The CRing Project

GNU Free Documentation License, v. 1.2

2010

Contents

Introduction

The following is a massively collaborative, open source textbook on commutative algebra. The project is currently in its infancy, and needs contributions! See the next chapter for how to contribute.

Prerequisites

The prerequisite is a basic acquaintance with modern algebra. While even the notion of a ring is introduced from scratch, it is done so rather rapidly, and the reader is advised to consult another source. In addition, the notes do not hesitate to use the language of categories. Besides that, the notes are mostly self-contained. (Material explaining the category theory should be added sometime.)

Genesis of the project

In the fall of 2010, Jacob Lurie taught a course (Math 221) on commutative algebra at Harvard. The course started with foundational material, but swiftly progressed to touch on a wide range of material, and culminated in the study of regular local rings. Akhil Mathew sat in on this course and took detailed ("live-TEXed") notes, which are still available on his website in unedited form at `http://people.fas.harvard.edu/~amathew`.

As the course was very well-taught, Akhil decided that it would be an interesting project to edit the notes I had taken into a mini-textbook of sort. This book started out as an attempt at such a project, and the initial contribution was his notes. However, the book is now intended to be a massively collaborative project.

N.B. The following project is not endorsed by Jacob Lurie.

Corrections

Please email corrections to `cring.project@gmail.com`.

Version

This file was last updated December 11, 2010.

Contributions

So far, the list of contributors is:

1. Adeel Khan
2. Geoffrey Lee
3. Akhil Mathew

It is hoped that eventually there will be a longer list of contributors!

A list of contributions will be maintained at `http://people.fas.harvard.edu/~amathew/contrib.html`.

How to contribute

To contribute, email submissions to `cring.project@gmail.com`. Contributions do not have to be polished; they can be rough sketches written for any purpose at all—half-finished homework writeups, term papers, blog posts, and others are all welcome.

Contributions in editing the chapters are also welcome. To do this, simply download the source, edit the files, and email the modifications to the same address.

Chapter 1

Foundations

Before beginning a proper study of commutative algebra, there is a set of basic definitions and general formalism (e.g. tensor products, projective modules, etc.) that one needs to assimilate, and the exposition of that is the purpose of the present chapter. It is assumed that the reader has at least some prior acquaintance with algebra, so the exposition will be occasionally quick.

1 Basic definitions

1.1 Historical remarks: unique factorization

We shall begin with a few historical remarks to motivate the subject. Since they will occasionally refer terms that have not yet been defined, the reader may wish to skip ahead occasionally.

Fermat's last theorem states that the equation

$$x^n + y^n = z^n \tag{1.1}$$

has no nontrivial solutions in the integers.

This result has a long history, and there have been many incorrect proofs. For instance, we could try to prove this by factoring the expression (1.1) for n odd. Let ζ be a primitive nth root of unity; then we find

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

We are tempted to ask how the product decomposition interacts with the power decomposition. The caveat is that though x, y, z are integers, the terms in the factorization actually live in $\mathbb{Z}[\zeta]$.

The problem is $\mathbb{Z}[\zeta]$. This is a legitimate "ring," as we shall see below. We can still talk about "primes" and "factorization" as we do over the integers. However, things go wrong. Over $\mathbb{Z}$, factorization is unique up to permuting the factors. Over $\mathbb{Z}[\zeta]$, you can still get a decomposition into irreducible factors, but in general it is not unique. The ring does not always have unique factorization.

Let us look at a failure of unique factorization. Consider the set $\mathbb{Z}[\sqrt{-5}]$ of complex numbers that look like $a + \sqrt{-5}b, a, b \in \mathbb{Z}$. We can write

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

you can convince yourself (see Exercise **??**) that these are two fundamentally different factorizations, even though the elements in question are irreducible. So 6 admits a nonunique factorization into irreducibles in $\mathbb{Z}[\sqrt{-5}]$.

In order to think about the failure of unique factorization, Dedekind introduced the theory of ideal numbers, now called **ideals.** Dedekind was trying to get to the bottom of what was going on. Let us look at the problem. Ideally, if you have a prime factor of 6, and a decomposition $6 = ab$, then that prime factor must divide a or b. This is not true, however. There is a new idea that one must introduce.

One should imagine an **ideal number** x such that x divides both 2 and $1+\sqrt{-5}$, but manages not to be 1. This mysterious x doesn't live in the ring $\mathbb{Z}[\sqrt{-5}]$; it can't, because they have no common factor. Yet we can talk about what ought to divide x. We know that 2 and $1+\sqrt{-5}$ are divisible by x. For instance, $2+1+\sqrt{-5}$ should be divisible by x, whatever this means. More generally, all linear combinations of 2 and $1 + \sqrt{-5}$ should be divisible by x.

It is not clear what this "x" should refer to. In fact, as we will see, x is really best identified with the set of elements that we have just said are divisible by it, according to the above rules. So, to avoid some kind of weird mysticism, we will think of x as a *subset* of R. This subset is what leads to *ideal* theory.

1.2 Basic definitions

Most fundamental is:

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 all the usual identities.

R 1 R is a group under addition.

R 2 The multiplication map is commutative and distributes over addition,

R 3 There is a **unit** (or **identity**) 1 such that $1x = 1 \cdot x = x$ for all $x \in R$.

Given a ring, a **subring** is a subset containing the identity which is closed under addition and multiplication.

Example 1.2. $\mathbb{Z}$ is a ring. This is the simplest example, but we shall have many more in the future.

The class of rings forms a *category*. Indeed, we can define a **homomorphism** (or **morphism**) of rings $R \xrightarrow{f} S$ as a map $f : R \to S$ that respects addition and multiplication. This means that

1. $f(1) = 1$ for $1, 1$ 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 $a, b \in R$.

To compose two morphisms, just compose them as functions.

The philosophy of Grothendieck, as expounded in his EGA, 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 1.3. 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 required to commute with the structure morphisms.

Example 1.4. Every ring is a $\mathbb{Z}$-algebra in a natural and unique way.

Now we move to something slightly less formal.

Definition 1.5. Let R be a ring. An **ideal** in R is a subset $I \subset R$ satisfying

1. $0 \in I$

2. $x, y \in I$ implies $x + y \in I$

3. $x \in I, y \in R$, then $xy \in I$.

One ought to think of an ideal as somehow generalizing the notion of "divisibility." This motivation is provided by:

Example 1.6. If R is a ring and $x \in R$, then the set of things divisible by x (i.e. the set xR of multiples of x) is an ideal. This is denoted (x). It is in fact the smallest ideal containing x. Such ideals are called **principal.**

More generally, if $x_1, \ldots, x_n \in R$, we denote by $(x_1, \ldots, x_n) \subset R$ the ideal consisting of elements of the form $\sum s_i r_i$ where the $s_i \in R$. This is the smallest ideal containing the $\{x_i\}$, and is called the ideal **generated by the x_i.**

You can do some of the same things with ideals as you can do with numbers. For instance, you can multiply them:

Definition 1.7. If I, J are ideals in a ring R, the product IJ is defined as the smallest ideal containing the products xy for all $x \in I, y \in J$. More explicitly, this is the set of all expressions

$$\sum x_i y_i$$

for $x_i \in I, y_i \in J$.

Example 1.8. We have $(x)(y) = (xy)$. This is straightforward.

Example 1.9. Let $R = \mathbb{Z}[\sqrt{-5}]$. The ideal

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

generated by both of them is the mysterious "x" we were talking about earlier in **??**.

This is not the trivial unit ideal (1); this is easy to check. However, it is also not principal.

EXERCISE 1.1. Show that $(2, 1+\sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$ is not principal.

The theory of ideals saves unique factorization. In the sequel, we shall prove:

Theorem 1.10 (Dedekind)**.** *Let $R = \mathbb{Z}[\sqrt{-5}]$ or $\mathbb{Z}[\zeta]$ (or more generally, any ring of integers in a finite extension of $\mathbb{Q}$). Let $I \subset R$ be an ideal, nonzero.*

Then I factors uniquely $I = \mathfrak{p}_1 \dots \mathfrak{p}_n$, where the $\mathfrak{p}_i$ are ideals that cannot be factored further, i.e. ***prime****.*

This is a theorem that belongs to a number theory class, but we will talk about it too.

After this series of technical definitions and discussion of unique factorization, we shall give several more examples.

EXERCISE 1.2. 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.

EXERCISE 1.3. 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 1.4. More generally, if R is a ring and G a commutative monoid, 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 **group ring**. The case of $G = \mathbb{Z}_{\geq 0}$ is the polynomial ring.

EXERCISE 1.5. 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 $\mathbb{Z} \to R$.

EXERCISE 1.6. 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 1.7. Let X be a set and R a ring. The set R^X of functions $f : X \to R$ is a ring. If $S \subset X$, then the set of functions $f : X \to R$ that vanish on S is an ideal.

EXERCISE 1.8. 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** $\to$ **Sets** assigning to each ring its underlying set is representable. (Hint: use a suitable polynomial ring.)

1.3 Another example: 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 (Exercise 1.2). 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 1.11. 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 1.10 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 1.12. 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 1.13. *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.

1.4 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 Exercise 1.2 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 1.14. Consider the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$. Recall that before we thought of the ring $\mathbb{C}[t]$ as a ring of meromorphic functions. Similarly each element of the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ 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 $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$; consider the collection of all functions $f \in \mathbb{C}[x_1, \ldots, x_n]$ 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 1.15. 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 in this class.

Theorem 1.16 (Hilbert's Nullstellensatz)**.** *If $I \subset \mathbb{C}[x_1, \ldots, x_n]$ 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.*[1]

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

Exercise 1.9. Assuming the Nullstellensatz, show that any *maximal* ideal in the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for $a_1, \ldots, a_n \in \mathbb{C}$. 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).

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

2 Modules over a commutative ring

We will now establish some basic terminology about modules.

2.1 Definitions

Suppose R is a commutative ring.

Definition 2.1. 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 2.2. 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*.[2] 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:

Definition 2.3. 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 1.10. If R is a ring and $R \to End(M)$ a homomorphism, then M is made into an R-module, and vice versa.

Example 2.4. if R is a ring, then R is an R-module by multiplication on the left.

Example 2.5. A $\mathbb{Z}$-module is the same thing as an abelian group.

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

Definition 2.6. 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:

$$\begin{array}{ccc} R \times M_0 & \longrightarrow & M_0 \\ \downarrow & & \downarrow \\ R \times M & \longrightarrow & M \end{array} .$$

Here the horizontal maps are multiplication.

Example 2.7. Let R be a (**commutative**) ring; then an ideal in R is the same thing as a submodule of R.

Example 2.8. 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 2.9. 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.

We shall next see that when one quotients by an *ideal*, one gets not merely a module but actually another *ring.*

Example 2.10. If R is a ring and $I \subset R$ an ideal, then R/I is an R-module. The multiplication is $a(b+I) = ab + I$.

As one easily checks, this descends further to a multiplication

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

such that there is a commutative diagram

$$\begin{array}{ccc} R \times R/I & \longrightarrow & R/I \\ & \searrow \quad \nearrow & \\ & R/I \times R/I & \end{array} .$$

In particular, R/I is a ring, under multiplication $(a+I)(b+I) = ab + I$.

Definition 2.11. R/I is called the **quotient ring** by the ideal I.

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 1.11. 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** $\to$ **Sets** sending a ring to its idempotents. Prove that it is corepresentable.

Exercise 1.12. Show that the functor assigning to each ring the set of elements annihilated by 2 is corepresentable.

Exercise 1.13. If $I \subset J \subset R$, then J/I is an ideal of R/I, and there is a canonical isomorphism

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

2.2 Some categorical constructions

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 introduce a few more basic notions.

Definition 2.12. 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 $a \in R, x \in M$.

Thus, for any commutative ring R, the class of R-modules and module-homomorphsims forms a **category.**

Example 2.13. If $a \in R$, then multiplication by a is a module-homomorphism $M \xrightarrow{a} M$ for any R-module M.

Definition 2.14. 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** $\mathrm{Im} f$ 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 $N/\mathrm{Im}(f)$.

EXERCISE 1.14. The universal property of the kernel is as follows. Let $M \xrightarrow{f} N$ 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. In particular, if we think of the hom-sets as abelian groups (i.e. $\mathbb{Z}$-modules)

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

EXERCISE 1.15. What is the universal property of the cokernel?

EXERCISE 1.16. On the category of modules, the functor assigning to each module M its underlying set is corepresentable (cf. Exercise **??**).

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.

Definition 2.15. 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 2.16. 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.

EXERCISE 1.17. The direct product is a product in the category of modules, and the direct sum is a coproduct.

TO BE ADDED: filtered colimits

2.3 Exactness

Finally, we introduce the notion of *exactness*.

Definition 2.17. 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 $g \circ f = 0$. So $M \to N \to P$ is zero. In particular, $\mathrm{Im}(f) \subset \ker(g)$.

This complex is **exact** (or exact at N) if $\mathrm{Im}(f) = \ker(g)$. So anything that is killed when you map 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 image of the map $f : A \to B$ is the same as the kernel of the map $g : B \to C$. A longer (possibly infinite) sequence of modules

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

will be called **exact** if it is exact at each step.

Example 2.18. 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.

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 image of g. So M'' can be thought of as the quotient M/M'.

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

Definition 2.19.

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 $0 \to M' \to M \to M''$. In particular, 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.

A functor is exact if and only if it is both left and right exact.
TO BE ADDED: further explanation, exactness of filtered colimits

2.4 Free modules

Definition 2.20. A module M is **free** if it is isomorphic to $\bigoplus_I R$ for some index set I.

3 Ideals

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

3.1 Prime and maximal ideals

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.

The notion of a "prime ideal" is intended to generalize the familiar idea of a prime number.

Definition 3.1. 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 3.2. If $R = \mathbb{Z}$ and $p \in R$, then $(p) \subset \mathbb{Z}$ is a prime ideal iff p is a prime number (or the opposite of a prime number) or zero.

Definition 3.3. An ideal $I \subset R$ is called **maximal**[3] 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 1.18. Find the maximal ideals in $\mathbb{C}[t]$.

Proposition 3.4. *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 $y \in I$. □

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 3.5. *Let R be a commutative ring. Then $I \subset R$ 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

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

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 can't happen by maximality) unless it were all of R. □

Corollary 3.6. *Let R be a nonzero commutative ring. Then R has a maximal ideal.*

Proof. Apply the lemma to the zero ideal. □

Corollary 3.7. *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 3.5 finishes the argument. □

3.2 Fields and integral domains

Recall:

Definition 3.8. 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 3.9. *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 can't 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 3.10. *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 3.11. 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 3.12. *An ideal $I \subset R$ is prime iff R/I is a domain.*

Exercise 1.19. Prove Proposition 3.12.

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.

Exercise 1.20. 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.*

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

Exercise 1.21. 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 $y \in R$.

3.3 Principal ideal domains

Definition 3.13. 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 3.14. $\mathbb{Z}$ is a PID. The only nontrivial fact to check here is that:

Proposition 3.15. *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 $I = (n)$. □

EXERCISE 1.22. A domain R is **euclidean** if there is a map $v : R \to \mathbb{Z}_{\geq 0}$ such that $v(xy) = v(x)v(y)$ and such that a type of division algorithm holds: if $a, b \in R$ with $b \neq 0$, there are $q, r \in R$ such that

$$a = qb + r$$

and $v(r) < v(b)$. Prove that a euclidean domain is principal.

EXERCISE 1.23. Prove that $\mathbb{Z}[i]$ is principal. (Use the previous exercise.)

EXERCISE 1.24. Prove that the polynomial ring $F[t]$ for F a field is principal.

Chapter 2

Three important functors

There are three functors that will be integral to our study of commutative algebra in the future: localization, the tensor product, and Hom. While localization is an *exact* functor, the tensor product and Hom are not. The failure of exactness in those cases leads to the theory of flatness and projectivity, and eventually the *derived functors* Tor and Ext that crop up in commutative algebra.

1 Localization

Localization is the process of making invertible a collection of elements in a ring. It is a generalization of the process of forming a quotient field of an integral domain.

1.1 Localization at a multiplicative subset

Let R be a commutative ring. We start by constructing the notion of *localization* in the most general sense.

We have already implicitly used this definition, but nonetheless, we make it formally:

Definition 1.1. A subset $S \subset R$ is a **multiplicative subset** if $1 \in S$ and if $x, y \in S$ implies $xy \in S$.

We now define the notion of *localization*. Formally, this means inverting things. This will give us a functor from R-modules to R-modules.

Definition 1.2. If M is an R-module, we define the module $S^{-1}M$ as the set of formal fractions

$$\{m/s, m \in M, s \in S\}$$

modulo an equivalence relation: where $m/s \sim m'/s'$ if and only if

$$t(s'm - m's) = 0$$

for some $t \in S$. The reason we need to include the t in the definition is that otherwise the relation would not be transitive (i.e. would not be an equivalence relation).

So two fractions agree if they agree when clearing denominators and multiplication.

It is easy to check that this is indeed an equivalence relation. Moreover $S^{-1}M$ is an abelian group with the usual addition of fractions

$$\frac{m}{s} + \frac{m'}{s'} = \frac{s'm + sm'}{ss'}$$

and it is easy to check that this is a legitimate abelian group.

Definition 1.3. Let M be an R-module and $S \subset R$ a multiplicative subset. The abelian group $S^{-1}M$ is naturally an R-module. We define

$$x(m/s) = (xm)/s, \quad x \in R.$$

It is easy to check that this is well-defined and makes it into a module.

Finally, we note that localization is a *functor* from the category of R-modules to itself. Indeed, given $f : M \to N$, there is a naturally induced map $S^{-1}M \overset{S^{-1}f}{\to} S^{-1}N$.

We now consider the special case when the localized module is the initial ring itself. Let $M = R$. Then $S^{-1}R$ is an R-module, and it is in fact a commutative ring in its own right. The ring structure is quite tautological:

$$(x/s)(y/s') = (xy/ss').$$

There is a map $R \to S^{-1}R$ sending $x \to x/1$, which is a ring-homomorphism.

Definition 1.4. For $S \subset R$ a multiplicative set, the localization $S^{-1}R$ is a commutative ring as above. In fact, it is an R-algebra; there is a natural map $\phi : R \to S^{-1}R$ sending $r \to r/1$.

We can, in fact, describe $\phi : R \to S^{-1}R$ by a *universal property*. Note that for each $s \in S$, $\phi(s)$ is invertible. This is because $\phi(s) = s/1$ which has a multiplicative inverse $1/s$. This property characterizes $S^{-1}R$.

For any commutative ring B, $\mathrm{Hom}(S^{-1}R, B)$ is naturally isomorphic to the subset of $\mathrm{Hom}(R, B)$ that send S to units. The map takes $S^{-1}R \to B$ to the pullback $R \to S^{-1}R \to B$. The proof of this is very simple. Suppose that $f : R \to B$ is such that $f(s) \in B$ is invertible for each $s \in S$. Then we must define $S^{-1}R \to B$ by sending r/s to $f(r)f(s)^{-1}$. It is easy to check that this is well-defined and that the natural isomorphism as claimed is true.

Let R be a ring, M an R-module, $S \subset R$ a multiplicatively closed subset. We defined a ring of fractions $S^{-1}R$ and an R-module $S^{-1}M$. But in fact this is a module over the ring $S^{-1}R$. We just multiply $(x/t)(m/s) = (xm/st)$.

In particular, localization at S gives a *functor* from R-modules to $S^{-1}R$-modules.

Exercise 2.1. Let R be a ring, S a multiplicative subset. Let T be the R-algebra $R[\{x_s\}_{s\in S}]/(\{sx_s - 1\})$. This is the polynomial ring in the variables x_s, one for each $s \in S$, modulo the ideal generated by $sx_s = 1$. Prove that this R-algebra is naturally isomorphic to $S^{-1}R$, using the universal property.

EXERCISE 2.2. Define a functor **Rings** $\to$ **Sets** sending a ring to its set of units, and show that it is representable.

1.2 Local rings

A special case of great importance in the future is when the multiplicative subset is the complement of a prime ideal, and we study this in the present subsection. Such localizations will be "local rings" and geometrically correspond to the process of zooming at a point.

Example 1.5. Let R be an integral domain and let $S = R - \{0\}$. This is a multiplicative subset because R is a domain. In this case, $S^{-1}R$ is just the ring of fractions by allowing arbitrary nonzero denominators; it is a field, and is called the **quotient field**. The most familiar example is the construction of $\mathbb{Q}$ as the quotient field of $\mathbb{Z}$.

We'd like to generalize this example.

Example 1.6. Let R be arbitrary and $\mathfrak{p}$ is a prime ideal. This means that $1 \notin \mathfrak{p}$ and $x, y \in R - \mathfrak{p}$ implies that $xy \in R - \mathfrak{p}$. Hence, the complement $S = R - \mathfrak{p}$ is multiplicatively closed. We get a ring $S^{-1}R$.

Definition 1.7. This ring is denoted $R_{\mathfrak{p}}$ and is called the **localization at $\mathfrak{p}$.** If M is an R-module, we write $M_{\mathfrak{p}}$ for the localization of M at $R - \mathfrak{p}$.

This generalizes the previous example (where $\mathfrak{p} = (0)$).

There is a nice property of the rings $R_{\mathfrak{p}}$. To elucidate this, we start with a lemma.

Lemma 1.8. *Let R be a nonzero commutative ring. The following are equivalent:*

1. *R has a unique maximal ideal.*
2. *If $x \in R$, then either x or $1 - x$ is invertible.*

Definition 1.9. In this case, we call R **local**. A local ring is one with a unique maximal ideal.

Proof of the lemma. First we prove (2) $\implies$ (1).

Assume R is such that for each x, either x or $1 - x$ is invertible. We will find the maximal ideal. Let $\mathfrak{M}$ be the collection of noninvertible elements of R. This is a subset of R, not containing 1, and it is closed under multiplication. Any proper ideal must be a subset of $\mathfrak{M}$, because otherwise that proper ideal would contain an invertible element.

We just need to check that $\mathfrak{M}$ is closed under addition. Suppose to the contrary that $x, y \in \mathfrak{M}$ but $x + y$ is invertible. We get (with $a = x/(x + y)$)

$$1 = \frac{x}{x+y} + \frac{y}{x+y} = a + (1 - a).$$

Then one of $a, 1-a$ is invertible. So either $x(x+y)^{-1}$ or $y(x+y)^{-1}$ is invertible, which implies that either x, y is invertible, contradiction.

Now prove the reverse direction. Assume R has a unique maximal ideal $\mathfrak{M}$. I claim that $\mathfrak{M}$ consists precisely of the noninvertible elements. To see this, first note that $\mathfrak{M}$ can't contain any invertible elements since it is proper. Conversely, suppose x is not invertible, i.e. $(x) \subsetneq R$. Then (x) is contained in a maximal ideal by Proposition 3.5, so $(x) \subset \mathfrak{M}$ since $\mathfrak{M}$ is unique among maximal ideals. Thus $x \in \mathfrak{M}$.

Suppose $x \in R$; we can write $1 = x + (1-x)$. Since $1 \notin \mathfrak{M}$, one of $x, 1-x$ must not be in $\mathfrak{M}$, so one of those must not be invertible. So (1) $\implies$ (2). The lemma is proved. □

Let us give some examples of local rings.

Example 1.10. Any field is a local ring because the unique maximal ideal is (0).

Example 1.11. Let R be any commutative ring and $\mathfrak{p} \subset R$ a prime ideal. Then $R_{\mathfrak{p}}$ is a local ring.

We state this as a result.

Proposition 1.12. *$R_{\mathfrak{p}}$ is a local ring if $\mathfrak{p}$ is prime.*

Proof. Let $\mathfrak{m} \subset R_{\mathfrak{p}}$ consist of elements x/s for $x \in \mathfrak{p}$ and $s \in R - \mathfrak{p}$. It is left as an exercise (using the primality of $\mathfrak{p}$) to the reader to see that whether the numerator belongs to $\mathfrak{p}$ is *independent* of the representation x/s used for it.

Then I claim that $\mathfrak{m}$ is the unique maximal ideal. First, note that $\mathfrak{m}$ is an ideal; this is evident since the numerators form an ideal. If $x/s, y/s'$ belong to $\mathfrak{m}$ with appropriate expressions, then the numerator of

$$\frac{xs' + ys}{ss'}$$

belongs to $\mathfrak{p}$, so this sum belongs to $\mathfrak{m}$. Moreover, $\mathfrak{m}$ is a proper ideal because $\frac{1}{1}$ is not of the appropriate form.

I claim that $\mathfrak{m}$ contains all other proper ideals, which will imply that it is the unique maximal ideal. Let $I \subset R_{\mathfrak{p}}$ be any proper ideal. Suppose $x/s \in I$. We want to prove $x/s \in \mathfrak{m}$. In other words, we have to show $x \in \mathfrak{p}$. But if not x/s would be invertible, and $I = (1)$, contradiction. This proves locality. □

Exercise 2.3. Any local ring is of the form $R_{\mathfrak{p}}$ for some ring R and for some prime ideal $\mathfrak{p} \subset R$.

Example 1.13. Let $R = \mathbb{Z}$. This is not a local ring; the maximal ideals are given by (p) for p prime. We can thus construct the localizations $\mathbb{Z}_{(p)}$ of all fractions $a/b \in \mathbb{Q}$ where $b \notin (p)$. Here $\mathbb{Z}_{(p)}$ consists of all rational numbers that don't have powers of p in the denominator.

Exercise 2.4. A local ring has no idempotents other than 0 and 1. (Recall that $e \in R$ is *idempotent* if $e^2 = e$.) In particular, the product of two rings is never local.

It may not yet be clear why localization is such a useful process. It turns out that many problems can be checked on the localizations at prime (or even maximal) ideals, so certain proofs can reduce to the case of a local ring. Let us give a small taste.

Proposition 1.14. *Let $f : M \to N$ be a homomorphism of R-modules. Then f is injective if and only if for every maximal ideal $\mathfrak{m} \subset R$, we have that $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective.*

Recall that, by definition, $M_{\mathfrak{m}}$ is the localization at $R - \mathfrak{m}$.

There are many variants on this (e.g. replace with surjectivity, bijectivity). This is a general observation that lets you reduce lots of commutative algebra to local rings, which are easier to work with.

Proof. Suppose first that each $f_{\mathfrak{m}}$ is injective. I claim that f is injective. Suppose $x \in M - \{0\}$. We must show that $f(x) \neq 0$. If $f(x) = 0$, then $f_{\mathfrak{m}}(x) = 0$ for every maximal ideal $\mathfrak{m}$. Then by injectivity it follows that x maps to zero in each $M_{\mathfrak{m}}$. We would now like to get a contradiction.

Let $I = \{a \in R : ax = 0 \in M\}$. This is proper since $x \neq 0$. So I is contained in some maximal ideal $\mathfrak{m}$. Then x maps to zero in $M_{\mathfrak{m}}$ by the previous paragraph; this means that there is $s \in R - \mathfrak{m}$ with $sx = 0 \in M$. But $s \notin I$, contradiction.

Now let us do the other direction. Suppose f is injective and $\mathfrak{m}$ a maximal ideal; we prove $f_{\mathfrak{m}}$ injective. Suppose $f_{\mathfrak{m}}(x/s) = 0 \in N_{\mathfrak{m}}$. This means that $f(x)/s = 0$ in the localized module, so that $f(x) \in M$ is killed by some $t \in R - \mathfrak{m}$. We thus have $f(tx) = t(f(x)) = 0 \in M$. This means that $tx = 0 \in M$ since f is injective. But this in turn means that $x/s = 0 \in M_{\mathfrak{m}}$. This is what we wanted to show. □

1.3 Localization is exact

Localization is to be thought of as a very mild procedure.

The next result says how inoffensive localization is. This result is a key tool in reducing problems to the local case.

Proposition 1.15. *Suppose $f : M \to N, g : N \to P$ and $M \to N \to P$ is exact. Let $S \subset R$ be multiplicatively closed. Then*

$$S^{-1}M \to S^{-1}N \to S^{-1}P$$

is exact.

Or, as one can alternatively express it, localization is an *exact functor.*

Before proving it, we note a few corollaries:

Corollary 1.16. *If $f : M \to N$ is surjective, then $S^{-1}M \to S^{-1}N$ is too.*

Proof. To say that $A \to B$ is surjective is the same as saying that $A \to B \to 0$ is exact. From this the corollary is evident. □

Similarly:

Corollary 1.17. *If $f : M \to N$ is injective, then $S^{-1}M \to S^{-1}N$ is too.*

Proof. To say that $A \to B$ is injective is the same as saying that $0 \to A \to B$ is exact. From this the corollary is evident. □

Proof of the proposition. We adopt the notation of the proposition. If the composite $g \circ f$ is zero, clearly the localization $S^{-1}M \to S^{-1}N \to S^{-1}P$ is zero too. Call the maps $S^{-1}M \to S^{-1}N, S^{-1}N \to S^{-1}P$ as ϕ, ψ. We know that $\psi \circ \phi = 0$ so $\ker(\psi) \supset \text{Im}(\phi)$. Conversely, suppose something belongs to $\ker(\psi)$. This can be written as a fraction

$$x/s \in \ker(\psi)$$

where $x \in N, s \in S$. This is mapped to

$$g(x)/s \in S^{-1}P,$$

which we're assuming is zero. This means that there is $t \in S$ with $tg(x) = 0 \in P$. This means that $g(tx) = 0$ as an element of P. But $tx \in N$ and its image of g vanishes, so tx must come from something in M. In particular,

$$tx = f(y) \text{ for some } y \in M.$$

In particular,

$$\frac{x}{s} = \frac{tx}{ts} = \frac{f(y)}{ts} = \phi(y/ts) \in \text{Im}(\phi).$$

This proves that anything belonging to the kernel of ψ lies in $\text{Im}(\phi)$. □

1.4 Nakayama's lemma

We now state a very useful criterion for determining when a module over a *local* ring is zero.

TO BE ADDED: definition of finitely generated

Lemma 1.18 (Nakayama's lemma)**.** *If R is a local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. If $\mathfrak{m}M = M$, then $M = 0$.*

Note that $\mathfrak{m}M$ is the submodule generated by products of elements of $\mathfrak{m}$ and M.

Remark. Once one has the theory of the tensor product, this equivalently states that if M is finitely generated, then

$$M \otimes_R R/\mathfrak{m} = M/\mathfrak{m}M \neq 0.$$

So to prove that a finitely generated module over a local ring is zero, you can reduce to studying the reduction to $R/\mathfrak{m}$. This is thus a very useful criterion.

Proof. Suppose M is generated by $\{x_1, \ldots, x_n\} \subset M$. This means that every element of M is a linear combination of elements of x_i. However, each $x_i \in \mathfrak{m}M$ by assumption. In particular, each x_i can be written as

$$x_i = \sum a_{ij} x_j, \text{ where } a_{ij} \in \mathfrak{m}.$$

If we let A be the matrix $\{a_{ij}\}$, then A sends the vector of the $\{x_i\}$ into itself. In particular, $(I - A)$ kills the vectors x_i.

Now $I - A$ is an n-by-n matrix in the ring R. We could, of course, reduce everything modulo $\mathfrak{m}$ to get the identity; this is because A consists of elements of $\mathfrak{m}$. It follows that the determinant must be congruent to 1 modulo $\mathfrak{m}$.

In particular, $\det(I - A)$ is invertible, since R is local. It follows that $I - A$ is itself invertible. This, however, is a contradiction, since it kills the vector $\{x_i\}$, unless all the x_i are zero. □

Nakayama's lemma highlights why it is so useful to work over a local ring. Thus, it is useful to reduce questions about general rings to questions about local rings.

Exercise 2.5. Give a counterexample to the conclusion of Nakayama's lemma when the module is not finitely generated.

Exercise 2.6. Let M be a finitely generated module over the ring R. Let $\mathfrak{J}$ be the Jacobson radical of R (cf. Exercise 1.21). If $\mathfrak{J}M = M$, then $M = 0$.

Exercise 2.7. Here is an alternative proof of Nakayama's lemma. Let R be local with maximal ideal $\mathfrak{m}$, and let M be a finitely generated module with $\mathfrak{m}M = M$. Let n be the minimal number of generators for M. If $n > 0$, pick generators $x_1, \ldots, x_n$. Then write $x_1 = a_1 x_1 + \cdots + a_n x_n$ where each $a_i \in \mathfrak{m}$. Deduce that x_1 is in the submodule generated by the $x_i, i \geq 2$, so that n was not actually minimal, contradiction.

2 The functor Hom

We continue to discuss some basic constructions that one can do with a module over a commutative ring. In any category, the morphisms between two objects form a set.[1] In many categories, however, the hom-sets have additional structure. The hom-sets between abelian groups are themselves abelian groups. The same situation holds for the category of modules over a commutative ring.

Definition 2.1. Let R be a commutative ring and M, N to be R-modules. We write $\mathrm{Hom}_R(M, N)$ for the set of all R-module homomorphisms $M \to N$. $\mathrm{Hom}_R(M, N)$ is an R-module because one can add homomorphisms $f, g : M \to N$ by adding them pointwise

$$(f + g)(m) = f(m) + g(m)$$

and one can multiply homomorphisms by elements in R:

$$(af)(m) = a(f(m)), \forall a \in A.$$

[1] This may depend on your set-theoretic foundations.

In particular, we get a bifunctor Hom, contravariant in the first variable and covariant in the second, of R-modules into R-modules.

2.1 Exactness

We now discuss the exactness properties of this construction of forming Hom-sets. The following result is basic and is, in fact, a reflection of the universal property of the kernel.

Proposition 2.2. *If M is an R-module, then the construction*

$$N \to \mathrm{Hom}_R(M, N)$$

is left exact (but not exact *in general).*

This means that if

$$0 \to N' \to N \to N''$$

is exact, then

$$0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'')$$

is exact as well.

Proof. First, we have to show that the map $\mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N)$ is injective; this is because $N' \to N$ is injective, and composition with $N' \to N$ can't kill any nonzero $M \to N'$. Similarly, exactness in the middle can be checked easily, and follows from Exercise 1.14; it states simply that a map $M \to N$ has image landing inside N' (i.e. factors through N') if and only if it composes to zero in N''. □

This functor $\mathrm{Hom}_R(M, \cdot)$ is not exact in general. Indeed:

Example 2.3. Suppose $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$. There is a short exact sequence

$$0 \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Let us apply $\mathrm{Hom}_R(M, \cdot)$. We get a *complex*

$$0 \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, 2\mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to 0.$$

The last term is $\mathbb{Z}/2\mathbb{Z}$; everything else is zero. This is not exact at the last point.

2.2 Projective modules

Sometimes, however, we do have exactness. We axiomatize this with the following.

Definition 2.4. An R-module M is called **projective** if $\mathrm{Hom}_R(M, \cdot)$ is exact.[2]

[2]It is possible to define a projective module over a noncommutative ring. The definition is the same, except that the Hom-sets are no longer modules, but simply groups.

Projective modules have a very clean characterization. They are the direct summands in free modules.

TO BE ADDED: check this

Proposition 2.5. *The following are equivalent for an R-module M:*

1. *M is projective.*
2. *Given any map $M \to N/N'$ from M into a quotient N/N', we can lift it to a map $M \to N$.*
3. *There is a module M' such that $M \oplus M'$ is free.*

Proof. The equivalence of 1 and 2 is just unwinding the definition of projectivity, because we just need to show that $\mathrm{Hom}_R(M, \cdot)$ preserves surjective maps, i.e. quotients. ($\mathrm{Hom}_R(M, \cdot)$ is already left-exact, after all.) To say that $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N/N')$ is just the statement that maps can be lifted.

Let us first show that 2 implies 3. Suppose M satisfies 2. Then choose a surjection $P \to M$ where P is free. (E.g. P the free module generated by all the elements of M.) Then we can write $M \simeq P/P'$ for $P' \subset P$. The isomorphism map $M \to P/P'$ leads to a lifting $M \to P$. In particular, there is a section of $P \to M$, namely this lifting. Then $P \simeq \ker(P \to M) \oplus \mathrm{Im}(M \to P) \simeq \ker(P \to M) \oplus M$, verifying 3 since P is free.

Now let us show that 3 implies 2. Suppose $M \oplus M'$ is free, isomorphic to P. Then a map $M \to N/N'$ can be extended to

$$P \to N/N'$$

by declaring it to be trivial on M'. But now $P \to N/N'$ can be lifted to N because P is free; we just lift the image of a basis, and this defines $P \to N$. Compose this with the inclusion $M \to P$, and get $M \to P \to N$ which is the lifting of $M \to N/N'$. $\square$

So projective modules are precisely those with the following lifting property. Consider a diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow & & \\ M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

where the bottom row is exact. Then, if P is projective, there is a lifting $P \to M$ making commutative the diagram

$$\begin{array}{ccccc} & & P & & \\ & \swarrow & \downarrow & & \\ M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

Corollary 2.6. *Let M be a module. Then there is a surjection $P \twoheadrightarrow M$, where P is projective.*

Proof. Indeed, we know (**??**) that we can always get a surjection from a free module. Since free modules are projective by Proposition 2.5, we are done. □

EXERCISE 2.8. Let R be a principal ideal domain, F' a submodule of a free module F. Show that F' is free. (Hint: well-order the set of generators of F, and climb up by transfinite induction.) In particular, any projective modules is free.

2.3 Injective modules

TO BE ADDED: the explanation via the small object argument

3 The tensor product

3.1 Bilinear maps

Let R be a commutative ring, as usual. We have just seen that the Hom-sets of R-modules are themselves R-modules. Consequently, if we have three R-modules M, N, P, we can think about module-homomorphisms

$$M \xrightarrow{\lambda} \mathrm{Hom}_R(N, P).$$

Suppose $x \in M, y \in N$. Then we can consider

$$\lambda(x) \in \mathrm{Hom}_R(N, P)$$

and thus the element

$$\lambda(x)(y) \in P.$$

We denote this element $\lambda(x)(y)$ by $\lambda(x, y)$ for convenience; it is a function of two variables $M \times N \to P$. There are certain properties of $\lambda(\cdot, \cdot)$ that we list below. Fix $x, x' \in M$; $y, y' \in N$; $a \in R$. Then:

1. $\lambda(x, y + y') = \lambda(x, y) + \lambda(x, y')$ because $\lambda(x)$ is additive.
2. $\lambda(x, ay) = a\lambda(x, y)$ because $\lambda(x)$ is an R-module homomorphism.
3. $\lambda(x + x', y) = \lambda(x, y) + \lambda(x', y)$ because λ is additive.
4. $\lambda(ax, y) = a\lambda(x, y)$ because λ is an R-module R-module homomorphism.

Conversely, given a function of two variables satisfying the above properties, it is easy to see that we can get a morphism of R-modules $M \to \mathrm{Hom}_R(N, P)$.

Definition 3.1. An **R-bilinear map** $\lambda : M \times N \to P$ is a map satisfying the above conditions. In particular, it has to be R-linear in each variable.

The previous discussion shows that there is a bijection between R-bilinear maps $M \times N \to P$ with R-module maps $M \to \mathrm{Hom}_R(N, P)$. Note that the first interpretation is symmetric in M, N; the second, by contrast, can be interpreted in terms of the old concepts of an R-module map. So both are useful.

EXERCISE 2.9. Prove that a $\mathbb{Z}$-bilinear map out of $\mathbb{Z}/2 \times \mathbb{Z}/3$ is identically zero, whatever the target module.

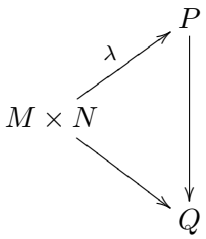
3.2 The tensor product

Given a bilinear map $M \times N \to P$ and a homomorphism $P \to P'$, we can clearly get a bilinear map $M \times N \to P'$ by composition. In particular, given M, N, there is a *contravariant functor* from R-modules to **Sets** sending any R-module P to the collection of R-bilinear maps $M \times N \to P$. As usual, we are interested in when this functor is *corepresentable.* As a result, we are interested in *universal* bilinear maps out of $M \times N$.

Definition 3.2. An R-bilinear map $\lambda : M \times N \to P$ is called **universal** if for all R-modules Q, the composition of $P \to Q$ with $M \times N \xrightarrow{\lambda} P$ gives a **bijection**

$$\mathrm{Hom}_R(P, Q) \simeq \{\text{bilinear maps } M \times N \to Q\}$$

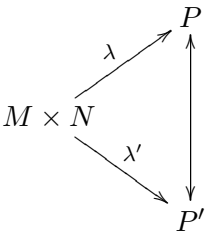
So, given a bilinear map $M \times N \to Q$, there is a **unique** map $P \to Q$ making the diagram



Alternatively, P *corepresents* the functor $Q \to \{\text{bilinear maps } M \times N \to Q\}$.

General nonsense says that given M, N, an universal R-bilinear map $M \times N \to P$ is **unique** up to isomorphism (if it exists). This is a general category theoretic observation, and follows from *Yoneda's lemma.* We can give a direct proof.

Suppose $M \times N \xrightarrow{\lambda} P$ was universal and $M \times N \xrightarrow{\lambda'} P'$ was also universal. Then by the universal property, there would be maps $P \to P'$ and $P' \to P$ making the following diagram commutative:



These compositions $P \to P' \to P, P' \to P \to P'$ have to be the identity because of the uniqueness part of the universal property.

We shall now show that this universal object does indeed exist.

Proposition 3.3. *Given M, N, a universal bilinear map out of $M \times N$ exists.*

Before proving it we make:

Definition 3.4. We denote the codomain of the universal map out of $M \times N$ by $M \otimes_R N$. This is called the **tensor product** of M, N.

Proof of Proposition 3.3. We will simply give a presentation of the tensor product by "generators and relations." Take the free R-module $M \otimes_R N$ generated by the symbols $\{x \otimes y\}_{x \in M, y \in N}$ and quotient out by the relations forced upon us by the definition of a bilinear map (for $x, x' \in M,\ y, y' \in N,\ a \in R$)

1. $(x + x') \otimes y = x \otimes y + x' \otimes y$.
2. $(ax) \otimes y = a(x \otimes y) = x \otimes (ay)$.
3. $x \otimes (y + y') = x \otimes y + x \otimes y'$.

We will abuse notation and denote $x \otimes y$ for its image in $M \otimes_R N$ (as opposed to the symbol generating the free module).

There is a bilinear map $M \times N \to M \otimes_R N$ sending $(x, y) \to x \otimes y$; the relations imposed imply that this map is a bilinear map. We have to check that it is universal, but this is actually quite direct.

Suppose we had a bilinear map $\lambda : M \times N \to P$. We must construct a linear map $M \otimes_R N \to P$. To do this, we can just give a map on generators, and shows that it is zero on each of the relations. It is easy to see that to make the appropriate diagrams commute, the linear map $M \otimes N \to P$ has to send $x \otimes y \to \lambda(x, y)$.

This factors through the relations on $x \otimes y$ by bilinearity and leads to an R-linear map $M \otimes_R N \to P$ such that the following diagram commutes:

$$\begin{array}{ccc} M \times N & \longrightarrow & M \otimes_R N \\ & \searrow^{\lambda} & \downarrow \\ & & P \end{array}.$$

It is easy to see that $M \otimes_R N \to P$ is unique because the $x \otimes y$ generate it. □

The theory of the tensor product allows you to do away with bilinear maps and just think of linear maps.

Given M, N, we have constructed an object $M \otimes_R N$. It remains to see the functoriality. I claim that $(M, N) \to M \otimes_R N$ is a *covariant functor* in two variables from R-modules to R-modules. In particular, if $M \to M', N \to N'$ are morphisms, there is a canonical map

$$M \otimes_R N \to M' \otimes_R N'.$$

We make some observations and prove a few basic properties. As the proofs will show, one powerful way to prove things about an object is to reason about its universal property. If two objects have the same universal property, they are isomorphic.

Proposition 3.5. *The tensor product is symmetric: for R-modules M, N, we have $M \otimes_R N \simeq N \otimes_R M$ canonically.*

Proof. This is clear from the universal properties: giving a bilinear map out of $M \times N$ is the same as a bilinear map out $N \times M$. Thus $M \otimes_R N$ and $N \otimes_R N$ have the same universal property. It is also clear from the explicit construction. □

Proposition 3.6. *For an R-module M, there is a canonical isomorphism $M \to M \otimes_R R$.*

Proof. If we think in terms of bilinear maps, this statement is equivalent to the statement that a bilinear map $\lambda : M \times R \to P$ is the same as a linear map $M \to N$. Indeed, to do this, restrict λ to $\lambda(\cdot, 1)$. Given $f : M \to N$, similarly, we take for λ as $\lambda(x, a) = af(x)$. This gives a bijection as claimed. □

Proposition 3.7. *The tensor product is associative. There are canonical isomorphisms $M \otimes_R (N \otimes_R P) \simeq (M \otimes_R N) \otimes_R P$.*

Proof. There are a few ways to see this: one is to build it explicitly from the construction given, sending $x \otimes (y \otimes z) \to (x \otimes y) \otimes z$.

More conceptually, both have the same universal property: by general categorical nonsense (Yoneda's lemma), we need to show that for all Q, there is a canonical bijection

$$\mathrm{Hom}_R(M \otimes (N \otimes P)), Q) \simeq \mathrm{Hom}_R((M \otimes N) \otimes P, Q)$$

where the R's are dropped for simplicity. But both of these sets can be identified with the set of trilinear maps[3] $M \times N \times P \to Q$. Indeed

$$\begin{aligned}
\mathrm{Hom}_R(M \otimes (N \otimes P), Q) &\simeq \text{bilinear } M \times (N \otimes P) \to Q \\
&\simeq \mathrm{Hom}(N \otimes P, \mathrm{Hom}(M, Q)) \\
&\simeq \text{bilinear } N \times P \to \mathrm{Hom}(M, Q) \\
&\simeq \mathrm{Hom}(N, \mathrm{Hom}(P, \mathrm{Hom}(M, Q)) \\
&\simeq \text{trilinear maps.}
\end{aligned}$$

□

3.3 The adjoint property

Finally, while we defined the tensor product in terms of a "universal bilinear map," we saw earlier that bilinear maps could be interpreted as maps into a suitable Hom-set. In particular, fix R-modules M, N, P. We know that the set of bilinear maps $M \times N \to P$ is naturally in bijection with

$$\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$$

as well as with

$$\mathrm{Hom}_R(M \otimes_R, N, P).$$

As a result, we find:

[3] Easy to define.

Proposition 3.8. *For R-modules M, N, P, there is a natural bijection*

$$\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \simeq \mathrm{Hom}_R(M \otimes_R N, P).$$

There is a more evocative way of phrasing the above natural bijection. Given N, let us define the functors F_N, G_N via

$$F_N(M) = M \otimes_R N, \quad G_N(P) = \mathrm{Hom}_R(N, P).$$

Then the above proposition states that there is a natural isomorphism

$$\mathrm{Hom}_R(F_N(M), P) \simeq \mathrm{Hom}_R(M, G_N(P)).$$

In particular, F_N and G_N are *adjoint functors*. So, in a sense, the operations of Hom and $\otimes$ are dual to each other.

Proposition 3.9. *Tensoring commutes with colimits.*

In particular, it follows that if $\{N_\alpha\}$ is a family of modules, and M is a module, then

$$M \otimes_R \bigoplus N_\alpha = \bigoplus M \otimes_R N_\alpha.$$

Exercise 2.10. Give an explicit proof of the above relation.

Proof. This is a formal consequence **TO BE ADDED:** proof □

3.4 The tensor product as base-change

Before this, we have considered the tensor product as a functor within a fixed category. Now, we shall see that when one takes the tensor product with a *ring*, one gets additional structure. As a result, we will be able to get natural functors between *different* module categories.

Suppose we have a ring-homomorphism $\phi : R \to R'$. In this case, any R'-module can be regarded as an R-module. In particular, there is a canonical functor of *restriction*

$$R' - \text{modules} \to R - \text{modules}.$$

We shall see that the tensor product provides an *adjoint* to this functor. Namely, if M has an R-module structure, then $M \otimes_R R'$ has an R' module structure where R' acts on the right. Since the tensor product is functorial, this gives a functor in the opposite direction:

$$R - \text{modules} \to R' - \text{modules}.$$

Let M' be an R'-module and M an R-module. In view of the above, we can talk about

$$\mathrm{Hom}_R(M, M')$$

by thinking of M' as an R-module.

Proposition 3.10. *There is a canonical isomorphism between*

$$\mathrm{Hom}_R(M, M') \simeq \mathrm{Hom}_{R'}(M \otimes_R R', M').$$

In particular, the restriction functor and the functor $M \to M \otimes_R R'$ are adjoints to each other.

Proof. We can describe the bijection explicitly. Given an R'-homomorphism $f : M \otimes_R R' \to M'$, we get a map

$$f_0 : M \to M'$$

sending

$$m \to m \otimes 1 \to f(m \otimes 1).$$

This is easily seen to be an R-module-homomorphism. Indeed,

$$f_0(ax) = f(ax \otimes 1) = f(\phi(a)(x \otimes 1)) = af(x \otimes 1) = af_0(x)$$

since f is an R'-module homomorphism.

Conversely, if we are given a homomorphism of R-modules

$$f_0 : M \to M'$$

then we can define

$$f : M \otimes_R R' \to M'$$

by sending $m \otimes r' \to r' f_0(m)$, which is a homomorphism of R' modules. This is well-defined because f_0 is a homomorphism of R-modules. We leave some details to the reader. □

Example 3.11. In the representation theory of finite groups, the operation of tensor product corresponds to the procedure of *inducing* a representation. Namely, if $H \subset G$ is a subgroup of a group G, then there is an obvious restriction functor from G-representations to H-representations. The adjoint to this is the induction operator. Since a H-representation (resp. a G-representation) is just a module over the group ring, the operation of induction is really a special case of the tensor product. Note that the group rings are generally not commutative, so this should be interpreted with some care.

4 Exactness properties of the tensor product

In general, the tensor product is not exact; it is only exact on the right, but it can fail to preserve injections. Yet in some important cases it *is* exact. We study that in the present section.

4.1 Right-exactness of the tensor product

We will start by talking about extent to which tensor products do preserve exactness under any circumstance. First, let's recall what is going on. If M, N are R-modules over the commutative ring R, we have defined another R-module $\mathrm{Hom}_R(M, N)$ of morphisms $M \to N$. This is left-exact as a functor of N. In other words, if we fix M and let N vary, then the construction of homming out of M preserves kernels.

In the language of category theory, this construction $N \to \mathrm{Hom}_R(M, N)$ has an adjoint. The other construction we discussed last time was this adjoint, and it is the tensor product. Namely, given M, N we defined a **tensor product** $M \otimes_R N$ such that giving a map $M \otimes_R N \to P$ into some R-module P is the same as giving a bilinear map $\lambda : M \times N \to P$, which in turn is the same as giving an R-linear map

$$M \to \mathrm{Hom}_R(N, P).$$

So we have a functorial isomorphism

$$\mathrm{Hom}_R(M \otimes_R N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

Alternatively, tensoring is the left-adjoint to the hom functor. By abstract nonsense, it follows that since $\mathrm{Hom}(M, \cdot)$ preserves cokernels, the left-adjoint preserves cokernels and is right-exact. We shall see this directly.

Proposition 4.1. *The functor $N \to M \otimes_R N$ is right-exact, i.e. preserves cokernels.*

In fact, the tensor product is symmetric, so it's right exact in either variable.

Proof. We have to show that if $N' \to N \to N'' \to 0$ is exact, then so is

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

There are a lot of different ways to think about this. For instance, we can look at the direct construction. The tensor product is a certain quotient of a free module.

$M \otimes_R N''$ is the quotient of the free module generated by $m \otimes n'', m \in M, n \in N''$ modulo the usual relations. The map $M \otimes N \to M \otimes N''$ sends $m \otimes n \to m \otimes n''$ if n'' is the image of n in N''. Since each n'' can be lifted to some n, it is obvious that the map $M \otimes_R N \to M \otimes_R N''$ is surjective.

Now we know that $M \otimes_R N''$ is a quotient of $M \otimes_R N$. But which relations do you have to impose on $M \otimes_R N$ to get $M \otimes_R N''$? In fact, each relation in $M \otimes_R N''$ can be lifted to a relation in $M \otimes_R N$, but with some redundancy. So the only thing to quotient out by is the statement that $x \otimes y, x \otimes y'$ have the same image in $M \otimes N''$. In particular, we have to quotient out by

$$x \otimes y - x \otimes y' \ , y - y' \in N'$$

so that if we kill off $x \otimes n'$ for $n' \in N' \subset N$, then we get $M \otimes N''$. This is a direct proof.

You can also give a conceptual proof. We'd like to know that $M \otimes N''$ is the cokernel of $M \otimes N' \to M \otimes N''$. In other words, we'd like to know that if we mapped

$M \otimes_R N$ into some P and the pull-back to $M \otimes_R N'$, it'd factor uniquely through $M \otimes_R N''$. Namely, we need to show that

$$\mathrm{Hom}_R(M \otimes N'', P) = \ker(\mathrm{Hom}_R(M \otimes N, P) \to \mathrm{Hom}_R(M \otimes N'', P)).$$

But the first is just $\mathrm{Hom}_R(N'', \mathrm{Hom}_R(M, P))$ by the adjointness property. Similarly, the second is just

$$\ker(\mathrm{Hom}_R(N, \mathrm{Hom}(M, P)) \to \mathrm{Hom}_R(N', \mathrm{Hom}_R(M, P))$$

but this last statement is $\mathrm{Hom}_R(N'', \mathrm{Hom}_R(M, P))$ by just the statement that $N'' = \mathrm{coker}(N' \to N)$. To give a map N'' into some module (e.g. $\mathrm{Hom}_R(M, P)$) is the same thing as giving a map out of N which kills N'. So we get the functorial isomorphism. □

Remark. Formation of tensor products is, in general, **not** exact.

Example 4.2. Let $R = \mathbb{Z}$. Let $M = \mathbb{Z}/2\mathbb{Z}$. Consider the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

which we can tensor with M, yielding

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to 0$$

I claim that the second thing $\mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z}$ is zero. This is because by tensoring with $\mathbb{Z}/2\mathbb{Z}$, we've made multiplication by 2 identically zero. By tensoring with $\mathbb{Q}$, we've made multiplication by 2 invertible. The only way to reconcile this is to have the second term zero. In particular, the sequence becomes

$$0 \to \mathbb{Z}/2\mathbb{Z} \to 0 \to 0 \to 0$$

which is not exact.

4.2 Flatness

In some cases, though, the tensor product is exact.

Definition 4.3. Let R be a commutative ring. An R-module M is called **flat** if the functor $N \to M \otimes_R N$ is exact. We already know that it right exact, so the only thing to be checked is that the operation of tensoring by M preserves injections.

Example 4.4. $\mathbb{Z}/2\mathbb{Z}$ is not flat as a $\mathbb{Z}$-module by Example 4.2.

Example 4.5. If R is a ring, then R is flat as an R-module, because tensoring by R is the identity functor.

More generally, if P is a projective module (i.e., homming out of P is exact), then P is flat.

Proof. If $P = \bigoplus_A R$ is free, then tensoring with P corresponds to taking the direct sum A times, i.e.

$$P \otimes_R M = \bigoplus_A M.$$

This is because tensoring with R preserves (finite or direct) infinite sums. The functor $M \to \bigoplus_A M$ is exact, so free modules are flat.

A projective module, as discussed earlier, is a direct summand of a free module. So if P is projective, $P \oplus P' \simeq \bigoplus_A R$ for some P'. Then we have that

$$(P \otimes_R M) \oplus (P' \otimes_R M) \simeq \bigoplus_A M.$$

If we had an injection $M \to M'$, then there is a direct sum decomposition yields a sequence of maps

$$P \otimes_R M' \to P \otimes_R M \to P \otimes_R M \oplus P \otimes_R M' \to \bigoplus_A M$$

and the composition map is injective since its sum with $P' \otimes M' \to P' \otimes M'$ is injective. FIX □

We now interpret localization as a tensor product.

Theorem 4.6. *Let R be a commutative ring, $S \subset R$ a multiplicative subset. Then there exists a canonical isomorphism of functors:*

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

In particular, $S^{-1}R$ is a flat R-module, because localization is an exact functor.

Proof. Here is a construction of ϕ. If $x/s \in S^{-1}M$ where $x \in M, s \in S$, we define

$$\phi(x/s) = (1/s) \otimes m.$$

Let us check that this is well-defined. Suppose $x/s = x'/s'$; then this means there is $t \in S$ with

$$xs't = x'st.$$

From this we need to check that $\phi(x/s) = \phi(x'/s')$, i.e. that $1/s \otimes x$ and $1/s' \otimes x'$ represent the same elements in the tensor product. But we know from the last statement that

$$\frac{1}{ss't} \otimes xs't = \frac{1}{ss't}x'st \in S^{-1}R \otimes M$$

and the first is just

$$s't(\frac{1}{ss't} \otimes x) = \frac{1}{s} \otimes x$$

by linearity, while the second is just

$$\frac{1}{s'} \otimes x'$$

similarly. One next checks that ϕ is an R-module homomorphism, which we leave to the reader.

Finally, we need to describe the inverse. The inverse $\psi : S^{-1}R \otimes M \to S^{-1}M$ is easy to construct because it's a map out of the tensor product, and we just need to give a bilinear map

$$S^{-1}R \times M \to S^{-1}M,$$

and this sends $(r/s, m)$ to mr/s.

It is easy to see that ϕ, ψ are inverses to each other by the definitions. □

It is, perhaps, worth making a small categorical comment, and offering an alternative argument. We are given two functors F, G from R-modules to $S^{-1}R$-modules, where $F(M) = S^{-1}R \otimes_R M$ and $G(M) = S^{-1}M$. By the universal property, the map $M \to S^{-1}M$ from an R-module to a tensor product gives a natural map

$$S^{-1}R \otimes_R M \to S^{-1}M,$$

that is a natural transformation $F \to G$.

Let us make a few other comments.

Remark. Let $\phi : R \to R'$ be a homomorphism of rings. Then, first of all, any R'-module can be regarded as an R-module by composition with ϕ. In particular, R' is an R-module.

If M is an R-module, we can define

$$M \otimes_R R'$$

as an R-module. But in fact this tensor product is an R'-module; it has an action of R'. If $x \in M$ and $a \in R'$ and $b \in R'$, multiplication of $(x \otimes a) \in M \otimes_R R'$ by $b \in R'$ sends this, *by definition*, to

$$b(x \otimes a) = x \otimes ab.$$

It is easy to check that this defines an action of R' on $M \otimes_R R'$. (One has to check that this action factors through the appropriate relations, etc.)

4.3 Tensor products of algebras

There is one other basic property of tensor products to discuss before moving on: namely, what happens when one tensors a ring with another ring. Let R be a commutative ring and suppose we have ring homomorphisms

$$\phi_0 : R \to R_0, \quad \phi_1 : R \to R_1.$$

Proposition 4.7. *Then $R_0 \otimes_R R_1$ has the structure of a commutative ring.*

Proof. Indeed, this multiplication multiplies two typical elements $x \otimes y, x' \otimes y'$ by sending them to $xx' \otimes yy'$. The ring structure is determined by this formula. One ought to check that this approach respects the relations of the tensor product. We will do so in an indirect way.

One can also think of this as follows. Multiplication is the same thing as giving an R-bilinear map

$$(R_0 \otimes_R R_1) \times (R_0 \otimes R_1) \to R_0 \otimes_R R_1,$$

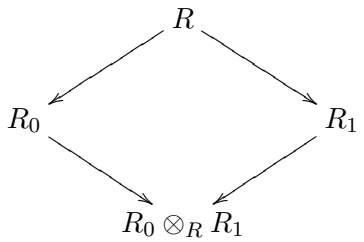
i.e. an R-linear map

$$(R_0 \otimes_R R_1) \otimes_R (R_0 \otimes R_1) \to R_0 \otimes_R R_1.$$

But the left side is isomorphic to $(R_0 \otimes_R R_0) \otimes_R (R_1 \otimes_R R_1)$. Since we have bilinear maps $R_0 \times R_0 \to R_0$ and $R_1 \times R_1 \to R_1$, we get linear maps $R_0 \otimes_R R_0 \to R_0$ and $R_1 \otimes_R R_1 \to R_1$. Tensoring these maps gives the multiplication as a bilinear map. It is easy to see that these two approaches are the same.

We now need to check that this operation is commutative and associative, with $1 \otimes 1$ as a unit; moreover, it distributes over addition. Distributivity over addition is built into the construction (i.e. in view of bilinearity). The rest (commutativity, associativity, units) can be checked directly on the generators, since we have distributivity. □

We can in fact describe the tensor product of R-algebras by a universal property. We will describe a commutative diagram:



Here $R_0 \to R_0 \otimes_R R_1$ sends $x \to x \otimes 1$; similarly for $R_1 \to R_0 \otimes_R R_1$. These are ring-homomorphisms, and it is easy to see that the above diagram commutes, since $r \otimes 1 = 1 \otimes r = r(1 \otimes 1)$ for $r \in R$.

In fact,

Proposition 4.8. *$R_0 \otimes_R R_1$ is universal with respect to this property: in the language of category theory, the above diagram is a pushout square.*

This means for any commutative ring B, and every pair of maps $u_0 : R_0 \to B$ and $u_1 : R_1 \to B$ such that the pull-backs $R \to R_0 \to B$ and $R \to R_1 \to B$ are the same, then we get a unique map of rings

$$R_0 \otimes_R R_1 \to B$$

which restricts on R_0, R_1 to the morphisms u_0, u_1 that we started with.

Proof. We make B into an R-module by the map $R \to R_0 \to B$ (or $R \to R_1 \to B$, it is the same by assumption). This map $R_0 \otimes_R R_1 \to B$ sends

$$x \otimes y \to u_0(x)u_1(y).$$

It is easy to check that $(x, y) \to u_0(x)u_1(y)$ is R-bilinear (because of the condition that the two pull-backs of u_0, u_1 to R are the same), and that it gives a homomorphism of rings $R_0 \otimes_R R_1 \to B$ which restricts to u_0, u_1 on R_0, R_1. One can check, for instance, that this is a homomorphism of rings by looking at the generators.

It is also clear that $R_0 \otimes_R R_1 \to B$ is unique, because we know that the map on elements of the form $x \otimes 1$ and $1 \otimes y$ is determined by u_0, u_1; these generate $R_0 \otimes_R R_1$, though. □

Chapter 3

The Spec of a ring

1 The spectrum of a ring

We shall now associate to every commutative ring a topological space Spec$R$ in a functorial manner. This construction is the basis for scheme-theoretic algebraic geometry and will be used frequently in the sequel.

1.1 Definition and examples

Definition 1.1. Let R be a commutative ring. The **spectrum** of R, denoted Spec$R$, is the collection of prime ideals of R.

We shall now make Spec$R$ into a topological space. First, we describe a collection of sets which will become the closed sets. If $I \subset R$ is an ideal, let

$$V(I) = \{\mathfrak{p} : \mathfrak{p} \supset I\} \subset \text{Spec}R.$$

Proposition 1.2. *There is a topology on* Spec$R$ *such that the closed subsets are of the form* $V(I)$ *for* $I \subset R$ *an ideal.*

Proof. Indeed:

1. $\emptyset = V((1))$ because (1) is not prime. So $\emptyset$ is closed.

2. Spec$R = V((0))$ because any ideal contains zero. So Spec$R$ is closed.

3. We show the closed sets are stable under intersections. Let $K_\alpha = V(I_\alpha)$ be closed subsets of Spec$R$ for α ranging over some index set. Let $I = \sum I_\alpha$. Then
$$V(I) = \bigcap K_\alpha = \bigcap V(I_\alpha),$$
which follows because I is the smallest ideal containing each I_α, so a prime contains every I_α iff it contains I.

4. The closed sets are closed under pairwise unions. If $K, K' \subset \mathrm{Spec}R$ are closed, we show $K \cup K'$ is closed. Say $K = V(I), K' = V(I')$. Then we claim:

$$K \cup K' = V(II').$$

Here II' is the ideal generated by products $ii', i \in I, i' \in I'$. If $\mathfrak{p}$ is **prime** and contains II', it must contain one of I, I'; this implies the displayed equation above and implies the result.

□

Definition 1.3. The topology on Spec$R$ defined above is called the **Zariski topology**.

In order to see the geometry of this construction, let us work several examples.

Example 1.4. Let $R = \mathbb{Z}$, and consider Spec$\mathbb{Z}$. Then every prime is generated by one element, since $\mathbb{Z}$ is a PID. We have that $\mathrm{Spec}\mathbb{Z} = \{(0)\} \cup \bigcup_{p \text{ prime}} \{(p)\}$. The picture is that one has all the familiar primes $(2), (3), (5), \ldots$, and then a special point (0).

Let us now describe the closed subsets. These are of the form $V(I)$ where $I \subset \mathbb{Z}$ is an ideal, so $I = (n)$ for some $n \in \mathbb{Z}$.

1. If $n = 0$, the closed subset is all of Spec$\mathbb{Z}$.

2. If $n \neq 0$, then n has finitely many prime divisors. So $V((n))$ consists of the prime ideals corresponding to these prime divisors.

The only closed subsets besides the entire space are the finite subsets that exclude (0).

Example 1.5. Say $R = \mathbb{C}[x, y]$ is a polynomial ring in two variables. What is Spec$R$? We won't give a complete answer. But we will write down several prime ideals.

1. For every pair of complex numbers $s, t \in \mathbb{C}$, the collection of polynomials $f \in R$ such that $f(s, t) = 0$ is a prime ideal $\mathfrak{m}_{s,t}$. In fact, it is maximal, as the residue field is all of $\mathbb{C}$. Indeed, $R/\mathfrak{m}_{s,t} \simeq \mathbb{C}$ under the map $f \to f(s, t)$.

   In fact,

   Theorem 1.6. *The $\mathfrak{m}_{s,t}$ are all the maximal ideals in R.*

   This will follow from the *Hilbert Nullstellensatz* to be proved later in the course.

2. $(0) \subset R$ is a prime ideal since R is a domain.

3. If $f(x,y) \in R$ is an irreducible polynomial, then (f) is a prime ideal. This is equivalent to unique factorization in R.[1]

To draw Spec$R$, we start by drawing $\mathbb{C}^2$, the collection of maximal ideals. Spec$R$ has additional (non-closed) points too, as described above, but for now let us consider the topology induced on $\mathbb{C}^2$ as a subspace of Spec$R$.

The closed subsets of Spec$R$ are subsets $V(I)$ where I is an ideal, generated by some polynomials $\{f_\alpha(x,y)\}$. It is of interest to determine the subset of $\mathbb{C}^2$ that $V(I)$ induces. In other words, we ask:

What points of $\mathbb{C}^2$ (with (s,t) identified with $\mathfrak{m}_{s,t}$) lie in $V(I)$?

Now we know that (s,t) corresponds to a point of I if and only if $I \subset \mathfrak{m}_{s,t}$. This is true iff all the f_α lie in $\mathfrak{m}_{s,t}$, i.e. if $f_\alpha(s,t) = 0$ for all α. So the closed subsets of $\mathbb{C}^2$ (with the induced Zariski topology) are precisely the subsets that can be defined by polynomial equations. This is **much** coarser than the usual topology. For instance, $\{(z_1,z_2) : \Re(z_1) \geq 0\}$ is not Zariski-closed.

The Zariski topology is so coarse because one has only algebraic data (namely, polynomials, or elements of R) to define the topology.

Exercise 3.1. Let R_1, R_2 be commutative rings. Give $R_1 \times R_2$ a natural structure of a ring, and describe Spec$(R_1 \times R_2)$ in terms of SpecR_1 and SpecR_2.

Exercise 3.2. Let X be a compact Hausdorff space, $C(X)$ the ring of real continuous functions $X \to \mathbb{R}$. The maximal ideals in Spec$C(X)$ are in bijection with the points of X, and the topology induced on X (as a subset of Spec$C(X)$) is just the usual topology.

Exercise 3.3. Prove the following result: if X, Y are compact Hausdorff spaces and $C(X), C(Y)$ the associated rings of continuous functions, if $C(X), C(Y)$ are isomorphic as $\mathbb{R}$-algebras, then X is homeomorphic to Y.

1.2 The radical ideal-closed subset correspondence

We now return to the case of an arbitrary commutative ring R. If $I \subset R$, we get a closed subset $V(I) \subset$ Spec$R$. It is called $V(I)$ because one is supposed to think of it as the places where the elements of I "vanish," as the elements of R are something like "functions." This analogy is perhaps best seen in the example of a polynomial ring over an algebraically closed field, e.g. Example 1.5 above.

The map from ideals into closed sets is very far from being injective in general, though by definition it is surjective.

Example 1.7. If $R = \mathbb{Z}$ and p is prime, then $I = (p), I' = (p^2)$ define the same subset (namely, $\{(p)\}$) of Spec$R$.

[1] To be proved later **??**.

We now ask the question of why the map from ideals to closed subsets fails to be injective. As we shall see, the entire problem disappears if we restrict to *radical* ideals.

Definition 1.8. If I is an ideal, then the **radical** $\mathrm{Rad}(I)$ or $\sqrt{I}$ is defined as

$$\mathrm{Rad}(I) = \{x \in R : x^n \in I \text{ for some } n\}.$$

An ideal is **radical** if it is equal to its radical. (This is equivalent to the earlier Definition **??**.)

Before proceeding, we must check:

Lemma 1.9. *If I an ideal, so is* $\mathrm{Rad}(I)$.

Proof. Clearly $\mathrm{Rad}(I)$ is closed under multiplication since I is. Suppose $x, y \in \mathrm{Rad}(I)$; we show $x + y \in \mathrm{Rad}(I)$. Then $x^n, y^n \in I$ for some n (large) and thus for all larger n. The binomial expansion now gives

$$(x+y)^{2n} = x^{2n} + \binom{2n}{1} x^{2n-1}y + \cdots + y^{2n},$$

where every term contains either x, y with power $\geq n$, so every term belongs to I. Thus $(x+y)^{2n} \in I$ and, by definition, we see then that $x + y \in \mathrm{Rad}(I)$. □

The map $I \to V(I)$ does in fact depend only on the radical of I. In fact, if I, J have the same radical $\mathrm{Rad}(I) = \mathrm{Rad}(J)$, then $V(I) = V(J)$. Indeed, $V(I) = V(\mathrm{Rad}(I)) = V(\mathrm{Rad}(J)) = V(J)$ by:

Lemma 1.10. *For any I, $V(I) = V(\mathrm{Rad}(I))$.*

Proof. Indeed, $I \subset \mathrm{Rad}(I)$ and therefore obviously $V(\mathrm{Rad}(I)) \subset V(I)$. We have to show the converse inclusion. Namely, we must prove:

If $\mathfrak{p} \supset I$, then $\mathfrak{p} \supset \mathrm{Rad}(I)$.

So suppose $\mathfrak{p} \subset I$ is prime and $x \in \mathrm{Rad}(I)$; then $x^n \in I \subset \mathfrak{p}$ for some n. But $\mathfrak{p}$ is prime, so whenever a product of things belongs to $\mathfrak{p}$, a factor does. Thus since $x^n = x.x \ldots .x$, we must have $x \in \mathfrak{p}$. So

$$\mathrm{Rad}(I) \subset \mathfrak{p}$$

proving the quoted claim, and thus the lemma. □

There is a converse to this remark:

Proposition 1.11. *If $V(I) = V(J)$, then* $\mathrm{Rad}(I) = \mathrm{Rad}(J)$.

So two ideals define the same closed subset iff they have the same radical.

Proof. We write down a formula for $\mathrm{Rad}(I)$ that will imply this at once.

Lemma 1.12. *For a commutative ring R and an ideal $I \subset R$,*

$$\mathrm{Rad}(I) = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}.$$

From this, it follows that $V(I)$ determines $\mathrm{Rad}(I)$. This will thus imply the proposition. We now prove the lemma:

Proof. 1. We show $\mathrm{Rad}(I) \subset \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$. In particular, this follows if we show that if a prime contains I, it contains $\mathrm{Rad}(I)$; but we have already discussed this above.

2. If $x \notin \mathrm{Rad}(I)$, we will show that there is a prime ideal $\mathfrak{p} \supset I$ not containing x. This will imply the reverse inclusion and the lemma.

We want to find $\mathfrak{p}$ not containing x, more generally not containing any power of x. In particular, we want $\mathfrak{p} \cap \left\{1, x, x^2 \dots, \right\} = \emptyset$. This set $S = \{1, x, \dots\}$ is multiplicatively closed, in that it contains 1 and is closed under finite products. Right now, it does not hit I; we want to find a *prime* containing I that does not hit $\{x^n, n \geq 0\}$.

More generally, we will prove:

Sublemma 1.13. *Let S be multiplicatively closed set in any ring R and let I be any ideal with $I \cap S = \emptyset$. There is a prime ideal $\mathfrak{p} \supset I$ and does not intersect S.*

In English, any ideal missing S can be enlarged to a prime ideal missing S. This is actually fancier version of a previous argument. We showed earlier that any ideal not containing the multiplicatively closed subset $\{1\}$ can be contained in a prime ideal not containing 1 in **??**.

Note that the sublemma clearly implies the lemma when applied to $S = \{1, x, \dots\}$.

Proof of the sublemma. Let $P = \{J : J \supset I, J \cap S = \emptyset\}$. Then P is a poset with respect to inclusion. Note that $P \neq \emptyset$ because $I \in P$. Also, for any nonempty linearly ordered subset of P, the union is in P (i.e. there is an upper bound). We can invoke Zorn's lemma to get a maximal element of P. This element is an ideal $\mathfrak{p} \supset I$ with $\mathfrak{p} \cap S = \emptyset$. I claim that $\mathfrak{p}$ is prime.

First of all, $1 \notin \mathfrak{p}$ because $1 \in S$. We need only check that if $xy \in \mathfrak{p}$, then $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Suppose otherwise, so $x, y \notin \mathfrak{p}$. Then $(x, \mathfrak{p}) \notin P$ or $\mathfrak{p}$ would not be maximal. Ditto for $(y, \mathfrak{p})$.

In particular, we have that these bigger ideals both intersect S. This means that there are

$$a \in \mathfrak{p}, r \in R \quad \text{suchthat} \quad a + rx \in S$$

and

$$b \in \mathfrak{p}, r' \in R \quad \text{suchthat} \quad b + r'y \in S.$$

Now S is multiplicatively closed, so multiply $(a + rx)(b + r'y) \in S$. We find:

$$ab + ar'y + brx + rr'xy \in S.$$

Now $a, b \in \mathfrak{p}$ and $xy \in \mathfrak{p}$, so all the terms above are in $\mathfrak{p}$, and the sum is too. But this contradicts $\mathfrak{p} \cap S = \emptyset$. □

□

□

The upshot of the previous lemmata is :

Proposition 1.14. *There is a bijection between the closed subsets of* Spec$R$ *and radical ideals* $I \subset R$.

1.3 Functoriality of Spec

The construction $R \to \text{Spec}R$ is functorial in R in a contravariant sense. That is, if $f : R \to R'$, there is a continuous map $\text{Spec}R' \to \text{Spec}R$. This map sends $\mathfrak{p} \subset R'$ to $f^{-1}(\mathfrak{p}) \subset R$, which is easily seen to be a prime ideal in R. Call this map $F : \text{Spec}R' \to \text{Spec}R$. So far, we have seen that Spec$R$ induces a contravariant functor from **Rings** $\to$ **Sets**.

Exercise 3.4. A contravariant functor $F : \mathcal{C} \to$ **Sets** (for some category $\mathcal{C}$) is called **representable** if it is naturally isomorphic to a functor of the form $X \to \text{Hom}(X, X_0)$ for some $X_0 \in \mathcal{C}$, or equivalently if the induced covariant functor on $\mathcal{C}^{\text{op}}$ is corepresentable.

The functor $R \to \text{Spec}R$ is not representable. (Hint: Indeed, a representable functor must send the initial object into a one-point set.)

Next, we check that the morphisms induced on Spec's from a ring-homomorphism are in fact *continuous* maps of topological spaces.

Proposition 1.15. Spec *induces a contravariant functor from* **Rings** *to the category* **Top** *of topological spaces.*

Proof. Let $f : R \to R'$. We need to check that this map $\text{Spec}R' \to \text{Spec}R$, which we call F, is continuous. That is, we must check that F^{-1} sends closed subsets of Spec$R$ to closed subsets of SpecR'.

More precisely, if $I \subset R$ and we take the inverse image $F^{-1}(V(I)) \subset \text{Spec}R'$, it is just the closed set $V(f(I))$. This is best left to the reader, but here is the justification. If $\mathfrak{p} \in \text{Spec}R'$, then $F(\mathfrak{p}) = f^{-1}(\mathfrak{p}) \supset I$ if and only if $\mathfrak{p} \supset f(I)$. So $F(\mathfrak{p}) \in V(I)$ if and only if $\mathfrak{p} \in V(f(I))$.

□

Example 1.16. Let R be a commutative ring, $I \subset R$ an ideal, $f : R \to R/I$. There is a map of topological spaces

$$F : \text{Spec}(R/I) \to \text{Spec}R.$$

This map is a closed embedding whose image is $V(I)$. Most of this follows because there is a bijection between ideals of R containing I and ideals of R/I, and this bijection preserves primality.

EXERCISE 3.5. Show that this map $\mathrm{Spec}R/I \to \mathrm{Spec}R$ is indeed a homeomorphism from $\mathrm{Spec}R/I \to V(I)$.

2 Basic open sets

2.1 A basis for the Zariski topology

In the previous section, we were talking about the Zariski topology. If R is a commutative ring, we recall that $\mathrm{Spec}R$ is defined to be the collection of prime ideals in R. This has a topology where the closed sets are the sets of the form

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}R : \mathfrak{p} \supset I\}.$$

There is another way to describe the Zariski topology in terms of *open* sets.

Definition 2.1. If $f \in R$, we let

$$U_f = \{\mathfrak{p} : f \notin \mathfrak{p}\}$$

so that U_f is the subset of $\mathrm{Spec}R$ consisting of primes not containing f. This is the complement of $V((f))$, so it is open.

Proposition 2.2. *The sets U_f form a basis for the Zariski topology.*

Proof. Suppose $U \subset \mathrm{Spec}R$ is open. We claim that U is a union of basic open sets U_f.

Now $U = \mathrm{Spec}R - V(I)$ for some ideal I. Then

$$U = \bigcup_{f \in I} U_f$$

because if an ideal is not in $V(I)$, then it fails to contain some $f \in I$, i.e. is in U_f for that f. Alternatively, we could take complements, whence the above statement becomes

$$V(I) = \bigcap_{f \in I} V((f))$$

which is clear. □

The basic open sets have nice properties.

1. $U_1 = \mathrm{Spec}R$ because prime ideals are not allowed to contain the unit element.
2. $U_0 = \emptyset$ because every prime ideal contains 0.
3. $U_{fg} = U_f \cap U_g$ because fg lies in a prime $\mathfrak{p}$ if and only if one of f, g does.

Now let us describe what the Zariski topology has to do with localization.

Example 2.3. Let R be a ring and $f \in R$. Consider $S = \{1, f, f^2, \dots\}$; this is a multiplicatively closed subset. Last week, we defined $S^{-1}R$.

Definition 2.4. For S the powers of f, we write $R[f^{-1}] = S^{-1}R$.

There is a map $\phi : R \to R[f^{-1}]$ and a corresponding map

$$\mathrm{Spec}R[f^{-1}] \to \mathrm{Spec}R$$

sending a prime $\mathfrak{p} \subset R[f^{-1}]$ to $\phi^{-1}(\mathfrak{p})$.

Proposition 2.5. *This map induces a homeomorphism of* $\mathrm{Spec}R[f^{-1}]$ *onto* $U_f \subset \mathrm{Spec}R$.

So if you take a commutative ring and invert an element, you just get an open subset of Spec. This is why it's called localization: you are restricting to an open subset on the Spec level when you invert something.

Proof. 1. First, we show that $\mathrm{Spec}R[f^{-1}] \to \mathrm{Spec}R$ lands in U_f. If $\mathfrak{p} \subset R[f^{-1}]$, then we must show that the inverse image $\phi^{-1}(\mathfrak{p})$ can't contain f. If otherwise, that would imply that $\phi(f) \in \mathfrak{p}$; however, $\phi(f)$ is invertible, and then $\mathfrak{p}$ would be (1).

2. Let's show that the map surjects onto U_f. If $\mathfrak{p} \subset R$ is a prime ideal not containing f, i.e. $\mathfrak{p} \in U_f$. We want to construct a corresponding prime in the ring $R[f^{-1}]$ whose inv. image is $\mathfrak{p}$.

   Let $\mathfrak{p}[f^{-1}]$ be the collection of all fractions

   $$\{\frac{x}{f^n}, x \in \mathfrak{p}\} \subset R[f^{-1}],$$

   which is evidently an ideal. Note that whether the numerator is in $\mathfrak{p}$ is **independent** of the representing fraction $\frac{x}{f^n}$ used.[2] In fact, $\mathfrak{p}[f^{-1}]$ is a prime ideal. Indeed, suppose

   $$\frac{a}{f^m}\frac{b}{f^n} \in \mathfrak{p}[f^{-1}].$$

   Then $\frac{ab}{f^{m+n}}$ belongs to this ideal, which means $ab \in \mathfrak{p}$; so one of $a, b \in \mathfrak{p}$ and one of the two fractions $\frac{a}{f^m}, \frac{b}{f^n}$ belongs to $\mathfrak{p}[f^{-1}]$. Also, $1/1 \notin \mathfrak{p}[f^{-1}]$.

   It is clear that the inverse image of $\mathfrak{p}[f^{-1}]$ is $\mathfrak{p}$, because the image of $x \in R$ is $x/1$, and this belongs to $\mathfrak{p}[f^{-1}]$ precisely wehn $x \in \mathfrak{p}$.

3. The map $\mathrm{Spec}R[f^{-1}] \to \mathrm{Spec}R$ is injective. Suppose $\mathfrak{p}, \mathfrak{p}'$ are prime ideals in the localization and the inverse images are the same. We must show that $\mathfrak{p} = \mathfrak{p}'$.

   Suppose $\frac{x}{f^n} \in \mathfrak{p}$. Then $x/1 \in \mathfrak{p}$, so $x \in \phi^{-1}(\mathfrak{p}) = \phi^{-1}(\mathfrak{p}')$. This means that $x/1 \in \mathfrak{p}'$, so $\frac{x}{f^n} \in \mathfrak{p}'$ too. So a fraction that belongs to $\mathfrak{p}$ belongs to $\mathfrak{p}'$. By symmetry the two ideals must be the same.

[2] Suppose $\frac{x}{f^n} = \frac{y}{f^k}$ for $y \in \mathfrak{p}$. Then there is N such that $f^N(f^k x - f^n y) = 0 \in \mathfrak{p}$; since $y \in \mathfrak{p}$ and $f \notin \mathfrak{p}$, it follows that $x \in \mathfrak{p}$.

4. We now know that the map $\psi : \mathrm{Spec}R[f^{-1}] \to U_f$ is a continuous bijection. It is left to see that it is a homeomorphism. We will show that it is open. In particular, we have to show that a basic open set on the left side is mapped to an open set on the right side. If $y/f^n \in R[f^{-1}]$, we have to show that $U_{y/f^n} \subset \mathrm{Spec}R[f^{-1}]$ has open image under ψ. We'll in fact show what open set it is .

   I claim that
   $$\psi(U_{y/f^n}) = U_{fy} \subset \mathrm{Spec}R.$$
   To see this, $\mathfrak{p}$ is contained in U_{f/y^n}. This mean that $\mathfrak{p}$ doesn't contain y/f^n. In particular, $\mathfrak{p}$ doesn't contain the multiple $yf/1$. So $\psi(\mathfrak{p})$ doesn't contain yf. This proves the inclusion $\subset$.

   To complete the proof of the claim, and the result, we must show that if $\mathfrak{p} \subset \mathrm{Spec}R[f^{-1}]$ and $\psi(\mathfrak{p}) = \phi^{-1}(\mathfrak{p}) \in U_{fy}$, then y/f^n doesn't belong to $\mathfrak{p}$. (This is kosher and dandy because we have a bijection.) But the hypothesis implies that $fy \notin \phi^{-1}(\mathfrak{p})$, so $fy/1 \notin \mathfrak{p}$. Dividing by f^{n+1} implies that
   $$y/f^n \notin \mathfrak{p}$$
   and $\mathfrak{p} \in U_{f/y^n}$.

□

If $\mathrm{Spec}R$ is a space, and f is thought of as a "function" defined on $\mathrm{Spec}R$, the space U_f is to be thought of as the set of points where f "doesn't vanish" or "is invertible." Thinking about rings in terms of their spectra is a very useful idea, though we don't make too much use of it.

We will bring it up when appropriate.

Remark. The construction $R \to R[f^{-1}]$ as discussed above is an instance of localization. More generally, we can define $S^{-1}R$ for $S \subset R$ multiplicativelly closed. We can define maps
$$\mathrm{Spec}S^{-1}R \to \mathrm{Spec}R.$$
How can you think about the construction in general? You can think of it as
$$\varinjlim_{f \in S} R[f^{-1}]$$
which is a direct limit when you invert more and more elements.

As an example, consider $S = R - \mathfrak{p}$ for a prime $\mathfrak{p}$, and for simplicity that R is countable. We can write $S = S_0 \cup S_1 \cup \ldots$, where each S_k is generated by a finite number of elements $f_0, \ldots, f_k$. Then $R_{\mathfrak{p}} = \varinjlim S_k^{-1}R$. So we have
$$S^{-1}R = \varinjlim_k R[f_0^{-1}, f_1^{-1}, \ldots, f_k^{-1}] = \varinjlim R[(f_0 \ldots f_k)^{-1}].$$
The functions we invert in this construction are precisely those which do not contain $\mathfrak{p}$, or where "the functions don't vanish." The idea is that to construct $\mathrm{Spec}S^{-1}R =$

Spec$R_{\mathfrak{p}}$, we keep cutting out from Spec$R$ vanishing locuses of various functions that do not intersect $\mathfrak{p}$. In the end, you don't restrict to an open set, but to a direct limit of this.

Chapter 4

Integrality and valuation rings

The notion of integrality is familiar from number theory: it is like "algebraic" but with monic polynomials. In algebraic geometry, integral extensions of rings correspond to correspondingly nice morphisms on the Spec's—when the extension is finitely generated, it turns out that the fibers are finite. That is, there are only finitely many ways to lift a prime ideal to the extension.

Rings that are *integrally closed* in their quotient field will play an important role for us. Such "normal domains" are, for example, regular in codimension one, which means that the theory of Weil divisors (**??**) applies to them. It is particularly nice because Weil divisors are sufficient to determine whether a function is regular on a normal variety. A canonical example of an integrally closed ring is a valuation ring; we shall see in this chapter that any integrally closed ring is an intersection of such.

1 Integrality

1.1 Fundamentals

Let us return to the ring $\mathbb{Z}[\sqrt{-5}]$; this is the canonical example of a ring where unique factorization fails. This is because, as we remember,

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

Five is a big number; why did we have to go all the way to five to get this to happen? What about $\mathbb{Z}[\sqrt{-3}]$?

Here we have

$$(1 - \sqrt{-3})(1 + \sqrt{-3}) = 4 = 2 \times 2.$$

These elements can be factored no more, and $1 - \sqrt{-3}$ and 2 are not associates (they differ by something which isn't a unit). So in this ring, we have a failure of unique factorization. For some reason, this doesn't bother people as much.

The reason this doesn't bother people is that $\mathbb{Z}[\sqrt{-3}]$ is contained in the larger ring

$$\mathbb{Z}[\frac{1 + \sqrt{-3}}{2}],$$

which does have unique factorization.

In fact, $\mathbb{Z}[\sqrt{-3}]$ is an index two subgroup of the larger ring. The reason is that the larger ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ can be described by the set of elements $a + b\sqrt{-3}$ where a, b are either both integers or both integers plus $\frac{1}{2}$, as is easily seen: this set is closed under addition and multiplication. Note that, by contrast, $\mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$ does not contain $\mathbb{Z}[\sqrt{-5}]$ as a finite index subgroup—it can't be slightly enlarged in the same sense. When you enlarge $\mathbb{Z}[\sqrt{-5}]$, you have to add a lot of stuff.

Definition 1.1. Let $R \subset R'$ be an inclusion of integral domains. An element $x \in R'$ is said to be **integral** over R if x satisfies a monic polynomial equation in $R[X]$, say

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0.$$

Example 1.2. $\frac{1+\sqrt{-3}}{2}$ is integral over $\mathbb{Z}$; it is in fact a sixth root of unity.

Example 1.3. $\frac{1+\sqrt{5}}{2}$ is not integral over $\mathbb{Z}$. To explain this, we need to work a bit more.

We pause for a useful definition.

Definition 1.4. 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.

Suppose $R \subset R'$ are domains. Let $x \in R'$.

Proposition 1.5. *$x \in R'$ is integral over R if and only if the subalgebra $R[x]$ (generated by R, x) is a finitely generated R-module.*

This for instance lets us show that $\frac{1+\sqrt{-5}}{2}$ is not integral over $\mathbb{Z}$, because when you keep taking powers, you get arbitrarily large denominators: the arbitrarily large denominators imply that it cannot be integral.

Proof. If $x \in R'$ is integral, then x satisfies

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0.$$

Then $R[x]$ is generated as an R-module by $1, x, \ldots, x^{n-1}$. This is because the submodule generated by $1, x, \ldots, x^{n-1}$ is closed under multiplication by R and by multiplication by x (by the above equation).

Now suppose x generates a subalgebra $R[x] \subset R'$ which is a finitely generated R-module. Then the increasing sequence of R-modules generated by $\{1\}, \{1, x\}, \{1, x, x^2\}, \ldots$ must stabilize, since the union is $R[x]$. It follows that some x^n can be expressed as a linear combination of smaller powers of x. □

Last time we talked about integral extensions. If $R \subset R'$, we say that an element $x \in R'$ is **integral** over R if either of the following equivalent conditions are satisfied:

1. There is a monic polynomial in $R[X]$ which vanishes on x.

2. $R[x] \subset R'$ is a finitely generated R-module.

Last time we supposed that R, R' were domains, but this is not really necessary. The first thing to do is to add a third equivalent condition.

Proposition 1.6. *$x \in R'$ is integral if and only if there exists a finitely generated R-submodule $M \subset R'$ such that $R \subset M$ and $xM \subset M$.*

Proof. It's obvious that the second condition above (equivalent to integrality) implies the condition of this proposition. Indeed, you could just take $M = R[x]$.

Now let us prove that if there exists such an M which is finitely generated, then x is integral. Just because M is finitely generated, the submodule $R[x]$ is not obviously finitely generated. In particular, this implication requires a bit of proof.

We shall prove that the condition of this proposition implies integrality. Suppose $y_1, \dots, y_k \in M$ generate M as R-module. Then multiplication by x gives an R-module map $M \to M$. In particular, we can write

$$xy_i = \sum a_{ij} y_j$$

where each $a_{ij} \in R$. These $\{a_{ij}\}$ may not be unique, but let us make some choices; we get a k-by-k matrix $A \in M_k(R)$. The claim is that x satisfies the characteristic polynomial of A.

Consider the matrix

$$(x1 - A) \in M_n(R').$$

Note that $(x1 - A)$ annihilates each y_i, by the choice of A. We can consider the adjoint $B = (x1 - A)^{adj}$. Then

$$B(x1 - A) = \det(x1 - A)1.$$

This product of matrices obviously annihilates each vector y_i. It follows that

$$(\det(x1 - A)y_i = 0, \quad \forall i,$$

which implies that $\det(x1 - A)$ kills M. This implies that $\det(x1 - A) = 0$ since $R \subset M$.

As a result, x satisfies the chaacteristic polynomial. □

We proved this to show that the set of integral elements is well behaved.

Theorem 1.7. *Let $R \subset R'$. Let $S = \{x \in R' : x \text{ is integral over } R\}$. Then S is a subring of R'. In particular, it is closed under addition and multiplication.*

Proof. Suppose $x, y \in S$. We can consider the finitely generated modules $R[x], R[y] \subset R'$ generated (as algebras) by x over R. By assumption, these are finitely generated R-modules. In particular, the tensor product

$$R[x] \otimes_R R[y]$$

is a finitely generated R-module. Indeed:

Lemma 1.8. *If M, N are finitely generated, then $M \otimes_R N$ is finitely generated.*

Proof. Indeed, if we have surjections $R^m \to M, R^n \to N$, we can tensor them; we get a surjection since the tensor product is right-exact. So have a surjection $R^{mn} = R^m \otimes_R R^n \to M \otimes_R N$. □

Back to the main proof. As stated, $R[x] \otimes_R R[y]$ is finitely generated as an R-module. We have a ring-homomorphism $R[x] \otimes_R R[y] \to R'$ which comes from the inclusions $R[x], R[y] \rightarrowtail R'$.

Let M be the image of $R[x] \otimes_R R[y]$ in R'. Then M is an R-submodule of R', indeed an R-subalgebra containing x, y. Also, M is finitely generated. Since $x + y, xy \in M$ and M is a subalgebra, it follows that

$$(x + y)M \subset M, \quad xyM \subset M.$$

Thus $x + y, xy$ are integral over R. □

2 Integral closure

Definition 2.1. If $R \subset R'$, then the set $S = \{x \in R' : x \text{ is integral}\}$ is called the **integral closure** of R in R'. We say that R is **integrally closed in** R' if $S = R'$.

When R is a domain, and K is the quotient field $R_{(0)}$, we shall simply say that R is **integrally closed** if it is integrally closed in K. Alternatively, some people say that R is **normal** in this case.

Example 2.2. The integers $\mathbb{Z} \subset \mathbb{C}$ have as integral closure the set of complex numbers x satisfying a monic polynomial with integral coefficients. This set is called the set of **algebraic integers**.

Example 2.3. i is an algebraic integer because it satisfies the equation $X^2 + 1 = 0$. $\frac{1-\sqrt{-3}}{2}$ is an algebraic integer, as we talked about last time; it is a sixth root of unity. On the other hand, $\frac{1+\sqrt{-5}}{2}$ is not an algebraic integer.

Example 2.4. Take $\mathbb{Z} \subset \mathbb{Q}$. The claim is that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, or simply—integrally closed.

Proof. We will build on this proof on Friday. Here is the point. Suppose $\frac{a}{b} \in \mathbb{Q}$ satisfying an equation

$$p(a/b) = 0, \quad p(t) = t^n + c_1 t^{n-1} + \cdots + c_0, \ \forall c_i \in \mathbb{Z}.$$

Assume that a, b have no common factors; we must prove that b has no prime factors, so is ± 1. If b had a prime factor, say q, then we must obtain a contradiction.

We interrupt with a fancy definition.

Definition 2.5. The **valuation at** q (or **q-adic valuation**) is the map $v_q : \mathbb{Q}^* \to \mathbb{Z}$ is the function sending $q^k(a/b)$ to k if $q \nmid a, b$. We extend this to all rational numbers via $v(0) = \infty$.

In general, this just counts the number of factors of q in the expression.

Note the general property that

$$v_q(x+y) \geq \min(v_q(x), v_q(y)).$$

If x, y are both divisible by some power of q, so is $x+y$; this is the statement above. We also have the useful property

$$v_q(xy) = v_q(x) + v_q(y).$$

Now return to the proof that $\mathbb{Z}$ is normal. We would like to show that

$$v_q(a/b) \geq 0.$$

This will prove that b is not divisible by q.

We are assuming that $p(a/b) = 0$. In particular,

$$\left(\frac{a}{b}\right)^n = -c_1 \left(\frac{a}{b}\right)^{n-1} - \cdots - c_0.$$

Apply v_q to both sides:

$$nv_q(a/b) \geq \min_i v_q(c_i(a/b)^{n-i}).$$

Since the $c_i \in \mathbb{Z}$, their valuations are nonnegative. In particular, the right hand side is at least

$$\min_i (n-i) v_q(a/b).$$

This cannot happen if $v_q(a/b) < 0$, because $n - i < n$ for each i. □

This argument applies more generally. If $R \subset K$ is a subring "defined by valuations," then R is integrally closed in K. We will talk more about this, and about valuation rings, next time. $\mathbb{Z}$ is defined by valuations in the sense that it consists of the elements of $\mathbb{Q}$ which have all nonnegative valuations.

We will finish this lecture by discussing what it means to be integrally closed geometrically.

Example 2.6. Here is a ring which is not integrally closed. Take $\mathbb{C}[x, y]/(x^2 - y^3)$.

In the complex plane, $\mathbb{C}^2$, this corresponds to the subvariety $C \subset \mathbb{C}^2$ defined by $x^2 = y^3$. In $\mathbb{R}^2$, this can be drawn: it has a singularity at $(x, y) = 0$.

Note that $x^2 = y^3$ if and only if there is a complex number z such that $x = z^3, y = z^2$. This complex number z can be recovered via x/y when $x, y \neq 0$. In particular, there is a map $\mathbb{C} \to C$ which sends $z \to (z^3, z^2)$. At every point other than the origin, the inverse can be recovered using rational functions. But this does not work at the origin.

We can think of $\mathbb{C}[x, y]/(x^2 - y^3)$ as the subring R' of $\mathbb{C}[z]$ generated by $\{z^n, n \neq 1\}$. There is a map from $\mathbb{C}[x, y]/(x^2 - y^3)$ sending $x \to z^3, y \to z^2$. Since these two domains are isomorphic, and R' is not integrally closed, it follows that $\mathbb{C}[x, y]/(x^2 - y^3)$ is not integrally closed. The element z can be thought of as an element of the fraction field of R' or of $\mathbb{C}[x, y]/(x^2 - y^3)$. It is integral, though.

The failure of integrally closedness has to do with the singularity at the origin.

We now give a generalization of the above example.

Example 2.7. This example is outside the scope of the present course. Say that $X \subset \mathbb{C}^n$ is given as the zero locus of some holomorphic functions $\{f_i : \mathbb{C}^n \to \mathbb{C}\}$. We just gave an example when $n = 2$. Assume that $0 \in X$, i.e. each f_i vanishes at the origin.

Let R be the ring of germs of holomorphic functions 0, in other words holomorphic functions from small open neighborhoods of zero. Each of these f_i becomes an element of R. The ring

$$R/(\{f_i\})$$

is called the ring of germs of holomorphic functions on X at zero.

Assume that R is a domain. This assumption, geometrically, means that near the point zero in X, X can't be broken into two smaller closed analytic pieces. The fraction field of R is to be thought of as the ring of germs of meromorphic functions on X at zero.

We state the following without proof:

Theorem 2.8. *Let g/g' be an element of the fraction field, i.e. $g, g' \in R$. Then g/g' is integral over R if and only if g/g' is bounded near zero.*

In the previous example of X defined by $x^2 = y^3$, the function x/y (defined near the origin on the curve) is bounded near the origin, so it is integral over the ring of germs of regular functions. The reason it is not defined near the origin is *not* that it blows up. In fact, it extends continuously, but not holomorphically, to the rest of the variety X.

3 Valuation rings

Today, we will talk about the notion of a "valuation ring."

Definition 3.1. A **valuation ring** is a domain R such that for every pair of elements $a, b \in R$, either $a \mid b$ or $b \mid a$.

Example 3.2. $\mathbb{Z}$ is not a valuation ring. Neither 2 divides 3 nor 3 divides 2.

Example 3.3. $\mathbb{Z}_{(p)}$, which is the set of all fractions of the form $a/b \in \mathbb{Q}$ where $p \nmid b$, is a valuation ring. To check whether a/b divides a'/b' or vice versa, you just have to check which is divisible by the larger power of p.

Remark. Let R be a valuation ring. Let K be the fraction field of R. Then for all $x \in K^*$, either x or x^{-1} belongs to R. Indeed, if $x = a/b,\ a, b \in R$, then either $a \mid b$ or $b \mid a$, so either x or $x^{-1} \in R$. This condition is equivalent to R's being a valuation ring.

Why are these called valuation rings? Well,

Definition 3.4. Let K be a field. A **valuation** on K is a map $v : K^* \to A$ for A is a totally ordered abelian group satisfying:

1. $v(xy) = v(x) + v(y)$. I.e., v is a homomorphism.

2. $v(x+y) \geq \min v(x), v(y)$. (We define $v(0) = \infty$ by convention; this is a formal constant bigger than everything in A.)

Suppose that K is a field and $v : K \to A \cup \{\infty\}$ is a valuation (i.e. $v(0) = \infty$). Define $R = \{x \in K : v(x) \geq 0\}$.

Proposition 3.5. *R as just defined is a valuation ring.*

Proof. First, we prove that R is a ring. R is closed under addition and multiplication by the two conditions

$$v(xy) = v(x) + v(y)$$

and

$$v(x + y) \geq \min v(x), v(y),$$

so if $x, y \in R$, then $x + y, xy$ have nonnegative valuations.

Note that $0 \in R$ because $v(0) = \infty$. Also $v(1) = 0$ since $v : K^* \to A$ is a homomorphism. So $1 \in R$ too. Finally, $-1 \in R$ because $v(-1) = 0$ since A is totally ordered. It follows that R is also a group.

Let us now show that R is a valuation ring. If $x \in K^*$, either $v(x) \geq 0$ or $v(x^{-1}) \geq 0$ since A is totally ordered.[1] So either $x, x^{-1} \in R$. □

In particular, the set of elements with nonnegative valuation is a valuation ring. The converse also holds. Whenever you have a valuation ring, it comes about in this manner.

Proposition 3.6. *Let R be a valuation ring with quotient field K. There is an ordered abelian group A and a valuation $v : K^* \to A$ such that R is the set of elements with nonnegative valuation.*

Proof. First, we construct A. In fact, it is the quotient of K^* by the subgroup of units R^* of R. We define an ordering by saying that $x \leq y$ if $y/x \in R$—this doesn't depend on the representatives in K^* chosen. Note that either $x \leq y$ or $y \leq x$ must hold, since R is a valuation ring. The combination of $x \leq y$ and $y \leq x$ implies that x, y are equivalent classes. The nonnegative elements in this group are those whose representatives in K^* belong to R.

It is easy to see that K^*/R^* in this way is a totally ordered abelian group with the image of 1 as the unit. The reduction map $K^* \to K^*/R^*$ defines a valuation whose corresponding ring is just R. We have omitted some details; for instance, it should be checked that the valuation of $x + y$ is at least the minimum of $v(x), v(y)$. □

To summarize:

[1] Otherwise $0 = v(x) + v(x^{-1}) < 0$, contradiction.

Every valuation ring R determines a valuation v from the fraction field of R into $A \cup \{\infty\}$ for A a totally ordered abelian group such that R is just the set of elements of K with nonnegative valuation. As long as we require that $v : K^* \to A$ is surjective, then A is uniquely determined as well.

Definition 3.7. A valuation ring R is **discrete** if we can choose A to be $\mathbb{Z}$.

Example 3.8. $\mathbb{Z}_{(p)}$ is a discrete valuation ring.

The notion of a valuation ring is a useful one.

3.1 General remarks

Let R be a commutative ring. Then Spec$R$ is the set of primes of R, equipped with a certain topology. The space Spec$R$ is almost never Hausdorff. It is almost always a bad idea to apply the familiar ideas from elementary topology (e.g. the fundamental group) to Spec$R$. Nonetheless, it has some other nice features that substitute for its non-Hausdorffness.

For instance, if $R = \mathbb{C}[x, y]$, then Spec$R$ corresponds to $\mathbb{C}^2$ with some additional nonclosed points. The injection of $\mathbb{C}^2$ with its usual topology into Spec$R$ is continuous. While in Spec$R$ you don't want to think of continuous paths, you can in $\mathbb{C}^2$.

Suppose you had two points $x, y \in \mathbb{C}^2$ and their images in Spec$R$. Algebraically, you can still think about algebraic curves passing through x, y. This is a subset of x, y defined by a single polynomial equation. This curve will have what's called a "generic point," since the ideal generated by this curve will be a prime ideal. The closure of this generic point will be precisely this algebraic curve—including x, y.

Remark. If $\mathfrak{p}, \mathfrak{p}' \in \text{Spec}R$, then

$$\mathfrak{p}' \in \overline{\{\mathfrak{p}\}}$$

iff

$$\mathfrak{p}' \supset \mathfrak{p}.$$

Why is this? Well, the closure of $\{\mathfrak{p}\}$ is just $V(\mathfrak{p})$, since this is the smallest closed subset of Spec$R$ containing $\mathfrak{p}$.

The point of this discussion is that instead of paths, one can transmit information from point to point in Spec$R$ by having one point be in a closure of another. However, we will show that this relation is contained by the theory of valuation rings.

Theorem 3.9. *Let R be a domain containing a prime ideal $\mathfrak{p}$. Let K be the fraction field of R.*

Then there is a valuation v on K defining a valuation ring $R' \subset K$ such that

1. *$R \subset R'$.*

2. $\mathfrak{p} = \{x \in R : v(x) > 0\}$.

Let us motivate this by the remark:

Remark. A valuation ring is automatically a local ring. A local ring is a ring where either $x, 1-x$ is invertible for all x in the ring. Let us show that this is true for a valuation ring.

If x belongs to a valuation ring R with valuation v, it is invertible if $v(x) = 0$. So if $x, 1-x$ were both noninvertible, then both would have positive valuation. However, that would imply that $v(1) \geq \min v(x), v(1-x)$ is positive, contradiction.

> If R' is any valuation ring (say defined by a valuation v), then R' is local with maximal ideal consisting of elements with positive valuation.

The theorem above says that there's a good supply of valuation rings. In particular, if R is any domain, $\mathfrak{p} \subset R$ a prime ideal, then we can choose a valuation ring $R' \supset R$ such that $\mathfrak{p}$ is the intersection of the maximal ideal of R' intersected with R. So the map $\mathrm{Spec}R' \to \mathrm{Spec}R$ contains $\mathfrak{p}$.

Proof. Without loss of generality, replace R by $R_{\mathfrak{p}}$, which is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. The maximal ideal intersects R only in $\mathfrak{p}$.

So, we can assume without loss of generality that

1. R is local.
2. $\mathfrak{p}$ is maximal.

Let P be the collection of all subrings $R' \subset K$ such that $R' \supset R$ but $\mathfrak{p}R' \neq R'$. Then P is a poset under inclusion. The poset is nonempty, since $R \in P$. Every totally ordered chain in P has an upper bound. If you have a totally ordered subring of elements in P, then you can take the union. We invoke:

Lemma 3.10. *Let R_α be a chain in P and $R' = \bigcup R_\alpha$. Then $R' \in P$.*

Proof. Indeed, it is easy to see that this is a subalgebra of K containing R. The thing to observe is that

$$\mathfrak{p}R' = \bigcup_\alpha \mathfrak{p}R_\alpha;$$

since by assumption, $1 \notin \mathfrak{p}R_\alpha$ (because each $R_\alpha \in P$), $1 \notin \mathfrak{p}R'$. In particular, $R' \notin P$. □

By the lemma, Zorn's lemma to the poset P. In particular, P has a maximal element R'. By construction, R' is some subalgebra of K and $\mathfrak{p}R' \neq R'$. Also, R' is maximal with respect to these properties.

We show first that R' is local, with maximal ideal $\mathfrak{m}$ satisfying

$$\mathfrak{m} \cap R = \mathfrak{p}.$$

The second part is evident from locality of R', since $\mathfrak{m}$ must contain the proper ideal $\mathfrak{p}R'$, and $\mathfrak{p} \subset R$ is a maximal ideal.

Suppose that $x \in R'$; we show that either $x, 1-x$ belongs to R'^* (i.e. is invertible). Take the ring $R'[x^{-1}]$. If x is noninvertible, this properly contains R'. By maximality, it follows that $\mathfrak{p}R'[x^{-1}] = R'[x^{-1}]$.

And we're out of time. We'll pick this up on Monday.

□

3.2 Valuation rings, continued

Let us set a goal for today.

First, recall the notion introduced last time. A **valuation ring** is a domain R where for all x in the fraction field of R, either x or x^{-1} lies in R. We saw that if R is a valuation ring, then R is local. That is, there is a unique maximal ideal $\mathfrak{m} \subset R$, automatically prime. Moreover, the zero ideal (0) is prime, as R is a domain. So if you look at the spectrum Spec$R$ of a valuation ring R, there is a unique closed point $\mathfrak{m}$, and a unique generic point (0). There might be some other prime ideals in Spec$R$; this depends on where the additional valuation lives.

Example 3.11. Suppose the valuation defining the valuation ring R takes values in $\mathbb{R}$. Then the only primes are $\mathfrak{m}$ and zero.

Let R now be any ring, with Spec$R$ containing prime ideals $\mathfrak{p} \subset \mathfrak{q}$. In particular, $\mathfrak{q}$ lies in the closure of $\mathfrak{p}$. As we will see, this implies that there is a map

$$\phi : R \to R'$$

such that $\mathfrak{p} = \phi^{-1}(0)$ and $\mathfrak{q} = \phi^{-1}(\mathfrak{m})$, where $\mathfrak{m}$ is the maximal ideal of R'. This statement says that the relation of closure in Spec$R$ is always controlled by valuation rings. In yet another phrasing, in the map

$$\text{Spec}R' \to \text{Spec}R$$

the closed point goes to $\mathfrak{q}$ and the generic point to $\mathfrak{p}$. This is our eventual goal.

To carry out this goal, we need some more elementary facts. Let us discuss things that don't have any obvious relation to it.

3.3 Some useful tools

OK. Let us recall:

Definition 3.12. A map of rings $\phi : R \to R'$ is **integral** if ϕ is injective and each element $x \in R'$ is integral over R (i.e. the image $\phi(R)$), or satisfies a monic polynomial whose coefficients lie in the image of the homomorphism ϕ.

We now interpret integrality in terms of the geometry of Spec.

Proposition 3.13 (Lying over)**.** *If $\phi : R \to R'$ is an integral extension, then the induced map*

$$\mathrm{Spec}R' \to \mathrm{Spec}R$$

is surjective.

Another way to state this, without mentioning $\mathrm{Spec}R'$, is that if $\mathfrak{p} \subset R$ is prime, then there exists $\mathfrak{q} \subset R'$ such that $\mathfrak{p}$ is the inverse image $\phi^{-1}(\mathfrak{q})$.

Proof. First, let us reduce to the case of a local ring. We replace R with $R_{\mathfrak{p}}$. We get a map

$$\phi_{\mathfrak{p}} : R_{\mathfrak{p}} \to (R - \mathfrak{p})^{-1}R'$$

which is injective if ϕ is, since localization is an exact functor. Here we have localized both R, R' at the multiplicative subset $(R - \mathfrak{p})$.

Note that $\phi_{\mathfrak{p}}$ is an integral extension too, i.e. every x/s with $x \in R', s \in R - \mathfrak{p}$ satisfies a monic polynomial with coefficients in $R_{\mathfrak{p}}$. To see this, note that x is integral over R, so there is a monic polynomial

$$x^n + a_1 x^{n-1} + \cdots + a_0 = 0, \quad \forall a_i \in R \ (= \phi(R)).$$

We can divide this by s^n:

$$(\frac{x}{s})^n + \frac{a_1}{s}(\frac{x}{s})^{n-1} + \cdots + \frac{a_0}{s^n} = 0,$$

where each fraction in the coefficient is in the image of $\phi_{\mathfrak{p}}$. That proves that $\phi_{\mathfrak{p}}$ is also integral.

We will prove the result for $\phi_{\mathfrak{p}}$. In particular, we will show that there is a prime ideal of $(R - \mathfrak{p})^{-1}R'$ that pulls back to $\mathfrak{p}R_{\mathfrak{p}}$. These will imply that if we pull this prime ideal back to R', it will pull back to $\mathfrak{p}$ in R. So it is sufficient for the proposition to handle the case of R local.

Upshot: we can assume R is local with maximal ideal $\mathfrak{p}$. We assume this now. So, we want to find a prime ideal $\mathfrak{q} \subset R'$ such that $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$. Since $\mathfrak{p}$ is already maximal, it will suffice to show that $\mathfrak{p} \subset \phi^{-1}(\mathfrak{q})$. In particular, we need to show that there is a prime ideal $\mathfrak{q}$ such that

$$\mathfrak{p}R' \subset \mathfrak{q}.$$

The pull-back of this will be $\mathfrak{p}$.

If $\mathfrak{p}R' \neq R'$, then $\mathfrak{q}$ exists, since every proper ideal of a ring is contained in a maximal ideal. In particular, we need to show that

$$\mathfrak{p}R' \neq R',$$

or that $\mathfrak{p}$ doesn't generate the unit ideal in R'. Suppose the contrary. Then $1 \in \mathfrak{p}R'$ and we can write

$$1 = \sum x_i \phi(y_i)$$

where $x_i \in R', y_i \in \mathfrak{p}$.

Let R'' be the subalgebra of R' generated by $\phi(R)$ and the x_i. Then $R'' \subset R'$ and is finitely generated over R, because it is generated by the x_i. However, R'' is actually finitely generated as an R-module too, because each x_i satisfies a monic polynomial with coefficients in R. This is where integrality comes in.

So we have that R'' is a finitely generated R-module. Also, the expression $1 = \sum x_i \phi(y_i)$ shows that $\mathfrak{p}R'' = R''$. However, this contradicts Nakayama's lemma. That brings the contradiction, showing that $\mathfrak{p}$ cannot generate (1) in R', proving the lying over theorem.

□

3.4 Back to the goal

Now we return to the goal of the lecture. Again, R was any ring, and we had primes $\mathfrak{p} \subset \mathfrak{q} \subset R$. We wanted a valuation ring R' and a map $\phi : R \to R'$ such that zero pulled back to $\mathfrak{p}$ and the maximal ideal pulled back to $\mathfrak{q}$.

What does it mean for $\mathfrak{p}$ to be the inverse image of $(0) \subset R'$? This means that $\mathfrak{p} = \ker \phi$. So we get an injection

$$R/\mathfrak{p} \rightarrowtail R'.$$

We will let R' be a subring of the quotient field K of the domain $R/\mathfrak{p}$. Of course, this subring will contain $R/\mathfrak{p}$.

In this case, we will get a map $R \to R'$ such that the pull-back of zero is $\mathfrak{p}$. What we want, further, to be true is that R' is a valuation ring and the pull-back of the maximal ideal is $\mathfrak{q}$.

This is starting to look at the problem we discussed last time. Namely, let's throw out R, and replace it with $R/\mathfrak{p}$. Moreover, we can replace R with $R_{\mathfrak{q}}$ and assume that R is local with maximal ideal $\mathfrak{q}$. What we need to show is that a valuation ring R' contained in the fraction field of R, containing R, such that the intersection of the maximal ideal of R' with R is equal to $\mathfrak{q} \subset R$. If we do this, then we will have accomplished our goal.

Lemma 3.14. *Let R be a local domain. Then there is a valuation subring R' of the quotient field of R that* dominates *R, i.e .the map $R \to R'$ is a* local *homomorphism.*

Let's find R' now.

Choose R' maximal such that $\mathfrak{q}R' \neq R'$. Such a ring exists, by Zorn's lemma. We gave this argument at the end last time.

Lemma 3.15. *R' as described is local.*

Proof. Look at $\mathfrak{q}R' \subset R'$; it is a proper subset, too, by assumption. In particular, $\mathfrak{q}R'$ is contained in some maximal ideal $\mathfrak{m} \subset R'$. Replace R' by $R'' = R'_{\mathfrak{m}}$. Note that

$$R' \subset R''$$

and

$$\mathfrak{q}R'' \neq R''$$

because $\mathfrak{m}R'' \neq R''$. But R' is maximal, so $R' = R''$, and R'' is a local ring. So R' is a local ring. □

Let $\mathfrak{m}$ be the maximal ideal of R'. Then $\mathfrak{m} \supset \mathfrak{q}R$, so $\mathfrak{m} \cap R = \mathfrak{q}$. All that is left to prove now is that R' is a valuation ring.

Lemma 3.16. *R' is integrally closed.*

Proof. Let R'' be its integral closure. Then $\mathfrak{m}R'' \neq R''$ by lying over, since $\mathfrak{m}$ (the maximal ideal of R') lifts up to R''. So R'' satisfies

$$\mathfrak{q}R'' \neq R''$$

and by maximality, we have $R'' = R'$. □

To summarize, we know that R' is a local, integrally closed subring of the quotient field of R, such that the maximal ideal of R' pulls back to $\mathfrak{q}$ in R. All we now need is:

Lemma 3.17. *R' is a valuation ring.*

Proof. Let x lie in the fraction field. We must show that either x or $x^{-1} \in R'$. Say $x \notin R'$. This means by maximality of R' that $R'' = R'[x]$ satisfies

$$\mathfrak{q}R'' = R''.$$

In particular, we can write

$$1 = \sum q_i x^i, \quad q_i \in \mathfrak{q}R' \subset R'.$$

This implies that

$$(1 - q_0) + \sum_{i>0} -q_i x^i = 0.$$

But $1 - q_0$ is invertible in R', since R' is local. We can divide by the highest power of x:

$$x^{-N} + \sum_{i>0} \frac{-q_i}{1 - q_0} x^{-N+i} = 0.$$

In particular, $1/x$ is integral over R'; this implies that $1/x \in R'$ since R' is integrally closed and q_0 is a nonunit. So R' is a valuation ring. □

We can state the result formally.

Theorem 3.18. *Let R be a ring, $\mathfrak{p} \subset \mathfrak{q}$ prime ideals. Then there is a homomorphism $\phi : R \to R'$ into a valuation ring R' with maximal ideal $\mathfrak{m}$ such that*

$$\phi^{-1}(0) = \mathfrak{p}$$

and

$$\phi^{-1}(\mathfrak{m}) = \mathfrak{q}.$$

There is a related fact which we now state.

Theorem 3.19. *Let R be any domain. Then the integral closure of R in the quotient field K is the intersection*

$$\bigcap R_\alpha$$

of all valuation rings $R_\alpha \subset K$ containing R.

So an element of the quotient field is integral over R if and only if its valuation is nonnegative at every valuation which is nonnegative on R.

Proof. The $\subset$ argument is easy, because one can check that a valuation ring is integrally closed. (Exercise.) The interesting direction is to assume that $v(x) \geq 0$ for all v nonnegative on R.

Let us suppose x is nonintegral. Suppose $R' = R[1/x]$ and I be the ideal $(x^{-1}) \subset R'$. There are two cases:

1. $I = R'$. Then in the ring R', x^{-1} is invertible. In particular, $x^{-1}P(x^{-1}) = 1$. Multiplying by a high power of x shows that x is integral over R. Contradiction.

2. Suppose $I \subsetneq R'$. Then I is contained in a maximal ideal $\mathfrak{q} \subset R'$. There is a valuation subring $R'' \subset K$, containing R', such that the corresponding valuation is positive on $\mathfrak{q}$. In particular, this valuation is positive on x^{-1}, so it is negative on x, contradiction.

□

So the integral closure has this nice characterization via valuation rings. In some sense, the proof that $\mathbb{Z}$ is integrally closed has the property that every integrally closed ring is integrally closed for that reason: it's the common nonnegative locus for some valuations.

Chapter 5

Noetherian rings and modules

The finiteness condition of a noetherian ring makes commutative algebra much nicer.

1 Basics

1.1 The noetherian condition

Definition 1.1. Let R be a commutative ring and M an R-module. We say that M is **noetherian** if every submodule of M is finitely generated.

Definition 1.2. R is **noetherian** if R is noetherian as an R-module. In particular, this says that all of its ideals are finitely generated.

Example 1.3. 1. Any field is noetherian. There are two ideals: (1) and (0).

2. Any PID is noetherian: any ideal is generated by one element. So $\mathbb{Z}$ is noetherian.

First, let's just think about the condition of modules. Here is a convenient reformulation of it.

Proposition 1.4. *M is a module over R. The following are equivalent:*

1. *M is noetherian.*

2. *Every chain of submodules of M, $M_0 \subset M_1 \subset \dots$, eventually stabilizes at some M_N. (Ascending chain condition.)*

Proof. Say M is noetherian and we have such a chain

$$M_0 \subset M_1 \subset \dots.$$

Write

$$M' = \bigcup M_i \subset M,$$

which is finitely generated since M is noetherian. Let it be generated by $x_1, \dots, x_n$. Each of these finitely many elements is in the union, so they are all contained in some M_N. This means that

$$M' \subset M_N, \quad \text{so} \quad M_N = M'$$

and the chain stabilizes.

For the converse, assume the ACC. Let $M' \subset M$ be any submodule. Define a chain of submodules $M_0 \subset M_1 \subset \cdots \subset M'$ as follows. First, just take $M_0 = \{0\}$. Take M_{n+1} to be M_n plus the submodule generated by some $x \in M' - M_n$, if this is possible. So M_0 is zero, M_1 is generated by some nonzero element of M', M_2 is M_1 together with some element of M' not in M_1. By construction, we have an ascending chain, so it stabilizes at some finite place. This means at some point, it is impossible to choose something in M' that does not belong to some M_N. In particular, M' is generated by N elements, since M_N is. □

1.2 Stability properties

Proposition 1.5. *If*

$$M' \rightarrowtail M \twoheadrightarrow M''$$

is an exact sequence of modules, then M is noetherian if and only if M', M'' are.

One direction says that noetherianness is preserved under subobjects and quotients.

Proof. If M is noetherian, then every submodule of M' is a submodule of M, so is finitely generated. So M' is noetherian too. Now we show that M'' is noetherian. Let $N \subset M''$ and let $\widetilde{N} \subset M$ the inverse image. Then $\widetilde{N}$ is finitely generated, so N—as the homomorphic image of $\widetilde{N}$—is finitely generated So M'' is noetherian.

Suppose M', M'' noetherian. We prove M noetherian. Let's verify the ascending chain condition. Consider

$$M_1 \subset M_2 \subset \cdots \subset M.$$

Let M_i'' denote the image of M_i in M'' and let M_i' be the intersection of M_i with M'. Here we think of M' as a submodule of M. These are ascending chains of submodules of M', M'', respectively, so they stabilize by noetherianness. So for some N, we have that $n \geq N$ implies

$$M_n' = M_{n+1}', \quad M_n'' = M_{n+1}''.$$

We claim that this implies, for such n,

$$M_n = M_{n+1}.$$

Why? Say $x \in M_{n+1} \subset M$. Then x maps into something in $M_{n+1}'' = M_n''$. So there is something in M_n, call it y, such that x, y go to the same thing in M''. In particular,

$$x - y \in M_{n+1}$$

goes to zero in M'', so $x - y \in M'$. Thus $x - y \in M'_{n+1} = M'_n$. In particular,

$$x = (x - y) + y \in M'_n + M_n = M_n.$$

So $x \in M_n$, and

$$M_n = M_{n+1}.$$

This proves the result. □

The class of noetherian modules is thus "robust." We can get from that the following.

Proposition 1.6. *If $\phi : A \to B$ is a surjection of commutative rings and A is noetherian, then B is noetherian too.*

Proof. Indeed, B is noetherian as an A-module; indeed, it is the quotient of a noetherian A-module (namely, A). However, it is easy to see that the A-submodules of B are just the B-modules in B, so B is noetherian as a B-module too. So B is noetherian. □

Another easy stability property:

Proposition 1.7. *Let R be a commutative ring, $S \subset R$ a multiplicatively closed subset. If R is noetherian, then $S^{-1}R$ is noetherian.*

I.e., the class of noetherian rings is closed under localization.

Proof. Say $\phi : R \to S^{-1}R$ is the canonical map. Let $I \subset S^{-1}R$ be an ideal. Then $\phi^{-1}(I) \subset R$ is an ideal, so finitely generated. It follows that

$$\phi^{-1}(I)(S^{-1}R) \subset S^{-1}R$$

is finitely generated as an ideal in $S^{-1}R$; the generators are the images of the generators of $\phi^{-1}(I)$.

Now we claim that

$$\phi^{-1}(I)(S^{-1}R) = I.$$

The inclusion $\subset$ is trivial. For the latter inclusion, if $x/s \in I$, then $x \in \phi^{-1}(I)$, so

$$x = (1/s)x \in (S^{-1}R)\phi^{-1}(I).$$

This proves the claim and implies that I is finitely generated. □

1.3 The basis theorem

Let us now prove something a little less formal.

Theorem 1.8 (Hilbert basis theorem)**.** *If R is a noetherian ring, then the polynomial ring $R[X]$ is noetherian.*

Proof. Let $I \subset R[X]$ be an ideal. We prove that it is finitely generated. For each $m \in \mathbb{Z}_{\geq 0}$, let $I(n)$ be the collection of elements $a \in R$ consisting of the coefficients of x^n of elements of I of degree $\leq n$. This is an ideal, as is easily seen.

In fact, we claim that

$$I(1) \subset I(2) \subset \dots$$

which follows because if $a \in I(1)$, there is an element $aX + \dots$ in I. Thus $X(aX + \dots) = aX^2 + \dots \in I$, so $a \in I(2)$. And so on.

Since R is noetherian, this chain stabilizes at some $I(N)$. Also, because R is noetherian, each $I(n)$ is generated by finitely many elements $a_{n,1}, \dots, a_{n,m_n} \in I(n)$. All of these come from polynomials $P_{n,i} \in I$ such that $P_{n,i} = a_{n,i}X^n + \dots$.

The claim is that the $P_{n,i}$ for $n \leq N$ and $i \leq m_n$ generate I. This is a finite set of polynomials, so if we prove the claim, we will have proved the basis theorem. Let J be the ideal generated by $\{P_{n,i}, n \leq N, i \leq m_n\}$. We know $J \subset I$. We must prove $I \subset J$.

We will show that any element $P(X) \in I$ of degree n belongs to J by induction on n. The degree is the largest nonzero coefficient. In particular, the zero polynomial does not have a degree, but the zero polynomial is obviously in J.

There are two cases. In the first case, $n \geq N$. Then we write

$$P(X) = aX^n + \dots.$$

By definition $a \in I(n) = I(N)$ since the chain of ideals $I(n)$ stabilized. Thus we can write a in terms of the generators: $a = \sum a_{N,i}\lambda_i$ for some $\lambda_i \in R$. Define the polynomial

$$Q = \sum \lambda_i P_{N,i} x^{n-N} \in J.$$

Then Q has degree n and the leading term is just a. In particular,

$$P - Q$$

is in I and has degree less than n. By the inductive hypothesis, this belongs to J, and since $Q \in J$, it follows that $P \in J$.

Now consider the case of $n < N$. Again, we write $P(X) = aX^n + \dots$. Then $a \in I(n)$. We can write

$$a = \sum a_{n,i}\lambda_i, \quad \lambda_i \in R.$$

But the $a_{n,i} \in I(n)$. The polynomial

$$Q = \sum \lambda_i P_{n,i}$$

belongs to J since $n < N$. In the same way, $P - Q \in I$ has a lower degree. Induction as before implies that $P \in J$. □

Example 1.9. Let k be a field. Then $k[x_1, \ldots, x_n]$ is noetherian for any n, by the Hilbert basis theorem and induction on n.

Example 1.10. Any finitely generated commutative ring R is noetherian. Indeed, then there is a surjection

$$\mathbb{Z}[x_1, \ldots, x_n] \twoheadrightarrow R$$

where the x_i get mapped onto generators in R. The former is noetherian by the basis theorem, and R is as a quotient noetherian.

Corollary 1.11. *Any ring R can be obtained as a filtered direct limit of noetherian rings.*

Proof. Indeed, R is the filtered direct limit of its finitely generated subrings. □

This observation is sometimes useful in commutative algebra and algebraic geometry, in order to reduce questions about arbitrary commutative rings to noetherian rings. Noetherian rings have strong finiteness hypotheses that let you get numerical invariants that may be useful. For instance, we can do things like inducting on the dimension for noetherian local rings.

Example 1.12. Take $R = \mathbb{C}[x_1, \ldots, x_n]$. For any algebraic variety V defined by polynomial equations, we know that V is the vanishing locus of some ideal $I \subset R$. Using the Hilbert basis theorem, we have shown that I is finitely generated. This implies that V can be described by *finitely* many polynomial equations.

1.4 More on noetherian rings

Let R be a noetherian ring.

Proposition 1.13. *An R-module M is noetherian if and only if M is finitely generated.*

Proof. The only if direction is obvious. A module is noetherian if and only if every submodule is finitely generated.

For the if direction, if M is finitely generated, then there is a surjection of R-modules

$$R^n \to M$$

where R is noetherian. So R^n is noetherian because it is a successive extension of copies of R and an extension of two noetherian modules is also noetherian. So M is a quotient of a noetherian module and is noetherian.

□

2 Associated primes

Today, we will continue with the structure theory for noetherian modules.

2.1 The support

The first piece of intuition to have is the following. Let R be noetherian; consider Spec$R$. An R-module M is supposed to be thought of as somehow spread out over Spec$R$. If $\mathfrak{p} \in \text{Spec}R$, then

$$\kappa(\mathfrak{p}) = \text{fr. field } R/\mathfrak{p}$$

which is the residue field of $R_{\mathfrak{p}}$. If M is any R-module, we can consider $M \otimes_R \kappa(\mathfrak{p})$ for each $\mathfrak{p}$; it is a vector space over $\kappa(\mathfrak{p})$. If M is finitely generated, then $M \otimes_R \kappa(\mathfrak{p})$ is a finite-dimensional vector space.

Definition 2.1. Let M be a finitely generated R-module. Then supp$M$ is defined to be the set of primes $\mathfrak{p} \in \text{Spec}R$ such that

$$M \otimes_R \kappa(\mathfrak{p}) \neq 0.$$

You're supposed to think of a module M as something like a vector bundle over Spec$R$. At each $\mathfrak{p} \in \text{Spec}R$, we associate the vector space $M \otimes_R \kappa(\mathfrak{p})$. It's not really a vector bundle, since the fibers don't have to have the same dimension. For instance, the support of the $\mathbb{Z}$-module $\mathbb{Z}/p$ just consists of the prime (p). The fibers don't have the same dimension.

Nonetheless, we can talk about the support, i.e. the set of spaces where the vector space is not zero.

Remark. $\mathfrak{p} \in \text{supp}M$ if and only if $M_{\mathfrak{p}} \neq 0$. This is because

$$(M \otimes_R R_{\mathfrak{p}})/\mathfrak{p}R_{\mathfrak{p}}(M \otimes_R R_{\mathfrak{p}}) = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} \kappa(\mathfrak{p})$$

and we can use Nakayama's lemma over the local ring $R_{\mathfrak{p}}$. (We are using the fact that M is finitely generated.)

Remark. $M = 0$ if and only if supp$M = \emptyset$. This is because $M = 0$ if and only if $M_{\mathfrak{p}} = 0$ for all localizations. We saw this earlier.

We will see soon that that supp$M$ is closed in Spec$R$. You imagine that M lives on this closed subset supp$M$, in some sense.

2.2 Associated primes

Throughout, R is noetherian.

Definition 2.2. Let M be a finitely generated R-module. The prime ideal $\mathfrak{p}$ is said to be **associated** to M if there exists an element $x \in M$ such that $\mathfrak{p}$ is the annihilator of x. The set of associated primes is $\text{Ass}(M)$.

Note that the annihilator of an element $x \in M$ is not necessarily prime, but it is possible that the annihilator might be prime, in which case it is associated.

The first claim is that there are some.

Proposition 2.3. *If $M \neq 0$, then there is an associated prime.*

Proof. Let I be a maximal element among the annihilators of nonzero elements $x \in M$. Then $1 \notin I$ because the annihilator of a nonzero element is not the full ring. The existence of I is guaranteed thanks to the noetherianness of R.[1]

So I is the annihilator $\mathrm{Ann}(x)$ of some $x \in M - \{0\}$. I claim that I is prime, hence an associated prime. Indeed, suppose $ab \in I$ where $a, b \in R$. This means that

$$(ab)x \neq 0.$$

Consider the annihilator of bx. This contains the annihilator of x, so I; it also contains a. Maximality tells us that either $bx = 0$ (in which case $b \in I$) or $\mathrm{Ann}(bx) = I$ and then $a \in \mathrm{Ann}(bx) = I$. So either $a, b \in I$. And I is prime. □

Proposition 2.4. *Any finitely generated R-module has only finitely many associated primes.*

The idea is going to be to use the fact that M is finitely generated to build M out of finitely many pieces, and use that to bound the number of associated primes to each piece.

Lemma 2.5. *Suppose we have an exact sequence of finitely generated R-modules*

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

Then

$$\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$$

Proof. The first claim is obvious. If $\mathfrak{p}$ is the annihilator of something in M', it is an annihilator of something in M (namely its image), because $M' \to M$ is injective.

The hard direction is the other direction. Suppose $\mathfrak{p} \in \mathrm{Ass}(M)$. Then there is $x \in M$ such that

$$\mathfrak{p} = \mathrm{Ann}(x).$$

Consider the submodule $Rx \subset M$. If $Rx \cap M' \neq 0$, then we can choose $y \in Rx \cap M' - \{0\}$. I claim that $\mathrm{Ann}(y) = \mathfrak{p}$ and so $\mathfrak{p} \in \mathrm{Ass}(M')$.

Now $y = ax$ for some $a \in R$. The annihilator of y is the set of elements $b \in R$ such that

$$abx = 0$$

or $ab \in \mathfrak{p}$. But $y = ax \neq 0$, so $a \notin \mathfrak{p}$. As a result, the condition $b \in \mathrm{Ann}(y)$ is the same as $b \in \mathfrak{p}$. In other words,

$$\mathrm{Ann}(y) = \mathfrak{p}$$

which proves the claim.

What if the intersection $Rx \cap M' = 0$. Let $\phi : M \twoheadrightarrow M''$ be the surjection. I claim that $\mathfrak{p} = \mathrm{Ann}(\phi(x))$ and $\mathfrak{p} \in \mathrm{Ass}(M'')$. The proof is as follows. Clearly $\mathfrak{p}$ annihilates $\phi(x)$ as it annihilates x. Suppose $a \in \mathrm{Ann}(\phi(x))$. This means that $\phi(ax) = 0$, so $ax \in \ker \phi$; but $\ker \phi \cap Rx = 0$. So $ax = 0$ and $a \in \mathfrak{p}$. So $\mathrm{Ann}(\phi(x)) = \mathfrak{p}$. □

[1] It is a well-known argument that in a noetherian ring, any subset of ideals contains a maximal element.

Lemma 2.6. *For any finitely generated R-module M, there exists a finite filtration*

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

such that the quotients are isomorphic to various $R/\mathfrak{p}_i$.

Proof. Let $M' \subset M$ be maximal among submodules for which such a filtration exists. What we'd like to show is that $M' = M$, but a priori we don't know this. Now M' is well-defined since 0 has a filtration and M is noetherian. There is a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_l = M' \subset M.$$

Now what can we say? If $M' = M$, we're done, as we said. Otherwise, look at the quotient $M/M' \neq 0$. There is an associated prime of M/M'. So there is a prime $\mathfrak{p}$ which is the annihilator of $x \in M/M'$. This means that there is an injection

$$R/\mathfrak{p} \to M/M'.$$

Now, we just make M' bigger by taking M_{l+1} as the inverse image in M of $R/\mathfrak{p} \subset M/M'$. We have thus extended this filtration one step further since $M_{l+1}/M_l \simeq R/\mathfrak{p}$, a contradiction since M' was maximal. □

Now we are in a position to meet the goal.

Pf of Proposition 2.4. Suppose M is finitely generated Take our filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_k = M.$$

By induction, we show that $\mathrm{Ass}(M_i)$ is finite for each i. It is obviously true for $i = 0$. In general, we have an exact sequence

$$0 \to M_i \to M_{i+1} \to R/\mathfrak{p}_i \to 0$$

which implies that

$$\mathrm{Ass}(M_{i+1}) \subset \mathrm{Ass}(M_i) \cup \mathrm{Ass}(R/\mathfrak{p}_i) = \mathrm{Ass}(M_i) \cup \{\mathfrak{p}_i\}.$$

This proves the claim and the proposition; it also shows that the number of associated primes is at most the length of the filtration.

□

Let us first describe how associated primes localize.

Proposition 2.7. *Let R noetherian, M finitely generated and $S \subset R$ multiplicatively closed. Then*

$$\mathrm{Ass}(S^{-1}M) = \left\{S^{-1}\mathfrak{p} : \mathfrak{p} \in \mathrm{Ass}(M), \mathfrak{p} \cap S = \emptyset\right\}.$$

Here $S^{-1}M$ is considered as an $S^{-1}R$-module.

We've seen that prime ideals in $S^{-1}R$ can be identified as a subset of $\mathrm{Spec}R$. This shows that this notion is compatible with localization.

Proof. We prove the easy direction. Suppose $\mathfrak{p} \in \mathrm{Ass}(M)$ and $\mathfrak{p} \cap S = \emptyset$. Then $\mathfrak{p} = \mathrm{Ann}(x)$ for some $x \in M$. Then the annihilator of $x/1$ is just $S^{-1}\mathfrak{p}$, as one easily sees. Thus $S^{-1}\mathfrak{p} \in \mathrm{Ass}(S^{-1}M)$.

The harder direction is left as an exercise. □

The next claim is that the support and the associated primes are related.

Proposition 2.8. *The support is the closure of the associated primes:*

$$\mathrm{supp}M = \bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \overline{\{\mathfrak{q}\}}$$

Corollary 2.9. $\mathrm{supp}(M)$ *is closed.*

Proof. Indeed, the above result says that

$$\mathrm{supp}M = \bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \overline{\{\mathfrak{q}\}}.$$

□

Corollary 2.10. *The ring R has finitely many minimal prime ideals.*

Proof. Indeed, every minimal prime ideal is an associated prime for the R-module R itself. Why is this? Well, $\mathrm{supp}R = \mathrm{Spec}R$. Thus every prime ideal of R contains an associated prime. And R has finitely many associated primes. □

Remark. So $\mathrm{Spec}R$ is the finite union of irreducible pieces $\overline{\mathfrak{q}}$ if R is noetherian.

Let us prove the proposition.

Proof. First, the easy direction. We show that $\mathrm{supp}(M)$ contains the set of primes $\mathfrak{p}$ containing an associated prime. So let $\mathfrak{q}$ be an associated prime and $\mathfrak{p} \supset \mathfrak{q}$. We show that

$$\mathfrak{p} \in \mathrm{supp}M, \ \textit{i.e.}\ M_{\mathfrak{p}} \neq 0.$$

But there is an injective map

$$R/\mathfrak{q} \to M$$

so an injective map

$$(R/\mathfrak{q})_{\mathfrak{p}} \to M_{\mathfrak{p}}$$

where the first thing is nonzero since nothing nonzero in $R/\mathfrak{q}$ can be annihilated by something not in $\mathfrak{p}$. So $M_{\mathfrak{p}} \neq 0$.

The hard direction is the converse. Say that $\mathfrak{p} \in \mathrm{supp}M$. We have to show that $\mathfrak{p}$ contains an associated prime. Now $M_{\mathfrak{p}} \neq 0$ and it is a finitely generated $R_{\mathfrak{p}}$-module, where $R_{\mathfrak{p}}$ is noetherian. So this has an associated prime.

$$\mathrm{Ass}(M_{\mathfrak{p}}) \neq \emptyset$$

and we can find an element $\mathfrak{q}_\mathfrak{p} \subset R_\mathfrak{p}$ in there, where $\mathfrak{q}$ is a prime of R contained in $\mathfrak{p}$. But by the above fact about localization and associated primes, we have that

$$\mathfrak{q} \in \mathrm{Ass}(M)$$

and we have already seen that $\mathfrak{q} \subset \mathfrak{p}$. This proves the other inclusion and establishes the result. □

We have just seen that $\mathrm{supp}M$ is a closed subset of $\mathrm{Spec}R$ and is a union of finitely many irreducible subsets. More precisely,

$$\mathrm{supp}M = \bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \overline{\{\mathfrak{q}\}}$$

though there might be some redundancy in this expression. Some associated prime might be contained in others.

Definition 2.11. A prime $\mathfrak{p} \in \mathrm{Ass}(M)$ is an **isolated** associated prime of M if it is minimal (with respect to the ordering on $\mathrm{Ass}(M)$); it is **embedded** otherwise.

So the embedded primes are not needed to describe the support of M.

2.3 The case of one associated prime

Proposition 2.12. *Let M be a finitely generated R-module. Then*

$$\mathrm{supp}M = \{\mathfrak{p} \in \mathrm{Spec}R : \mathfrak{p} \text{ contains an associated prime}\}.$$

Definition 2.13. A finitely generated R-module M is **$\mathfrak{p}$-primary** if

$$\mathrm{Ass}(M) = \{\mathfrak{p}\}.$$

If $\mathrm{Ass}(M)$ consists of a point, we call M **primary**.

For the remainder of this lecture, R is a noetherian ring, and M a finitely generated R-module. $S \subset R$ is a multiplicatively closed subset.

2.4 A loose end

Let us start with an assertion we made last time, but we didn't prove. Namely, that

$$\mathrm{Ass}(S^{-1}M) = \left\{S^{-1}\mathfrak{p}, \mathfrak{p} \in \mathrm{Ass}(M), \mathfrak{p} \cap S = \emptyset\right\}.$$

We proved the easy direction, that if $\mathfrak{p} \in \mathrm{Ass}(M)$ and does not intersect S, then $S^{-1}\mathfrak{p}$ is an associated prime of $S^{-1}M$.

Proposition 2.14. *The reverse inclusion also holds.*

Proof. Let $\mathfrak{q} \in \mathrm{Ass}(S^{-1}M)$. This means that $\mathfrak{q} = \mathrm{Ann}(x/s)$ for some $x \in M$, $s \in S$.

Call the map $R \to S^{-1}R$ to be ϕ. Then $\phi^{-1}(\mathfrak{q})$ is the set of elements $a \in R$ such that

$$\frac{ax}{s} = 0 \in S^{-1}M.$$

In other words, by definition of the localization, this is

$$\bigcup_{t \in S} \{a \in R : atx = 0 \in M\} = \bigcup \mathrm{Ann}(tx) \subset R.$$

We know, however, that among elements of the form $\mathrm{Ann}(tx)$, there is a *maximal* element $I = \mathrm{Ann}(t_0 x)$ for some $t_0 \in S$. Indeed, R is noetherian. Then if you think about any other annihilator $I' = \mathrm{Ann}(tx)$, then I', I are both contained in $\mathrm{Ann}(t_0 tx)$. However,

$$I \subset \mathrm{Ann}(t_0 x)$$

and I is maximal, so $I = \mathrm{Ann}(t_0 tx)$ and

$$I' \subset I.$$

That is I contains all these other annihilators. In particular, the big union above, i.e. $\phi^{-1}(\mathfrak{q})$, is just

$$I = \mathrm{Ann}(t_0 x).$$

It follows that $\phi^{-1}(\mathfrak{q})$ is the annihilator of $\mathrm{Ann}(t_0 x)$, so this is an associated prime of M. This means that every associated prime of $S^{-1}M$ comes from an associated prime of M. That completes the proof. □

2.5 Primary modules

Definition 2.15. Let $\mathfrak{p} \subset R$ be prime, M a finitely generated R-module. Then M is **$\mathfrak{p}$-primary** if

$$\mathrm{Ass}(M) = \{\mathfrak{p}\}.$$

Let's say that the zero module is not primary.

A module is **primary** if it is $\mathfrak{p}$-primary for some $\mathfrak{p}$, i.e. has precisely one associated prime.

Proposition 2.16. *Let M be a finitely generated R-module. Then M is $\mathfrak{p}$-primary if and only if, for every $m \in M - \{0\}$, the annihilator $\mathrm{Ann}(m)$ has radical $\mathfrak{p}$.*

Proof. We first need a small observation.

Lemma 2.17. *If M is $\mathfrak{p}$-primary, so is any nonzero submodule of M is $\mathfrak{p}$-primary.*

Proof. Indeed, any associated prime of the submodule is an associated prime of M. Note that the submodule, if it is nonzero, it has an associated prime. That has to be $\mathfrak{p}$. □

Assume first M to be $\mathfrak{p}$-primary. Let $x \in M$, $x \neq 0$. Let $I = \mathrm{Ann}(x)$. So by definition there is an injection

$$R/I \to M$$

sending $1 \to x$. As a result, R/I is $\mathfrak{p}$-primary by the above lemma. We want to know that $\mathfrak{p} = \mathrm{Rad}(I)$. We saw that the support $\mathrm{supp}R/I = \{\mathfrak{q} : \mathfrak{q} \supset I\}$ is the union of the closures of the associated primes. In this case,

$$\mathrm{supp}(R/I) = \{\mathfrak{q} : \mathfrak{q} \supset \mathfrak{p}\}.$$

But we know that $\mathrm{Rad}(I) = \bigcap_{\mathfrak{q} \supset I} \mathfrak{q}$, which by the above is just $\mathfrak{p}$. This proves that $\mathrm{Rad}(I) = \mathfrak{p}$. We have shown that if R/I is primary, then I has radical $\mathfrak{p}$.

The converse is easy. Suppose the condition holds and $\mathfrak{q} \in \mathrm{Ass}(M)$, so $\mathfrak{q} = \mathrm{Ann}(x)$ for $x \neq 0$. But then $\mathrm{Rad}(\mathfrak{q}) = \mathfrak{p}$, so

$$\mathfrak{q} = \mathfrak{p}$$

and $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. □

We have another characterization.

Proposition 2.18. *Let $M \neq 0$ be a finitely generated R-module. Then M is primary iff for each $a \in R$, either multiplication $a : M \to M$ is injective or nilpotent.*

Proof. Suppose M to be $\mathfrak{p}$-primary. Then multiplication by anything in $\mathfrak{p}$ is nilpotent because the annihilator of everything nonzero has radical $\mathfrak{p}$. But if $a \notin \mathfrak{p}$, then $\mathrm{Ann}(x)$ for $x \in M - \{0\}$ has radical $\mathfrak{p}$ and cannot contain a.

Other direction, now. Assume that every element of a acts either injectively or nilpotently on M. Let $I \subset R$ be the collection of elements $a \in R$ such that $a^n M = 0$ for n large. Then I is an ideal; it is closed under addition by the binomial formula. If $a, b \in I$ and a^n, b^n act by zero, then $(a+b)^{2n}$ acts by zero as well.

I claim that I is actually prime. If $a, b \notin I$, then a, b act by multiplication injectively on I. So $a : M \to M, b : M \to M$ are injective. However, a composition of injections is injective, so ab acts injectively and $ab \notin I$. So I is prime.

We need now to check that if $x \in M$ is nonzero, then $\mathrm{Ann}(x)$ has radical I. This is because something $a \in R$ has a power that kills x, multiplication $M \xrightarrow{a} M$ can't be injective, so it must be nilpotent. Conversely, if $a \in I$, then a power of a is nilpotent, so it must kill x. □

So we have this notion of a primary module. The idea is that all the torsion is somehow concentrated in some prime.

3 Primary decomposition

This is the structure theorem for modules over a noetherian ring, in some sense.

Definition 3.1. Let M be a finitely generated R-module. A submodule $N \subset M$ is **$\mathfrak{p}$-coprimary** if M/N is $\mathfrak{p}$-primary.

Similarly, we can say that $N \subset M$ is **coprimary**.

Definition 3.2. $N \subsetneq M$ is **irreducible** if whenever $N = N_1 \cap N_2$ for $N_1, N_2 \subset M$, then either one of N_1, N_2 equals N. It is not nontrivially the intersection of larger submodules.

Proposition 3.3. *An irreducible submodule $N \subset M$ is coprimary.*

Proof. Say $a \in R$. We'd like to show that

$$M/N \xrightarrow{a} M/N$$

is either injective or nilpotent. Consider the following submodule of M/N:

$$K(n) = \{x \in M/N : a^n x = 0\}.$$

Then $K(0) \subset K(1) \subset \ldots$; this chain stops by noetherianness as the quotient module is noetherian. In particular, $K(n) = K(2n)$ for large n.

In particular, if $x \in M/N$ is divisible by a^n (n large) and nonzero, then $a^n x$ is also nonzero. Indeed, say $x = a^n y$; then $y \notin K(n)$, so $a^n x = a^{2n} y \neq 0$ or we would have $y \in K(2n) = K(n)$. In M/N, the submodules

$$a^n(M/N) \cap \ker(a^n)$$

are equal to zero for large n. But our assumption was that N is irreducible. So one of these submodules of M/N is zero. I.e., either $a^n(M/N) = 0$ or $\ker a^n = 0$. We get either injectivity or nilpotence on M/N. This proves the result. □

Proposition 3.4. *M has an irreducible decomposition. There exist finitely many irreducible submodules $N_1, \ldots, N_k$ with*

$$N_1 \cap \cdots \cap N_k = 0.$$

In other words,

$$M \to \bigoplus M/N_i$$

is injective. So a finitely generated module over a noetherian ring can be imbedded in a direct sum of primary modules.

Proof. Let $M' \subset M$ be a maximal submodule of M such that M' cannot be written as an intersection of finitely many irreducible submodules. If no such M' exists, then we're done, because then 0 can be written as an intersection of finitely many irreducible submodules.

Now M' is not irreducible, or it would be the intersection of one irreducible submodule. Then M' can be written as $M_1' \cap M_2'$ for two strictly larger submodules of M. But M_1', M_2' admit decompositions as intersections of irreducibles. So M' does as well, contradiction. □

For any M, we have an **irreducible decomposition**

$$0 = \bigcap N_i$$

for the N_i a finite set of irreducible (and thus coprimary) submodules. This decomposition here is highly non-unique and non-canonical. Let's try to pare it down to something which is a lot more canonical.

The first claim is that we can collect together modules which are coprimary for some prime.

Lemma 3.5. *Let $N_1, N_2 \subset M$ be $\mathfrak{p}$-coprimary submodules. Then $N_1 \cap N_2$ is also $\mathfrak{p}$-coprimary.*

Proof. We have to show that $M/N_1 \cap N_2$ is $\mathfrak{p}$-primary. Indeed, we have an injection

$$M/N_1 \cap N_2 \rightarrowtail M/N_1 \oplus M/N_2$$

which implies that $\mathrm{Ass}(M/N_1 \cap N_2) \subset \mathrm{Ass}(M/N_1) \cup \mathrm{Ass}(M/N_2) = \{\mathfrak{p}\}$. So we're done. □

In particular, if we don't want irreducibility but only primariness in the decomposition

$$0 = \bigcap N_i,$$

we can assume that each N_i is $\mathfrak{p}_i$ coprimary for some prime $\mathfrak{p}_i$ with the $\mathfrak{p}_i$ distinct.

Definition 3.6. Such a decomposition of zero is called a **primary decomposition**.

We can further assume that

$$N_i \not\supset \bigcap_{j \neq i} N_j$$

or we could omit one of the N_i. Let's assume that the decomposition is minimal. Then the decomposition is called a **reduced primary decomposition**.

Again, what this tells us is that $M \rightarrowtail \bigoplus M/N_i$. What we have shown is that M can be imbedded in a sum of pieces, each of which is $\mathfrak{p}$-primary for some prime, and the different primes are distinct.

This is **not** unique. However,

Proposition 3.7. *The primes $\mathfrak{p}_i$ that appear in a reduced primary decomposition of zero are uniquely determined. They are the associated primes of M.*

Proof. All the associated primes of M have to be there, because we have the injection

$$M \rightarrowtail \bigoplus M/N_i$$

so the associated primes of M are among those of M/N_i (i.e. the $\mathfrak{p}_i$).

The hard direction is to see that each $\mathfrak{p}_i$ is an associated prime. I.e. if M/N_i is $\mathfrak{p}_i$-primary, then $\mathfrak{p}_i \in \mathrm{Ass}(M)$; we don't need to use primary modules except for primes

in the associated primes. Here we need to use the fact that our decomposition has no redundancy. Without loss of generality, it suffices to show that $\mathfrak{p}_1$, for instance, belongs to $\mathrm{Ass}(M)$. We will use the fact that

$$N_1 \not\supset N_2 \cap \dots.$$

So this tells us that $N_2 \cap N_3 \cap \dots$ is not equal to zero, or we would have a containment. We have a map

$$N_2 \cap \dots \cap N_k \to M/N_1;$$

it is injective, since the kernel is $N_1 \cap N_2 \cap \dots \cap N_k = 0$ as this is a decomposition. However, M/N_1 is $\mathfrak{p}_1$-primary, so $N_2 \cap \dots \cap N_k$ is $\mathfrak{p}_1$-primary. In particular, $\mathfrak{p}_1$ is an associated prime of $N_2 \cap \dots \cap N_k$, hence of M. □

The primes are determined. The factors are not. However, in some cases they are.

Proposition 3.8. *Let $\mathfrak{p}_i$ be a minimal associated prime of M, i.e. not containing any smaller associated prime. Then the submodule N_i corresponding to $\mathfrak{p}_i$ in the reduced primary decomposition is uniquely determined: it is the kernel of*

$$M \to M_{\mathfrak{p}_i}.$$

Proof. We have that $\bigcap N_j = \{0\} \subset M$. When we localize at $\mathfrak{p}_i$, we find that

$$(\bigcap N_j)_{\mathfrak{p}_i} = \bigcap (N_j)_{\mathfrak{p}_i} = 0$$

as localization is an exact functor. If $j \neq i$, then M/N_j is $\mathfrak{p}_j$ primary, and has only $\mathfrak{p}_j$ as an associated prime. It follows that $(M/N_j)_{\mathfrak{p}_i}$ has no associated primes, since the only associated prime could be $\mathfrak{p}_j$, and that's not contained in $\mathfrak{p}_j$. In particular, $(N_j)_{\mathfrak{p}_i} = M_{\mathfrak{p}_i}$.

Thus, when we localize the primary decomposition at $\mathfrak{p}_i$, we get a trivial primary decomposition: most of the factors are the full $M_{\mathfrak{p}_i}$. It follows that $(N_i)_{\mathfrak{p}_i} = 0$. When we draw a commutative diagram

$$\begin{array}{ccc} N_i & \longrightarrow & (N_i)_{\mathfrak{p}_i} = 0 \\ \downarrow & & \downarrow \\ M & \longrightarrow & M_{\mathfrak{p}_i}. \end{array}$$

we find that N_i goes to zero in the localization.

Now if $x \in \ker(M \to M_{\mathfrak{p}_i}$, then $sx = 0$ for some $s \notin \mathfrak{p}_i$. When we take the map $M \to M/N_i$, sx maps to zero; but s acts injectively on M/N_i, so x maps to zero in M/N_i, i.e. is zero in N_i. □

This has been abstract, so:

Example 3.9. Let $R = \mathbb{Z}$. Let $M = \mathbb{Z} \oplus \mathbb{Z}/p$. Then zero can be written as

$$\mathbb{Z} \cap \mathbb{Z}/p$$

as submodules of M. But $\mathbb{Z}$ is $\mathfrak{p}$-coprimary, while $\mathbb{Z}/p$ is (0)-coprimary.

This is not unique. We could have considered

$$\{(n, n), n \in \mathbb{Z}\} \subset M.$$

However, the zero-coprimary part has to be the p-torsion. This is because (0) is the minimal ideal.

The decomposition is always unique, in general, if we have no inclusions among the prime ideals. For $\mathbb{Z}$-modules, this means that primary decomposition is unique for torsion modules. Any torsion group is a direct sum of the p-power torsion over all primes p.

Chapter 6

Unique factorization and the class group

Today, we will talk about unique factorization.

0.1 Unique factorization

Let R be a domain.

Definition 0.10. A nonzero element $x \in R$ is **prime** if (x) is a prime ideal.

In other words, x is not a unit, and if $x \mid ab$, then either $x \mid a$ or $x \mid b$.

Definition 0.11. A domain R is **factorial** if every nonzero noninvertible element $x \in R$ factors as a product $x_1 \dots x_n$ where each x_i is prime.

A simple observation:

Proposition 0.12. *This factorization is essentially unique, that is up to multiplication by units.*

Proof. Let $x \in R$ be a nonunit. Say $x = x_1 \dots x_n = y_1 \dots y_m$ were two different prime factorizations. Then $m, n > 0$.

We have that $x_1 \mid y_1 \dots y_m$, so $x_1 \mid y_i$ for some i. But y_i is prime. So x_1 and y_i differ by a unit. By removing each of these, we can get a smaller set of nonunique factorizations. Namely, we find that

$$x_2 \dots x_n = y_1 \dots \hat{y_i} \dots y_m$$

and then we can induct on the number of factors. □

The motivating example is of course:

Example 0.13. $\mathbb{Z}$ is factorial. This is the fundamental theorem of arithmetic.

0.2 A ring-theoretic criterion

Definition 0.14. Let R be a domain. A prime ideal $\mathfrak{p} \subset R$ is said to be of **height one** if $\mathfrak{p}$ is minimal among ideals containing x for some nonzero $x \in R$.

So a prime of height one is not the zero prime, but it is as close to zero as possible, in some sense. When we later talk about dimension theory, we will talk about primes of any height. In a sense, $\mathfrak{p}$ is "almost" generated by one element.

Theorem 0.15. *Let R be a noetherian domain. The following are equivalent:*

1. *R is factorial.*
2. *Every height one prime is principal.*

Proof. Let's first show 1) implies 2). Assume R is factorial and $\mathfrak{p}$ is height one, minimal containing (x) for some $x \neq 0 \in R$. Then x is a nonunit, and it is nonzero, so it has a prime factorization

$$x = x_1 \dots x_n, \quad \text{each } x_i \text{ prime.}$$

Some $x_i \in \mathfrak{p}$ because $\mathfrak{p}$ is prime. In particular,

$$\mathfrak{p} \supset (x_i) \supset (x).$$

But (x_i) is prime itself, and it contains (x). The minimality of $\mathfrak{p}$ says that $\mathfrak{p} = (x_i)$.

Conversely, suppose every height one prime is principal. Let $x \in R$ be nonzero and a nonunit. We want to factor x as a product of primes. Consider the ideal $(x) \subsetneq R$. As a result, (x) is contained in a prime ideal. Since R is noetherian, there is a minimal prime ideal $\mathfrak{p}$ containing (x). Then $\mathfrak{p}$, being a height one prime, is principal—say $\mathfrak{p} = (x_1)$. It follows that $x_1 \mid x$ and x_1 is prime. Say

$$x = x_1 x_1'.$$

If x_1' is a nonunit, repeat this process to get $x_1' = x_2 x_2'$ with x_2 a prime element. Keep going; inductively we have

$$x_k = x_{k+1} x_{k+1}'.$$

If this process stops, with one of the x_k' a unit, we get a prime factorization of x. Suppose the process continues forever. Then we would have

$$(x) \subsetneq (x_1') \subsetneq (x_2') \subsetneq (x_3') \subsetneq \dots,$$

which is impossible by noetherianness. □

We have seen that unique factorization can be formulated in terms of prime ideals.

0.3 Locally factorial domains

Definition 0.16. A noetherian domain R is said to be **locally factorial** if $R_{\mathfrak{p}}$ is factorial for each $\mathfrak{p}$ prime.

Example 0.17. The coordinate ring $\mathbb{C}[x_1, \ldots, x_n/I$ of an algebraic variety is locally factorial if the variety is smooth. We may talk about this later.

Example 0.18 (Nonexample)**.** Let R be $\mathbb{C}[A, B, C, D]/(AD - BC)$. The spectrum of R has maximal ideals consisting of 2-by-2 matrices of determinant zero. This variety is very singular at the origin. It is not even locally factorial at the origin.

The failure of unique factorization comes from the fact that

$$AD = BC$$

in this ring R. This is a protypical example of a ring without unique factorization. The reason has to do with the fact that the variety has a singularity at the origin.

0.4 The Picard group

Definition 0.19. Let R be a commutative ring. An R-module I is **invertible** if there exists J such that

$$I \otimes_R J \simeq R.$$

Invertibility is with respect to the tensor product.

Remark. You're supposed to think of a module as giving something like a vector bundle on Spec$R$. An invertible module looks like a line bundle on Spec$R$.

There are many equivalent characterizations.

Proposition 0.20. *Let R be a ring, I an R-module. TFAE:*

1. *I is invertible.*
2. *I is finitely generated and $I_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$ for all primes $\mathfrak{p} \subset R$.*
3. *I is finitely generated and there exist $a_1, \ldots, a_n \in R$ which generate (1) in R such that*
$$I[a_i^{-1}] \simeq R[a_i^{-1}].$$

Proof. First, we show that if I is invertible, then I is finitely generated Suppose $I \otimes_R J \simeq R$. This means that $1 \in R$ corresponds to an element

$$\sum i_k \otimes j_k \in I \otimes_R J.$$

Thus, there exists a finitely generated submodule $I_0 \subset I$ such that the map $I_0 \otimes J \to I \otimes J$ is surjective. Tensor this with I, so we get a surjection

$$I_0 \simeq I_0 \otimes J \otimes I \to I \otimes J \otimes I \simeq I$$

which leads to a surjection $I_0 \twoheadrightarrow I$. This implies that I is finitely generated

We now show 1 implies 2. Note that if I is invertible, then $I \otimes_R R'$ is an invertible R' module for any R-algebra R'; to get an inverse, tensor the inverse of I with R'. In particular, $I_{\mathfrak{p}}$ is an invertible $R_{\mathfrak{p}}$-module for each $\mathfrak{p}$. As a result,

$$I_{\mathfrak{p}}/\mathfrak{p}I_{\mathfrak{p}}$$

is invertible over $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. This means that $I_{\mathfrak{p}}/\mathfrak{p}I_{\mathfrak{p}}$ is a one-dimensional vector space over the residue field. (The invertible modules over a vector space are the one-dimensional spaces.) Choose an element $x \in I_{\mathfrak{p}}$ which generates $I_{\mathfrak{p}}/\mathfrak{p}I_{\mathfrak{p}}$. Since $I_{\mathfrak{p}}$ is finitely generated, this shows that x generates $I_{\mathfrak{p}}$.

We get a surjection $\alpha : R_{\mathfrak{p}} \twoheadrightarrow I_{\mathfrak{p}}$ carrying $1 \to x$. I claim that:

This map is injective.

This will imply that $I_{\mathfrak{p}}$ is free of rank 1. Well, let J be an inverse of I in R-modules; the same argument provides a surjection $\beta : R_{\mathfrak{p}} \to J_{\mathfrak{p}}$. We get a map

$$R_{\mathfrak{p}} \overset{\alpha}{\twoheadrightarrow} I_{\mathfrak{p}} \overset{\beta'}{\twoheadrightarrow} R_{\mathfrak{p}}$$

(where $\beta = \beta \otimes 1_{I_{\mathfrak{p}}}$) whose composite must be multiplication by a unit, since the ring is local. Thus the composite is injective and α is injective.

Now we show 2 implies 3. Suppose I is finitely generated and $I_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$ for all $\mathfrak{p}$. I claim that for each $\mathfrak{p}$, we can choose an element x of $I_{\mathfrak{p}}$ generating $I_{\mathfrak{p}}$. By multiplying by the denominator, we can assume that $x \in I$. Then if $\{x_1, \dots, x_n\} \subset I$ generates I, then we have equalities

$$s_i x_i = a_i x \in R$$

for some $s_i \notin \mathfrak{p}$ as x generates $I_{\mathfrak{p}}$. This means that x generates I after inverting the s_i. It follows that $I[1/a] = R[1/a]$ where $a = \prod s_i \notin \mathfrak{p}$. In particular, we find that there is an open covering $\{\mathrm{Spec}R[1/a_{\mathfrak{p}}]\}$ of $\mathrm{Spec}R$ (where $a_{\mathfrak{p}} \notin \mathfrak{p}$) on which I is isomorphic to R. To say that these cover $\mathrm{Spec}R$ is to say that the $a_{\mathfrak{p}}$ generate 1.

Finally, let's do the implication 3 implies 1. Assume that we have the situation of $I[1/a_i] \simeq R[1/a_i]$. We want to show that I is invertible. We start by showing that I is **finitely presented**. This means that there is an exact sequence

$$R^m \to R^n \to I \to 0,$$

i.e. I is the cokernel of a map between free modules of finite rank. To see this, first, we've assumed that I is finitely generated. So there is a surjection

$$R^n \twoheadrightarrow I$$

with a kernel $K \rightarrowtail R^n$. We must show that K is finitely generated. Localization is an exact functor, so $K[1/a_i]$ is the kernel of $R[1/a_i]^n \to I[1/a_i]$. However, we have an exact sequence

$$K[1/a_i] \rightarrowtail R[1/a_i]^n \twoheadrightarrow R[1/a_i]$$

by the assumed isomorphism $I[1/a_i] \simeq R[1/a_i]$. But since a free module is projective, this sequence splits and we find that $K[1/a_i]$ is finitely generated. If it's finitely generated, it's generated by finitely many elements in K. As a result, we find that there is a map

$$R^N \to K$$

such that the localization to $\mathrm{Spec} R[1/a_i]$ is surjective. This implies by the homework that $R^N \to K$ is surjective.[1] Thus K is finitely generated.

In any case, we have shown that the module I is finitely presented. **Define** $J = \mathrm{Hom}_R(I, R)$ as the candidate for its dual. This construction is compatible with localization. We can choose a finite presentation $R^m \to R^n \to I \to 0$, which leads to a sequence

$$0 \to J \to \mathrm{Hom}(R^n, R) \to \mathrm{Hom}(R^m, R).$$

It follows that the formation of J commutes with localization. In particular, this argument shows that

$$J[1/a] = \mathrm{Hom}_{R[1/a]}(I[1/a], R[1/a]).$$

One can check this by using the description of J. By construction, there is a canonical map $I \otimes J \to R$. I claim that this map is invertible.

For the proof, we use the fact that one can check for an isomorphism locally. It suffices to show that

$$I[1/a] \otimes J[1/a] \to R[1/a]$$

is an isomorphism for some collection of a's that generate the unit ideal. However, we have $a_1, \ldots, a_n$ that generate the unit ideal such that $I[1/a_i]$ is free of rank 1, hence so is $J[1/a_i]$. It thus follows that $I[1/a_i] \otimes J[1/a_i]$ is an isomorphism. □

Definition 0.21. Let R be a commutative ring. We define the **Picard group** $\mathrm{Pic}(R)$ to be the set of isomorphism classes of invertible R-modules. This is an abelian group under the tensor product; the identity element is given by R.

Next time, we will continue talking about the Picard group and how it controls the failure of unique factorization.

Last time, for a commutative ring R, we defined the **Picard group** $\mathrm{Pic}(R)$ as the set of isomorphism classes of invertible R-modules. The group structure is given by the tensor product.

0.5 Cartier divisors

Assume furthermore that R is a domain. We now introduce:

Definition 0.22. A **Cartier divisor** for R is a submodule $M \subset K(R)$ such that M is invertible.

[1] To check that a map is surjective, just check at the localizations at any maximal ideal.

In other words, a Cartier divisor is an invertible fractional ideal. Alternatively, it is an invertible R-module M with a nonzero map $M \to K(R)$. **Once this map is nonzero, it is automatically injective,** since injectivity can be checked at the localizations, and any module-homomorphism from a domain into its quotient field is either zero or injective (because it is multiplication by some element).

We now make this into a group.

Definition 0.23. Given $(M, a : M \hookrightarrow K(R))$ and $(N, b : N \hookrightarrow K(R))$, we define the sum to be

$$(M \otimes N, a \otimes b : M \otimes N \hookrightarrow K(R)).$$

The map $a \otimes b$ is nonzero, so by what was said above, it is an injection. Thus the Cartier divisors from an abelian group $\mathrm{Cart}(R)$.

By assumption, there is a homomorphism

$$\mathrm{Cart}(R) \to \mathrm{Pic}(R)$$

mapping $(M, M \hookrightarrow K(R)) \to M$.

Proposition 0.24. *The map* $\mathrm{Cart}(R) \to \mathrm{Pic}(R)$ *is surjective. In other words, any invertible R-module can be embedded in $K(R)$.*

Proof. Let M be an invertible R-module. Indeed, we know that $M_{(0)} = M \otimes_R K(R)$ is an invertible $K(R)$-module, so a one-dimensional vector space over $K(R)$. In particular, $M_{(0)} \simeq K(R)$. There is a nonzero homomorphic map

$$M \to M_{(0)} \simeq K(R),$$

which is automatically injective by the discussion above. □

What is the kernel of $\mathrm{Cart}(R) \to \mathrm{Pic}(R)$? This is the set of Cartier divisors which are isomorphic to R itself. In other words, it is the set of $(R, R \hookrightarrow K(R))$. This data is the same thing as the data of a nonzero element of $K(R)$. So the kernel of

$$\mathrm{Cart}(R) \to \mathrm{Pic}(R)$$

has kernel isomorphic to $K(R)^*$. We have a short exact sequence

$$K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0.$$

0.6 Weil divisors and Cartier divisors

Now, we want to assume $\mathrm{Cart}(R)$ if R is "good." The "goodness" in question is to assume that R is locally factorial, i.e. that $R_{\mathfrak{p}}$ is factorial for each $\mathfrak{p}$. This is true, for instance, if R is the coordinate ring of a smooth algebraic variety.

Proposition 0.25. *If R is locally factorial and noetherian, then the group* $\mathrm{Cart}(R)$ *is a free abelian group. The generators are in bijection with the height one primes of R.*

We start by discussing Weil divisors.

Definition 0.26. A **Weil divisor** for R is a formal linear combination $\sum n_i[\mathfrak{p}_i]$ where the $\mathfrak{p}_i$ range over height one primes of R. So the group of Weil divisors is the free abelian group on the height one primes of R. We denote this group by $\mathrm{Weil}(R)$.

Now assume that R is a locally factorial, noetherian domain. We shall produce an isomorphism

$$\mathrm{Weil}(R) \simeq \mathrm{Cart}(R)$$

that sends $[\mathfrak{p}_i]$ to that height one prime $\mathfrak{p}_i$ together with the imbedding $\mathfrak{p}_i \hookrightarrow R \to K(R)$.

We first check that this is well-defined. Since $\mathrm{Weil}(R)$ is free, all we have to do is check that each $\mathfrak{p}_i$ is a legitimate Cartier divisor. In other words, we need to show that:

Proposition 0.27. *If $\mathfrak{p} \subset R$ is a height one prime and R locally factorial, then $\mathfrak{p}$ is invertible.*

Proof. In the last lecture, we gave a criterion for invertibility: namely, being locally trivial. We have to show that for any prime $\mathfrak{q}$, we have that $\mathfrak{p}_\mathfrak{q}$ is isomorphic to $R_\mathfrak{q}$. If $\mathfrak{p} \not\subset \mathfrak{q}$, then $\mathfrak{p}_\mathfrak{q}$ is the entire ring $R_\mathfrak{q}$, so this is obvious. Conversely, suppose $\mathfrak{p} \subset \mathfrak{q}$. Then $\mathfrak{p}_\mathfrak{q}$ is a height one prime of $R_\mathfrak{q}$: it is minimal over some element in $R_\mathfrak{q}$.

Thus $\mathfrak{p}_\mathfrak{q}$ is principal, in particular free of rank one, since $R_\mathfrak{q}$ is factorial. We saw last time that being factorial is equivalent to the principalness of height one primes. □

We need to define the inverse map

$$\mathrm{Cart}(R) \to \mathrm{Weil}(R).$$

In order to do this, start with a Cartier divisor $(M, M \hookrightarrow K(R))$. We then have to describe which coefficient to assign a height one prime. To do this, we use a local criterion.

Let's first digress a bit. Consider a locally factorial domain R and a prime $\mathfrak{p}$ of height one. Then $R_\mathfrak{p}$ is factorial. In particular, its maximal ideal $\mathfrak{p}R_\mathfrak{p}$ is height one, so principal. It is the principal ideal generated by some $t \in R_\mathfrak{p}$. Now we show:

Proposition 0.28. *Every nonzero ideal in $R_\mathfrak{p}$ is of the form (t^n) for some unique $n \geq 0$.*

Proof. Let $I_0 \subset R_\mathfrak{p}$ be nonzero. If $I_0 = R_\mathfrak{p}$, then we're done—it's generated by t^0. Otherwise, $I_0 \subsetneq R_\mathfrak{p}$, so contained in $\mathfrak{p}R_\mathfrak{p} = (t)$. So let $I_1 = \{x \in R_\mathfrak{p} : tx \in I_0\}$. Thus

$$I_1 = t^{-1}I_0.$$

I claim now that $I_1 \neq I_0$, i.e. that there exists $x \in R_\mathfrak{p}$ such that $x \notin I_0$ but $tx \in I_0$. The proof comes from the theory of associated primes. Look at $R_\mathfrak{p}/I_0$; it has at least one associated prime as it is nonzero.

Since it is a torsion module, this associated prime must be $\mathfrak{p}R_{\mathfrak{p}}$ since the only primes in $R_{\mathfrak{p}}$ are (0) and (t), **which we have not yet shown**. So there exists an element in the quotient R/I_0 whose annihilator is precisely (t). Lifting this gives an element in R which when multiplied by (t) is in I_0 but which is not in I_0. So $I_0 \subsetneq I_1$.

Proceed as before now. Define $I_2 = \{x \in R_{\mathfrak{p}} : tx \in I_1\}$. This process must halt since we have assumed noetherianness. We must have $I_m = I_{m+1}$ for some m, which would imply that some $I_m = R_{\mathfrak{p}}$ by the above argument. It then follows that $I_0 = (t^m)$ since each I_i is just tI_{i+1}. □

We thus have a good structure theory for ideals in R localized at a height one prime. Let us make a more general claim.

Proposition 0.29. *Every nonzero finitely generated $R_{\mathfrak{p}}$-submodule of the fraction field $K(R)$ is of the form (t^n) for some $n \in \mathbb{Z}$.*

Proof. Say that $M \subset K(R)$ is such a submodule. Let $I = \{x \in R_{\mathfrak{p}}, xM \subset R_{\mathfrak{p}}\}$. Then $I \neq 0$ as M is finitely generated M is generated over $R_{\mathfrak{p}}$ by a finite number of fractions $a_i/b_i, b_i \in R$. Then the product $b = \prod b_i$ brings M into $R_{\mathfrak{p}}$.

We know that $I = (t^m)$ for some m. In particular, $t^m M$ is an ideal in R. In particular,

$$t^m M = t^p R$$

for some p, in particular $M = t^{p-m}R$.

□

Now let's go back to the main discussion. R is a noetherian locally factorial domain; we want to construct a map

$$\mathrm{Cart}(R) \to \mathrm{Weil}(R).$$

Given $(M, M \hookrightarrow K(R))$ with M invertible, we want to define a formal sum $\sum n_i[\mathfrak{p}_i]$. For every height one prime $\mathfrak{p}$, let us look at the local ring $R_{\mathfrak{p}}$ with maximal ideal generated by some $t_{\mathfrak{p}} \in R_{\mathfrak{p}}$. Now $M_{\mathfrak{p}} \subset K(R)$ is a finitely generated $R_{\mathfrak{p}}$-submodule, so generated by some $t_{\mathfrak{p}}^{n_{\mathfrak{p}}}$. So we map $(M, M \hookrightarrow K(R))$ to

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}}[\mathfrak{p}].$$

First, we have to check that this is well-defined. In particular, we have to show:

Proposition 0.30. *For almost all height one $\mathfrak{p}$, we have $M_{\mathfrak{p}} = R_{\mathfrak{p}}$. In other words, the integers $n_{\mathfrak{p}}$ are almost all zero.*

Proof. We can always assume that M is actually an ideal. Indeed, choose $a \in R$ with $aM = I \subset R$. As Cartier divisors, we have $M = I - (a)$. If we prove the result for I and (a), then we will have proved it for M (note that the $n_{\mathfrak{p}}$'s are additive

invariants[2]). So because of this additivity, it is sufficient to prove the proposition for actual (i.e. nonfractional) ideals.

Assume thus that $M \subset R$. All of these $n_{\mathfrak{p}}$ associated to M are at least zero because M is actually an ideal. What we want is that $n_{\mathfrak{p}} \leq 0$ for almost all $\mathfrak{p}$. In other words, we must show that

$$M_{\mathfrak{p}} \supset R_{\mathfrak{p}} \quad \text{almost all } \mathfrak{p}.$$

To do this, just choose any $x \in M - 0$. There are finitely many minimal primes containing (x) (by primary decomposition applied to $R/(x)$). Every other height one prime $\mathfrak{q}$ does not contain (x).[3] This states that $M_{\mathfrak{q}} \supset x/x = 1$, so $M_{\mathfrak{q}} \supset R_{\mathfrak{q}}$.

The key claim we've used in this proof is the following. If $\mathfrak{q}$ is a height one prime in a domain R containing some nonzero element (x), then $\mathfrak{q}$ is minimal among primes containing (x). In other words, we can test the height one condition at any nonzero element in that prime. Alternatively:

Lemma 0.31. *There are no nontrivial containments among height one primes.*

□

Anyway, we have constructed maps between $\mathrm{Cart}(R)$ and $\mathrm{Weil}(R)$. The map $\mathrm{Cart}(R) \to \mathrm{Weil}(R)$ takes $M \to \sum n_{\mathfrak{p}}[\mathfrak{p}]$. The other map $\mathrm{Weil}(R) \to \mathrm{Cart}(R)$ takes $[\mathfrak{p}] \to \mathfrak{p} \subset K(R)$. The composition $\mathrm{Weil}(R) \to \mathrm{Weil}(R)$ is the identity. Why is that? Start with a prime $\mathfrak{p}$; that goes to the Cartier divisor $\mathfrak{p}$. Then we need to finitely generatedre the multiplicities at other height one primes. But if $\mathfrak{p}$ is height one and $\mathfrak{q}$ is a height one prime, then if $\mathfrak{p} \neq \mathfrak{q}$ the lack of nontrivial containment relations implies that the multiplicity of $\mathfrak{p}$ at $\mathfrak{q}$ is zero. We have shown that

$$\mathrm{Weil}(R) \to \mathrm{Cart}(R) \to \mathrm{Weil}(R)$$

is the identity.

Now we have to show that $\mathrm{Cart}(R) \to \mathrm{Weil}(R)$ is injective. Say we have a Cartier divisor $(M, M \hookrightarrow K(R))$ that maps to zero in $\mathrm{Weil}(R)$, i.e. all its multiplicities $n_{\mathfrak{p}}$ are zero at height one primes. We show that $M = R$.

First, assume $M \subset R$. It is sufficient to show that at any maximal ideal $\mathfrak{m} \subset R$, we have

$$M_{\mathfrak{m}} = R_{\mathfrak{m}}.$$

What can we say? Well, $M_{\mathfrak{m}}$ is principal as M is invertible, being a Cartier divisor. Let it be generated by $x \in R_{\mathfrak{m}}$; suppose x is a nonunit (or we're already done). But $R_{\mathfrak{m}}$ is factorial, so $x = x_1 \dots x_n$ for each x_i prime. If $n > 0$, then however M has nonzero multiplicity at the prime ideal $(x_i) \subset R_{\mathfrak{m}}$. This is a contradiction.

The general case of M not really a subset of R can be handled similarly: then the generating element x might lie in the fraction field. So x, if it is not a unit in R, is a product of some primes in the numerator and some primes in the denominator. The nonzero primes that occur lead to nonzero multiplicities.

[2]To see this, localize at $\mathfrak{p}$—then if M is generated by t^a, N generated by t^b, then $M \otimes N$ is generated by t^{a+b}.

[3]Again, we're using something about height one primes not proved yet.

0.7 Recap and a loose end

Last time, it was claimed that if R is a locally factorial domain, and $\mathfrak{p} \subset R$ is of height one, then every prime ideal of $R_{\mathfrak{p}}$ is either maximal or zero. This follows from general dimension theory. This is equivalent to the following general claim about height one primes:

> There are no nontrivial inclusions among height one primes for R a locally factorial domain.

Proof. Suppose $\mathfrak{q} \subsetneq \mathfrak{p}$ is an inclusion of height one primes.

Replace R by $R_{\mathfrak{p}}$. Then R is local with some maximal ideal $\mathfrak{m}$, which is principal with some generator x. Then we have an inclusion

$$0 \subset \mathfrak{q} \subset \mathfrak{m}.$$

This inclusion is proper. However, $\mathfrak{q}$ is principal since it is height one in the factorial ring $R_{\mathfrak{p}}$. This cannot be since every element is a power of x times a unit. (Alright, this wasn't live TEXed well.) □

Last time, we were talking about $\mathrm{Weil}(R)$ and $\mathrm{Cart}(R)$ for R a locally factorial noetherian domain.

1. $\mathrm{Weil}(R)$ is free on the height one primes.
2. $\mathrm{Cart}(R)$ is the group of invertible submodules of $K(R)$.

We produced an isomorphism

$$\mathrm{Weil}(R) \simeq \mathrm{Cart}(R).$$

Remark. Geometrically, what is this? Suppose $R = \mathbb{C}[X_1, \ldots, X_n]/I$ for some ideal I. Then the maximal ideals, or closed points in $\mathrm{Spec}R$, are certain points in $\mathbb{C}^n$; they form an irreducible variety if R is a domain. The locally factorial condition is satisfied, for instance, if the variety is *smooth*. In this case, the Weil divisors correspond to sums of irreducible varieties of codimension one—which correspond to the primes of height one. The Weil divisors are free on the set of irreducible varieties of codimension one.

The Cartier divisors can be thought of as "linear combinations" of subvarieties which are locally defined by one equation. It is natural to assume that the condition of being defined by one equation corresponds to being codimension one. This is true by the condition of R locally factorial.

In general, we can always construct a map

$$\mathrm{Cart}(R) \to \mathrm{Weil}(R),$$

but it is not necessarily an isomorphism.

0.8 Further remarks on $\mathrm{Weil}(R)$ and $\mathrm{Cart}(R)$

Recall that the Cartier group fits in an exact sequence:

$$K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0,$$

because every element of $\mathrm{Cart}(R)$ determines its isomorphism class, and every element of $K(R)^*$ determines a free module of rank one. Contrary to what was stated last time, it is **not true** that exactness holds on the right. In fact, the kernel is the group R^* of units of R. So the exact sequence runs

$$0 \to R^* \to K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0.$$

This is true for *any* domain R. For R locally factorial and noetherian, we know that $\mathrm{Cart}(R) \simeq \mathrm{Weil}(R)$, though.

We can think of this as a generalization of unique factorization.

Proposition 0.32. *R is factorial if and only if R is locally factorial and $\mathrm{Pic}(R) = 0$.*

Proof. Assume R is locally factorial and $\mathrm{Pic}(R) = 0$. Then every prime ideal of height one (an element of $\mathrm{Weil}(R)$, hence of $\mathrm{Cart}(R)$) is principal, which implies that R is factorial. And conversely. □

In general, we can think of the exact sequence above as a form of unique factorization for a locally factorial domain: any invertible fractional ideal is a product of height one prime ideals.

Let us now give an example.

0.9 Discrete valuation rings and Dedekind rings

Example 0.33. Let R be a noetherian local domain whose prime ideals are (0) and the maximal ideal $\mathfrak{m} \neq 0$. In this condition, I claim:

Proposition 0.34. *TFAE:*

1. *R is factorial.*
2. *$\mathfrak{m}$ is principal.*
3. *R is integrally closed.*
4. *R is a valuation ring with value group $\mathbb{Z}$.*

Definition 0.35. A ring satisfying these conditions is called a **discrete valuation ring** (**DVR**). A discrete valuation ring necessarily has only two prime ideals. In fact, a valuation ring with value group $\mathbb{Z}$ satisfies all the above conditions.

Proof. Suppose R is factorial. Then every prime ideal of height one is principal. But $\mathfrak{m}$ is the only prime that can be height one (it's minimal over any nonzero nonunit of R. Thus 1 implies 2, and similarly 2 implies 1.

1 implies 3 is true for any R: factorialness implies integrally closedness. This is either either homework on the problem set or an easy exercise one can do for yourself.

4 implies 2 because one chooses an element $x \in R$ such that the valuation of x is one. Then, it is easy to see that x generates $\mathfrak{m}$: if $y \in \mathfrak{m}$, then the valuation of y is at least one, so $y/x \in R$ and $y = (y/x)x \in (x)$.

The implication 2 implies 4 was essentially done last time. Suppose $\mathfrak{m}$ is principal, generated by t. Last time, we saw that *all* nonzero ideals of R have the form (t^n) for some $n > 0$. If $x \in R$, we define the valuation of x to be n if $(x) = (t^n)$. One can easily check that this is a valuation on R which extends to the quotient field by additivity.

The interesting part of the argument is the claim that 3 implies 2. Suppose R is integrally closed; I claim that $\mathfrak{m}$ is principal. Choose $x \in \mathfrak{m} - \{0\}$. If $(x) = \mathfrak{m}$, we're done. Otherwise, we can look at $\mathfrak{m}/(x) \neq 0$. We have a finitely generated module over a noetherian ring which is nonzero, so it has an associated prime. That associated prime is either zero or $\mathfrak{m}$. But 0 is not an associated prime because every element in the module is killed by x. So $\mathfrak{m}$ is an associated prime.

Thus, there is $y \in \mathfrak{m}$ such that $y \notin (x)$ and $\mathfrak{m}y \subset (x)$. In particular, $y/x \in K(R) - R$ but

$$(y/x)\mathfrak{m} \subset R.$$

There are two cases:

1. Suppose $(y/x)\mathfrak{m} = R$. Then we can write $\mathfrak{m} = R(x/y)$. So $\mathfrak{m}$ is principal. (This argument shows that $x/y \in R$.)

2. The other possibility is that $y/x\mathfrak{m} \subsetneq R$. In this case, this is an ideal, so

   $$(y/x)\mathfrak{m} \subset \mathfrak{m}.$$

   In particular, multiplication by y/x carries $\mathfrak{m}$ to itself. So multiplication by y/x stabilizes the finitely generated module $\mathfrak{m}$. By the usual characteristic polynomial argument, we see that y/x is integral over R. In particular, $y/x \in R$, as R was integrally closed, a contradiction as $y \notin (x)$.

□

We now introduce a closely related notion.

Definition 0.36. A **Dedekind ring** is a noetherian domain R such that

1. R is integrally closed.

2. Every nonzero prime ideal of R is maximal.

Remark. If R is Dedekind, then any nonzero element is height one. This is evident since every nonzero prime is maximal.

If R is Dedekind, then R is locally factorial. In fact, the localization of R at a nonzero prime $\mathfrak{p}$ is a DVR.

Proof. $R_{\mathfrak{p}}$ has precisely two prime ideals: (0) and $\mathfrak{p}R_{\mathfrak{p}}$. As a localization of an integrally closed domain, it is integrally closed. So $R_{\mathfrak{p}}$ is a DVR by the above result (hence factorial). □

Assume R is Dedekind now. We have an exact sequence

$$0 \to R^* \to K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0.$$

Here $\mathrm{Cart}(R) \simeq \mathrm{Weil}(R)$. But $\mathrm{Weil}(R)$ is free on the nonzero primes, or equivalently maximal ideals, R being Dedekind. In fact, however, $\mathrm{Cart}(R)$ has a simpler description.

Proposition 0.37. *Suppose R is Dedekind. Then* $\mathrm{Cart}(R)$ *consists of all nonzero finitely generated submodules of $K(R)$ (i.e.* ***fractional ideals****).*

This is the same thing as saying as every nonzero finitely generated submodule of $K(R)$ is invertible.

Proof. Suppose $M \subset K(R)$ is nonzero and finitely generated It suffices to check that M is invertible after localizing at every prime, i.e. that $M_{\mathfrak{p}}$ is an invertible—or equivalently, trivial, $R_{\mathfrak{p}}$-module. At the zero prime, there is nothing to check. We might as well assume that $\mathfrak{p}$ is maximal. Then $R_{\mathfrak{p}}$ is a DVR and $M_{\mathfrak{p}}$ is a finitely generated submodule of $K(R_{\mathfrak{p}}) = K(R)$.

Let S be the set of integers n such that there exists $x \in M_{\mathfrak{p}}$ with $v(x) = n$, for v the valuation of $R_{\mathfrak{p}}$. By finite generation of M, S is bounded below. Thus S has a least element k. There is an element of $M_{\mathfrak{p}}$, call it x, with valuation k.

It is easy to check that $M_{\mathfrak{p}}$ is generated by x, and is in fact free with generator x. The reason is simply that x has the smallest valuation of anything in $M_{\mathfrak{p}}$. □

What's the upshot of this?

Theorem 0.38. *If R is a Dedekind ring, then any nonzero ideal $I \subset R$ is invertible, and therefore uniquely described as a product of powers of (nonzero) prime ideals, $I = \prod \mathfrak{p}_i^{n_i}$.*

Proof. This is simply because I is in $\mathrm{Cart}(R) = \mathrm{Weil}(R)$ by the above result. □

This is Dedekind's generalization of unique factorization.

We now give the standard examples:

Example 0.39.

1. Any PID is Dedekind.
2. If K is a finite extension of $\mathbb{Q}$, and set R to be the integral closure of $\mathbb{Z}$ in K, then R is a Dedekind ring. The ring of integers in any number field is a Dedekind ring.

3. If R is the coordinate ring of an algebraic variety which is smooth and irreducible of dimension one, then R is Dedekind.

4. Let X be a compact Riemann surface, and let $S \subset X$ be a nonempty finite subset. Then the ring of meromorphic functions on X with poles only in S is Dedekind. The maximal ideals in this ring are precisely those corresponding to points of $X - S$.

Chapter 7

Dimension theory

Today, we'd like to start talking about dimension theory. But first we need a little something else.

0.10 Some definitions

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

Definition 0.40. M is **simple** if $M \neq 0$ and M has no nontrivial submodules.

Definition 0.41. M is **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.

Remark. M is simple iff it is isomorphic $R/\mathfrak{m}$ for $\mathfrak{m} \subset R$ an ideal. Why? Well, it must contain a cyclic submodule generated by $x \in M - \{0\}$. So it must contain a submodule isomorphic to R/I, and simplicity implies that $M \simeq R/I$ for some I. If I is not maximal, then we will get a nontrivial submodule of R/I. Conversely, it's easy to see that $R/\mathfrak{m}$ is simple for $\mathfrak{m}$ maximal.

Proposition 0.42. *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.

Suppose $M \neq 0$ is noetherian and artinian. Let $M_1 \subset M$ be a minimal nonzero submodule, possible by artinianness. 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 minimal M_2 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 hit M. Note that since M is noetherian, we cannot continue this strictly ascending chain forever. □

Proposition 0.43. *In this case, the length of the filtration is well-defined. That is, any two filtrations on M with simple quotients have the same length.*

Definition 0.44. This number is called the **length** of M and is denoted $\ell(M)$.

Proof. Let us introduce a temporary definition: $l(M)$ is the length of the *minimal* filtration on M. A priori, we don't know that $\ell(M)$ makes any sense. **We will show that any filtration 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'd 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 imply that $n = 0, 1$ respectively. So we can assume $l(M) \geq 2$. 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 can replace the filtrations of $M_{n-1}, N_{l(M)-1}$ such that the next term after that is K, because any two filtrations on these proper submodules have the same length. 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.

□

0.11 Introduction to dimension theory

Let R be a ring.

Question. What is a good definition for $\dim(R)$? Actually, more generally, we want the dimension at a point.

Geometrically, think of Spec$R$, for any ring; pick some point corresponding to a maximal ideal $\mathfrak{m} \subset R$. We want to define the **dimension of** R at $\mathfrak{m}$. This is to be thought of kind of like "dimension over the complex numbers," for algebraic varieties defined over $\mathbb{C}$. But it should be purely algebraic.

What might you do?

Here's an idea. For a topological space X to be n-dimensional at $x \in X$, this should mean that there are n coordinates at the point x. The point x is defined by the zero locus of n points on the space.

Definition 0.45 (Proposal)**.** We could try defining $\dim_{\mathfrak{m}} R$ to be the number of gnerators of $\mathfrak{m}$.

This is a bad definition, as $\mathfrak{m}$ may not have the same number of generators as $\mathfrak{m}R_{\mathfrak{m}}$. We want our definition to be local. So this leads us to:

Definition 0.46. If R is a (noetherian) *local* ring with maximal ideal $\mathfrak{m}$, then the **embedding dimension** of R is the minimal number of gnerators for $\mathfrak{m}$.

By Nakayama's lemma, this is the minimal number of gnerators of $\mathfrak{m}/\mathfrak{m}^2$, or the $R/\mathfrak{m}$-dimension of that vector space. However, this isn't going to coincide with the dimension of an algebraic variety.

Example 0.47. Let $R = \mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$, which is the coordinate ring of a cubic curve. Let us localize at the prime ideal $\mathfrak{p} = (t^2, t^3)$: we get $R_{\mathfrak{p}}$.

Now Spec$R$ is singular at the origin. In fact, as a result, $\mathfrak{p}R_{\mathfrak{p}} \subset R_{\mathfrak{p}}$ needs two generators, but the variety it corresponds to is one-dimensional.

So the embedding dimension is the smallest dimension into which you can embed R into a smooth space. But for singular varieties this is not the dimension we want.

Well, we can consider the sequence of finite-dimensional vector spaces

$$\mathfrak{m}^k/\mathfrak{m}^{k+1}.$$

Computing these dimensions gives some invariant that describes the local geometry of Spec$R$.

Example 0.48. Consider the local ring $(R, \mathfrak{m}) = \mathbb{C}[t]_{(t)}$. Then $\mathfrak{m} = (t)$ and $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is one-dimensional, generated by t^k.

Example 0.49. Consider $R = \mathbb{C}[t^2, t^3]_{(t^2,t^3)}$, the local ring of $y^2 = x^3$ at zero. Then $\mathfrak{m}^n$ is generated by $t^{2n}, t^{2n+1}, \ldots$. $\mathfrak{m}^{n+1}$ is generated by $t^{2n+2}, t^{2n+3}, \ldots$. So the quotients all have dimension two. The dimension of these quotients is a little larger than we expected, but they don't grow.

Example 0.50. Consider $R = \mathbb{C}[x, y]_{(x,y)}$. Then $\mathfrak{m}^k$ is generated by polynomials homogeneous in degree k. So $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ has dimensions that *grow* in k. This is a genuinely two-dimensional example.

This is the difference that we want to quantify to be the dimension.

Proposition 0.51. *Let $(R, \mathfrak{m})$ be a local noetherian ring. Then there exists a polynomial $f \in \mathbb{Q}[t]$ such that*

$$\ell(R/\mathfrak{m}^n) = \sum_{i=0}^{n-1} \dim \mathfrak{m}^i/\mathfrak{m}^{i+1} = f(n) \quad \forall n \gg 0.$$

Moreover, $\deg f \leq \dim \mathfrak{m}/\mathfrak{m}^2$.

Note that this polynomial is well-defined, as any two polynomials agreeing for large n coincide. Note also that $R/\mathfrak{m}^n$ is artinian so of finite length, and that we have used the fact that the length is additive for short exact sequences. We would have liked to write $\dim R/\mathfrak{m}^n$, but we can't, in general, so we use the substitute of the length.

Based on this, we define

Definition 0.52. The **dimension** of R is the degree of the polynomial f above.

Example 0.53. Consider $R = \mathbb{C}[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$. What is the polynomial f above? Well, $R/\mathfrak{m}^k$ looks like the set of polynomials of degree $< k$ in $\mathbb{C}$. The dimension as a vector space is given by some binomial coefficient $\binom{n+k-1}{n}$. This is a polynomial in k of degree n. So R is n-dimensional. Which is what we wanted.

Example 0.54. Let R be a DVR. Then $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is of length one for each k. So $R/\mathfrak{m}^k$ has length k. Thus we can take $f(t) = t$ so R has dimension one.

Now we have to prove the proposition, i.e. that there is always such a polynomial.

Proof. Let $S = \bigoplus_n \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Then S has a natural grading, and in fact it is a graded ring in a natural way from the map

$$\mathfrak{m}^{n_1} \times \mathfrak{m}^{n_2} \to \mathfrak{m}^{n_1+n_2}.$$

(It is the associated graded ring of the $\mathfrak{m}$-adic filtration.) Note that $S_0 = R/\mathfrak{m}$ is a field.

Choose n generators $x_1, \ldots, x_n \in \mathfrak{m}$, where n is what we called the embedding dimension of R. So these n generators give generators of S_1 as an S_0-vector space. In fact, they generate S as an S_0-algebra because S is generated by degree one terms over S_0. So S is a graded quotient of the polynomial ring $\kappa[t_1, \ldots, t_n]$ for $\kappa = R/\mathfrak{m}$. Note that $\ell(R/\mathfrak{m}^a) = \dim_\kappa(S_0) + \cdots + \dim_\kappa(S_{a-1})$ for any a, thanks to the filtration.

It will now suffice to prove the following more general proposition.

Proposition 0.55. *Let M be any finitely generated graded module over the polynomial ring $\kappa[x_1, \ldots, x_n]$. Then there exists a polynomial $f_M \in \mathbb{Q}[t]$ of degree $\leq n$, such that*

$$f_M(t) = \sum_{s \leq t} \dim M_s \quad t \gg 0.$$

Applying this to $M = S$ will give the desired result. We can forget about everything else, and look at this problem over graded polynomial rings.

This function is called the **Hilbert function**.

Proof. Note that if we have an exact sequence of gaded modules over the polynomial ring,

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

and $f_{M'}, f_{M''}$ exist as polynomials, then f_M exists and

$$f_M = f_{M'} + f_{M''}.$$

This is obvious from the definitions. We will induct on n.

If $n = 0$, then M is a finite-dimensional graded vector space over κ, and the grading must be concentrated in finitely many degrees. Thus the result is evident as $f_M(t)$ will just equal $\dim M$ (which will be the appropriate dimension for $t \gg 0$).

Suppose $n > 0$. Let x be one of the variables $x_1, \ldots, x_n$. Then consider

$$0 \subset \ker(x : M \to M) \subset \ker(x^2 : M \to M) \subset \ldots.$$

This must stabilize by noetherianness at some $M' \subset M$. Each of the quotients $\ker(x^i)/\ker(x^{i+1})$ is a finitely generated module over $\kappa[x_1, \ldots, x_n]/(x)$, which is a smaller polynomial ring. So each of these subquotients $\ker(x^i)/\ker(x^{i+1})$ has a Hilbert function of degree $\leq n - 1$.

Thus M' has a Hilbert function which is the sum of the Hilbert functions of these subquotients. In particular, $f_{M'}$ exists. If we show that $f_{M/M'}$ exists, then f_M necessarily exists. So we might as well show that the Hilbert function f_M exists when x is a non-zerodivisor on M.

We are out of time, so next time we will finish the proof. □

□

We started last time talking about the dimension theory about local noetherian rings.

0.12 Hilbert polynomials

Last time, we were in the middle of the proof of a lemma.

Suppose $S = k[x_1, \ldots, x_n]$ is a polynomial ring over a field k. It is a graded ring; the m-th graded piece is the set of polynomials homogeneous of degree m. Let M be a finitely generated graded S-module.

Definition 0.56. The **Hilbert function** H_M of M is defined via $H_M(m) = \dim_k M_m$. This is always finite for M a finitely generated graded S-module, as M is a quotient of copies of S (or twisted pieces).

Similarly, we define

$$H_M^+(m) = \sum_{m' \leq m} H_M(m').$$

This measures the dimension of $\deg m$ and below.

What we were proving last time was that:

Proposition 0.57. *There exist polynomials $f_M(t), f_M^+(t) \in \mathbb{Q}[t]$ such that $f_M(t) = H_M(t)$ and $f_M^+(t) = H_M^+(t)$ for sufficiently large t. Moreover, $\deg f_M \leq n - 1, \deg f_M^+ \leq n$.*

In other words, the Hilbert functions eventually become polynomials.

These polynomials don't generally have integer coefficients, but they are close, as they take integer values at large values. In fact, they take integer values everywhere.

Remark. A function $f : \mathbb{Z} \to \mathbb{Z}$ is polynomial iff

$$f(t) = \sum_n c_n \binom{t}{n}, \quad c_n \in \mathbb{Z}.$$

So f is a $\mathbb{Z}$-linear function of binomial coefficients.

Proof. Note that the set $\left\{\binom{t}{n}\right\}$ forms a basis for the set of polynomials, that is $\mathbb{Q}[t]$. It is clear that $f(t)$ can be written as $\sum c_n \binom{t}{n}$ for the $c_n \in \mathbb{Q}$. By looking at the function $\Delta f(t) = f(t) - f(t-1)$ (which takes values in $\mathbb{Z}$) and the fact that $\Delta\binom{t}{n} = \binom{t}{n-1}$, it is easy to see that the $c_n \in \mathbb{Z}$ by induction on the degree. It is also easy to see that the binomial coefficients take values in $\mathbb{Z}$. □

Remark. The same remark applies if f is polynomial and $f(t) \in \mathbb{Z}$ for $t \gg 0$, by the same argument. It follows that $f(t) \in \mathbb{Z}$ for all t.

Let us now prove the proposition.

Proof. I claim, first, that the polynomiality of $H_M(t)$ (for t large) is equivalent to that of $H_M^+(t)$ (for t large). This is because H_M is the successive difference of H_M^+, i.e. $H_M(t) = H_M^+(t) - H_M^+(t-1)$. Similarly

$$H_M^+(t) = \sum_{t' \leq t} H_M(t),$$

and the successive sums of a polynomial form a polynomial.

So if f_M exists as in the proposition, then f_M^+ exists. Let us now show that f_M exists. Moreover, we will show that f_M has degree $\leq n-1$, which will prove the result, since f_M^+ has degree one higher.

Induction on n. When $n = 0$, this is trivial, since $H_M(t) = 0$ for $t \gg 0$. In the general case, we reduced to the case of M having no x_1-torsion. The argument for this reduction can be found in the previous lecture.

So M has a filtration

$$M \supset x_1 M \supset x_1^2 M \supset \dots$$

which is an exhaustive filtration of M in that nothing can be divisible by powers of x_1 over and over, for considerations of degree. Multiplication by x_1 raises the degree by one. This states that $\bigcap x_1^m M = 0$.

Let $N = M/x_1 M \simeq x_1^m M / x_1^{m+1} M$ since $M \xrightarrow{x_1} M$ is injective. Now N is a graded module over $k[x_2, \dots, x_n]$, and by the inductive hypothesis on n So there is a polynomial f_N^+ of degree $\leq n-1$ such that

$$f_N^+(t) = \sum_{t' \leq t} \dim N_{t'}, \quad t \gg 0.$$

Let's look at M_t, which has a finite filtration

$$M_t \supset (x_1 M)_t \supset (x_1^2 M)_t \supset \dots$$

which has successive quotients that are the graded pieces of $N \simeq M/x_1M \simeq x_1M/x_1^2M \simeq \dots$ in dimensions $t, t-1, \dots$. We find that

$$(x_1^2M)_t/(x_1^3M)_t \simeq N_{t-2},$$

for instance. We find that

$$\dim M_t = \dim N_t + \dim N_{t-1} + \dots$$

which implies that $f_M(t)$ exists and coincides with f_N^+. □

0.13 Back to dimension theory

Example 0.58. Let R be a local noetherian ring with maximal ideal $\mathfrak{m}$. Then we have the module $M = \bigoplus \mathfrak{m}_1^k/\mathfrak{m}_1^{k+1}$ over the ring $(R/\mathfrak{m})[x_1, \dots, x_n]$ where $x_1, \dots, x_n$ are generators of $\mathfrak{m}$.

The upshot is that

$$f_M^+(t) = \ell(R/\mathfrak{m}^t), \quad t \gg 0.$$

This is a polynomial of degree $\leq n$.

Definition 0.59. The **dimension** of R is the degree of f_M^+.

Remark. As we have seen, the dimension is at most the number of gnerators of $\mathfrak{m}$. So the dimension is at most the embedding dimension.

Definition 0.60. If R is local noetherian, N a finite R-module, define

$$M = \bigoplus \mathfrak{m}^a N/\mathfrak{m}^{a+1}N,$$

which is a module over the associated graded ring $\bigoplus \mathfrak{m}^a/\mathfrak{m}^{a+1}$, which in turn is a quotient of a polynomial ring. It too has a Hilbert polynomial. We say that the **dimension of** N is the degree of the Hilbert polynomial f_M^+. Evaluated at $t \gg 0$, this gives the length $\ell(N/\mathfrak{m}^tN)$.

Proposition 0.61. $\dim R$ *is the same as* $\dim R/\mathrm{Rad}R$.

I.e., the dimension doesn't change when you kill off nilpotent elements, which is what you would expect, as nilpotents don't affect $\mathrm{Spec}(R)$.

Proof. For this, we need a little more information about Hilbert functions. We thus digress substantially.

Proposition 0.62. *Suppose we have an exact sequence*

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

of gaded modules over a polynomial ring $k[x_1, \dots, x_n]$. *Then*

$$f_M(t) = f_{M'}(t) + f_{M''}(t), \quad f_M^+(t) = f_{M'}^+(t) + f_{M''}^+(t).$$

As a result, $\deg f_M = \max \deg f_{M'}, \deg f_{M''}$.

Proof. The first part is obvious as the dimension is additive on vector spaces. The second part follows because Hilbert functions have nonnegative leading coefficients. □

In particular,

Corollary 0.63. *Say we have an exact sequence*

$$0 \to N' \to N \to N'' \to 0$$

of finite R-modules. Then $\dim N = \max(\dim N', \dim N'')$.

Proof. We have an exact sequence

$$0 \to K \to N/\mathfrak{m}^t N \to N''/\mathfrak{m}^t N'' \to 0$$

where K is the kernel. Here $K = (N' + \mathfrak{m}^t N)/\mathfrak{m}^t N = N'/(N' \cap \mathfrak{m}^t N)$. This is not quite $N'/\mathfrak{m}^t N'$, but it's pretty close. We have a surjection

$$N'/\mathfrak{m}^t N \twoheadrightarrow N'/(N' \cap \mathfrak{m}^t N) = K.$$

In particular,

$$\ell(K) \leq \ell(N'/\mathfrak{m}^t N').$$

On the other hand, we have the Artin-Rees lemma, which gives an inequality in the opposite direction. We have a containment

$$\mathfrak{m}^t N' \subset N' \cap \mathfrak{m}^t N \subset \mathfrak{m}^{t-c} N'$$

for some c. This implies that $\ell(K) \geq \ell(N'/\mathfrak{m}^{t-c} N')$.

Define $M = \bigoplus \mathfrak{m}^t N/\mathfrak{m}^{t+1} N$, and define M', M'' similarly in terms of N', N''. Then we have seen that

$$\boxed{f_M^+(t-c) \leq \ell(K) \leq f_M^+(t).}$$

We also know that the length of K plus the length of $N''/\mathfrak{m}^t N''$ is $f_M^+(t)$, i.e.

$$\ell(K) + f_{M''}^+(t) = f_M^+(t).$$

Now the length of K is a polynomial in t which is pretty similar to $f_{M'}^+$, in that the leading coefficient is the same. So we have an approximate equality $f_{M'}^+(t) + f_{M''}^+(t) \simeq f_M^+(t)$. This implies the result since the degree of f_M^+ is $\dim N$ (and similarly for the others). □

Finally, let us return to the claim about dimension and nilpotents. Let R be a local noetherian ring and $I = \mathrm{Rad}(R)$. Then I is a finite R-module. In particular, I is nilpotent, so $I^n = 0$ for $n \gg 0$. We will show that

$$\dim R/I = \dim R/I^2 = \dots$$

which will imply the result, as eventually the powers become zero.

In particular, we have to show for each k,

$$\dim R/I^k = \dim R/I^{k+1}.$$

There is an exact sequence

$$0 \to I^k/I^{k+1} \to R/I^{k+1} \to R/I^k \to 0.$$

The dimension of these rings is the same thing as the dimensions as R-modules. So we can use this short exact sequence of modules. By the previous result, we are reduced to showing that

$$\dim I^k/I^{k+1} \leq \dim R/I^k.$$

Well, note that I kills I^k/I^{k+1}. In particular, I^k/I^{k+1} is a finitely generated R/I^k-module. There is an exact sequence

$$\bigoplus_N R/I^k \to I^k/I^{k+1} \to 0$$

which implies that $\dim I^k/I^{k+1} \leq \dim \bigoplus_N R/I^k = \dim R/I^k$. □

Example 0.64. Let $\mathfrak{p} \subset \mathbb{C}[x_1, \ldots, x_n]$ and let $R = (\mathbb{C}[x_1, \ldots, x_n]/\mathfrak{p})_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m}$. What is $\dim R$? What does dimension mean for coordinate rings over $\mathbb{C}$?

Recall by the Noether normalization theorem that there exists a polynomial ring $\mathbb{C}[y_1, \ldots, y_m]$ contained in $S = \mathbb{C}[x_1, \ldots, x_n]/\mathfrak{p}$ and S is a finite integral extension over this polynomial ring. We claim that

$$\dim R = m.$$

There is not sufficient time for that today.

Last time, we were talking about the dimension theory of local noetherian rings.

0.14 Recap

Let $(R, \mathfrak{m})$ be a local noetherian ring. Let M be a finitely generated R-module. We defined the **Hilbert polynomial** of M to be the polynomial which evaluates at $t \gg 0$ to $\ell(M/\mathfrak{m}^t M)$. We proved last time that such a polynomial always exists, and called its degree the **dimension of** M. More accurately, we shall start calling it $\dim \operatorname{supp} M$.

Recall that $\operatorname{supp} M = \{\mathfrak{p} : M_{\mathfrak{p}} \neq 0\}$. To make sense of this, we must show:

Proposition 0.65. $\dim M$ *depends only on* $\operatorname{supp} M$.

In fact, we shall show:

Proposition 0.66. $\dim M = \max_{\mathfrak{p} \in \operatorname{supp} M} \dim R/\mathfrak{p}$.

Proof. There is a finite filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_m = M,$$

such that each of the successive quotients is isomorphic to $R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$. But if you have a short exact sequence of modules, the dimension in the middle is the maximum of the dimensions at the two ends. Iterating this, we see that the dimension of M is the sup of the dimension of the successive quotients. But the $\mathfrak{p}_i$'s that occur are all in $\mathrm{supp} M$, so we find

$$\dim M = \max_{\mathfrak{p}_i} R/\mathfrak{p}_i \leq \max_{\mathfrak{p} \in \mathrm{supp} M} \dim R/\mathfrak{p}.$$

We must show the reverse inequality. But fix any prime $\mathfrak{p} \in \mathrm{supp} M$. Then $M_{\mathfrak{p}} \neq 0$, so one of the $R/\mathfrak{p}_i$ localized at $\mathfrak{p}$ must be nonzero, as localization is an exact functor. Thus $\mathfrak{p}$ must contain some $\mathfrak{p}_i$. So $R/\mathfrak{p}$ is a quotient of $R/\mathfrak{p}_i$. In particular,

$$\dim R/\mathfrak{p} \leq \dim R/\mathfrak{p}_i.$$

□

Having proved this, we throw out the notation $\dim M$, and henceforth write instead $\dim \mathrm{supp} M$.

0.15 The dimension of an affine ring

Last time, we made a claim. If R is a domain and a finite module over a polynomial ring $k[x_1, \ldots, x_n]$, then $R_{\mathfrak{m}}$ for any maximal $\mathfrak{m} \subset R$ has dimension n. This connects the dimension with the transcendence degree.

First, let us talk about finite extensions of rings. Let R be a commutative ring and let $R \to R'$ be a morphism that makes R' a finitely generated R-module (in particular, integral over R). Let $\mathfrak{m}' \subset R'$ be maximal. Let $\mathfrak{m}$ be the pull-back to R, which is also maximal (as $R \to R'$ is integral). Let M be a finitely generated R'-module, hence also a finitely generated R-module.

We can look at $M_{\mathfrak{m}}$ as an $R_{\mathfrak{m}}$-module or $M_{\mathfrak{m}'}$ as an $R'_{\mathfrak{m}'}$-module. Either of these will be finitely generated.

Proposition 0.67. $\dim \mathrm{supp} M_{\mathfrak{m}} \geq \dim \mathrm{supp} M_{\mathfrak{m}'}$.

Here $M_{\mathfrak{m}}$ is an $R_{\mathfrak{m}}$-module, $M_{\mathfrak{m}'}$ is an $R'_{\mathfrak{m}'}$-module.

Proof. Consider $R/\mathfrak{m} \to R'/\mathfrak{m}R' \to R'/\mathfrak{m}'$. Then we see that $R'/\mathfrak{m}R'$ is a finite $R/\mathfrak{m}$-module, so a finite-dimensional $R/\mathfrak{m}$-vector space. In particular, $R'/\mathfrak{m}R'$ is of finite length as an $R/\mathfrak{m}$-module, in particular an artinian ring. It is thus a product of local artinian rings. These artinian rings are the localizations of $R'/\mathfrak{m}R'$ at ideals of R' lying over $\mathfrak{m}$. One of these ideals is $\mathfrak{m}'$. So in particular

$$R'/\mathfrak{m}R \simeq R'/\mathfrak{m}' \times \text{other factors}.$$

The nilradical of an artinian ring being nilpotent, we see that $\mathfrak{m}'^c R'_{\mathfrak{m}'} \subset \mathfrak{m} R'_{\mathfrak{m}}$ for some c.

OK, I'm not following this—too tired. Will pick this up someday. □

Proposition 0.68. $\dim \operatorname{supp} M_{\mathfrak{m}} = \max_{\mathfrak{m}'|\mathfrak{m}} \dim \operatorname{supp} M_{\mathfrak{m}'}$.

This means $\mathfrak{m}'$ lies over $\mathfrak{m}$.

Proof. Done similarly, using artinian techniques. I'm kind of tired. □

Example 0.69. Let $R' = \mathbb{C}[x_1, \dots, x_n]/\mathfrak{p}$. Noether normalization says that there exists a finite injective map $\mathbb{C}[y_1, \dots, y_a] \to R'$. The claim is that

$$\dim R'_{\mathfrak{m}} = a$$

for any maximal ideal $\mathfrak{m} \subset R'$. We are set up to prove a slightly weaker definition. In particular (see below for the definition of the dimension of a non-local ring), by the proposition, we find the weaker claim

$$\dim R' = a,$$

as the dimension of a polynomial ring $\mathbb{C}[y_1, \dots, y_a]$ is a. (**I don't think we have proved this yet.**)

0.16 Dimension in general

Definition 0.70. If R is a noetherian ring, we define $\dim(R) = \sup_{\mathfrak{p}} R_{\mathfrak{p}}$ for $\mathfrak{p} \in \operatorname{Spec}(R)$ maximal. This may be infinite. The localizations can grow arbitrarily large in dimension, but these examples are kind of pathological.

0.17 A topological characterization

We now want a topological characterization of dimension. So, first, we want to study how dimension changes as we do things to a module. Let M be a finitely generated R-module over a local noetherian ring R. Let $x \in \mathfrak{m}$ for $\mathfrak{m}$ as the maximal ideal. You might ask

What is the relation between $\dim \operatorname{supp} M$ and $\dim \operatorname{supp} M/xM$?

Well, M surjects onto M/xM, so we have the inequality $\geq$. But we think of dimension as describing the number of parameters you need to describe something. The number of parameters shouldn't change too much with going from M to M/xM. Indeed, as one can check,

$$\operatorname{supp} M/xM = \operatorname{supp} M \cap V(x)$$

and intersecting $\operatorname{supp} M$ with the "hypersurface" $V(x)$ should shrink the dimension by one.

We thus make:

Prediction.

$$\dim \operatorname{supp} M/xM = \dim \operatorname{supp} M - 1.$$

Obviously this is not always true, e.g. if x acts by zero on M. But we want to rule that out. Under reasonable cases, in fact, the prediction is correct:

Proposition 0.71. *Suppose $x \in \mathfrak{m}$ is a nonzerodivisor on M. Then*

$$\dim \operatorname{supp} M/xM = \dim \operatorname{supp} M - 1.$$

Proof. To see this, we look at Hilbert polynomials. Let us consider the exact sequence

$$0 \to xM \to M \to M/xM \to 0$$

which leads to an exact sequence for each t,

$$0 \to xM/(xM \cap \mathfrak{m}^t M) \to M/\mathfrak{m}^t M \to M/(xM + \mathfrak{m}^t M) \to 0.$$

For t large, the lengths of these things are given by Hilbert polynomials, as the thing on the right is $M/xM \otimes_R R/\mathfrak{m}^t$. We have

$$f_M^+(t) = f_{M/xM}^+(t) + \ell(xM/(xM \cap \mathfrak{m}^t M), \quad t \gg 0.$$

In particular, $\ell(xM/(xM \cap \mathfrak{m}^t M))$ is a polynomial in t. What can we say about it? Well, $xM \simeq M$ as x is a nonzerodivisor. In particular

$$xM/(xM \cap \mathfrak{m}^t M) \simeq M/N_t$$

where

$$N_t = \left\{a \in M : xa \in \mathfrak{m}^t M\right\}.$$

In particular, $N_t \supset \mathfrak{m}^{t-1} M$. This tells us that $\ell(M/N_t) \leq \ell(M/\mathfrak{m}^{t-1}M) = f_M^+(t-1)$ for $t \gg 0$. Combining this with the above information, we learn that

$$f_M^+(t) \leq f_{M/xM}^+(t) + f_M^+(t-1),$$

which implies that $f_{M/xM}^+(t)$ is at least the successive difference $f_M^+(t) - f_M^+(t-1)$. This last polynomial has degree $\dim \operatorname{supp} M - 1$. In particular, $f_{M/xM}^+(t)$ has degree at least $\dim \operatorname{supp} M - 1$. This gives us one direction, actually the hard one. We showed that intersecting something with codimension one doesn't drive the dimension down too much.

Let us now do the other direction. We essentially did this last time via the Artin-Rees lemma. We know that $N_t = \left\{a \in M : xa \in \mathfrak{m}^t\right\}$. The Artin-Rees lemma tells us that there is a constant c such that $N_{t+c} \subset \mathfrak{m}^t M$ for all t. Therefore, $\ell(M/N_{t+c}) \geq \ell(M/\mathfrak{m}^t M) = f_M^+(t), t \gg 0$. Now remember the exact sequence $0 \to M/N_t \to M/\mathfrak{m}^t M \to M/(xM + \mathfrak{m}^t M) \to 0$. We see from this that

$$\ell(M/\mathfrak{m}^t M) = \ell(M/N_t) + f_{M/xM}^+(t) \geq f_M^+(t-c) + f_{M/xM}^+(t), \quad t \gg 0,$$

which implies that

$$f_{M/xM}^+(t) \leq f_M^+(t) - f_M^+(t-c),$$

so the degree must go down. And we find that $\deg f_{M/xM}^+ < \deg f_M^+$. □

This gives us an algorithm of computing the dimension of an R-module M. First, it reduces to computing $\dim R/\mathfrak{p}$ for $\mathfrak{p} \subset R$ a prime ideal. We may assume that R is a domain and that we are looking for $\dim R$. Geometrically, this corresponds to taking an irreducible component of $\mathrm{Spec}R$.

Now choose any $x \in R$ such that x is nonzero but noninvertible. If there is no such element, then R is a field and has dimension zero. Then compute $\dim R/x$ (recursively) and add one.

Notice that this algorithm said nothing about Hilbert polynomials, and only talked about the structure of prime ideals.

0.18 Recap

Last time, we were talking about dimension theory. Recall that R is a local noetherian ring with maximal ideal $\mathfrak{m}$, M a finitely generated R-module. We can look at the lengths $\ell(M/\mathfrak{m}^t M)$ for varying t; for $t \gg 0$ this is a polynomial function. The degree of this polynomial is called the **dimension** of $\mathrm{supp}M$.

Remark. If $M = 0$, then we define $\dim \mathrm{supp}M = -1$ by convention.

Last time, we showed that if $M \neq 0$ and $x \in \mathfrak{m}$ such that x is a nonzerodivisor on M (i.e. $M \xrightarrow{x} M$ injective), then

$$\boxed{\dim \mathrm{supp}M/xM = \dim \mathrm{supp}M - 1.}$$

Using this, we could give a recursion for calculating the dimension. To compute $\dim R = \dim \mathrm{Spec}R$, we note three properties:

1. $\dim R = \sup_{\mathfrak{p} \text{ a minimal prime}} R/\mathfrak{p}$. Intuitively, this says that a variety which is the union of irreducible components has dimension equal to the maximum of these irreducibles.

2. $\dim R = 0$ for R a field. This is obvious from the definitions.

3. If R is a domain, and $x \in \mathfrak{m} - \{0\}$, then $\dim R/(x) + 1 = \dim R$. This is obvious from the boxed formula as x is a nonzerodivisor.

These three properties *uniquely characterize* the dimension invariant.

More precisely, if $d : \{\text{local noetherian rings}\} \to \mathbb{Z}_{\geq 0}$ **satisfies the above three properties, then** $d = \dim$**.**

Proof. Induction on $\dim R$. It is clearly sufficient to prove this for R a domain. If R is a field, then it's clear; if $\dim R > 0$, the third condition lets us reduce to a case covered by the inductive hypothesis (i.e. go down). □

Let us rephrase 3 above:

3': If R is a domain and not a field, then

$$\dim R = \sup_{x \in \mathfrak{m} - 0} \dim R/(x) + 1.$$

Obviously 3' implies 3, and it is clear by the same argument that 1,2, 3' characterize the notion of dimension.

0.19 Another notion of dimension

We shall now define another notion of dimension, and show that it is equivalent to the older one by showing that it satisfies these axioms.

Definition 0.72. Let R be a commutative ring. A **chain of prime ideals** in R is a finite sequence

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

This chain is said to have **length** n**.**

Definition 0.73. The **Krull dimension** of R is equal to the maximum length of any chain of prime ideals. This might be ∞, but we will soon see this cannot happen for R local and noetherian.

Remark. For any maximal chain $\{\mathfrak{p}_i, 0 \leq i \leq n\}$ of primes (i.e. which can't be expanded), we must have that $\mathfrak{p}_0$ is minimal prime and $\mathfrak{p}_n$ a maximal ideal.

Theorem 0.74. *For a noetherian local ring R, the Krull dimension of R exists and is equal to the usual* $\dim R$*.*

Proof. We will show that the Krull dimension satisfies the above axioms. For now, write Krdim for Krull dimension.

1. First, note that $\mathrm{Krdim}(R) = \max_{\mathfrak{p} \in R \text{ minimal}} \mathrm{Krdim}(R/\mathfrak{p})$. This is because any chain of prime ideals in R contains a minimal prime. So any chain of prime ideals in R can be viewed as a chain in *some* $R/\mathfrak{p}$, and conversely.

2. Second, we need to check that $\mathrm{Krdim}(R) = 0$ for R a field. This is obvious, as there is precisely one prime ideal.

3. The third condition is interesting. We must check that for $(R, \mathfrak{m})$ a local domain,
$$\mathrm{Krdim}(R) = \max_{x \in \mathfrak{m} - \{0\}} \mathrm{Krdim}(R/(x)) + 1.$$
If we prove this, we will have shown that condition 3' is satisfied by the Krull dimension. It will follow by the inductive argument above that $\mathrm{Krdim}(R) = \dim(R)$ for any R. There are two inequalities to prove. First, we must show
$$\mathrm{Krdim}(R) \geq \mathrm{Krdim}(R/x) + 1, \quad \forall x \in \mathfrak{m} - 0.$$
So suppose $k = \mathrm{Krdim}(R/x)$. We want to show that there is a chain of prime ideals of length $k+1$ in R. So say $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k$ is a chain of length k in $R/(x)$. The inverse images in R give a proper chain of primes in R of length k, all of which contain (x) and thus properly contain 0. Thus adding zero will give a chain of primes in R of length $k+1$.

   Conversely, we want to show that if there is a chain of primes in R of length $k+1$, then there is a chain of length k in $R/(x)$ for some $x \in \mathfrak{m} - \{0\}$. Let us write the chain of length $k+1$:
$$\mathfrak{q}_{-1} \subset \mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_k \subset R.$$

Now evidently $\mathfrak{q}_0$ contains some $x \in \mathfrak{m} - 0$. Then the chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_k$ can be identified with a chain in $R/(x)$ for this x. So for this x, we have that $\mathrm{Krdim} R \leq \sup \mathrm{Krdim} R/(x) + 1$.

□

There is thus a combinatorial definition of definition.

Remark. Geometrically, let $X = \mathrm{Spec} R$ for R an affine ring over $\mathbb{C}$ (a polynomial ring mod some ideal). Then R has Krull dimension $\geq k$ iff there is a chain of irreducible subvarieties of X,

$$X_0 \supset X_1 \supset \cdots \supset X_k.$$

Remark (**Warning!**). Let R be a local noetherian ring of dimension k. This means that there is a chain of prime ideals of length k, and no longer chains. Thus there is a maximal chain whose length is k. However, not all maximal chains in $\mathrm{Spec} R$ have length k.

Example 0.75. Let $R = (\mathbb{C}[X, Y, Z]/(XY, XZ))_{(X,Y,Z)}$. It is left as an exercise to the reader to see that there are maximal chains of length not two.

There are more complicated local noetherian *domains* which have maximal chains of prime ideals not of the same length. These examples are not what you would encounter in daily experience, and are necessarily complicated. This cannot happen for finitely generated domains over a field.

Example 0.76. An easier way all maximal chains could fail to be of the same length is if $\mathrm{Spec} R$ has two components (in which case $R = R_0 \times R_1$ for rings R_0, R_1).

0.20 Yet another definition

Let's start by thinking about the definition of a module. Recall that if $(R, \mathfrak{m})$ is a local noetherian ring and M a finitely generated R-module, and $x \in \mathfrak{m}$ is a nonzerodivisor on M, then

$$\dim \mathrm{supp} M/xM = \dim \mathrm{supp} M - 1.$$

Question. What if x is a zerodivisor?

This is not necessarily true (e.g. if $x \in \mathrm{Ann}(M)$). Nonetheless, we claim that even in this case:

Proposition 0.77. *For any $x \in \mathfrak{m}$,*

$$\boxed{\dim \mathrm{supp} M \geq \dim \mathrm{supp} M/xM \geq \dim \mathrm{supp} M - 1.}$$

The upper bound on $\dim M/xM$ is obvious as M/xM is a quotient of M. The lower bound is trickier.

Proof. Let $N = \{a \in M : x^n a = 0 \text{ for some } n\}$. We can construct an exact sequence

$$0 \to N \to M \to M/N \to 0.$$

Let $M'' = M/N$. Now x is a nonzerodivisor on M/N by construction. We claim that

$$0 \to N/xN \to M/xM \to M''/xM'' \to 0$$

is exact as well. For this we only need to see exactness at the beginning, i.e. injectivity of $N/xN \to M/xM$. So we need to show that if $a \in N$ and $a \in xM$, then $a \in xN$.

To see this, suppose $a = xb$ where $b \in M$. Then if $\phi : M \to M''$, then $\phi(b) \in M''$ is killed by x as $x\phi(b) = \phi(bx) = \phi(a)$. This means that $\phi(b) = 0$ as $M'' \xrightarrow{x} M''$ is injective. Thus $b \in N$ in fact. So $a \in xN$ in fact.

From the exactness, we see that (as x is a nonzerodivisor on M'')

$$\begin{aligned}\dim M/xM &= \max(\dim M''/xM'', \dim N/xN) \geq \max(\dim M'' - 1, \dim N) \\ &\geq \max(\dim M'', \dim N) - 1.\end{aligned}$$

The reason for the last claim is that $\mathrm{supp}N/xN = \mathrm{supp}N$ as N is x-torsion, and the dimension depends only on the support. But the thing on the right is just $\dim M - 1$. □

As a result, we find:

Proposition 0.78. $\dim \mathrm{supp}M$ *is the minimal integer n such that there exist elements $x_1, \dots, x_n \in \mathfrak{m}$ with $M/(x_1, \dots, x_n)M$ has finite length.*

Note that n always exists, since we can look at a bunch of gnerators of the maximal ideal, and $M/\mathfrak{m}M$ is a finite-dimensional vector space and is thus of finite length.

Proof. Induction on $\dim \mathrm{supp}M$. Note that $\dim \mathrm{supp}(M) = 0$ if and only if the Hilbert polynomial has degree zero, i.e. M has finite length or that $n = 0$ (n being defined as in the statement).

Suppose $\dim \mathrm{supp}M > 0$.

1. We first show that there are $x_1, \dots, x_{\dim M}$ with $M/(x_1, \dots, x_{\dim M})M$ have finite length. Let $M' \subset M$ be the maximal submodule having finite length. There is an exact sequence

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

   where $M'' = M/M'$ has no finite length submodules. In this case, we can basically ignore M', and replace M by M''. The reason is that modding out by M' doesn't affect either n or the dimension.

   So let us replace M with M'' and thereby assume that M has no finite length submodules. In particular, M does not contain a copy of $R/\mathfrak{m}$, i.e. $\mathfrak{m} \notin$

$\mathrm{Ass}(M)$. By prime avoidance, this means that there is $x_1 \in \mathfrak{m}$ that acts as a nonzerodivisor on M. Thus

$$\dim M/x_1M = \dim M - 1.$$

The inductive hypothesis says that there are $x_2, \ldots, x_{\dim M}$ with

$$(M/x_1M)/(x_2, \ldots, x_{\dim M})(M/xM) \simeq M/(x_1, \ldots, x_{\dim M})M$$

of finite length. This shows the claim.

2. Conversely, suppose that there $M/(x_1, \ldots, x_n)M$ has finite length. Then we claim that $n \geq \dim M$. This follows because we had the previous result that modding out by a single element can chop off the dimension by at most 1. Recursively applying this, and using the fact that dim of a finite length module is zero, we find

$$0 = \dim M/(x_1, \ldots, x_n)M \geq \dim M - n.$$

□

Corollary 0.79. *Let $(R, \mathfrak{m})$ be a local noetherian ring. Then $\dim R$ is equal to the minimal n such that there exist $x_1, \ldots, x_n \in R$ with $R/(x_1, \ldots, x_n)R$ is artinian. Or, equivalently, such that $(x_1, \ldots, x_n)$ contains a power of $\mathfrak{m}$.*

Remark. We manifestly have here that the dimension of R is at most the embedding dimension. Here, we're not worried about generating the maximal ideal, but simply something containing a power of it.

We have been talking about dimension. Let R be a local noetherian ring with maximal ideal $\mathfrak{m}$. Then, as we have said in previous lectures, $\dim R$ can be characterized by:

1. The minimal n such that there is an n-primary ideal generated by n elements $x_1, \ldots, x_n \in \mathfrak{m}$. That is, the closed point $\mathfrak{m}$ of $\mathrm{Spec}R$ is cut out *set-theoretically* by the intersection $\bigcap V(x_i)$. This is one way of saying that the closed point can be defined by n parameters.

2. The *maximal* n such that there exists a chain of prime ideals

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n.$$

3. The degree of the Hilbert polynomial $f^+(t)$, which equals $\ell(R/\mathfrak{m}^t)$ for $t \gg 0$.

0.21 Consequences of the notion of dimension

Let R be a local noetherian ring. The following is now clear from what we have shown:

Theorem 0.80 (Krull's Hauptidealsatz)**.** *R has dimension 1 if and only if there is a nonzerodivisor $x \in \mathfrak{m}$ such that $R/(x)$ is artinian.*

Remark. Let R be a domain. We said that a nonzero prime $\mathfrak{p} \subset R$ is **height one** if $\mathfrak{p}$ is minimal among the prime ideals containing some nonzero $x \in R$.

According to Krull's Hauptidealsatz, $\mathfrak{p}$ has height one **if and only if** $\dim R_{\mathfrak{p}} = 1$**.**

We can generalize the notion of $\mathfrak{p}$ as follows.

Definition 0.81. Let R be a noetherian ring (not necessarily local), and $\mathfrak{p} \in \mathrm{Spec}R$. Then we define the **height** of $\mathfrak{p}$, denoted height($\mathfrak{p}$), as $\dim R_{\mathfrak{p}}$. We know that this is the length of a maximal chain of primes in $R_{\mathfrak{p}}$. This is thus the maximal length of prime ideals of R,

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$

that ends in $\mathfrak{p}$. This is the origin of the term "height."

Remark. Sometimes, the height is called the **codimension**. This corresponds to the codimension in Spec$R$ of the corresponding irreducible closed subset of Spec$R$.

0.22 Further remarks

We can recast earlier notions in terms of dimension.

Remark. A noetherian ring has dimension zero if and only if R is artinian. Indeed, R has dimension zero iff all primes are maximal.

Remark. A noetherian domain has dimension zero iff it is a field. Indeed, in this case (0) is maximal.

Remark. R has dimension ≤ 1 if and only if every non-minimal prime of R is maximal. That is, there are no chains of length ≥ 2.

Remark. A (noetherian) domain R has dimension ≤ 1 iff every nonzero prime ideal is maximal.

In particular,

Proposition 0.82. *R is Dedekind iff it is a noetherian, integrally closed domain of dimension 1.*

0.23 Change of rings

Let $f : R \to R'$ be a map of noetherian rings.

Question. What is the relationship between $\dim R$ and $\dim R'$?

A map f gives a map $\mathrm{Spec}R' \to \mathrm{Spec}R$, where $\mathrm{Spec}R'$ is the union of various fibers over the points of $\mathrm{Spec}R$. You might imagine that the dimension is the dimension of R plus the fiber dimension. This is sometimes true.

Now assume that R, R' are *local* with maximal ideals $\mathfrak{m}, \mathfrak{m}'$. Assume furthermore that f is local, i.e. $f(\mathfrak{m}) \subset \mathfrak{m}'$.

Theorem 0.83. $\dim R' \leq \dim R + \dim R'/\mathfrak{m}R'$. *Equality holds if $f : R \to R'$ is flat.*

Here $R'/\mathfrak{m}R'$ is to be interpreted as the "fiber" of $\mathrm{Spec}R'$ above $\mathfrak{m} \in \mathrm{Spec}R$. The fibers can behave weirdly as the basepoint varies in $\mathrm{Spec}R$, so we can't expect equality in general.

Remark. Let us review flatness as it has been a while. An R-module M is *flat* iff the operation of tensoring with M is an exact functor. The map $f : R \to R'$ is *flat* iff R' is a flat R-module. Since the construction of taking fibers is a tensor product (i.e. $R'/\mathfrak{m}R' = R' \otimes_R R/\mathfrak{m}$), perhaps the condition of flatness here is not as surprising as it might be.

Proof. Let us first prove the inequality. Say

$$\dim R = a,\ \dim R'/\mathfrak{m}R' = b.$$

We'd like to see that

$$\dim R' \leq a + b.$$

To do this, we need to find $a + b$ elements in the maximal ideal $\mathfrak{m}'$ that generate a $\mathfrak{m}'$-primary ideal of R'.

There are elements $x_1, \ldots, x_a \in \mathfrak{m}$ that generate an $\mathfrak{m}$-primary ideal $I = (x_1, \ldots, x_a)$ in R. There is a surjection $R'/IR' \twoheadrightarrow R'/\mathfrak{m}R'$. The kernel $\mathfrak{m}R'/IR'$ is nilpotent since I contains a power of $\mathfrak{m}$. We've seen that nilpotents *don't* affect the dimension. In particular,

$$\dim R'/IR' = \dim R'/\mathfrak{m}R' = b.$$

There are thus elements $y_1, \ldots, y_b \in \mathfrak{m}'/IR'$ such that the ideal $J = (y_1, \ldots, y_b) \subset R'/IR'$ is $\mathfrak{m}'/IR'$-primary. The inverse image of J in R', call it $\overline{J} \subset R'$, is $\mathfrak{m}'$-primary. However, $\overline{J}$ is generated by the $a + b$ elements

$$f(x_1), \ldots, f(x_a), \overline{y_1}, \ldots, \overline{y_b}$$

if the $\overline{y_i}$ lift y_i.

But we don't always have equality. Nonetheless, if all the fibers are similar, then we should expect that the dimension of the "total space" $\mathrm{Spec}R'$ is the dimension

of the "base" Spec$R$ plus the "fiber" dimension Spec$R'/\mathfrak{m}R'$. *The precise condition of f flat articulates the condition that the fibers "behave well."* Why this is so is something of a mystery, for now. But for some evidence, take the present result about fiber dimension.

Anyway, let us now prove equality for flat R-algebras. As before, write $a = \dim R, b = \dim R'/\mathfrak{m}R'$. We'd like to show that

$$\dim R' \geq a + b.$$

By what has been shown, this will be enough. This is going to be tricky since we now need to give *lower bounds* on the dimension; finding a sequence $x_1, \dots, x_{a+b}$ such that the quotient $R/(x_1, \dots, x_{a+b})$ is artinian would bound *above* the dimension.

So our strategy will be to find a chain of primes of length $a + b$. Well, first we know that there are primes

$$\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_b \subset R'/\mathfrak{m}R'.$$

Let $\overline{\mathfrak{q}_i}$ be the inverse images in R'. Then the $\overline{\mathfrak{q}_i}$ are a strictly ascending chain of primes in R' where $\overline{\mathfrak{q}_0}$ contains $\mathfrak{m}R'$. So we have a chain of length b; we need to extend this by additional terms.

Now $f^{-1}(\overline{\mathfrak{q}_0})$ contains $\mathfrak{m}$, hence is $\mathfrak{m}$. Since $\dim R = a$, there is a chain $\{\mathfrak{p}_i\}$ of prime ideals of length a going down from $f^{-1}(\overline{\mathfrak{q}_0}) = \mathfrak{m}$. We are now going to find primes $\mathfrak{p}_i' \subset R'$ forming a chain such that $f^{-1}(\mathfrak{p}_i') = \mathfrak{p}_i$. In other words, we are going to *lift* the chain $\mathfrak{p}_i$ to SpecR'. We can do this at the first stage for $i = a$, where $\mathfrak{p}_a = \mathfrak{m}$ and we can set $\mathfrak{p}_a' = \overline{\mathfrak{q}_0}$. If we can indeed do this lifting, and catenate the chains $\overline{\mathfrak{q}_j}, \mathfrak{p}_i'$, then we will have a chain of the appropriate length.

We will proceed by descending induction. Assume that we have $\mathfrak{p}_{i+1}' \subset R'$ and $f^{-1}(\mathfrak{p}_{i+1}') = \mathfrak{p}_{i+1} \subset R$. We want to find $\mathfrak{p}_i' \subset \mathfrak{p}_{i+1}'$ such that $f^{-1}(\mathfrak{p}_i') = \mathfrak{p}_i$. The existence of that prime is a consequence of the following general fact.

Theorem 0.84 (Going down)**.** *Let $f : R \to R'$ be a flat map of noetherian commutative rings. Suppose $\mathfrak{q} \in$ SpecR', and let $\mathfrak{p} = f^{-1}(\mathfrak{q})$. Suppose $\mathfrak{p}_0 \subset \mathfrak{p}$ is a prime of R. Then there is a prime $\mathfrak{q}_0 \subset \mathfrak{q}$ with*

$$f^{-1}(\mathfrak{q}_0) = \mathfrak{p}_0.$$

Proof. We may replace R' with $R'_{\mathfrak{q}}$. There is still a map

$$R \to R'_{\mathfrak{q}}$$

which is flat as localization is flat. The maximal ideal in $R'_{\mathfrak{q}}$ has inverse image $\mathfrak{p}$. So the problem now reduces to finding *some* $\mathfrak{p}_0$ in the localization that pulls back appropriately.

Anyhow, throwing out the old R and replacing with the localization, we may assume that R' is local and $\mathfrak{q}$ the maximal ideal. (The condition $\mathfrak{q}_0 \subset \mathfrak{q}$ is now automatic.)

The claim now is that we can replace R with $R/\mathfrak{p}_0$ and R' with $R'/\mathfrak{p}_0R' = R' \otimes R/\mathfrak{p}_0$. We can do this because base change preserves flatness (see below), and

in this case we can reduce to the case of $\mathfrak{p}_0 = (0)$—in particular, R is a domain. Taking these quotients just replaces $\mathrm{Spec} R, \mathrm{Spec} R'$ with closed subsets where all the action happens anyhow.

Under these replacements, we now have:

1. R' is local with maximal ideal $\mathfrak{q}$
2. R is a domain and $\mathfrak{p}_0 = (0)$.

We want a prime of R' that pulls back to (0) in R. I claim that any minimal prime of R' will work. Suppose otherwise. Let $\mathfrak{q}_0 \subset R'$ be a minimal prime, and suppose $x \in R \cap f^{-1}(\mathfrak{q}_0) - \{0\}$. But $\mathfrak{q}_0 \in \mathrm{Ass}(R')$. So $f(x)$ is a zerodivisor on R'. Thus multiplication by x on R' is not injective.

But, R is a domain, so $R \xrightarrow{x} R$ is injective. Tensoring with R' must preserve this, implying that $R' \xrightarrow{x} R'$ is injective because R' is flat. This is a contradiction. □

We used:

Lemma 0.85. *Let $R \to R'$ be a flat map, and S an R-algebra. Then $S \to S \otimes_R R'$ is a flat map.*

Proof. The construction of taking an S-module with $S \otimes_R R'$ is an exact functor, because that's the same thing as taking an S-module, restricting to R, and tensoring with R'. □

The proof of the fiber dimension theorem is now complete.

□

We are done with the syllabus, and will now do "bonus" material.

Chapter 8

GNU Free Documentation License

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1 APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms

of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The **"Document"**, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as **"you"**. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A **"Modified Version"** of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A **"Secondary Section"** is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The **"Invariant Sections"** are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The **"Cover Texts"** are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A **"Transparent"** copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called **"Opaque"**.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The **"Title Page"** means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section **"Entitled XYZ"** means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as **"Acknowledgements"**, **"Dedications"**, **"Endorsements"**, or **"History"**.) To **"Preserve the Title"** of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2 VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3 COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4 MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the

Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5 COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6 COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7 AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is

called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8 TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9 TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10 FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

11 ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright ©YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.