Contents

Chapter 8
Unique factorization and the class group

Commutative rings in general do not admit unique factorization. Nonetheless, for many rings ("integrally closed" rings), which includes the affine coordinate rings one obtains in algebraic geometry when one studies smooth varieties, there is an invariant called the "class group" that measures the failure of unique factorization. This "class group" is a certain quotient of codimension one primes (geometrically, codimension one subvarieties) modulo rational equivalence.

Many even nicer rings have the convenient property that their localizations at prime ideals *factorial*, a key example being the coordinate ring of an affine nonsingular variety. For these even nicer rings, an alternative method of defining the class group can be given: the class group corresponds to the group of isomorphism classes of *invertible modules*. Geometrically, such invertible modules are line bundles on the associated variety (or scheme).

§1 Unique factorization

1.1 Definition

We begin with the nicest of all possible cases, when the ring itself admits unique factorization.

Let R be a domain.

Definition 1.1 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 $x \mid b$.

We restate the earlier **??** slightly.

Definition 1.2 A domain R is **factorial** (or a **unique factorization domain**, or a **UFD**) if every nonzero noninvertible element $x \in R$ factors as a product $x_1 \dots x_n$ where each x_i is prime.

Recall that a *principal ideal domain* is a UFD (**??**), as is a *euclidean* domain (**??**); actually, a euclidean domain is a PID. Previously, we imposed something seemingly slightly stronger: that the factorization be unique. We next show that we get that for free.

Proposition 1.3 (The fundamental theorem of arithmetic) *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 1.4 $\mathbb{Z}$ is factorial. This is the fundamental theorem of arithmetic, and follows because $\mathbb{Z}$ is a euclidean domain. The same observation applies to a polynomial ring over a field by **??**.

1.2 Gauss's lemma

We now show that factorial rings are closed under the operation of forming polynomial rings.

Theorem 1.5 (Gauss's lemma) *If R is factorial, so is the polynomial ring $R[X]$.*

In general, if R is a PID, $R[X]$ will *not* be a PID. For instance, $\mathbb{Z}[X]$ is not a PID: the prime ideal $(2, X)$ is not principal.

Proof. In the course of this proof, we shall identify the prime elements in $R[X]$. We start with a lemma that allows us to compare factorizations in $K[X]$ (for K the quotient field) and $R[X]$; the advantage is that we already know the polynomial ring over a *field* to be a UFD.

Lemma 1.6 *Suppose R is a unique factorization domain with quotient field K. Suppose $f \in R[X]$ is irreducible in $R[X]$ and there is no nontrivial common divisor of the coefficients of f. Then f is irreducible in $K[X]$.*

With this in mind, we say that a polynomial in $R[X]$ is **primitive** if the coefficients have no common divisor in R.

Proof. Indeed, suppose we had a factorization

$$f = gh, \quad g, h \in K[X],$$

where g, h have degree ≥ 1. Then we can clear denominators to find a factorization

$$rf = g'h'$$

where $r \in R - \{0\}$ and $g', h' \in R[X]$. By clearing denominators as little as possible, we may assume that g', h' are primitive. To be precise, we divide g', h' by their *contents.* Let us define:

Definition 1.7 The **content** $\mathrm{Cont}(f)$ of a polynomial $f \in R[X]$ is the greatest common divisor of its coefficients. The content of an element f in $K[X]$ is defined by considering $r \in R$ such that $rf \in R[X]$, and taking $\mathrm{Cont}(rf)/r$. This is well-defined, modulo elements of R^*, and we have $\mathrm{Cont}(sf) = s \,\mathrm{Cont}\, f$ if $s \in K$.

To say that the content lies in R is to say that the polynomial is in $R[X]$; to say that the content is a unit is to say that the polynomial is primitive. Note that a monic polynomial in $R[X]$ is primitive.

So we have:

Lemma 1.8 *Any element of $K[X]$ is a product of* $\mathrm{Cont}(f)$ *and something primitive in $R[X]$.*

Proof. Indeed, $f/\mathrm{Cont}(f)$ has content a unit. It therefore cannot have anything in the denominator. Indeed, if it had a term r/p^iX^n where $r, p \in R$ and $p \nmid r$ is prime, then the content would divide r/p^i. It thus could not be in R. ▲

Lemma 1.9 $\mathrm{Cont}(fg) = \mathrm{Cont}(f)\,\mathrm{Cont}(g)$ *if $f, g \in K[X]$.*

Proof. By dividing f, g by their contents, it suffices to show that the product of two primitive polynomials in $R[X]$ (i.e. those with no common divisor of all their coefficients) is itself primitive. Indeed, suppose f, g are primitive and $p \in R$ is a prime. Then $\overline{f}, \overline{g} \in R/(p)[X]$ are nonzero. Their product $\overline{f}\overline{g}$ is also not zero because $R/(p)[X]$ is a domain, p being prime. In particular, p is not a common factor of the coefficients of fg. Since p was arbitrary, this completes the proof. ▲

So return to the main proof. We know that $f = gh$. We divided g, h by their contents to get $g', h' \in R[X]$. We had then

$$rf = g'h', \quad r \in K^*.$$

Taking the contents, and using the fact that f, g', h' are primitive, we have then:

$$r = \operatorname{Cont}(g') \operatorname{Cont}(h') = 1 \quad (\text{modulo } R^*).$$

But then $f = r^{-1}g'h'$ shows that f is not irreducible in $R[X]$, contradiction. ▲

Let R be a ring. Recall that an element is **irreducible** if it admits no nontrivial factorization. The product of an irreducible element and a unit is irreducible. Call a ring **finitely irreducible** if every element in the ring admits a factorization into finitely many irreducible elements.

Lemma 1.10 *A ring R is finitely irreducible if every ascending sequence of* principal *ideals in R stabilizes.*

A ring such that every ascending sequence of ideals (not necessarily principal) stabilizes is said to be *noetherian;* this is a highly useful finiteness condition on a ring.

Proof. Suppose R satisfies the ascending chain condition on principal ideals. Then let $x \in R$. We would like to show it can be factored as a product of irreducibles. So suppose x is not the product of finitely many irreducibles. In particular, it is reducible: $x = x_1 x_1'$, where neither factor is a unit. One of this cannot be written as a finite product of irreducibles. Say it is x_1. Similarly, we can write $x_1 = x_2 x_2''$ where one of the factors, wlog x_2, is not the product of finitely many irreducibles. Repeating inductively gives the ascending sequence

$$(x) \subset (x_1) \subset (x_2) \subset \dots,$$

and since each factorization is nontrivial, the inclusions are each nontrivial. This is a contradiction. ▲

Lemma 1.11 *Suppose R is a UFD. Then every ascending sequence of principal ideals in $R[X]$ stabilizes. In particular, $R[X]$ is finitely irreducible.*

Proof. Suppose $(f_1) \subset (f_2) \subset \dots \in R[X]$. Then each $f_{i+1} \mid f_i$. In particular, the degrees of f_i are nonincreasing, and consequently stabilize. Thus for $i \gg 0$, we have $\deg f_{i+1} = \deg f_i$. We can thus assume that all the degrees are the same. In this case, if $i \gg 0$ and $k > 0$, $f_i/f_{i+k} \in R[X]$ must actually lie in R as R is a domain. In particular, throwing out the first few elements in the sequence if necessary, it follows that our sequence looks like

$$f, f/r_1, f/(r_1 r_2), \dots$$

where the $r_i \in R$. However, we can only continue this a finite amount of time before the r_i's will have to become units since R is a UFD. (Or $f = 0$.) So the sequence of ideals stabilizes. ▲

Lemma 1.12 *Every element in $R[X]$ can be factored into a product of irreducibles.*

Proof. Now evident from the preceding lemmata. ▲

Suppose P is an irreducible element in $R[X]$. I claim that P is prime. There are two cases:

1. $P \in R$ is a prime in R. Then we know that $P \mid f$ if and only if the coefficients of f are divisible by P. In particular, $P \mid f$ iff $P \mid \mathrm{Cont}(f)$. It is now clear that $P \mid fg$ if and only if P divides one of $\mathrm{Cont}(f), \mathrm{Cont}(g)$ (since $\mathrm{Cont}(fg) = \mathrm{Cont}(f)\,\mathrm{Cont}(g)$).

2. P does not belong to R. Then P must have content a unit or it would be divisible by its content. So P is irreducible in $K[X]$ by the above reasoning.

   Say we have an expression
   $$P \mid fg, \quad f, g \in R[X].$$
   Since P is irreducible, hence prime, in the UFD (even PID) $K[X]$, we have that P divides one of f, g in $K[X]$. Say we can write
   $$f = qP, q \in K[X].$$
   Then taking the content shows that $\mathrm{Cont}(q) = \mathrm{Cont}(f) \in R$, so $q \in R[X]$. It follows that $P \mid f$ in $R[X]$.

We have shown that every element in $R[X]$ factors into a product of prime elements. From this, it is clear that $R[X]$ is a UFD. ▲

Corollary 1.13 *The polynomial ring $k[X_1, \dots, X_n]$ for k a field is factorial.*

Proof. Induction on n. ▲

1.3 Factoriality and height one primes

We now want to give a fancier criterion for a ring to be a UFD, in terms of the lattice structure on $\mathrm{Spec}\, R$. This will require a notion from dimension theory (to be developed more fully later).

Definition 1.14 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 1.15 *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.

1.4 Factoriality and normality

We next state a generalization of the "rational root theorem" as in high school algebra.

Proposition 1.16 *A factorial domain is integrally closed.*

Proof. **TO BE ADDED:** proof – may be in the queue already ▲

§2 Weil divisors

2.1 Definition

We start by discussing Weil divisors.

Definition 2.1 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 $\mathrm{Weil}(R)$.

The geometric picture behind Weil divisors is that a Weil divisor is like a hypersurface: a subvariety of codimension one.

2.2 Valuations

2.3 Nagata's lemma

We finish with a fun application of the exact sequence of Weil divisors to a purely algebraic statement about factoriality.

Lemma 2.2 *Let A be a normal noetherian domain.*

Theorem 2.3 *Let A be a noetherian domain, $x \in A - \{0\}$. Suppose (x) is prime and A_x is factorial. Then A is factorial.*

Proof. We first show that A is normal (hence regular in codimension one). Indeed, A_x is normal. So if $t \in K(A)$ is integral over A, it lies in A_x. So we need to check that if $a/x^n \in A_x$ is integral over A and $x \nmid x$, then $n = 0$. Suppose we had an equation

$$(a/x^n)^N + b_1(a/x^n)^{N-1} + \cdots + b_N = 0.$$

Multiplying both sides by x^{nN} gives that

$$a^N \in xR,$$

so $x \mid a$ by primality.

Now we use the exact sequence

$$(x) \to \mathrm{Cl}(A) \to \mathrm{Cl}(A_x) \to 0.$$

The end is zero, and the image of the first map is zero. So $\mathrm{Cl}(A) = 0$. Thus A is a UFD. ▲

§3 Locally factorial domains

3.1 Definition

Definition 3.1 A noetherian domain R is said to be **locally factorial** if $R_{\mathfrak{p}}$ is factorial for each $\mathfrak{p}$ prime.

Example 3.2 The coordinate ring $\mathbb{C}[x_1, \dots, x_n/I$ of an algebraic variety is locally factorial if the variety is smooth. We may talk about this later.

Example 3.3 (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 prototypical example of a ring without unique factorization. The reason has to do with the fact that the variety has a singularity at the origin.

3.2 The Picard group

Definition 3.4 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 In topology, one is often interested in classifying *vector bundles* on spaces. In algebraic geometry, a module M over a ring R gives (as in **??**) a sheaf of abelian groups over the topological space $\operatorname{Spec} R$; this is supposed to be an analogy with the theory of vector bundles. (It is not so implausible since the Serre-Swan theorem (**??**) gives an equivalence of categories between the vector bundles over a compact space X and the projective modules over the ring $C(X)$ of continuous functions.) In this analogy, the invertible modules are the *line bundles*. The definition has a counterpart in the topological setting: for instance, a vector bundle $\mathcal{E} \to X$ over a space X is a line bundle (that is, of rank one) if and only if there is a vector bundle $\mathcal{E}' \to X$ such that $\mathcal{E} \otimes \mathcal{E}'$ is the trivial bundle $X \times \mathbb{R}$.

There are many equivalent characterizations.

Proposition 3.5 *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 $a_1, \dots, a_n \in R$ 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

Step 1: 1 implies 2. 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 of $I \otimes_R R'$, 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 the *field* $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. 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, Nakayama's lemma shows that x generates $I_{\mathfrak{p}}$.

We get a surjection $\alpha : R_{\mathfrak{p}} \twoheadrightarrow I_{\mathfrak{p}}$ carrying $1 \to x$. We claim that this map is injective. This will imply that $I_{\mathfrak{p}}$ is free of rank 1. So, let J be an inverse of I among R-modules, so that $I \otimes_R J = R$; the same argument as above provides a surjection $\beta : R_{\mathfrak{p}} \to J_{\mathfrak{p}}$. Then $\beta' = \beta \otimes 1_{I_{\mathfrak{p}}} : I_{\mathfrak{p}} \to R_{\mathfrak{p}}$ is also a surjection. Composing, we get a surjective map

$$R_{\mathfrak{p}} \overset{\alpha}{\twoheadrightarrow} I_{\mathfrak{p}} \overset{\beta'}{\twoheadrightarrow} R_{\mathfrak{p}}$$

whose composite must be multiplication by a unit, since the ring is local. Thus the composite is injective and α is injective. It follows that α is an isomorphism, so that $I_{\mathfrak{p}}$ is free of rank one.

Step 2: 2 implies 3. Now we show 2 implies 3. Suppose I is finitely generated with generators $\{x_1, \dots, x_n\} \subset I$ and $I_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$ for all $\mathfrak{p}$. Then for each $\mathfrak{p}$, we can choose an element x of $I_{\mathfrak{p}}$ generating $I_{\mathfrak{p}}$ as $R_{\mathfrak{p}}$-module. By multiplying by the denominator, we can assume that $x \in I$. By assumption, we can then find $a_i, s_i \in R$ with

$$s_i x_i = a_i x \in R$$

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 $\{\operatorname{Spec} R[1/a_{\mathfrak{p}}]\}$ of $\operatorname{Spec} R$ (where $a_{\mathfrak{p}} \notin \mathfrak{p}$) on which I is isomorphic to R. To say that these cover $\operatorname{Spec} R$ 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 $\operatorname{Spec} R[1/a_i]$ 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** $J = \operatorname{Hom}_R(I, R)$ 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

$$0 \to J \to \operatorname{Hom}(R^n, R) \to \operatorname{Hom}(R^m, R).$$

It follows that the formation of J commutes with localization. In particular, this argument shows that

$$J[1/a] = \operatorname{Hom}_{R[1/a]}(I[1/a], R[1/a]).$$

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 $a_1, \dots, a_n$ 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 3.6 Let R be a commutative ring. We define the **Picard group** $\operatorname{Pic}(R)$ to be the set of isomorphism classes of invertible R-modules. This is an abelian group; the addition law is defined so that the sum of the classes represented by M, N is $M \otimes_R N$. The identity element is given by R.

The Picard group is thus analogous (cf. **??**) to the set of isomorphism classes of line bundles on a topological space (which is also an abelian group). While the latter can often be easily computed (for a nice space X, the line bundles are classified by elements of $H^2(X, \mathbb{Z})$), the interpretation in the algebraic setting is more difficult.

[1] To check that a map is surjective, just check at the localizations at any maximal ideal.

3.3 Cartier divisors

Assume furthermore that R is a domain. We now introduce:

Definition 3.7 A **Cartier divisor** for R is a submodule $M \subset K(R)$ such that M is invertible.

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 3.8 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 3.9 *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

$$K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0.$$

3.4 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 3.10 *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.*

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 3.11 *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 3.12 *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 3.13 *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 3.14 *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 3.15 *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

[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.

$x = x_1 \dots x_n$ 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.

3.5 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 Weil(R) and Cart(R) for R a locally factorial noetherian domain.

1. Weil(R) is free on the height one primes.

2. 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 $R = \mathbb{C}[X_1, \dots, X_n]/I$ for some ideal I. Then the maximal ideals, or closed points in 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.

3.6 Further remarks on Weil(R) and 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 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 3.16 *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 Weil(R), hence of 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. **TO BE ADDED:** ?

CRing Project contents

CRing Project bibliography

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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