of R-modules indexed by $(I, \leq)$ is a family $(M_i)_{i \in I}$ of R-modules together with a family $(\alpha_j^i: M_i \to M_j)_{i \leq j}$ of R-linear maps such that $\alpha_i^i = \mathrm{id}_{M_i}$ and $\alpha_k^j \circ \alpha_j^i = \alpha_k^i$ all $i \leq j \leq k$.

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

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

CRITERION

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

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

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

CONSTRUCTION

Let

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

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

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

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

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

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

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

AN EXAMPLE

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

PROOF. When $h|h'$, say, $h' = hg$, there is a unique homomorphism $A_h \to A_{h'}$ respecting the maps $A \to A_h$ and $A \to A_{h'}$, namely, $\frac{a}{h} \mapsto \frac{ag}{h'}$, and so the rings A_h form a direct system indexed by the set S. When $h \in S$, the homomorphism $A \to S^{-1}A$ extends uniquely to a homomorphism $\frac{a}{h} \mapsto \frac{a}{h} : A_h \to S^{-1}A$ (6.1), and these homomorphisms are compatible with the maps in the direct system. Now apply the criterion p21 to see that $S^{-1}A$ is the direct limit of the A_h. □

8 Tensor Products

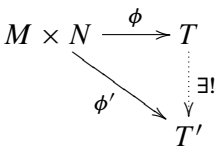
TENSOR PRODUCTS OF MODULES

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

$$\begin{aligned}
\phi(x + x', y) &= \phi(x, y) + \phi(x', y), && x, x' \in M, \quad y \in N \\
\phi(x, y + y') &= \phi(x, y) + \phi(x, y'), && x \in M, \quad y, y' \in N \\
\phi(rx, y) &= r\phi(x, y), && r \in R, \quad x \in M, \quad y \in N \\
\phi(x, ry) &= r\phi(x, y), && r \in R, \quad x \in M, \quad y \in N,
\end{aligned}$$

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

An R-module T together with an R-bilinear map $\phi : M \times N \to T$ is called the ***tensor product*** of M and N over R if it has the following universal property: every R-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 $M \otimes_R N$. Note that

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

Construction

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

$$\sum r_i(x_i, y_i), \quad r_i \in R, \quad x_i \in M, \quad y_i \in N.$$

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

$$\begin{aligned}
(x + x', y) - (x, y) - (x', y), &\quad x, x' \in M, \quad y \in N\\
(x, y + y') - (x, y) - (x, y'), &\quad x \in M, \quad y, y' \in N\\
(rx, y) - r(x, y), &\quad r \in R, \quad x \in M, \quad y \in N\\
(x, ry) - r(x, y), &\quad r \in R, \quad x \in M, \quad y \in N,
\end{aligned}$$

and define

$$M \otimes_R N = R^{(M\times N)}/K.$$

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

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

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

$$\sum r_i(x_i \otimes y_i), \quad r_i \in R, \quad x_i \in M, \quad y_i \in N,$$

and all relations among these symbols are generated by the following

$$\begin{aligned}
(x + x') \otimes y &= x \otimes y + x' \otimes y\\
x \otimes (y + y') &= x \otimes y + x \otimes y'\\
r(x \otimes y) &= (rx) \otimes y = x \otimes ry.
\end{aligned}$$

The pair $(M \otimes_R N, (x, y) \mapsto x \otimes y)$ has the correct universal property.

Extension of scalars

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

$$\mathrm{Hom}_{R\text{-linear}}(M, N) \simeq \mathrm{Hom}_{A\text{-linear}}(A \otimes_R M, N), \quad N \text{ an } A\text{-module}. \tag{7}$$

Behaviour with respect to direct limits

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

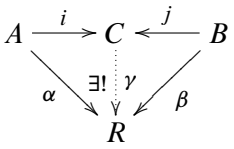
$$\varinjlim_{i\in I} M_i \otimes_R \varinjlim_{j\in J} N_j \simeq \varinjlim_{(i,j)\in I\times J} M_i \otimes_R N_j.$$

PROOF. Using the universal properties of direct limits and tensor products, one sees easily that $\varinjlim(M_i \otimes_R N_j)$ 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) $\alpha: A \to R$ and $\beta: B \to R$, there exists a unique homomorphism $\gamma: C \to R$ such that $\gamma \circ i = \alpha$ and $\gamma \circ j = \beta$:



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

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

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

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

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

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

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

EXAMPLE 8.2. The algebra B, together with the given map $k \to B$ and the identity map $B \to B$, has the universal property characterizing $k \otimes_k B$. In terms of the constructive definition of tensor products, the map $c \otimes b \mapsto cb: k \otimes_k B \to B$ is an isomorphism.

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

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

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

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

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

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

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

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

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

REMARK 8.4. (a) If (b_α) is a family of generators (resp. basis) for B as a k-module, then $(1 \otimes b_\alpha)$ is a family of generators (resp. basis) for $A \otimes_k B$ as an A-module.

(b) 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

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

(c) If A and B are algebras of k-valued functions on sets S and T respectively, then $(f \otimes g)(x, y) = f(x)g(y)$ 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 R. For each $r \geq 0$, set

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

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

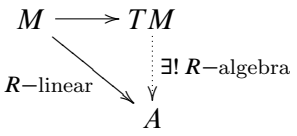
$$TM = \bigoplus\nolimits_{r \geq 0} T^r M.$$

This can be made into a noncommutative graded R-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 $m_1 \otimes \cdots \otimes m_{r+s}$.

Any R-linear map from M to an R-algebra A (not necessarily commutative) extends uniquely to an R-algebra homomorphism $TM \to A$.



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

THE SYMMETRIC ALGEBRA OF A MODULE

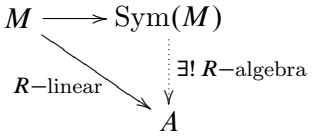
The ***symmetric algebra*** $\mathrm{Sym}(M)$ of an R-module M is the quotient of TM by the ideal generated by all elements of $T^2 M$ of the form

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

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

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

Any R-linear map $M \to A$ from M to a commutative R-algebra A extends uniquely to an R-algebra homomorphism $\mathrm{Sym}(M) \to A$ (because it extends to an R-algebra homomorphism $TM \to A$, which factors through $\mathrm{Sym}(M)$ because A is commutative).



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

9 Flatness

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

$$0 \to N' \to N \to N'' \to 0 \tag{8}$$

is exact, then the sequence

$$M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$$

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

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

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

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

Moreover, if M and N are nonzero, then $M \otimes_R N$ need not be 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.[8]

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

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

It is ***faithfully flat*** if, in addition,

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

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

Thus, a homomorphism $R \to S$ of rings is flat if and only if $S \otimes_R -$ is an exact functor, i.e.,

$$0 \to S \otimes_R N' \to S \otimes_R N \to S \otimes_R N'' \to 0 \tag{9}$$

is exact whenever (8) is exact.

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

[8] It was once customary to require a ring to have an identity element $1 \neq 0$ (see, for example, Northcott 1953, p3). However, tensor products do not always exist in the category of such objects, .

PROPOSITION 9.2. *Let $i: R \to S$ be faithfully flat.*
(a) A sequence (8) is exact if and only if (9) is exact.
(b) For any R-module M, the sequence

$$0 \to M \xrightarrow{d_0} S \otimes_R M \xrightarrow{d_1} S \otimes_R S \otimes_R M \qquad (*)$$
$$\begin{cases} d_0(m) &= 1 \otimes m, \\ d_1(s \otimes m) &= 1 \otimes s \otimes m - s \otimes 1 \otimes m \end{cases}$$

is exact.

PROOF. (a) We have to show that (8) is exact if (9) is exact. Let N be the kernel of $M' \to M$. Then, because $R \to S$ is flat, $S \otimes_R N$ is the kernel of $S \otimes_R M' \to S \otimes_R M$, which is zero by assumption. Because $R \to S$ is *faithfully* flat, this implies that $N = 0$. This proves the exactness at M', and the proof of exactness elsewhere is similar.

(b) Assume first that there exists an R-linear section to $R \to S$, i.e., an R-linear map $f: S \to R$ such that $f \circ i = \mathrm{id}_R$, and define

$$k_0: S \otimes_R M \to M, \qquad k_0(s \otimes m) = f(s)m$$
$$k_1: S \otimes_R S \otimes_R M \to S \otimes_R M, \qquad k_1(s \otimes s' \otimes m) = f(s)s' \otimes m.$$

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

$$k_1 \circ d_1 + d_0 \circ k_0 = \mathrm{id}_{S \otimes_R M}$$

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

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

$$S \otimes_R (S \otimes_R M) \simeq (S \otimes_R S) \otimes_S (S \otimes_R M).$$

Now $S \to S \otimes_R S$ has an S-linear section, namely, $f(s \otimes s') = ss'$, and so we can apply the first part. □

COROLLARY 9.3. *If $R \to S$ is faithfully flat, then it is injective with image the set of elements on which the maps*

$$\begin{cases} s &\mapsto 1 \otimes s \\ s &\mapsto s \otimes 1 \end{cases} : S \to S \otimes_R S$$

coincide.

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

PROPOSITION 9.4. *Let $R \to R'$ be a homomorphism of rings. If $R \to S$ is flat (or faithfully flat), then so also is $R' \to S \otimes_R R'$.*

PROOF. For any R'-module,

$$(S \otimes_R R') \otimes_{R'} M \simeq S \otimes_R M,$$

from which the statement follows. □

PROPOSITION 9.5. *For any multiplicative subset S of a ring R and R-module M,*

$$S^{-1}R \otimes_R M \simeq S^{-1}M.$$

Therefore the homomorphism $r \mapsto \frac{r}{1}: R \to S^{-1}R$ is flat.

PROOF. To give an $S^{-1}R$-module is the same as giving an R-module on which the elements of S act invertibly. Therefore $S^{-1}R \otimes_R M$ and $S^{-1}M$ satisfy the same universal property (see §8, especially (7)), which proves the first statement. As $M \rightsquigarrow S^{-1}M$ is exact (6.10), so also is $M \rightsquigarrow S^{-1}R \otimes_R M$, which proves the second statement. □

PROPOSITION 9.6. *The following conditions on a flat homomorphism $\varphi: R \to S$ are equivalent:*

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

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

$$S \otimes_R M \simeq S/\varphi(\mathfrak{m})S.$$

As $S \otimes_R M \neq 0$, we have that $\varphi(\mathfrak{m})S \neq S$.

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

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

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

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

THEOREM 9.7 (GENERIC FLATNESS). *Let $A \subset B$ be finitely generated k-algebras with A an integral domain. Then for some nonzero elements a of A and b of B, the homomorphism $A_a \to B_b$ is faithfully flat.*

PROOF. Let K be the field of fractions of A. Then $K \otimes_A B$ is the ring of fractions of B with respect to the multiplicative subset $A \smallsetminus \{0\}$ (see 9.5), and so the kernel of $B \to K \otimes_A B$ 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 3.5), and so there exists a nonzero $c \in A$ such that $cb = 0$ for *all* $b \in \mathfrak{n}$. Let $\frac{b}{c^r}$ lie in the kernel of $B_c \to K \otimes_{A_c} B_c$. The same argument shows that $\frac{a}{c^s}\frac{b}{c^r} = 0$ 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 $cb = 0$ and $\frac{b}{c^r} = 0$ in B_c. This shows that, after replacing A with A_c and B with B_c, we may suppose that the map $B \to K \otimes_A B$ is injective. We shall identify B with its image in $K \otimes_A B$.

As $K \otimes_A B$ is a finitely generated K-algebra, the Noether normalization theorem (5.11) shows that there exist elements $x_1, \dots, x_m$ of $K \otimes_A B$ such that $K[x_1, \dots, x_m]$ is a polynomial ring over K and $K \otimes_A B$ is a finite $K[x_1, \dots, x_m]$-algebra. After multiplying

each x_i by an element of A, we may suppose that it lies in B. Let $\{b_1, \dots, b_n\}$ generate B as an A-algebra. After possibly enlarging this set, we may suppose that it spans $K \otimes_A B$ as a $K[x_1, \dots, x_m]$-module. For each pair (i, j), write $b_i b_j = \sum_k p_{ijk} b_k$ with $p_{ijk} \in K[x_1, \dots, x_m]$. There exists a nonzero $a \in A$ such that $a \cdot p_{ijk} \in A[x_1, \dots, x_m]$ for all i, j, k. Now each $p_{ijk} \in A_a[x_1, \dots, x_m]$, and it follows that every monomial in the b_is lies in the $A_a[x_1, \dots, x_m]$-module spanned by the $\{b_1, \dots, b_n\}$. Therefore $B \subset \sum_i A_a[x_1, \dots, x_m] \cdot b_i$, and so $B_a = \sum_i A_a[x_1, \dots, x_m] \cdot b_i$. This shows that, after replacing A with A_a and B with B_a, we may suppose that B is a finite $A[x_1, \dots, x_m]$-algebra.

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

Let $L = K(x_1, \dots, x_n)$ be the field of fractions of $A[x_1, \dots, x_m]$, and let $b_1, \dots, b_r$ be elements of B that form a basis for $L \otimes_{A[x_1,\dots,x_m]} B$ as an L-vector space. Thus, each element b of B is a sum $\sum_i c_i b_i$ with $c_i \in L$, and so $qb = \sum_i (qc_i) b_i \in \sum_i A[x_1, \dots, x_m] \cdot b_i$ for some nonzero $q \in A[x_1, \dots, x_m]$. As B is a finite $A[x_1, \dots, x_m]$-algebra, it follows that there exists a nonzero element q of $A[x_1, \dots, x_m]$ such that $qB \subset \sum_i A[x_1, \dots, x_n] \cdot b_i$, and so $B_q = \sum_i A[x_1, \dots, x_n]_q \cdot b_i$. In other words, the map

$$(c_1, \dots, c_r) \mapsto \sum c_i b_i \colon A[x_1, \dots, x_m]_q^r \to B_q \tag{10}$$

is surjective. This map becomes an isomorphism when tensored with L over $A[x_1, \dots, x_m]$, which implies that its kernel is torsion. But $A[x_1, \dots, x_n]_q^r$ is a torsion-free $A[x_1, \dots, x_m]$-module, and so the map (10) is an isomorphism. Thus B_q is free of finite rank over $A[x_1, \dots, x_m]_q$. Let a be some nonzero coefficient of the polynomial q, and consider the maps

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

The first and third arrows realize their targets as nonzero free modules over their sources, and so are faithfully flat. The middle arrow is flat by (9.5). Let $\mathfrak{m}$ be a maximal ideal in A_a. Then $\mathfrak{m} A_a[x_1, \dots, x_m]$ does not contain the polynomial q because the coefficient a of q is invertible in A_a. Hence $\mathfrak{m} A_a[x_1, \dots, x_m]_q$ is a proper ideal of $A_a[x_1, \dots, x_m]_q$, and so the map $A_a \to A_a[x_1, \dots, x_m]_q$ is faithfully flat (apply 9.6). This completes the proof. □

10 The Hilbert Nullstellensatz

THEOREM 10.1 (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 K is finite over k, and equals it 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 is generated by $x_1, \dots, x_r$ with $r \geq 1$. If K is not algebraic over k, then at least one x_i, say x_1, is not algebraic over k. Then, $k[x_1]$ is a polynomial ring in one symbol over k, and its

field of fractions $k(x_1)$ is a subfield of K. Clearly K is generated as a $k(x_1)$-algebra by $x_2,\dots,x_r$, and so the induction hypothesis implies that $x_2,\dots,x_r$ are algebraic over $k(x_1)$. Proposition 5.5 shows that there exists a $c \in k[x_1]$ such that $cx_2,\dots,c_rx_r$ are integral over $k[x_1]$. Let $f \in K = k[x_1,\dots,x_r]$. For a sufficiently large N, $c^N f \in k[x_1, cx_2,\dots,cx_r]$, and so $c^N f$ is integral over $k[x_1]$ (5.3). When we apply this statement to an element f of $k(x_1)$, (5.8) shows that $c^N f \in k[x_1]$. Therefore, $k(x_1) = \bigcup_N c^{-N}k[x_1]$, but this is absurd, because $k[x_1]$ ($\simeq k[X]$) has infinitely many distinct monic irreducible polynomials[9] that can occur as denominators of elements of $k(x_1)$. □

THEOREM 10.2 (NULLSTELLENSATZ). *Every proper ideal $\mathfrak{a}$ in $k[X_1,\dots,X_n]$ has a zero in $(k^{\mathrm{al}})^n \stackrel{\text{def}}{=} k^{\mathrm{al}} \times \cdots \times k^{\mathrm{al}}$.*

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

THEOREM 10.3 (STRONG NULLSTELLENSATZ). *For an ideal $\mathfrak{a}$ in $k[X_1,\dots,X_n]$, let $Z(\mathfrak{a})$ be the set of zeros of $\mathfrak{a}$ in $(k^{\mathrm{al}})^n$. If a polynomial $h \in k[X_1,\dots,X_n]$ is zero on $Z(\mathfrak{a})$, then some power of h lies in $\mathfrak{a}$.*

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

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

If $(a_1,\dots,a_n,b)$ satisfies the first m equations, then $(a_1,\dots,a_n) \in Z(\mathfrak{a})$; consequently, $h(a_1,\dots,a_n) = 0$, and $(a_1,\dots,a_n,b)$ doesn't satisfy the last equation. Therefore, the equations are inconsistent, and so, according to the Nullstellensatz (10.2), there exist $f_i \in k[X_1,\dots,X_n,Y]$ such that

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

in $k[X_1,\dots,X_n,Y]$. On applying the homomorphism

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

to the above equality, we obtain the identity

$$1 = \textstyle\sum_i f_i(X_1,\dots,X_n,h^{-1}) \cdot g_i(X_1,\dots,X_n) \tag{11}$$

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

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

[9] When k is infinite, there are infinitely many polynomials $X-a$, and when k is finite, we can adapt Euclid's argument: if $p_1,\dots,p_r$ are monic irreducible polynomials in $k[X]$, then $p_1\cdots p_r + 1$ is divisible by a monic irreducible polynomial distinct from $p_1,\dots,p_r$.

for some N_i. Let N be the largest of the N_i. On multiplying (11) by h^N we obtain an identity

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

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

PROPOSITION 10.4. *The radical of an ideal in $k[X_1, \dots, X_n]$ is equal to the intersection of the maximal ideals containing it.*

PROOF. Let $\mathfrak{a}$ be an ideal in $k[X_1, \dots, X_n]$. Because $\operatorname{rad}(\mathfrak{a})$ is the smallest radical ideal containing $\mathfrak{a}$ and maximal ideals are radical $\operatorname{rad}(\mathfrak{a}) \subset \bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$.

Conversely, suppose h is contained in all maximal ideals containing $\mathfrak{a}$, and let $(a_1, \dots, a_n) \in Z(\mathfrak{a})$. The evaluation map

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

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

11 The max spectrum of a ring

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

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

PROPOSITION 11.1. *There are the following relations:*

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

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

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

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

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

For $h \in A$, let

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

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

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

The sets $D(h)$ form a base for the topology on V.

We let $\operatorname{spm} A$ denote the set of maximal ideals in A endowed with its Zariski topology. For any element h of A, $\operatorname{spm} A_h \simeq D(h)$ (see 6.5), and for any ideal $\mathfrak{a}$ in A, $\operatorname{spm} A/\mathfrak{a} \simeq V(\mathfrak{a})$ (isomorphisms of topological spaces).

THE MAX SPECTRUM OF A FINITELY GENERATED k-ALGEBRA

Let A be a finitely generated k-algebra. For any maximal ideal $\mathfrak{m}$ of A, the field $k(\mathfrak{m}) \stackrel{\text{def}}{=} A/\mathfrak{m}$ is a finitely generated k-algebra, and so $k(\mathfrak{m})$ is algebraic over k (Zariski's lemma, 10.1). Therefore, $k(\mathfrak{m})$ is a finite field extension of k, and so equals 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

$$\operatorname{Hom}_{k\text{-alg}}(A, k^{\mathrm{al}}) \to \operatorname{spm} A. \tag{12}$$

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 of k^{al}.[10] Therefore, the fibres of (12) are exactly the orbits of $\operatorname{Gal}(k^{\mathrm{al}}/k)$. 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 (12) is a bijection.

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

$$Z(\mathfrak{a}) \to \operatorname{spm} A \tag{13}$$

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

ASIDE 11.2. Let $k = \mathbb{R}$ or $\mathbb{C}$. Let X be a set and let A be a k-algebra of k-valued functions on X. In analysis, X is called the ***spectrum*** of A if, for every k-algebra homomorphism $\varphi\colon A \to k$, there exists a unique $x \in X$ such that $\varphi(f) = f(x)$ for all $f \in A$ (see, for example, Cartier 2007, 3.3.1, footnote).

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 7.2 shows that this realizes A as a ring of k-valued functions on X. Moreover, because (13) is an isomorphism in this case, for every 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.

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

JACOBSON RINGS

DEFINITION 11.3. A ring A is ***Jacobson*** if every prime ideal in A is an intersection of maximal ideals.

A field is Jacobson. The ring $\mathbb{Z}$ is Jacobson because every nonzero prime ideal is maximal and $(0) = \bigcap_{p=2,3,5,\dots}(p)$. A principal ideal domain (more generally, a Dedekind domain) is Jacobson if it has an infinite number of maximal ideals. A local ring is Jacobson if and only if its maximal ideal is its only prime ideal. Proposition 10.4 shows that every finitely generated algebra over a field is Jacobson.

PROPOSITION 11.4. *The radical of an ideal in a Jacobson ring is equal to the intersection of the maximal ideals containing it. (Therefore, the radical ideals are precisely the intersections of maximal ideals.)*

PROOF. Proposition 2.2 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 11.5. Any ring of finite type over a Jacobson ring is a Jacobson ring (EGA IV 10.4.6). Moreover, if B is of finite type over A and A is Jacobson, then the map $A \to B$ defines a continuous homomorphism $\operatorname{spm} B \to \operatorname{spm} A$.

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

We study more closely the Zariski topology on $\operatorname{spm} A$. For each subset S of A, let $V(S)$ be the set of maximal ideals containing S, and for each subset W of $\operatorname{spm} A$, let $I(W)$ be the intersection of the maximal ideals in W. Thus $V(S)$ is a closed subset of $\operatorname{spm} A$ and $I(W)$ is a radical ideal in A. If $V(\mathfrak{a}) \supset W$, then $\mathfrak{a} \subset I(W)$, and so $V(\mathfrak{a}) \supset VI(W)$. Therefore $VI(W)$ is the closure of W (smallest closed subset of $\operatorname{spm} A$ containing W); in particular, $VI(W) = W$ if W is closed.

PROPOSITION 11.6. *Let V be a closed subset of* $\operatorname{spm} A$.

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

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

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

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

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

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

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

DEFINITION 11.7. A nonempty topological space is said to be ***irreducible*** if it is not the union of two proper closed subsets; equivalently, if any two nonempty open subsets have a nonempty intersection, or if 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 contradicting the second condition.

PROPOSITION 11.8. *Let W be a closed subset of* $\operatorname{spm} A$*. If W is irreducible, then $I(W)$ is prime; the converse is true if A is a Jacobson ring. In particular, the max spectrum of a Jacobson ring A is irreducible if and only if the nilradical of A is prime.*

PROOF. $\Rightarrow$: Assume W is irreducible, and suppose $fg \in I(W)$. For each $\mathfrak{m} \in W$, either $f \in \mathfrak{m}$ or $g \in \mathfrak{m}$, and so $W \subset V(f) \cup V(g)$. Hence

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

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

$\Leftarrow$: Assume $I(W)$ is prime, and suppose $W = V(\mathfrak{a}) \cup V(\mathfrak{b})$ with $\mathfrak{a}$ and $\mathfrak{b}$ radical ideals — we have to show that W equals $V(\mathfrak{a})$ or $V(\mathfrak{b})$. Recall (11.1c) that $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$ and that $\mathfrak{a} \cap \mathfrak{b}$ is radical; hence $I(W) = \mathfrak{a} \cap \mathfrak{b}$ (by 11.4). If $W \neq V(\mathfrak{a})$, then there exists an $f \in \mathfrak{a} \smallsetminus I(W)$. For all $g \in \mathfrak{b}$,

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

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

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

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

EXAMPLE 11.9. Let $f \in k[X_1, \ldots, X_n]$. According to Theorem 4.6, $k[X_1, \ldots, X_n]$ is a unique factorization domain, and so (f) is a prime ideal if and only if f is irreducible (4.1). Thus

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

On the other hand, suppose f factors,

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

Then

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

[10] In a noetherian ring A, a proper ideal $\mathfrak{q}$ is said to ***primary*** if every zero-divisor in $A/\mathfrak{q}$ is nilpotent.

PROPOSITION 11.10. *Let V be a noetherian topological space. Then V is a finite union of irreducible closed subsets, $V = V_1 \cup \ldots \cup V_m$. Moreover, if the decomposition is irredundant in the sense that there are no inclusions among the V_i, then the V_i are uniquely determined up to order.*

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

Suppose that

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

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

The V_i given uniquely by the proposition are called the ***irreducible components*** of V. They are the maximal closed irreducible subsets of V. In Example 11.9, the $V(f_i)$ are the irreducible components of $V(f)$.

COROLLARY 11.11. *A radical ideal $\mathfrak{a}$ in a noetherian Jacobson ring is a finite intersection of prime ideals, $\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n$; if there are no inclusions among the $\mathfrak{p}_i$, then the $\mathfrak{p}_i$ are uniquely determined up to order.*

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

REMARK 11.12. (a) An irreducible topological space is connected, but a connected topological space need not be irreducible. For example, $Z(X_1X_2)$ is the union of the coordinate axes in k^2, which is connected but not irreducible. A closed subset V of $\operatorname{spm} A$ is not connected if and only if there exist ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{a} \cap \mathfrak{b} = I(V)$ and $\mathfrak{a} + \mathfrak{b} \neq A$.

(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 §13). 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 11.9.

12 Dimension theory for finitely generated k-algebras

Throughout this section, A is a finitely generated algebra over field k and an integral domain. We define the transcendence degree of A over k, $\operatorname{tr\,deg}_k A$, to be the transcendence degree over k of the field of fractions of A (see FT[11] §8). Thus A has transcendence degree d if it contains an algebraically independent set of d elements, but no larger set (FT 8.12).

[11] FT = Fields and Galois Theory, available on my website.

PROPOSITION 12.1. *For any linear forms $\ell_1, \dots, \ell_m$ in $X_1, \dots, X_n$, the quotient ring $k[X_1, \dots, X_n]/(\ell_1, \dots, \ell_m)$ is an integral domain of transcendence degree equal to the dimension of the subspace of k^n defined by the equations*

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

PROOF. This follows from the more precise statement:

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

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

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

and so

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

□

PROPOSITION 12.2. *For any irreducible polynomial f in $k[X_1, \dots, X_n]$, the quotient ring $k[X_1, \dots, X_n]/(f)$ has transcendence degree $n-1$.*

PROOF. Let

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

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

PROPOSITION 12.3. *For any nonzero prime ideal $\mathfrak{p}$ in the k-algebra A,*

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

PROOF. Write

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

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

Suppose otherwise. Then there is a nontrivial algebraic relation among the x_i and f, which we can write

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

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

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

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

PROPOSITION 12.4. *Let A be a unique factorization domain. If $\mathfrak{p}$ is a prime ideal in A such that $\operatorname{tr\,deg}_k A/\mathfrak{p} = \operatorname{tr\,deg}_k A - 1$, then $\mathfrak{p} = (f)$ for some $f \in A$.*

PROOF. The ideal $\mathfrak{p}$ is nonzero because otherwise A and $A/\mathfrak{p}$ would have the same transcendence degree. Therefore $\mathfrak{p}$ contains a nonzero polynomial, and even an irreducible polynomial f, because it is prime. According to (4.1), the ideal (f) is prime. If $(f) \neq \mathfrak{p}$, then

$$\operatorname{tr\,deg}_k A \overset{12.3}{>} \operatorname{tr\,deg}_k A/\mathfrak{p} \overset{12.3}{>} \operatorname{tr\,deg}_k A/(f) \overset{12.2}{=} \operatorname{tr\,deg}_k A - 1,$$

which contradicts the hypothesis. □

THEOREM 12.5. *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 12.6. *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 $g(X)$ be the minimum polynomial of α over K, say,

$$g(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0.$$

Then r divides the degree n of L/K, and $\operatorname{Nm}_{L/K}(\alpha) = \pm a_0^{\frac{n}{r}}$ (FT 5.40). Moreover, a_0 lies in A by (5.9). From the equation

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

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

PROOF (OF THEOREM 12.5). Write $\operatorname{rad}(f)$ as an irredundant intersection of prime ideals $\operatorname{rad}(f) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$. 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 is an integral domain with the same transcendance degree as A, and $\operatorname{rad}(\frac{f}{1}) = S_h^{-1}\mathfrak{p}_1$. Therefore, after replacing A with A_h, we may assume that $\operatorname{rad}(f)$ itself is prime, say, equal to $\mathfrak{p}$.

According to the Noether normalization theorem (5.11), there exist algebraically independent elements $x_1, \dots, x_d$ in A such that A is a finite $k[x_1, \dots, x_d]$-algebra. Note that $d = \operatorname{tr\,deg}_k A$. According to the lemma, $f_0 \stackrel{\text{def}}{=} \operatorname{Nm}(f)$ lies in $k[x_1, \dots, x_d]$, and we shall show that $\mathfrak{p} \cap k[x_1, \dots, x_d] = \operatorname{rad}(f_0)$. Therefore, the homomorphism

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

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

$$\operatorname{tr\,deg}_k A/\mathfrak{p} = \operatorname{tr\,deg}_k k[x_1, \dots, x_d]/\operatorname{rad}(f_0) \stackrel{12.2}{=} d - 1,$$

as required.

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

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

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

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

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

COROLLARY 12.7. *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 12.8. *The length d of any maximal (i.e., nonrefinable) chain of distinct prime ideals*

$$\mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0 \tag{14}$$

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 (12.7), 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 12.9. 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 12.10. We classify the prime ideals $\mathfrak{p}$ in $k[X, Y]$. If $A/\mathfrak{p}$ has dimension 2, then $\mathfrak{p} = (0)$. If $A/\mathfrak{p}$ has dimension 1, then $\mathfrak{p} \neq 0$ and so it contains a nonzero polynomial, and hence a nonzero irreducible polynomial f (being a prime ideal). Then $\mathfrak{p} \supset (f)$, and so equals (f). 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 12.11. Let A be a finitely generated k-algebra whose nilradical $\mathfrak{N}$ is prime (not necessarily an integral domain). Then every maximal chain of distinct prime ideals in A has length $\operatorname{tr}\deg_k(A/\mathfrak{N})$. (Apply Theorem 12.8 to $A/\mathfrak{N}$.)

13 Primary decompositions

In this section, A is an arbitrary commutative ring.

DEFINITION 13.1. An ideal $\mathfrak{q}$ in A is ***primary*** if it is proper and

$$ab \in \mathfrak{q},\ b \notin \mathfrak{q} \implies a^n \in \mathfrak{q} \text{ for some } n \geq 1.$$

Thus, a proper ideal $\mathfrak{q}$ in A is primary if and only if all zero-divisors in $A/\mathfrak{q}$ are nilpotent. Clearly prime ideals are primary, and an ideal (m) in $\mathbb{Z}$ is primary if and only if m is a power of a prime.

PROPOSITION 13.2. *The radical of a primary ideal $\mathfrak{q}$ is a prime ideal containing $\mathfrak{q}$, and it is contained in every other prime ideal containing $\mathfrak{q}$ (i.e., it is the smallest prime ideal containing $\mathfrak{p}$).*

PROOF. Let $ab \in \operatorname{rad}(\mathfrak{q})$, so that some power, say $a^n b^n$, of ab lies in $\mathfrak{q}$. If b is not in $\operatorname{rad}(\mathfrak{q})$, then b^n is not in $\mathfrak{q}$, and so some power of a^n lies in $\mathfrak{q}$, which implies that $a \in \operatorname{rad}(\mathfrak{q})$. Hence $\operatorname{rad}(\mathfrak{q})$ is prime.

Let $\mathfrak{p}$ be a second prime ideal containing $\mathfrak{q}$, and let $a \in \operatorname{rad}(\mathfrak{q})$. For some n, $a^n \in \mathfrak{q} \subset \mathfrak{p}$, which implies that $a \in \mathfrak{p}$. □

When $\mathfrak{q}$ is a primary ideal and $\mathfrak{p}$ is its radical, we say that $\mathfrak{q}$ is ***$\mathfrak{p}$-primary.***

PROPOSITION 13.3. *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. Let $ab \in \mathfrak{q}$; we have to show that either $a \in \mathfrak{m}$ or $b \in \mathfrak{q}$. If $a \notin \mathfrak{m}$, then $(a) + \mathfrak{m} = A$, and so $1 = aa' + m$ for some $a' \in A$ and $m \in \mathfrak{m}$. Therefore, $b = baa' + bm \in \mathfrak{q}$. □

PROPOSITION 13.4. *Let $\varphi\colon A \to B$ be a homomorphism of rings. If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in B, then $\mathfrak{q}^c \stackrel{\text{def}}{=} \varphi^{-1}(\mathfrak{q})$ is a $\mathfrak{p}^c$-primary ideal in A.*

PROOF. The map $A/\mathfrak{q}^c \to B/\mathfrak{q}$ is injective, and so every zero-divisor in $A/\mathfrak{q}^c$ is nilpotent. This shows that $\mathfrak{q}^c$ is primary, and therefore $\operatorname{rad}(\mathfrak{q}^c)$-primary. But (see 2.8), $\operatorname{rad}(\mathfrak{q}^c) = \operatorname{rad}(\mathfrak{q})^c = \mathfrak{p}^c$, as claimed. □

LEMMA 13.5. *Let $\mathfrak{q}$ and $\mathfrak{p}$ be a pair of ideals in A such that $\mathfrak{q} \subset \mathfrak{p} \subset \operatorname{rad}(\mathfrak{q})$. If*

$$ab \in \mathfrak{q} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{q}, \tag{15}$$

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

PROOF. Clearly $\mathfrak{q}$ is primary because if $ab \in \mathfrak{q}$ but $b \notin \mathfrak{q}$, then $a \in \mathfrak{p}$, and so some power of a lies in $\mathfrak{q}$. Therefore $\mathfrak{p}' \stackrel{\text{def}}{=} \operatorname{rad}(\mathfrak{q})$ is prime. By assumption $\mathfrak{p} \subset \mathfrak{p}'$, and it remains to show that they are equal. Let $a \in \mathfrak{p}'$, 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 (15). □

PROPOSITION 13.6. *A finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.*

PROOF. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ be $\mathfrak{p}$-primary, and let $\mathfrak{q} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$. We show that the pair of ideals $\mathfrak{q} \subset \mathfrak{p}$ satisfies the conditions of (13.5).

Let $a \in \mathfrak{p}$; since some power of a belongs to each $\mathfrak{q}_i$, a sufficiently high power of it will belong to all of them, and so $\mathfrak{p} \subset \operatorname{rad}(\mathfrak{q})$.

Let $ab \in \mathfrak{q}$ but $a \notin \mathfrak{p}$. Then $ab \in \mathfrak{q}_i$ but $a \notin \mathfrak{p}$, and so $b \in \mathfrak{q}_i$. Since this is true for all i, we have that $b \in \mathfrak{q}$. □

The ***minimal prime ideals*** of an ideal $\mathfrak{a}$ are the minimal elements of the set of prime ideals containing $\mathfrak{a}$.

DEFINITION 13.7. A ***primary decomposition*** of an ideal $\mathfrak{a}$ is a finite set of primary ideals whose intersection is $\mathfrak{a}$.

DEFINITION 13.8. A primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ of $\mathfrak{a}$ is ***minimal*** if

(a) the prime ideals $\operatorname{rad}(\mathfrak{q}_i)$ are distinct, and
(b) no $\mathfrak{q}_i$ can be omitted, i.e., for no i is $\mathfrak{q}_i \supset \bigcap_{j \neq i} \mathfrak{q}_j$.

If $\mathfrak{a}$ admits a primary decomposition, then it admits a minimal primary decomposition, because Proposition 13.6 can be used to combine primary ideals with the same radical, and any $\mathfrak{q}_i$ that fails (b) can simply be omitted. The prime ideals occurring as the radical of an ideal in a minimal primary decomposition of $\mathfrak{a}$ are said to ***belong*** to $\mathfrak{a}$.

PROPOSITION 13.9. *Suppose $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary for $i = 1, \dots, n$. Then the minimal prime ideals of $\mathfrak{a}$ are the minimal elements of the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.*

PROOF. Let $\mathfrak{p}$ be a prime ideal containing $\mathfrak{a}$, and let $\mathfrak{q}_i'$ be the image of $\mathfrak{q}_i$ in the integral domain $A/\mathfrak{p}$. Then $\mathfrak{p}$ contains $\mathfrak{q}_1 \cdots \mathfrak{q}_n$, and so $\mathfrak{q}_1' \cdots \mathfrak{q}_n' = 0$. This implies that, for some i, $\mathfrak{q}_i' = 0$, and so $\mathfrak{p}$ contains $\mathfrak{q}_i$. Now (13.2) shows that $\mathfrak{p}$ contains $\mathfrak{p}_i$. □

In particular, if $\mathfrak{a}$ admits a primary decomposition, then it has only finitely many minimal prime ideals, and so its radical is a *finite* intersection of prime ideals.

For an ideal $\mathfrak{a}$ in A and an element $x \in A$, we let

$$(\mathfrak{a}\colon x) = \{a \in A \mid ax \in \mathfrak{a}\}.$$

It is again an ideal in A.

THEOREM 13.10. *Let $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ be a minimal primary decomposition of $\mathfrak{a}$, and let $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$. Then*

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

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

PROOF. TBA. □

THEOREM 13.11. *In a noetherian ring, every ideal admits a primary decomposition.*

An ideal $\mathfrak{a}$ is said to be ***irreducible*** if

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \text{ } (\mathfrak{b}, \mathfrak{c} \text{ ideals}) \implies \mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}.$$

The theorem is a consequence of the following more precise statement.

PROPOSITION 13.12. *Let A be a noetherian ring.*
(a) *Every ideal in A can be expressed as a finite intersection of irreducible ideals.*
(b) *Every irreducible ideal in A is primary.*

PROOF. (a) Suppose (a) fails, and let $\mathfrak{a}$ be maximal among the ideals for which it fails. Then, in particular, $\mathfrak{a}$ itself is not irreducible, and so $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ with $\mathfrak{b}$ and $\mathfrak{c}$ properly containing $\mathfrak{a}$. Because $\mathfrak{a}$ is maximal, both $\mathfrak{b}$ and $\mathfrak{c}$ can be expressed as finite intersections of irreducible ideals, but then so can $\mathfrak{a}$.

(b) Let $\mathfrak{a}$ be irreducible, and consider the quotient ring $A' \stackrel{\text{def}}{=} A/\mathfrak{a}$. Let a be a zero-divisor in A', say $ab = 0$ with $b \neq 0$. We have to show that a is nilpotent. As A' is noetherian, the chain of ideals

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

becomes constant, say, $(0 : (a^m)) = (0 : (a^{m+1})) = \cdots$. Let $c \in (a^m) \cap (b)$. Because $c \in (b)$, we have $ca = 0$; because $c \in (a^m)$, we have $c = da^m$ for some $d \in A$; but now $(da^m)a = 0$, and so $d \in (0 : a^{m+1}) = (0 : a^m)$, which implies that $c = 0$. Hence $(a^m) \cap (b) = (0)$. Because $\mathfrak{a}$ is irreducible, so also is the zero ideal in A', and it follows that $a^m = 0$. □

PROPOSITION 13.13. *Let $\mathfrak{m}$ be a maximal ideal in a noetherian ring A. A proper ideal $\mathfrak{a}$ of A is $\mathfrak{m}$-primary if and only if it contains a power of $\mathfrak{m}$.*

PROOF. By definition, if $\mathfrak{a}$ is $\mathfrak{m}$-primary, then $\mathfrak{m} = \operatorname{rad}(\mathfrak{a})$, and so $\mathfrak{a}$ contains a power of $\mathfrak{m}$ by Proposition 3.11. Conversely, suppose that $\mathfrak{m}^r \subset \mathfrak{a}$. 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. □

14 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 14.1. *An artinian ring has Krull dimension zero; in other words, every prime ideal is maximal.*

PROOF. Let $\mathfrak{p}$ be a prime ideal of an artinian ring A, and let $A' = A/\mathfrak{p}$. Then A' is an artinian integral domain. For any nonzero element a of A', the chain $(a) \supset (a^2) \supset \cdots$ eventually becomes constant, and so $a^n = a^{n+1}b$ for some $b \in A'$ and $n \geq 1$. We can cancel a^n to obtain $1 = ab$. It follows that a is a unit, A' is a field, and $\mathfrak{p}$ is maximal. □

COROLLARY 14.2. *In an artinian ring, the radical and the Jacobson radical coincide.*

PROOF. The first is the intersection of the prime ideals (2.2), and the second is the intersection of the maximal ideals (2.4). □

PROPOSITION 14.3. *An artinian ring has only finitely many maximal ideals.*

PROOF. Let $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ be minimal in the set of all finite intersections of maximal ideals in the artinian ring A. Then any other maximal ideal $\mathfrak{m}$ contains $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$. This implies that $\mathfrak{m}$ equals one of the $\mathfrak{m}_i$, because otherwise there exists an $a_i \in \mathfrak{m}_i \smallsetminus \mathfrak{m}$ for each i, and $a_1 \cdots a_n$ lies in $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_n$ but not $\mathfrak{m}$ (because $\mathfrak{m}$ is prime), which is a contradiction. □

PROPOSITION 14.4. *In an artinian ring, some power of the radical is zero.*

PROOF. Let $\mathfrak{N}$ be the nilradical of the artinian ring A. The chain $\mathfrak{N} \supset \mathfrak{N}^2 \supset \cdots$ eventually becomes constant, and so $\mathfrak{N}^n = \mathfrak{N}^{n+1} = \cdots$ for some $n \geq 1$. Suppose $\mathfrak{N}^n \neq 0$. Then there exist ideals $\mathfrak{a}$ such that $\mathfrak{a} \cdot \mathfrak{N}^n \neq 0$, for example $\mathfrak{N}$, and we may suppose that $\mathfrak{a}$ has been chosen to be minimal among such ideals. There exists $a \in \mathfrak{a}$ 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 $a = ax = ax^2 = \cdots = a0$ because $x \in \mathfrak{N}$. This contradicts the definition of a, and so $\mathfrak{N}^n = 0$. □

LEMMA 14.5. *Let A be a ring in which some finite product of maximal ideals is zero. Then A is artinian if and only if it is noetherian.*

PROOF. Suppose $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$ with the $\mathfrak{m}_i$ maximal ideals (not necessarily distinct), and consider

$$A \supset \mathfrak{m}_1 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_{r-1} \supset \mathfrak{m}_1 \cdots \mathfrak{m}_r \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_n = 0.$$

The action of A on the quotient $M_r \stackrel{\text{def}}{=} \mathfrak{m}_1 \cdots \mathfrak{m}_{r-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_r$ factors through the field $A/\mathfrak{m}_r$, and the subspaces of the vector space M_r are in one-to-one correspondence with the ideals of A contained between $\mathfrak{m}_1 \cdots \mathfrak{m}_{r-1}$ and $\mathfrak{m}_1 \cdots \mathfrak{m}_r$. If A is either artinian or noetherian, then M_r satisfies a chain condition on subspaces and so it is finite-dimensional as a vector space and both artinian and noetherian as an A-module. Now repeated applications of Proposition 3.3 (resp. its analogue for artinian modules) show that if A is artinian (resp. noetherian), then it is noetherian (resp. artinian) as an A-module, and hence as a ring. □

THEOREM 14.6. *A ring is artinian if and only if it is noetherian of dimension zero.*

PROOF. $\Rightarrow$: Let A be an artinian ring. After (14.1), it remains to show that A is noetherian, but according to (14.2), (14.3), and (14.4), some finite product of maximal ideals is zero, and so this follows from the lemma.

$\Leftarrow$: Let A be a noetherian ring of dimension zero. The zero ideal admits a primary decomposition (13.11), and so A has only finitely many minimal prime ideals, which are all maximal because $\dim A = 0$. Hence $\mathfrak{N}$ is a finite intersection of maximal ideals (2.2), and since some power of $\mathfrak{N}$ is zero (3.11), we again have that some finite product of maximal ideals is zero, and so can apply the lemma. □

THEOREM 14.7. *Every artinian ring is (uniquely) a product of local artinian rings.*

PROOF. Let A be artinian, and let $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ be the distinct maximal ideals in A. We saw in the proof of (14.6) 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 2.10 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. □

15 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. 2.7). Note that $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}^e \overset{\text{def}}{=} \mathfrak{p}A_{\mathfrak{p}}$ (by 6.5). 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 $\mathfrak{p}^{(n)}$.

LEMMA 15.1. *The ideal $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.*

PROOF. According to Proposition 13.3, the ideal $(\mathfrak{p}^e)^n$ is $\mathfrak{p}^e$-primary. Hence (see 13.4), $((\mathfrak{p}^e)^n)^c$ is $(\mathfrak{p}^e)^c$-primary. But $\mathfrak{p}^{ec} = \mathfrak{p}$ (see 6.5), and

$$\left(\left(\mathfrak{p}^e\right)^n\right)^c \overset{2.8}{=} \left((\mathfrak{p}^n)^e\right)^c \overset{\text{def}}{=} \mathfrak{p}^{(n)}. \tag{16}$$

□

LEMMA 15.2. *Consider ideals $\mathfrak{a} \subset \mathfrak{p}' \subset \mathfrak{p}$ with $\mathfrak{p}'$ prime. If $\mathfrak{p}'$ is a minimal prime ideal of $\mathfrak{a}$, then $\mathfrak{p}'^e$ is a minimal prime ideal of $\mathfrak{a}^e$ (extension relative to $A \to A_{\mathfrak{p}}$).*

PROOF. If not, there exists a prime ideal $\mathfrak{p}'' \neq \mathfrak{p}'^e$ such that $\mathfrak{p}'^e \supset \mathfrak{p}'' \supset \mathfrak{a}^e$. Now, by (6.5),

$$\mathfrak{p}' = \mathfrak{p}'^{ec} \supsetneq \mathfrak{p}''^c \supset \mathfrak{a}^{ec} \supset \mathfrak{a},$$

which contradicts the minimality of $\mathfrak{p}$. □

THEOREM 15.3 (KRULL'S PRINCIPAL IDEAL THEOREM). *Let A be a noetherian ring. For any nonunit $b \in A$, the height of a minimal prime ideal $\mathfrak{p}$ of (b) is at most one.*

PROOF. Consider $A \to A_{\mathfrak{p}}$. According to Lemma 15.2, $\mathfrak{p}^e$ is a minimal prime ideal of $(b)^e = (\frac{b}{1})$, and (6.5) 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 14.6). 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

$$\mathfrak{p}_1^{(s)} + (b) = \mathfrak{p}_1^{(s+1)} + (b) = \mathfrak{p}_1^{(s+2)} + (b) = \cdots . \tag{17}$$

We claim that, for any $m \geq s$,

$$\mathfrak{p}_1^{(m)} \subset (b)\mathfrak{p}_1^{(m)} + \mathfrak{p}_1^{(m+1)}. \tag{18}$$

Let $x \in \mathfrak{p}_1^{(m)}$. Then

$$x \in (b) + \mathfrak{p}_1^{(m)} \overset{(17)}{=} (b) + \mathfrak{p}_1^{(m+1)},$$

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 (15.1) and $ab = x - x' \in \mathfrak{p}_1^{(m)}$ but $b \notin \mathfrak{p}_1$, we have that $a \in \mathfrak{p}_1^{(m)}$. Now $x = ab + x' \in (b)\mathfrak{p}_1^{(m)} + \mathfrak{p}_1^{(m+1)}$ as claimed.

We next show that, for any $m \geq s$,

$$\mathfrak{p}_1^{(m)} = \mathfrak{p}_1^{(m+1)}.$$

As $b \in \mathfrak{p}$, (18) 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 (3.6).

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

$$\bigcap\nolimits_{m\geq s} \mathfrak{p}_1^{(m)} \overset{(16)}{=} \bigcap\nolimits_{m\geq s} ((\mathfrak{p}_1^e)^m)^c = (\bigcap\nolimits_{m\geq s} (\mathfrak{p}_1^e)^m)^c \overset{3.10}{=} (0)^c,$$

and so for any $x \in \mathfrak{p}_1^s$, there exists an $a \in A \smallsetminus \mathfrak{p}_1$ such that $ax = 0$. Let $x \in \mathfrak{p}_1$; then $ax^s = 0$ for some $a \in A \smallsetminus \mathfrak{p}_1 \supset A \smallsetminus \mathfrak{p}_2$, and so $x \in \mathfrak{p}_2$ (because $\mathfrak{p}_2$ is prime). We have shown that $\mathfrak{p}_1 = \mathfrak{p}_2$, as required. □

LEMMA 15.4. *Let $\mathfrak{p}$ be a prime ideal in a noetherian ring A, and let S be a finite set of prime ideals in A, none of which contains $\mathfrak{p}$. If there exists a chain of distinct prime ideals*

$$\mathfrak{p} \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0,$$

then there exists such a chain with $\mathfrak{p}_1$ not contained in any ideal in S.

PROOF. We first prove this in the special case that the chain has length 2. Suppose that $\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_0$ are distinct prime ideals and that $\mathfrak{p}$ is not contained in any prime ideal in S. According to Proposition 2.5, there exists an element

$$a \in \mathfrak{p} \smallsetminus (\mathfrak{p}_0 \cup \bigcup\{\mathfrak{p}' \in S\}).$$

As $\mathfrak{p}$ contains $(a) + \mathfrak{p}_0 \subset \mathfrak{p}$, it also contains a minimal prime ideal $\mathfrak{p}_1'$ of $(a) + \mathfrak{p}_0$. 0Now $\mathfrak{p}_1'/\mathfrak{p}_0$ 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 15.5. *Let A be a noetherian ring. For any proper ideal $\mathfrak{a} = (a_1, \dots, a_m)$, the height of a minimal prime ideal of $\mathfrak{a}$ is at most m.*

PROOF. For $m = 1$, this was just proved. Thus, we may suppose $m \geq 2$ and that the theorem has been proved for ideals generated by $m-1$ elements. Let $\mathfrak{p}$ be a minimal prime ideal of $\mathfrak{a}$, and let $\mathfrak{p}'_1, \dots, \mathfrak{p}'_t$ be the minimal prime ideals of $(a_2, \dots, a_m)$. Each $\mathfrak{p}'_i$ has height at most $m-1$. If $\mathfrak{p}$ is contained in one of the $\mathfrak{p}'_i$, it will have height $\leq m-1$, and so we may suppose that it isn't.

Let $\mathfrak{p}$ have height d. We have to show that $d \leq m$. According to the lemma, there exists a chain of distinct prime ideals

$$\mathfrak{p} = \mathfrak{p}_d \supset \mathfrak{p}_{d-1} \supset \cdots \supset \mathfrak{p}_0, \quad d \geq 1,$$

with $\mathfrak{p}_1$ not contained in any $\mathfrak{p}'_i$, and so Proposition 2.5 shows that there exists a

$$b \in \mathfrak{p}_1 \smallsetminus \bigcup\nolimits_{i=1}^{r} \mathfrak{p}'_i.$$

We next show that $\mathfrak{p}$ is a minimal prime ideal of $(b, a_2, \dots, a_m)$. Certainly $\mathfrak{p}$ contains a minimal prime ideal $\mathfrak{p}'$ of this ideal. As $\mathfrak{p}' \supset (a_2, \dots, a_m)$, it 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 $\bar{\mathfrak{p}} \stackrel{\text{def}}{=} \mathfrak{p}/(a_2, \dots, a_m)$ has height at least 2 in $\bar{A} \stackrel{\text{def}}{=} A/(a_2, \dots, a_m)$. But $\bar{\mathfrak{p}}$ is a minimal ideal in $\bar{A}$ of the principal ideal $(a_1, \dots, a_n)/(a_2, \dots, a_n)$, which contradicts Theorem 15.3. Hence $\mathfrak{p}$ is minimal, as claimed.

But now $\mathfrak{p}/(b)$ is a minimal prime ideal of $(b, a_2, \dots, a_m)$ in $R/(b)$, and so the height of $\mathfrak{p}/(b)$ is at most $m-1$ (by induction). The prime ideals

$$\mathfrak{p}/(b) = \mathfrak{p}_d/(b) \supset \mathfrak{p}_{d-1}/(b) \supset \cdots \supset \mathfrak{p}_1/(b)$$

are distinct, and so $d - 1 \leq m - 1$. This completes the proof that $d = m$. □

The ***height*** of an ideal in a noetherian ring is the minimum height of a prime ideal containing it.

The following provides a (strong) converse to Theorem 15.5.

THEOREM 15.6. *Let A be a noetherian ring, and let $\mathfrak{a}$ be a proper ideal of A of height r. Then there exist r elements $a_1, \dots, a_r$ of $\mathfrak{a}$ such that, for each $i \leq r$, $(a_1, \dots, a_i)$ has height i.*

PROOF. If $r = 0$, then we take the empty set of a_is. Thus, suppose $r \geq 1$. There are only finitely many prime ideals of height 0, because such an ideal is a minimal prime ideal of (0), and none of these ideals can contain $\mathfrak{a}$ because it has height ≥ 1. Proposition 2.5 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 15.3 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

$$a_2 \in \mathfrak{a} \smallsetminus \bigcup\{\text{prime ideals of height } 1 \text{ containing } (a_1)\}.$$

By construction, (a_1, a_2) has height at least 2, and so Theorem 15.5 shows that it has height exactly 2.

This completes the proof when $r = 2$, and when $r > 2$ we can continue in this fashion until it is complete.

COROLLARY 15.7. *Every prime ideal of height r in a noetherian ring arises as a minimal prime ideal for an ideal generated by r elements.*

PROOF. According to the theorem, an ideal $\mathfrak{a}$ of height r contains an ideal $(a_1, \dots, a_r)$ of height r. If $\mathfrak{a}$ is prime, then it is a minimal ideal of $(a_1, \dots, a_r)$. □

COROLLARY 15.8. *Let A be a commutative noetherian ring, and let $\mathfrak{a}$ be an ideal in A that can be generated by n elements. For any prime ideal $\mathfrak{p}$ in A containing $\mathfrak{a}$,*

$$\operatorname{ht}(\mathfrak{p}/\mathfrak{a}) \leq \operatorname{ht}(\mathfrak{p}) \leq \operatorname{ht}(\mathfrak{p}/\mathfrak{a}) + n.$$

PROOF. The first inequality follows immediately from the correspondence between ideals in A and in $A/\mathfrak{a}$.

Denote the quotient map $A \to A' \stackrel{\text{def}}{=} A/\mathfrak{a}$ by $a \mapsto a'$. Let $\operatorname{ht}(\mathfrak{p}/\mathfrak{a}) = d$. Then there exist elements $a_1, \dots, a_d$ in A such that $\mathfrak{p}/\mathfrak{a}$ is a minimal prime ideal of $(a_1', \dots, a_d')$. Let $b_1, \dots, b_n$ generate $\mathfrak{a}$. Then $\mathfrak{p}$ is a minimal prime ideal of $(a_1, \dots, a_d, b_1, \dots, b_n)$, and hence has height $\leq d + n$. □

16 Regular local rings

Throughout this section, A is a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field k. Recall that A has finite height d, equal to the height of $\mathfrak{m}$. According to (15.5), the ideal $\mathfrak{m}$ requires at least d generators; when it can be generated by d elements, the ring A is said to be ***regular***. In other words (see 3.7) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq d$, 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 this is true in general.

LEMMA 16.1. *Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$, and let $c \in \mathfrak{m} \setminus \mathfrak{m}^2$. Denote the quotient map $A \to A' \stackrel{\text{def}}{=} A/(c)$ by $a \mapsto a'$. Then*

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k \mathfrak{m}'/\mathfrak{m}'^2 + 1$$

where $\mathfrak{m}' \stackrel{\text{def}}{=} \mathfrak{m}/(c)$ is the maximal ideal of A'.

PROOF. Let $e_1, \dots, e_n$ be elements of $\mathfrak{m}$ such that $\{e_1', \dots, e_n'\}$ is a k-linear basis for $\mathfrak{m}'/\mathfrak{m}'^2$. We shall show that $\{e_1, \dots, e_n, c\}$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$.

As $e_1', \dots, e_n'$ span $\mathfrak{m}'/\mathfrak{m}'^2$, they generate the ideal $\mathfrak{m}'$ (see 3.7), and so $\mathfrak{m} = (e_1, \dots, e_n) + (c)$, which implies that $\{e_1, \dots, e_n, c\}$ spans $\mathfrak{m}/\mathfrak{m}^2$.

Suppose that $a_1, \dots, a_{n+1}$ are elements of A such that

$$a_1e_1 + \cdots + a_ne_n + a_{n+1}c \equiv 0 \bmod \mathfrak{m}^2. \tag{19}$$

Then

$$a_1'e_1' + \cdots + a_n'e_n' \equiv 0 \bmod \mathfrak{m}'^2,$$

and so $a_1', \dots, a_n' \in \mathfrak{m}'$. It follows that $a_1, \dots, a_n \in \mathfrak{m}$. Now (19) 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 (19) is the trivial one. □

PROPOSITION 16.2. *If A is regular, then so also is $A/(a)$ for any $a \in \mathfrak{m} \setminus \mathfrak{m}^2$; moreover, $\dim A = \dim A/(a) + 1$.*

PROOF. With the usual notations, (15.8) shows that

$$\operatorname{ht}(\mathfrak{m}') \le \operatorname{ht}(\mathfrak{m}) \le \operatorname{ht}(\mathfrak{m}') + 1.$$

Therefore

$$\dim_k(\mathfrak{m}'/\mathfrak{m}'^2) \ge \operatorname{ht}(\mathfrak{m}') \ge \operatorname{ht}(\mathfrak{m}) - 1 = \dim_k(\mathfrak{m}/\mathfrak{m}^2) - 1 = \dim_k(\mathfrak{m}'/\mathfrak{m}'^2).$$

Equalities must hold throughout, which proves that A' is regular with dimension $\dim A - 1$. □

THEOREM 16.3. *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 properly contains a principal ideal $\mathfrak{a} = (a)$ that properly contains a prime ideal $\mathfrak{p}$. Let $b \in \mathfrak{p}$, and suppose $b \in \mathfrak{a}^n = (a^n)$ 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 $b \in \bigcap_n \mathfrak{a}^n \stackrel{3.10}{=} \{0\}$. Therefore $\mathfrak{p} = \{0\}$, and so A is an integral domain.

We now assume $d \ge 1$, and proceed by induction on d. Let $a \in \mathfrak{m} \setminus \mathfrak{m}^2$. 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 $a \in \mathfrak{m} \setminus \mathfrak{m}^2$, 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 (§13) that S is finite. We have shown that $\mathfrak{m} \setminus \mathfrak{m}^2 \subset \bigcup\{\mathfrak{p} \mid \mathfrak{p} \in S\}$, and so $\mathfrak{m} \subset \mathfrak{m}^2 \cup \bigcup\{\mathfrak{p} \mid \mathfrak{p} \in S\}$. It follows from Proposition 2.6 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 16.4. *A regular local ring of dimension 1 is a principal ideal domain (with a single nonzero prime ideal).*

PROOF. TBA. □

17 Connections with geometry

Throughout this section, k is a field.

For a finitely generated k-algebra A, define $\operatorname{Spm} A$ to be the pair $(\operatorname{spm} A, A)$. We (temporarily) call such a pair an ***affine algebraic space***. When A is geometrically reduced (i.e., $A \otimes_k k^{\mathrm{al}}$ is reduced) we call $\operatorname{Spm} A$ and ***affine algebraic variety***. The affine algebraic spaces (resp. varieties) form a category with the obvious notion of morphism, in which finite products exist.

TANGENT SPACES

For $V = \operatorname{Spm} A$, define $V(R) = \operatorname{Hom}_{k\text{-algebra}}(A, R)$.

Let $k[\varepsilon]$ be the ring of dual numbers (so $\varepsilon^2 = 0$). For an affine algebraic variety V over k, the map $\varepsilon \mapsto 0 \colon k[\varepsilon] \to k$ defines a map

$$V(k[\varepsilon]) \to V(k).$$

For any $a \in V(k)$, we define the ***tangent space*** to V at a, $\operatorname{Tgt}_a(V)$, to be the fibre of this map over a.

PROPOSITION 17.1. *There is a canonical isomorphism*

$$\operatorname{Tgt}_a(V) \simeq \operatorname{Hom}_{k\text{-lin}}(\mathfrak{m}_a/\mathfrak{m}_a^2, k).$$

This follows from the next two lemmas.

Let $V = V(\mathfrak{a}) \subset k^n$, and assume that the origin o lies on V. Let $\mathfrak{a}_\ell$ be the ideal generated by the linear terms f_ℓ of the $f \in \mathfrak{a}$. By definition, $T_o(V) = V(\mathfrak{a}_\ell)$. Let $A_\ell = k[X_1, \dots, X_n]/\mathfrak{a}_\ell$, and let $\mathfrak{m}$ be the maximal ideal in $k[V]$ consisting of the functions zero at o; thus $\mathfrak{m} = (x_1, \dots, x_n)$.

LEMMA 17.2. *There is a canonical isomorphism*

$$\operatorname{Hom}_{k\text{-lin}}(\mathfrak{m}/\mathfrak{m}^2, k) \xrightarrow{\simeq} \operatorname{Hom}_{k\text{-alg}}(A_\ell, k).$$

PROOF. Let $\mathfrak{n} = (X_1, \dots, X_n)$ be the maximal ideal at the origin in $k[X_1, \dots, X_n]$. Then $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathfrak{n}/(\mathfrak{n}^2 + \mathfrak{a})$, and as $f - f_\ell \in \mathfrak{n}^2$ for every $f \in \mathfrak{a}$, it follows that $\mathfrak{m}/\mathfrak{m}^2 \simeq \mathfrak{n}/(\mathfrak{n}^2 + \mathfrak{a}_\ell)$. Let $f_{1,\ell}, \dots, f_{r,\ell}$ be a basis for the vector space $\mathfrak{a}_\ell$. From linear algebra we know that there are $n - r$ linear forms $X_{i_1}, \dots, X_{i_{n-r}}$ forming with the $f_{i,\ell}$ a basis for the linear forms on k^n. Then $X_{i_1} + \mathfrak{m}^2, \dots, X_{i_{n-r}} + \mathfrak{m}^2$ form a basis for $\mathfrak{m}/\mathfrak{m}^2$ as a k-vector space, and the lemma shows that $A_\ell \simeq k[X_{i_1} \dots, X_{i_{n-r}}]$. A homomorphism $\alpha \colon A_\ell \to k$ of k-algebras is determined by its values $\alpha(X_{i_1}), \dots, \alpha(X_{i_{n-r}})$, and they can be arbitrarily given. Since the k-linear maps $\mathfrak{m}/\mathfrak{m}^2 \to k$ have a similar description, the first isomorphism is now obvious. □

LEMMA 17.3. *There is a canonical isomorphism*

$$\operatorname{Hom}_{k\text{-alg}}(A_\ell, k) \xrightarrow{\simeq} T_o(V).$$

PROOF. To give a k-algebra homomorphism $A_\ell \to k$ is the same as to give an element $(a_1, \dots, a_n) \in k^n$ such that $f(a_1, \dots, a_n) = 0$ for all $f \in A_\ell$, which is the same as to give an element of $T_P(V)$. □

NONSINGULAR POINTS AND REGULAR POINTS

The ***dimension*** of an affine algebraic space $\operatorname{Spm} A$ is the Krull dimension of A. Therefore, if A is integral, then it is the transcendence degree over k of the field of fractions of A.An $a \in V(k)$ is nonsingular if $\dim \operatorname{Tgt}_a(V) = \dim V$, and V is nonsingular if every point $a \in V(k)$ is nonsingular.

PROPOSITION 17.4. *Let V be an affine algebraic space over an algebraically closed field k, and identify V with $V(k)$. The set of nonsingular points of V is open, and it is nonempty for an affine algebraic variety.*

PROOF. TBA. □

An affine algebraic variety V over a field k is ***smooth*** if $V_{k^{\mathrm{al}}}$ is nonsingular.

AFFINE ALGEBRAIC SCHEMES, SPACES, AND VARIETIES

TBA.

References

CARTIER, P. 2007. A primer of Hopf algebras, pp. 537–615. *In* Frontiers in number theory, physics, and geometry. II. Springer, Berlin. Preprint available at IHES.

KRULL, W. 1938. Dimensionstheorie in stellenringen. *J. Reine Angew. Math.* 179:204–226.

NAGATA, M. 1962. Local rings. Interscience Tracts in Pure and Applied Mathematics, No. 13. Interscience Publishers, New York-London.

NORTHCOTT, D. G. 1953. Ideal theory. Cambridge Tracts in Mathematics and Mathematical Physics, No. 42. Cambridge, at the University Press.

Index