Contents

Chapter 1
Foundations

The present foundational chapter will introduce the notion of a ring and, next, that of a module over a ring. These notions will be the focus of the present book. Most of the chapter will be definitions.

We begin with a few historical remarks. Fermat's last theorem states that the equation

$$x^n + y^n = z^n$$

has no nontrivial solutions in the integers, for $n \geq 3$. We could try to prove this by factoring the expression on the left hand side. We can write

$$(x+y)(x+\zeta y)(x+\zeta^2 y)\dots(x+\zeta^{n-1}y) = z^n,$$

where ζ is a primitive nth root of unity. Unfortunately, the factors lie in $\mathbb{Z}[\zeta]$, not the integers $\mathbb{Z}$. Though $\mathbb{Z}[\zeta]$ is still a *ring* where we have notions of primes and factorization, just as in $\mathbb{Z}$, we will see that prime factorization is not always unique in $\mathbb{Z}[\zeta]$. (If it were always unique, then we could at least one important case of Fermat's last theorem rather easily; see the introductory chapter of [Was97] for an argument.)

For instance, consider the ring $\mathbb{Z}[\sqrt{-5}]$ of complex numbers of the form $a + b\sqrt{-5}$, where $a, b \in \mathbb{Z}$. Then we have the two factorizations

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

Both of these are factorizations of 6 into irreducible factors, but they are fundamentally different.

In part, commutative algebra grew out of the need to understand this failure of unique factorization more generally. We shall have more to say on factorization in the future, but here we just focus on the formalism. The basic definition for studying this problem is that of a *ring*, which we now introduce.

§1 Commutative rings and their ideals

1.1 Rings

We shall mostly just work with commutative rings in this book, and consequently will just say "ring" for one such.

Definition 1.1 A **commutative ring** is a set R with an addition map $+ : R \times R \to R$ and a multiplication map $\times : R \times R \to R$ that satisfy the following conditions.

1. R is a group under addition.

2. The multiplication map is commutative and distributes over addition. This means that $x \times (y + z) = x \times y + x \times z$ and $x \times y = y \times x$.

3. There is a **unit** (or **identity element**), denoted by 1, such that $1 \times x = x$ for all $x \in R$.

We shall typically write xy for $x \times y$.

Given a ring, a **subring** is a subset that contains the identity element and is closed under addition and multiplication.

A *noncommutative* (i.e. not necessarily commutative) ring is one satisfying the above conditions, except possibly for the commutativity requirement $xy = yx$. For instance, there is a noncommutative ring of 2-by-2 matrices over $\mathbb{C}$. We shall not work too much with noncommutative rings in the sequel, though many of the basic results (e.g. on modules) do generalize.

Example 1.2 $\mathbb{Z}$ is the simplest example of a ring.

Exercise 1.1 Let R be a commutative ring. Show that the set of polynomials in one variable over R is a commutative ring $R[x]$. Give a rigorous definition of this.

Example 1.3 For any ring R, we can consider the polynomial ring $R[x_1, \ldots, x_n]$ which consists of the polynomials in n variables with coefficients in R. This can be defined inductively as $(R[x_1, \ldots, x_{n-1}])[x_n]$, where the procedure of adjoining a single variable comes from the previous **??** 1.1.

We shall see a more general form of this procedure in Example 1.9.

Exercise 1.2 If R is a commutative ring, recall that an **invertible element** (or, somewhat confusingly, a **unit**) $u \in R$ is an element such that there exists $v \in R$ with $uv = 1$. Prove that v is necessarily unique.

Exercise 1.3 Let X be a set and R a ring. The set R^X of functions $f : X \to R$ is a ring.

1.2 The category of rings

The class of rings forms a category. Its morphisms are called ring homomorphisms.

Definition 1.4 A **ring homomorphism** between two rings R and S as a map $f : R \to S$ that respects addition and multiplication. That is,

1. $f(1_R) = 1_S$, where 1_R and 1_S are the respective identity elements.

2. $f(a + b) = f(a) + f(b)$ for $a, b \in R$.

3. $f(ab) = f(a)f(b)$ for $a, b \in R$.

There is thus a *category* **Ring** whose objects are commutative rings and whose morphisms are ring-homomorphisms.

The philosophy of Grothendieck, as expounded in his EGA [GD], is that one should always do things in a relative context. This means that instead of working with objects, one should work with *morphisms* of objects. Motivated by this, we introduce:

Definition 1.5 Given a ring A, an ***A*-algebra** is a ring R together with a morphism of rings (a **structure morphism**) $A \to R$. There is a category of A-algebras, where a morphism between A-algebras is a ring-homomorphism that is required to commute with the structure morphisms.

So if R is an A-algebra, then R is not only a ring, but there is a way to multiply elements of R by elements of A (namely, to multiply $a \in A$ with $r \in R$, take the image of a in R, and multiply that by r). For instance, any ring is an algebra over any subring.

We can think of an A-algebra as an arrow $A \to R$, and a morphism from $A \to R$ to $A \to S$ as a commutative diagram

$$\begin{tikzcd}
R \arrow[rr] & & S \\
& A \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

This is a special case of the *undercategory* construction.

If B is an A-algebra and C a B-algebra, then C is an A-algebra in a natural way. Namely, by assumption we are given morphisms of rings $A \to B$ and $B \to C$, so composing them gives the structure morphism $A \to C$ of C as an A-algebra.

Example 1.6 Every ring is a $\mathbb{Z}$-algebra in a natural and unique way. There is a unique map (of rings) $\mathbb{Z} \to R$ for any ring R because a ring-homomorphism is required to preserve the identity. In fact, $\mathbb{Z}$ is the *initial object* in the category of rings: this is a restatement of the preceding discussion.

Example 1.7 If R is a ring, the polynomial ring $R[x]$ is an R-algebra in a natural manner. Each element of R is naturally viewed as a "constant polynomial."

Example 1.8 $\mathbb{C}$ is an $\mathbb{R}$-algebra.

Here is an example that generalizes the case of the polynomial ring.

Example 1.9 If R is a ring and G a commutative monoid,[1] then the set $R[G]$ of formal finite sums $\sum r_i g_i$ with $r_i \in R, g_i \in G$ is a commutative ring, called the **moniod ring** or **group ring** when G is a group. Alternatively, we can think of elements of $R[G]$ as infinite sums $\sum_{g \in G} r_g g$ with R-coefficients, such that almost all the r_g are zero. We can define the multiplication law such that

$$\left(\sum r_g g\right)\left(\sum s_g g\right) = \sum_h \left(\sum_{gg'=h} r_g s_{g'} \right) h.$$

This process is called *convolution.* We can think of the multiplication law as extended the group multiplication law (because the product of the ring-elements corresponding to g, g' is the ring element corresponding to $gg' \in G$).

The case of $G = \mathbb{Z}_{\geq 0}$ is the polynomial ring. In some cases, we can extend this notion to formal infinite sums, as in the case of the formal power series ring; see **??** below.

Exercise 1.4 The ring $\mathbb{Z}$ is an *initial object* in the category of rings. That is, for any ring R, there is a *unique* morphism of rings $\mathbb{Z} \to R$. We discussed this briefly earlier; show more generally that A is the initial object in the category of A-algebras for any ring A.

Exercise 1.5 The ring where $0 = 1$ (the **zero ring**) is a *final object* in the category of rings. That is, every ring admits a unique map to the zero ring.

Exercise 1.6 Let $\mathcal{C}$ be a category and $F : \mathcal{C} \to \mathbf{Sets}$ a covariant functor. Recall that F is said to be **corepresentable** if F is naturally isomorphic to $X \to \mathrm{Hom}_{\mathcal{C}}(U, X)$ for some object $U \in \mathcal{C}$. For instance, the functor sending everything to a one-point set is corepresentable if and only if $\mathcal{C}$ admits an initial object.

Prove that the functor **Rings** → **Sets** assigning to each ring its underlying set is representable. (Hint: use a suitable polynomial ring.)

[1] That is, there is a commutative multiplication on G with an identity element, but not necessarily with inverses.

The category of rings is both complete and cocomplete. To show this in full will take more work, but we can here describe what certain cases (including all limits) look like. As we saw in **??** 1.6, the forgetful functor **Rings** → **Sets** is corepresentable. Thus, if we want to look for limits in the category of rings, here is the approach we should follow: we should take the limit first of the underlying sets, and then place a ring structure on it in some natural way.

Example 1.10 (Products) The **product** of two rings R_1, R_2 is the set-theoretic product $R_1 \times R_2$ with the multiplication law $(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$. It is easy to see that this is a product in the category of rings. More generally, we can easily define the product of any collection of rings.

To describe the coproduct is more difficult: this will be given by the *tensor product* to be developed in the sequel.

Example 1.11 (Equalizers) Let $f, g : R \rightrightarrows S$ be two ring-homomorphisms. Then we can construct the **equalizer** of f, g as the subring of R consisting of elements $x \in R$ such that $f(x) = g(x)$. This is clearly a subring, and one sees quickly that it is the equalizer in the category of rings.

As a result, we find:

Proposition 1.12 **Rings** *is complete.*

As we said, we will not yet show that **Rings** is cocomplete. But we can describe filtered colimits. In fact, filtered colimits will be constructed just as in the set-theoretic fashion. That is, the forgetful functor **Rings** → **Sets** commutes with *filtered* colimits (though not with general colimits).

Example 1.13 (Filtered colimits) Let I be a filtering category, $F : I \to \mathbf{Rings}$ a functor. We can construct $\varinjlim_I F$ as follows. An object is an element (x, i) for $i \in I$ and $x \in F(i)$, modulo equivalence; we say that (x, i) and (y, j) are equivalent if there is a $k \in I$ with maps $i \to k, j \to k$ sending x, y to the same thing in the ring $F(k)$.

To multiply (x, i) and (y, j), we find some $k \in I$ receiving maps from i, j, and replace x, y with elements of $F(k)$. Then we multiply those two in $F(k)$. One easily sees that this is a well-defined multiplication law that induces a ring structure, and that what we have described is in fact the filtered colimit.

1.3 Ideals

An *ideal* in a ring is analogous to a normal subgroup of a group. As we shall see, one may quotient by ideals just as one quotients by normal subgroups. The idea is that one wishes to have a suitable *equivalence relation* on a ring R such that the relevant maps (addition and multiplication) factor through this equivalence relation. It is easy to check that any such relation arises via an ideal.

Definition 1.14 Let R be a ring. An **ideal** in R is a subset $I \subset R$ that satisfies the following.

1. $0 \in I$.
2. If $x, y \in I$, then $x + y \in I$.
3. If $x \in I$ and $y \in R$, then $xy \in I$.

There is a simple way of obtaining ideals, which we now describe. Given elements $x_1, \ldots, x_n \in R$, we denote by $(x_1, \ldots, x_n) \subset R$ the subset of linear combinations $\sum r_i x_i$, where $r_i \in R$. This is clearly an ideal, and in fact the smallest one containing all x_i. It is called the ideal **generated** by $x_1, \ldots, x_n$. A **principal ideal** (x) is one generated by a single $x \in R$.

Example 1.15 Ideals generalize the notion of divisibility. Note that in $\mathbb{Z}$, the set of elements divisible by $n \in \mathbb{Z}$ forms the ideal $I = n\mathbb{Z} = (n)$. We shall see that every ideal in $\mathbb{Z}$ is of this form: $\mathbb{Z}$ is a *principal ideal domain.*

Indeed, one can think of an ideal as axiomatizing the notions that "divisibility" ought to satisfy. Clearly, if two elements are divisible by something, then their sum and product should also be divisible by it. More generally, if an element is divisible by something, then the product of that element with anything else should also be divisible. In general, we will extend (in the chapter on Dedekind domains) much of the ordinary arithmetic with $\mathbb{Z}$ to arithmetic with *ideals* (e.g. unique factorization).

Example 1.16 We saw in **??** 1.3 that if X is a set and R a ring, then the set R^X of functions $X \to R$ is naturally a ring. If $Y \subset X$ is a subset, then the subset of functions vanishing on Y is an ideal.

Exercise 1.7 Show that the ideal $(2, 1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$ is not principal.

1.4 Operations on ideals

There are a number of simple operations that one may do with ideals, which we now describe.

Definition 1.17 The sum $I + J$ of two ideals $I, J \subset R$ is defined as the set of sums

$$\{x + y : x \in I, y \in J\}.$$

Definition 1.18 The product IJ of two ideals $I, J \subset R$ is defined as the smallest ideal containing the products xy for all $x \in I, y \in J$. This is just the set

$$\left\{\sum x_i y_i : x_i \in I, y_i \in J\right\}.$$

We leave the basic verification of properties as an exercise:

Exercise 1.8 Given ideals $I, J \subset R$, verify the following.

1. $I + J$ is the smallest ideal containing I and J.
2. IJ is contained in I and J.
3. $I \cap J$ is an ideal.

Example 1.19 In $\mathbb{Z}$, we have the following for any m, n.

1. $(m) + (n) = (\gcd\{m, n\})$,
2. $(m)(n) = (mn)$,
3. $(m) \cap (n) = (\mathrm{lcm}\{m, n\})$.

Proposition 1.20 *For ideals $I, J, K \subset R$, we have the following.*

1. *Distributivity: $I(J + K) = IJ + IK$.*
2. *$I \cap (J + K) = I \cap J + I \cap K$ if $I \supset J$ or $I \supset K$.*
3. *If $I + J = R$, $I \cap J = IJ$.*

Proof. 1 and 2 are clear. For 3, note that $(I+J)(I \cap J) = I(I \cap J) + J(I \cap J) \subset IJ$. Since $IJ \subset I \cap J$, the result follows. ▲

EXERCISE 1.9 There is a *contravariant* functor **Rings** → **Sets** that sends each ring to its set of ideals. Given a map $f : R \to S$ and an ideal $I \subset S$, we define an ideal $f^{-1}(I) \subset R$; this defines the functoriality. This functor is not representable, as it does not send the initial object in **Rings** to the one-element set. We will later use a *subfunctor* of this functor, the Spec construction, when we replace ideals with "prime" ideals.

1.5 Quotient rings

We next describe a procedure for producing new rings from old ones. If R is a ring and $I \subset R$ an ideal, then the quotient group R/I is a ring in its own right. If $a+I, b+I$ are two cosets, then the multiplication is $(a+I)(b+I) = ab+I$. It is easy to check that this does not depend on the coset representatives a, b. In other words, as mentioned earlier, the arithmetic operations on R *factor* through the equivalence relation defined by I.

As one easily checks, this becomes to a multiplication

$$R/I \times R/I \to R/I$$

which is commutative and associative, and whose identity element is $1+I$. In particular, R/I is a ring, under multiplication $(a+I)(b+I) = ab+I$.

Definition 1.21 R/I is called the **quotient ring** by the ideal I.

The process is analogous to quotienting a group by a normal subgroup: again, the point is that the equivalence relation induced on the algebraic structure—either the group or the ring—by the subgroup (or ideal)—is compatible with the algebraic structure, which thus descends to the quotient.

The reduction map $\phi \colon R \to R/I$ is a ring-homomorphism with a *universal property.* Namely, for any ring B, there is a map

$$\mathrm{Hom}(R/I, B) \to \mathrm{Hom}(R, B)$$

on the hom-sets by composing with the ring-homomorphism ϕ; this map is injective and the image consists of all homomorphisms $R \to B$ which vanish on I. Stated alternatively, to map out of R/I (into some ring B) is the same thing as mapping out of R while killing the ideal $I \subset R$.

This is best thought out for oneself, but here is the detailed justification. The reason is that any map $R/I \to B$ pulls back to a map $R \to R/I \to B$ which annihilates I since $R \to R/I$ annihilates I. Conversely, if we have a map

$$f : R \to B$$

killing I, then we can define $R/I \to B$ by sending $a+I$ to $f(a)$; this is uniquely defined since f annihilates I.

EXERCISE 1.10 If R is a commutative ring, an element $e \in R$ is said to be **idempotent** if $e^2 = e$. Define a covariant functor **Rings** → **Sets** sending a ring to its idempotents. Prove that it is corepresentable. (Answer: the corepresenting object is $\mathbb{Z}[X]/(X - X^2)$.)

EXERCISE 1.11 Show that the functor assigning to each ring the set of elements annihilated by 2 is corepresentable.

EXERCISE 1.12 If $I \subset J \subset R$, then J/I is an ideal of R/I, and there is a canonical isomorphism

$$(R/I)/(J/I) \simeq R/J.$$

1.6 Zerodivisors

Let R be a commutative ring.

Definition 1.22 If $r \in R$, then r is called a **zerodivisor** if there is $s \in R, s \neq 0$ with $sr = 0$. Otherwise r is called a **nonzerodivisor.**

As an example, we prove a basic result on the zerodivisors in a polynomial ring.

Proposition 1.23 *Let $A = R[x]$. Let $f = a_n x^n + \dots + a_0 \in A$. If there is a non-zero polynomial $g \in A$ such that $fg = 0$, then there exists $r \in R \smallsetminus \{0\}$ such that $f \cdot r = 0$.*

So all the coefficients are zerodivisors.

Proof. Choose g to be of minimal degree, with leading coefficient bx^d. We may assume that $d > 0$. Then $f \cdot b \neq 0$, lest we contradict minimality of g. We must have $a_i g \neq 0$ for some i. To see this, assume that $a_i \cdot g = 0$, then $a_i b = 0$ for all i and then $fb = 0$. Now pick j to be the largest integer such that $a_j g \neq 0$. Then $0 = fg = (a_0 + a_1 x + \cdots a_j x^j)g$, and looking at the leading coefficient, we get $a_j b = 0$. So $\deg(a_j g) < d$. But then $f \cdot (a_j g) = 0$, contradicting minimality of g. ▲

Exercise 1.13 The product of two nonzerodivisors is a nonzerodivisor, and the product of two zerodivisors is a zerodivisor. It is, however, not necessarily true that the *sum* of two zerodivisors is a zerodivisor.

§2 Further examples

We now illustrate a few important examples of commutative rings. The section is in large measure an advertisement for why one might care about commutative algebra; nonetheless, the reader is encouraged at least to skim this section.

2.1 Rings of holomorphic functions

The following subsection may be omitted without impairing understanding.

There is a fruitful analogy in number theory between the rings $\mathbb{Z}$ and $\mathbb{C}[t]$, the latter being the polynomial ring over $\mathbb{C}$ in one variable (**??** 1.1). Why are they analogous? Both of these rings have a theory of unique factorization: that is, factorization into primes or irreducible polynomials. (In the latter, the irreducible polynomials have degree one.) Indeed we know:

1. Any nonzero integer factors as a product of primes (possibly times -1).
2. Any nonzero polynomial factors as a product of an element of $\mathbb{C}^* = \mathbb{C} - \{0\}$ and polynomials of the form $t - a, a \in \mathbb{C}$.

There is another way of thinking of $\mathbb{C}[t]$ in terms of complex analysis. This is equal to the ring of holomorphic functions on $\mathbb{C}$ which are meromorphic at infinity. Alternatively, consider the Riemann sphere $\mathbb{C} \cup \{\infty\}$; then the ring $\mathbb{C}[t]$ consists of meromorphic functions on the sphere whose poles (if any) are at ∞.

This description admits generalizations. Let X be a Riemann surface. (Example: take the complex numbers modulo a lattice, i.e. an elliptic curve.) Suppose that $x \in X$. Define R_x to be the ring of meromorphic functions on X which are allowed poles only at x (so are everywhere else holomorphic).

Example 2.1 Fix the notations of the previous discussion. Fix $y \neq x \in X$. Let R_x be the ring of meromorphic functions on the Riemann surface X which are holomorphic on $X - \{x\}$, as before. Then the collection of functions that vanish at y forms an *ideal* in R_x.

There are lots of other ideals. For instance, fix two points $y_0, y_1 \neq x$; we look at the ideal of R_x that vanish at both y_0, y_1.

For any Riemann surface X, the conclusion of Dedekind's theorem (??) applies. In other words, the ring R_x as defined in the example admits unique factorization of ideals. We shall call such rings **Dedekind domains** in the future.

Example 2.2 Keep the preceding notation.

Let $f \in R_x$, nonzero. By definition, f may have a pole at x, but no poles elsewhere. f vanishes at finitely many points $y_1, \dots, y_m$. When X was the Riemann sphere, knowing the zeros of f told us something about f. Indeed, in this case f is just a polynomial, and we have a nice factorization of f into functions in R_x that vanish only at one point. In general Riemann surfaces, this is not generally possible. This failure turns out to be very interesting.

Let $X = \mathbb{C}/\Lambda$ be an elliptic curve (for $\Lambda \subset \mathbb{C}^2$ a lattice), and suppose $x = 0$. Suppose we are given $y_1, y_2, \dots, y_m \in X$ that are nonzero; we ask whether there exists a function $f \in R_x$ having simple zeros at $y_1, \dots, y_m$ and nowhere else. The answer is interesting, and turns out to recover the group structure on the lattice.

Proposition 2.3 *A function $f \in R_x$ with simple zeros only at the $\{y_i\}$ exists if and only if $y_1 + y_2 + \cdots + y_n = 0$ (modulo Λ).*

So this problem of finding a function with specified zeros is equivalent to checking that the specific zeros add up to zero with the group structure.

In any case, there might not be such a nice function, but we have at least an ideal I of functions that have zeros (not necessarily simple) at $y_1, \dots, y_n$. This ideal has unique factorization into the ideals of functions vanishing at y_1, functions vanishing at y_2, so on.

2.2 Ideals and varieties

We saw in the previous subsection that ideals can be thought of as the vanishing of functions. This, like divisibility, is another interpretation, which is particularly interesting in algebraic geometry.

Recall the ring $\mathbb{C}[t]$ of complex polynomials discussed in the last subsection. More generally, if R is a ring, we saw in **??** 1.1 that the set $R[t]$ of polynomials with coefficients in R is a ring. This is a construction that can be iterated to get a polynomial ring in several variables over R.

Example 2.4 Consider the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$. Recall that before we thought of the ring $\mathbb{C}[t]$ as a ring of meromorphic functions. Similarly each element of the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$ gives a function $\mathbb{C}^n \to \mathbb{C}$; we can think of the polynomial ring as sitting inside the ring of all functions $\mathbb{C}^n \to \mathbb{C}$.

A question you might ask: What are the ideals in this ring? One way to get an ideal is to pick a point $x = (x_1, \dots, x_n) \in \mathbb{C}^n$; consider the collection of all functions $f \in \mathbb{C}[x_1, \dots, x_n]$ which vanish on x; by the usual argument, this is an ideal.

There are, of course, other ideals. More generally, if $Y \subset \mathbb{C}^n$, consider the collection of polynomial functions $f : \mathbb{C}^n \to \mathbb{C}$ such that $f \equiv 0$ on Y. This is easily seen to be an ideal in the polynomial ring. We thus have a way of taking a subset of $\mathbb{C}^n$ and producing an ideal. Let I_Y be the ideal corresponding to Y.

This construction is not injective. One can have $Y \neq Y'$ but $I_Y = I_{Y'}$. For instance, if Y is dense in $\mathbb{C}^n$, then $I_Y = (0)$, because the only way a continuous function on $\mathbb{C}^n$ can vanish on Y is for it to be zero.

There is a much closer connection in the other direction. You might ask whether all ideals can arise in this way. The quick answer is no—not even when $n = 1$. The ideal $(x^2) \subset \mathbb{C}[x]$ cannot be obtained in this way. It is easy to see that the only way we could get this as I_Y is for $Y = \{0\}$, but I_Y in this case is just (x), not (x^2). What's going wrong in this example is that (x^2) is not a *radical* ideal.

Definition 2.5 An ideal $I \subset R$ is **radical** if whenever $x^2 \in I$, then $x \in I$.

The ideals I_Y in the polynomial ring are all radical. This is obvious. You might now ask whether this is the only obstruction. We now state a theorem that we will prove later.

Theorem 2.6 (Hilbert's Nullstellensatz) *If $I \subset \mathbb{C}[x_1, \dots, x_n]$ is a radical ideal, then $I = I_Y$ for some $Y \subset \mathbb{C}^n$. In fact, the canonical choice of Y is the set of points where all the functions in Y vanish.*[2]

This will be one of the highlights of the present course. But before we can get to it, there is much to do.

Exercise 1.14 Assuming the Nullstellensatz, show that any *maximal* ideal in the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$ for $a_1, \dots, a_n \in \mathbb{C}$. An ideal of a ring is called **maximal** if the only ideal that contains it is the whole ring (and it itself is not the whole ring).

As a corollary, deduce that if $I \subset \mathbb{C}[x_1, \dots, x_n]$ is a proper ideal (an ideal is called **proper** if it is not equal to the entire ring), then there exists $(x_1, \dots, x_n) \in \mathbb{C}^n$ such that every polynomial in I vanishes on the point $(x_1, \dots, x_n)$. This is called the **weak Nullstellensatz.**

§3 Modules over a commutative ring

We will now establish some basic terminology about modules.

3.1 Definitions

Suppose R is a commutative ring.

Definition 3.1 An R**-module** M is an abelian group M with a map $R \times M \to M$ (written $(a, m) \to am$) such that

M 1 $(ab)m = a(bm)$ for $a, b \in R, m \in M$, i.e. there is an associative law.

M 2 $1m = m$; the unit acts as the identity.

M 3 There are distributive laws on both sides: $(a + b)m = am + bm$ and $a(m + n) = am + an$ for $a, b \in R,\ m, n \in M$.

Another definition can be given as follows.

Definition 3.2 If M is an abelian group, $End(M)$ is the set of homomorphisms $f : M \to M$. This can be made into a (noncommutative) *ring.*[3] Addition is defined pointwise, and multiplication is by composition. The identity element is the identity function 1_M.

We made the following definition earlier for commutative rings, but for clarity we re-state it:

[2] Such a subset is called an algebraic variety.

[3] A noncommutative ring is one satisfying all the usual axioms of a ring except that multiplication is not required to be commutative.

Definition 3.3 If R, R' are rings (possibly noncommutative) then a function $f : R \to R'$ is a **ring-homomorphism** or **morphism** if it is compatible with the ring structures, i.e

1. $f(x + y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$
3. $f(1) = 1$.

The last condition is not redundant because otherwise the zero map would automatically be a homomorphism. The alternative definition of a module is left to the reader in the following exercise.

Exercise 1.15 If R is a ring and $R \to \mathit{End}(M)$ a homomorphism, then M is made into an R-module, and vice versa.

Example 3.4 If R is a ring, then R is an R-module by multiplication on the left.

Example 3.5 A $\mathbb{Z}$-module is the same thing as an abelian group.

Definition 3.6 If M is an R-module, a subset $M_0 \subset M$ is a **submodule** if it is a subgroup (closed under addition and inversion) and is closed under multiplication by elements of R, i.e. $aM_0 \subset M_0$ for $a \in R$. A submodule is a module in its own right. If $M_0 \subset M$ is a submodule, there is a commutative diagram:

$$\begin{tikzcd}
R \times M_0 \arrow[r] \arrow[d] & M_0 . \arrow[d] \\
R \times M \arrow[r] & M
\end{tikzcd}$$

Here the horizontal maps are multiplication.

Example 3.7 Let R be a (**commutative**) ring; then an ideal in R is the same thing as a submodule of R.

Example 3.8 If A is a ring, an A-algebra is an A-module in an obvious way. More generally, if A is a ring and R is an A-algebra, any R-module becomes an A-module by pulling back the multiplication map via $A \to R$.

Dual to submodules is the notion of a *quotient module*, which we define next:

Definition 3.9 Suppose M is an R-module and M_0 a submodule. Then the abelian group M/M_0 (of cosets) is an R-module, called the **quotient module** by M_0.

Multiplication is as follows. If one has a coset $x + M_0 \in M/M_0$, one multiplies this by $a \in R$ to get the coset $ax + M_0$. This does not depend on the coset representative.

3.2 The categorical structure on modules

So far, we have talked about modules, but we have not discussed morphisms between modules, and have yet to make the class of modules over a given ring into a category. This we do next.

Let us thus introduce a few more basic notions.

Definition 3.10 Let R be a ring. Suppose M, N are R-modules. A map $f : M \to N$ is a **module-homomorphism** if it preserves all the relevant structures. Namely, it must be a homomorphism of abelian groups, $f(x + y) = f(x) + f(y)$, and second it must preserve multiplication:

$$f(ax) = af(x)$$

for $a \in R, x \in M$.

A simple way of getting plenty of module-homomorphisms is simply to consider multiplication by a fixed element of the ring.

Example 3.11 If $a \in R$, then multiplication by a is a module-homomorphism $M \stackrel{a}{\to} M$ for any R-module M.[4] Such homomorphisms are called **homotheties.**

If $M \stackrel{f}{\to} N$ and $N \stackrel{g}{\to} P$ are module-homomorphisms, their composite $M \stackrel{g \circ f}{\to} P$ clearly is too. Thus, for any commutative ring R, the class of R-modules and module-homomorphisms forms a **category**.

Exercise 1.16 The initial object in this category is the zero module, and this is also the final object.

In general, a category where the initial object and final object are the same (that is, isomorphic) is called a *pointed category.* The common object is called the *zero object.* In a pointed category $\mathcal{C}$, there is a morphism $X \to Y$ for any two objects $X, Y \in \mathcal{C}$: if $*$ is the zero object, then we can take $X \to * \to Y$. This is well-defined and is called the *zero morphism.* One can easily show that the composition (on the left or the right) of a zero morphism is a zero morphism (between a possibly different set of objects).

In the case of the category of modules, the zero object is clearly the zero module, and the zero morphism $M \to N$ sends $m \mapsto 0$ for each $m \in M$.

Definition 3.12 Let $f : M \to N$ be a module homomorphism. In this case, the **kernel** $\ker f$ of f is the set of elements $m \in M$ with $f(m) = 0$. This is a submodule of M, as is easy to see.

The **image** $\operatorname{Im} f$ of f (the set-theoretic image, i.e. the collection of all $f(x), x \in M$) is also a submodule of N.

The **cokernel** of f is defined by $N/\operatorname{Im}(f)$.

Exercise 1.17 The universal property of the kernel is as follows. Let $M \stackrel{f}{\to} N$ be a morphism with kernel $K \subset M$. Let $T \to M$ be a map. Then $T \to M$ factors through the kernel $K \to M$ if and only if its composition with f (a morphism $T \to N$) is zero. That is, an arrow $T \to K$ exists in the diagram (where the dotted arrow indicates we are looking for a map that need not exist)

$$\begin{tikzcd} & T \arrow[ld, dashed] \arrow[d] & \\ K \arrow[r] & M \arrow[r, "f"] & N \end{tikzcd}$$

if and only if the composite $T \to N$ is zero. In particular, if we think of the hom-sets as abelian groups (i.e. $\mathbb{Z}$-modules)

$$\operatorname{Hom}_R(T, K) = \ker \left(\operatorname{Hom}_R(T, M) \to \operatorname{Hom}_R(T, N) \right).$$

In other words, one may think of the kernel as follows. If $X \stackrel{f}{\to} Y$ is a morphism, then the kernel $\ker(f)$ is the equalizer of f and the zero morphism $X \stackrel{0}{\to} Y$.

Exercise 1.18 What is the universal property of the cokernel?

Exercise 1.19 On the category of modules, the functor assigning to each module M its underlying set is corepresentable (cf. **??** 1.6). What is the corepresenting object?

We shall now introduce the notions of *direct sum* and *direct product.* Let I be a set, and suppose that for each $i \in I$, we are given an R-module M_i.

[4] When one considers modules over noncommutative rings, this is no longer true.

Definition 3.13 The **direct product** $\prod M_i$ is set-theoretically the cartesian product. It is given the structure of an R-module by addition and multiplication pointwise on each factor.

Definition 3.14 The **direct sum** $\bigoplus_I M_i$ is the set of elements in the direct product such that all but finitely many entries are zero. The direct sum is a submodule of the direct product.

Example 3.15 The direct product is a product in the category of modules, and the direct sum is a coproduct. This is easy to verify: given maps $f_i : M \to M_i$, then we get get a unique map $f : M \to \prod M_i$ by taking the product in the category of sets. The case of a coproduct is dual: given maps $g_i : M_i \to N$, then we get a map $\bigoplus M_i \to N$ by taking the *sum* g of the g_i: on a family $(m_i) \in \bigoplus M_i$, we take $g(m_i) = \sum_I g_i(m_i)$; this is well-defined as almost all the m_i are zero.

Example 3.15 shows that the category of modules over a fixed commutative ring has products and coproducts. In fact, the category of modules is both complete and cocomplete (see **??** for the definition). To see this, it suffices to show that (by **??** and its dual) that this category admits equalizers and coequalizers.

The equalizer of two maps

$$M \overset{f,g}{\rightrightarrows} N$$

is easily checked to be the submodule of M consisting of $m \in M$ such that $f(m) = g(m)$, or, in other words, the kernel of $f - g$. The coequalizer of these two maps is the quotient module of N by the submodule $\{f(m) - g(m), m \in M\}$, or, in other words, the cokernel of $f - g$.

Thus:

Proposition 3.16 *If R is a ring, the category of R-modules is complete and cocomplete.*

Example 3.17 Note that limits in the category of R-modules are calculated in the same way as they are for sets, but colimits are not. That is, the functor from R-modules to **Sets**, the forgetful functor, preserves limits but not colimits. Indeed, we will see that the forgetful functor is a right adjoint (Proposition 6.3), which implies it preserves limits (by **??**).

3.3 Exactness

Finally, we introduce the notion of *exactness.*

Definition 3.18 Let $f : M \to N$ be a morphism of R-modules. Suppose $g : N \to P$ is another morphism of R-modules.

The pair of maps is a **complex** if $g \circ f = 0 : M \to N \to P$. This is equivalent to the condition that $\mathrm{Im}(f) \subset \ker(g)$.

This complex is **exact** (or exact at N) if $\mathrm{Im}(f) = \ker(g)$. In other words, anything that is killed when mapped to P actually comes from something in M.

We shall often write pairs of maps as sequences

$$A \xrightarrow{f} B \xrightarrow{g} C$$

and say that the sequence is exact if the pair of maps is, as in Definition 3.18. A longer (possibly infinite) sequence of modules

$$A_0 \to A_1 \to A_2 \to \dots$$

will be called a **complex** if each set of three consecutive terms is a complex, and **exact** if it is exact at each step.

Example 3.19 The sequence $0 \to A \xrightarrow{f} B$ is exact if and only if the map f is injective. Similarly, $A \xrightarrow{f} B \to 0$ is exact if and only if f is surjective. Thus, $0 \to A \xrightarrow{f} B \to 0$ is exact if and only if f is an isomorphism.

One typically sees this definition applied to sequences of the form

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0,$$

which, if exact, is called a **short exact sequence**. Exactness here means that f is injective, g is surjective, and f maps onto the kernel of g. So M'' can be thought of as the quotient M/M'.

Example 3.20 Conversely, if M is a module and $M' \subset M$ a submodule, then there is a short exact sequence

$$0 \to M' \to M \to M/M' \to 0.$$

So every short exact sequence is of this form.

Suppose F is a functor from the category of R-modules to the category of S-modules, where R, S are rings. Then:

Definition 3.21

1. F is called **additive** if F preserves direct sums.
2. F is called **exact** if F is additive and preserves exact sequences.
3. F is called **left exact** if F is additive and preserves exact sequences of the form $0 \to M' \to M \to M''$. Equivalently, F preserves kernels.
4. F is **right exact** if F is additive and F preserves exact sequences of the form $M' \to M \to M'' \to 0$, i.e. F preserves cokernels.

The reader should note that much of homological algebra can be developed using the more general setting of an *abelian category,* which axiomatizes much of the standard properties of the category of modules over a ring. Such a generalization turns out to be necessary when many natural categories, such as the category of chain complexes or the category of sheaves on a topological space, are not naturally categories of modules. We do not go into this here, cf. [ML98].

A functor F is exact if and only if it is both left and right exact. This actually requires proof, though it is not hard. Namely, right-exactness implies that F preserves cokernels. Left-exactness implies that F preserves kernels. F thus preserves images, as the image of a morphism is the kernel of its cokernel. So if

$$A \to B \to C$$

is a short exact sequence, then the kernel of the second map is equal to the image of the first; we have just seen that this is preserved under F.

From this, one can check that left-exactness is equivalent to requiring that F preserve finite limits (as an additive functor, F automatically preserves products, and we have just seen that F is left-exact iff it preserves kernels). Similarly, right-exactness is equivalent to requiring that F preserve finite colimits. So, in *any* category with finite limits and colimits, we can talk about right or left exactness of a functor, but the notion is used most often for categories with an additive structure (e.g. categories of modules over a ring).

Exercise 1.20 Suppose whenever $0 \to A' \to A \to A'' \to 0$ is short exact, then $FA' \to FA \to FA'' \to 0$ is exact. Prove that F is right-exact. So we get a slightly weaker criterion for right-exactness.

Do the same for left-exact functors.

3.4 Split exact sequences

Let $f : A \to B$ be a map of sets which is injective. Then there is a map $g : A \to B$ such that the composite $g \circ f : A \xrightarrow{f} B \xrightarrow{g} A$ is the identity. Namely, we define g to be the inverse of f on $f(A)$ and arbitrarily on $B - f(A)$. Conversely, if $f : A \to B$ admits an element $g : B \to A$ such that $g \circ f = 1_A$, then f is injective. This is easy to see, as any $a \in A$ can be "recovered" from $f(a)$ (by applying g).

In general, however, this observation does not generalize to arbitrary categories.

Definition 3.22 Let $\mathcal{C}$ be a category. A morphism $A \xrightarrow{f} B$ is called a **split injection** if there is $g : B \to A$ with $g \circ f = 1_A$.

Exercise 1.21 (General nonsense) Suppose $f : A \to B$ is a split injection. Show that f is a categorical monomorphism. (Idea: the map $\mathrm{Hom}(C, A) \to \mathrm{Hom}(C, B)$ becomes a split injection of sets thanks to g.)

TO BE ADDED: what is a categorical monomorphism? Maybe omit the exercise

In the category of sets, we have seen above that *any* monomorphism is a split injection. This is not true in other categories, in general.

Exercise 1.22 Consider the morphism $\mathbb{Z} \to \mathbb{Z}$ given by multiplication by 2. Show that this is not a split injection: no left inverse g can exist.

We are most interested in the case of modules over a ring.

Proposition 3.23 *A morphism $f : A \to B$ in the category of R-modules is a split injection if and only if:*

1. *f is injective.*
2. *$f(A)$ is a direct summand in B.*

The second condition means that there is a submodule $B' \subset B$ such that $B = B' \oplus f(A)$ (internal direct sum). In other words, $B = B' + f(A)$ and $B' \cap f(A) = \{0\}$.

Proof. Suppose the two conditions hold, and we have a module B' which is a complement to $f(A)$. Then we define a left inverse

$$B \xrightarrow{g} A$$

by letting $g|_{f(A)} = f^{-1}$ (note that f becomes an *isomorphism* $A \to f(A)$) and $g|_{B'} = 0$. It is easy to see that this is indeed a left inverse, though in general not a right inverse, as g is likely to be non-injective.

Conversely, suppose $f : A \to B$ admits a left inverse $g : B \to A$. The usual argument (as for sets) shows that f is injective. The essentially new observation is that $f(A)$ is a direct summand in B. To define the complement, we take $\ker(g) \subset B$. It is easy to see (as $g \circ f = 1_A$) that $\ker(g) \cap f(A) = \{0\}$. Moreover, $\ker(g) + f(A)$ fills B: given $b \in B$, it is easy to check that

$$b - f(g(b)) \in \ker(g).$$

Thus we find that the two conditions are satisfied. ▲

TO BE ADDED: further explanation, exactness of filtered colimits

3.5 The five lemma

The five lemma will be a useful tool for us in proving that maps are isomorphisms. Often this argument is used in inductive proofs. Namely, we will see that often "long exact sequences" (extending infinitely in one or both directions) arise from short exact sequences in a natural way. In such events, the five lemma will allow us to prove that certain morphisms are isomorphisms by induction on the dimension.

Theorem 3.24 *Suppose given a commutative diagram*

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & D \arrow[r] \arrow[d] & E \arrow[d] \\
A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & D' \arrow[r] & E'
\end{tikzcd}$$

such that the rows are exact and the four vertical maps $A \to A', B \to B', D \to D', E \to E'$ are isomorphisms. Then $C \to C'$ is an isomorphism.

This is the type of proof that goes by the name of "diagram-chasing," and is best thought out visually for oneself, even though we give a complete proof.

Proof. We have the diagram

$$\begin{tikzcd}
A \arrow[r, "k"] \arrow[d, "a"] & B \arrow[r, "l"] \arrow[d, "b"] & C \arrow[r, "m"] \arrow[d, "g"] & D \arrow[r, "n"] \arrow[d, "d"] & E \arrow[d, "e"] \\
F \arrow[r, "p"'] & G \arrow[r, "q"'] & H \arrow[r, "r"'] & I \arrow[r, "s"'] & J
\end{tikzcd}$$

▲

where the rows are exact at B, C, D, G, H, I and the squares commute. In addition, suppose that a, b, d, e are isomorphisms. We will show that g is an isomorphism.

We show that g is surjective:

Suppose that $h \in H$. Since d is surjective, there exists an element $d \in D$ such that $r(h) = d(d) \in I$. By the commutativity of the rightmost square, $s(r(h)) = e(n(d))$. The exactness at I means that $\operatorname{Im} r = \ker s$, so hence $e(n(d)) = s(r(h)) = 0$. Because e is injective, $n(d) = 0$. Then $d \in \ker(n) = \operatorname{Im}(m)$ by exactness at D. Therefore, there is some $c \in C$ such that $m(c) = d$. Now, $d(m(c)) = d(d) = r(h)$ and by the commutativity of squares, $d(m(c)) = r(g(c))$, so therefore $r(g(c)) = r(h)$. Since r is a homomorphism, $r(g(c) - h) = 0$. Hence $g(c) - h \in \ker r = \operatorname{Im} q$ by exactness at H.

Therefore, there exists $g \in G$ such that $q(g) = g(c) - h$. b is surjective, so there is some $b \in B$ such that $b(b) = g$ and hence $q(b(b)) = g(c) - h$. By the commutativity of squares, $q(b(b)) = g(l(b)) = g(c) - h$. Hence $h = g(c) - g(l(b)) = g(c - l(b))$, and therefore g is surjective.

So far, we've used that b and g are surjective, e is injective, and exactness at D, H, I.

We show that g is injective:

Suppose that $c \in C$ and $g(c) = 0$. Then $r(g(c)) = 0$, and by the commutativity of squares, $d(m(c)) = 0$. Since d is injective, $m(c) = 0$, so $c \in \ker m = \operatorname{Im} l$ by exactness at C. Therefore, there is $b \in B$ such that $l(b) = c$. Then $g(l(b)) = g(c) = 0$, and by the commutativity of squares, $q(b(b)) = 0$. Therefore, $b(b) \in \ker q$, and by exactness at G, $b(b) \in \ker q = \operatorname{Im} p$.

There is now $f \in F$ such that $p(f) = b(b)$. Since a is surjective, this means that there is $a \in A$ such that $f = a(a)$, so then $b(b) = p(a(a))$. By commutativity of squares, $b(b) = p(a(a)) = b(k(a))$, and hence $b(k(a) - b) = 0$. Since b is injective, we have $k(a) - b = 0$, so $k(a) = b$. Hence $b \in \operatorname{Im} k = \ker l$ by commutativity of squares, so $l(b) = 0$. However, we defined b to satisfy $l(b) = c$, so therefore $c = 0$ and hence g is injective.

Here, we used that a is surjective, b, d are injective, and exactness at B, C, G.

Putting the two statements together, we see that g is both surjective and injective, so g is an isomorphism. We only used that b, d are isomorphisms and that a is surjective, e is injective, so we can slightly weaken the hypotheses; injectivity of a and surjectivity of e were unnecessary.

§4 Ideals

The notion of an *ideal* has already been defined. Now we will introduce additional terminology related to the theory of ideals.

4.1 Prime and maximal ideals

Recall that the notion of an ideal generalizes that of divisibility. In elementary number theory, though, one finds that questions of divisibility basically reduce to questions about primes. The notion of a "prime ideal" is intended to generalize the familiar idea of a prime number.

Definition 4.1 An ideal $I \subset R$ is said to be **prime** if

P 1 $1 \notin I$ (by convention, 1 is not a prime number)

P 2 If $xy \in I$, either $x \in I$ or $y \in I$.

Example 4.2 If $R = \mathbb{Z}$ and $p \in R$, then $(p) \subset \mathbb{Z}$ is a prime ideal iff p or $-p$ is a prime number in $\mathbb{N}$ or if p is zero.

If R is any commutative ring, there are two obvious ideals. These obvious ones are the zero ideal (0) consisting only of the zero element, and the unit element (1) consisting of all of R.

Definition 4.3 An ideal $I \subset R$ is called **maximal**[5] if

M 1 $1 \notin I$

M 2 Any larger ideal contains 1 (i.e., is all of R).

So a maximal ideal is a maximal element in the partially ordered set of proper ideals (an ideal is **proper** if it does not contain 1).

Exercise 1.23 Find the maximal ideals in $\mathbb{C}[t]$.

Proposition 4.4 *A maximal ideal is prime.*

Proof. First, a maximal ideal does not contain 1.

Let $I \subset R$ be a maximal ideal. We need to show that if $xy \in I$, then one of $x, y \in I$. If $x \notin I$, then $(I, x) = I + (x)$ (the ideal generated by I and x) strictly contains I, so by maximality contains 1. In particular, $1 \in I + (x)$, so we can write

$$1 = a + xb$$

where $a \in I, b \in R$. Multiply both sides by y:

$$y = ay + bxy.$$ ▲

Both terms on the right here are in I ($a \in I$ and $xy \in I$), so we find that $y \in I$.

[5] Maximal with respect to not being the unit ideal.

Given a ring R, what can we say about the collection of ideals in R? There are two obvious ideals in R, namely (0) and (1). These are the same if and only if $0 = 1$, i.e. R is the zero ring. So for any nonzero commutative ring, we have at least two distinct ideals.

Next, we show that maximal ideals always *do* exist, except in the case of the zero ring.

Proposition 4.5 *Let R be a commutative ring. Let $I \subset R$ be a proper ideal. Then I is contained in a maximal ideal.*

Proof. This requires the axiom of choice in the form of Zorn's lemma. Let P be the collection of all ideals $J \subset R$ such that $I \subset J$ and $J \neq R$. Then P is a poset with respect to inclusion. P is nonempty because it contains I. Note that given a (nonempty) linearly ordered collection of ideals $J_\alpha \in P$, the union $\bigcup J_\alpha \subset R$ is an ideal: this is easily seen in view of the linear ordering (if $x, y \in \bigcup J_\alpha$, then both x, y belong to some J_γ, so $x + y \in J_\gamma$; multiplicative closure is even easier). The union is not all of R because it does not contain 1.

This implies that P has a maximal element by Zorn's lemma. This maximal element may be called $\mathfrak{M}$; it's a proper element containing I. I claim that $\mathfrak{M}$ is a maximal ideal, because if it were contained in a larger ideal, that would be in P (which cannot happen by maximality) unless it were all of R. ▲

Corollary 4.6 *Let R be a nonzero commutative ring. Then R has a maximal ideal.*

Proof. Apply the lemma to the zero ideal. ▲

Corollary 4.7 *Let R be a nonzero commutative ring. Then $x \in R$ is invertible if and only if it belongs to no maximal ideal $\mathfrak{m} \subset R$.*

Proof. Indeed, x is invertible if and only if $(x) = 1$. That is, if and only if (x) is not a proper ideal; now Proposition 4.5 finishes the argument. ▲

4.2 Fields and integral domains

Recall:

Definition 4.8 A commutative ring R is called a **field** if $1 \neq 0$ and for every $x \in R - \{0\}$ there exists an **inverse** $x^{-1} \in R$ such that $xx^{-1} = 1$.

This condition has an obvious interpretation in terms of ideals.

Proposition 4.9 *A commutative ring with $1 \neq 0$ is a field iff it has only the two ideals $(1), (0)$.*

Alternatively, a ring is a field if and only if (0) is a maximal ideal.

Proof. Assume R is a field. Suppose $I \subset R$. If $I \neq (0)$, then there is a nonzero $x \in I$. Then there is an inverse x^{-1}. We have $x^{-1}x = 1 \in I$, so $I = (1)$. In a field, there is thus no room for ideals other than (0) and (1).

To prove the converse, assume every ideal of R is (0) or (1). Then for each $x \in R$, $(x) = (0)$ or (1). If $x \neq 0$, the first cannot happen, so that means that the ideal generated by x is the unit ideal. So 1 is a multiple of x, implying that x has a multiplicative inverse. ▲

So fields also have an uninteresting ideal structure.

Corollary 4.10 *If R is a ring and $I \subset R$ is an ideal, then I is maximal if and only if R/I is a field.*

Proof. The basic point here is that there is a bijection between the ideals of R/I and ideals of R containing I.

Denote by $\phi : R \to R/I$ the reduction map. There is a construction mapping ideals of R/I to ideals of R. This sends an ideal in R/I to its inverse image. This is easily seen to map to ideals of R containing I. The map from ideals of R/I to ideals of R containing I is a bijection, as one checks easily.

It follows that R/I is a field precisely if R/I has precisely two ideals, i.e. precisely if there are precisely two ideals in R containing I. These ideals must be (1) and I, so this holds if and only if I is maximal. ▲

There is a similar characterization of prime ideals.

Definition 4.11 A commutative ring R is an **integral domain** if for all $x, y \in R$, $x \neq 0$ and $y \neq 0$ imply $xy \neq 0$.

Proposition 4.12 *An ideal $I \subset R$ is prime iff R/I is a domain.*

Exercise 1.24 Prove Proposition 4.12.

Any field is an integral domain. This is because in a field, nonzero elements are invertible, and the product of two invertible elements is invertible. This statement translates in ring theory to the statement that a maximal ideal is prime.

Finally, we include an example that describes what *some* of the prime ideals in a polynomial ring look like.

Example 4.13 Let R be a ring and P a prime ideal. We claim that $PR[x] \subset R[x]$ is a prime ideal.

Consider the map $\tilde{\phi} : R[x] \to (R/P)[x]$ with $\tilde{\phi}(a_0 + \cdots + a_n x^n) = (a_0 + P) + \cdots + (a_n + P)x^n$. This is clearly a homomorphism because $\phi : R \to R/P$ is, and its kernel consists of those polynomials $a_0 + \cdots + a_n x^n$ with $a_0, \ldots, a_n \in P$, which is precisely $P[x]$. Thus $R[x]/P[x] \simeq (R/P)[x]$, which is an integral domain because R/P is an integral domain. Thus $P[x]$ is a prime ideal.

However, if P is a maximal ideal, then $P[x]$ is never a maximal ideal because the ideal $P[x] + (x)$ (the polynomials with constant term in P) always strictly contains $P[x]$ (because if $x \in P[x]$ then $1 \in P$, which is impossible). Note that $P[x] + (x)$ is the kernel of the composition of $\tilde{\phi}$ with evaluation at 0, i.e $(\mathrm{ev}_0 \circ \tilde{\phi}) : R[x] \to R/P$, and this map is a surjection and R/P is a field, so that $P[x] + (x)$ is the maximal ideal in $R[x]$ containing $P[x]$.

Exercise 1.25 Let R be a domain. Consider the set of formal quotients $a/b, a, b \in R$ with $b \neq 0$. Define addition and multiplication using usual rules. Show that the resulting object $K(R)$ is a ring, and in fact a *field.* The natural map $R \to K(R)$, $r \to r/1$, has a universal property. If $R \hookrightarrow L$ is an injection of R into a field L, then there is a unique morphism $K(R) \to L$ of fields extending $R \to L$. This construction will be generalized when we consider *localization.* This construction is called the **quotient field.**

Note that a non-injective map $R \to L$ will *not* factor through the quotient field!

Exercise 1.26 Let R be a commutative ring. Then the **Jacobson radical** of R is the intersection $\bigcap \mathfrak{m}$ of all maximal ideals $\mathfrak{m} \subset R$. Prove that an element x is in the Jacobson radical if and only if $1 - yx$ is invertible for all $y \in R$.

4.3 Prime avoidance

The following fact will come in handy occasionally. We will, for instance, use it much later to show that an ideal consisting of zerodivisors on a module M is contained in associated prime.

Theorem 4.14 (Prime avoidance) *Let $I_1, \dots, I_n \subset R$ be ideals. Let $A \subset R$ be a subset which is closed under addition and multiplication. Assume that at least $n-2$ of the ideals are prime. If $A \subset I_1 \cup \dots \cup I_n$, then $A \subset I_j$ for some j.*

The result is frequently used in the following specific case: if an ideal I is contained in a finite union $\bigcup \mathfrak{p}_i$ of primes, then $I \subset \mathfrak{p}_i$ for some i.

Proof. Induct on n. If $n = 1$, the result is trivial. The case $n = 2$ is an easy argument: if $a_1 \in A \smallsetminus I_1$ and $a_2 \in A \smallsetminus I_2$, then $a_1 + a_2 \in A \smallsetminus (I_1 \cup I_2)$.

Now assume $n \geq 3$. We may assume that for each j, $A \not\subset I_1 \cup \dots \cup \hat{I_j} \cup \cdots I_n$.[6] Fix an element $a_j \in A \smallsetminus (I_1 \cup \dots \cup \hat{I_j} \cup \cdots I_n)$. Then this a_j must be contained in I_j since $A \subset \bigcup I_j$. Since $n \geq 3$, one of the I_j must be prime. We may assume that I_1 is prime. Define $x = a_1 + a_2 a_3 \cdots a_n$, which is an element of A. Let's show that x avoids *all* of the I_j. If $x \in I_1$, then $a_2 a_3 \cdots a_n \in I_1$, which contradicts the fact that $a_i \notin I_j$ for $i \neq j$ and that I_1 is prime. If $x \in I_j$ for $j \geq 2$. Then $a_1 \in I_j$, which contradicts $a_i \notin I_j$ for $i \neq j$. ▲

4.4 The Chinese remainder theorem

Let m, n be relatively prime integers. Suppose $a, b \in \mathbb{Z}$; then one can show that the two congruences $x \equiv a \mod m$ and $x \equiv b \mod n$ can be solved simultaneously in $x \in \mathbb{Z}$. The solution is unique, moreover, modulo mn. The Chinese remainder theorem generalizes this fact:

Theorem 4.15 (Chinese remainder theorem) *Let $I_1, \dots I_n$ be ideals in a ring R which satisfy $I_i + I_j = R$ for $i \neq j$. Then we have $I_1 \cap \dots \cap I_n = I_1 \dots I_n$ and the morphism of rings*

$$R \to \bigoplus R/I_i$$

is an epimorphism with kernel $I_1 \cap \dots \cap I_n$.

Proof. First, note that for any two ideals I_1 and I_2, we have $I_1 I_2 \subset I_1 \cap I_2$ and $(I_1 + I_2)(I_1 \cap I_2) \subset I_1 I_2$ (because any element of $I_1 + I_2$ multiplied by any element of $I_1 \cap I_2$ will clearly be a sum of products of elements from both I_1 and I_2). Thus, if I_1 and I_2 are coprime, i.e. $I_1 + I_2 = (1) = R$, then $(1)(I_1 \cap I_2) = (I_1 \cap I_2) \subset I_1 I_2 \subset I_1 \cap I_2$, so that $I_1 \cap I_2 = I_1 I_2$. This establishes the result for $n = 2$.

If the ideals $I_1, \dots, I_n$ are pairwise coprime and the result holds for $n-1$, then

$$\bigcap_{i=1}^{n-1} I_i = \prod_{i=1}^{n-1} I_i.$$

Because $I_n + I_i = (1)$ for each $1 \leq i \leq n-1$, there must be $x_i \in I_n$ and $y_i \in I_i$ such that $x_i + y_i = 1$. Thus, $z_n = \prod_{i=1}^{n-1} y_i = \prod_{i=1}^{n-1} (1 - x_i) \in \prod_{i=1}^{n-1} I_i$, and clearly $z_n + I_n = 1 + I_n$ since each $x_i \in I_n$. Thus $I_n + \prod_{i=1}^{n-1} I_i = I_n + \bigcap_{i=1}^{n-1} I_i = (1)$, and we can now apply the $n = 2$ case to conclude that $\bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i$.

Note that for any i, we can construct a z_i with $z_i \in I_j$ for $j \neq i$ and $z_i + I_i = 1 + I_i$ via the same procedure.

Define $\phi : R \to \bigoplus R/I_i$ by $\phi(a) = (a + I_1, \dots, a + I_n)$. The kernel of ϕ is $\bigcap_{i=1}^{n} I_i$, because $a + I_i = 0 + I_i$ iff $a \in I_i$, so that $\phi(a) = (0 + I_1, \dots, 0 + I_n)$ iff $a \in I_i$ for all i, that is, $a \in \bigcap_{i=1}^{n} I_i$. Combined with our previous result, the kernel of ϕ is $\prod_{i=1}^{n} I_i$.

Finally, recall that we constructed $z_i \in R$ such that $z_i + I_i = 1 + I_i$, and $z + I_j = 0 + I_j$ for all $j \neq i$, so that $\phi(z_i) = (0 + I_1, \dots, 1 + I_i, \dots, 0 + I_n)$. Thus, $\phi(a_1 z_1 + \dots + a_n z_n) = (a_1 + I_1, \dots, a_n + I_n)$ for all $a_i \in R$, so that ϕ is onto. By the first isomorphism theorem, we have that $R/I_1 \cdots I_n \simeq \bigoplus_{i=1}^{n} R/I_i$.

[6] The hat means omit I_j.

§5 Some special classes of domains

5.1 Principal ideal domains

Definition 5.1 A ring R is a **principal ideal domain** or **PID** if $R \neq 0$, R is not a field, R is a domain, and every ideal of R is principal.

These have the next simplest theory of ideals. Each ideal is very simple—it's principal—though there might be a lot of ideals.

Example 5.2 $\mathbb{Z}$ is a PID. The only nontrivial fact to check here is that:

Proposition 5.3 *Any nonzero ideal $I \subset \mathbb{Z}$ is principal.*

Proof. If $I = (0)$, then this is obvious. Else there is $n \in I - \{0\}$; we can assume $n > 0$. Choose $n \in I$ as small as possible and positive. Then I claim that the ideal I is generated by (n). Indeed, we have $(n) \subset I$ obviously. If $m \in I$ is another integer, then divide m by n, to find $m = nb + r$ for $r \in [0, n)$. We find that $r \in I$ and $0 \leq r < n$, so $r = 0$, and m is divisible by n. And $I \subset (n)$.

So $I = (n)$. ▲

A module M is said to be *finitely generated* if there exist elements $x_1, \dots, x_n \in M$ such that any element of M is a linear combination (with coefficients in R) of the x_i. (We shall define this more formally below.) One reason that PIDs are so convenient is:

Theorem 5.4 (Structure theorem) *If M is a finitely generated module over a principal ideal domain R, then M is isomorphic to a direct sum*

$$M \simeq \bigoplus_{i=1}^{n} R/a_i,$$

for various $a_i \in R$ (possibly zero).

TO BE ADDED: at some point, the proof should be added. This is important!

5.2 Unique factorization domains

The integers $\mathbb{Z}$ are especially nice because of the fundamental theorem of arithmetic, which states that every integer has a unique factorization into primes. This is not true for every integral domain.

Definition 5.5 An element of a domain R is **irreducible** if it cannot be written as the product of two non-unit elements of R.

Example 5.6 Consider the integral domain $\mathbb{Z}[\sqrt{-5}]$. We saw earlier that

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

which means that 6 was written as the product of two non-unit elements in different ways. $\mathbb{Z}[\sqrt{-5}]$ does not have unique factorization.

Definition 5.7 A domain R is a **unique factorization domain** or **UFD** if every non-unit $x \in R$ satisfies

1. x can be written as a product $x = p_1 p_2 \cdots p_n$ of irreducible elements $p_i \in R$

2. if $x = q_1q_2\cdots q_m$ where $q_i \in R$ are irreducible then the p_i and q_i are the same up to order and multiplication by units.

Example 5.8 $\mathbb{Z}$ is a UFD, while $\mathbb{Z}[\sqrt{-5}]$ is not. In fact, many of our favorite domains have unique factorization. We will prove that all PIDs are UFDs. In particular, in **??** 1.27 and **??** 1.28, we saw that $\mathbb{Z}[i]$ and $F[t]$ are PIDs, so they also have unique factorization.

Theorem 5.9 *Every principal ideal domain is a unique factorization domain.*

Proof. Suppose that R is a principal ideal domain and x is an element of R. We first demonstrate that x can be factored into irreducibles. If x is a unit or an irreducible, then we are done. Therefore, we can assume that x is reducible, which means that $x = x_1x_2$ for non-units $x_1, x_2 \in R$. If there are irreducible, then we are again done, so we assume that they are reducible and repeat this process. We need to show that this process terminates.

Suppose that this process continued infinitely. Then we have an infinite ascending chain of ideals, where all of the inclusions are proper: $(x) \subset (x_1) \subset (x_{11}) \subset \cdots \subset R$. We will show that this is impossible because any infinite ascending chain of ideals $I_1 \subset I_2 \subset \cdots \subset R$ of a principal ideal domain eventually becomes stationary, i.e. for some n, $I_k = I_n$ for $k \geq n$. Indeed, let $I = \bigcup_{i=1}^{\infty} I_i$. This is an ideal, so it is principally generated as $I = (a)$ for some a. Since $a \in I$, we must have $a \in I_N$ for some N, which means that the chain stabilizes after I_N.

It remains to prove that this factorization of x is unique. We induct on the number of irreducible factors n of x. If $n = 0$, then x is a unit, which has unique factorization up to units. Now, suppose that $x = p_1\cdots p_n = q_1\cdots q_m$ for some $m \geq n$. Since p_1 divides x, it must divide the product $q_1\cdots q_m$ and by irreducibility, one of the factors q_i. Reorder the q_i so that p_1 divides q_1. However, q_1 is irreducible, so this means that p_1 and q_1 are the same up to multiplication by a unit u. Canceling p_1 from each of the two factorizations, we see that $p_2\cdots p_n = uq_2\cdots q_m = q_2'\cdots q_m$. By induction, this shows that the factorization of x is unique up to order and multiplication by units. ▲

5.3 Euclidean domains

A euclidean domain is a special type of principal ideal domain. In practice, it will often happen that one has an explicit proof that a given domain is euclidean, while it might not be so trivial to prove that it is a UFD without the general implication below.

Definition 5.10 An integral domain R is a **euclidean domain** if there is a function $|\cdot| : R \to Z_{\geq 0}$ (called the norm) such that the following hold.

1. $|a| = 0$ iff $a = 0$.

2. For any nonzero $a, b \in R$ there exist $q, r \in R$ such that $b = aq + r$ and $|r| < |a|$.

In other words, the norm is compatible with division with remainder.

Theorem 5.11 *A euclidean domain is a principal ideal domain.*

Proof. Let R be an euclidean domain, $I \subset R$ and ideal, and b be the nonzero element of smallest norm in I. Suppose $a \in I$. Then we can write $a = qb + r$ with $0 \leq r < |b|$, but since b has minimal nonzero absolute value, $r = 0$ and $b|a$. Thus $I = (b)$ is principal. ▲

As we will see, this implies that any euclidean domain admits *unique factorization.*

Proposition 5.12 *Let F be a field. Then the polynomial ring $F[t]$ is a euclidean domain. In particular, it is a PID.*

Proof. We define **TO BE ADDED:** ▲

Exercise 1.27 Prove that $\mathbb{Z}[i]$ is principal. (Define the norm as $N(a+ib) = a^2 + b^2$.)

Exercise 1.28 Prove that the polynomial ring $F[t]$ for F a field is principal.

It is *not* true that a PID is necessarily euclidean. Nevertheless, it was shown in [Gre97] that the converse is "almost" true. Namely, [Gre97] defines the notion of an **almost euclidean domain.** A domain R is almost euclidean if there is a function $d : R \to \mathbb{Z}_{\geq 0}$ such that

1. $d(a) = 0$ iff $a = 0$.
2. $d(ab) \geq d(a)$ if $b \neq 0$.
3. If $a, b \in R - \{0\}$, then either $b \mid a$ or there is $r \in (a, b)$ with $d(r) < d(b)$.

It is easy to see by the same argument that an almost euclidean domain is a PID. (Indeed, let R be an almost euclidean domain, and $I \subset R$ a nonzero ideal. Then choose $x \in I - \{0\}$ such that $d(x)$ is minimal among elements in I. Then if $y \in I - \{0\}$, either $x \mid y$ or $(x, y) \subset I$ contains an element with smaller d. The latter cannot happen, so the former does.) However, in fact:

Proposition 5.13 ([Gre97]) *A domain is a PID if and only if it is almost euclidean.*

Proof. Indeed, let R be a PID. Then R is a UFD (Theorem 5.9), so for any $x \in R$, there is a factorization into prime elements, unique up to units. If x factors into n elements, we define $d(x) = n$; we set $d(0) = 0$. The first two conditions for an almost euclidean domain are then evident.

Let $x = p_1 \dots p_m$ and $y = q_1 \dots q_n$ be two elements of R, factored into irreducibles. Suppose $x \nmid y$. Choose a generator b of the (principal) ideal (x, y); then obviously $y \mid b$ so $d(y) \leq d(b)$. But if $d(y) = d(b)$, then the number of factors of y and b is the same, so $y \mid b$ would imply that y and b are associates. This is a contradiction, and implies that $d(y) < d(b)$.

Remark We have thus seen that a euclidean domain is a PID, and a PID is a UFD. Both converses, however, fail. By Gauss's lemma (**??**), the polynomial ring $\mathbb{Z}[X]$ has unique factorization, though the ideal $(2, X)$ is not principal.

In [Cam88], it is shown that the ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID but not euclidean (i.e. there is *no* euclidean norm on it).

According to [Cla11], sec. 8.3, Proposition 5.13 actually goes back to Hasse (and these norms are sometimes called "Dedekind-Hasse norms").

§6 Basic properties of modules

6.1 Free modules

We now describe a simple way of constructing modules over a ring, and an important class of modules.

Definition 6.1 A module M is **free** if it is isomorphic to $\bigoplus_I R$ for some index set I. The cardinality of I is called the **rank**.

Example 6.2 R is the simplest example of a free module.

Free modules have a *universal property.* Namely, recall that if M is an R-module, then to give a homomorphism

$$R \to M$$

is equivalent to giving an element $m \in M$ (the image of 1). By the universal product of the direct sum (which is the coproduct in the category of modules), it follows that to give a map

$$\bigoplus_I \to M$$

is the same as giving a map of *sets* $I \to M$. In particular:

Proposition 6.3 *The functor $I \mapsto \bigoplus_I R$ from* **Sets** *to R-modules is the* left adjoint *to the forgetful functor from R-modules to* **Sets***.*

The claim now is that the notion of "rank" is well-defined for a free module. To see this, we will have to use the notion of a *maximal ideal* (Definition 4.3) and Corollary 4.10. Indeed, suppose $\bigoplus_I R$ and $\bigoplus_J R$ are isomorphic; we must show that I and J have the same cardinality. Choose a maximal ideal $\mathfrak{m} \subset R$. Then, by applying the functor $M \to M/\mathfrak{m}M$, we find that the $R/\mathfrak{m}$-*vector spaces*

$$\bigoplus_I R/\mathfrak{m}, \quad \bigoplus_J R/\mathfrak{m}$$

are isomorphic. By linear algebra, I and J have the same cardinality.

Free modules have a bunch of nice properties. The first is that it is very easy to map out of a free module.

Example 6.4 Let I be an indexing set, and M an R-module. Then to give a morphism

$$\bigoplus_I R \to M$$

is equivalent to picking an element of M for each $i \in I$. Indeed, given such a collection of elements $\{m_i\}$, we send the generator of $\bigoplus_I R$ with a 1 in the ith spot and zero elsewhere to m_i.

Example 6.5 In a domain, every principal ideal (other than zero) is a free module of rank one.

Another way of saying this is that the free module $\bigoplus_I R$ represents the functor on modules sending M to the *set* M^I. We have already seen a special case of this for I a one-element set (**??** 1.19).

The next claim is that free modules form a reasonably large class of the category of R-modules.

Proposition 6.6 *Given an R-module M, there is a free module F and a surjection*

$$F \twoheadrightarrow M.$$

Proof. We let F to be the free R-module on the elements e_m, one for each $m \in M$. We define the map

$$F \to M$$

by describing the image of each of the generators e_m: we just send each e_m to $m \in M$. It is clear that this map is surjective. ▲

We close by making a few remarks on matrices. Let M be a free module of rank n, and fix an isomorphism $M \simeq R^n$. Then we can do linear algebra with M, even though we are working over a ring and not necessarily a field, at least to some extent. For instance, we can talk about n-by-n matrices over the ring R, and then each of them induces a transformation, i.e. a module-homomorphism, $M \to M$; it is easy to see that every module-homomorphism between free modules is of this form. Moreover, multiplication of matrices corresponds to composition of homomorphisms, as usual.

Example 6.7 Let us consider the question of when the transformation induced by an n-by-n matrix is invertible. The answer is similar to the familiar one from linear algebra in the case of a field. Namely, the condition is that the determinant be invertible.

Suppose that an $n \times n$ matrix A over a ring R is invertible. This means that there exists A^{-1} so that $AA^{-1} = I$, so hence $1 = \det I = \det(AA^{-1}) = (\det A)(\det A^{-1})$, and therefore, $\det A$ must be a unit in R.

Suppose instead that an $n \times n$ matrix A over a ring R has an invertible determinant. Then, using Cramer's rule, we can actually construct the inverse of A.

We next show that if R is a commutative ring, the category of modules over R contains enough information to reconstruct R. This is a small part of the story of *Morita equivalence,* which we shall not enter into here.

Example 6.8 Suppose R is a commutative ring, and let $\mathcal{C}$ be the category of R-modules. The claim is that $\mathcal{C}$, as an *abstract* category, determines R. Indeed, the claim is that R is canonically the ring of endomorphisms of the identity functor $1_{\mathcal{C}}$.

Such an *endomorphism* is given by a natural transformation $\phi : 1_{\mathcal{C}} \to 1_{\mathcal{C}}$. In other words, one requires for each R-module M, a homomorphism of R-modules $\phi_M : M \to M$ such that if $f : M \to N$ is any homomorphism of modules, then there is a commutative square

$$\begin{tikzcd}
M \arrow[r, "\phi_M"] \arrow[d, "f"] & M \arrow[d] \\
N \arrow[r, "\phi_N"] & N.
\end{tikzcd}$$

Here is a simple way of obtaining such endomorphisms. Given $r \in R$, we consider the map $r : M \to m$ which just multiplies each element by r. This is a homomorphism, and it is clear that it is natural in the above sense. There is thus a map $R \to \mathrm{End}(1_{\mathcal{C}})$ (note that multiplication corresponds to composition of natural transformations). This map is clearly injective; different $r, s \in R$ lead to different natural transformations (e.g. on the R-module R).

The claim is that *any* natural transformation of $1_{\mathcal{C}}$ is obtained in this way. Namely, let $\phi : 1_{\mathcal{C}} \to 1_{\mathcal{C}}$ be such a natural transformation. On the R-module R, ϕ must be multiplication by some element $r \in R$ (because $\mathrm{Hom}_R(R, R)$ is given by such homotheties). Consequently, one sees by drawing commutative diagrams that $\phi : R^{\oplus S} \to R^{\oplus S}$ is of this form for any set S. So ϕ is multiplication by r on any free R-module. Since any module M is a quotient of a free module F, we can draw a diagram

$$\begin{tikzcd}
F \arrow[r, "\phi_F"] \arrow[d] & F \arrow[d] \\
M \arrow[r, "\phi_M"] & M.
\end{tikzcd}$$

Since the vertical arrows are surjective, we find that ϕ_F must be given by multiplication by r too.

6.2 Finitely generated modules

The notion of a "finitely generated" module is analogous to that of a finite-dimensional vector space.

Definition 6.9 An R-module M is **finitely generated** if there exists a surjection $R^n \to M$ for some n. In other words, it has a finite number of elements whose "span" contains M.

The basic properties of finitely generated modules follow from the fact that they are stable under extensions and quotients.

Proposition 6.10 *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence. If M', M'' are finitely generated, so is M.*

Proof. Suppose $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact. Then g is surjective, f is injective, and $\ker(g) = \operatorname{im}(f)$. Now suppose M' is finitely generated, say by $\{a_1, \dots, a_s\}$, and M'' is finitely generated, say by $\{b_1, \dots, b_t\}$. Because g is surjective, each $g^{-1}(b_i)$ is non-empty. Thus, we can fix some $c_i \in g^{-1}(b_i)$ for each i.

For any $m \in M$, we have $g(m) = r_1 b_1 + \cdots + r_t b_t$ for some $r_i \in R$ because $g(m) \in M''$ and M'' is generated by the b_i. Thus $g(m) = r_1 g(c_i) + \cdots r_t g(c_t) = g(r_1 c_1 + \cdots + r_t c_t)$, and because g is a homomorphism we have $m - (r_1 c_1 + \cdots + r_t c_t) \in \ker(g) = \operatorname{im}(f)$. But M' is generated by the a_i, so the submodule $\operatorname{im}(f) \subset M$ is finitely generated by the $d_i = f(a_i)$.

Thus, any $m \in M$ has $m - (r_1 c_1 + \cdots + r_t c_t) = r_{t+1} d_1 + \cdots + r_{t+s} d_s$ for some $r_1, \dots, r_{t+s}$, thus M is finitely generated by $c_1, \dots, c_t, d_1, \dots, d_s$.

The converse is false. It is possible for finitely generated modules to have submodules which are *not* finitely generated. As we shall see in Chapter 5, this does not happen over *noetherian* rings.

Example 6.11 Consider the ring $R = \mathbb{C}[X_1, X_2, \dots,]$ and the ideal $(X_1, X_2, \dots)$. This ideal is a submodule of the finitely generated R-module R, but it is not finitely generated.

Exercise 1.29 Show that a quotient of a finitely generated module is finitely generated.

Exercise 1.30 Consider a *split* exact sequence $0 \to M' \to M \to M'' \to 0$. In this case, show that if M is finitely generated, so is M'.

6.3 Finitely presented modules

Over messy rings, the notion of a finitely presented module is often a good substitute for that of a finitely generated one. In fact, we are going to see (**??**), that there is a general method of reducing questions about finitely presented modules over arbitrary rings to finitely generated modules over finitely generated $\mathbb{Z}$-algebras.

Throughout, fix a ring R.

Definition 6.12 An R-module M is **finitely presented** if there is an exact sequence

$$R^m \to R^n \to M \to 0.$$

The point of this definition is that M is the quotient of a free module R^n by the "relations" given by the images of the vectors in R^m. Since R^m is finitely generated, M can be represented via finitely many generators *and* finitely many relations.

The reader should compare this with the definition of a **finitely generated** module; there we only require an exact sequence

$$R^n \to M \to 0.$$

As usual, we establish the usual properties of finitely presented modules.

We start by showing that if a finitely presented module M is generated by finitely many elements, the "module of relations" among these generators is finitely generated itself. The condition of finite presentation only states that there is *one* such set of generators such that the module of generators is finitely generated.

Proposition 6.13 *Suppose M is finitely presented. Then if $R^m \twoheadrightarrow M$ is a surjection, the kernel is finitely generated.*

Proof. Let K be the kernel of $R^m \twoheadrightarrow M$. Consider an exact sequence

$$F' \to F \to M \to 0$$

where F', F are finitely generated and free, which we can do as M is finitely presented. Draw a commutative and exact diagram

$$\begin{tikzcd}
 & F' \arrow[r] & F \arrow[r] \arrow[d, dashed] & M \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & K \arrow[r] & R^m \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

The dotted arrow $F \to R^m$ exists as F is projective. There is induced a map $F' \to K$. We get a commutative and exact diagram

$$\begin{tikzcd}
 & F' \arrow[r] \arrow[d, "f"] & F \arrow[r] \arrow[d, "g"] & M \arrow[r] \arrow[d] & 0 , \\
0 \arrow[r] & K \arrow[r] & R^m \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

to which we can apply the snake lemma. There is an exact sequence

$$0 \to \mathrm{Coker}(f) \to \mathrm{Coker}(g) \to 0,$$

which gives an isomorphism $\mathrm{Coker}(f) \simeq \mathrm{Coker}(g)$. However, $\mathrm{Coker}(g)$ is finitely generated, as a quotient of R^m. Thus $\mathrm{Coker}(f)$ is too. Since we have an exact sequence

$$0 \to \mathrm{Im}(f) \to K \to \mathrm{Coker}(f) \to 0,$$

and $\mathrm{Im}(f)$ is finitely generated (as the image of a finitely generated object, F'), we find by Proposition 6.10 that $\mathrm{Coker}(f)$ is finitely generated. ▲

Proposition 6.14 *Given an exact sequence*

$$0 \to M' \to M \to M'' \to 0,$$

if M', M'' are finitely presented, so is M.

In general, it is not true that if M is finitely presented, then M' and M'' are. For instance, it is possible that a submodule of the free, finitely generated module R (i.e. an ideal), might fail to be finitely generated. We shall see in Chapter 5 that this does not happen over a *noetherian* ring.

Proof. Indeed, suppose we have exact sequences

$$F_1' \to F_0' \to M' \to 0$$

and

$$F_1'' \to F_0'' \to M'' \to 0$$

where the F's are finitely generated and free. We need to get a similar sequence for M. Let us stack these into a diagram

$$\begin{tikzcd}
 & F_1' \arrow[d] & & F_1'' \arrow[d] & \\
 & F_0' \arrow[d] & & F_0'' \arrow[d] & \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

However, now, using general facts about projective modules (**??**), we can splice these presentations into a resolution

$$F_1' \oplus F_1'' \to F_0' \oplus F_0'' \to M \to 0,$$

which proves the assertion. ▲

Corollary 6.15 *The (finite) direct sum of finitely presented modules is finitely presented.*

Proof. Immediate from Proposition 6.14 ▲

6.4 Modules of finite length

A much stronger condition on modules that of finite generation is that of *finite length.* Here, basically any operation one does will eventually terminate.

Let R be a commutative ring, M an R-module.

Definition 6.16 M is **simple** if $M \neq 0$ and M has no nontrivial submodules.

Exercise 1.31 A torsion-free abelian group is never a simple $\mathbb{Z}$-module.

Proposition 6.17 *M is simple if and only if it is isomorphic to $R/\mathfrak{m}$ for $\mathfrak{m} \subset R$ a maximal ideal.*

Proof. Let M be simple. Then M must contain a cyclic submodule Rx generated by some $x \in M - \{0\}$. So it must contain a submodule isomorphic to R/I for some ideal I, and simplicity implies that $M \simeq R/I$ for some I. If I is not maximal, say properly contained in J, then we will get a nontrivial submodule J/I of $R/I \simeq M$. Conversely, it is easy to see that $R/\mathfrak{m}$ is simple for $\mathfrak{m}$ maximal. ▲

Exercise 1.32 (Schur's lemma) Let $f : M \to N$ be a module-homomorphism, where M, N are both simple. Then either $f = 0$ or f is an isomorphism.

Definition 6.18 M is of **finite length** if there is a finite filtration $0 \subset M^0 \subset \cdots \subset M^n = M$ where each M^i/M^{i-1} is simple.

Exercise 1.33 Modules of finite length are closed under extensions (that is, if $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then if M', M'' are of finite length, so is M).

In the next result (which will not be used in this chapter), we shall use the notions of a *noetherian* and an *artinian* module. These notions will be developed at length in **??**, and we refer the reader there for more explanation. A module is *noetherian* if every ascending chain $M_1 \subset M_2 \subset \dots$ of submodules stabilizes, and it is *artinian* if every descending chain stabilizes.

Proposition 6.19 *M is finite length iff M is both noetherian and artinian.*

Proof. Any simple module is obviously both noetherian and artinian: there are two submodules. So if M is finite length, then the finite filtration with simple quotients implies that M is noetherian and artinian, since these two properties are stable under extensions (Proposition 1.5 and Proposition 4.3 of Chapter 5).

Suppose $M \neq 0$ is noetherian and artinian. Let $M_1 \subset M$ be a minimal nonzero submodule, which exists as M is artinian. This is necessarily simple. Then we have a filtration

$$0 = M_0 \subset M_1.$$

If $M_1 = M$, then the filtration goes up to M, and we have that M is of finite length. If not, find a submodule M_2 that contains M_1 and is minimal among submodules containing M_1; then the quotient M_2/M_1 is simple. We have the filtration

$$0 = M_0 \subset M_1 \subset M_2,$$

which we can keep continuing until at some point we reach M. Note that since M is noetherian, we cannot continue this strictly ascending chain forever. ▲

Exercise 1.34 In particular, any submodule or quotient module of a finite length module is of finite length. Note that the analog is not true for finitely generated modules unless the ring in question is noetherian.

Our next goal is to show that the length of a filtration of a module with simple quotients is well-defined. For this, we need:

Lemma 6.20 *Let $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ be a filtration of M with simple quotients. Let $N \subset M$. Then the filtration $0 = M_0 \cap N \subset M_1 \cap N \subset \cdots \subset N$ has simple or zero quotients.*

Proof. Indeed, for each i, $(N \cap M_i)/(N \cap M_{i-1})$ is a submodule of M_i/M_{i-1}, so is either zero or simple. ▲

Theorem 6.21 (Jordan-Hölder) *Let M be a module of finite length. In this case, any two filtrations on M with simple quotients have the same length.*

Definition 6.22 This number is called the **length** of M and is denoted $\ell(M)$.

Proof (Proof of Theorem 6.21). Let us introduce a temporary definition: $l(M)$ is the length of the *minimal* filtration on M. We will show that any filtration of M (with simple quotients) is of length $l(M)$. This is the proposition in another form.

The proof of this claim is by induction on $l(M)$. Suppose we have a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

with simple quotients. We would like to show that $n = l(M)$. By definition of $l(M)$, there is another filtration

$$0 = N_0 \subset \cdots \subset N_{l(M)} = M.$$

If $l(M) = 0, 1$, then M is zero or simple, which will necessarily imply that $n = 0, 1$ respectively. So we can assume $l(M) \geq 2$. We can also assume that the result is known for strictly smaller submodules of M.

There are two cases:

1. $M_{n-1} = N_{l(M)-1}$. Then $M_{n-1} = N_{l(M)-1}$ has l at most $l(M) - 1$. Thus by the inductive hypothesis any two filtrations on M_{n-1} have the same length, so $n - 1 = l(M) - 1$, implying what we want.

2. We have $M_{n-1} \cap N_{l(M)-1} \subsetneq M_{n-1}, N_{l(M)-1}$. Call this intersection K.

   Now we have two filtrations of these modules $M_{n-1}, N_{l(M)-1}$ whose quotients are simple. We can replace them such that the next term before them is K. To do this, consider the filtrations

   $$0 = M_0 \cap K \subset M_1 \subset K \subset \dots M_{n-1} \cap K = K \subset M_{n-1}$$

   and

   $$0 = N_0 \cap K \subset M_1 \subset K \subset \dots N_{l(M)-1} \cap K = K \subset N_{l(M)-1}.$$

These filtrations have simple or zero quotients by Lemma 6.20, and since $M_{n-1}/K = M_{n-1}/M_{n-1} \cap N_{l(M)-1} = M/M_{n-1}$ is simple, and similarly for $N_{l(M)-1}/K$. We can throw out redundancies to eliminate the zero terms. So we get two new filtrations of M_{n-1} and $N_{l(M)-1}$ whose second-to-last term is K.

By the inductive hypothesis any two filtrations on either of these proper submodules $M_{n-1}, N_{l(M)-1}$ have the same length. Thus the lengths of the two new filtrations are $n-1$ and $l(M)-1$, respectively. So we find that $n-1 = l(K)+1$ and $l(M)-1 = l(K)+1$ by the inductive hypothesis. This implies what we want. ▲

Exercise 1.35 Prove that the successive quotients M_i/M_{i-1} are also determined (up to permutation).

CRing Project contents

CRing Project bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BBD82] A. A. Beĭlinson, J. Bernstein, and P. Deligne. Faisceaux pervers. In *Analysis and topology on singular spaces, I (Luminy, 1981)*, volume 100 of *Astérisque*, pages 5–171. Soc. Math. France, Paris, 1982.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7.* Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Cam88] Oscar Campoli. A principal ideal domain that is not a euclidean domain. *American Mathematical Monthly*, 95(9):868–871, 1988.

[CF86] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original.

[Cla11] Pete L. Clark. Factorization in euclidean domains. 2011. Available at `http://math.uga.edu/~pete/factorization2010.pdf`.

[dJea10] Aise Johan de Jong et al. *Stacks Project*. Open source project, available at `http://www.math.columbia.edu/algebraic_geometry/stacks-git/`, 2010.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[For91] Otto Forster. *Lectures on Riemann surfaces*, volume 81 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. Translated from the 1977 German original by Bruce Gilligan, Reprint of the 1981 English translation.

[GD] Alexander Grothendieck and Jean Dieudonné. *Élements de géometrie algébrique.* Publications Mathématiques de l'IHÉS.

[Ger] Anton Geraschenko (mathoverflow.net/users/1). Is there an example of a formally smooth morphism which is not smooth? MathOverflow. `http://mathoverflow.net/questions/200` (version: 2009-10-08).

[Gil70] Robert Gilmer. An existence theorem for non-Noetherian rings. *The American Mathematical Monthly*, 77(6):621–623, 1970.

[Gre97] John Greene. Principal ideal domains are almost euclidean. *The American Mathematical Monthly*, 104(2):154–156, 1997.

[Gro57] Alexander Grothendieck. Sur quelques points d'algèbre homologique. *Tôhoku Math. J. (2)*, 9:119–221, 1957.

[Har77] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hat02] Allen Hatcher. *Algebraic topology.* Cambridge University Press, Cambridge, 2002. Available at `http://www.math.cornell.edu/~hatcher/AT/AT.pdf`.

[Hov07] Mark Hovey. *Model Categories.* American Mathematical Society, 2007.

[KS06] Masaki Kashiwara and Pierre Schapira. *Categories and sheaves*, volume 332 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 2006.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LR08] T. Y. Lam and Manuel L. Reyes. A prime ideal principle in commutative algebra. *J. Algebra*, 319(7):3006–3027, 2008.

[Mar02] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002. An introduction.

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series.* Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[McC76] John McCabe. A note on Zariski's lemma. *The American Mathematical Monthly*, 83(7):560–561, 1976.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series.* Princeton University Press, Princeton, N.J., 1980.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1998.

[Per04] Hervé Perdry. An elementary proof of Krull's intersection theorem. *The American Mathematical Monthly*, 111(4):356–357, 2004.

[Qui] Daniel Quillen. Homology of commutative rings. Mimeographed notes.

[Ray70] Michel Raynaud. *Anneaux locaux henséliens.* Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, Berlin, 1970.

[RG71] Michel Raynaud and Laurent Gruson. Critères de platitude et de projectivité. Techniques de "platification" d'un module. *Invent. Math.*, 13:1–89, 1971.

[Ser65] Jean-Pierre Serre. *Algèbre locale. Multiplicités*, volume 11 of *Cours au Collège de France, 1957–1958, rédigé par Pierre Gabriel. Seconde édition, 1965. Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1965.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser09] Jean-Pierre Serre. How to use finite fields for problems concerning infinite fields. 2009. arXiv:0903.0517v2.

[SGA72] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos.* Lecture Notes in Mathematics, Vol. 269. Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1).* Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[Tam94] Günter Tamme. *Introduction to étale cohomology.* Universitext. Springer-Verlag, Berlin, 1994. Translated from the German by Manfred Kolster.

[Vis08] Angelo Vistoli. Notes on Grothendieck topologies, fibered categories, and descent theory. *Published in* FGA Explained, 2008. arXiv:math/0412512v4.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1997.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1994.