

Lectures on Commutative Algebra

Sudhir R. Ghorpade

Department of Mathematics
Indian Institute of Technology Bombay
Powai, Mumbai 400 076, India

E-Mail: srg@math.iitb.ac.in
URL: <http://www.math.iitb.ac.in/~srg/>



Annual Foundation School - II
(Sponsored by the National Board for Higher Mathematics)
Bhaskaracharya Pratishthana, Pune
and
Department of Mathematics, University of Pune
June 2006

Contents

1	Rings and Modules	3
1.1	Ideals and Radicals	3
1.2	Polynomial rings and Localization of rings	8
1.3	Modules	11
1.4	Zariski Topology	12
	Exercises	14
2	Noetherian Rings	17
2.1	Noetherian Rings and Modules	17
2.2	Primary Decomposition of Ideals	19
2.3	Artinian Rings and Modules	23
2.4	Krull's Principal Ideal Theorem	27
	Exercises	29
3	Integral Extensions	32
3.1	Integral Extensions	32
3.2	Noether Normalization	35
3.3	Finiteness of Integral Closure	38
	Exercises	42
4	Dedekind Domains	44
4.1	Dedekind Domains	45
4.2	Extensions of Primes	50
	Exercises	53
A	Primary Decomposition of Modules	55
A.1	Associated Primes of Modules	55
A.2	Primary Decomposition of Modules	58
	Exercises	62
	References	62

Chapter 1

Rings and Modules

In this chapter, we shall review a number of basic notions and results concerning rings and modules. First, let us settle the basic terminology and notation that we shall use throughout these notes.

By a ring we mean a commutative ring with identity. For sets I, J , we write $I \subseteq J$ to denote that I is a subset of J and $I \subset J$ to denote that I is a proper subset of J , that is, $I \subseteq J$ and $I \neq J$. We denote the set of nonnegative integers by \mathbb{N} and for any $n \in \mathbb{N}$, by \mathbb{N}^n we denote the set of all n -tuples of elements of \mathbb{N} . We sometimes use the abbreviation ‘iff’ to mean ‘if and only if’.

1.1 Ideals and Radicals

Historically, the notion of an ideal arose in an attempt to prove Fermat’s Last Theorem (see Chapter 4 for more on this). From a formal viewpoint, an ideal of a ring is analogous to a normal subgroup of a group. More precisely, an *ideal* of a ring A is a subset I of A satisfying (i) I is a subgroup of A with respect to addition, and (ii) whenever $a \in I$ and $x \in A$, we have $ax \in I$. If A is a ring and I is an ideal of A , then we can construct a new ring, denoted by A/I and called the *residue class ring* or the *quotient ring* obtained from “moding out” A by I . The elements of A/I are the cosets $x+I := \{x+a : a \in I\}$ where x varies over A . Addition and multiplication in A/I is defined by $(x+I)+(y+I) = (x+y)+I$ and $(x+I)(y+I) = xy+I$. The fact that I is an ideal of A ensures that this addition and multiplication is well-defined and A/I is a ring with respect to these operations. Passing to A/I from A has the effect of making I the null element. We have a natural surjective homomorphism $q : A \rightarrow A/I$ given by $q(x) := x+I$ for $x \in A$. The kernel of q is precisely the ideal I . Conversely, if $\phi : A \rightarrow B$ is any ring homomorphism (that is, a map of rings satisfying $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$ for every $x, y \in A$), then the kernel of ϕ (which, by definition, is the set of all $a \in A$ such that $\phi(a) = 0$) is an ideal of A ;

moreover, if $I = \ker \phi$ denotes the kernel of ϕ , then A/I is isomorphic to the image of ϕ . In short, residue class ring and homomorphic image are identical notions. If I is an ideal of a ring A , then there is a one-to-one correspondence between the ideals of A containing I and the ideals of A/I given by $J \mapsto q(J) = J/I$ and $J' \mapsto q^{-1}(J')$.

An easy way to generate examples of ideals is to look at ideals generated by a bunch of elements of the ring. Given a ring A and elements $a_1, \dots, a_n \in A$, the set

$$(a_1, \dots, a_n) := \{ a_1x_1 + \dots + a_nx_n : x_1, \dots, x_n \in A \}$$

is clearly an ideal of A and it is called the *ideal generated by* a_1, \dots, a_n . More generally, given any ring A and a subset E of A , by EA we denote the set of all finite A -linear combinations of elements of E . Clearly, EA is an ideal of A and it is called the *ideal generated by* E . Ideals generated by a single element are called *principal*. Thus, an ideal I of a ring A is called a *principal ideal* if $I = (a)$ for some $a \in A$. By a *principal ideal ring* or *PIR* we mean a ring in which every ideal is principal. An integral domain which is also a PIR is called a *principal ideal domain* or simply, a *PID*.

All the basic algebraic operations are applicable to ideals of a ring. Let A be a ring and let I and J be ideals of A . The *sum* of I and J is defined by $I + J := \{a + b : a \in I, b \in J\}$, whereas the *product* of I and J is defined by $IJ := \{\sum a_i b_i : a_i \in I, b_i \in J\}$. Clearly, $I + J$ and IJ are ideals of A . It may be remarked that the product IJ is closely related, but not quite the same as, the ideal $I \cap J$ given by the intersection of I and J . For example, if A is a PID, $I = (a)$ and $J = (b)$, then $IJ = (ab)$ whereas $I \cap J = (\ell)$ and $I + J = (d)$, where $\ell = \text{LCM}(a, b)$ and $d = \text{GCD}(a, b)$. Analogue of division is given by the *colon ideal* $(I : J) := \{a \in A : aJ \subseteq I\}$. Note that $(I : J)$ ideal of A . If J equals a principal ideal (x) , then $(I : J)$ is often denoted simply by $(I : x)$. For example, if A is a PID, $I = (a)$ and $J = (b)$, then $(I : J) = (a/d)$, where $d = \text{GCD}(a, b)$. We can also consider the *radical* of an ideal I . It is defined by $\sqrt{I} := \{a \in A : a^n \in I \text{ for some } n \geq 1\}$ and it is readily seen to be an ideal of A (by Binomial Theorem!). One says that I is a *radical ideal* if $\sqrt{I} = I$. Note that the notions of sum and intersections of ideals extend easily to arbitrary families of ideals, whereas the notion of a product of ideals extends easily to finite families of ideals.

Having defined algebraic operations for ideals, it is natural to see if the basic notions of arithmetic find an analogue in the setting of ideals. It turns out that the notion of a prime number has two distinct analogues as follows. Let A be a ring and I be an ideal of A . We say that I is *prime* if $I \neq A$ and for any $a, b \in A$, whenever $ab \in I$, we have $a \in I$ or $b \in I$. We say that I is *maximal* if for any ideal J of A satisfying $I \subseteq J$, we have $J = I$ or $J = A$. The set of all prime ideals of A is denoted by $\text{Spec}(A)$, whereas the set of all maximal ideals of A is denoted by $\text{Max}(A)$. It is easy to see that

I is a prime ideal if and only if A/I is an integral domain, and also that I is a maximal ideal if and only if A/I is a field. Using this (or alternatively, by a simple direct argument), we see that every maximal ideal is prime, that is, $\text{Max}(A) \subseteq \text{Spec}(A)$.

Examples 1.1. (i) If A is the zero ring, then $\text{Spec}(A) = \emptyset = \text{Max}(A)$.

(ii) If A is a field, then $\text{Spec}(A) = \{(0)\} = \text{Max}(A)$.

(iii) If $A = \mathbb{Z}$, then $\text{Spec}(A) = \{(0)\} \cup \{(p) : p \text{ is a prime number}\}$, and $\text{Max}(A) = \{(p) : p \text{ is a prime number}\}$.

If A is a ring and P is a nonunit ideal of A , that is, P is an ideal of A satisfying $P \neq A$, then it is evident that P is a prime ideal if and only if P satisfies the following property: if $\bigcap_{j=1}^n I_j \subseteq P$ for any ideals I_1, \dots, I_n of A , then $I_j \subseteq P$ for some j . It may be interesting to note that there is also the following counterpart where instead of an intersection of ideals contained in a prime ideal, we have an ideal contained in a union of prime ideals.

Proposition 1.2 (Prime Avoidance Lemma). *Let I, P_1, \dots, P_n be ideals in a ring A such that P_1, \dots, P_n are prime. If $I \subseteq \bigcup_{j=1}^n P_j$, then $I \subseteq P_j$ for some j .*

Proof. The case $n = 1$ is trivial. Suppose $n > 1$. If there exist $x_i \in I \setminus \bigcup_{j \neq i} P_j$ for $1 \leq i \leq n$, then we have a contradiction since $x_1 + x_2 x_3 \dots x_n \in I \setminus \bigcup_i P_i$. Thus $I \subseteq \bigcup_{j \neq i} P_j$, for some i . The case of $n = 1$ being trivial, the result now follows using induction on n . \square

Remark 1.3. An easy alteration of the above proof shows that Proposition 1.2 holds under the weaker hypothesis that I is a subset of A closed under addition and multiplication, and P_1, \dots, P_n are ideals of A such that at least $n - 2$ of them are prime. If A contains a field, then Proposition 1.2 can be proved, by elementary vector space arguments, without assuming any of the P_i 's to be prime.

The notion of congruence modulo an integer has a straightforward analogue for ideals. If A is a ring and I is an ideal of A , then for any $x, y \in A$ we say that $x \equiv y \pmod{I}$ if $x - y \in I$. More interestingly, Chinese Remainder Theorem for integers has the following analogue for ideals.

Proposition 1.4 (Chinese Remainder Theorem). *Let I_1, I_2, \dots, I_n be pairwise comaximal ideals in a ring A (i.e., $I_i + I_j = A$ for all $i \neq j$). Then:*

(i) $I_1 I_2 \dots I_n = I_1 \cap I_2 \cap \dots \cap I_n$.

(ii) *Given any $x_1, \dots, x_n \in A$, there exists $x \in A$ such that $x \equiv x_j \pmod{I_j}$ for $1 \leq j \leq n$.*

(iii) The map $x + I_1 I_2 \cdots I_n \mapsto (x + I_1, \dots, x + I_n)$ defines an isomorphism of $A/I_1 I_2 \cdots I_n$ onto the direct sum $A/I_1 \oplus A/I_2 \oplus \cdots \oplus A/I_n$.

Proof. (i) Clearly, $I_1 I_2 \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n$. To prove the other inclusion, we induct on n . The case of $n = 1$ is trivial. Next, if $n = 2$, then we can find $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. Now, $a \in I_1 \cap I_2$ implies that $a = aa_1 + aa_2$, and thus $a \in I_1 I_2$. Finally, if $n > 2$, then as in (i), let $J_1 = I_2 \cdots I_n$ and note that $I_1 + J_1 = A$. Hence by induction hypothesis and the case of two ideals, $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 \cap J_1 = I_1 J_1 = I_1 I_2 \cdots I_n$.

(ii) Given any $i \in \{1, \dots, n\}$, let $J_i = I_1 \cdots I_{i-1} I_{i+1} \cdots I_n$. Since $I_i + J_i = A$, we can find $a_{ij} \in J_i$ such that $a_{ij} \equiv 1 \pmod{I_i}$, for all $j \neq i$. Let $a_i = \prod_{j \neq i} a_{ij}$. Then $a_i \equiv 1 \pmod{I_i}$ and $a_i \in J_i$. Thus $I_i + J_i = A$. Now, $x = x_1 a_1 + \cdots + x_n a_n$ satisfies $x \equiv x_j \pmod{I_j}$ for $1 \leq j \leq n$.

(iii) The map $x + I_1 I_2 \cdots I_n \mapsto (x + I_1, \dots, x + I_n)$ is clearly well-defined and a homomorphism. By (i), it is surjective and by (ii), it is injective. \square

Of course, not every notion concerning rings is a straightforward analogue of an algebraic or arithmetic notion applicable to integers. There are some basic notions, such as those defined below, which would be quite redundant or useless in the realm of integers.

Let A be a ring. An element a of A is said to be a *zerodivisor* if there is $b \in A$ with $b \neq 0$ such that $ab = 0$. We will denote the set of all zerodivisors in A by $\mathcal{Z}(A)$. Note that $\mathcal{Z}(A) = \{a \in A : (0 : a) \neq 0\}$. An element of A which is not a zerodivisor is called a *nonzerodivisor* (sometimes abbreviated as *nzd*). Elements of $\sqrt{(0)}$, that is, those elements $a \in A$ for which $a^n = 0$ for some $n \in \mathbb{N}$, are said to be *nilpotent*. The set $\sqrt{(0)}$ of all nilpotent elements in a ring A is called the *nilradical* of A . If A is a nonzero ring, then clearly every nilpotent element of A is a zerodivisor, that is, $\sqrt{(0)} \subseteq \mathcal{Z}(A)$.

Interestingly, each of the above notions is neatly connected with prime ideals. To begin with, the set of all nonzerodivisors in a ring enjoys properties similar to complements of prime ideals. More precisely, it is a multiplicatively closed set in the following sense.

Definition 1.5. A subset S of a ring A is said to be *multiplicatively closed* if it satisfies the following: (i) $1 \in S$ and (ii) if $a \in S$ and $b \in S$, then $ab \in S$.

Examples 1.6. (i) If A is an integral domain, then $A^* = A \setminus \{0\}$ is multiplicatively closed. More generally, as remarked earlier, the set of all nonzerodivisors in any ring A is a multiplicatively closed subset of A .

(ii) If P is a prime ideal of a ring A , then $A \setminus P$ multiplicatively closed. More generally, if $\{P_\alpha : \alpha \in \Lambda\}$ is a family of prime ideals of a ring A , then $A \setminus \bigcup_{\alpha \in \Lambda} P_\alpha$ is a multiplicatively closed subset of A . Note that if I is any ideal in a ring A , then $A \setminus I$ is multiplicatively closed if and only if I is a prime ideal.

- (iii) Given any element a of a ring A , the set $S = \{a^n : n \in \mathbb{N}\}$ of powers of a is a multiplicatively closed subset of A . In particular, $\{1\}$ is multiplicatively closed and it is clearly the smallest among the multiplicatively closed subsets of A .
- (iv) If a ring A is a subring of a ring B and S is a multiplicatively closed subset of A , then S is a multiplicatively closed subset of B .

Lemma 1.7. *Let A be a ring. If I is an ideal and S is a multiplicatively closed subset of A such that $I \cap S = \emptyset$, then there exists a prime ideal P of A such that $I \subseteq P$ and $P \cap S = \emptyset$. Moreover P is maximal among the family of ideals J of A satisfying $I \subseteq J$ and $J \cap S = \emptyset$.*

Proof. Consider the family $\{J : J \text{ an ideal of } A \text{ with } I \subseteq J \text{ and } J \cap S = \emptyset\}$ and Zornify! \square

Corollary 1.8. *Let I be a nonunit ideal of a ring A . Then there is a maximal ideal \mathfrak{m} of A such that $I \subseteq \mathfrak{m}$. In particular, every nonzero ring has a maximal ideal and the spectrum of a nonzero ring is nonempty.*

Proof. The first assertion follows from Lemma 1.7 with $S = \{1\}$. To prove the second assertion, take $I = (0)$. \square

Corollary 1.9. *Let A be a ring and I be any ideal of A . Then*

$$\sqrt{I} = \bigcap_{\substack{P \in \text{Spec}(A) \\ I \subseteq P}} P. \quad \text{In particular,} \quad \sqrt{(0)} = \bigcap_{P \in \text{Spec}(A)} P.$$

Proof. Clearly $\sqrt{I} \subseteq P$ for every prime ideal P of A containing I . On the other hand, if $a \in P$ for every $P \in \text{Spec}(A)$ with $I \subseteq P$, but $a \notin \sqrt{I}$, then applying Lemma 1.7 to $S := \{a^n : n \in \mathbb{N}\}$, we arrive at a contradiction. \square

If a is a nilpotent element of a ring A then $a^n = 0$ for some $n \in \mathbb{N}$, and hence $(1 - a)(1 + a + a^2 + \cdots + a^{n-1}) = 1$. In other words, we have a valid geometric series expansion

$$\frac{1}{1 - a} = 1 + a + \cdots + a^{n-1},$$

which shows that $1 - a$ is a unit in A . In fact, a similar argument shows that if $a \in A$ is nilpotent, then $1 - ab$ is a unit in A for any $b \in A$. It follows that $\sqrt{(0)} \subseteq \{a \in A : 1 - ab \text{ is a unit for every } b \in A\}$. The set $\{a \in A : 1 - ab \text{ is a unit for every } b \in A\}$ will be denoted by $\mathcal{J}(A)$ and called the *Jacobson radical* of A . The following result shows that the Jacobson radical of A is an ideal of A and it is, in fact, the intersection of all the maximal ideals of A . It also gives an alternative proof of the fact that the nilradical is contained in the Jacobson radical.

Proposition 1.10. *Let A be a ring. Then*

$$\mathcal{J}(A) = \bigcap_{\mathfrak{m} \in \text{Max}(A)} \mathfrak{m}$$

Proof. Let $a \in \mathcal{J}(A)$. If $a \notin \mathfrak{m}$ for some $\mathfrak{m} \in \text{Max}(A)$, then $\mathfrak{m} + (a)$ is an ideal of A with $\mathfrak{m} \subset \mathfrak{m} + (a)$. Since \mathfrak{m} is maximal, we have $\mathfrak{m} + (a) = A$. Hence there is $m \in \mathfrak{m}$ and $b \in A$ such that $m + ab = 1$. Now \mathfrak{m} contains the unit $m = 1 - ab$, and this is a contradiction. On the other hand, if a is in \mathfrak{m} for every $\mathfrak{m} \in \text{Max}(A)$, then so is ab for every $b \in A$. Now if $1 - ab$ is not a unit in A for some $b \in A$, then by Corollary 1.8, there is $\mathfrak{m} \in \text{Max}(A)$ such that $1 - ab \in \mathfrak{m}$, but then $1 \in \mathfrak{m}$, which is a contradiction. \square

1.2 Polynomial rings and Localization of rings

Forming the residue class ring or the quotient ring is one of the three fundamental processes in Algebra for constructing new rings from a given ring. The other two processes are forming the polynomial ring in one or several variables with coefficients in the given ring and forming the localization of the given ring. We shall first review the former and then describe the latter.

Polynomial Ring: Let A be a ring and n be a nonnegative integer. We denote by $A[X_1, \dots, X_n]$ the ring of all polynomials in the variables X_1, \dots, X_n with coefficients in A . Elements of $A[X_1, \dots, X_n]$ look like

$$f = \sum a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}, \quad a_{i_1 \dots i_n} \in A,$$

where (i_1, \dots, i_n) vary over a finite subset of \mathbb{N}^n . A typical term (excluding the coefficient), viz., $X_1^{i_1} \dots X_n^{i_n}$, is called a *monomial*; its (usual) *degree* is $i_1 + \dots + i_n$. Such a monomial is said to be *squarefree* if $i_r \leq 1$ for $1 \leq r \leq n$. If $f \neq 0$, then the (total) *degree* of f is defined by $\deg f = \max\{i_1 + \dots + i_n : a_{i_1 \dots i_n} \neq 0\}$. Usual convention is that $\deg 0 = -\infty$. With this in view, for every $f, g \in A[X_1, \dots, X_n]$, we have $\deg(f + g) \leq \max\{\deg f, \deg g\}$ and in case A is a domain, then $\deg fg = \deg f + \deg g$. A *homogeneous polynomial* of degree d in $A[X_1, \dots, X_n]$ is simply a finite A -linear combination of monomials of degree d . The set of all homogeneous polynomials of degree d is denoted by $A[X_1, \dots, X_n]_d$. Note that any $f \in A[X_1, \dots, X_n]$ can be uniquely written as $f = f_0 + f_1 + \dots$, where $f_i \in A[X_1, \dots, X_n]_i$ and $f_i = 0$ for $i > \deg f$; we may call f_i 's to be the *homogeneous components* of f . If $f \neq 0$ and $d = \deg f$, then clearly $f_d \neq 0$ and $f = f_0 + f_1 + \dots + f_d$. An ideal I of $A[X_1, \dots, X_n]$ is said to be a *homogeneous ideal* (resp: *monomial ideal*) if it is generated by homogeneous polynomials (resp: monomials). Henceforth, when we use a notation such as $k[X_1, \dots, X_n]$, it will be tacitly assumed that k denotes a field and X_1, \dots, X_n are independent indeterminates over k (and, of course, $n \in \mathbb{N}$).

The process of localization described next generalizes the construction of the field of fractions of an integral domain, which in turn, is a generalization of the formal construction of rational numbers from integers.

Localization: Let A be a ring and S be a multiplicatively closed subset of A . Define a relation \sim on $A \times S$ as follows. Given any $(a, s), (b, t) \in A \times S$,

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

It is easy to see that \sim defines an equivalence relation on $A \times S$. Let us denote the equivalence class of $(a, s) \in A \times S$ by a/s (or by $\frac{a}{s}$), and let $S^{-1}A$ denote the set of equivalence classes of elements of $A \times S$. Define addition and multiplication on $S^{-1}A$ by

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{and} \quad \left(\frac{a}{s}\right) \left(\frac{b}{t}\right) = \frac{ab}{st} \quad \text{for any } (a, s), (b, t) \in A \times S.$$

It can be easily seen that these binary operations are well defined and that $S^{-1}A$ is a ring with respect to them. The ring $S^{-1}A$ is called the *ring of fractions* or the *localization* of A with respect to multiplicatively closed subset S . Passing to $S^{-1}A$ from A has the effect of making the elements of S units. In case $0 \in S$, we see that $S^{-1}A$ is the zero ring, and conversely, if $S^{-1}A$ is the zero ring, then $0 \in S$.

Examples 1.11. Let A be a ring.

- (i) If A is an integral domain and $S = A \setminus \{0\}$, then $S^{-1}A$ is nothing but the quotient field or the field of fractions of A . Note that in this case the equivalence relation \sim on $A \times S$ takes the simpler form: $(a, s) \sim (b, t) \iff (at - bs) = 0$. More generally, this is the case when all the elements of S are nonzerodivisors. In general, if S is the set of all nonzerodivisors in A , then $S^{-1}A$ is called the *total quotient ring* of A .
- (ii) Let $S = A \setminus \mathfrak{p}$, where \mathfrak{p} is a prime ideal of A . In this case $S^{-1}A$ is customarily denoted by $A_{\mathfrak{p}}$. The set $\mathfrak{p}A_{\mathfrak{p}} := \{a/s : a \in \mathfrak{p}, s \in S\}$ is an ideal of $A_{\mathfrak{p}}$ and an element of $A_{\mathfrak{p}}$ that is not in $\mathfrak{p}A_{\mathfrak{p}}$ is a unit in $A_{\mathfrak{p}}$. It follows that $\mathfrak{p}A_{\mathfrak{p}}$ is the only maximal ideal of the ring $A_{\mathfrak{p}}$. In other words $A_{\mathfrak{p}}$ is a local ring [A *local ring* is a ring with only one maximal ideal].

In general, we have the natural homomorphism

$$\phi : A \rightarrow S^{-1}A \quad \text{defined by} \quad \phi(a) := \frac{a}{1} \text{ for } a \in A.$$

The map ϕ is not injective, in general, and its kernel is given by

$$\ker \phi = \{a \in A : sa = 0 \text{ for some } s \in S\} = \bigcup_{s \in S} (0 : s).$$

In particular, ϕ is injective if S consists of nonzerodivisors; in this case A may be regarded as a subring of $S^{-1}A$. Given an ideal \mathfrak{a} of A , the ideal of $S^{-1}A$ generated by $\phi(\mathfrak{a})$ is called the *extension* of \mathfrak{a} , and is denoted by $\mathfrak{a}S^{-1}A$ or by $S^{-1}\mathfrak{a}$. For an ideal \mathfrak{b} of $S^{-1}A$, the inverse image $\phi^{-1}(\mathfrak{b})$ is an ideal of A and is called the *contraction* of \mathfrak{b} to A . By abuse of language, the contraction of \mathfrak{b} is sometimes denoted by $\mathfrak{b} \cap A$. Basic properties of extension and contraction are described in the following result.

Proposition 1.12. *Let A be a ring and S be a multiplicatively closed subset of A . Given any ideal \mathfrak{a} of A and an ideal \mathfrak{b} of $S^{-1}A$, we have the following:*

- (i) *If $\mathfrak{a} = \mathfrak{b} \cap A$, then $\mathfrak{b} = S^{-1}\mathfrak{a} = S^{-1}(\mathfrak{b} \cap A)$. In particular, \mathfrak{b} is the extension of some ideal of A .*
- (ii) $S^{-1}\mathfrak{a} \cap A = \bigcup_{s \in S} (\mathfrak{a} : s)$. *In particular, $S^{-1}\mathfrak{a} = S^{-1}A \Leftrightarrow \mathfrak{a} \cap S \neq \emptyset$.*
- (iii) \mathfrak{a} *is a contraction of an ideal of $S^{-1}A$ if and only if every element of S is a nonzerodivisor in A/\mathfrak{a} ; in this case $\mathfrak{a} = S^{-1}\mathfrak{a} \cap A$.*
- (iv) *The prime ideals of $S^{-1}A$ are in one-to-one correspondence with the prime ideals of A which do not meet S .*

Proof. (i) Since $\mathfrak{a} = \mathfrak{b} \cap A = \phi^{-1}(\mathfrak{b})$, we have $\phi(\mathfrak{a}) \subseteq \mathfrak{b}$ and hence $S^{-1}\mathfrak{a} \subseteq \mathfrak{b}$. On the other hand, if $a \in A$ and $s \in S$ are such that $a/s \in \mathfrak{b}$, then $a/1 = (s/1)(a/s) \in \mathfrak{b}$, and hence $a \in \mathfrak{b} \cap A = \mathfrak{a}$, and this shows that $a/s \in S^{-1}\mathfrak{a}$. Thus, $\mathfrak{b} = S^{-1}\mathfrak{a}$.

(ii) Given any $x \in A \cap S^{-1}\mathfrak{a}$, we have $x/1 = a/t$ for some $a \in \mathfrak{a}$ and $t \in S$, and so $u(tx - a) = 0$ for some $u \in S$. Now $s = ut \in S$ and $sx \in \mathfrak{a}$, that is, $x \in (\mathfrak{a} : s)$. On the other hand, if $x \in (\mathfrak{a} : s)$ for some $s \in S$, then $sx \in \mathfrak{a}$, and so $x/1 = (1/s)(sx/1) \in S^{-1}\mathfrak{a}$, that is, $x \in A \cap S^{-1}\mathfrak{a}$. This shows that $S^{-1}\mathfrak{a} \cap A$ is the union of $(\mathfrak{a} : s)$ as s varies over S . In particular, $S^{-1}\mathfrak{a} = S^{-1}A$ if and only if $1 \in (\mathfrak{a} : s)$ for some $s \in S$, that is, $\mathfrak{a} \cap S \neq \emptyset$.

(iii) Observe that $s \in S$ is a nonzerodivisor in A/\mathfrak{a} if and only if $(\mathfrak{a} : s) = \mathfrak{a}$. With this in view, (iii) is an immediate consequence of (ii).

(iv) If \mathfrak{q} is a prime ideal of $S^{-1}A$, then $\mathfrak{q} \cap A = \phi^{-1}(\mathfrak{q})$ is a prime ideal of A , being the inverse image of a prime ideal under a ring homomorphism. Moreover, since $\mathfrak{q} \neq S^{-1}A$, we see from (i) above that $\mathfrak{q} \cap A$ is disjoint from S . On the other hand, suppose \mathfrak{p} is a prime ideal of A such that $\mathfrak{p} \cap S = \emptyset$. Then by (ii) above, $S^{-1}\mathfrak{p} \neq S^{-1}A$. Further, if $x, y \in \mathfrak{p}$ and $s, t \in S$ are such that $(x/s)(y/t) \in S^{-1}\mathfrak{p}$, then $uxy \in \mathfrak{p}$ for some $u \in S$. Since \mathfrak{p} is prime and $\mathfrak{p} \cap S = \emptyset$, it follows that $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, which implies that $x/s \in S^{-1}\mathfrak{p}$ or $y/t \in S^{-1}\mathfrak{p}$. Thus $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$. So, in view of (i) and (iii) above, it follows that the processes of contraction and extension set up the desired one-to-one correspondence. \square

1.3 Modules

Let A be a ring. An A -module is simply a vector space except that the scalars come from the ring A instead of a field. Apart from vector spaces over a field, basic examples of A -modules are: ideals I of A , residue class rings A/I , polynomial rings $A[X_1, \dots, X_n]$ and localizations $S^{-1}A$. The notions of submodules, quotient modules, direct sums of modules and isomorphism of modules are defined in an obvious fashion. The concept of localization (w.r.t. multiplicatively closed subsets of A) also carries over to A -modules. A direct sum of (isomorphic) copies of A is called a *free A -module*. The finite direct sum

$$A^n := \underbrace{A \oplus \cdots \oplus A}_{n \text{ times}}$$

is referred to as the free A -module of rank n .

Let M be an A -module. Given submodules $\{M_i\}$ of M , their sum

$$\sum M_i := \left\{ \sum x_i : x_i \in M_i \text{ and all except finitely many } x_i\text{'s are } 0 \right\}$$

is a submodule of M . Products of submodules do not make sense but of course, intersections of submodules of M does. Further, the colon operation has an interesting and important counterpart. If M_1 and M_2 are submodules of M , we define

$$(M_1 : M_2) := \{a \in A : aM_2 \subseteq M_1\}.$$

Note that $(M_1 : M_2)$ is an ideal of A . The ideal $(0 : M)$ is called the *annihilator* of M and is denoted by $\text{Ann}(M)$; for $x \in M$, we may write $\text{Ann}(x)$ for the ideal $(0 : x)$, i.e., for $\text{Ann}(Ax)$. Note that if I is an ideal of A , then $\text{Ann}(A/I) = I$ and if $\text{Ann}(M) \supseteq I$, then M may be regarded as an A/I -module. Let us also note that for any submodules M_1, M_2 of M , we always have the isomorphisms $(M_1 + M_2)/M_2 \simeq M_1/(M_1 \cap M_2)$, and, if $M_2 \subseteq M_1$ and N is a submodule of M_2 , then $(M_1/N)/(M_2/N) \simeq M_1/M_2$.

We say that M is *finitely generated* (f. g.) or that M is a *finite A -module* if there exist $x_1, \dots, x_n \in M$ such that $M = Ax_1 + \cdots + Ax_n$; in this case $\{x_1, \dots, x_n\}$ is referred to as a *set of generators* of M . Note that an A -module M is finitely generated if and only if M is isomorphic to A^n/K for some $n \in \mathbb{N}$ and a submodule K of the free A -module A^n .

In general, and unlike in the case of vector spaces, if an A -module M is finitely generated, then a submodule of M need not be finitely generated. For example, if $A = \mathbb{C}[X_1, X_2, \dots]$ is the polynomial ring in infinitely many variables and $I = (X_1, X_2, \dots)$ is the ideal of A generated by all the variables, then A is finitely generated as an A -module, but the A -submodule I of A is not finitely generated. We shall see in Chapter 2 that if every ideal

of A is finitely generated, then every submodule of a finitely generated A -module is finitely generated. Meanwhile let us note here a very useful property of finitely generated A -modules.

Lemma 1.13 (Nakayama's Lemma). *Let M be a finitely generated A -module and I be an ideal of A such that $IM = M$. Then $(1 - a)M = 0$ for some $a \in I$. In particular, if $I \neq A$ and if A is a domain or a local ring, then $M = 0$.*

Proof. Write $M = Ax_1 + \cdots + Ax_n$. Then $x_i = \sum_{j=1}^n a_{ij}x_j$, for some $a_{ij} \in I$. Let $d = \det(\delta_{ij} - a_{ij})$. Then $d = 1 - a$, for some $a \in I$, and, by Cramer's rule, $dx_j = 0$ for all j . \square

Remark 1.14. The 'determinant trick' in the above proof shows more generally that if M and I are as in Lemma 1.13 and $\phi : M \rightarrow M$ is an A -linear map such that $\phi(M) \subseteq IM$, then $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$ for some $a_1, \dots, a_n \in I$. Thus, Nakayama's Lemma may be considered as an analogue of the Cayley-Hamilton Theorem of Linear Algebra.

1.4 Zariski Topology

Let A be a ring. Given any subset E of A , we define,

$$V(E) := \{\mathfrak{p} \in \text{Spec}(A) : E \subseteq \mathfrak{p}\}.$$

In case $E = \{f\}$ for some $f \in A$, then $V(E)$ may be denoted simply by $V(f)$. Note that if I is the ideal of A generated by E , then $V(E) = V(I) = V(\sqrt{I})$. In particular,

$$\{V(E) : E \subseteq A\} = \{V(I) : I \text{ an ideal of } A\} = \{V(J) : J \text{ a radical ideal of } A\}.$$

The following facts follow directly from definition.

1. $V(0) = \text{Spec}(A)$ and $V(1) = \emptyset$.
2. $\bigcap_{\alpha \in \Lambda} V(E_\alpha) = V\left(\bigcup_{\alpha \in \Lambda} E_\alpha\right)$, for any family $\{E_\alpha : \alpha \in \Lambda\}$ of subsets of A .
3. $\bigcup_{i=1}^m V(E_i) = V\left(\bigcap_{i=1}^m E_i\right)$, for any $m \in \mathbb{N}$ and subsets E_1, \dots, E_m of A .

Thus the family $\{V(E) : E \subseteq A\}$ satisfies all the axioms of closed sets for a topology on $\text{Spec}(A)$. The resulting topology on $\text{Spec}(A)$ is called the *Zariski topology*. For example, if $A = \mathbb{C}[X]$, then using the Fundamental Theorem of Algebra we see that $\text{Spec}(\mathbb{C}[X]) = \{(X - \alpha) : \alpha \in \mathbb{C}\} \cup \{(0)\}$; thus $\text{Spec}(A)$ can be identified with the Riemann sphere $\widehat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ (or the projective line $\mathbb{P}_{\mathbb{C}}^1$). The Zariski topology on $\text{Spec}(\mathbb{C}[X])$ coincides

with the cofinite topology¹ on $\widehat{\mathbb{C}}$. Reverting to the general case, for any $V \subseteq \text{Spec}(A)$, we define

$$I(V) := \{f \in A : f \in P \text{ for all } P \in V\} = \bigcap_{P \in V} P.$$

Clearly, $I(V)$ is an ideal of A (in fact, a radical ideal); it is called the *vanishing ideal* of V . For example, if $A = \mathbb{C}[X]$ and \mathfrak{a} is a nonzero ideal of A , then $\mathfrak{a} = (h(X))$ for some nonzero polynomial $h(X) \in \mathbb{C}[X]$. Further, if $\alpha_1, \dots, \alpha_m$ are the distinct roots of $h(X)$ in \mathbb{C} , then $V = V(\mathfrak{a}) = \{\alpha_1, \dots, \alpha_m\}$ and $I(V) = \{f \in \mathbb{C}[X] : f(\alpha_i) = 0 \text{ for } i = 1, \dots, m\}$ is the ideal of polynomials which vanish at the roots of $h(X)$.

The following result may be viewed as a version of Hilbert's Nullstellensatz (see Corollary 3.19 in Chapter 3). However, here the proof is trivial.

We shall use here the following notation and terminology.

Proposition 1.15. *Let A be a ring.*

- (i) *If \mathfrak{a} is a nonunit ideal of A , then $V(\mathfrak{a})$ is nonempty.*
- (ii) *If \mathfrak{a} is an ideal of A and $V = V(\mathfrak{a})$ then $I(V) = \sqrt{\mathfrak{a}}$.*

Proof. Corollary 1.8 implies (i) and Corollary 1.9 implies (ii). □

The Zariski topology has a number of interesting properties. To begin with, let us note that the *principal open sets*

$$D_f := \text{Spec}(A) \setminus V(f) = \{\mathfrak{p} \in \text{Spec}(A) : f \notin \mathfrak{p}\}, \quad \text{where } f \in A,$$

form a base for the the Zariski topology on $\text{Spec}(A)$. The Zariski topology is almost never Hausdorff (or T_2). In fact, as part (ii) of the proposition below shows, a singleton set can be dense. On the other hand, part (iv) of the same proposition shows that $\text{Spec}(A)$ with the Zariski topology is a T_0 topological space.

Proposition 1.16. *Let A be a ring and $\mathfrak{p}, \mathfrak{q} \in \text{Spec}(A)$. We have the following:*

- (i) $\mathfrak{p} \in \text{Max}(A) \iff \{\mathfrak{p}\}$ is closed subset of $\text{Spec}(A)$.
- (ii) $\overline{\{\mathfrak{p}\}} := \text{closure of } \{\mathfrak{p}\} = V(\mathfrak{p})$. Consequently, $\mathfrak{q} \in \overline{\{\mathfrak{p}\}} \iff \mathfrak{p} \subseteq \mathfrak{q}$. In particular, if A is an integral domain, then $\overline{\{(0)\}} = \text{Spec}(A)$.
- (iii) If $\mathfrak{p} \neq \mathfrak{q}$, then there exists a neighbourhood of \mathfrak{p} which does not intersect \mathfrak{q} or a neighbourhood of \mathfrak{q} which does not intersect \mathfrak{p} .

¹The cofinite topology on any set X is defined as follows. A subset U of X is open if and only if $U = X$ or $U = X \setminus F$ where F is a finite subset of X .

Proof. (i) If $\mathfrak{p} \in \text{Max } A$, then $\{\mathfrak{p}\} = V(\mathfrak{p})$, and hence $\{\mathfrak{p}\}$ is closed. Conversely, if $\mathfrak{p} \in \text{Spec}(A)$ is such that $\{\mathfrak{p}\}$ is a closed, then $\{\mathfrak{p}\} = V(\mathfrak{a})$ for some ideal \mathfrak{a} of A . Clearly, $\mathfrak{a} \neq A$ and so by Corollary 1.8, there is $\mathfrak{m} \in \text{Max}(A)$ such that $\mathfrak{a} \subseteq \mathfrak{m}$. Hence $\mathfrak{m} \in V(\mathfrak{a}) = \{\mathfrak{p}\}$ and so $\mathfrak{p} = \mathfrak{m}$ is maximal.

(ii) If V is a closed subset of $\text{Spec}(A)$ containing \mathfrak{p} , then $V = V(\mathfrak{a})$ for some ideal \mathfrak{a} of A . Consequently $\mathfrak{a} \subseteq \mathfrak{p}$, and hence $V(\mathfrak{p}) \subseteq V(\mathfrak{a})$. It follows that $V(\mathfrak{p})$ is the smallest closed set containing $\{\mathfrak{p}\}$, and thus $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$. In case A is a domain, (0) is a prime ideal and we have $V(\{(0)\}) = \text{Spec}(A)$, that is, $\overline{\{(0)\}} = \text{Spec}(A)$.

(iii) If $\mathfrak{p} \neq \mathfrak{q}$, then $\mathfrak{p} \not\subseteq \mathfrak{q}$ or $\mathfrak{q} \not\subseteq \mathfrak{p}$. Suppose $\mathfrak{p} \not\subseteq \mathfrak{q}$. Then there is $f \in \mathfrak{p} \setminus \mathfrak{q}$; now D_f is an open set that contains \mathfrak{q} but does not contain \mathfrak{p} . \square

Recall that a topological space X is *quasi-compact* if every open cover of X has a finite subcover; X is *compact* if it is quasi-compact and Hausdorff.

Proposition 1.17. *Spec(A) is quasi-compact in the Zariski topology.*

Proof. Given an open cover of $\text{Spec}(A)$, we can refine it to an open cover of $\text{Spec}(A)$ consisting of principal open sets. This implies that $\text{Spec}(A)$ is the union of D_f where f vary over a subset Λ of A . Consequently, the intersection of $V(f)$ as f varies over Λ is empty, and so $V(\mathfrak{a}) = \emptyset$, where \mathfrak{a} is the ideal of A generated by Λ . By part (ii) of Proposition 1.15, we see that $\mathfrak{a} = A$, and hence there are $f_1, \dots, f_m \in \Lambda$ and $g_1, \dots, g_m \in A$ such that $f_1g_1 + \dots + f_mg_m = 1$. This implies that $\{D_{f_i} : i = 1, \dots, m\}$ cover $\text{Spec}(A)$, and hence the given open cover of $\text{Spec}(A)$ has a finite subcover. \square

Exercises

Throughout the following exercises A denotes a ring.

1. Let $\phi : A \rightarrow B$ be a homomorphism of rings. If J is an ideal of B , then show that $\phi^{-1}(J)$ is an ideal of A . Further, show that $J \in \text{Spec}(B)$ implies $\phi^{-1}(J) \in \text{Spec}(A)$. Is it true that $J \in \text{Max}(B)$ implies $\phi^{-1}(J) \in \text{Max}(A)$? Also, is it true that if I is an ideal of A , then $\phi(I)$ is an ideal of B ? What if ϕ is surjective? Further, if ϕ is surjective, then is it true that $I \in \text{Spec}(A)$ implies $\phi(I) \in \text{Spec}(B)$, and that $I \in \text{Max}(A)$ implies $\phi(I) \in \text{Max}(B)$? Justify your answers.
2. Let I be an ideal of A and $q : A \rightarrow A/I$ be the natural homomorphism given by $x \mapsto x + I$. Show that $J \mapsto q(J)$ defines a bijective map from the ideals of A containing I and the ideals of A/I . Further, show that this bijection preserves inclusions, primality and maximality.
3. Assume that A is a PID. Given any $a, b \in A$, let $d = \text{GCD}(a, b)$ and $\ell = \text{LCM}(a, b)$. If $I = (a)$ and $J = (b)$, then show that

$$IJ = (ab), \quad I \cap J = (\ell), \quad I + J = (d), \quad \text{and} \quad (I : J) = (a/d).$$

Are these results valid if A is an arbitrary ring. What if A is a UFD? Justify your answer.

4. Consider ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ of A and the following three equalities.

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}, \quad (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}\mathfrak{b}, \quad \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}).$$

In each case, determine if the equality is valid for arbitrary $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$. If yes, then give a proof; otherwise give a counterexample. Also, if the answer is no, then determine if either of the inclusions \subseteq and \supseteq is valid, in general.

5. If I is an ideal of A , then show that \sqrt{I} is an ideal of A .
6. Show that colons commute with intersections, whereas radicals commute with finite intersections. More precisely, if $\{I_\alpha : \alpha \in \Lambda\}$ is a family of ideals of a ring A and J is any ideal of A , then show that

$$\bigcap_{i \in \Lambda} (I_i : J) = \left(\bigcap_{i \in \Lambda} I_i : J \right) \quad \text{and if } \Lambda \text{ is finite, then } \sqrt{\bigcap_{i \in \Lambda} I_i} = \bigcap_{i \in \Lambda} \sqrt{I_i}.$$

Give examples to show that these results do not hold (for finite families) if intersections are replaced by products.

7. Suppose A is not the zero ring and let \mathfrak{N} be the nilradical of A . Show that the following are equivalent.
- (i) A has exactly one prime ideal.
 - (ii) Every element of A is either a unit or a nilpotent.
 - (iii) A/\mathfrak{N} is a field.

8. Let k be a field. Show that $\dim_k k[X_1, \dots, X_n]_d = \binom{n+d-1}{d}$.

9. Let $f(X) = a_0 + a_1X + \dots + a_nX^n \in A[X]$. Prove the following:

- (i) f is a unit in $A[X]$ if and only if a_0 is unit in A and a_1, a_2, \dots, a_n are nilpotent in A .
- (ii) f is a nilpotent in $A[X]$ if and only if a_0, a_1, \dots, a_n are nilpotent in A .
- (iii) f is a zero divisor in $A[X]$ if and only if there exists $a \in A$ with $a \neq 0$ such that $af = 0$.

10. Let S be any multiplicatively closed subset of A . Consider the relation on $A \times S$ defined by $(a, s) \sim (b, t) \iff (at - bs) = 0$. Determine if \sim is an equivalence relation.

11. Given any $f \in A$, let $S = \{f^n : n \in \mathbb{N}\}$ and $A_f = S^{-1}A$. Show that A_f is isomorphic to $A[X]/(Xf - 1)$.
12. Let S and T be multiplicatively closed subsets of A with $S \subseteq T$ and let U denote the image of T under the natural map $\phi : A \rightarrow S^{-1}A$. Show that $T^{-1}A$ is isomorphic to $U^{-1}(S^{-1}A)$.
13. Show that localization commutes with taking homomorphic images. More precisely, if I is an ideal of a ring A and S is a multiplicatively closed subset of A , then show that $S^{-1}A/S^{-1}I$ is isomorphic to $\overline{S}^{-1}(A/I)$, where \overline{S} denotes the image of S in A/I .
14. Let A be an integral domain. Fix a quotient field K of A and consider the localization $A_{\mathfrak{p}}$, where $\mathfrak{p} \in \text{Spec}(A)$, as subrings of K . Show that

$$A = \bigcap_{\mathfrak{p} \in \text{Spec}(A)} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \in \text{Max}(A)} A_{\mathfrak{m}}.$$

15. Consider the following ring-theoretic properties that A can have: (i) integral domain, (ii) field, (iii) PIR, (iv) PID, and (v) UFD. For each of these, determine if the property is preserved under the passage from A to a (i) residue class ring, (ii) polynomial ring, or (iii) localization.
16. Let M be an A -module and S be a multiplicatively closed subset of A . Define carefully the localization $S^{-1}M$ of M at S . With ideals replaced by A -submodules, determine which of the notions and results in Section 1.2 has an analogue in the setting of modules.
17. Let (A, \mathfrak{m}) be a local ring [which means that A is a local ring and \mathfrak{m} is its unique maximal ideal] and M be a finitely generated A -module. For $x \in M$, let \overline{x} denotes the image of x in the A/\mathfrak{m} -module $M/\mathfrak{m}M$. Given any $x_1, \dots, x_r \in M$, show that $\{x_1, \dots, x_r\}$ is a minimal set of generators of M if and only if $\{\overline{x}_1, \dots, \overline{x}_r\}$ is a basis for the A/\mathfrak{m} -vector space $M/\mathfrak{m}M$. Deduce that any two minimal set of generators of M have the same cardinality, namely, $\dim_{A/\mathfrak{m}} M/\mathfrak{m}M$.
18. Assume that A is not the zero ring and let $m, n \in \mathbb{N}$. Use Exercise 17 to show that A^m and A^n are isomorphic as A -modules iff $m = n$.
19. Given any $f, g \in A$, show that the principal open sets D_f and D_g of $\text{Spec } A$ satisfy the following.
 - (i) $D_f = \emptyset \iff f$ is nilpotent,
 - (ii) $D_f = \text{Spec}(A) \iff f$ is a unit,
 - (iii) $D_f \cap D_g = D_{fg}$, and
 - (iv) $D_f = D_g \iff \sqrt{(f)} = \sqrt{(g)}$.
20. Given any $f \in A$, show that the principal open set D_f is quasi-compact. Further show that an open subset of $\text{Spec}(A)$ is quasi-compact if and only if it is a finite union of principal open sets.

Chapter 2

Noetherian Rings

In this chapter we shall study a class of rings and modules named after E. Noether (1921), who first realized their importance. Basic results proved in this chapter include the Basis Theorem that goes back to the work of Hilbert (1890) on $\mathbb{C}[X_1, \dots, X_n]$ and the Primary Decomposition Theorem for ideals that goes back to the work of Lasker (1905) also on $\mathbb{C}[X_1, \dots, X_n]$.

2.1 Noetherian Rings and Modules

Proposition 2.1. *Let A be a ring. The following conditions are equivalent.*

- (i) (Finite Generation Condition) *Every ideal of A is finitely generated.*
- (ii) (Ascending Chain Condition or the a.c.c.) *If I_1, I_2, \dots are ideals of A with $I_1 \subseteq I_2 \subseteq \dots$, then there exists $m \geq 1$ such that $I_n = I_m$ for $n \geq m$.*
- (iii) (Maximality Condition) *Every nonempty set of ideals of A has a maximal element.*

Proof. (i) \Rightarrow (ii): Given a chain $I_1 \subseteq I_2 \subseteq \dots$ of ideals of A , the union $I = \cup_{n \geq 1} I_n$ is an ideal of A . Thus by (i), there are $a_1, \dots, a_r \in I$ such that $I = (a_1, \dots, a_r)$. Now, if $m \in \mathbb{N}$ is such that $a_i \in I_m$ for $i = 1, \dots, r$, then we clearly have $I_n = I_m$ for $n \geq m$.

(ii) \Rightarrow (iii): Let \mathcal{F} be a nonempty set of ideals of A that does not have a maximal element. Since \mathcal{F} is nonempty, there is some $I_1 \in \mathcal{F}$. Moreover, I_1 is not a maximal element, and so there is $I_2 \in \mathcal{F}$ such that $I_1 \subset I_2$. Further, I_2 is not a maximal element, and so there is $I_3 \in \mathcal{F}$ such that $I_2 \subset I_3$. Continuing in this way, we obtain a strictly ascending chain $I_1 \subset I_2 \subset \dots$ of ideals in \mathcal{F} . This contradicts (ii).

(iii) \Rightarrow (i): Let I be an ideal of A and consider the set \mathcal{F} of ideals J of A such that $J \subseteq I$ and J is finitely generated. By (iii), \mathcal{F} has a maximal element, say \mathfrak{a} . If there is some $x \in I \setminus \mathfrak{a}$, then $\mathfrak{a} + Ax \in \mathcal{F}$, which contradicts the maximality of \mathfrak{a} . Thus $I = \mathfrak{a} \in \mathcal{F}$, and hence I is finitely generated. \square

A ring which satisfies either (and hence all) of the three equivalent conditions in Proposition 2.1 is said to be *noetherian*. The class of noetherian rings has a remarkable property that it is closed w.r.t. each of the three fundamental processes mentioned in Section 1.2. Indeed, if A is a noetherian ring, then it is trivial to check that A/I is noetherian for every ideal I of A and also that $S^{-1}A$ is noetherian, for every multiplicatively closed subset S of A . Moreover, the following basic result implies, using induction, that if A is noetherian, then $A[X_1, \dots, X_n]$ is noetherian.

Proposition 2.2 (Hilbert Basis Theorem). *If A is noetherian, then so is $A[X]$.*

Proof. Let I be any ideal of $A[X]$. For $0 \neq f \in I$, let $\text{LC}(f)$ denote the leading coefficient of f , and let $J := \{0\} \cup \{\text{LC}(f) : f \in I, f \neq 0\}$. Then J is an ideal of A , and so we can find $f_1, \dots, f_r \in I \setminus \{0\}$ such that $J = (\text{LC}(f_1), \dots, \text{LC}(f_r))$. Let $d = \max\{\deg f_i : 1 \leq i \leq r\}$. For $0 \leq i < d$, let $J_i = \{0\} \cup \{\text{LC}(f) : f \in I, \deg f = i\}$; then J_i is an ideal of A , and so we can find $f_{i1}, \dots, f_{ir_i} \in I \setminus \{0\}$ such that $J_i = (\text{LC}(f_{i1}), \dots, \text{LC}(f_{ir_i}))$. Let I' be the ideal of $A[X]$ generated by $\{f_1, \dots, f_r\} \cup \{f_{ij} : 0 \leq i < d, 1 \leq j \leq r_i\}$. Clearly, $I' \subseteq I$ and for any $0 \neq f \in I$, we easily see that there is $f' \in I'$ such that $\deg(f - f') < \deg f$. Thus an inductive argument yields $I = I'$. \square

A field as well as a PID (e.g., \mathbb{Z} , the ring of integers) is clearly noetherian. Starting from these and using iterations of the three fundamental processes, we obtain an abundant supply of noetherian rings. Especially important among these are finitely generated algebras over a field or, more generally, over a noetherian ring. Let us recall the relevant definitions.

Definition 2.3. Let B be a ring and let A be a subring of B . Given any $b_1, \dots, b_n \in B$, we denote by $A[b_1, \dots, b_n]$ the smallest subring of B containing A and the elements b_1, \dots, b_n . This subring consists of all polynomial expressions $f(b_1, \dots, b_n)$ as f varies over $A[X_1, \dots, X_n]$. We say that B is a *finitely generated (f.g.) A -algebra* or an *A -algebra of finite type* if there exist $b_1, \dots, b_n \in B$ such that $B = A[b_1, \dots, b_n]$. Finitely generated k -algebras, where k is a field, are sometimes called *affine rings*.

Note that a ring B is a f.g. A -algebra if and only if $B \simeq A[X_1, \dots, X_n]/I$ for some $n \in \mathbb{N}$ and some ideal I of $A[X_1, \dots, X_n]$. Hence it follows from the Hilbert basis theorem that finitely generated algebras over noetherian rings are noetherian. In particular, every affine ring is noetherian.

Now let us turn to modules. In the remainder of this section, we fix a ring A and consider A -modules. By submodules of a given A -module, we always mean A -submodules.

To begin with, let us note that we have the following straightforward analogue of Proposition 2.1.

Proposition 2.4. *Let M be an A -module. The following conditions are equivalent.*

- (i) **(Finite Generation Condition)** Every submodule of M is finitely generated.
- (ii) **(a.c.c.)** If N_1, N_2, \dots are submodules of M with $N_1 \subseteq N_2 \subseteq \dots$, then there exists $m \geq 1$ such that $N_n = N_m$ for $n \geq m$.
- (iii) **(Maximality Condition)** Every nonempty set of submodules of M has a maximal element.

Proof. The proof of Proposition 2.1 carries over verbatim with ideals replaced by A -submodules. \square

We define a module to be *noetherian* if it satisfies any (and hence all) of the equivalent conditions in Proposition 2.4. Notice that if A is any ring, then A is noetherian as an A -module if and only if A is a noetherian ring. Thus, the terminology for modules is consistent with that for rings.

Proposition 2.5. *Let M be an A -module and N be a submodule of M . Then*

$$M \text{ is noetherian} \iff \text{both } N \text{ and } M/N \text{ are noetherian.}$$

Proof. The a.c.c. on M clearly implies the a.c.c. on N . Moreover, an ascending chain of A -submodules of M/N gives rise to an ascending chain of A -submodules of M . Thus, if M is noetherian, then so is N and M/N . Conversely, if both N and M/N are noetherian, then for any ascending chain $M_0 \subseteq M_1 \subseteq \dots$ of A -submodules of M , we can find $p, q \in \mathbb{N}$ such that $M_i \cap N = M_p \cap N$ for $i \geq p$ and $(M_i + N)/N \simeq (M_q + N)/N$ for $i \geq q$. If $m = \max\{p, q\}$, then for any $i \geq m$, we have $M_m \subseteq M_i$. Further, if $x \in M_i$, then $x = y + n$ for some $y \in M_m$ and $n \in N$; now $n \in M_i \cap N = M_m \cap N$, and hence $x \in M_m$. Thus $M_i = M_m$ for $i \geq m$. So M is noetherian. \square

Corollary 2.6. *If M_1, \dots, M_n are noetherian A -modules, then so is $\bigoplus_{i=1}^n M_i$. In particular, if A is a noetherian ring, then A^n is a noetherian A -module.*

Proof. Given any $n \geq 1$, let $M = \bigoplus_{i=1}^n M_i$ and $N = \bigoplus_{i=1}^{n-1} M_i$. Observe that $M_n \simeq M/N$ and use Proposition 2.5 together with induction on n . \square

Proposition 2.7. *If A is noetherian and M is a finitely generated A -module, then M is noetherian.*

Proof. Since M is finitely generated, $M \simeq A^n/N$ for some $n \in \mathbb{N}$ and a submodule N of A^n . Now apply Corollary 2.6 and Proposition 2.5. \square

2.2 Primary Decomposition of Ideals

Ideals in noetherian rings admit a decomposition which is somewhat similar, though much cruder, to the decomposition of positive integers into prime-powers.

Definition 2.8. An ideal \mathfrak{q} in a ring A is said to be *primary* if $\mathfrak{q} \neq A$ and for any $a, b \in A$,

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

If \mathfrak{q} is a primary ideal, then its radical $\sqrt{\mathfrak{q}}$ is readily seen to be a prime ideal; if $\mathfrak{p} = \sqrt{\mathfrak{q}}$, then we say that \mathfrak{q} is \mathfrak{p} -primary or that \mathfrak{q} is a primary ideal belonging to \mathfrak{p} or that \mathfrak{q} is primary to \mathfrak{p} .

Remark 2.9. If \mathfrak{q} is an ideal such that $\sqrt{\mathfrak{q}}$ is prime, then \mathfrak{q} needn't be primary; in fact, even a power of a prime ideal can fail to be primary. [Example: \mathfrak{p}^2 , where \mathfrak{p} is the image in $k[X, Y, Z]/(XY - Z^2)$ of (X, Z) .] However, if $\sqrt{\mathfrak{q}}$ is a maximal ideal \mathfrak{m} , then \mathfrak{q} is easily seen to be \mathfrak{m} -primary. [Indeed, if $ab \in \mathfrak{q}$ and $a \notin \mathfrak{m} = \sqrt{\mathfrak{q}}$, then $\sqrt{\mathfrak{q} + Aa} \subseteq \mathfrak{m} + Aa = A$, and so $1 \in \mathfrak{q} + Aa$, which implies $b \in \mathfrak{q}$.] On the other hand, if \mathfrak{q} is \mathfrak{p} -primary, then \mathfrak{q} needn't be a power of \mathfrak{p} , even when \mathfrak{p} is maximal. [Example: $\mathfrak{q} = (X^2, Y)$ in $k[X, Y]$.] It may be noted, however, that if A is a noetherian ring and \mathfrak{q} is a \mathfrak{p} -primary ideal of A , then \mathfrak{q} does contain some power of \mathfrak{p} .

Proposition 2.10 (Primary Decomposition Theorem for ideals). *Let A be a noetherian ring and I be any ideal of A with $I \neq A$. Then we have the following.*

- (i) *There exist primary ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_h$ in A such that $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h$.*
- (ii) *In (i) above, $\mathfrak{q}_1, \dots, \mathfrak{q}_h$ can be chosen such that $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ for $1 \leq i \leq h$, and $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are distinct, where $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.*
- (iii) *If $\mathfrak{q}_i, \mathfrak{p}_i$ are as in (ii) above, then $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are unique; in fact, $\{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}$ is precisely the set of prime ideals among the ideals $(I : x)$ where x varies over elements of A . Moreover, if \mathfrak{p}_i is minimal among $\mathfrak{p}_1, \dots, \mathfrak{p}_h$, i.e. $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for $j \neq i$, then the corresponding primary ideal \mathfrak{q}_i is also unique.*

Proof: Classical proof of (i) is in two steps. First, one considers *irreducible ideals*, viz., nonunit ideals that are not finite intersections of strictly larger ideals. The maximality condition readily implies that every ideal of A is a finite intersection of irreducible ideals. Next, if I is irreducible and $ab \in I$ are such that $b \notin I$ and no power of a is in I , then we consider the chain $(I : a) \subseteq (I : a^2) \subseteq \dots$. By a.c.c., $(I : a^n) = (I : a^{n+1})$ for some n , and now it is easy to verify that $I = (I + Aa^n) \cap (I + Ab)$, which is a contradiction. Thus I is primary and (i) is proved. Proving (ii) is easy since if $\mathfrak{p}_i = \mathfrak{p}_j$, then $\mathfrak{q}_i \cap \mathfrak{q}_j$ is primary and it can replace both \mathfrak{q}_i and \mathfrak{q}_j in the decomposition. To prove (iii), let $i \in \{1, \dots, h\}$. Find $c_i \in (\bigcap_{j \neq i} \mathfrak{q}_j) \setminus \mathfrak{q}_i$. Then $\mathfrak{q}_i \subseteq (I : c_i) \subseteq \mathfrak{p}_i$, and so there is $k \geq 1$ such that $\mathfrak{p}_i^k \subseteq (I : c_i)$ and $\mathfrak{p}_i^{k-1} \not\subseteq (I : c_i)$. Choose $y \in \mathfrak{p}_i^{k-1} \setminus (I : c_i)$, and let $x_i = yc_i$. We claim that $\mathfrak{p}_i = (I : x_i)$. Clearly, $\mathfrak{p}_i \subseteq (I : x_i)$. Further, if there is $x \in (I : x_i) \setminus \mathfrak{p}_i$, then $xyz_i \in I \subseteq \mathfrak{q}_i$. Since \mathfrak{q}_i is primary and $x \notin \mathfrak{p}_i$, we obtain $yz_i \in \mathfrak{q}_i$ and so by the choice of c_i , we

have $yc_i \in I$, that is, $y \in (I : c_i)$, which is a contradiction. This proves the claim. Conversely, suppose $(I : x)$ is a prime ideal \mathfrak{p} for some $x \in A$. Then $\mathfrak{p} = (\cap \mathfrak{q}_i : x) = \cap (\mathfrak{q}_i : x)$, and thus $(\mathfrak{q}_i : x) \subseteq \mathfrak{p}$ for some i . Hence $x \notin \mathfrak{q}_i$ and $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \subseteq \sqrt{(\mathfrak{q}_i : x)} \subseteq \mathfrak{p}$. Also, $a \in \mathfrak{p} \Rightarrow ax \in I \subseteq \mathfrak{q}_i \Rightarrow a \in \mathfrak{p}_i$. Thus $\mathfrak{p} = \mathfrak{p}_i$. Finally, the uniqueness of the primary component \mathfrak{q}_i corresponding to a minimal prime \mathfrak{p}_i can be proved by localizing at \mathfrak{p}_i . \square

Definition 2.11. A decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h$, as in (i) above is called a *primary decomposition* of I . If $\mathfrak{q}_1, \dots, \mathfrak{q}_h$ satisfy the conditions in (ii), then it is called an *irredundant (primary) decomposition* of I ; the uniquely determined primes $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are called the *associated primes* of I (in A) and the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}$ is denoted by $\text{Ass}(A/I)$. An associated prime \mathfrak{p}_i is called a *minimal prime* or an *isolated prime* of I if $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for all $j \neq i$; otherwise \mathfrak{p}_i is called an *embedded prime* of I . The set of minimal primes of I in A is denoted by $\text{Min}(A/I)$. It may be noted that $\text{Min}(A/I)$ coincides with the set of minimal elements of $V(I)$, i.e, the minimal primes of I in A are precisely the minimal elements among the prime ideals of A containing I .

It is easy to see that primary decompositions are neatly preserved under the fundamental processes of forming polynomial rings, quotient rings (by smaller ideals), and localizations w.r.t. multiplicatively closed subsets that are disjoint from all associated primes. If S is an arbitrary multiplicatively closed subset of A and $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h$, then

$$S^{-1}I = \bigcap_{\mathfrak{p}_i \cap S = \emptyset} S^{-1}\mathfrak{q}_i \quad \text{and} \quad S^{-1}I \cap A = \bigcap_{\mathfrak{p}_i \cap S = \emptyset} \mathfrak{q}_i.$$

A special case of this is of some interest. Suppose $\mathfrak{p} \in \text{Spec } A$ and $I = \mathfrak{p}^n$. We have seen that I need not be a primary ideal. But \mathfrak{p} is contained in any associated prime of I . Hence \mathfrak{p} is the only minimal prime of I , and so by Proposition 2.10, there is a unique \mathfrak{p} -primary ideal in any irredundant primary decomposition of \mathfrak{p}^n ; this primary ideal is denoted by $\mathfrak{p}^{(n)}$ and is called the *n th symbolic power* of \mathfrak{p} . Note that this symbolic power is alternatively given by $\mathfrak{p}^{(n)} = \mathfrak{p}^n A_{\mathfrak{p}} \cap A$. Indeed $\mathfrak{p}^n A_{\mathfrak{p}}$ is a primary ideal of $A_{\mathfrak{p}}$, being a power of the (unique) maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$; its contraction to A is primary and this is precisely the primary component of \mathfrak{p} in \mathfrak{p}^n .

Examples 2.12. (i) Let $A = k[X, Y]$ and $I = (X^2, XY)$. Then $I = (X) \cap (X^2, Y)$ gives an irredundant primary decomposition of I . The associated primes of I are $\mathfrak{p}_1 = (X)$ and $\mathfrak{p}_2 = (X, Y)$; clearly, \mathfrak{p}_1 is minimal, while \mathfrak{p}_2 is embedded. Observe that $I = (X) \cap (X^2, Y + cX)$ is also an irredundant primary decomposition of I , for any $c \in k$.

(ii) Let $A = k[X, Y, Z]/(XY - Z^2)$ and write x, y, z for the images of X, Y, Z in A , respectively. We have seen that if $\mathfrak{p} = (x, z)$, then \mathfrak{p} is prime but $\mathfrak{p}^2 = (x^2, xz, z^2)$ is not primary. Now $y \in A \setminus \mathfrak{p}$ and thus

$x = z^2/y$ is in $\mathfrak{p}^2 A_{\mathfrak{p}} \cap A$. In fact, it can be seen that $\mathfrak{p}^{(2)} = (x, z^2)$ and that $\mathfrak{p}^2 = (x, z^2) \cap (x^2, y, z)$ is a primary decomposition of \mathfrak{p}^2 in A .

The following result is a nice application of primary decomposition (Proposition 2.10) and Nakayama's Lemma (Proposition 1.13).

Proposition 2.13 (Krull's Intersection Theorem). *Suppose A is noetherian and I is any ideal of A . Then there exists $a \in I$ such that $(1 - a) \cap_{n=0}^{\infty} I^n = 0$. In particular, if $I \neq A$, and A is a local ring, then $\cap_{n=0}^{\infty} I^n = 0$.*

Proof. Let $J = \cap_{n=0}^{\infty} I^n$. Write $IJ = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}_{r+1} \cap \cdots \cap \mathfrak{q}_h$, where \mathfrak{q}_i are \mathfrak{p}_i -primary ideals with $\mathfrak{p}_i \supseteq I$ for $1 \leq i \leq r$ and $\mathfrak{p}_j \not\supseteq I$ for $r < j \leq h$. Fix some $y_j \in I \setminus \mathfrak{p}_j$ for $r < j \leq h$. Then $x \in J \Rightarrow xy_j \in IJ \Rightarrow xy_j \in \mathfrak{q}_j \Rightarrow x \in \mathfrak{q}_j$. Thus $J \subseteq \mathfrak{q}_{r+1} \cap \cdots \cap \mathfrak{q}_h$. Also, since $I \subseteq \mathfrak{p}_i$ for $1 \leq i \leq r$, there exists $m \geq 1$ such that $I^m \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$. Since $J \subseteq I^m$, it follows that $J \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h = IJ$. Thus $IJ = J$. Now apply Nakayama's Lemma. \square

It may be remarked that Krull's Intersection Theorem is usually proved using a result known as the Artin-Rees Lemma. Importance of Krull Intersection Theorem stems from the fact that it paves the way for a Hausdorff topology on a noetherian local ring. See [AM, Ch. 10] for more on this.

We end this section by introducing the notions, ascribed to Krull (1928), of the dimension of a ring and the height of a prime ideal.

Definition 2.14. Let A be a ring. The (*Krull*) *dimension* of A is defined as the maximum of the lengths of chains of prime ideals of A , that is,

$$\dim A := \max \{n : \exists \mathfrak{p}_0, \mathfrak{p}_1, \dots, \mathfrak{p}_n \in \text{Spec } A \text{ such that } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n\};$$

in case A has no prime ideals (which happens only when A is the zero ring), we set $\dim A = -1$, and in case the set of lengths of chains of prime ideals of A is unbounded, we set $\dim A = \infty$. Given any prime ideal \mathfrak{p} of A , the *height* of \mathfrak{p} is defined by $\text{ht } \mathfrak{p} = \dim A_{\mathfrak{p}}$. Equivalently, $\text{ht } \mathfrak{p}$ is the maximum of the lengths of chains $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ of prime ideals of A with $\mathfrak{p}_n = \mathfrak{p}$.

If A is a noetherian ring, the concept of height can be extended to any nonunit ideal I of A by putting $\text{ht } I = \min\{\text{ht } \mathfrak{p} : \mathfrak{p} \in \text{Ass}(A/I)\}$. Note that

$$\text{ht } I = \min\{\text{ht } \mathfrak{p} : \mathfrak{p} \in \text{Min}(A/I)\} = \min\{\text{ht } \mathfrak{p} : \mathfrak{p} \in V(I)\}.$$

Examples 2.15. (i) A field has dimension 0. A PID which is not a field (such as, for example, \mathbb{Z} or $k[X]$) has dimension 1.

(ii) If R is a local ring and I is primary for the unique maximal ideal of R , then $\dim(R/I) = 0$. More generally, if I is any nonunit ideal of a ring A and \mathfrak{p} is a minimal prime of I in A , then $\dim(A_{\mathfrak{p}}/IA_{\mathfrak{p}}) = 0$.

(iii) In the polynomial ring $k[X_1, \dots, X_n]$ we have a chain of prime ideals of length n given by $(0) \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \dots, X_n)$; consequently, $\dim k[X_1, \dots, X_n] \geq n$. Similarly, $\text{ht}(X_1, \dots, X_r) \geq r$.

2.3 Artinian Rings and Modules

Throughout this section A denotes a ring and M denotes an A -module. By a submodule of M , we mean an A -submodule of M . Here is a result similar to Proposition 2.1 with descending chains instead of ascending chains.

Proposition 2.16. *The following conditions are equivalent.*

- (i) (d.c.c.) *If N_1, N_2, \dots are submodules of M with $N_1 \supseteq N_2 \supseteq \dots$, then there exists $m \geq 1$ such that $N_n = N_m$ for $n \geq m$.*
- (ii) (Minimality Condition) *Every nonempty family of submodules of M has a minimal element.*

Proof. The proof of “(i) \Rightarrow (ii)” is identical to that of “(ii) \Rightarrow (iii)” in Proposition 2.1 with ideals replaced by submodules and “ \subset ” replaced by “ \supset ”. Conversely, if $N_1 \supseteq N_2 \supseteq \dots$ is a descending chain of submodules of M and N_m is a minimal element of $\{N_i : i \geq 1\}$, then $N_n = N_m$ for $n \geq m$. \square

We define M to be *artinian* if it satisfies either (and hence both) of the conditions in Proposition 2.16. We say that A is an *artinian ring* if it is artinian as an A -module. This means that A satisfies the d.c.c. on ideals or equivalently, every nonempty set of ideals of A has a minimal element.

Examples 2.17. (i) If V is a vector space over a field k , then it is clear that V is finite dimensional if and only if V satisfies the d.c.c as well as the a.c.c., that is, if and only if V is an artinian module and also a noetherian module. In particular, a finite dimensional vector space is an artinian module and a field is an artinian ring.

(ii) If p is a prime number and $n \in \mathbb{N}$, then $\mathbb{Z}/(p^n)$ is an Artinian \mathbb{Z} -module. To see this, it suffices to observe that the \mathbb{Z} -submodules of $\mathbb{Z}/(p^n)$ correspond to (p^m) for $m = 0, 1, \dots, n$, and these are linearly ordered. Note also that $\mathbb{Z}/(p^n)$ is an artinian ring.

(iii) If k is a field and $A = k[X]$, then $(X) \supset (X^2) \supset (X^3) \supset \dots$ is an infinite strictly descending chains of ideals of A . Thus A is not artinian.

Examples (i) and (iii) above show that an analogue of Hilbert Basis Theorem is not true for artinian rings. However, it is easy to see that if A is artinian, then so is A/I as well as $S^{-1}A$ for any ideal I of A and a multiplicatively closed subset S of A . In the case of modules, we have the following analogues of the results in Section 2.1 for noetherian modules.

Proposition 2.18. *Let N be a submodule of M and let M_1, \dots, M_n be any A -modules. Then we have the following.*

- (i) *M is artinian \iff both N and M/N are artinian.*

(ii) M_i is artinian for $i = 1, \dots, n \implies \bigoplus_{i=1}^n M_i$ is artinian.

(iii) A is artinian and M is a f.g. A -module $\implies M$ is artinian.

Proof. (i), (ii) and (iii) follow from arguments similar to those in the proofs of Proposition 2.5, Corollary 2.6 and Proposition 2.7, respectively. \square

For a finite dimensional vector space over a field, there are several ways of defining the dimension. For example, as the cardinality of (i) a basis or (ii) a minimal generating set or (iii) a maximal linearly independent set. Yet another way is to define the dimension as the length of maximal chains of subspaces of V . Indeed, if $\dim V = n$, then there is a maximal chain $V = V_0 \supset V_1 \supset \dots \supset V_n$ of subspaces and its length (= the number of inclusion signs) is n . Moreover, every maximal chain looks like this. It turns out that the notion of length extends to a slightly more general setting.

In general, a *chain* of submodules of M is a strictly descending sequence $M = M_0 \supset M_1 \supset \dots \supset M_n = 0$ of submodules of M ; the *length* of such a chain is n . A *maximal chain*, i.e., a chain in which no extra submodules can be added, is called a *composition series* of M . Note that a chain $M = M_0 \supset M_1 \supset \dots \supset M_n = 0$ of submodules of M is a composition series of M if and only if M_{i-1}/M_i is simple (that is, it has no submodules other than 0 and itself) for each $i = 1, \dots, n$. We define the *length* of M , denoted by $\ell_A(M)$ or simply by $\ell(M)$, to be the minimum of the lengths of composition series of M . In case M has no composition series, we set $\ell(M) = \infty$.

Proposition 2.19. *Assume that M has finite length. Then we have the following.*

- (i) Every submodule N of M has finite length. Also, $N \subset M \implies \ell(N) < \ell(M)$.
- (ii) Every chain of submodules of M has length $\leq \ell(M)$.
- (iii) A chain of submodules of M is a composition series iff its length is $\ell(M)$.
- (iv) Every chain of submodules of M can be refined to a composition series.

Proof. Let $n = \ell(M)$ and let $M = M_0 \supset M_1 \supset \dots \supset M_n = 0$ be a composition series of M of length n . Then M_{i-1}/M_i is simple for $i = 1, \dots, n$.

(i) Given a submodule N of M , let $N_i = N \cap M_i$ for $i = 0, 1, \dots, n$. Then N_{i-1}/N_i can be viewed as a submodule of M_{i-1}/M_i ; since the latter is simple, we have $N_{i-1} = N_i$ or $N_{i-1}/N_i = M_{i-1}/M_i$. Thus, throwing away repetitions in the sequence $N = N_0 \supseteq N_1 \supseteq \dots \supseteq N_n = 0$, we obtain a composition series for N of length $\leq n$. Hence $\ell(N) \leq n = \ell(M)$. Further, if $\ell(N) = n$, then we must have $N_{i-1}/N_i = M_{i-1}/M_i$ for $i = 1, \dots, n$. Consequently, $N_{n-1} = M_{n-1}$, and so $N_{n-2} = M_{n-2}$, and continuing in this way, we obtain $N = M$. It follows that $N \subset M$ implies $\ell(N) < \ell(M)$.

(ii) If $M = M'_0 \supset M'_1 \supset \dots \supset M'_r = 0$ is any chain of submodules of M , then by (i), $n = \ell(M) > \ell(M'_1) > \dots > \ell(M'_r) = 0$, and hence $r \leq n$.

(iii) If $M = M'_0 \supset M'_1 \supset \cdots \supset M'_r = 0$ is a composition series of M , then $r \leq n$, by (ii). Also, $r \leq n$ by the definition of length. Thus $r = \ell(M)$. Conversely, if $r = \ell(M)$ and the chain is not a composition series, then we can insert some terms to get a chain of length $> \ell(M)$. This contradicts (ii).

(iv) In view of (iii), if a chain is not a composition series, then new terms can be added to it until its length becomes n , as desired. \square

Proposition 2.20. M has finite length $\iff M$ is both noetherian and artinian.

Proof. If $\ell(M) < \infty$, then by Proposition 2.19, any chain of submodules of M is finite, and hence the a.c.c. as well as the d.c.c. is satisfied by M . Conversely, if M is noetherian, then there is a maximal submodule $M_1 \subset M$; further, if $M_1 \neq 0$, then there is a maximal submodule $M_2 \subset M_1$. If M is also artinian, then the descending chain $M \supset M_1 \supset M_2 \supset \cdots$ must be finite. Thus if M is both noetherian and artinian, then M has a composition series of finite length, and hence $\ell(M) < \infty$. \square

Corollary 2.21. Let V be a vector space over a field k . Then

V is finite dimensional $\iff V$ is noetherian $\iff V$ is artinian.

Proof. If V is finite dimensional, then $\ell(V) = \dim_k V < \infty$, and so by Proposition 2.20, V is both noetherian and artinian. On the other hand, if $\dim V$ is not finite, then we can find an infinite linearly independent set $\{x_1, x_2, \dots\}$ in V . Now if $L_n = \text{span}\{x_1, \dots, x_n\}$ and $R_n = \text{span}\{x_n, x_{n+1}, \dots\}$, then considering the subspaces $L_1 \subset L_2 \subset \cdots$ and $R_1 \supset R_2 \supset \cdots$, we see that V is neither noetherian nor artinian. This proves the desired equivalence. \square

Proposition 2.22. Let N be a submodule of M . Then

M has finite length \iff both N and M/N have finite length.

Moreover, if M has finite length, then $\ell(M) = \ell(N) + \ell(M/N)$.

Proof. The equivalence follows from Propositions 2.5, 2.18 (i), and 2.20. Moreover, if $\ell(M) < \infty$, then combining a composition series of N and (the inverse image of) a composition series of M/N we obtain a composition series of M . Thus, in view of Proposition 2.18, $\ell(M) = \ell(N) + \ell(M/N)$. \square

Proposition 2.23. If the zero ideal of A is a product $\mathfrak{m}_1 \cdots \mathfrak{m}_r$ of (not necessarily distinct) maximal ideals of A , then A is noetherian if and only if A is artinian.

Proof. Let $I_0 = A$ and $I_j = \mathfrak{m}_1 \cdots \mathfrak{m}_j$ for $j = 1, \dots, r$. Since $I_r = 0$, by finite induction on r and using Propositions 2.5 and 2.18 (i), we see that I_{i-1}/I_j is noetherian (resp: artinian) for all $j = 1, \dots, r$ if and only if A is noetherian (resp: artinian). But each I_{i-1}/I_j is annihilated by \mathfrak{m}_j and thus it is not only an A -module but also an A/\mathfrak{m}_j -module, that is, a vector space over the field A/\mathfrak{m}_j . Hence by Corollary 2.21, I_{i-1}/I_j is noetherian if and only if it is artinian. This yields the desired result. \square

We will now use the previous proposition to derive a useful and interesting characterization of artinian rings. But first, let us derive some simpler properties of artinian rings.

Proposition 2.24. *Let A be an artinian ring. Then we have the following.*

(i) A is a domain $\iff A$ is a field.

(ii) $\text{Spec}(A) = \text{Max}(A)$. In particular, $\sqrt{(0)} = \mathcal{J}(A)$.

(iii) $\text{Max}(A)$ is finite.

(iv) If $\mathfrak{N} = \sqrt{(0)}$ is the nilradical of A , then $\mathfrak{N}^m = (0)$ for some $m \in \mathbb{N}$.

Proof. (i) Given any $a \in A$, applying the d.c.c. to the chain $(a) \supseteq (a^2) \supseteq \dots$, we see that $(a^n) = (a^{n+1})$ for some $n \geq 1$. Hence $a^n = ba^{n+1}$ for some $b \in A$. Now if A is a domain and $a \neq 0$, then $a^n \neq 0$ and hence $ba = 1$. Thus an artinian domain is a field. The converse is trivial.

(ii) Given any $\mathfrak{p} \in \text{Spec}(A)$, apply (i) to A/\mathfrak{p} . This gives $\text{Spec}(A) = \text{Max}(A)$. Consequently, $\sqrt{(0)} = \mathcal{J}(A)$, by Propositions 1.9 and 1.10.

(iii) If A is the zero ring, there is nothing to prove. Assume that $A \neq 0$. Consider the set \mathcal{F} of all finite intersections of maximal ideals of A . This is nonempty and hence has a minimal element, say $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$. Now for any $\mathfrak{m} \in \text{Max}(A)$, $\mathfrak{m} \cap \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r \in \mathcal{F}$. Hence by the minimality of $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$, we see that $\mathfrak{m} \supseteq \mathfrak{m} \cap \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$, and this implies $\mathfrak{m} \supseteq \mathfrak{m}_i$ for some i . Since \mathfrak{m}_i is maximal, we obtain $\mathfrak{m} = \mathfrak{m}_i$. It follows that $\text{Max}(A) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_r\}$.

(iv) Applying d.c.c. to the chain $\mathfrak{N} \supseteq \mathfrak{N}^2 \supseteq \dots$, we see that there is $m \geq 1$ with $\mathfrak{N}^n = \mathfrak{N}^m$ for $n \geq m$. Suppose, if possible, $I := \mathfrak{N}^m$ is nonzero. Then the set $\{J : J \text{ an ideal of } A \text{ with } IJ \neq (0)\}$ is nonempty; hence it has a minimal element, say J_0 . Since $IJ_0 \neq (0)$, there is $a \in J_0$ such that $I(a) \neq (0)$. Hence $J_0 = (a)$, by the minimality of J_0 . Further $I^2 = I$ and so $I(I(a)) = I(a) \neq (0)$. Hence $I(a) = (a)$, again by the minimality of $J_0 = (a)$. It follows that $a = ua$ for some $u \in I$, and consequently, $a = u^j a$ for all $j \geq 1$. But, $u \in I \subseteq \sqrt{(0)}$, and hence $u^j = 0$ for some $j \geq 1$. Thus, $a = 0$, which is a contradiction. It follows that $\mathfrak{N}^m = I = (0)$. \square

Proposition 2.25. *A ring is artinian iff it is noetherian and zero dimensional.*

Proof. Suppose A is an artinian ring. Then by part (ii) of Proposition 2.24, $\dim A = 0$. Further, by parts (iii) and (iv) of Proposition 2.24, we see that $(\mathfrak{m}_1 \mathfrak{m}_2 \dots \mathfrak{m}_r)^m = (\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r)^m = 0$ for some $m \geq 1$ and (finitely many) maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ of A . Hence by Proposition 2.23, A is noetherian. Conversely, if A is noetherian and $\dim A = 0$, then every prime ideal of A is maximal, and hence in view of Proposition 2.10, $\sqrt{(0)}$ is an intersection $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$ of maximal ideals of A . Since A is noetherian, $(\mathfrak{m}_1 \mathfrak{m}_2 \dots \mathfrak{m}_r)^m = (\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r)^m = 0$ for some $m \geq 1$, and hence by Proposition 2.23, A is artinian. \square

2.4 Krull's Principal Ideal Theorem

In this section we shall prove an important result in dimension theory of commutative rings, due to Krull (1929), called the Principal Ideal Theorem or the *Hauptidealsatz*. The proof given here is along classical lines and will use the notion of symbolic powers introduced in Section 2.2. For a more modern approach, using the so called Dimension Theorem, one may consult [AM] or [M2].

Proposition 2.26 (Krull's Principal Ideal Theorem). *Let A be a noetherian ring and \mathfrak{p} be a minimal prime of a principal ideal (a) of A . Then $\text{ht } \mathfrak{p} \leq 1$.*

Proof. By localizing at \mathfrak{p} , we can and will assume that A is a local ring with \mathfrak{p} as its unique maximal ideal. Let \mathfrak{p}_1 be any prime ideal of A such that $\mathfrak{p}_1 \subset \mathfrak{p}$. It suffices to show that $\text{ht } \mathfrak{p}_1 = 0$. Since \mathfrak{p} is a minimal prime of (a) and the unique maximal ideal of A , we see that $\dim A/(a) = 0$ and $a \notin \mathfrak{p}_1$. Consider

$$(a) + \mathfrak{p}_1 \supseteq (a) + \mathfrak{p}_1^{(2)} \supseteq (a) + \mathfrak{p}_1^{(3)} \supseteq \dots,$$

where $\mathfrak{p}_1^{(n)}$ denotes the n th symbolic power of \mathfrak{p}_1 . This corresponds to a descending chain of ideals of $A/(a)$. By Proposition 2.25, $A/(a)$ is artinian, and hence there is $n \geq 1$ such that $(a) + \mathfrak{p}_1^{(n)} = (a) + \mathfrak{p}_1^{(n+1)}$. In particular, given any $x \in \mathfrak{p}_1^{(n)}$, we can write $x = ab + y$ for some $b \in A$ and $y \in \mathfrak{p}_1^{(n+1)}$. Now $ab \in \mathfrak{p}_1^{(n)}$ and since $a \notin \mathfrak{p}_1$ and $\mathfrak{p}_1^{(n)}$ is \mathfrak{p}_1 -primary, we see that $b \in \mathfrak{p}_1^{(n)}$. Thus, $\mathfrak{p}_1^{(n)} = (a)\mathfrak{p}_1^{(n)} + \mathfrak{p}_1^{(n+1)}$. Hence by Nakayama's Lemma (applied to the module $\mathfrak{p}_1^{(n)}/\mathfrak{p}_1^{(n+1)}$), we obtain $\mathfrak{p}_1^{(n)} = \mathfrak{p}_1^{(n+1)}$. This implies that $\mathfrak{p}_1^n A_{\mathfrak{p}_1} = \mathfrak{p}_1^{n+1} A_{\mathfrak{p}_1} = (\mathfrak{p}_1 A_{\mathfrak{p}_1})(\mathfrak{p}_1^n A_{\mathfrak{p}_1})$. Applying Nakayama's Lemma once again (this time to the $A_{\mathfrak{p}_1}$ -module $\mathfrak{p}_1^n A_{\mathfrak{p}_1}$), we obtain $\mathfrak{p}_1^n A_{\mathfrak{p}_1} = 0$. It follows that $\mathfrak{p}_1 A_{\mathfrak{p}_1}$ is the only prime ideal of $A_{\mathfrak{p}_1}$ and $\dim A_{\mathfrak{p}_1} = 0$, that is, $\text{ht } \mathfrak{p}_1 = 0$. \square

The above result can be readily generalized.

Proposition 2.27 (Generalized Krull's Principal Ideal Theorem). *Let A be a noetherian ring and \mathfrak{p} be a minimal prime of an ideal (a_1, \dots, a_r) generated by r elements of A . Then $\text{ht } \mathfrak{p} \leq r$. Consequently, $\text{ht } (a_1, \dots, a_r) \leq r$.*

Proof. By localizing at \mathfrak{p} , we can and will assume that A is a local ring with \mathfrak{p} as its unique maximal ideal. This implies that (a_1, \dots, a_r) is \mathfrak{p} -primary. We shall now proceed by induction on r . Proposition 2.26 settles the case $r = 1$. Suppose $r > 1$ and the result holds for $r - 1$. Let \mathfrak{p}_1 be any prime ideal of A such that $\mathfrak{p}_1 \subset \mathfrak{p}$ and \mathfrak{p}_1 is maximal among prime ideals of A strictly contained in \mathfrak{p} . It suffices to show that $\text{ht } \mathfrak{p}_1 \leq r - 1$. To begin with, note that not all a_i ($1 \leq i \leq r$) can be in \mathfrak{p}_1 . Assume, without loss of generality, that $a_1 \notin \mathfrak{p}_1$. Now, $\mathfrak{p}_1 \subset \mathfrak{p}_1 + (a_1) \subseteq \mathfrak{p}$, and hence \mathfrak{p} is a minimal prime of $\mathfrak{p}_1 + (a_1)$. But \mathfrak{p} is also the unique maximal ideal of A . Hence

$\mathfrak{p}_1 + (a_1)$ is \mathfrak{p} -primary, and since A is noetherian, there is $m \geq 1$ such that $\mathfrak{p}^m \subseteq \mathfrak{p}_1 + (a_1)$. In particular, for $i = 2, \dots, r$ we can write $a_i^m = y_i + x_i a_1$ for some $y_i \in \mathfrak{p}_1$ and $x_i \in A$. Now (a_1, \dots, a_r) is \mathfrak{p} -primary and $a_i^m \in (a_1, y_2, \dots, y_r)$ for $1 \leq i \leq r$. Hence $\mathfrak{p}^N \subseteq (a_1, y_2, \dots, y_r)$ for some large enough $N \geq 1$. Hence \mathfrak{p} is a minimal prime of (a_1, y_2, \dots, y_r) , and therefore $\mathfrak{p}/(y_2, \dots, y_r)$ is a minimal prime of $(a_1, y_2, \dots, y_r)A/(y_2, \dots, y_r)$. But the latter is a principal ideal of $A/(y_2, \dots, y_r)$. Hence by Proposition 2.26, the height of $\mathfrak{p}/(y_2, \dots, y_r)$ is ≤ 1 , and therefore, the height of $\mathfrak{p}_1/(y_2, \dots, y_r)$ is ≤ 0 . It follows that \mathfrak{p}_1 is a minimal prime of (y_2, \dots, y_r) , and so by the induction hypothesis, $\text{ht } \mathfrak{p}_1 \leq r - 1$. This proves that $\text{ht } \mathfrak{p} \leq r$. \square

The above result has a number of interesting consequences. We outline some of them below.

1. Every ideal of a noetherian ring is of finite height.
2. The d.c.c. is satisfied by the prime ideals in a noetherian ring.
3. In the polynomial ring $k[X_1, \dots, X_r]$, we have $\text{ht}(X_1, \dots, X_r) = r$.
4. Let A be a noetherian domain. Then A is a UFD if and only if every height 1 prime ideal of A is principal.

Of these assertions, the first is obvious from Proposition 2.27, while the second follows from the first. To see the third, recall from Example 2.15 (iii), that $\text{ht}(X_1, \dots, X_r) \geq r$; the other inequality $\text{ht}(X_1, \dots, X_r) \leq r$ follows from Proposition 2.27. Finally, the fourth assertion that gives a characterization of UFD's can be proved as follows. If A is a UFD and \mathfrak{p} a height 1 prime ideal of A , then there is $a \in \mathfrak{p}$ such that a is irreducible (check!); moreover, since A is a UFD, (a) is a nonzero prime ideal of A with $(a) \subseteq \mathfrak{p}$. But since $\text{ht } \mathfrak{p} = 1$, we must have $\mathfrak{p} = (a)$, that is, \mathfrak{p} is principal. Conversely, suppose every height 1 prime ideal of A is principal. Since A is a noetherian domain, it satisfies a.c.c. on principal ideals of A , and hence every nonzero element of A can be factored as a product of irreducible elements. Thus it suffices to show that an irreducible element of A is prime. Let $a \in A$ be irreducible. If \mathfrak{p} is a minimal prime of (a) , then $\text{ht } \mathfrak{p} \leq 1$. Moreover, since \mathfrak{p} contains $a \neq 0$, it follows that $\text{ht } \mathfrak{p} = 1$. Hence by our hypothesis, \mathfrak{p} is principal, that is, $\mathfrak{p} = (b)$ for some $b \in A$. Now, a is irreducible and $(a) \subseteq (b) \neq A$ implies $(a) = (b) = \mathfrak{p}$. Hence (a) is a prime ideal of A and so a is prime.

Remark 2.28. A converse of (Generalized) Krull's Principal Ideal Theorem is true. Namely, if A is noetherian and $\mathfrak{p} \in \text{Spec}(A)$ has height r , then \mathfrak{p} is a minimal prime of an ideal generated by r elements of A . This can be proved as an easy consequence of Prime Avoidance Lemma and Proposition 2.27, and we leave the details as an exercise. This converse can be used to prove the following interesting characterization of the dimension of a local ring.

Let R be a local ring with \mathfrak{m} as its unique maximal ideal. By a *system of parameters* for R we mean elements x_1, \dots, x_d of R such that (x_1, \dots, x_d) is \mathfrak{m} -primary, that is, $\mathfrak{m}^n \subseteq (x_1, \dots, x_d)$ for some $n \in \mathbb{N}$. Define

$$s(R) := \min\{d \in \mathbb{N} : \exists \text{ a system of parameters for } R \text{ with } d \text{ elements}\}.$$

Then $s(R) = \dim R$. Indeed, if (x_1, \dots, x_d) is \mathfrak{m} -primary, then \mathfrak{m} is a minimal prime of (x_1, \dots, x_d) , and so by Proposition 2.27, $\dim R = \text{ht } \mathfrak{m} \leq d$. Thus $\dim R \leq s(R)$. On the other hand, if $\dim R = \text{ht } \mathfrak{m} = d$, then by the (above mentioned) converse of Krull's Principal Ideal Theorem, there exist $x_1, \dots, x_d \in R$ such that \mathfrak{m} is a minimal prime of (x_1, \dots, x_d) . But since \mathfrak{m} is the unique maximal ideal of R , it follows that (x_1, \dots, x_d) is \mathfrak{m} -primary. This shows that $s(R) \leq d = \dim R$.

Exercises

Throughout the following exercises A denotes a ring.

1. Let $A = k[X_1, X_2, \dots]$ be the polynomial ring in infinitely many variables with coefficients in a field k . Prove that A is not noetherian.
2. Let \mathfrak{q} be an ideal of A and $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Show that if A is noetherian, then $\mathfrak{p}^n \subseteq \mathfrak{q}$ for some $n \in \mathbb{N}$. Is this result valid if A is not noetherian? Justify your answer.
3. Let \mathfrak{q} be a nonunit ideal of A . Show that \mathfrak{q} is primary if and only if every zerodivisor in A/\mathfrak{q} is nilpotent.
4. Let \mathfrak{q} be a \mathfrak{p} -primary ideal and x be an element of A . Show that if $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = (1)$, whereas if $x \notin \mathfrak{q}$, then $(\mathfrak{q} : x)$ is \mathfrak{p} -primary, and in particular, $\sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$. Further show that if $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.
5. Show that if \mathfrak{q} is an ideal of A such that $\sqrt{\mathfrak{q}} \in \text{Max}(A)$, then \mathfrak{q} is primary.
6. Let $A = \mathbb{Z}[X]$ and consider the ideals $\mathfrak{q} = (4, X)$ and $\mathfrak{m} = (2, X)$. Show that \mathfrak{m} is a maximal ideal of A and \mathfrak{q} is \mathfrak{m} -primary, but \mathfrak{q} is not a power of \mathfrak{m} .
7. Let $A = k[X, Y]$ and $I = (X^2, XY, Y^2)$. Show that $I = (X^2, Y) \cap (X, Y^2)$ is a primary decomposition of I . Is this an irredundant primary decomposition of I ? Justify your answer.
8. Let I be a radical ideal and $I = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_h$ be an irredundant primary decomposition of I , where \mathfrak{q}_i is \mathfrak{p}_i -primary for $1 \leq i \leq h$. Show that $I = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_h$. Deduce that I has no embedded component, and that $\mathfrak{q}_i = \mathfrak{p}_i$ for $1 \leq i \leq h$.

9. Given an ideal I of A , define $\mathcal{Z}(A/I) := \{x \in A : (I : x) \neq I\} \cup \{0\}$. Show that $\mathcal{Z}(A/I)$ is the union of the associated primes of I , that is,

$$\mathcal{Z}(A/I) = \bigcup_{\mathfrak{p} \in \text{Ass}(A/I)} \mathfrak{p} \quad \text{and deduce that} \quad \mathcal{Z}(A) = \bigcup_{\mathfrak{p} \in \text{Ass}(A/(0))} \mathfrak{p},$$

where $\mathcal{Z}(A)$ denotes the set of all zerodivisors of A .

10. Let I be a nonunit ideal of A and $\text{Ass}(A/I)$ be the set of associated primes of I in A . Show that the minimal elements in $\text{Ass}(A/I)$ are precisely the minimal elements in the set $V(I) = \{\mathfrak{p} \in \text{Spec } A : \mathfrak{p} \supseteq I\}$ of primes containing I .
11. Let S be a multiplicative closed subset of A and \mathfrak{q} be a \mathfrak{p} -primary ideal of A . Show that if $S \cap \mathfrak{p} \neq \emptyset$, then $S^{-1}\mathfrak{q} = S^{-1}A$, whereas if $S \cap \mathfrak{p} = \emptyset$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$ -primary and $S^{-1}\mathfrak{q} \cap A = \mathfrak{q}$. Deduce that if I is any ideal of A and $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h$ is a primary decomposition of I in A , then

$$S^{-1}I = \bigcap_{\mathfrak{p}_i \cap S = \emptyset} S^{-1}\mathfrak{q}_i \quad \text{and} \quad S^{-1}I \cap A = \bigcap_{\mathfrak{p}_i \cap S = \emptyset} \mathfrak{q}_i.$$

12. Let $A = k[X, Y, Z]/(XY - Z^2)$ and write x, y, z for the images of X, Y, Z in A , respectively. Show that $\mathfrak{p} = (x, z)$ is a prime ideal of A , but $\mathfrak{p}^2 = (x^2, xz, z^2)$ is not primary. Further show that $x \notin \mathfrak{p}^2$, but $x \in \mathfrak{p}^{(2)}$.
13. Given an ideal I of A , let $I[X]$ denote the set of all polynomials in $A[X]$ with coefficients in I . Show that $IA[X] = I[X]$ and also that
- (i) $\mathfrak{p} \in \text{Spec}(A) \implies \mathfrak{p}[X] \in \text{Spec}(A[X])$;
 - (ii) \mathfrak{q} is \mathfrak{p} -primary $\implies \mathfrak{q}[X]$ is $\mathfrak{p}[X]$ -primary;
 - (iii) \mathfrak{p} is a minimal prime of $I \implies \mathfrak{p}[X]$ is a minimal prime of $I[X]$;
 - (iv) $I = \bigcap_{i=1}^n \mathfrak{q}_i$ a primary decomposition of I
 $\implies I[X] = \bigcap_{i=1}^n \mathfrak{q}_i[X]$ a primary decomposition of $I[X]$.
14. Let Δ be a simplicial complex with vertex set $V = \{1, 2, \dots, n\}$, and let F_1, F_2, \dots, F_m be the facets (that is, maximal faces) of Δ . Let I_Δ be the ideal of $k[X_1, \dots, X_n]$ generated by the monomials $X_{i_1} \cdots X_{i_r}$ for which $\{i_1, \dots, i_r\} \notin \Delta$. Given any face F of Δ , let P_F be the ideal of $k[X_1, \dots, X_n]$ generated by the variables X_{j_1}, \dots, X_{j_s} , where $\{j_1, \dots, j_s\} = V \setminus F$. Prove that each P_F is a prime ideal and that $I_\Delta = P_{F_1} \cap \cdots \cap P_{F_m}$ is an irredundant primary decomposition of I_Δ .

15. Let J be a monomial ideal of $k[X_1, \dots, X_n]$ and let u, v be relatively prime monomials in $k[X_1, \dots, X_n]$. Show that $(J, uv) = (J, u) \cap (J, v)$. Also show that if e_1, \dots, e_n are positive integers, then $(X_1^{e_1}, \dots, X_n^{e_n})$ is (X_1, \dots, X_n) -primary. Use these facts to determine the associated primes and a primary decomposition of the ideal (X^2YZ, Y^2Z, YZ^3) of $k[X, Y, Z]$.
16. Consider \mathbb{Q}/\mathbb{Z} as a \mathbb{Z} -module. Determine if it is a noetherian module?
17. Determine the dimension of the ring $\mathbb{Z}[X]$ of polynomials in one variable with integer coefficients.
18. Suppose A is noetherian and I is any ideal of A . Show that $\dim A/I = \max\{\dim A/\mathfrak{p} : \mathfrak{p} \in \text{Ass}(A/I)\} = \max\{\dim A/\mathfrak{p} : \mathfrak{p} \in \text{Min}(A/I)\}$.
19. Let Δ be a simplicial complex with vertex set $V = \{1, 2, \dots, n\}$ and I_Δ be the ideal of $k[X_1, \dots, X_n]$ as defined in Q. 14 of Problem Set 2. Consider the residue class ring $R_\Delta := k[X_1, \dots, X_n]/I_\Delta$. Show that $\dim R_\Delta = d + 1$, where d is the (topological) dimension of Δ . [Note: R_Δ is called the *face ring* or the *Stanley-Reisner ring* associated to Δ .]
20. Assume that A is a noetherian ring. If $a \in A$ is a nonzerodivisor and \mathfrak{p} is a minimal prime of (a) , then prove that $\text{ht } \mathfrak{p} = 1$.
21. Give an example of a minimal prime \mathfrak{p} of a principal ideal of a noetherian ring such that $\text{ht } \mathfrak{p} = 0$.
22. Show that every artinian ring is isomorphic to a direct sum of finitely many artinian local rings. (Hint: Use Proposition 2.24 and the Chinese Remainder Theorem.)
23. Give an example of a zero dimensional local ring that is not noetherian.
24. Prove the converse of Krull's Principal Ideal Theorem: If A is noetherian and $\mathfrak{p} \in \text{Spec}(A)$ has height r , then there exists $a_1, \dots, a_r \in \mathfrak{p}$ such that \mathfrak{p} is a minimal prime of (a_1, \dots, a_r) .
25. Give an example of a prime ideal \mathfrak{p} of height 1 in a noetherian ring A such that \mathfrak{p} is not principal.

Chapter 3

Integral Extensions

3.1 Integral Extensions

The theory of algebraic field extensions has a useful analogue to ring extensions, which is discussed in this section.

Let B be a ring and A be a subring of B . We may express this by saying that B is a (ring) extension of A or that B is an overring of A .

Definition 3.1. An element $x \in B$ is said to be *integral* over A if it satisfies a monic polynomial with coefficients in A , i.e., $x^n + a_1x^{n-1} + \cdots + a_n = 0$ for some $a_1, \dots, a_n \in A$. If every element of B is integral over A , then we say that B is an *integral extension* of A or that B is *integral* over A .

Evidently, if $x \in B$ satisfies $x^n + a_1x^{n-1} + \cdots + a_n = 0$, where $a_1, \dots, a_n \in A$, then $1, x, x^2, \dots, x^{n-1}$ generate $A[x]$ as an A -module. And if B' is a subring of B containing $A[x]$ such that $B' = Ax_1 + \cdots + Ax_n$, then for any $b \in B'$, we can write $bx_i = \sum a_{ij}x_j$ for some $a_{ij} \in A$, and hence b satisfies the monic polynomial $\det(X\delta_{ij} - a_{ij})$ in $A[X]$. Thus we obtain the following criteria.

$$\begin{aligned} x \in B \text{ is integral over } A &\iff A[x] \text{ is a finite } A\text{-module} \\ &\iff \text{a subring } B' \text{ of } B \text{ containing } A[x] \\ &\quad \text{is a finite } A\text{-module.} \end{aligned}$$

In particular, if B is a finite A -module, then B is integral over A . The converse is true if we further assume (the necessary condition) that B is a f.g. A -algebra. This follows by observing that the above criteria implies, using induction, that if $x_1, \dots, x_n \in B$ are integral over A , then $A[x_1, \dots, x_n]$ is a finite A -module. This observation also shows that the elements of B which are integral over A form a subring, say C , of B . If $C = A$, we say that A is *integrally closed* in B . A domain is called *integrally closed* or *normal* if it is integrally closed in its quotient field. Note that if S is a multiplicatively

closed subset of A , B is integral over A , and J is an ideal of B , then $S^{-1}B$ (resp: B/J) is integral over $S^{-1}A$ (resp: $A/J \cap A$).

Example 3.2. Let $B := k[X, Y]/(Y - X^2)$, and let x, y denote the images of X, Y in B so that $B = k[x, y]$. Let $A = k[y]$. Then x is integral over A , and hence B is integral over A . On the other hand, if $B = k[X, Y]/(XY - 1) = k[x, y]$, then x is not integral over $A = k[y]$. It may be instructive to note, indirectly, that $B \simeq k[Y, 1/Y]$ is not a finite $k[Y]$ -module. These examples correspond, roughly, to the fact that the projection of the parabola $y = x^2$ along the x -axis onto the y -axis is a ‘finite’ map in the sense that the inverse image of every point is at ‘finite distance’, whereas in the case of the hyperbola $xy = 1$, this isn’t so. Similar examples in “higher dimensions” can be constructed by considering projections of surfaces onto planes, solids onto 3-space, and so on.

Basic results about integral extensions are as follows. In the seven results given below, B denotes an integral extension of A and $\mathfrak{p} \in \text{Spec}(A)$.

Proposition 3.3. (i) Assume that B (and hence A) is a domain. Then

$$A \text{ is a field} \iff B \text{ is a field.}$$

(ii) Let $\mathfrak{q} \in \text{Spec}(B)$ be such that $\mathfrak{q} \cap A = \mathfrak{p}$. Then

$$\mathfrak{p} \text{ is maximal} \iff \mathfrak{q} \text{ is maximal.}$$

(iii) Let $\mathfrak{q}, \mathfrak{q}' \in \text{Spec}(B)$ be such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}' \cap A = \mathfrak{q} \cap A$. Then $\mathfrak{q} = \mathfrak{q}'$.

Corollary 3.4. $\dim B \leq \dim A$. In particular, if B is a domain and $\dim A \leq 1$, then $\dim A = \dim B$.

Proposition 3.5 (Lying Over Theorem). There exists a prime ideal \mathfrak{q} of B such that $\mathfrak{q} \cap A = \mathfrak{p}$. In particular, $\mathfrak{p}B \cap A = \mathfrak{p}$.

Proposition 3.6 (Going Up Theorem). If \mathfrak{q} is a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, and \mathfrak{p}' is a prime ideal of A such that $\mathfrak{p} \subseteq \mathfrak{p}'$, then there exists a prime ideal \mathfrak{q}' of B such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}' \cap A = \mathfrak{p}'$.

Corollary 3.7. $\dim A = \dim B$.

Proposition 3.8 (Going Down Theorem). Assume that A and B are domains and A is normal. If \mathfrak{q} is a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, and \mathfrak{p}' is a prime ideal of A such that $\mathfrak{p}' \subseteq \mathfrak{p}$, then there exists a prime ideal \mathfrak{q}' of B such that $\mathfrak{q}' \subseteq \mathfrak{q}$ and $\mathfrak{q}' \cap A = \mathfrak{p}'$.

Corollary 3.9. Assume that A and B are domains and A is normal. Then for any prime ideal \mathfrak{q} of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, we have $\text{ht } \mathfrak{p} = \text{ht } \mathfrak{q}$.

Sketch of Proofs of Propositions 3.3, 3.5, 3.6 and 3.8. Easy manipulations with integral equations of relevant elements proves the first assertion of Proposition 3.3; the second and third assertions follow from the first one by passing to quotient rings and localizations respectively. To prove Proposition 3.5, first localize at \mathfrak{p} and, then, note that if $\mathfrak{p}B_0 = B_0$, where $B_0 = (A \setminus \mathfrak{p})^{-1}B$, then $\mathfrak{p}B' = B'$ for some f.g. A -algebra B' ; now B' is a finite A -module and Nakayama's Lemma applies. Proposition 3.6 follows by applying Proposition 3.5 to appropriate quotient rings. To prove Proposition 3.8, consider the multiplicatively closed subset $S = (A \setminus \mathfrak{p}')(B \setminus \mathfrak{q}) = \{ab : a \in A \setminus \mathfrak{p}', b \in B \setminus \mathfrak{q}\}$ of B and note that it suffices to prove $\mathfrak{p}'B \cap S = \emptyset$ [because, then there exists a prime ideal \mathfrak{q}' of B such that $\mathfrak{p}'B \subseteq \mathfrak{q}'$ and $\mathfrak{q}' \cap S = \emptyset$, and this will have the desired properties]. To this end, let $x \in \mathfrak{p}'B \cap S$. Let K and L denote the quotient fields of A and B respectively. Let \overline{L} be a normal extension of K containing L and \overline{B} the integral closure of A in \overline{L} . Since $\mathfrak{p}' \subseteq A$ and $x \in \mathfrak{p}'B$, all the conjugates of x w.r.t L/K are in $\mathfrak{p}'\overline{B}$. Hence the coefficients of the minimal polynomial, say $f(X)$, of x over K are in $\mathfrak{p}'\overline{B} \cap A = \mathfrak{p}'$ (since A is normal!). Write $f(X) = X^d + c_1X^{d-1} + \cdots + c_d$, and $x = ab$, where $c_1, \dots, c_d \in \mathfrak{p}'$, $a \in A \setminus \mathfrak{p}'$ and $b \in B \setminus \mathfrak{q}$. Clearly, $X^d + (c_1/a)X^{d-1} + \cdots + (c_d/a^d)$ is the minimal polynomial of b over K . But A is normal and b is integral over A implies that $c_i = c'_i a^i$ for some $c'_i \in A$ ($1 \leq i \leq d$). Since $c_i \in \mathfrak{p}'$ and $a \notin \mathfrak{p}'$, we have $c'_i \in \mathfrak{p}'$ for $1 \leq i \leq d$. Hence $b^d \in \mathfrak{p}'B \subseteq \mathfrak{p}B \subseteq \mathfrak{q}$, and so $b \in \mathfrak{q}$, which is a contradiction. \square

For a more leisurely proof of the results above, see [AM, pp. 61–64] or [ZS, pp. 257–264].

Remark 3.10. It may be noted that Corollary 3.7 is an analogue of the simple fact that if L/K is an algebraic extension of fields containing a common subfield k , then $\text{tr.deg.}_k L = \text{tr.deg.}_k K$. Recall that if K is a ring containing a field k , then elements $\theta_1, \dots, \theta_d$ of K are said to be *algebraically independent* over k if they do not satisfy any algebraic relation over k , i.e., $f(\theta_1, \dots, \theta_d) \neq 0$ for any $0 \neq f \in k[X_1, \dots, X_d]$. A subset of K is *algebraically independent* if every finite collection of elements in it are algebraically independent. If K is a field then any two maximal algebraically independent subsets have the same cardinality, called the *transcendence degree* of K/k and denoted by $\text{tr.deg.}_k K$; such subsets are then called *transcendence bases* of K/k ; note that an algebraically independent subset S is a transcendence basis of K/k iff K is algebraic over $k(S)$, the smallest subfield of K containing k and S . If B is a domain containing k and K is its quotient field, then one sets $\text{tr.deg.}_k B = \text{tr.deg.}_k K$. Finally, note that $k[X_1, \dots, X_d]$ and its quotient field $k(X_1, \dots, X_d)$ are clearly of transcendence degree d over k . On the other hand, if $\theta_1, \dots, \theta_d$ are algebraically independent over k , then $k[\theta_1, \dots, \theta_d]$ and $k(\theta_1, \dots, \theta_d)$ are k -isomorphic to the polynomial ring $k[X_1, \dots, X_d]$ and the rational function field $k(X_1, \dots, X_d)$, respectively.

A good reference for this material is Chapter 2 of [ZS].

3.2 Noether Normalization

In this section we prove a basic result in Dimension Theory, known as Noether's Normalization Lemma. This result has a number of useful consequences. For example, we will show that for a special class of rings, the notions of Krull dimension and transcendence degree are closely related. Also, we will prove a famous result known as Hilbert's Nullstellensatz.

An essential ingredient in the proof of Noether's Normalization Lemma can be formulated and proved in the form of a lemma, which is of independent interest and use. As an application, we shall compute the dimension of $k[X_1, \dots, X_n]$ and the height of any prime ideal in $k[X_1, \dots, X_n]$ generated by a subset of the variables X_1, \dots, X_n .

The key idea in the proof of the following lemma may be explained by revisiting the example of hyperbola $xy = 1$. We have noticed that the projection from the hyperbola onto the y -axis is not 'finite'. However, if we tilt the axes a bit, e.g., via the coordinate change $X' = X$, $Y' = Y - cX$ for some $c \neq 0$, then the projection becomes a 'finite' map. A similar trick works in general.

Lemma 3.11 (Tilting of Axes Lemma). *Let k be a field and $B = k[X_1, \dots, X_n]$. Given any nonconstant polynomial $f \in B$, there exist $X'_2, \dots, X'_n \in B$ such that f, X'_2, \dots, X'_n are algebraically independent over k and*

$$f = cX_1^m + g_1X_1^{m-1} + \dots + g_m$$

for some $c \in k$, $c \neq 0$ and $g_1, \dots, g_m \in k[X'_2, \dots, X'_n]$. Moreover, X'_2, \dots, X'_n can be chosen such that $X'_i = X_i - X_1^{m_i}$ for some $m_i \geq 1$ ($2 \leq i \leq n$). In case k is infinite, we can choose X'_2, \dots, X'_n to be homogeneous linear polynomials of the form $X'_i = X_i - c_i X_1$ for some $c_i \in k$ ($2 \leq i \leq n$). In particular, B is integral over $A = k[f, X'_2, \dots, X'_n]$. Also, $fB \cap A = fA$ and B/fB is integral over A/fA .

Proof. Let e be an integer greater than any of the exponents of X_1, \dots, X_n appearing in f , and let $m_i = e^{i-1}$ for $2 \leq i \leq n$. In the 'new variables' X_1 and $X'_i = X_i - X_1^{m_i}$ ($2 \leq i \leq n$), a monomial $X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ appearing in f becomes $X_1^{i_1} (X'_2 + X_1^{m_2})^{i_2} \dots (X'_n + X_1^{m_n})^{i_n}$, and this is clearly monic in X_1 of degree $i_1 + i_2 e + \dots + i_n e^{n-1}$. By our choice of e , these degrees are distinct for different values of (i_1, \dots, i_n) , and if m is the maximum of these degrees, then f clearly has the desired form. In case k is infinite, we let $m = \deg f$ and write $f = f_0 + f_1 + \dots + f_m$, where $f_i \in k[X_1, \dots, X_n]_i$. Since $f_m \neq 0$, we can find $c_2, \dots, c_n \in k$ such that $f_m(1, c_2, \dots, c_n) \neq 0$. Now with $X'_i = X_i - c_i X_1$, for $2 \leq i \leq m$, we have $f = f_m(1, c_2, \dots, c_n) X_1^m + g_1 X_1^{m-1} + \dots + g_m$ for some $g_1, \dots, g_m \in k[X'_2, \dots, X'_n]$. Finally, since $B = k[X_1, X'_2, \dots, X'_n]$, it follows that B is integral over $A = k[f, X'_2, \dots, X'_n]$. In particular, $\text{tr.deg.}_k A = n$, and hence

f, X'_2, \dots, X'_n are algebraically independent over k , and A is isomorphic to a polynomial ring in n variables over k . This implies that A is a normal domain and thus if $fh \in A$ for some $h \in B$, then $h \in A$, being in the quotient field of A and integral over A . Thus $fB \cap A = fA$ and consequently, B/fB is integral over A/fA . \square

Corollary 3.12. $\dim k[X_1, \dots, X_n] = n$. In particular, $\text{ht}(X_1, \dots, X_r) = r$, for $1 \leq r \leq n$.

Proof. Let $B = k[X_1, \dots, X_n]$. Since $(X_1) \subset (X_1, X_2) \subset \dots \subset (X_1, \dots, X_n)$ is a chain of prime ideals of B of length n , we have $\dim B \geq n$. We prove $\dim B \leq n$ by induction on n . The case of $n = 0$ is obvious. For the inductive step, let $P_0 \subset P_1 \subset \dots \subset P_m$ be a chain of prime ideals of B of length $m > 0$. Choose $0 \neq f \in P_1$. By Lemma 3.11, we obtain $X'_2, \dots, X'_n \in B$ such that B is integral over $A = k[f, X'_2, \dots, X'_n]$. Hence by Proposition 3.3, $A \cap P_1 \subset \dots \subset A \cap P_m$ is a chain of prime ideals of A of length $m - 1$, containing fA . Passing to A/fA and using the induction hypothesis, we see that $m - 1 \leq n - 1$. Hence $m \leq n$. \square

Proposition 3.13 (Noether's Normalization Lemma). Let $B = k[x_1, \dots, x_n]$ be a f.g. algebra over a field k and $J_1 \subseteq \dots \subseteq J_m$ be a chain of nonunit ideals of B . Then there exist $\theta_1, \dots, \theta_d \in B$ and nonnegative integers $r_1 \leq \dots \leq r_m$ satisfying the following.

- (i) $\theta_1, \dots, \theta_d$ are algebraically independent over k ,
- (ii) B is integral over $A = k[\theta_1, \dots, \theta_d]$; in particular, B is a finite A -module,
- (iii) $J_i \cap A = (\theta_1, \dots, \theta_{r_i})A$ for $1 \leq i \leq m$.

Moreover, if k is infinite, then $\theta_1, \dots, \theta_d$ can be chosen to be k -linear combinations of x_1, \dots, x_n .

Proof. It suffices to prove the result when $B = k[X_1, \dots, X_n]$ is the polynomial ring in n variables over k (because in general, $B \simeq B'/J'_0$ where $B' = k[X_1, \dots, X_n]$ and J'_0 is an ideal of B' ; now if J'_1, \dots, J'_m are the ideals of B' , containing J'_0 , corresponding to J_1, \dots, J_m respectively, then applying the result to B' and the chain $J'_0 \subseteq J'_1 \subseteq \dots \subseteq J'_m$, we obtain $\theta'_1, \dots, \theta'_n$ and r'_0, r'_1, \dots, r'_m , and it is easily seen that the images $\theta_1, \dots, \theta_d$ of $\theta'_{r'_0+1}, \dots, \theta'_n$ in B and the integers r_1, \dots, r_m defined by $r_i = r'_i - r'_0$ have the desired properties). Thus we shall now assume that $B = k[X_1, \dots, X_n]$. Let us induct on m . Note that the case $m = 0$ is obvious.

Consider the case when $m = 1$. Here, we induct on n . The case $n = 0$ being trivial, assume that $n \geq 1$. We may also assume that $J_1 \neq 0$. Let $0 \neq f \in J_1$. Then we can find X'_2, \dots, X'_n as in Lemma 3.11. By the induction hypothesis, there exist $\theta_2, \dots, \theta_n \in A' = k[X'_2, \dots, X'_n]$ such that $\theta_2, \dots, \theta_n$ are algebraically independent over k , A' is integral over $k[\theta_2, \dots, \theta_n]$, and

there exists $r \geq 1$ such that $J_1 \cap k[\theta_2, \dots, \theta_n] = (\theta_2, \dots, \theta_r)$. Hence $A = A'[f]$ is integral over $k[f, \theta_2, \dots, \theta_n]$, and therefore so is B . Consequently, $\text{tr.deg.}_k k[f, \theta_2, \dots, \theta_n] = \text{tr.deg.}_k B = n$, and so if we let $\theta_1 = f$, then $\theta_1, \dots, \theta_n$ are algebraically independent over k . Moreover, since $f \in J_1$ and $J_1 \cap k[\theta_1, \dots, \theta_n] = (\theta_1) + J_1 \cap k[\theta_2, \dots, \theta_n] = (\theta_1, \dots, \theta_r)$.

If $m > 1$ and we assume that the result holds for $m - 1$, then for the chain $J_1 \subseteq \dots \subseteq J_{m-1}$, there exist $\theta'_1, \dots, \theta'_n \in B$ and nonnegative integers r'_1, \dots, r'_{m-1} satisfying conditions such as (i), (ii) and (iii). Let $r = r'_{m-1}$. Using the previous case (of $m = 1$), we can find $\theta''_{r+1}, \dots, \theta''_n$ in $B'' = k[\theta'_{r+1}, \dots, \theta'_n]$, and an integer $s \geq r$ such that $\theta''_{r+1}, \dots, \theta''_n$ are algebraically independent over k , B'' is integral over $A'' = k[\theta'_{r+1}, \dots, \theta'_n]$, and $J_m \cap A'' = (\theta''_{r+1}, \dots, \theta''_n)$. Define $\theta_i = \theta'_i$ if $1 \leq i \leq r$ and $\theta_i = \theta''_i$ if $r + 1 \leq i \leq n$; also $r_i = r'_i$ if $1 \leq i \leq m - 1$ and $r_m = s$. Now B'' is integral over A'' implies that $B''[\theta'_1, \dots, \theta'_r]$ is integral over $A''[\theta'_1, \dots, \theta'_r]$. Also, B is integral over $k[\theta'_1, \dots, \theta'_n] = B''[\theta'_1, \dots, \theta'_r]$, and hence over $A''[\theta'_1, \dots, \theta'_r] = k[\theta_1, \dots, \theta_n]$. Consequently, $\text{tr.deg.}_k k[\theta_1, \dots, \theta_n] = \text{tr.deg.}_k B = n$, and hence $\theta_1, \dots, \theta_n$ are algebraically independent over k . Checking that $J_i \cap k[\theta_1, \dots, \theta_n] = (\theta_1, \dots, \theta_{r_i})$ is an easy exercise. \square

Corollary 3.14. *If B is domain and a f.g. k -algebra, then $\dim B = \text{tr.deg.}_k B$. Consequently, $\dim B[X_1, \dots, X_n] = \dim B + n$.*

Proof. Apply Proposition 3.13 for the singleton chain (0), and use Corollary 3.7 and Corollary 3.12. \square

Corollary 3.15. *If B is a domain and a f.g. algebra over a field k , and P is a prime ideal of B , then $\dim B = \text{ht } P + \dim B/P$.*

Proof. Apply Proposition 3.13 for the singleton chain P , and use Corollary 3.7 and Corollary 3.9. \square

Example 3.16. If B is not a domain then result of 3.15 is not necessarily true. For example, let $B = k[X, Y, Z]/(XY, XZ) = k[x, y, z]$ and $\mathfrak{p} = (y, z)$. Then $\dim B = 2$, whereas $\text{ht } \mathfrak{p} = 0$ and $\dim B/\mathfrak{p} = 1$.

Definition 3.17. A ring A is said to be *catenary* if for any two prime ideals $\mathfrak{p} \subset \mathfrak{q}$ of A , all maximal chains of prime ideals between \mathfrak{p} and \mathfrak{q} have the same length. A ring A is said to be *universally catenary* if every finitely generated ring over A is catenary.

Corollary 3.18. *Every affine k -algebra over a field k is universally catenary.*

Proof. Since a finitely generated rings over an affine k -algebra is also an affine k -algebra, it suffices to show that affine k -algebras are catenary. Let B be an affine k -algebra and $\mathfrak{p} \subset \mathfrak{q}$ be a chain of prime ideals of B . Passing to B/\mathfrak{p} , we can and will assume that B is a domain and $\mathfrak{p} = (0)$. Let $(0) = \mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \dots \subset \mathfrak{q}_m = \mathfrak{q}$ be a maximal chain of distinct prime ideals of B between

(0) and \mathfrak{q} . By Noether's Normalization Lemma, there is a corresponding chain $(0) \subset \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m$ of prime ideals of the polynomial ring $A := k[\theta_1, \dots, \theta_d]$ with $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ and $\mathfrak{p}_i := (\theta_1, \dots, \theta_{r_i})$ for $0 \leq i \leq m$ and some nonnegative integers $r_0 \leq r_1 \leq \cdots \leq r_m$. Now, by Corollary 3.9 and Corollary 3.12, we have $r_{i+1} = \text{ht } \mathfrak{p}_{i+1} = \text{ht } \mathfrak{q}_{i+1} > \text{ht } \mathfrak{q}_i = \text{ht } \mathfrak{p}_i = r_i$ for $0 \leq i < m$. Moreover, if $r_{i+1} > r_i + 1$ for some i , then using the Going Down Theorem (Proposition 3.8) and Corollary 3.9, we can find a prime ideal \mathfrak{q}' of B such that $\mathfrak{q}_i \subset \mathfrak{q}' \subset \mathfrak{q}_{i+1}$. This contradicts the maximality of $(0) = \mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m = \mathfrak{q}$. Thus, $r_{i+1} = r_i + 1$ for $0 \leq i < m$. Further, it is easily seen that $r_0 = 0$, and so $r_m = m$. It follows that $\text{ht } \mathfrak{q} = m$. This completes the proof. \square

Corollary 3.19 (Hilbert's Nullstellensatz). *Let k be a field. Then we have*

- (i) *If K is a field and a f.g. k -algebra, then K is algebraic over k .*
- (ii) *If k is algebraically closed, and \mathfrak{m} is a maximal ideal of $k[X_1, \dots, X_n]$, then there exist $\alpha_1, \dots, \alpha_n \in k$ such that $\mathfrak{m} = (X_1 - \alpha_1, \dots, X_n - \alpha_n)$.*
- (iii) *If k is algebraically closed, and I is a nonunit ideal of $k[X_1, \dots, X_n]$, then there exists $(\alpha_1, \dots, \alpha_n) \in k^n$ such that $f(\alpha_1, \dots, \alpha_n) = 0$, for each $f \in I$.*

Proof. (i) By Proposition 3.13, K is integral over $A := k[\theta_1, \dots, \theta_d]$, and, by Proposition 3.3, A is a field. Since A is isomorphic to a polynomial ring in d variables, it follows that $d = 0$, and so K is algebraic over k .

(ii) Let $K = k[X_1, \dots, X_n]/\mathfrak{m}$. Then by (i) and the assumption on k , we find that $K \simeq k$. Let $\alpha_1, \dots, \alpha_n$ be the unique elements of k corresponding to the images of X_1, \dots, X_n in K . Now $(X_1 - \alpha_1, \dots, X_n - \alpha_n) \subseteq \mathfrak{m}$, and the former is clearly a maximal ideal of $k[X_1, \dots, X_n]$.

(iii) If I is a nonunit ideal of $k[X_1, \dots, X_n]$, then $I \subseteq \mathfrak{m}$, for some maximal ideal \mathfrak{m} of $k[X_1, \dots, X_n]$. Now apply (ii). \square

3.3 Finiteness of Integral Closure

The aim of this section is to prove that if A is a domain and an affine k -algebra, then the integral closure of A in a finite extension L of its quotient field K is a finite A -module. The case when L/K is separable is relatively easy. This, together with Noether Normalization yields the general result.

First, let us recall a few basic facts from field theory. Let L/K be a field extension, that is, L is a field and K is a subfield of L . We say that L/K is *finite* if L is finite-dimensional as a vector space over K . The vector space dimension $\dim_K L$ is denoted by $[L : K]$ and called the *degree* of L over K . If L/K is finite and $\alpha \in L$, then the trace of the K -linear map $L \rightarrow L$ given by $x \mapsto \alpha x$ is called the *trace* of α and is denoted by $\text{Tr}_{L/K}(\alpha)$ or simply,

by $\text{Tr}(\alpha)$. It is easy to see that $\text{Tr}_{L/K}$ is a K -linear map of L into K , and $\text{Tr}(a) = [L : K]a$ for all $a \in K$.

A finite field extension L/K is said to be *algebraic* if every $\alpha \in L$ satisfies a nonzero polynomial in $K[X]$. Such a polynomial is unique if we require it to be monic and irreducible; in that case it is called the *minimal polynomial* of α over K and denoted by $\text{Irr}(\alpha, L/K)$. An algebraic extension L/K is said to be *separable* if $\text{Irr}(\alpha, L/K)$ has distinct roots for every $\alpha \in L$. Now suppose L/K is finite separable of degree $n := [L : K]$ and $\alpha \in L$. The degree, say d , of $\text{Irr}(\alpha, L/K)$ divides n , and the distinct roots of $\text{Irr}(\alpha, L/K)$, each repeated n/d times, are called the *conjugates* of α w.r.t L/K . Thus, $\alpha \in L$ has exactly n conjugates w.r.t. L/K . The sum of these n conjugates is precisely the trace of α . Equivalently, $\text{Tr}_{L/K}(\alpha)$ is the sum of all $\sigma(\alpha)$ as σ varies over all K -homomorphisms of L into an algebraic closure of K containing L .

If L/K is a finite extension of degree n and $\{\alpha_1, \dots, \alpha_n\}$ is any K -basis of L , then the determinant of the $n \times n$ matrix $(\text{Tr}_{L/K}(\alpha_i \alpha_j))$ is called the *discriminant* of L/K w.r.t. $\{\alpha_1, \dots, \alpha_n\}$. The vanishing of this is independent of the choice of a K -basis. In case L/K is separable, L has a K -basis of the form $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ for some $\alpha \in L$. With respect to this basis, the discriminant is a Vandermonde determinant and hence nonzero. Consequently, the bilinear form $L \times L \rightarrow K$ given by $(x, y) \mapsto \text{Tr}_{L/K}(xy)$ is nondegenerate.

Lemma 3.20. *Let A be a domain, K be the quotient field of A and L be a field extension of K . Then we have the following.*

- (i) *If $\alpha \in L$ is algebraic over K , then there exists $c \in A$ such that $c \neq 0$ and $c\alpha$ is integral over A . Consequently, if $\{\alpha_1, \dots, \alpha_n\}$ is a K -basis of L , then there exists $d \in A$ such that $d \neq 0$ and $\{d\alpha_1, \dots, d\alpha_n\}$ is a K -basis of L whose elements are integral over A .*
- (ii) *If A is normal, L/K is finite separable and $\alpha \in L$ is integral over A , then $\text{Tr}_{L/K}(\alpha) \in A$.*

Proof. (i) If α satisfies the monic polynomial $X^n + a_1 X^{n-1} + \dots + a_n \in K[X]$, then we can find a common denominator $c \in A$ such that $c \neq 0$ and $a_i = c_i/c$ for some $c_i \in A$. Multiplying the above polynomial by c^n , we get a monic polynomial in $A[X]$ satisfied by $c\alpha$.

(ii) If $\alpha \in L$ is integral over A , then so is each of its conjugate. Hence $\text{Tr}(\alpha)$ is integral over A . Since $\text{Tr}(\alpha) \in K$ and A is normal, it follows that $\text{Tr}(\alpha) \in A$. \square

We are now ready to prove the Finiteness Theorem in the separable case.

Proposition 3.21. *Let A be a normal domain and K be its quotient field. Let L/K be a finite separable extension of degree n and B be the integral closure of A in L .*

Then B is contained in a free A -module generated by n elements. In particular, if A is also noetherian, then B is a finite A -module and a noetherian ring.

Proof. Using part (i) of Lemma 3.20, we can find a K -basis $\{\alpha_1, \dots, \alpha_n\}$ of L , which is contained in B . Let $\{\beta_1, \dots, \beta_n\}$ be a dual basis, w.r.t. the non-degenerate bilinear form $\text{Tr}_{L/K}(xy)$, corresponding to $\{\alpha_1, \dots, \alpha_n\}$. Given any $x \in B$, we can write $x = \sum_j b_j \beta_j$ for some $b_j \in K$. Now $\text{Tr}(\alpha_i x) = \sum_j b_j \text{Tr}(\alpha_i \beta_j) = b_i$. Moreover, since $\alpha_i x$ is integral over A , it follows from Lemma 3.20 that $b_i \in A$. Thus B is contained in the A -module generated by β_1, \dots, β_n . This module is free since β_1, \dots, β_n are linearly independent over K . \square

When A is a PID, the conclusion of Proposition 3.21 can be sharpened. using the following lemma.

Lemma 3.22. *Let A be a PID, M be an A -module generated by n elements x_1, \dots, x_n and let N be a submodule of M . Then N is generated by at most n elements. In fact, we can find $a_{ij} \in A$ for $1 \leq i \leq j \leq n$ such that*

$$N = Ay_1 + \dots + Ay_n \quad \text{where} \quad y_i = \sum_{j \geq i} a_{ij} x_j \quad \text{for } 1 \leq i \leq n. \quad (3.1)$$

Proof. We have $M = Ax_1 + \dots + Ax_n$. Let us use induct on n . Define

$$I := \{a \in A : ax_1 + a_2x_2 + \dots + a_nx_n \in N \text{ for some } a_2, \dots, a_n \in A\}.$$

Then I is an ideal of A and thus $I = (a_{11})$ for some $a_{11} \in A$. Also, there exist $a_{12}, \dots, a_{1n} \in A$ such that $y_1 \in N$ where $y_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n$. If $n = 1$, we have $N = Ix_1 = Ay_1$, where $y_1 = a_{11}x_1$ and thus the result is proved in this case. If $n > 1$, then let $M_1 = Ax_2 + \dots + Ax_n$ and $N_1 = N \cap M_1$. By induction hypothesis, we can find $a_{ij} \in A$ for $2 \leq i \leq j \leq n$ such that $N_1 = Ay_2 + \dots + Ay_n$ where $y_i = \sum_{j \geq i} a_{ij} x_j$ for

$$N_1 = Ay_2 + \dots + Ay_n \quad \text{where} \quad y_i = \sum_{j \geq i} a_{ij} x_j \quad \text{for } 2 \leq i \leq n.$$

Now if $y \in N$, then $y = a_1x_1 + a_2x_2 + \dots + a_nx_n$ for some $a_1, \dots, a_n \in A$. Moreover $a_1 \in I$ and thus $a_1 = \lambda_1 a_{11}$ for some $\lambda_1 \in A$. Hence $y - \lambda_1 y_1 \in N_1$ and so $y - \lambda_1 y_1 = \lambda_2 y_2 + \dots + \lambda_n y_n$ for some $\lambda_2, \dots, \lambda_n \in A$. It follows that $N = Ay_1 + \dots + Ay_n$ and $y_i = \sum_{j \geq i} a_{ij} x_j$, as desired. \square

Corollary 3.23. *Let A, K, L, n, B be as in the Finiteness Theorem. Assume that A is a PID. Then B is a free A -module of rank n , i.e., there exist n linearly independent elements $y_1, \dots, y_n \in B$ such that $B = Ay_1 + \dots + Ay_n$.*

Proof. Follows from Finiteness Theorem 3.21 and Lemma 3.22 (i). \square

The above Corollary applied in the particular case of $A = \mathbb{Z}$, shows that the ring of integers of a number field always has a \mathbb{Z} -basis. Such a basis is called an *integral basis* of that ring or of the corresponding number field.

Now let us prove the general case of the Finiteness Theorem. Again it may be useful to recall some pertinent facts from field theory.

A finite field extension L/K is said to be *normal* if $\text{Irr}(\alpha, K)$ has all its roots in L for every $\alpha \in L$. If L/K is a finite extension, then we can find a normal extension L^*/K such that L^* contains L and no proper subfield of L^* containing L is normal over K . Such an extension L^* is necessarily finite over K and is unique upto a K -isomorphism; it is called the *normal closure* of L over K . Given any field extension L/K , the set of all K -automorphisms of L is a group, called the *Galois group* of L/K and denoted by $\text{Gal}(L/K)$. From Galois theory, we know that if H is a finite subgroup of $\text{Gal}(L/K)$ and $L^H := \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$ is the *fixed field* of H in L , then L/L^H is a finite, separable and normal extension with $\text{Gal}(L/L^H) = H$. If L/K is a finite normal extension and $H = \text{Gal}(L/K)$, then every element of L^H is *purely inseparable* over K , i.e, every $\alpha \in L^H$ satisfies $\alpha^q \in K$ where q is some power of the characteristic of K . In other words, L^H/K is a *purely inseparable* extension.

Theorem 3.24. *Let A be a domain and an affine k -algebra, and K be its quotient field. Let L be a finite extension of K and B be the integral closure of A in L . Then B is a finite A -module, and hence an affine k -algebra.*

Proof. By Noether's Normalization Lemma, A is integral over a polynomial ring $A_0 = k[X_1, \dots, X_d]$. Consequently, B is integral over A_0 and hence B is the integral closure of A in L . Moreover, if B is a finite A_0 -module, then clearly, it is a finite A -module. Thus, we may assume without loss of generality that $A = k[X_1, \dots, X_d]$. In particular, A is a noetherian normal domain. Now, let L^* be the normal closure of L over K and B^* be the integral closure of A in L^* . If B^* is a finite A -module, then so is B because A is noetherian. Thus we may also assume without loss of generality that L/K is a finite normal extension.

Let L' be the fixed field of $\text{Gal}(L/K)$ in L . Then L/L' is finite, separable and normal, whereas L'/L is finite and purely inseparable. If $L' = K$, then the desired result follows from Proposition 3.21. If not, then the characteristic, say p , of K is nonzero. Moreover, $L' = K(f_1^{1/q}, \dots, f_r^{1/q})$ for some $f_1, \dots, f_r \in K$, where q is a some power of p . Let k' be the finite extension of k obtained by adjoining to k the q th roots of the coefficients of the (numerators and denominators of the) rational functions f_1, \dots, f_r . Then L' is a subfield of $L'' := k'(X_1^{1/q}, \dots, X_d^{1/q})$. The ring $B'' := k'[X_1^{1/q}, \dots, X_d^{1/q}]$ is integral over $A = k[X_1, \dots, X_d]$ and is a f.g. A -algebra. Hence B'' is a finite A -module. Also, B'' is normal (being isomorphic to a polynomial ring) and therefore it is the integral closure of A in L'' . In particular B' is a subring

of B'' , and hence B' is a finite A -module. Finally, since B is also the integral closure of B' in L , in view of Proposition 3.21, we see that B is a finite A -module. \square

Remark 3.25. Even the seemingly simplest case $L = K$ of the above theorem is not obvious. In fact, the general case can be easily reduced to this case. In general, the integral closure of a noetherian domain in its quotient field need not be noetherian. A theorem of Krull and Akizuki says that for one dimensional noetherian domains A , the integral closure of A , and more generally, its subrings containing A , are noetherian. In dimension two, Mori and Nagata prove that the integral closure of a noetherian domain A is noetherian but it may have subrings containing A that are not noetherian. In dimension three, there are counterexamples to show that the integral closure of a noetherian domain need not be noetherian. However, the integral closure of a noetherian domain in a finite extension of its quotient field is always a *Krull ring*. A useful generalisation of affine k -algebras is to an important class of rings known as *Nagata rings* or *pseudo-geometric rings* or (noetherian) *universally Japanese rings*.¹ For more on these matters, see Matsumura [M1] or Nagata [Na].

Exercises

1. If a rational number satisfies a monic polynomial in $\mathbb{Z}[X]$, then show that it must be an integer. Deduce that \mathbb{Z} is a normal domain. More generally, show that any UFD is a normal domain.
2. If B/A is an integral extension of rings, then show that B/J is integral over $A/J \cap A$ for every ideal J of A . Further, if S is a multiplicatively closed subset of A , then show that $S^{-1}B$ is an integral extension of $S^{-1}A$.
3. Consider the subring $A = \mathbb{Z}[\sqrt{5}]$ of \mathbb{C} and let $\alpha = (1 + \sqrt{5})/2$. Show that α is in the quotient field of A and α is integral over A , but $\alpha \notin A$.
4. If A is a normal domain and S is a multiplicatively closed subset of A such that $0 \notin S$, then show that $S^{-1}A$ is a normal domain.
5. Show that if A is a domain, then A is normal if and only if $A[X]$ is normal.
6. If A is a domain, then show that A is integrally closed in the polynomial ring $A[X]$. What if A is not a domain?

¹A domain A is called a *Krull ring* if $A_{\mathfrak{p}}$ is a PID for all $\mathfrak{p} \in \text{Spec } A$ with $\text{ht } \mathfrak{p} = 1$ and every nonzero principal ideal of A is intersection of primary ideals belonging to height 1 primes. A noetherian ring A is called a *Nagata ring* if for every $\mathfrak{p} \in \text{Spec } A$, the integral closure of A/\mathfrak{p} in a finite extension of its quotient field is a finite A/\mathfrak{p} -module.

7. Let $A = k[X, Y]/(Y^2 - X^2 - X^3)$ and write $A = k[x, y]$ where x, y denote the images of X, Y in A , respectively. Show that A is a domain and the element y/x is in the quotient field of A and it is integral over A , but $y/x \notin A$. Can you determine the integral closure of A in its quotient field?
8. Let $A = k[X, Y]/(Y^2 - X^3)$. Show that A is a domain, but A is not normal. Further show that A is isomorphic to the subring $k[t^2, t^3]$ of the polynomial ring $k[t]$, and that the integral closure of A in its quotient field is isomorphic to $k[t]$.
9. Let A be a domain and consider the localizations $A_{\mathfrak{m}}$ of A at $\mathfrak{m} \in \text{Max}(A)$ as subrings of a fixed quotient field K of A . Show that if $A_{\mathfrak{m}}$ is normal for each $\mathfrak{m} \in \text{Max}(A)$, then so is A .
10. Prove Corollaries 3.4, 3.7 and 3.9 using the propositions preceding them.
11. Let $\{A_{\alpha} : \alpha \in \Lambda\}$ be a family of subrings of a field K such that each A_{α} is a normal domain. Prove that the intersection of the A_{α} , as α varies over Λ , is normal.
12. If A is a normal domain, K is its quotient field, and x is an element of a field extension L of K such that x is integral over A , then show that the minimal polynomial of x over K has its coefficients in A .
13. Let k be an infinite field and $f \in k[X_1, \dots, X_n]$ be a nonzero polynomial. Prove that there exist $a_1, \dots, a_n \in k$ such that $f(a_1, \dots, a_n) \neq 0$. Further, show that if $n \geq 1$ and f is nonconstant and homogeneous, then there exist $c_2, \dots, c_n \in k$ such that $f(1, c_2, \dots, c_n) \neq 0$.
14. Suppose k is an algebraically closed field and $f, g \in k[X, Y]$. Determine a primary decomposition of $(f, g)k[X, Y]$. Show that if f and g are not divisible by any nonconstant polynomial in $k[X, Y]$, then they have only finitely many common zeros in k^2 .
15. If A is an affine k -algebra, then show that the Jacobson radical of A (which, by definition, is the intersection of all maximal ideals of A) coincides with the nilradical $\sqrt{(0)}$ of A .
16. If in Lemma 3.22, we further assume that $A = \mathbb{Z}$ and that N contains a \mathbb{Q} -basis of K , then show that the conclusion can be refined as follows. *The quotient module M/N is a finite set and we can choose $a_{ij} \in A$, for $1 \leq i \leq j \leq n$, satisfying (3.1) and with the additional property*

$$a_{ii} > 0 \text{ for } 1 \leq i \leq n \quad \text{and} \quad |M/N| = a_{11}a_{22} \cdots a_{nn} = \det(a_{ij}) \quad (3.2)$$

where, by convention, $a_{ij} = 0$ for $j < i$.

Chapter 4

Dedekind Domains

In the investigation of Fermat's last theorem and higher reciprocity laws, mathematicians in the 19th century were led to ask if the unique factorization property enjoyed by the integers also holds in the ring of integers in an algebraic number field, especially in the ring of cyclotomic integers. In 1844, E. Kummer showed that this does not hold, in general. About three years later, he showed that the unique factorization in such rings, or at least in rings of cyclotomic integers, is possible if numbers are replaced by the so called "ideal numbers". Kummer's work was simplified and furthered by R. Dedekind¹. The concept of an ideal in a ring was thus born. In effect, Dedekind showed that the ring of integers of an algebraic number field has the following property:

Every nonzero ideal in this ring factors uniquely as a product of prime ideals.

Integral domains with this property are now known as *Dedekind domains* (or also *Dedekind rings*)². In a famous paper³, Emmy Noether gave a set

¹Dedekind published his ideas as a supplement to Dirichlet's lectures on Number Theory, which were first published in 1863. Dedekind's supplements occur in the third and fourth editions, published in 1879 and 1894, of Dirichlet's *Vorlesungen über Zahlentheorie*. Another approach towards understanding and extending the ideas of Kummer was developed by L. Kronecker, whose work was apparently completed in 1859 but was not published until 1882. For more historical details, see the article "The Genesis of Ideal Theory" by H. Edwards, published in *Archives for History of Exact Sciences*, Vol. 23 (1980), and the articles by P. Ribenboim and H. Edwards in "Number Theory Related to Fermat's Last Theorem", Birkhäuser, 1982.

²The term *Dedekind domains* was coined by I.S. Cohen [*Duke Math. J.* **17** (1950), pp. 27–42]. In fact, Cohen defines a Dedekind domain to be an integral domain in which every nonzero proper ideals factors as a product of prime ideals, and he notes that the uniqueness of factorization is automatic, thanks to Matsusita [*Japan J. Math.* **19** (1944), pp. 97–110].

³*Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, *Math. Ann.* **96** (1927), pp. 26–61. The *Aufbau* paper followed another famous paper *Idealtheorie in Ringbereichen* [*Math. Ann.* **83** (1921), pp. 24–66] in which rings with ascending chain condition on ideals are studied; the term *noetherian rings* for such rings may have been coined by Chevalley [*Ann. Math.* **44** (1943), pp. 690–708]. Emmy Noether had a great appreciation of Dedekind's work and her favorite expression to students was *Alles steht schon bei Dedekind!*

of abstract axioms for rings whose ideal theory agrees with that of ring of integers of an algebraic number field. This leads to a characterization of Dedekind domains. In the next section, we will take this abstract characterization as the definition of a Dedekind domain, and then prove properties such as the unique factorization of ideals as a consequence. In the subsequent sections, we study the phenomenon of ramification and discuss a number of basic results concerning it.

4.1 Dedekind Domains

An integral domain A is called a *Dedekind domain* if A is noetherian, normal and every nonzero prime ideal in A is maximal. Note that the last condition is equivalent to saying that $\dim A \leq 1$, or in other words, either A is a field or A is one dimensional.

Example 4.1. Any PID is a Dedekind domain (check!). In particular, \mathbb{Z} and the polynomial ring $k[X]$ over a field k are Dedekind domains.

Example 4.2. The ring $\mathbb{Z}[\sqrt{-5}]$, which is the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{-5})$ is a Dedekind domain. Indeed, this ring is noetherian being the quotient of a polynomial ring over \mathbb{Z} , it is normal being the ring of integers of a number field, and it is one dimensional, being an integral extension of \mathbb{Z} . However, $\mathbb{Z}[\sqrt{-5}]$ is not a PID because, for instance, the ideal $P = (2, 1 + \sqrt{-5})$ is not principal. Indeed if P were generated by a single element $a + b\sqrt{-5}$, then a would have to be an even integer which divides 1, and this is impossible. As it turns out, the fact that the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$ is not a PID is related to failure of unique factorization in $\mathbb{Z}[\sqrt{-5}]$, which is illustrated by the two distinct factorizations 2×3 and $(1 + \sqrt{-5})(1 - \sqrt{-5})$ of the number 6. Note, however, that if we pass to ideals and consider the principal ideal (6) generated by 6 in $\mathbb{Z}[\sqrt{-5}]$, then there is no problem because

$$(6) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

and it can be seen that the ideals on the right are distinct prime ideals and the above factorization of (6) into prime ideals is unique up to rearrangement of factors.

Many more examples of Dedekind domains can be generated from the following basic result.

Theorem 4.3 (Extension Theorem). *Let A be a Dedekind domain, K its quotient field, L a finite separable extension of K , and B the integral closure of A in L . Then B is a Dedekind domain.*

Proof. By Finiteness Theorem 3.21, B is noetherian. It is obvious that A is normal. Lastly, by Corollary 3.7 we see that $\dim B = \dim A \leq 1$. \square

Since \mathbb{Z} is a Dedekind domain, we obtain as an immediate consequence the following corollary.

Corollary 4.4. *If K is a number field, then \mathcal{O}_K , the ring of integers of K , is a Dedekind domain.*

We now proceed to prove a number of basic properties of Dedekind domains. In particular, we shall establish the fact about unique factorization of ideals as products of prime ideals, which was alluded to in the beginning of this section.

Definition 4.5. Let A be a domain and K be its quotient field. By a *fractionary ideal* of A we mean an A -submodule J of K such that $dJ \subseteq A$ for some $d \in A, d \neq 0$.

Note that a finitely generated A -submodule of K is a fractionary ideal of A . Conversely, if A is noetherian, then every fractionary ideal of A is finitely generated.

To distinguish from fractionary ideals, the (usual) ideals of A are sometimes called the *integral ideals* of A . Products of fractionary ideals is defined in the same way as the product of integral ideals, and w.r.t. this product, the set

$$\mathcal{F}_A = \{J : J \text{ a fractionary ideal of } A \text{ and } J \neq (0)\}$$

of nonzero fractionary ideals of A is a commutative monoid with A as its identity element. Note that \mathcal{F}_A contains the subset of nonzero principal fractionary ideals, viz.,

$$\mathcal{P}_A = \{Ax : x \in K, \text{ and } x \neq (0)\}$$

and this subset is, in fact, a group. In case A is a PID, we see easily (from Corollary 3.23, for example) that $\mathcal{F}_A = \mathcal{P}_A$, and in this case \mathcal{F}_A is a group. We will soon show that more generally, if A is any Dedekind domain, then \mathcal{F}_A is a group.

Lemma 4.6. *Every nonzero ideal of a noetherian ring A contains a finite product of nonzero prime ideals of A .*

Proof. Assume the contrary. Then the family of nonzero nonunit ideals of A not containing a finite product of nonzero prime ideals of A is nonempty. Let I be a maximal element of this family. Then $I \neq A$ and I can not be prime. Hence there exist $a, b \in A \setminus I$ such that $ab \in I$. Now $I + Aa$ and $I + Ab$ are ideals strictly larger than I , and $I \supseteq (I + Aa)(I + Ab)$. In particular, $I + Aa$ and $I + Ab$ are nonzero nonunit ideals. So by the maximality of I , both $I + Aa$ and $I + Ab$ contain a finite product of nonzero prime ideals, and hence so does I . This is a contradiction. \square

Lemma 4.7. *Let A be a noetherian normal domain and K be its quotient field. If $x \in K$ and I is a nonzero ideal of A such that $xI \subseteq I$, then $x \in A$.*

Proof. Since $xI \subseteq I$, we have $x^n I \subseteq I$ for $n \geq 1$. Thus if we let $J = A[x]$, then $J I \subseteq I$. In particular, if $d \in I$, $d \neq 0$, then $dJ \subseteq A$. So J is a fractionary ideal of A and since A is noetherian, $J = A[x]$ is a f.g. A -module. Therefore, x is integral over A and since A is normal, $x \in A$. \square

Lemma 4.8. *Let A be a Dedekind domain and K be its quotient field. If P is any nonzero prime ideal of A , then*

$$P' = (A :_K P) = \{x \in K : xP \subseteq A\}$$

is a fractionary ideal of A , which strictly contains A . Moreover, $PP' = A = P'P$. In particular, P is invertible and $P^{-1} = P'$.

Proof. Clearly, P' is an A -module. Also, $dP' \subseteq A$ for any $d \in P$, $d \neq 0$. Thus P' is a fractional ideal of A . It is clear that $P' \supseteq A$. To show that $P' \neq A$, choose any $d \in P$, $d \neq 0$. By Lemma 4.6, we can find nonzero prime ideals P_1, \dots, P_n of A such that $(d) \supseteq P_1 \cdots P_n$. Suppose n is the least positive integer with this property. Now, $P_1 \cdots P_n \subseteq P$, and since P is prime, we have $P_i \subseteq P$ for some i . But A is a 1-dimensional ring, and so $P_i = P$. Define $I = P_1 \cdots P_{i-1} P_{i+1} \cdots P_n$ (note that $I = A$ if $n = 1$). Then by the minimality of n , $I \not\subseteq (d)$. Let $c \in I$ be such that $c \notin (d)$. Then $cd^{-1} \notin A$. But $PI \subseteq (d)$, and this implies that $P(c) \subseteq (d)$, and so $cd^{-1} \in P'$. Thus $P' \neq A$. Next, to show that $PP' = A$, observe that $P = PA \subseteq PP' \subseteq A$. Thus PP' is an (integral) ideal of A containing the maximal ideal P . Hence $PP' = A$ or $PP' = P$. But if $x \in P' \setminus A$, then by Lemma 4.7, $xP \not\subseteq P$, and hence $PP' \neq P$. It follows that $PP' = A$. \square

Theorem 4.9. *If A is a Dedekind domain, then \mathcal{F}_A , the set of nonzero fractionary ideals of A , forms an abelian group (w.r.t products of fractionary ideals).*

Proof. It suffices to show that every nonzero (integral) ideal of A is invertible, because if $J \in \mathcal{F}_A$, then dJ is a nonzero ideal of A for some $d \in A$, $d \neq 0$, and $(d)(dJ)^{-1}$ is then the inverse of J .

Now if some nonzero ideal of A is not invertible, then we can find a nonzero ideal I of A , which is not invertible and which is maximal with this property. Clearly $I \neq A$ and so there is a nonzero prime ideal P of A such that $I \subseteq P$. By Lemma 4.8, P^{-1} exists and $I = IA \subseteq IP^{-1} \subseteq PP^{-1} = A$. Moreover, if $I = IP^{-1}$, then by Lemma 4.7, $P^{-1} \subseteq A$, which contradicts Lemma 4.8. Thus IP^{-1} is an ideal of A which is strictly larger than I . So by the maximality of I , the ideal IP^{-1} is invertible. But then so is $I = (IP^{-1})P$. This is a contradiction. \square

Theorem 4.10. *Let A be a Dedekind domain. Then every nonzero ideal I of A can be factored as a product of prime ideals, and this factorization is unique up to a rearrangement of the factors. More generally, every nonzero fractional ideal J of A factors as $J = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_h^{e_h}$, for some nonnegative integer h , distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ and nonzero integers e_1, \dots, e_h .⁴ Furthermore, the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ and the exponents e_1, \dots, e_h are uniquely determined by J .*

Proof. Assume for a moment that the assertion for integral ideals is proved. Then for any $J \in \mathcal{F}_A$, there exists $d \in A$, $d \neq 0$ such that dJ is a nonzero ideal of A . Now if $dJ = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ and $(d) = \mathfrak{q}_1 \cdots \mathfrak{q}_l$, where \mathfrak{p}_i and \mathfrak{q}_j are prime ideals then $J = \mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_l^{-1}$. Moreover, if we also have $J = P_1 \cdots P_m Q_1^{-1} \cdots Q_n^{-1}$ for some prime ideals P_i and Q_j (necessarily nonzero but not necessarily distinct), then $\mathfrak{p}_1 \cdots \mathfrak{p}_k Q_1 \cdots Q_n = \mathfrak{q}_1 \cdots \mathfrak{q}_l P_1 \cdots P_m$ and the uniqueness for factorization of integral ideals can be used. This yields the desired results for nonzero fractional ideals.

To prove the existence of factorization of nonzero ideals of A into prime ideals, we can proceed as in the proof of Theorem 4.9. Thus, let I be a nonzero ideal of A which can not be factored as a product of prime ideals and which is maximal with this property. Then $I \neq A$ and if P is a nonzero prime ideal containing I , then IP^{-1} is an ideal of A which is strictly larger than I . So by the maximality of I , the ideal IP^{-1} is a product of prime ideals. Multiplying on the right by P , we find that I is also a product of prime ideals. This is a contradiction.

To prove the uniqueness, let I be any nonzero ideal of A and suppose $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some $r \geq 0$ and prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. We induct on r to show that any other factorization of I as a product of prime ideals differs from $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ by a rearrangement of factors. If $r = 0$, this is evident since a nonempty product of prime ideals will be contained in any one of the factors, which is a proper subset of A . Assume that $r \geq 1$ and the result holds for ideals which are products of $r - 1$ prime ideals. Now if $I = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ for some $s \geq 0$ and prime ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_s$, then it is clear that $s > 0$. Moreover, $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{p}_1$ implies that $\mathfrak{q}_j \subseteq \mathfrak{p}_1$ for some j . But since $I \neq (0)$, each \mathfrak{q}_j is a nonzero prime ideal and hence maximal. Thus $\mathfrak{q}_j = \mathfrak{p}_1$. Multiplying I by \mathfrak{p}_1^{-1} we find that $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_{j-1} \mathfrak{q}_{j+1} \cdots \mathfrak{q}_s$. Thus by induction hypothesis $r - 1 = s - 1$ and $\mathfrak{p}_2, \dots, \mathfrak{p}_r$ are the same as $\mathfrak{q}_1, \dots, \mathfrak{q}_{j-1}, \mathfrak{q}_{j+1}, \dots, \mathfrak{q}_s$ after a rearrangement. This implies that $r = s$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ equal $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ after a rearrangement. \square

Remark 4.11. Either of the following four conditions can be taken as a definition for an integral domain A to be a Dedekind domain.

- (1) A is noetherian, normal and every nonzero prime ideal of A is maximal.

⁴As per usual conventions, $\mathfrak{p}^{-m} = (\mathfrak{p}^{-1})^m$, for any positive integer m . Also, when $h = 0$, a product such as $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_h^{e_h}$ is the empty product and it equals $(1) = A$.

- (2) Nonzero fractional ideals of A form a group with respect to multiplication.
- (3) Every nonzero ideal of A factors uniquely as a product of prime ideals.
- (4) Every nonzero ideal of A factors as a product of prime ideals.

Note that (3) \Rightarrow (4) is obvious and from Theorems 4.9 and 4.10, we have (1) \Rightarrow (2) and (1) \Rightarrow (3). Moreover, if (2) holds, then A is noetherian because if I is a nonzero ideal of A , then $II^{-1} = A$ implies that $\sum_{i=1}^n a_i b_i = 1$ for some $a_i \in I$, $b_i \in I^{-1}$, and consequently, $I = (a_1, \dots, a_n)$. Further, if (2) holds, then as in the proof of Theorem 4.10, the existence of a nonzero ideal of A which can not be factored as a product of prime ideals leads to a contradiction. This shows that (2) \Rightarrow (4). Hence, to prove the equivalence of (1), (2), (3) and (4) it suffice to show that (4) \Rightarrow (1). This can be done but it needs a little bit of work; for details, we refer to [ZS, Ch. V, §6].

We have seen in Example 4.2 that a Dedekind domain need not be a UFD. On the other hand, if a Dedekind domain A is a UFD and P is any nonzero prime ideal of A , then P must contain an irreducible element because otherwise there will be an infinite strictly ascending chain $(a_1) \subset (a_2) \subset \dots$ of principal ideals contained in P , contradicting that A is noetherian. Now if $p \in P$ is irreducible, then (p) is a nonzero prime ideal, and hence maximal. Hence, $P = (p)$. Next, by Theorem 4.10, every nonzero ideal of A is a product of prime ideals and therefore, it is principal. Thus A is a PID. Consequently, if a Dedekind domain A is a UFD, then $\mathcal{F}_A = \mathcal{P}_A$ or in other words, the quotient group $\mathcal{F}_A/\mathcal{P}_A$ is trivial.

Definition 4.12. Let A be a Dedekind domain and K be its quotient field. The *ideal class group* of A , denoted by \mathcal{C}_A , is defined to be the quotient $\mathcal{F}_A/\mathcal{P}_A$. When K is a number field and $A = \mathcal{O}_K$ is its ring of integers, \mathcal{C}_A is often denoted by \mathcal{C}_K and called the *ideal class group* of K . The elements of \mathcal{C}_K are called the *ideal classes* of K .

As remarked earlier, if A is a Dedekind domain, then

$$A \text{ is a UFD} \iff A \text{ is a PID} \iff \mathcal{C}_A \text{ is trivial.}$$

Thus the size of the ideal class group \mathcal{C}_A is a measure of how far A is from being a UFD. In the case when K is a number field and $A = \mathcal{O}_K$, it turns out that \mathcal{C}_K is a finite (abelian) group. The order of this group is denoted by h_K and is called the *class number* of K .

We end this section with a result which gives a sufficient condition for a Dedekind domain to be a PID.

Proposition 4.13. *A local Dedekind domain is a PID. More generally, a Dedekind domain that has only finitely many maximal ideals is a PID.*

Proof. Let A be a Dedekind domain with only finitely many maximal ideals, say, P_1, \dots, P_r . Note that the ideals P_1, \dots, P_r , and more generally, their powers $P_1^{m_1}, \dots, P_r^{m_r}$ are pairwise comaximal. Fix any $i \in \{1, \dots, r\}$. Note that $P_i \neq P_i^2$ (because otherwise $P_i = A$). So we can find $a_i \in P_i \setminus P_i^2$. By Chinese Remainder Theorem [cf. Prop. 1.4], there exists $a \in A$ such that

$$a \equiv a_i \pmod{P_i^2} \quad \text{and} \quad a \equiv 1 \pmod{P_j} \quad \text{for } 1 \leq j \leq r, j \neq i.$$

Now, (a) is a nonzero ideal of A with $(a) \subseteq P_i$, and the factorization of (a) into prime ideals can neither contain P_j for any $j \neq i$ nor can it contain a power of P_i with exponent 2 or more. Hence $(a) = P_i$. Since every nonzero ideal of A is a product of the P_i 's, it must be principal. Thus A is a PID. \square

Remark 4.14. A ring with only finitely many maximal ideals is sometimes called a *semilocal ring*. Thus the above Proposition says that a semilocal Dedekind domain is a PID. In the case of local Dedekind domains, we can, in fact, say more. Namely, a local Dedekind domain is what is called a discrete valuation ring or a DVR. An integral domain A with quotient field K is a *discrete valuation ring* if there exists a map $v : K \setminus \{0\} \rightarrow \mathbb{Z}$ with the properties

$$v(xy) = v(x) + v(y) \quad \text{and} \quad v(x+y) \geq \min\{v(x), v(y)\} \quad \text{for all } x, y \in K \setminus \{0\}$$

and $A = \{x \in K : x = 0 \text{ or } v(x) \geq 0\}$. The map v is called a *valuation* of K and A is called its *valuation ring*. In case A is a local Dedekind domain, A has only one nonzero prime ideal, i say P , and for any nonzero element x of the quotient field of A , we can write $Ax = P^n$ for a unique integer n , and the map given by $x \mapsto n$ is a valuation of K whose valuation ring is A .

4.2 Extensions of Primes

In the ring \mathcal{O}_K of integers of a number field K , a prime p of \mathbb{Z} may not remain a prime. For instance in the ring of integers of $\mathbb{Q}(\sqrt{-1})$, namely, in the ring $\mathbb{Z}[i]$ ⁵, the rational primes 2 and 5 are no longer primes but 3 is. However, by Theorem 4.10, the ideal generated by p in this ring can be uniquely factored as a product of prime ideals. Roughly speaking, the phenomenon of a prime splitting into several primes in an extension, is known as ramification. In this context, there is a beautiful analogue of the formula $\sum_{i=1}^g e_i f_i = n$, which holds when a monic polynomial $f(X)$ of degree n with coefficients in a field F , factors as $f(X) = p_1(X)^{e_1} \cdots p_g(X)^{e_g}$, where $g \geq 0$, $e_i > 0$ and $p_i(X)$ are distinct monic irreducible polynomials in $F[X]$ of degree f_i . We now proceed to give some relevant definitions and prove the $\sum_{i=1}^g e_i f_i = n$ formula in the general setting of Dedekind domains.

⁵Elements of $\mathbb{Z}[i]$ are often called the *Gaussian integers*. These were first studied by C. F. Gauss in his work on biquadratic reciprocity.

In this section, we shall assume that A, K, L, B are as in the Extension Theorem 4.3. We will also let n denote the degree of L/K .

Definition 4.15. Let \mathfrak{p} be a prime ideal of A . A prime ideal P of B is said to *lie over* \mathfrak{p} if $P \cap A = \mathfrak{p}$.

Since B is a Dedekind domain, for any nonzero prime ideal \mathfrak{p} of A , the extension $\mathfrak{p}B$ of \mathfrak{p} to B is a nonzero ideal of B and hence it can be uniquely written as

$$\mathfrak{p}B = \prod_{i=1}^g P_i^{e_i}$$

where P_1, P_2, \dots, P_g are distinct nonzero prime ideals of B and e_i are positive integers.

Definition 4.16. With \mathfrak{p}, P_i , etc. as above, the positive integer e_i is called the *ramification index* of P_i over \mathfrak{p} and is denoted by $e(P_i/\mathfrak{p})$; the field degree $[B/P_i : A/\mathfrak{p}]$ is called the *residue degree* (or the *residue class degree*) of P_i over \mathfrak{p} and is denoted by $f(P_i/\mathfrak{p})$. If $e_i > 1$ for some i , then we say that \mathfrak{p} is *ramified* in B (or in L). Otherwise, it is said to be *unramified*.⁶ The extension L/K is said to be *unramified* if every nonzero prime ideal of A is unramified in L .

We are now ready to prove the main result of this section.

Theorem 4.17. Let A, K, L, B be as above and $n = [L : K]$. Suppose \mathfrak{p} is a nonzero prime ideal of A and we have

$$\mathfrak{p}B = \prod_{i=1}^g P_i^{e_i}$$

where P_1, P_2, \dots, P_g are distinct prime ideals of B and e_1, \dots, e_g are positive integers. Then, upon letting $f_i = [B/P_i : A/\mathfrak{p}]$, we have

$$\sum_{i=1}^g e_i f_i = n.$$

Proof. Let $S = A \setminus \mathfrak{p}$ and $A' = S^{-1}A$ be the localization of A at \mathfrak{p} . Then $B' = S^{-1}B$ is the integral closure of A' in L , and $\mathfrak{p}B' = P_1^{e_1} \dots P_g^{e_g}$, where $P'_i = P_i B'$. Moreover, the primes P'_1, \dots, P'_g are distinct, $A'/\mathfrak{p}A' \simeq A/\mathfrak{p}$ and $B'/P'_i \simeq B/P_i$. Thus we see that in order to prove the equality $\sum e_i f_i = n$, we can replace A, B, \mathfrak{p}, P_i by $A', B', \mathfrak{p}', P'_i$ respectively.

⁶To be accurate, we should define \mathfrak{p} to be *ramified* if $e_i > 1$ for some i or B/P_i is inseparable over A/\mathfrak{p} for some i . However, in number theoretic applications, A/\mathfrak{p} will usually be a finite field and so the question of separability of residue field extensions doesn't arise.

In view of the observations above, we shall assume without loss of generality that A is a local Dedekind domain with \mathfrak{p} as its unique nonzero prime ideal. Then, by the Corollary 3.23, B is a free A -module of rank $n = [L : K]$. Write $B = Ay_1 + \cdots + Ay_n$, where y_1, \dots, y_n are some elements of B . Now for the vector space $B/\mathfrak{p}B$ over A/\mathfrak{p} , we clearly have

$$B/\mathfrak{p}B = \sum_{i=1}^n (A/\mathfrak{p}) \bar{y}_i$$

where \bar{y}_i denotes the residue class of $y_i \bmod \mathfrak{p}B$. Moreover,

$$\sum \bar{a}_i \bar{y}_i = 0 \implies \sum a_i y_i \in \mathfrak{p}B \implies a_i \in \mathfrak{p}$$

where $a_i \in A$ and \bar{a}_i denotes its residue class mod \mathfrak{p} , and the last implication follows since $\{y_1, \dots, y_n\}$ is a free A -basis of B . It follows that $\bar{y}_1, \dots, \bar{y}_n$ are linearly independent over A/\mathfrak{p} , and hence

$$\dim_{A/\mathfrak{p}} B/\mathfrak{p}B = n.$$

Now we count the same dimension by a different method. First, note that since P_1, \dots, P_g are distinct maximal ideals, $P_1^{e_1}, \dots, P_g^{e_g}$ are pairwise comaximal. Since $\mathfrak{p}B = P_1^{e_1} \cdots P_g^{e_g}$, by Chinese Remainder Theorem, we get an isomorphism (of rings as well as of (A/\mathfrak{p}) -vector spaces)

$$B/\mathfrak{p}B \simeq \bigoplus_{i=1}^g B/P_i^{e_i}.$$

Now let us find the dimension of the A/\mathfrak{p} -vector space B/P^e where $P = P_i$ and $e = e_i$ for some i . First, we note that for any $j \geq 1$, $\mathfrak{p}P^j \subseteq P^{j+1}$, and hence P^j/P^{j+1} can be considered as a vector space over A/\mathfrak{p} . We claim that we have an isomorphism

$$B/P^e \simeq B/P \oplus P/P^2 \oplus \cdots \oplus P^{e-1}/P^e.$$

To see this, use induction on e and the fact that for $e > 1$, we clearly have

$$B/P^{e-1} \simeq \frac{B/P^e}{P^{e-1}/P^e}.$$

Next, we note that B is a Dedekind domain having only finitely many prime ideals (in fact, (0) and P_1, \dots, P_g are the only primes of B), and so B must be a PID. Let t be a generator of P , and consider the map

$$B/P \rightarrow P^j/P^{j+1}$$

induced by the multiplication map $x \mapsto t^j x$ of $B \rightarrow P^j$. This map is an A/\mathfrak{p} -homomorphism, and it is clearly bijective. So

$$\dim_{A/\mathfrak{p}}(P^j/P^{j+1}) = \dim_{A/\mathfrak{p}}(B/P) = f(P/\mathfrak{p})$$

and consequently, from the above direct sum representations, we get

$$\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{i=1}^g \dim_{A/\mathfrak{p}}(B/P_i^{e_i}) = \sum_{i=1}^g e_i f_i,$$

which yields the desired identity. This completes the proof. \square

Examples:

1. Consider the quadratic field $K = \mathbb{Q}(i)$, where i denotes a square root of -1 . We know that \mathcal{O}_K is the ring $\mathbb{Z}[i]$ of Gaussian integers. If p is a prime $\equiv 1 \pmod{4}$, then we know (by a classical result of Fermat) that p can be written as a sum of two squares. Thus there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2 = (a + bi)(a - bi)$. It can be seen that $(a + bi)$ and $(a - bi)$ are distinct prime ideals in \mathcal{O}_K . Thus for the prime ideal $p\mathbb{Z}$, we have $g = 2$, $e_1 = e_2 = 1$ and (since $\sum e_i f_i = 2$) $f_1 = f_2 = 1$. On the other hand, it is not difficult to see that a prime $\equiv 3 \pmod{4}$ generates a prime ideal in $\mathbb{Z}[i]$ and so for such a prime, we have $g = 1 = e_1$ and $f_1 = 2$. The case of $p = 2$ is special. We have $2 = (1 + i)(1 - i)$. But $(1 + i)$ and $(1 - i)$ differ only by a unit (namely, $-i$) and thus they generate the same prime ideal. So 2 is a ramified prime and for it, we have $g = 1 = f_1$ and $e_1 = 2$.

The last example illustrates the following definition.

Definition 4.18. A nonzero prime ideal \mathfrak{p} of A is said to be *totally ramified* in L (or in B) if $\mathfrak{p}B = P^n$ for some prime ideal P of B .

Exercises

1. If d is a squarefree positive integer, then determine the units in the ring $\mathbb{Z}[\sqrt{-d}]$.
2. Prove that in the ring $\mathbb{Z}[\sqrt{-5}]$, the two factorizations of 6 given by $(2)(3)$ and $(1 + \sqrt{-5})(1 - \sqrt{-5})$ are indeed distinct, that is, the factors are not associates of each other. Also show that the principal ideal (6) admits the factorization

$$(6) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

and that the ideals on the right are distinct prime ideals.

3. Let $i = \sqrt{-1}$ and consider the ring $\mathbb{Z}[i]$ of Gaussian integers. Prove that $\mathbb{Z}[i]$ is a normal domain. Deduce that $\mathbb{Z}[i]$ is a Dedekind domain. Is $\mathbb{Z}[i]$ a PID? Justify your answer.

4. Let A be a Dedekind domain with quotient field K . If S is any multiplicatively closed subset of A such that $0 \notin S$, then show that the localization $S^{-1}A$ of A at S is a Dedekind domain with quotient field K . Moreover, if L is an algebraic extension of K , then show that the integral closure of $S^{-1}A$ in L is $S^{-1}B$.

$$(i) \quad n_{\mathfrak{p}}(J_1 J_2) = n_{\mathfrak{p}}(J_1) + n_{\mathfrak{p}}(J_2) \text{ and } n_{\mathfrak{p}}(J_1 J_2^{-1}) = n_{\mathfrak{p}}(J_1) - n_{\mathfrak{p}}(J_2).$$

$$(ii) \quad n_{\mathfrak{p}}(J_1 + J_2) = \min \{n_{\mathfrak{p}}(J_1), n_{\mathfrak{p}}(J_2)\}.$$

$$(iii) \quad n_{\mathfrak{p}}(J_1 \cap J_2) = \max \{n_{\mathfrak{p}}(J_1), n_{\mathfrak{p}}(J_2)\}.$$

5. Let A be a Dedekind domain. If P is a nonzero prime ideal of A and e a positive integer, then show that A/P^e is a principal ideal ring. Use this and the Chinese Remainder Theorem to show that if I is any nonzero ideal of A , then A/I is a principal ideal ring. Deduce that every ideal of A can be generated by two elements.

6. With \mathfrak{p} and P_i as above, show that a prime ideal P of B lies over \mathfrak{p} iff $P = P_i$ for some i . Also show that $\mathfrak{p}B \cap A = \mathfrak{p} = P_i^{e_i} \cap A$. Deduce that $B/\mathfrak{p}B$ as well as $B/P_i^{e_i}B$ can be regarded as vector spaces over the field A/\mathfrak{p} . Further show that B/P_i is a field extension of A/\mathfrak{p} whose degree is at most n .

7. Let A, K, L, B and \mathfrak{p} be as above. Suppose L' is a finite separable extension of L and B' is the integral closures of B in L' . Show that B' is the integral closure of A in L' . Further, if P a prime of B lying over \mathfrak{p} and P' a prime of B' lying over P , then show that P' lies over \mathfrak{p} and the following transitivity relations hold:

$$e(P'/\mathfrak{p}) = e(P'/P)e(P/\mathfrak{p}) \quad \text{and} \quad f(P'/\mathfrak{p}) = f(P'/P)f(P/\mathfrak{p}).$$

Appendix A

Primary Decomposition of Modules

We shall discuss here an extension of the notions of associated primes and primary decomposition to the case of modules over (noetherian) rings. The classical case of ideals I in (noetherian) rings A corresponds, in this general set-up, to the case of A -modules A/I ; remembering this may be helpful in understanding some of the concepts and results below.

A.1 Associated Primes of Modules

Taking into consideration the modern viewpoint that the notion of associated primes is more fundamental than primary decomposition, we shall derive in this section basic results about associated primes without mentioning primary submodules or primary decomposition.

Throughout this section, we let A denote a ring and M an A -module. Recall that for any $x \in M$, the *annihilator* of x , denoted by $(0 : x)$, is the ideal $\{a \in A : ax = 0\}$ of A . On the other hand, for any $a \in A$, by $(0 : a)_M$ we denote the submodule $\{x \in M : ax = 0\}$ of M . The *annihilator* of M , denoted by $\text{Ann}(M)$, is the ideal $\{a \in A : aM = 0\}$ of A . An element $a \in A$ is said to be a *zerodivisor* of M if $(0 : a)_M \neq 0$, i.e., if $ax = 0$ for some $x \in M$ with $x \neq 0$. The set of all zerodivisors of M is denoted by $\mathcal{Z}(M)$. An element $a \in A$ is said to be *nilpotent* for M if $a^n M = 0$ for some $n \geq 1$. In other words, a is nilpotent for M iff $a \in \sqrt{\text{Ann}(M)}$.

Definition A.1. A prime ideal \mathfrak{p} of A is called an *associated prime* of M if $\mathfrak{p} = (0 : x)$ for some $x \in M$. The set of all associated primes of M is denoted by $\text{Ass}_A(M)$, or simply by $\text{Ass}(M)$. Minimal elements of $\text{Ass}(M)$ are called the *minimal primes* of M , and the remaining elements of $\text{Ass}(M)$ are called the *embedded primes* of M .

Note that if $\mathfrak{p} = (0 : x) \in \text{Ass}(M)$, then the map $a \mapsto ax$ of $A \rightarrow M$ defines an embedding (i.e., an injective A -module homomorphism) $A/\mathfrak{p} \hookrightarrow M$. Conversely, if for $\mathfrak{p} \in \text{Spec } A$, we have an embedding $A/\mathfrak{p} \hookrightarrow M$, then clearly $\mathfrak{p} \in \text{Ass}(M)$. It may also be noted that if M is isomorphic to some A -module M' , then $\text{Ass}(M) = \text{Ass}(M')$.

Lemma A.2. *Let I be an ideal of A . Any maximal element of the family $\{(0 : y) : y \in M, y \neq 0 \text{ and } (0 : y) \supseteq I\}$ is a prime ideal. In particular, if A is noetherian, then $\text{Ass}(M) \neq \emptyset$ iff $M \neq 0$.*

Proof. Let $\mathcal{F} := \{(0 : y) : y \in M, y \neq 0 \text{ and } (0 : y) \supseteq I\}$ and $(0 : x)$ be a maximal element of \mathcal{F} . Then $(0 : x) \neq A$ since $x \neq 0$. Moreover, if $a, b \in A$ are such that $ab \in (0 : x)$ and $a \notin (0 : x)$, then $ax \neq 0$ and $b \in (0 : ax) \supseteq (0 : x) \supseteq I$. Since $(0 : x)$ is maximal, $(0 : ax) = (0 : x)$. Thus $b \in (0 : x)$. This proves that $(0 : x)$ is a prime ideal. The last assertion follows by taking $I = (0)$. \square

Corollary A.3. *If A is noetherian, then*

$$\mathcal{Z}(M) = \bigcup_{\mathfrak{p} \in \text{Ass}(M)} \mathfrak{p}.$$

Proof. It is obvious that every $\mathfrak{p} \in \text{Ass}(M)$ is in $\mathcal{Z}(M)$. Conversely, if $a \in \mathcal{Z}(M)$, then $ax = 0$ for some $x \in M$ with $x \neq 0$. Upon letting $I := (0 : x)$ in Lemma A.2, we see that $a \in \mathfrak{p}$ for some $\mathfrak{p} \in \text{Ass}(M)$. \square

Lemma A.4. *Given any submodule N of M , we have*

$$\text{Ass}(N) \subseteq \text{Ass}(M) \subseteq \text{Ass}(N) \cup \text{Ass}(M/N).$$

More generally, given any chain $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ submodules of M , we have

$$\text{Ass}(M) \subseteq \bigcup_{i=1}^n \text{Ass}(M_i/M_{i-1}).$$

Proof. The inclusion $\text{Ass}(N) \subseteq \text{Ass}(M)$ is obvious. Let $x \in M$ be such that $(0 : x) \in \text{Ass}(M)$. If $(0 : x) \notin \text{Ass}(N)$, then we claim that $(0 : x) = (0 : \bar{x}) \in \text{Ass}(M/N)$, where \bar{x} denotes the image of x in M/N . To see this, note that $(0 : x) \subseteq (0 : \bar{x})$ and if $a \in A$ is such that $a\bar{x} = 0 \neq ax$, then $ax \in N$ and $a \notin (0 : x)$. Further, since $(0 : x)$ is prime, $b \in (0 : ax) \Leftrightarrow ba \in (0 : x) \Leftrightarrow b \in (0 : x)$. Hence $(0 : x) = (0 : ax) \in \text{Ass}(N)$, which is a contradiction. Thus $\text{Ass}(M) \subseteq \text{Ass}(N) \cup \text{Ass}(M/N)$. The last assertion follows from this by induction on n . \square

The inclusions $\text{Ass}(N) \subseteq \text{Ass}(M)$ and $\text{Ass}(M) \subseteq \text{Ass}(N) \cup \text{Ass}(M/N)$ in the above Lemma can, in general, be proper. This may be seen, for instance, when A is a domain and $M = A$ by taking $N = 0$ or $N =$ a nonzero prime ideal of A .

Corollary A.5. *Given any A -modules M_1, \dots, M_h , we have*

$$M \simeq \bigoplus_{i=1}^h M_i \implies \text{Ass}(M) = \bigcup_{i=1}^h \text{Ass}(M_i).$$

Proof. Follows using induction on h by noting that the case of $h = 2$ is a consequence of the first assertion in Lemma A.4. \square

Having discussed some of the properties of associated primes of quotient modules, we now describe what happens to an associated prime upon localization. Before that, let us recall that if S is multiplicatively closed subset of A , then the map $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ gives a one-to-one correspondence of $\{\mathfrak{p} \in \text{Spec } A : \mathfrak{p} \cap S = \emptyset\}$ onto $\text{Spec } S^{-1}A$.

Lemma A.6. *Suppose A is noetherian and S is a multiplicatively closed subset of A . Then*

$$\text{Ass}_{S^{-1}A}(S^{-1}M) = \{S^{-1}\mathfrak{p} : \mathfrak{p} \in \text{Ass}(M) \text{ and } \mathfrak{p} \cap S = \emptyset\}$$

Proof. If $\mathfrak{p} \in \text{Ass}(M)$ and $S \cap \mathfrak{p} = \emptyset$, then we have an embedding $A/\mathfrak{p} \hookrightarrow M$, which induces an embedding $S^{-1}A/S^{-1}\mathfrak{p} \hookrightarrow S^{-1}M$. And $S^{-1}\mathfrak{p} \in \text{Spec } S^{-1}A$ since $S \cap \mathfrak{p} = \emptyset$. Thus $S^{-1}\mathfrak{p} \in \text{Ass}_{S^{-1}A}(S^{-1}M)$. On the other hand, given any $\mathfrak{p}' \in \text{Ass}_{S^{-1}A}(S^{-1}M)$, we have $\mathfrak{p}' = S^{-1}\mathfrak{p}$ for some $\mathfrak{p} \in \text{Spec } A$ with $\mathfrak{p} \cap S = \emptyset$. Also, $\mathfrak{p}' = (0 : \frac{x}{1})$ for some $x \in M$. Write $\mathfrak{p} = (a_1, \dots, a_n)$. Now $\frac{a_i}{1} \cdot \frac{x}{1} = 0$ in $S^{-1}M$ for $1 \leq i \leq n$, and thus there exists $t \in S$ such that $ta_i x = 0$ for $1 \leq i \leq n$. This implies that $\mathfrak{p} \subseteq (0 : tx)$. Further, if $a \in (0 : tx)$, then $\frac{a}{1} \in (0 : \frac{x}{1}) = S^{-1}\mathfrak{p}$ so that $sa \in \mathfrak{p}$ for some $s \in S$, and hence $a \in \mathfrak{p}$. Thus $\mathfrak{p} \in \text{Ass}(M)$. \square

Note that the above result implies that if $\mathfrak{p} \in \text{Ass}(M)$, then $\mathfrak{p}A_{\mathfrak{p}} \in \text{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$. So, in particular, $M_{\mathfrak{p}} \neq 0$.

Definition A.7. The set $\{\mathfrak{p} \in \text{Spec } A : M_{\mathfrak{p}} \neq 0\}$ is called the *support* of M and is denoted by $\text{Supp}(M)$.

Lemma A.8. $\text{Supp}(M) \subseteq \{\mathfrak{p} \in \text{Spec } A : \mathfrak{p} \supseteq \text{Ann}(M)\}$. Moreover, if M is f. g., then these two sets are equal.

Proof. If $\mathfrak{p} \in \text{Spec } A$ and $M_{\mathfrak{p}} \neq 0$, then there is $x \in M$ such that $\frac{x}{1} \neq 0$ in $M_{\mathfrak{p}}$. Now $a \in \text{Ann}(M) \implies ax = 0 \implies a \notin A \setminus \mathfrak{p} \implies a \in \mathfrak{p}$. Thus $\mathfrak{p} \supseteq \text{Ann}(M)$. Next, suppose M is f. g. and $\mathfrak{p} \in \text{Spec } A$ contains $\text{Ann}(M)$. Write $M = Ax_1 + \dots + Ax_n$. If $M_{\mathfrak{p}} = 0$, we can find $a \in A \setminus \mathfrak{p}$ such that $ax_i = 0$ for $1 \leq i \leq n$. But then $aM = 0$, i.e., $a \in \text{Ann}(M)$, which is a contradiction. \square

Theorem A.9. *Suppose A is noetherian and M is finitely generated. Then there exists a chain $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ of submodules of M such that $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, for some $\mathfrak{p}_i \in \text{Spec } A$ ($1 \leq i \leq n$). Moreover, for any such chain of submodules, we have $\text{Ass}(M) \subseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} \subseteq \text{Supp}(M)$; furthermore, the minimal elements of these three sets coincide.*

Proof. The case of $M = 0$ is trivial. Suppose $M \neq 0$. Then there exists $\mathfrak{p}_1 \in \text{Spec } A$ such that A/\mathfrak{p}_1 is isomorphic to a submodule M_1 of M . If $M_1 \neq M$, we apply the same argument to M/M_1 to find $\mathfrak{p}_2 \in \text{Spec } A$, and a submodule M_2 of M such that $M_2 \supseteq M_1$ and $A/\mathfrak{p}_2 \simeq M_2/M_1$. By (3.1), M has no strictly ascending chain of submodules, and therefore the above process must terminate. This yields the first assertion. Moreover, $\text{Ass}(M_i/M_{i-1}) = \text{Ass}(A/\mathfrak{p}_i) = \{\mathfrak{p}_i\}$, and so by Lemma A.4, we see that $\text{Ass}(M) \subseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. Since localisation commutes with homomorphic images, $(M_i/M_{i-1})_{\mathfrak{p}_i} \simeq A_{\mathfrak{p}_i}/\mathfrak{p}_i A_{\mathfrak{p}_i} \neq 0$. Hence $(M_i)_{\mathfrak{p}_i} \neq 0$. Thus $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} \subseteq \text{Supp}(M)$. Lastly, if $\mathfrak{p} \in \text{Supp}(M)$, then $M_{\mathfrak{p}} \neq 0$ and so $\text{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) \neq \emptyset$. Now Lemma A.6 shows that there exists $\mathfrak{q} \in \text{Ass}(M)$ with $\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset$, i.e., $\mathfrak{q} \subseteq \mathfrak{p}$. This implies the last assertion. \square

Corollary A.10. *If A is noetherian and M is f. g., then $\text{Ass}(M)$ is finite. Furthermore, the minimal primes of M are precisely the minimal elements among the prime ideals of A containing $\text{Ann}(M)$.*

Proof. Follows from Theorem A.9 in view of Lemma A.8. \square

Remark A.11. A chain $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ of submodules of M is sometimes called a *filtration* of M . Using a filtration as in Theorem A.9, it is often possible to reduce questions about modules to questions about integral domains.

A.2 Primary Decomposition of Modules

We continue to let A denote a ring and M an A -module. As in the case of ideals, the primary decomposition of modules into primary submodules will be achieved using the auxiliary notion of irreducible submodules. To compare the notions and results discussed in this section to those in the classical case, you may substitute A for M .

Definition A.12. Let Q be a submodule of M . We say that Q is *primary* if $Q \neq M$ and for any $a \in A$ and $x \in M$, we have

$$ax \in Q \text{ and } x \notin Q \implies a^n M \subseteq Q \text{ for some } n \geq 1.$$

We say that Q is *irreducible* if $Q \neq M$ and for any submodules N_1 and N_2 of M we have

$$Q = N_1 \cap N_2 \implies Q = N_1 \text{ or } Q = N_2.$$

Lemma A.13. *Let Q be a submodule of M . If $Q \neq M$, then*

$$Q \text{ is primary} \iff \mathcal{Z}(M/Q) = \sqrt{\text{Ann}(M/Q)}.$$

Also, if Q is primary, then $\text{Ann}(M/Q)$ is a primary ideal of A .

Proof. The first assertion is an immediate consequence of the definition. To prove the last assertion, suppose Q is primary. Then $\text{Ann}(M/Q) \neq M$ since $Q \neq M$. If $a, b \in A$ are such that $ab \in \text{Ann}(M/Q)$ and $b \notin \text{Ann}(M/Q)$, then we can find $x \in M$ such that $bx \notin Q$. Now, $a(bx) \in Q$ and hence $a^n M \subseteq Q$, i.e., $a^n \in \text{Ann}(M/Q)$ for some $n \geq 1$. Thus, $\text{Ann}(M/Q)$ is a primary ideal of A . \square

If Q is a primary submodule of M and we let $\mathfrak{p} = \sqrt{\text{Ann}(M/Q)}$, then by Lemma A.13, \mathfrak{p} is a prime ideal of A and we say that Q is \mathfrak{p} -primary.

Corollary A.14. *Assume that A is noetherian and M is f. g.. Let Q be a submodule of M . Then*

$$Q \text{ is primary} \iff \text{Ass}(M/Q) \text{ is singleton.}$$

Moreover, given any $\mathfrak{p} \in \text{Spec } A$, we have

$$Q \text{ is } \mathfrak{p}\text{-primary} \iff \text{Ass}(M/Q) = \{\mathfrak{p}\}.$$

Proof. An easy exercise using Corollary A.3, Corollary A.10, Exercise 3 and Lemma A.13. \square

As we shall see in the sequel, the characterization of primary submodules (of f. g. modules over noetherian rings) in Corollary A.14 above is extremely useful. For this reason perhaps, it is sometimes taken as a definition of primary submodules [of arbitrary modules]. At any rate, we may tacitly use the characterizations in Corollary A.14 of primary and \mathfrak{p} -primary submodules in several of the proofs below.

Lemma A.15. *Suppose A is noetherian, M is f. g., and Q_1, \dots, Q_r are \mathfrak{p} -primary submodules of M , where r is a positive integer. Then $Q_1 \cap \dots \cap Q_r$ is also \mathfrak{p} -primary.*

Proof. Clearly, $Q_1 \cap \dots \cap Q_r \neq M$. Moreover, there is a natural injective homomorphism of $M/Q_1 \cap \dots \cap Q_r$ into $M/Q_1 \oplus \dots \oplus M/Q_r$. Therefore, in view of Lemma A.4, Corollary A.5 and Corollary A.14, we see that

$$\emptyset \neq \text{Ass}(M/Q_1 \cap \dots \cap Q_r) \subseteq \text{Ass} \left(\bigoplus_{i=1}^r M/Q_i \right) = \bigcup_{i=1}^r \text{Ass}(M/Q_i) = \{\mathfrak{p}\}.$$

Thus it follows from Corollary A.14 that $Q_1 \cap \dots \cap Q_r$ is \mathfrak{p} -primary. \square

Lemma A.16. *If M is noetherian, then every submodule of M is a finite intersection of irreducible submodules of M .*

Proof. Assume the contrary. Then we can find a maximal element, say Q , among the submodules of M which aren't finite intersections of irreducible submodules of M . Now Q can't be irreducible. Also $Q \neq M$ (because M is the intersection of the empty family of irreducible submodules of M). Hence $Q = N_1 \cap N_2$ for some submodules N_1 and N_2 of M with $N_1 \neq Q$ and $N_2 \neq Q$. By maximality of Q , both N_1 and N_2 are finite intersections of irreducible submodules of M . But then so is Q , which is a contradiction. \square

Lemma A.17. *Suppose A is noetherian, M is f. g., and Q is an irreducible submodule of M . Then Q is primary.*

Proof. Since $Q \neq M$, $\text{Ass}(M/Q) \neq \emptyset$. Suppose $\text{Ass}(M/Q)$ contains two distinct prime ideals $\mathfrak{p}_1 = (0 : \bar{x}_1)$ and $\mathfrak{p}_2 = (0 : \bar{x}_2)$, where \bar{x}_1, \bar{x}_2 denote the images in M/Q of some elements x_1, x_2 of M . Clearly \bar{x}_1 and \bar{x}_2 are nonzero elements of M/Q . We claim that $A\bar{x}_1 \cap A\bar{x}_2 = \{0\}$. Indeed, if $a\bar{x}_1 = b\bar{x}_2$, with $a, b \in A$, is nonzero, then $a \notin (0 : \bar{x}_1)$ and $b \notin (0 : \bar{x}_2)$. Since $(0 : \bar{x}_1)$ is prime, we find that $(0 : \bar{x}_1) = (0 : a\bar{x}_1)$ (check!). Similarly, $(0 : \bar{x}_2) = (0 : b\bar{x}_2)$. This gives $\mathfrak{p}_1 = \mathfrak{p}_2$, which is a contradiction. Now if $y \in (Q + Ax_1) \cap (Q + Ax_2)$, then $y = y_1 + ax_1 = y_2 + bx_2$ for some $y_1, y_2 \in Q$ and $a, b \in A$. But then $a\bar{x}_1 = b\bar{x}_2$ in M/Q and thus $y \in Q$. It follows that $Q = (Q + Ax_1) \cap (Q + Ax_2)$. Also since $\bar{x}_1 \neq 0 \neq \bar{x}_2$, we have $(Q + Ax_1) \neq Q \neq (Q + Ax_2)$. This contradicts the irreducibility of Q . Thus $\text{Ass}(M/Q)$ is singleton so that Q is primary. \square

Lemma A.18. *Suppose A is noetherian, M is f. g., Q is a \mathfrak{p} -primary submodule of M . Then the inverse image of $Q_{\mathfrak{p}}$ under the natural map $M \rightarrow M_{\mathfrak{p}}$ (given by $x \mapsto \frac{x}{1}$) is Q .*

Proof. Suppose $x \in M$ is such that $\frac{x}{1} \in Q_{\mathfrak{p}}$. Then $tx \in Q$ for some $t \in A \setminus \mathfrak{p}$. If $x \notin Q$, then \bar{x} , the image of x in M/Q , is nonzero, and thus $t \in \mathcal{Z}(M/Q)$. Hence from Corollary A.14, we see that $t \in \mathfrak{p}$, which is a contradiction. \square

Remark A.19. Given any $\mathfrak{p} \in \text{Spec } A$ and a submodule Q' of $M_{\mathfrak{p}}$, the inverse image of Q' under the natural map $M \rightarrow M_{\mathfrak{p}}$ is often denoted by $Q' \cap M$. Thus Lemma A.18 can be expressed by saying that if Q is a \mathfrak{p} -primary submodule of M , then $Q_{\mathfrak{p}} \cap M = Q$. Note that we have been tacitly using the fact that if Q is any submodule of M and S is any multiplicatively closed subset of A , then $S^{-1}Q$ can be regarded as a submodule of $S^{-1}M$.

Theorem A.20 (Primary Decomposition Theorem for Modules). *Suppose A is noetherian, M is f. g., and N is any submodule of M . Then we have*

- (i) $N = Q_1 \cap \cdots \cap Q_h$ for some primary submodules Q_1, \dots, Q_h of M .

- (ii) In (i) above, Q_1, \dots, Q_h can be so chosen that $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$ for $1 \leq i \leq h$, and $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are distinct, where $\mathfrak{p}_i := \sqrt{\text{Ann}(M/Q_i)}$.
- (iii) If Q_i and \mathfrak{p}_i are as in (ii) above, then $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are unique; in fact, we have $\{\mathfrak{p}_1, \dots, \mathfrak{p}_h\} = \text{Ass}(M/N)$. Moreover, if \mathfrak{p}_i is minimal among $\mathfrak{p}_1, \dots, \mathfrak{p}_h$, i.e., $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for $j \neq i$, then the corresponding primary submodule Q_i is also unique; in fact, $Q_i = N_{\mathfrak{p}_i} \cap M$.

Proof. Clearly, (i) is a direct consequence of Lemma A.4 and Corollary A.5. Given a decomposition as in (i), we can use Corollary A.3 to reduce it by grouping together the primary submodules having the same associated prime so as to ensure that the associated primes become distinct. Then we can successively remove the primary submodules contained in the intersections of the remaining submodules. This yields (ii). Now let Q_1, \dots, Q_h be as in (ii). Fix some i with $1 \leq i \leq h$. Let $P_i = \bigcap_{j \neq i} Q_j$. Clearly, $N \subset P_i$ and $N \neq P_i$. Thus we have

$$0 \neq \frac{P_i}{N} = \frac{P_i}{P_i \cap Q_i} \simeq \frac{P_i + Q_i}{Q_i} \hookrightarrow M/Q_i,$$

and hence, in view of Lemmas A.2 and A.4, we find that $\emptyset \neq \text{Ass}(P_i/N) \subseteq \text{Ass}(M/Q_i) = \{\mathfrak{p}_i\}$. Thus $\{\mathfrak{p}_i\} = \text{Ass}(P_i/N) \subseteq \text{Ass}(M/N)$. On the other hand, since $N = Q_1 \cap \dots \cap Q_h$, M/N is isomorphic to a submodule of $\bigoplus_{j=1}^h M/Q_j$, and so by Corollary A.5,

$$\text{Ass}(M/N) \subseteq \bigcup_{j=1}^h \text{Ass}(M/Q_j) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}.$$

This proves that $\text{Ass}(M/N) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}$. In particular, $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are unique. Now suppose, without loss of generality, that \mathfrak{p}_1 is minimal among $\mathfrak{p}_1, \dots, \mathfrak{p}_h$. Then for $j > 1$, $\mathfrak{p}_1 \not\supseteq \mathfrak{p}_j$, i.e., $(A \setminus \mathfrak{p}_1) \cap \mathfrak{p}_j \neq \emptyset$, and hence by Lemma A.6, we find that $\text{Ass}_{A_{\mathfrak{p}_1}}((M/Q_j)_{\mathfrak{p}_1}) = \emptyset$; thus by Lemma A.4, $(M/Q_j)_{\mathfrak{p}_1} = 0$, i.e., $M_{\mathfrak{p}_1} = (Q_j)_{\mathfrak{p}_1}$. It follows that $N_{\mathfrak{p}_1} = (Q_1)_{\mathfrak{p}_1} \cap \dots \cap (Q_h)_{\mathfrak{p}_1} = (Q_1)_{\mathfrak{p}_1}$, and, in view of Lemma A.18 and Remark A.19, we obtain that $Q_1 = (Q_1)_{\mathfrak{p}_1} \cap M = N_{\mathfrak{p}_1} \cap M$. This proves (iii). \square

Definition A.21. A decomposition $N = Q_1 \cap \dots \cap Q_h$, as in (i) above is called a *primary decomposition* of N . If Q_1, \dots, Q_h satisfy the conditions in (ii), then it is called an *irredundant (primary) decomposition* of N .

It may be remarked that the examples of primary ideals, primary decomposition of ideals, etc., discussed in the last chapter, constitute examples in this general set-up as well. Thus the pathologies which arise in the case of ideals [see, for instance, Example 2.12] continue to exist for f. g. modules over noetherian rings.

Exercises

1. Let G be a finite abelian group of order n . Suppose $n = p_1^{e_1} \cdots p_h^{e_h}$, where p_1, \dots, p_h are distinct prime numbers and e_1, \dots, e_h are positive integers. Let P_i denote the p_i -Sylow subgroups of G for $1 \leq i \leq h$. Show that as a \mathbb{Z} -module, we have $\text{Ass}(P_i) = p_i\mathbb{Z}$ for each $i = 1, \dots, h$. Deduce that $\text{Ass}(G) = \{p_1\mathbb{Z}, \dots, p_h\mathbb{Z}\}$. More generally, if M is a finitely generated abelian group, then $M = \mathbb{Z}^r \oplus T$ for some $r \geq 0$ and some finite abelian group T . If $r > 0$, then show that $\text{Ass}(M) = \{l_0\mathbb{Z}, l_1\mathbb{Z}, \dots, l_s\mathbb{Z}\}$, where $l_0 := 0$ and l_1, \dots, l_s are the prime numbers dividing the order of T .
2. Show that if A is a noetherian ring, M is a f. g. A -module, and I is an ideal of A consisting only of zerodivisors of M , then there exists some $x \in M$ such that $x \neq 0$ and $Ix = 0$.
3. Show that if A is noetherian ring and M is a f. g. A -module, then

$$\sqrt{\text{Ann}(M)} = \bigcap_{\mathfrak{p} \in \text{Ass}(M)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \text{Supp}(M)} \mathfrak{p} = \bigcap_{\substack{\mathfrak{p} \text{ a minimal} \\ \text{prime of } M}} \mathfrak{p}.$$

4. Prove Corollary A.14.
5. Let G be a finite abelian group of order n . Let the notation be as in the Exercise 1 above. Define $Q_i := P_1 + \cdots + P_{i-1} + P_{i+1} + \cdots + P_h$ for $1 \leq i \leq h$. Show that Q_i is $p_i\mathbb{Z}$ -primary and $(0) = Q_1 \cap \cdots \cap Q_h$ is an irredundant primary decomposition of (0) . Further, show that each of the associated primes of (0) in G is minimal. Deduce that an irredundant primary decomposition of (0) in G is unique. In general, if N is a subgroup of G , i.e., a \mathbb{Z} -submodule of G , and if we let $\Lambda := \{i : 1 \leq i \leq h \text{ and } N + Q_i \neq G\}$, then show that $N = \bigcap_{i \in \Lambda} (N + Q_i)$ is an irredundant primary decomposition of N , and this too is unique.

References

- [Ab] S. S. Abhyankar, *Algebraic Geometry for Scientists and Engineers*, American Math. Society, 1990.
- [AM] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison–Wesley, 1969.
- [Bo] N. Bourbaki, *Commutative Algebra*, Hermann, 1972.
- [BH] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, 1993.
- [Ei] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer–Verlag, 1995.
- [Ka] I. Kaplansky, *Commutative Rings*, The University of Chicago Press, 1974.
- [KS] A. I. Kostrikin and I. R. Shafarevich (Eds), *Algebra I: Basic Notions of Algebra*, Springer–Verlag, 1990.
- [Ku] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1985.
- [M1] H. Matsumura, *Commutative Algebra*, Benjamin, 1970.
- [M2] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1986.
- [Na] M. Nagata, *Local Rings*, Wiley Interscience, New York, 1962.
- [N1] D. G. Northcott, *Ideal Theory*, Cambridge University Press, 1953.
- [N2] D. G. Northcott, *Lessons on Rings, Modules and Multiplicities*, Cambridge University Press, 1968.
- [Sh] R. Y. Sharp, *Steps in Commutative Algebra*, Cambridge University Press, 1990.
- [Ta] D. E. Taylor, From rainbows to rings: a history of the idea of the spectrum, in: *Fourier techniques and applications* (Kensington, 1983), pp. 221–224, Plenum Press, 1985.
- [ZS] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1, Van Nostrand, 1958.