Shandong University | Advanced Modern Algebra

Lecture 12: Some Commutative Algebra

May 12, 2023

Lecturer: Bin Guan

This lecture refers to §12.1, §15.3 and §15.4 in [1]. All the equation numbers without reference labels are from this book.

1 Noetherian rings and Noetherian modules

Recall that we have the following inclusions among classes of commutative rings with identity:

$$\{\text{Fields}\} \subsetneqq \{\text{Euclidean Domains}\} \subsetneqq \{\text{P.I.D.s}\} \subsetneqq \{\text{U.F.D.s}\} \subsetneqq \{\text{Integral Domains}\}$$

with all containments being proper; a polynomial ring $k[x]$ in a variable x over a field k is a Euclidean Domain, and the polynomial ring $k[x_1, \ldots, x_n]$ is a U.F.D.(Unique Factorization Domain). However the latter ring is not a P.I.D.(Principal Ideal Domain) unless $n = 1$.

Actually, ideals in such polynomial rings, although not necessarily principal, are always finitely generated. General rings with this property are given a special name:

Theorem ([1] §12.1 Theorem 1)**.** *Let R be a ring and let M be a left R-module. Then TFAE:*

*(1) M satisfies the **ascending chain condition** on submodules (or **A.C.C.** on submodules), i.e., whenever*

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

is an increasing chain of submodules of M, then there is a positive integer m such that for all $k \geq m$, $M_k = M_m$ (so the chain becomes stationary at stage m:

$$M_1 \subseteq \cdots \subseteq M_{m-1} \subseteq M_m = M_{m+1} = M_{m+2} = \cdots).$$

(2) Every nonempty set of submodules of M contains a maximal element under inclusion.

(3) Every submodule of M is finitely generated.

*The left R-module M is said to be a **Noetherian** R-module if it satisfies any of the above equivalent conditions. The ring R is said to be **Noetherian** if it is Noetherian as a left module over itself, i.e., if there are no infinite increasing chains of left ideals in R.*

One can formulate analogous notions of A.C.C. on right and on two-sided ideals in a (possibly noncommutative) ring R. For noncommutative rings these properties need not be related.

Example. *Any P.I.D. R is a Noetherian ring due to condition (3) in the theorem with $M = R$. Then every nonempty set of ideals of R has a maximal element, and R satisfies the A.C.C. on two-sides ideals, which is equivalent to the descending chain condition (D.C.C.) on elements in this case.*

A Noetherian ring may have arbitrarily long ascending chains of ideals and may have infinitely long descending chains of ideals. For example, $\mathbb{Z}$ has the infinite descending chain

$$(2) \supsetneqq (4) \supsetneqq (8) \supsetneqq \cdots$$

*i.e., a Noetherian ring need not satisfy the **descending chain condition** on ideals (**D.C.C.**). We shall see in the future, however, that a commutative ring satisfying D.C.C. on ideals necessarily also satisfies A.C.C., i.e., is Noetherian; such rings are called **Artinian**.*

Example. *Even if M itself is a finitely generated R-module, submodules of M need not be finitely generated, so the condition that M be a Noetherian R-module is in general stronger than the condition that M be a finitely generated R-module.*

Take M to be the cyclic R-module R itself where R is the polynomial ring in infinitely many variables $x_1, x_2, \ldots$ with coefficients in some field k. The submodule (i.e. 2-sided ideal) generated by $\{x_1, x_2, \ldots\}$ cannot be generated by any finite set (note that one must show that no finite subset of this ideal will generate it).

Proof of Theorem 1. [(1) $\Rightarrow$ (2)] Assume M is Noetherian and let Σ be any nonempty collection of submodules of M. Choose any $M_1 \in \Sigma$. If M_1 is a maximal element of Σ then (2) holds, so assume M_1 is not maximal. Then there is some $M_2 \in \Sigma$ such that $M_1 \subsetneqq M_2$. If M_2 is maximal in Σ, (2) holds, so we may assume there is an $M_3 \in \Sigma$ properly containing M_2. Proceeding in this way one sees that if (2) fails we can produce an infinite strictly increasing chain of elements of Σ, contrary to (1).

[(2) $\Rightarrow$ (3)] Assume (2) holds and let N be any submodule of M. Let Σ be the collection of all finitely generated submodules of N. Since $0 \in \Sigma$, this collection is nonempty. By (2) Σ contains a maximal element N'. If $N' \subsetneqq N$, let $x \in N - N'$. Since $N' \in \Sigma$, the submodule N' is finitely generated by assumption, hence also the submodule generated by N' and x is finitely generated. This contradicts the maximality of N', so $N = N'$ is finitely generated.

[(3) $\Rightarrow$ (1)] Assume (3) holds and let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ be a chain of submodules of M. Let $N = \bigcup_{i=1}^{\infty} M_i$ and note that N is a submodule. By (3) N is finitely generated by, say, $a_1, a_2, \ldots, a_n$. Since $a_i \in N$ for all i, each a_i lies in one of the submodules in the chain, say M_{j_i}. Let $m = \max\{j_1, j_2, \ldots, j_n\}$. Then $a_i \in M_m$ for all i so the module they generate is contained in M_m, i.e., $N \subseteq M_m$. This implies $M_m = N = M_k$ for all $k \geq m$, which proves (1). □

Proposition ([1] §15.1 Proposition 1)**.** *If I is an ideal of the Noetherian ring R, then the quotient R/I is a Noetherian ring. Any homomorphic image of a Noetherian ring is Noetherian.*

Proof. Any infinite ascending chain of ideals in the quotient R/I would correspond by the Third Isomorphism Theorem to an infinite ascending chain of ideals in R. This gives the first statement, and the second follows by the First Isomorphism Theorem. □

A polynomial ring in n variables can be considered as a polynomial ring in one variable with coefficients in a polynomial ring in $n-1$ variables. By following this inductive approach we can deduce that $k[x_1, x_2, \ldots, x_n]$ is Noetherian from the following more general result.

Theorem ([1] §9.6 Theorem 21, Hilbert's Basis Theorem)**.** *If R is a Noetherian ring then so is the polynomial ring $R[x]$.*

Since a field is clearly Noetherian, Hilbert's Basis Theorem and induction immediately give:

Corollary ([1] §9.6 Corollary 22)**.** *The polynomial ring $k[x_1, x_2, \ldots, x_n]$ with coefficients from a field k is Noetherian, i.e., very ideal in this ring is finitely generated.*

If I is an ideal in $k[x_1, x_2, \ldots, x_n]$ generated by a (possibly infinite) set S of polynomials, the above corollary shows that I is finitely generated, and in fact I is generated by a finite number of the polynomials from the set S (cf. [1] §9.6 Exercise 1).

Let k be a field. Recall that a ring R is a **k-algebra** if k is contained in the center of R and the identity of k is the identity of R.

Definition. *The ring R is a **finitely generated k-algebra** if R is generated as a ring by k together with some finite set $r_1, r_2, \ldots, r_n$ of elements of R.*

*Let R and S be k-algebras. A map $\psi : R \to S$ is a **k-algebra homomorphism** if ψ is a ring homomorphism that is the identity on k.*

If R is a k-algebra then R is both a ring and a vector space over k, and it is important to distinguish the sense in which elements of R are generators for R. For example, the polynomial ring $k[x_1, \ldots, x_n]$ in a finite number of variables over k is a finitely generated k-algebra since $x_1, \ldots, x_n$ are ring generators, but for $n > 0$ this ring is an *infinite* dimensional vector space over k.

Corollary ([1] §15.1 Corollary 5)**.** *The ring R is a finitely generated k-algebra if and only if there is some surjective k-algebra homomorphism $\varphi : k[x_1, \ldots, x_n] \to R$ from the polynomial ring in a finite number of variables onto R that is the identity map on k. Any finitely generated k-algebra is therefore Noetherian.*

Proof. If R is generated as a k-algebra by $r_1, \ldots, r_n$, then we may define the map φ by $\varphi(x_i) := r_i$ for all i and $\varphi(a) := a$ for all $a \in k$. Then φ extends uniquely to a surjective ring homomorphism.

Conversely, given a surjective homomorphism φ, the images of $x_1, \ldots, x_n$ under φ then generate R as a k-algebra, proving that R is finitely generated.

Since $k[x_1, \ldots, x_n]$ is Noetherian by [1] §9.6 Corollary 22, any finitely generated k-algebra is therefore the quotient of a Noetherian ring, hence also Noetherian by [1] §15.1 Proposition 1. □

Example. *Suppose the k-algebra R is finite dimensional as a vector space over k, for example when $R = k[x]/(f(x))$, where f is any nonzero polynomial in $k[x]$. Then in particular R is a finitely generated k-algebra, since a vector space basis also generates R as a ring.*

In this case since ideals are also k-subspaces, any ascending or descending chain of ideals has at most $\dim_k R + 1$ distinct terms, hence R satisfies both A.C.C. and D.C.C. on ideals.

The basic idea behind "algebraic geometry" is to equate geometric questions with algebraic questions involving ideals in rings such as $k[x_1, \ldots, x_n]$. The Noetherian nature of these rings reduces many questions to consideration of finitely many algebraic equations (and this was in turn one of the main original motivations for Hilbert's Basis Theorem).

2 Integral extensions

In this section we consider the important concept of an integral extension of rings, which is a generalization to rings of algebraic extensions of fields. This leads to the definition of the "integers" in finite extensions of $\mathbb{Q}$ (the basic subject of algebraic number theory) and is also related to the existence of tangent lines for algebraic curves.

2.1 Integral elements

Definition. *Suppose R is a subring of the commutative ring S with $1_R = 1_S$ (i.e., $1 = 1_S \in R$).*

- *An element $s \in S$ is **integral** over R if s is the root of a monic polynomial in $R[x]$.*
- *The ring S is an **integral extension** of R (or just **integral** over R) if every $s \in S$ is integral over R.*
- *The **integral closure** of R in S is the set of elements of S that are integral over R.*
- *The ring R is said to be **integrally closed** in S if R is equal to its integral closure in S. The integral closure of an integral domain R in its field of fractions is called the **normalization** of R. An integral domain is called **integrally closed** or **normal** if it is integrally closed in its field of fractions.*

Example. *Every integer is integral over $\mathbb{Z}$; $\sqrt[3]{2}$ is integral over $\mathbb{Z}$; every n^{th} root of unity is integral over $\mathbb{Z}$ since it is a root of $x^n - 1 \in \mathbb{Z}[x]$; in particular $\omega = \zeta_3 = \frac{1}{2}(-1 + \sqrt{-3})$ is integral over $\mathbb{Z}$.*

$\frac{\sqrt{2}}{2}$ is not integral over $\mathbb{Z}$ but is integral over $\mathbb{Z}[\frac{1}{2}]$. Actually an element α in some field extension of $\mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if α is algebraic over $\mathbb{Q}$ and its (monic) minimal polynomial $m_{\alpha,\mathbb{Q}}(x)$ has coefficients in $\mathbb{Z}$. (This can be shown using Gauss' Lemma, cf. [1] §15.3 Proposition 28.) In particular a rational number is integral over $\mathbb{Z}$ if and only if it is in $\mathbb{Z}$.

*Let K be an extension field of $\mathbb{Q}$. An element $\alpha \in K$ is called an **algebraic integer** if α is integral over $\mathbb{Z}$, i.e., if α is the root of some monic polynomial with coefficients in $\mathbb{Z}$. The integral closure of $\mathbb{Z}$ in K is called the **ring of integers** of K, and is denoted by $\mathcal{O}_K$. For example, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ and $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$.*

*Because the integers $\mathbb{Z}$ are the algebraic integers in $\mathbb{Q}$, for emphasis (and clarity) the elements of $\mathbb{Z}$ are sometimes referred to as the "**rational integers**" to distinguish them from the "integers" in extensions of finite degree over $\mathbb{Q}$ (called **number fields**).*

Proposition ([1] §15.3 Proposition 23)**.** *Let R be a subring of the commutative ring S with $1 \in R$ and let $s \in S$. Then TFAE (the following are equivalent):*

(1) s is integral over R,

(2) $R[s]$ is a finitely generated R-module (where $R[s]$ is the ring of all R-linear combinations of powers of s), and

(3) $s \in T$ for some subring T, $R \subseteq T \subseteq S$, that is a finitely generated R-module.

Proof. Exercise. □

Corollary ([1] §15.3 Corollaries 24 & 25)**.** *Let R be a subring of the commutative ring S with $1 \in R$ and let $s, t \in S$.*

(1) If s and t are integral over R then so are $s \pm t$ and st.

(2) The integral closure of R in S is a subring of S containing R.

(3) Integrality is transitive: let S be a subring of T; if T is integral over S and S is integral over R, then T is integral over R.

(4) The integral closure of R in S is integrally closed in S.

Exercise ([1] §15.3 p.693)**.** *Show that any U.F.D. (Unique Factorization Domain) is integrally closed (and therefore $\mathbb{Z}$ and $\mathbb{Z}[i]$ are both integrally closed).*

2.2 Algebraic integers

Theorem ([1] §15.3 Theorem 29)**.** *Let K be a number field of degree n over $\mathbb{Q}$.*

*(1) The ring $\mathcal{O}_K$ of integers in K is a Noetherian ring and is a free $\mathbb{Z}$-module of rank n. An **integral basis** for the number field K is defined to be a basis of the ring $\mathcal{O}_K$ considered as a free $\mathbb{Z}$-module.*

(2) For every $\beta \in K$ there is some nonzero $d \in \mathbb{Z}$ such that $d\beta$ is an algebraic integer. In particular, K is the field of fractions of $\mathcal{O}_K$.

(3) If $\beta_1, \beta_2, \ldots, \beta_n$ is any $\mathbb{Q}$-basis of K, then there is an integer d such that $d\beta_1, d\beta_2, \ldots, d\beta_n$ is a basis for a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank n. Any basis of the $\mathbb{Z}$-module $\mathcal{O}_K$ is also a basis for K as a vector space over $\mathbb{Q}$.

Example. *The ring of integers in $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$, with an integral basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ (cf. [2] Remark 2.25 & Proposition 2.34)*

Example. *The ring of integers in the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity is $\mathbb{Z}[\zeta_n]$, where ζ_n is any primitive n^{th} root of 1. The elements $1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}$ are an integral basis. It is clear that ζ_n is an algebraic integer since it is a root of $x^n - 1$, so the ring $\mathbb{Z}[\zeta_n]$ is contained in the ring of integers. The proof that this is the full ring of algebraic integers in $\mathbb{Q}(\zeta_n)$ can be found in [2] Proposition 6.2 and Theorem 6.4.*

Exercise ([1] §15.3 p.698)**.** *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic extension of $\mathbb{Q}$ for some squarefree integer D. Show that*

$$\mathcal{O}_K = \mathbb{Z}[\omega] = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \omega$$

with integral basis $\{1, \omega\}$, where

$$\omega \coloneqq \begin{cases} \sqrt{D}, & \text{if } D \equiv 2, 3 \bmod 4, \\ \dfrac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \bmod 4. \end{cases}$$

Recall that any U.F.D. is integrally closed. Note that $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\sqrt{5}]$ are not integrally closed, and one can verify that neither of them is a U.F.D.

We remark here (cf. [2]) that, it was Dedekind who found the correct definition of the ring of integers in a number fields. Earlier authors either luckily chose the correct ring, e.g., Kummer chose $\mathbb{Z}[\zeta_n]$ as the ring of integers in $\mathbb{Q}(\zeta_n)$, or unluckily chose the wrong ring, e.g., Euler gave a proof of Fermat's Last Theorem for the exponent 3, which becomes correct when the ring $\mathbb{Z}[\sqrt{-3}]$ is replaced in the proof by its integral closure $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Exercise. *Use a computer algebra system (*Magma[1]*,* PARI/GP[2]*,* SageMath[3]*, etc.) to find an integral basis of the ring of integers in $K = \mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, the maximal real subfield of the cyclotomic field, where $n = 7$ and $n = 9$. (Display your code in the verbatim environment.) Verify your answer in the online database* LMFDB[4].

2.3 Extensions and contractions of ideals

Let $\varphi : R \to S$ be a homomorphism of commutative rings.

- If I is an ideal in R, then the ideal $\varphi(I)S$ of S generated by the image of I is called the **extension** of I to S, denoted ${}^eI$.
- If J is an ideal of S, then the ideal $\varphi^{-1}(J)$ is called the **contraction** in R of J, denoted ${}^cJ$.

In the special case where R is a subring of S and φ is the natural injection, the **extension** of $I \subseteq R$ is the ideal IS in S; and the **contraction** of $J \subseteq S$ is the ideal $J \cap R$ of R.

Exercise. *Let $\varphi : R \to S$ be a homomorphism of commutative rings, I be an ideal of R and J be an ideal of S. Show that*

(1) I is contained in the contraction of its extension to S, in particular, $I \subseteq IS \cap R$;

(2) J contains the extension of its contraction in R, in particular, $(J \cap R)S \subseteq J$.

Give explicit examples to show that equality need not hold in either situation.

If Q is a prime ideal in S, then its contraction is prime in R (although the contraction of a maximal ideal need not be maximal). On the other hand, if P is a prime ideal in R, its extension need not be prime (or even proper) in S; moreover, it is not generally true that P is the contraction of a prime ideal of S.

For integral ring extensions, however, the situation is more controlled:

Theorem ([1] §15.3 Theorem 26 & Corollary 27)**.** *Let R be a subring of the commutative ring S with $1 \in R$ and suppose that S integral over R.*

(1) Assume that S is an integral domain. Then R is a field if and only if S is a field.

*(2) If Q is a prime ideal in S, then its contraction $P := Q \cap R$ is prime in R. We say that Q **lies over** P in this case. Moreover, P is maximal if and only if Q is maximal.*

(3) Let P be a prime ideal in R. Then there is a prime ideal Q in S with $P = Q \cap R$:

$$\begin{array}{cc} S & Q \\ | & | \\ R & P \end{array}$$

(4) Assume S is finitely generated (as a ring) over R. If P is a maximal ideal in R, then there is a nonzero and finite number of maximal ideals Q of S lying over P.

[1] Available at `http://magma.maths.usyd.edu.au/calc/`
[2] `http://pari.math.u-bordeaux.fr/gp.html`
[3] `http://www.sagemath.org/`
[4] `http://www.lmfdb.org/NumberField/`

Proof. (1) Assume first that R is a field and let s be a nonzero element of S. Then s is integral over R, so

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0$$

for some $a_0, a_1, \ldots, a_{n-1}$ in R. Since S is an integral domain, we may assume $a_0 \neq 0$ (otherwise cancel factors of s). Then

$$s(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1) = -a_0,$$

and since $-a_0^{-1} \in R$, this shows that $-a_0^{-1}(s^{n-1} + a_{n-1}s^{n-2} + \cdots + a_1)$ is an inverse for s in S, so S is a field.

Conversely, suppose S is a field and r is a nonzero element of R. Since $r^{-1} \in S$ is integral over R we have

$$r^{-m} + b_{m-1}r^{-m+1} + \cdots + b_1 r^{-1} + b_0 = 0$$

for some $b_0, \ldots, b_{m-1} \in R$. Then $r^{-1} = -(b_{m-1} + \cdots + b_1 r^{m-2} + b_0 r^{m-1}) \in R$, so R is a field. (In general, this shows that $R \cap S^\times = R^\times$ whenever S is integral over R.)

(2) The first statement can be shown directly from the definition of prime ideals.

For the second statement, observe that the integral domain S/Q is an integral extension of R/P (reducing the monic polynomial over R satisfied by $s \in S$ modulo Q gives a monic polynomial satisfied by $\bar{s} \in S/Q$ over $R/(Q \cap R)$). By (1), S/Q is a field if and only if R/P is a field, i.e., Q is maximal if and only if P is maximal.

(3) Cf. [1] §15.4 Corollary 50.

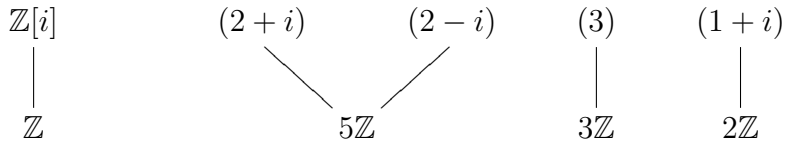
(4) There exists at least one maximal ideal Q lying over P by part (3) of the theorem, so we must see why there are only finitely many such maximal ideals in S. If Q is a maximal ideal of S with $Q \cap R = P$, then S/Q is a field containing the field R/P. To prove that there are only finitely many possible Q, it suffices to prove that there are only finitely many homomorphisms from S to a field containing R/P that extend the homomorphism from R to R/P.

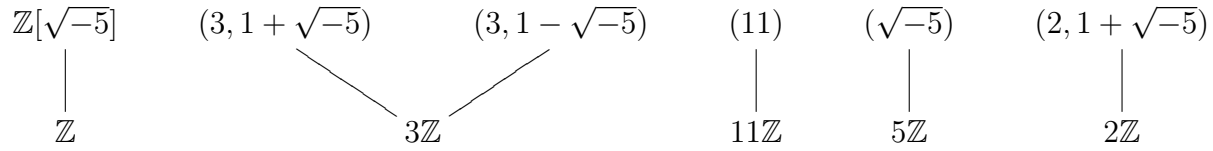
Let $S = R[s_1, \ldots, s_n]$, where the elements s_i are integral over R by assumption, and let $p_i(x)$ be a monic polynomial with coefficients in R satisfied by s_i. If Q is a maximal ideal of S, then $S/Q = (R/P)[\bar{s}_1, \ldots, \bar{s}_n]$ is the field extension of the field R/P with generators $\bar{s}_1, \ldots, \bar{s}_n$. The element $\bar{s}_i$ is a root of the monic polynomial $\bar{p}_i(x)$ with coefficients in R/P obtained by reducing the coefficients of $p_i(x)$ mod P. There are only a finite number of possible roots of this monic polynomial (in a fixed algebraic closure of R/P), and so only finitely many possible field extensions of the form $(R/P)[\bar{s}_1, \ldots, \bar{s}_n]$, which proves the statement. □

If $\mathfrak{p}$ is a nonzero prime ideal in the ring of integers $\mathcal{O}_K$ of a number field K, then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. If $\alpha \in \mathfrak{p}$, then the constant term of the minimal polynomial for α over $\mathbb{Q}$ (i.e. the **norm** of α) is then an element in $\mathfrak{p} \cap \mathbb{Z}$, which shows that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ is also a nonzero prime ideal in $\mathbb{Z}$. By (3) in the above theorem, every prime ideal (p) in $\mathbb{Z}$ arises in this way.

Since $p\mathbb{Z}$ is a maximal ideal, it also follows from (2) in the above theorem that, all nonzero prime ideals in $\mathcal{O}_K$ are maximal, and then by (4), there are finitely many prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ with $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

Example. *The following diagrams show three different types of prime ideals in $\mathcal{O}_K = \mathbb{Z}[i]$ where $K = \mathbb{Q}(i)$, and in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ where $K = \mathbb{Q}(\sqrt{-5})$:*





Here (α) denotes the ideal in $\mathcal{O}_K$ generated by $\alpha \in \mathcal{O}_K$.

Exercise ([1] §8.3 Theorem 18 & Exercise 8)**.** *Show the ideals listed in the above diagrams are all prime.*

We shall see later ([1] §16.3 Corollary 16) that every nonzero ideal in the ring of integers of a number field can be written uniquely as the product of prime ideals, and in the case of the ideal $p\mathcal{O}_K$ the distinct prime factors are precisely the finitely many ideals $\mathfrak{p}$ in $\mathcal{O}_K$ lying over $p\mathbb{Z}$. This property replaces the unique factorization of elements in $\mathcal{O}_K$ into primes (which need not hold since $\mathcal{O}_K$ need not be a U.F.D.).

Theorem ([1] §15.3 Theorem 26(3), the Going-up Theorem)**.** *Let R be a subring of the commutative ring S with $1 \in R$ and suppose that S integral over R.*

Let $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_n$ be a chain of prime ideals in R and suppose there are prime ideals $Q_1 \subseteq Q_2 \subseteq \cdots \subseteq Q_m$ of S with $P_i = Q_i \cap R$, $1 \leq i \leq m$ and $m < n$. Then the ascending chain of ideals can be completed, i.e., there are prime ideals $Q_{m+1} \subseteq \cdots \subseteq Q_n$ in S such that $P_i = Q_i \cap R$ for all i, and $Q_m \subseteq Q_{m+1}$:

$$\begin{array}{ccccccccc} S & & Q_1 & \subseteq & \cdots & \subseteq & Q_m & \subseteq \cdots \subseteq & Q_n \\ | & & | & & & & | & & | \\ R & & P_1 & \subseteq & \cdots & \subseteq & P_m & \subseteq \cdots \subseteq & P_n \end{array}$$

Proof. Exercise. □

Remark. *The Going-up Theorem fails for the rings $\mathbb{Z} \subseteq \mathbb{Z}[x]$: consider the prime ideals $(0) \subseteq (2)$ of $\mathbb{Z}$, and the prime ideal $Q_1 = (1+2x)$ of $\mathbb{Z}[x]$; then $Q_1 \cap \mathbb{Z} = (0)$, but a prime ideal Q_2 of $\mathbb{Z}[x]$ containing Q_1 and such that $Q_2 \cap \mathbb{Z} = (2)$ would have to contain $(2, 1+2x) = \mathbb{Z}[x]$.*

Theorem ([1] §15.3 Theorem 26(4), the Going-down Theorem)**.** *Let R be a subring of the commutative ring S with $1 \in R$ and suppose that S integral over R. Assume that S is an integral domain and R is integrally closed.*

Let $P_1 \supseteq P_2 \supseteq \cdots \supseteq P_n$ be a chain of prime ideals in R and suppose there are prime ideals $Q_1 \supseteq Q_2 \supseteq \cdots \supseteq Q_m$ of S with $P_i = Q_i \cap R$, $1 \leq i \leq m$ and $m < n$. Then the descending chain of ideals can be completed, i.e., there are prime ideals $Q_{m+1} \supseteq \cdots \supseteq Q_n$ in S such that $P_i = Q_i \cap R$ for all i, and $Q_m \supseteq Q_{m+1}$:

$$\begin{array}{ccccccccc} S & & Q_1 & \supseteq & \cdots & \supseteq & Q_m & \supseteq \cdots \supseteq & Q_n \\ | & & | & & & & | & & | \\ R & & P_1 & \supseteq & \cdots & \supseteq & P_m & \supseteq \cdots \supseteq & P_n \end{array}$$

Proof. Cf. [1] §15.4 Exercise 24. □

3 Localization

The idea of "localization at a prime" in a ring is an extremely powerful and pervasive tool in algebra for isolating the behavior of the ideals in a ring. It is an algebraic analogue of the familiar idea of localizing at a point when considering questions of, for example, the differentiability of a function $f(x)$ on the real line. In fact one of the important applications (and also one of the original motivations for the development) of this technique is to translate such "local" properties in the geometry of affine algebraic spaces to corresponding properties of their coordinate rings.

3.1 Ring of fractions

We first consider a very general construction of "rings of fractions". Let D be a multiplicatively closed subset of a commutative ring R containing 1 (i.e., $1 \in D$, and $ab \in D$ if $a, b \in D$). Recall that when D does not contain 0 or any zero divisors, the **ring of fractions** of R with respect to D is defined in [1] §7.5 by

$$D^{-1}R := \{(r, d) \mid r \in R, d \in D\} / \sim,$$

with the equivalence relation defined by

$$(r, d) \sim (r', d') \qquad \text{if and only if} \qquad rd' = r'd.$$

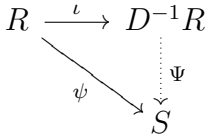
The equivalence class of (r, d) under $\sim$ is denoted by $r/d = \frac{r}{d}$, and the addition and multiplication are defined as those of rational numbers:

$$\frac{r}{d} + \frac{r'}{d'} := \frac{rd' + r'd}{dd'}, \qquad \frac{r}{d} \times \frac{r'}{d'} := \frac{rr'}{dd'}.$$

If R is an integral domain and $D = R - \{0\}$, $D^{-1}R$ is called the **field of fractions** or **quotient field** of R.

When we allow D to contain zero or zero divisors, the next result constructs a new ring $D^{-1}R$ which is the "smallest" ring in which the elements of D become units. In this case R need not embed as a subring of $D^{-1}R$.

Theorem ([1] §15.4 Theorem 36 & Corollary 37)**.** *Let R be a commutative ring with 1 and let D be a multiplicatively closed subset of R containing 1. Then there is a commutative ring $D^{-1}R$ and a ring homomorphism $\iota : R \to D^{-1}R$ satisfying the following **universal property**: for any homomorphism $\psi : R \to S$ of commutative rings that sends 1 to 1 such that $\psi(d)$ is a unit in S for every $d \in D$, there is a unique homomorphism $\Psi : D^{-1}R \to S$ such that $\Psi \circ \iota = \psi$, and the diagram*



*commutes. The ring $D^{-1}R$ is called the **ring of fractions** of R with respect to D. or the **localization** of R at D. Moreover,*

- $\ker \iota = \{r \in R \mid xr = 0$ *for some* $x \in D\}$*; in particular, $\iota : R \to D^{-1}R$ is an injection if and only if D does not contain zero or any zero divisors of R, and*
- $D^{-1}R = 0$ *if and only if* $0 \in D$*, hence if and only if D contains nilpotent elements.*

Proof. As in the proof of [1] §7.5 Theorem 15, we can still define

$$D^{-1}R := \{(r, d) \mid r \in R, d \in D\} / \sim,$$

where the equivalence class of (r, d) under $\sim$ is denoted by $r/d = \frac{r}{d}$, and $\iota : R \to D^{-1}R$ is given by $r \mapsto r/1$. But when D contains zero or any zero divisors of R, $rd' = r'd$ cannot define an equivalence relation $(r, d) \sim (r', d')$ since the transitivity may not hold any more: if $(r, d) \sim (r', d')$ and $(r', d') \sim (r'', d'')$ then $rd' - r'd = 0$ and $r'd'' - r''d' = 0$; multiplying the first equation by d'' and the second by d and adding gives $(rd'' - r''d)d' = 0$, which will not imply $rd'' = r''d$ if d' is a zero divisor. To fix this, we define a relation on $R \times D$ by

$$(r, d) \sim (r', d') \qquad \text{if and only if} \qquad (rd' - r'd)x = 0 \text{ for some } x \in D.$$

The proof of the theorem is left as an exercise. □

Example. *Let R be any commutative ring with 1 and let f be any element of R. Let D be the multiplicative set $\{f^n \mid n \geq 0\}$ of nonnegative powers of f in R. Define $R_f = D^{-1}R$. Then every element of R_f can be written in the form a/f^m for some $a \in R$, $m \in \mathbb{Z}_{\geq 0}$, and*

$$\frac{a}{f^m} = \frac{b}{f^n} \qquad \text{if and only if} \qquad (af^n - bf^m)f^k = 0 \text{ for some } k.$$

If R is an integral domain with field of fractions F and $f \neq 0$, then R_f is the subring of F of elements that can be written in the form a/f^m, $a \in R$, $m \in \mathbb{Z}_{\geq 0}$.

Note that $R_f = 0$ if and only if f is nilpotent. If f is not nilpotent, then f becomes a unit in R_f, and the following exercise shows that

$$R_f \cong R[x]/(xf - 1),$$

where $R[x]$ is the polynomial ring in the variable x. Note also that R_f and R_{f^n} are naturally isomorphic for any $n \geq 1$, since both f and f^n are units in both rings.

If f is a zero divisor then $\iota : R \to R_f$ does not embed R into R_f. For example, let $R = k[x, y]/(xy)$, and take $f = x$. Then x is a unit in R_x and y is mapped to 0 (explicitly: $y = xy/x = 0$ in R_x). In this case $\iota(R) = k[x] \subseteq R_x = k[x, x^{-1}]$.

Exercise ([1] §15.4 Exercise 18)**.** *In the notation above, prove that $R_f \cong R[x]/(xf - 1)$ if f is not nilpotent in R.* [Hint: Show that the map $\varphi : R[x] \to R_f$ defined by $\varphi(r) = r/1$ and $\varphi(x) = 1/f$ gives a surjective ring homomorphism and the universal property gives an inverse.]

Example (Localizing at a Prime)**.** *Let P be a prime ideal in any commutative ring R and let $D = R - P$. By definition of a prime ideal, D is multiplicatively closed. Passing to the ring $D^{-1}R$ in this case is called **localizing** R at P and the ring $D^{-1}R$ is denoted by R_P. Every element of R not in P becomes a unit in R_P.*

For example, if $R = \mathbb{Z}$ and $P = (p)$ is a prime ideal, then

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b \right\} \subseteq \mathbb{Q},$$

and every integer b not divisible by p is a unit in $\mathbb{Z}_{(p)}$.

Note that this is not the ring $\mathbb{Z}_p$ of p-adic integers (defined in [1] §7.6 Exercise 11). Indeed, $\mathbb{Z}_{(p)}$, as a subring of $\mathbb{Q}$, is countable, while $\mathbb{Z}_p$ is not, and we have $\mathbb{Z}_{(p)} \subsetneq \mathbb{Z}_p$.

Exercise. *Write $\frac{1}{3} \in \mathbb{Z}_{(5)}$ in terms of a formal power series in $\mathbb{Z}_5$. Use Hensel's Lemma to show that $x^2 + 1$ has a root in $\mathbb{Z}_5$ but not in $\mathbb{Z}_{(5)}$.*

Example. *If Σ is any nonempty set and k is a field, let $R \subseteq \{f : \Sigma \to k\}$ be any ring of k-valued functions on Σ containing the constant functions (for instance, the ring of all continuous real valued functions on the closed interval $[0, 1]$). For any $a \in \Sigma$ let*

$$M_a \coloneqq \{f \in R \mid f(a) = 0\}$$

be the ideal of functions in R that vanish at a. Then

$$M_a = \ker\left(R \to k,\ f \mapsto f(a)\right)$$

i.e., M_a is the kernel of the ring homomorphism from R to the field k given by evaluating each function in R at a. Since R contains the constant functions, evaluation is surjective, hence $R/M_a \cong k$ and so M_a is a maximal (hence also prime) ideal.

The localization of R at this prime ideal is then

$$R_{M_a} = \left\{ \frac{f}{g} \mid f, g \in R,\ g(a) \neq 0 \right\}.$$

Each function in R_{M_a} can then be evaluated at a by $(f/g)(a) = f(a)/g(a)$, and this value does not depend on the choice of representative for the equivalence class f/g, so R_{M_a} becomes a ring of k-valued "rational functions" defined at a.

For example, let R be the ring of all continuous real valued functions on the closed interval $[0, 1]$. If we are only interested in the behavior of functions near the point $a \in [0, 1]$, a function in the multiplicatively closed subset $D = R - M_a$ (a function that does not vanish at a) does not vanish in some open neighborhood of a. Therefore, by restricting such function to a small neighborhood, we get a nonvanishing function and therefore it is possible to take its multiplicative inverse. Thus, R_{M_a} can be thought of as the result of concentrating attention to small neighborhoods of the point a, which explains from where the term "localization" comes from.

3.2 Localizations of ideals

We next consider extensions and contractions of ideals with respect to the map $\iota : R \to D^{-1}R$ defined by $r \mapsto r/1$. Recall that, if I is an ideal of R, the **extension** of I to $D^{-1}R$ is ${}^eI := \iota(I)D^{-1}R$; and if J is an ideal of $D^{-1}R$, the **contraction** of J to R is ${}^cJ := \iota^{-1}(J)$.

If I is an ideal of R then it is easy to see that every element of ${}^eI$ can be written in the form a/d for some $a \in I$ and $d \in D$, so the extension of I to $D^{-1}R$ is also frequently denoted by $D^{-1}I$.

Proposition ([1] §15.4 Proposition 38)**.** *In the preceding notation we have*

(1) For any ideal J of $D^{-1}R$ we have $J = {}^e({}^cJ)$. In particular, every ideal of $D^{-1}R$ is the extension of some ideal of R, and distinct ideals of $D^{-1}R$ have distinct contractions in R.

(2) For any ideal I of R we have

$${}^c({}^eI) = \{r \in R \mid dr \in I \text{ for some } d \in D\}.$$

Also, ${}^eI = D^{-1}R$ if and only if $I \cap D \neq \emptyset$.

(3) Extension and contraction give a bijective correspondence

$$\{\text{prime ideals } P \text{ of } R \text{ with } P \cap D = \emptyset\} \underset{c}{\overset{e}{\rightleftharpoons}} \{\text{prime ideals } D^{-1}P \text{ of } D^{-1}R\}.$$

(4) If R is Noetherian (or Artinian) then $D^{-1}R$ is Noetherian (Artinian, respectively).

Proof. Exercise. □

We recall the definition of an important type of ring: a conunutative ring with 1 that has a unique maximal ideal is called a **local ring**.

Proposition ([1] §15.4 Proposition 46)**.** *For any commutative ring R with 1, let R_P be the localization of R at the prime ideal P and let ${}^eP$ be the extension of P to R_P.*

(1) The ring R_P is a local ring with unique maximal ideal ${}^eP$. The contraction of ${}^eP$ to R is P, i.e., ${}^c({}^eP) = P$, and the map from R to R_P induces an injection of the integral domain R/P into $R_P/{}^eP$. The quotient $R_P/{}^eP$ is a field and is isomorphic to the fraction field of the integral domain R/P.

(2) If R is an integral domain, then R_P is an integral domain. The ring R injects into the local ring R_P, and, identifying R with its image in R_P, the unique maximal ideal of R_P is PR_P.

(3) The prime ideals in R_P are in bijective correspondence with the prime ideals of R contained in P. If P is a minimal nonzero prime ideal of R then R_P has a unique nonzero prime ideal.

Proof. Exercise. □

Example. *Recall that if $R = \mathbb{Z}$ and $P = (p) = p\mathbb{Z}$ is a prime ideal, then*

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b \right\} \subseteq \mathbb{Q},$$

and every integer b not divisible by p is a unit in $\mathbb{Z}_{(p)}$. So the extension of any prime ideal $P' = p'\mathbb{Z}$ to $\mathbb{Z}_{(p)}$ is $p'\mathbb{Z}_{(p)} = \mathbb{Z}_{(p)}$ unless $p' \in p\mathbb{Z}$. The above proposition says that $\mathbb{Z}_{(p)}$ has a unique maximal ideal $p\mathbb{Z}_{(p)}$, which is also the unique nonzero prime ideal.

Example. *Let $P = (2, x)$ be a prime ideal of $R = \mathbb{Z}[x]$. Then*

$$R_P = \mathbb{Z}[x]_{(2,x)} = \left\{ \frac{f(x)}{g(x)} \in \mathbb{Q}(x) \;\middle|\; g(x) \notin (2, x) \right\} \subseteq \mathbb{Q}(x).$$

It is a local ring with unique maximal ideal $PR_P = (2, x)\mathbb{Z}[x]_{(2,x)}$.

The prime ideals in R_P are in bijective correspondence with the prime ideals of R contained in P. For example, the extensions of (2), (x), and $(x^2 + 2)$ to $\mathbb{Z}[x]_{(2,x)}$ are all prime; they are all contained in the unique maximal ideal.

3.3 Localizations of modules

Suppose now that M is an R-module and D is a multiplicatively closed subset of R containing 1 as above. Then the ideas used in the construction of $D^{-1}R$ can be used to construct a $D^{-1}R$-module $D^{-1}M$ from M in a similar fashion, as follows. Define the relation on DxM by

$$(d, m) \sim (d', m') \qquad \text{if and only if} \qquad x(dm' - d'm) = 0 \text{ for some } x \in D,$$

which is easily checked to be an equivalence relation. Let m/d denote the equivalence class of (d, m) and let $D^{-1}M$ denote the set of equivalence classes. It is then straightforward to verify that the operations

$$\frac{m}{d} + \frac{m'}{d'} \coloneqq \frac{d'm + dm'}{dd'} \qquad \text{and} \qquad \frac{r}{d} \cdot \frac{m}{d'} \coloneqq \frac{rm}{dd'}$$

are well defined and give $D^{-1}M$ the structure of a $D^{-1}R$-module, called the **module of fractions** of M with respect to D or the **localization** of M at D.

Note that the localization $D^{-1}M$ is also an R-module (since each $r \in R$ acts by $r/1$ on $D^{-1}M$), and there is an R-module homomorphism

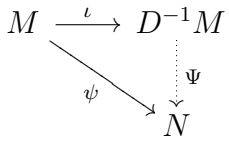
$$\iota : M \to D^{-1}M \qquad \text{defined by} \qquad m \mapsto m/1.$$

It follows directly from the definition of the equivalence relation that

$$\ker \iota = \{m \in M \mid dm = 0 \text{ for some } d \in D\}.$$

The homomorphism ι has a universal property analogous to that in [1] §15.4 Theorem 36. Suppose N is an R-module with the property that left multiplication on N by d is a bijection of N for every

$d \in D$. If $\psi : M \to N$ is any R-module homomorphism, then there is a unique R-module homomorphism $\Psi : D^{-1}M \to N$ such that $\Psi \circ \iota = \psi$, and the diagram



commutes.

If M and N are R-modules and $\varphi : M \to N$ is an R-module homomorphism, then for any multiplicative set D in R, it is easy to check that there is an induced $D^{-1}R$-module homomorphism $D^{-1}M \to D^{-1}N$ defined by $m/d \mapsto \varphi(m)/d$.

Exercise ([1] §15.4 Exercise 15)**.** *Let $R = \mathbb{Z}[\sqrt{-5}]$ be the ring of integers in the quadratic field $Q(\sqrt{-5})$, and let I be the prime ideal $(2, 1+\sqrt{-5})$ of R generated by 2 and $1+\sqrt{-5}$. Recall that every nonzero prime ideal P of R contains a prime $p \in \mathbb{Z}$.*

(a) If P is a prime ideal of R not containing 2, prove that $I_P = R_P$.

(b) If P is a prime ideal of R containing 2, prove that $P = I$ and that $I_P = (1+\sqrt{-5})R_P$.

(c) Prove that $I_P \cong R_P$ as R_P-modules for every prime ideal P of R, but that I and R are not isomorphic R-modules. [Hint: Observe that $I \cong R$ as R-modules if and only if I is a *principal* ideal.]

The next result shows that the localization of M at D is related to the tensor product.

Proposition ([1] §15.4 Proposition 41)**.** *Let D be a multiplicatively closed subset of R containing 1 and let M be an R-module. Then*

$$D^{-1}M \cong D^{-1}R \otimes_R M$$

as $D^{-1}R$-modules, i.e., $D^{-1}M$ is the $D^{-1}R$-module obtained by extension of scalars from the R-module M.

Sketch of proof. • The map $D^{-1}R \times M \to D^{-1}M$ defined by $(r/d, m) \mapsto rm/d$ is well defined and R-balanced, so induces a homomorphism from $D^{-1}R \otimes_R M$ to $D^{-1}M$.
• The map $m/d \mapsto (1/d) \otimes m$ gives a well defined inverse homomorphism.
Hence $D^{-1}M$ is isomorphic to $D^{-1}R \otimes_R M$ as an R-module since these inverse isomorphisms are also $D^{-1}R$-module homomorphisms. □

Example ([1] §15.4 p.719)**.** *Let $R = \mathbb{Z}$ and let $\mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at the nonzero prime ideal (p). Any abelian group M is a $\mathbb{Z}$-module so we may localize M at (p) by forming $M_{(p)}$. This abelian group is the same as the quotient of M with respect to the subgroup of elements whose order is finite and not divisible by p.*

If M is a finite (or, more generally, torsion) abelian group, then $M_{(p)}$ is a p-group, and is the Sylow p-subgroup or p-primary component of M. The localization $M_{(0)}$ of M at (0) is the trivial group. For a specific example, let $M = \mathbb{Z}/6\mathbb{Z}$ be the cyclic group of order 6, considered as a $\mathbb{Z}$-module. Then the localization of M at $p = 2$ is $\mathbb{Z}/2\mathbb{Z}$, at $p = 3$ is $\mathbb{Z}/3\mathbb{Z}$, and reduces to 0 at all other prime ideals of $\mathbb{Z}$.

Localizing a ring R or an R-module M at D behaves very well with respect to algebraic operations on rings and modules, as the following proposition shows:

Proposition ([1] §15.4 Proposition 42)**.** *Let R be a commutative ring with 1 and let $D^{-1}R$ be its localization with respect to the multiplicatively closed subset D of R containing 1.*

(1) Localization commutes with finite sums and intersections of ideals:
If I and J are ideals of R, then

$$D^{-1}(I+J) = D^{-1}(I) + D^{-1}(J) \qquad \textit{and} \qquad D^{-1}(I \cap J) = D^{-1}I \cap D^{-1}(J).$$

(2) Localization commutes with quotients:

$$D^{-1}R/D^{-1}I \cong D^{-1}(R/I),$$

(where the localization on the right is with respect to the image of D in the quotient R/I).

(3) Localization commutes with finite sums, intersections and quotients of modules:
If N and N' are submodules of the R-module M, then
(a) $D^{-1}(N+N') = D^{-1}N + D^{-1}N'$ and $D^{-1}(N \cap N') = D^{-1}N \cap D^{-1}N'$;
(b) $D^{-1}N$ is a submodule of $D^{-1}M$ and $D^{-1}M/D^{-1}N = D^{-1}(M/N)$.

(4) Localization commutes with finite direct sums of modules:
If M and N are R-modules, then $D^{-1}(M \oplus N) \cong D^{-1}M \oplus D^{-1}N$.

(5) Localization is exact (i.e., $D^{-1}R$ is a flat R-module):
If $0 \to L \to M \to N \to 0$ is a short exact sequence of R-modules, then the induced sequence $0 \to D^{-1}L \to D^{-1}M \to D^{-1}N \to 0$ of $D^{-1}R$-modules is also exact.

Exercise ([1] §15.4 Exercise 16)**.** *Prove that localization commutes with tensor products:*
For any R-modules M, N, and multiplicatively closed set D in R, there is a unique isomorphism of $D^{-1}R$-modules

$$\varphi : (D^{-1}M) \otimes_{D^{-1}R} (D^{-1}N) \to D^{-1}(M \otimes_R N), \quad \textit{such that} \quad (m/d) \otimes (n/d') \mapsto (m \otimes n)/dd'.$$

3.4 The local–global principle

Let M be an R-module, let $\mathfrak{p}$ be a prime ideal of R and set $D = R - \mathfrak{p}$. The $R_{\mathfrak{p}}$-module $D^{-1}M$ is called the **localization** of M at $\mathfrak{p}$, and is denoted by $M_{\mathfrak{p}}$.

By [1] §15.4 Proposition 41, $M_{\mathfrak{p}}$ can also be identified with the tensor product $R_{\mathfrak{p}} \otimes_R M$. When R is an integral domain and $\mathfrak{p} = (0)$, $M_{(0)}$ is a module over the field of fractions F of R, i.e., is a vector space over F.

The element $m/1$ is zero in $M_{\mathfrak{p}}$ if and only if $rm = 0$ for some $r \in R - \mathfrak{p}$, so localizing at $\mathfrak{p}$ annihilates the $\mathfrak{p}'$-torsion elements of M for primes $\mathfrak{p}'$ not contained in $\mathfrak{p}$. In particular, localizing at (0) over an integral domain annihilates the torsion subgroup of M.

Exercise. *If R is an integral domain with field of fractions F, show that* $\operatorname{rank}(M) = \dim_F M_{(0)}$.
[Recall that in [1] §12.1, the **rank** of the R-module M is defined to be the maximum number of R-linearly independent elements of M).]

Localization of a module M at a prime $\mathfrak{p}$ in general produces a simpler module $M_{\mathfrak{p}}$ whose properties are easier to determine. It is then of interest to translate these "local" properties of $M_{\mathfrak{p}}$ back into "global" information about the module M itself. For example, the most basic question of whether a module M is 0 can be answered locally:

Proposition ([1] §15.4 Proposition 47)**.** *Let M be an R-module. Then TFAE (the following are equivalent):*

(1) $M = 0$*,*

(2) $M_{\mathfrak{p}} = 0$ *for all prime ideals* $\mathfrak{p}$ *of* R*, and*

(3) $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* R*.*

Proof. The implications (1) implies (2) implies (3) are obvious, so it remains to prove that (3) implies (1).

Suppose m is a nonzero element in M, and consider the annihilator $I = \{r \in R \mid rm = 0\}$ of m in R. Since m is nonzero, I is a proper ideal in R. Let $\mathfrak{m}$ be a maximal ideal of R containing I.

Consider the element $m/1$ in the corresponding localization $M_{\mathfrak{m}}$ of M. If this element were 0, then $rm = 0$ for some $r \in R - \mathfrak{m}$. But then r would be an element in I not contained in $\mathfrak{m}$, a contradiction. Hence $M_{\mathfrak{m}} \neq 0$, which proves that (3) implies (1). □

Exercise ([1] §15.4 Exercise 13)**.** *Prove that, if N and N' are two R-submodules of an R-module M with $N_{\mathfrak{p}} = N'_{\mathfrak{p}}$ in the localization $M_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of R (or just for every maximal ideal), then $N = N'$.*

It is not in general true that a property shared by all of the localizations of a module M is also shared by M. For example, all of the localizations of a ring R can be integral domains without R itself being an integral domain (for example, $R = \mathbb{Z}/6\mathbb{Z}$).

Nevertheless, a great deal of information can be ascertained from studying the various possible localizations, and this is what makes this technique so useful. If R is an integral domain, for example, then each of the localizations $R_{\mathfrak{p}}$ can be considered as a subring of the fraction field F of R that contains R; the next exercise shows that the elements of R are the only elements of F contained in every localization.

Exercise ([1] §15.4 Proposition 48)**.** *Let R be an integral domain. Show that R is the intersection of the localizations of R: $R = \cap_{\mathfrak{p}} R_{\mathfrak{p}}$. In fact, $R = \cap_{\mathfrak{m}} R_{\mathfrak{m}}$ is the intersection of the localizations of R at the maximal ideals $\mathfrak{m}$ of R.*

Other related exercises in [1]

§15.1 1 2 3 9
§15.3 2 3 5 6 9 10
§15.4 1 2 4 12 14 19 20 21 22

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[2] J. S. Milne. Algebraic number theory (v3.08). Available at `https://www.jmilne.org/math/CourseNotes/ANT.pdf`, 2020.