8430 HANDOUT 2: ORDERS, PRE/ALMOST/DEDEKIND DOMAINS, AND THE PICARD GROUP

PETE L. CLARK

1. Dedekind domains

To the reader: although this section is concerned with properties of Dedekind domains, it turns out that many of the most important properties of Dedekind domains are *characteristic* properties, i.e., not only does any Dedekind domain enjoy the property, but conversely any integral domain which enjoys that property is a Dedekind domain. Since the rings of initial interest to us, namely $\mathbb{Z}[\sqrt{-n}]$, are in general non-maximal orders in quadratic fields, in the following section we will be faced with the following task: knowing that certain desirable properties of Dedekind domains cannot possibly hold for non-maximal orders, can we find slightly weaker properties that still hold for these "almost Dedekind domains"? All this is to say that in this section we will be performing the following dance: "Let R be any integral domain; now let R be a Dedekind domain; *now* let R be any (or maybe Noetherian, etc.) integral domain..." So prepare yourself for it!

Convention: As is common in the study of Dedekind rings, we will often use "ideal" to mean "nonzero ideal." Since it will be immediately apparent whether or not any given assertion pertains to the zero ideal, this ought not to cause confusion.

1.1. Basic properties.

Let us collect some basic (not necessarily easy!) properties of Dedekind rings. I do not honestly expect to need to use all of these, but it is comforting to have them in one place if we need them.

Theorem 1. *(Localization of Dedekind domains) Let R be a Dedekind domain with quotient field K and $S \subset R$ a multiplicatively closed set.*
a) The localization $S^{-1}R = \{\frac{x}{y} \in K \mid x \in R, y \in S\}$ is a Dedekind domain.
b) If $\mathfrak{p}$ is a prime ideal of R, then $R_{\mathfrak{p}} := (R - \mathfrak{p})^{-1}R$ is a discrete valuation ring.
c) Conversely, a domain whose localization at every (nonzero!) prime ideal is a discrete valuation ring is necessarily a Dedekind domain.

In other words, the "local analogue" of a Dedekind domain is a discrete valuation ring (DVR).[1] The intermediate concept of PID is much more ephemeral.

The following is a serious theorem:

Theorem 2. *(Krull-Akizuki) Let R be a one-dimensional Noetherian domain, with quotient field K, and let L/K be a finite field extension. Let S be any intermediate ring $R \subset S \subset L$.*

[1] Topics such as localization and DVR's are covered very casually here. They are not discussed in Cox's book and hence are not necessary to understand the main theorems in the case of orders in quadratic fields, but they will be used for a theorem at the end of these notes.

a) S is (at most) one-dimensional and Noetherian.
b) Thus S is a Dedekind domain iff it is integrally closed; this occurs, in particular, if S is the integral closure of R in L.

Proof: For the proof of part a) see [Kap]. Observe that part b) follows immediately, since integral closures are integrally closed.

Corollary 3. *The ring of integers of a number field is a Dedekind domain.*

Proof: Apply the theorem with $R = \mathbb{Z}$, $K = \mathbb{Q}$, L our number field. Since the ring of integers of L is, by definition, the integral closure of R in L, it is integrally closed.

We would also like to know that the ring of integers of a number field is finitely generated as a $\mathbb{Z}$-module. One can prove this in a down-to-earth way, or by appealing to the following supplementary result.

Theorem 4. *Let R be a Noetherian, integrally closed domain with quotient field K, and L/K a finite **separable** field extension. Then the integral closure of R in L is finitely generated as an R-module.*

Proof: See e.g. [ZS, Ch. V, § 4].

Theorem 5. *Let R be an integrally closed domain with quotient field K, let L/K be a finite **separable** field extension, and let S be the integral closure of R in L. For any maximal ideal $\mathfrak{p}$ of R, the set of prime ideals $\mathfrak{P}$ of S which lie over $\mathfrak{p}$ – i.e., such that $\mathfrak{P} \cap R = \mathfrak{p}$ is nonempty and finite.*

Proof: You should know that any homomorphism of rings $\varphi : R \rightarrow S$, pulling back ideals $\mathfrak{P} \mapsto \varphi^{-1}(\mathfrak{P})$ defines a map from ideals of S to ideals of R which carries prime ideals to prime ideals (i.e., induces a map on prime spectra $\varphi^* : \operatorname{Spec} S \rightarrow \operatorname{Spec} S$). When S/R is an extension ring – i.e., when φ is injective – the pullback map is (visibly) just intersection with R. When, as here, S/R is an integral extension, the **Going Up Theorem** [e.g. Atiyah-Macdonald] asserts (in particular) that φ^* is surjective, i.e., every prime ideal of R lies under some prime ideal of S. For the finiteness, see Lang's *Algebra*, Corollary VII.2.2 (p. 340 in the – presumably final – revised third edition). The gist of it is that by separability, we can pass to the Galois closure M of L/K and it suffices to prove the result there, in which case it follows from the important fact that the (finite!) Galois group of M over K acts *transitively* on the set of prime ideals lying over $\mathfrak{p}$.

1.2. **Fractional ideals.** In any commutative ring R, if I, J are ideals, we can define the product IJ as the ideal generated by all products ij with $i \in I$, $j \in J$; slightly more concretely, this is the set of all finite sums $\sum_n i_n j_n$ of such products. This product operation is compatible with inclusion, in the sense that $I_1 \subset I_2$ implies $I_1 J \subset I_2 J$. The collection of all nonzero ideals in a commutative ring R forms a monoid under the ideal product, denoted $\mathcal{I}(R)$.

Exercise 2.1.1: (General Chinese Remainder Theorem) Let R be a commutative ring and $I_1, \ldots, I_n$ a set of ideals of R which are **pairwise coprime**: for all $i \neq j$, $I_i + I_j = R$. Define a natural homomorphism of rings

$$\Phi : R \rightarrow \bigoplus_{i=1}^{n} R/I_i.$$

Show that Φ is surjective and that its kernel is $I = \cap_{i=1}^n I_i = \prod_{i=1}^n I_i$. (The last equality is a bit tricky to show: you may wish to consult Lorenzini, *An Invitation to Arithmetic Geometry*, Lemma III.2.4, p. 89).

Theorem 6. *For an integral domain R, TFAE:*
(i) R is a Dedekind domain.
(ii) All ideals of R factor uniquely into products of prime ideals.
(iii) For any ideal I of R, there is an ideal J of R such that $IJ = (\alpha)$ is principal.

Proof: See e.g. [ZS, Ch. V, §6].

In essence, Theorem 6 asserts that the multiplicative structure of the ideals in a Dedekind domain is analogous to that of the usual positive integers under multiplication (which can be naturally identified with the ideals in the Dedekind domain $\mathbb{Z}$). More precisely, if $\mathcal{P}$ is the set of prime ideals of R, then $\mathcal{I}$ is $\bigoplus_{P\in\mathcal{P}}\mathcal{N}$, the free commutative monoid with generating set $\mathcal{P}$. In other words, any nonzero ideal can be expressed as $I = \prod_P P^{v_P(I)}$, where $v_P(I) \in \mathcal{N}$ and all but finitely many exponents are equal to zero. Note that if $0 \neq f \in R$, the factorization of the principal ideal $(f) = \prod_P P^{v_P(f)}$ associates to each prime P a discrete valuation $f \mapsto v_P(f)$.

This has many important consequences:

Proposition 7. *Let R be a Dedekind domain.*
a) (Cancellation) If $I_1,\ I_2,\ J$ are ideals of R such that $I_1J = I_2J$, then $I_1 = I_2$.
b) (To contain is to divide) For ideals I, J of R, TFAE:
(i) $I \supset J$.
(ii) There exists K such that $IK = J$.
(iii) For all primes P, $v_P(I) \geq v_P(J)$.
c) For ideals $I = \prod_P P^{v_P(I)}$, $J = \prod_P P^{v_P(J)}$, then

$$I + J = \prod_P P^{\min(v_P(I),v_P(J))}$$

is the unique ideal A with the property that $K \mid I,\ K \mid J \implies K \mid A$. In other words, it can be viewed as $\gcd(I, J)$*, the greatest common divisor of I and J.*
d) Similarly

$$I \cap J = \prod_P P^{\max(v_P(I),v_P(J))}$$

is the unique ideal B with the property that $I \mid K,\ J \mid K \implies B \mid K$. In other words, it can be viewed as $\operatorname{lcm}(I, J)$*, the least common multiple of I and J.*

Exercise 2.1.2: Prove Proposition 7.

Exercise 2.1.3: (Dedekind's Chinese Remainder Theorem) Let R be a Dedekind domain. Let $P_1, \ldots, P_n$ be distinct prime ideals.
a) Show that for any $a_1, \ldots, a_n \in \mathbb{Z}^+$, the ideals $P_1^{a_1}, \ldots, P_n^{a_n}$ are pairwise coprime.
b) Conclude that there is a canonical isomorphism of rings

$$R/(\prod_{i=1}^n P_i^{a_i}) \xrightarrow{\sim} \bigoplus_{i=1}^n R/P_i^{a_i}.$$

It is often more pleasant to deal with groups that monoids. If M is a commutative monoid, then there is a canonical commutative group $G(M)$ associated to M, called the **group completion** (or **Grothendieck group**) of M along with a monoid homomorphism $G : M \rightarrow G(M)$. $G(M)$ is defined, up to unique isomorphism, by the following universal mapping property: for any group H and any monoid homomorphism $\varphi : M \rightarrow H$, there exists a unique group homomorphism $\Phi : G(M) \rightarrow H$ such that $\varphi = \Phi \circ G$.

Exercise 2.1.4: Let G be a multiplicatively written commutative monoid.
a) Show that the group completion $G(M)$ can be explicitly constructed as follows: it is the set of all equivalence classes of pairs $(a, b) \in M \times M$, where $(a, b) \sim (c, d)$ iff there exists $m \in M$ such that $mad = mbc$, under the product $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$. The map G is $a \mapsto [(a, 0)]$.
b) Show that the homomorphism $G : M \rightarrow G(M)$ is injective iff M has the cancellation property: for $a, b, m \in M$, $ma = mb \implies a = b$.
c) For a set S, let $FCM(S) = \bigoplus_{s \in S} \mathcal{N}$ be the free commutative monoid on S. Check that M has the cancellation property and the group completion is the free commutative group $\bigoplus_{s \in S} \mathbb{Z}$ on S.

In particular the monoid $\mathcal{I}(M)$, being the free commutative monoid on the prime ideals, injects into its group completion, which is $\bigoplus_{P \in \mathcal{P}} \mathbb{Z}$. We write $\mathrm{Frac}(R)$ for $G(\mathcal{I}(M))$ and call it the group of fractional ideals of R. But this is just a formal definition: what *is* a fractional ideal, other than a formal quotient of two ideals?

Definition: For an integral domain R with quotient field K, a **fractional ideal** is a nonzero R-submodule I of K such that $\alpha I \subset R$ for some $\alpha \in R \setminus 0$.

Lemma 8. *Let R be a domain.*
a) Every nonzero finitely generated R-submodule of K is a fractional ideal.
b) The converse holds iff R is Noetherian.

Proof: If $I = R\frac{a_1}{b_1} + \ldots + R\frac{a_n}{b_n}$, then $(b_1 \cdots b_n)I \subset R$. Conversely, for any $\alpha \in K^\times$, multiplication by α gives an R-module isomorphism from I to αI. So if αI is an ideal in the Noetherian ring R, it is finitely generated as an R-module, hence so is I.

Remark: In the lecture, I defined a fractional ideal to be a nonzero finitely generated R-submodule of K and then noted somewhat sheepishly that every integral ideal of R is a fractional ideal iff R is Noetherian. In the absence of the Noetherian hypothesis, it is correct to require the weaker "scaling condition" $\exists \alpha \mid \alpha I \subset R$. This distinction doesn't matter in our application of the results – for sure the rings R we care about will be Noetherian – but it indicates that in proofs one should be able to work with the scaling condition, and in fact it is usually easier to do so than to check that modules are finitely generated.

One can think of a fractional ideal informally as being of the form I' "divided by" (α). In fact, for any nonzero $\alpha \in K$, the set $R(\alpha^{-1})$ is a fractional ideal of R, written (α^{-1}). Evidently a fractional ideal can be written in such a form iff as an R-module it has a single generator; such fractional ideals are said to be **principal**.

Lemma 9. *a) For two fractional ideals I, J of a domain R, the product*

$$I \cdot J = \sum_n i_n j_n$$

is again a fractional ideal.
b) The fractional ideals of R form a commutative monoid under multiplication.

Proof: It is no problem to see that $I \cdot J$ is an R-submodule of K. Also, if $\alpha I \subset R$ and $\beta J \subset R$, then $(\alpha\beta)IJ \subset R$. Evidently $R \cdot I = I$ for any fractional ideal R.

Observe that any commutative ring is in particular a commutative monoid under multiplication. The invertible elements in this monoid are precisely the units of R, and they form a subgroup $R^\times$, the group of units. A moment's thought shows that this is a general fact about commutative monoids: if M is a commutative monoid, then the set

$$M^G = \{m \in M \mid \exists m',\ mm' = e\}$$

of invertible elements is a subgroup of M, in fact the largest possible subgroup. To be explicit, a fractional ideal I of a domain R is **invertible** if there exists another fractional ideal J such that $IJ = R$.

Lemma 10. *Let R be a domain and I a fractional ideal of R.*
Define $I^* = \{a \in K \mid aI \subset R\}$.
a) I^* is a fractional ideal of R.
b) In general we have $II^* \subset R$. I is invertible iff $II^* = R$.
c) If I is invertible, I^* is the unique inverse so can (and shall) be denoted by I^{-1}.

Proof: If $a \in I^*$ and $x \in R$, then $xaI = a(xI) \subset aI \subset R$, so $xa \in I^*$. Therefore I^* is an R-submodule. To see that I^* is a fractional ideal, suppose first that $I = (\alpha)$ is principal. Then $I^* = (\alpha^{-1})$ so is also a fractional ideal – and moreover in this case it is clear that $II^* = R$. In general we can write $I = R\alpha_1 + \ldots + R\alpha_n$, and then $I^* = \bigcap_{i=1}^n (\alpha_i^{-1}) \supset (\alpha_1^{-1} \cdots \alpha_n^{-1})$, so $I^* \neq 0$. If $a \in I^*$ then $a\alpha_1 \in R$, i.e., $\alpha_1 I^* \subset R$, so I^* is a fractional ideal, proving part a). The relation $II^* \subset R$ is immediate from the definition of I^*; more precisely, I^* is the largest subset of R such that this relation holds, and it is a fractional ideal. Thus if there is any fractional ideal J such that $IJ = R$, then $J \subset I^*$ and hence $II^* = R$. This proves b). Finally, if $IJ = R$ then $J = I^*IJ = I^*R = I^*$: of course this is just the usual argument that inverses are unique whenever they exist.

Let us write $J(R)$ for the subgroup $\text{Frac}(R)^G$ of invertible fractional ideals of a domain R. Thus $J(R)$ sits inside $\text{Frac}(R)$ as the group of all invertible elements. It is natural to ask about the difference between $J(R)$ and $\text{Frac}(R)$: is every fractional ideal invertible?

Proposition 11. *For a domain R, TFAE:*
(i) $J(R) = \text{Frac}(R)$, i.e., every fractional ideal is invertible.
(ii) The fractional ideals $\text{Frac}(R)$ form a group under multiplication.
(iii) R is a Dedekind domain.

Proof: (i) and (ii) are obviously equivalent. According to Theorem 2, R is Dedekind iff for all nonzero ideals I of R, there exists an ideal J such that $IJ = (\alpha)$. Suppose this latter condition holds. Then for any fractional ideal I, there exists β such that

$\beta I = I'$ is integral, and applying the condition we get an integral ideal J such that $(\alpha) = I'J = \beta IJ$, and then $I(\beta\alpha^{-1})J = R$. The converse is similar.

Again, this is both good and bad news: this very nice property is satisfied for Dedekind domains and only for Dedekind domains: in the general case we will need to grapple with noninvertible fractional ideals. But let's push that aside for now. At last, for the rest of this section we shall assume that R is a Dedekind domain!

First let's nail down the group structure of $\mathrm{Frac}(R)$. We know that integral ideals factor uniquely into primes $P \in \mathcal{P}$, and we know that for every prime ideal P there exists an inverse fractional ideal $P^{-1} = P^*$. Of course, like in any commutative group, we have relations$(IJ)^{-1} = I^{-1}J^{-1}$, so if

$$I = \prod_{P \in \mathcal{P}} P^{v_P(I)},$$

it follows immediately that

$$I^{-1} = \prod_{P \in \mathcal{P}} P^{-v_P(I)}.$$

In particular for any $\alpha \in R \setminus 0$, we have

$$(\alpha^{-1}) = \prod_{P \in \mathcal{P}} P^{-v_P(\alpha)}$$

hence an arbitrary fractional ideal I can be written as $(\alpha^{-1})I'$ for integral I and $\alpha \in R \setminus 0$, and then

$$I = \prod_{P \in \mathcal{P}} P^{v_P(I') - v_P(\alpha)}.$$

In particular the valuation v_P on R extends to a discrete valuation $v_P : K^\times \to \mathbb{Z}$ on the quotient field. So for instance we could define a P-adic absolute value on K by $||\alpha||_P = e^{-v_P(\alpha)}$, with the convention that $\mathrm{ord}_P(0) = \infty$ and $||0||_P = 0$. (Here I really do mean $e = 2.71828\ldots$ but it doesn't matter: taking an exponential to any base $c > 1$ would work as well. The choice of e rather than, say, 2, as the base is a common convention – I think the idea is to choose a base which is manifestly of no arithmetic significance! In certain special cases – especially, when the residue field of the valuation ring is finite – it is desirable to take a more clever choice of base, but not in this level of generality.) It is then often useful to **complete** K with respect to P – e.g., in the simplest case $K = \mathbb{Q}$, $P = (p)$ for a prime number p, we would get the field $\mathbb{Q}_p$ of p-adic numbers. But we don't need to complete anything just yet.

In particular every nonmaximal order in a number field is going to have some "bad" – i.e., non-invertible – ideals. Let us push this aside for the moment: our first order of business is to see what happens with Dedekind domains.

2. The ideal class group of a Dedekind domain

After bathing in the soothingly abstract theory of the previous section, let us recall that the point of all this is to gain some insight into when a prime ideal P in a Dedekind domain (or later, a slightly more general ring) is principal. As advertised, for a Dedekind domain R there is a (multiplicatively written) commutative group $\operatorname{Pic}(R)$ and a monoid mapping

$$[\;] : \mathcal{I}(R) \to \operatorname{Pic}(R)$$

which associates to every ideal I of R its **ideal class** $[I] \in \operatorname{Pic}(R)$, in such a way that $[IJ] = [I][J]$ – i.e., a monoid homomorphism – and such that $[I] = 1 \in \operatorname{Pic}(R)$ iff I is principal. Note the situation: we have (or wish to have) a monoid homomorphism from a commutative monoid to a commutative group. By the general nonsense of the preceding section, such a thing must factor uniquely through the group completion of $\mathcal{I}(R)$, namely the group $\operatorname{Frac}(R)$ of all fractional ideals.

On the other hand, it is possible and (I hope) somewhat enlightening to see that the ideal class homomorphism can be defined directly on the level of integral ideals. Namely, what $\operatorname{Pic}(R)$ is supposed to be is some sort of quotient of $\mathcal{I}(R)$ which regards two ideals as equal iff they differ, multiplicatively speaking, by a principal ideal. Well, what are we waiting for? Define an equivalence relation $\sim$ on integral ideals of R: $I \sim J$ iff there exist $\alpha, \beta \in R \setminus 0$ such that $\alpha I = \beta J$. This is easily seen to be an equivalence relation which is moreover **compatible** with the monoid structure in a natural sense. Indeed:

Exercise 2.2.1:
Let M be a commutative monoid and $\sim$ an equivalence relation on M.
a) We say that $\sim$ is compatible (with the monoid structure) if $x_1 \sim x_2$, $y_1 \sim y_2$ implies $x_1 y_1 \sim x_2 y_2$. Show that the equivalence relation $\sim$ on $\mathcal{I}(R)$ is compatible.
b) Given any monoid M and compatible equivalence relation $\sim$, the quotient $M' = M/\sim$ – i.e., the set of equivalence classes under $\sim$ – can be endowed with a unique monoid structure making the quotient map $M \to M'$ into a monoid homomorphism.[2]

So we have a monoid structure on $\mathcal{I}(R)/\sim$ of equivalence classes of integral ideals. In fact we can do this for any integral domain R. But the key point is as follows:

Proposition 12. *a) For a domain R, TFAE:*
(i) The monoid $\mathcal{I}(R)/\sim$ is a group.
(ii) R is a Dedekind domain.
b) If I is an ideal in a Dedekind domain, then $[I] = 1 \iff I$ is principal.

Exercise 2.2.2: Prove Proposition 12.

So for a Dedekind domain R the object $\mathcal{I}(R)/\sim$ is exactly what we want: let's give it a nice fancy name: $\operatorname{Pic}(R)$, the **Picard group** of R. We will see later that the Picard group can be defined for an arbitrary integral domain, but not with the definition just given: it won't even be a group. Therefore in the case of a Dedekind domain one also – and perhaps more often, depending upon one's mathematical cultural background – refers to this group as $\operatorname{Cl}(R)$, the **ideal class group** of R.

Now let us define it again in terms of fractional ideals and try to see why this

[2] This is just a fancy way of saying that the product on M is well-defined on equivalence classes, which is indeed almost exactly the same thing as saying the equivalence relation is compatible. At least we didn't express the quotient in terms of a universal mapping property...

second definition, although manifestly equivalent to the first, is somehow "better". (Roughly, it is always better to work with a group than a monoid, if possible.) Namely, we know the monoid homomorphism factors through to give a group homomorphism

$$\Phi : \mathrm{Frac}(R) \to \mathrm{Cl}(R),$$

just defined by writing a fractional ideal as the quotient IJ^{-1} of two integral ideals and putting

$$\Phi : IJ^{-1} = [I][J]^{-1}.$$

Since the original class map [ ] was surjective (as is any quotient map), so too is Φ. Notice that the kernel of Φ is precisely the subgroup of principal fractional ideals, which we will now give a name to: $\mathrm{Prin}(R)$.

Proposition 13. *The group* $\mathrm{Prin}(R)$ *of principal fractional ideals of R is canonically isomorphic to $F^{\times}/R^{\times}$.*

Exercise 2.2.3: Prove Proposition 13.

So for any Dedekind domain R, we have an exact sequence:

$$1 \to R^{\times} \to F^{\times} \to \mathrm{Frac}(R) \xrightarrow{\Phi} \mathrm{Cl}(R) \to 1.$$

Note how clean this looks: we get a presentation for the class group in terms of easily defined maps between not very scary-looking abelian groups. Of course the simplicity is entirely deceptive: understanding the structure of the class group and the class homomorphism Φ for a Dedekind domain is one of the great problems in algebra and number theory.

Speaking of number theory, one has the following fundamental result:

Theorem 14. *Suppose that R is either the full ring of integrers of a number field K or the coordinate ring $k[C]$ of a smooth, geometrically integral affine curve over a field k. Then* $\mathrm{Cl}(R)$ *is a finite commutative group.*

It would take us too far out of our way to prove this result here: see [Dino, Ch. 5]. Moreover, when R is the ring of integers of an imaginary quadratic field, we will later use quadratic forms to give a very concrete and useful description of $\mathrm{Cl}(R)$, from which it will be clear not only that it is finite in all cases, but (better!) how to compute it in any given case.

Wht can be said about the class homomorphism Φ in this level of generality?

First, it is determined by its restriction to $\mathcal{P}$, the set of prime ideals of R. In particular, $\Phi(\mathcal{P})$ generates $\mathrm{Cl}(R)$, and for our problem we are most interested in where the primes go.

Here is one of the few general facts I know about Φ:

Theorem 15. *(Claborn, Clark) Let R be a Dedekind domain and let $\mathcal{P}' \subset \mathcal{P}$ be the set of* ***non****-principal prime ideals. TFAE:*
(i) $\mathcal{P}'$ is empty.
(ii) $\mathcal{P}'$ is finite.
(iii) R is a PID.

Proof: The only nontrivial implication is (ii) $\implies$ (iii). For this, enumerate the nonprincipal primes $P_1, \ldots, P_n$, let I be an integral ideal, and suppose that

$$I = P_1^{a_1} \cdots P_n^{a_n} Q_1^{b_1} \cdots Q_m^{b_m}.$$

(As usual, we allow zero exponents.) By the Chinese Remainder Theorem we may choose an $\alpha \in R$ such that $v_{P_i}(\alpha) = a_i$ for all i – note that we want equality, not just $v_{P_i}(\alpha) \geq a_i$, so you should definitely think about how to get this from CRT if you've never seen such an argument before. Now consider the fractional ideal $(\alpha^{-1})I$; it factors as

$$(\alpha^{-1})I = Q_1^{b_1} \cdots Q_m^{b_m} R_1^{c_1} \cdots R_l^{c_l},$$

where the R_i's are some other prime ideals, but disjoint from the P_i's: essentially CRT says we can find a principal ideal that does exactly what we want it to at any finite set of primes at the expense of total ignorance of what happens at the other primes. But all of the (fractional) ideals in the factorization of $(\alpha^{-1})I$ are principal, so $(\alpha^{-1})I = (\beta)$ for some $\beta \in K^\times$ and then $I = (\alpha\beta)$ is principal!

Remark: Note that, among other things, the proof illustrates the utility of working with fractional ideals even if one is truly nterested in integral ideals (or even just prime ideals). You may wish to try to recast the proof so that it avoids fractional ideals. (Had I been able to do this myself, I would have presented it earlier on!)

It seems that Theorem 15 first appeared in a 1965 paper of L. Claborn [Cla65]. I discovered it independently while preparing this course, so I have jointly attributed it to myself, but this is rather tongue in cheek: surely the great algebraists of the early 20th century knew it and just never bothered to write it down (or maybe they did...) It is really a quite easy result. However, I will mention some related, and very striking, results of Claborn later on.

Corollary 16. *Let R be a Dedekind with quotient field K. Suppose that R has only finitely many prime ideals. Then not only is R a PID, but the integral closure S of R in any finite separable field extension L/K is a PID.*

Proof: The statement for R follows immediately from Theorem 15. More generally, each prime $\mathfrak{P}$ of S lies over a unique prime $\mathfrak{P} \cap R$ of R, and by Theorem 15 there are only finitely many primes of S lying over any one prime $\mathfrak{p}$ of R, so S has only finitely many primes as well.

Corollary 17. *(Washington) There are infinitely many prime numbers.*

Proof: If there were only finitely many prime numbers, the Dedekind ring $\mathbb{Z}$ would have finitely many prime ideals, and hence by Corollary 16 not only would $\mathbb{Z}$ be a PID (no contradiction yet...) but so would be the ring of integers $\mathcal{O}_K$ in every number field K! We know that's not true, having seen e.g. that for $p \equiv 1 \pmod 4$, $\mathbb{Z}[\sqrt{-p}]$ is the full ring of integers of $\mathbb{Q}(\sqrt{-p})$ and is not a PID.

Remark: I mean of course, that this *proof* of Corollary 17 is due to Larry Washington. (I hope you know to whom the original proof is credited!) Washington's proof appears in P. Ribenboim's *The Book of Prime Number Records.*

Exercise 2.2.4: What other Dedekind domains can you show have infinitely many prime ideals using this method of proof? A good place to start would be $\mathbb{F}_p[t]$ –

which to be sure, Euclid's argument also works to show has infinitely many prime ideals – and see if you can systematically build a quadratic extension in which the integral closure is not a PID. Does Washington's proof *always* work – i.e., suppose R is a Dedekind domain whose integral closure in every finite separable field extension is a PID. Must R have finitely many prime ideals?[3]

Exercise 2.2.5: Let R be a Dedekind ring whose quotient field K is algebraically closed. Prove/disprove: $R = K$.

Remark: The idea of using CRT to make approximations is an extremely important one in number theory. In fact, FYI, let me tell you the following cognate result, which has both weaker hypotheses and a slightly weaker conclusion.

Theorem 18. *(Artin-Whaples Approximation Theorem) Let F be a field, and let $|| \ ||_1, \ldots, || \ ||_n$ be a finite set of absolute values on F, each determining a metric $d_i(x, y) = ||x - y||_i$ and hence a topology τ_i. Endow the space F^n with the product topology $(F, \tau_1) \times \ldots \times (F, \tau_n)$. Show that the following are equivalent:*
(i) The diagonal image $\{(x, \ldots, x) \mid x \in F\}$ of F in F^n is dense.
(ii) For all $i \neq j$, the topologies τ_i and τ_j are distinct.

Exercise 2.2.6*: Prove Theorem 18. (Hint: look it up. I would.)

What does this have to do with CRT? Let F be the quotient field of a Dedekind domain R, and let $P_1, \ldots, P_n$ be a finite set of distinct primes. The corresponding discrete valuations v_P determine absolute values $|| \ ||_P$ as above, and it is not hard to see that they give rise to distinct topologies (e.g. one can argue from the fact that the valuation rings are distinct). Applying the theorem in this gives: if you have any n elements $\alpha_1, \ldots, \alpha_n \in F$ (not necessarily distinct) and any integers $a_1, \ldots, a_n$, then there is a $\alpha \in F$ such that for all i, $v_{P_i}(\alpha - \alpha_i) \geq a_i$. In particular, if you choose α_i to itself have $v_{P_i}(\alpha_i) > a_i$, then the non-Archimedean triangle inequality gives $v_{P_i}(\alpha) = a_i$ for all i. In other words, you can find a α such that the fractional ideal (α) has whatever exponents you like at any finite set of primes of your own choosing. This is slightly different from CRT in that when the a_i's are all non-negative, CRT says we can take $\alpha \in R$, whereas a Dedekind ring does not even appear in the statement of the Artin-Whaples theorem. Notice though that in the proof of Theorem 15 we did not need $\alpha \in R$, so in this case the weaker conclusion is fine. (It often is.) The principal advantage of the Artin-Whaples theorem is that when applied to a number field we can also include **Archimedean** absolute values. To get a flavor for this, apply the theorem to $F = \mathbb{Q}$ and a set of finitely many p-adic absolute values together with the standard Archimedean absolute value. The theorem then says that in any open interval I on the real line and any n-tuple of integers $(a_1, \ldots, a_n)$ you can find a rational number r lying in I and such that $\mathrm{ord}_{p_i}(r) = a_i$ for each of an arbitrary, but finite, set of primes.

There is even more to say about this result, but I will withhold for now except to say that this result is often referred to (in particular, by me) as **The Weak Approximation Theorem.**[4]

[3] I have no idea what the answer to this is.

[4] Strong Approximation is a much more specific and technical statement involving adele groups...

Finally, Theorem 18 is a very basic example of a **Moving Lemma** in arithmetic geometry. I urge you to ask [Dino] for more details if you are curious.

Ah, I had promised some results of Claborn on Dedekind domains and class groups:

Theorem 19. *(Claborn,* [Cla65], [Cla66]*)*
a) There is a Dedekind domain R with no *principal prime ideals.*
b) Suppose R is a Dedekind domain whose class group $\mathrm{Cl}(R)$ is a torsion group. Then for any proper subgroup H of $\mathrm{Cl}(R)$ there are infinitely many primes P such that $[P] \in \mathrm{Cl}(R) \setminus H$.
c) For any commutative group G, there is a Dedekind domain R with $\mathrm{Cl}(R) \cong G$.
d) There is a Dedekind ring which is not the integral closure of a PID.

Note part b) applies when $\mathrm{Cl}(R)$ is finite, giving a sort of equidistribution result.

I have not looked over the proofs in detail, but at a glance they strike me as being rather accessible. Especially, his example for part (d) is more elementary than some of the things discussed in this handout, but negatively resolved a 1958 conjecture of Zariski and Samuel. (In fact I had been wondering about it as well until I saw his paper.) This might make a good topic for a presentation for someone who is algebraically inclined. Both papers are posted on the main course page.

3. A Case Study: $R = \mathbb{Z}[\sqrt{-3}]$

Let us now try to address the question of what the Picard group of a non-Dedekind domain R should be. It seems best to begin with an example.

Example: In some sense, the ring $R = \mathbb{Z}[\sqrt{-3}]$ is the simplest integral domain which is not a Dedekind domain. (E.g. every finite integral domain is a field; this includes any domain of positive characteristic which is finitely generated as a $\mathbb{Z}$-module. The next simplest integral domain is $\mathbb{Z}$, which is of course Dedekind. Next come the quadratic orders, and the one with smallest (in absolute value) discriminant which is not Dedekind is $\mathbb{Z}[\sqrt{-3}]$.) As we saw in our study of the form $x^2 + 3y^2$, the unique prime ideal $\mathfrak{p}_2$ of norm 2 is not principal, but every other prime ideal is principal. As mentioned in class at the time, according to Theorem 15 this behavior is not possible for a Dedekind ring. As mentioned at the time, it is a matter of opinion and perspective whether this phenomenon of exactly one nonprincipal prime is "pathological": it certainly made our study of primes of the form $x^2 + 3y^2$ work out nicely.

But by Theorem 6, the ring $\mathbb{Z}[\sqrt{-3}]$ must have certain pathologies: there must be at least one ideal which does not factor into primes as well as at least one non-invertible ideal. It seems clear that somehow 2 should have a role to play here, so let's look at the principal prime ideal (2), of norm 4. Again, the only prime ideal which contains 2 is $\mathfrak{p}_2$. To be quite concrete, $\mathfrak{p}_2 = \langle 1 + \sqrt{-3}, 1 - \sqrt{-3} \rangle$. (How did I know this? We are looking for an ideal which has index 2 as a subgroup of the rank two free commutative group $\mathbb{Z}1 + \mathbb{Z}\sqrt{-3} \cong \mathbb{Z}^2$. The lattice $\mathbb{Z}^2$ has only finitely many sublattices of any given index; for instance it is easy to see that it has exactly $p + 1 = \# \mathrm{PP}^1(\mathbb{F}_p)$ subgroups of prime index p, so 3 subgroups of index 2. If you write down the other two, you will see immediately that they are not ideals in the ring.) For any "factored" ideal I we have

$$I = P_1^{a_1} \cdots P_n^{a_n} \subset \bigcap_i P_i^{a_i} \subset P_i$$

so if the ideal (2) factors at all, it would be $\mathfrak{p}_2^a$ for some positive integer a. Since (2) has norm 4 and $\mathfrak{p}_2$ has norm 2, one might reasonably expect that (2) is the square of $\mathfrak{p}_2$. However:

Exercise 2.3.1: Show that $\mathfrak{p}_2^2 = (2)\mathfrak{p}_2$.

But that implies that for any positive integer a we have

$$\mathfrak{p}_2^a = (2)^{a-1}\mathfrak{p}_2.$$

In particular, no power of the ideal $\mathfrak{p}_2$ is principal, and hence no power is equal to (2). So the ideal (2) cannot be factored into a product of primes at all, let alone uniquely so factored. (In fact I seem to recall that any integral domain in which all ideals can be factored into primes *in at least one way* is a Dedekind domain, i.e., the uniqueness of factorization follows from the existence. This is in contrast to factorization of elements into irreducible elements, of course, which is possible in any Noetherian domain but generally not unique.) Also, you can check that the norm of $\mathfrak{p}_2^a$ is 2^a, so for $a > 1$,

$$2^a = N(\mathfrak{p}_2^a) = N((2)^{a-1}\mathfrak{p}_2) \neq N((2)^{a-1}\mathfrak{p}_2) = 2^{2a-1}.$$

In other words, the map $N : \mathcal{I}(\mathbb{Z}[\sqrt{-3}]) \to \mathbb{Z}^+$ is not multiplicative, which is a bit distressing.

Exercise 2.3.2: Let R be an integral domain **with finite quotients**, i.e., such that for each nonzero ideal I, R/I is finite, and define as usual $N(I) = \#R/I$.
a) Show that if R is a Dedekind domain, then $N(IJ) = N(I)N(J)$. (Hint: Use the Chinese Remainder Theorem.)
b) Show that in any case, $N((\alpha)I) = N(\alpha)N(I)$.
c) Use part b) to extend the norm map to a map $N : \mathrm{Frac}(R) \to \mathbb{Q}^+$.
d) Extend the norm map to fractional R-ideals (in the only reasonable way), and show that it satisfies the above properties.

The purpose of the following exercise is to prove a weaker form of the Chinese Remainder Theorem which holds, in particular, for a nonmaximal order in a number field.

Exercise 2.3.3: Recall that a **primary ideal** J in a commutative ring R is one for which the only zero divisors in R/J are nilpotents. (Equivalently, the radical of J is prime.) Suppose that R is a Noetherian domain with finite quotients.
a) Show that every primary ideal has prime power norm.
b) Suppose that $N(K_1) = p^a$, $N(K_2) = p^b$ (i.e., powers of the same prime p). Show that $N(K_1 \cap K_2) = p^c$ for some $c \geq \max(a, b)$.
c) Suppose now that $N(K_1) = p^a$, $N(K_2) = q^b$ for primes $p \neq q$. Show that K_1 and K_2 are coprime, i.e., $K_1 + K_2 = R$.
d) Let I be an ideal of R. Show that there are distinct prime numbers $p_1, \ldots, p_n$,

positive integers $a_1, \ldots, a_n$ and ideals $J_1, \ldots, J_n$ such that $I = J_1 \cdots J_n$, $N(J_i) = p_i^{a_i}$. (Hint: Thanks to work of Noether and Lasker, we are entitled to a **primary decomposition** of I, i.e., a set of primary ideals K_i such that $I = K_1 \cap \cdots \cap K_n$. Collect together all ideals whose norms are powers of a common prime. Finally apply part c) and Exercise 2.3.2.)

What can we say about the quotient monoid $\mathcal{I}(R)/\sim$ of ideals modulo equivalence? We have the identity element 1 which corresponds to the image of every principal ideal, and we just saw that we have a nontrivial class $\epsilon := [\mathfrak{p}_2]$.

Exercise 2.3.4: Let I be an ideal of $R = \mathbb{Z}[\sqrt{-3}]$. By Exercise 2.3.3, I factors as $J_1 \cdot J_2$, where $N(J_1) = 2^a$ and $N(J_2)$ is odd.
a) Show that J_2 is principal.
b) Show that if a is odd, there is exactly one ideal of norm 2^a is $\mathfrak{p}_2^a$, whereas if a is even, there are two: $\mathfrak{p}_2^a$ and $(2)^{\frac{a}{2}}$.
d) Deduce that $Q(R) = \mathcal{I}(R)/\sim\, = \{1, [\mathfrak{p}_2]\}$.

Thus the monoid $Q(R) := \mathcal{I}(R)/\sim$ has a strange structure: it has the identity element 1 and then one further element e which is nontrivial and idempotent: $e^2 = e$. If $f : Q(R) \rightarrow H$ is any monoid map into a commutative group H, we have $f(1) = 1$, $f(e) = f(e^2) = f(e)^2$, hence $f(e) = 1$ – i.e., f is the trivial map. It follows that the group completion $G(Q(R))$ is the trivial group. Notice that this is problematic for us: we wanted a group $\operatorname{Pic}(R)$ together with a monoid homomorphism $\mathcal{I}(R) \rightarrow \operatorname{Pic}(R)$ such that an ideal becomes trivial in $\operatorname{Pic}(R)$ iff it is principal. But we've just carefully checked that that is impossible in the ring $\mathbb{Z}[\sqrt{-3}]$: the nonprincipal ideal $\mathfrak{p}_2$ is an idempotent in the monoid, so will get "cancelled out" upon being mapped into any group.

Well, what's wrong with just looking at the class map $\Phi : \mathfrak{p} \rightarrow \mathcal{I}(R)/\sim$: doesn't this retain all the information we want? Indeed it does, but in some sense it gives more information than we can handle.[5] In particular, recall again that the class map Φ is ridiculously far away from being equidistributed: there is one prime which maps to the idempotent guy e, and every other prime maps to 1.

The point is that something similar is going to happen for any nonmaximal quadratic order $\mathcal{O}$. Namely, the ideal class monoid $Q(\mathcal{O})$ will be a finite commutative monoid which is not a group. Like any commutative monoid, it will have a largest possible subgroup, the group of invertible elements, i.e., the classes of integral ideals which are **invertible** as fractional ideals. This largest subgroup $Q(\mathcal{O})^G$ of $Q(\mathcal{O})$ is the group we want: it is what we shall call the **Picard group** $\operatorname{Pic}(\mathcal{O})$ of the ring $\mathcal{O}$.

This is an important step for us: the commutative group $\operatorname{Pic}(\mathcal{O})$ of a quadratic order will be the primary object of our affections for the remainder of the course. So let us emphasize that what we have shown above is that $\operatorname{Pic}(\mathbb{Z}[\sqrt{-3}])$ is the trivial group. Soon enough we will use quadratic forms to show that for any imaginary quadratic order $\mathcal{O}$, $\operatorname{Pic}(\mathcal{O})$ is finite. In fact this is true for any order in a number

[5] TC: I want the ideal class monoid. JN: **YOU CAN'T HANDLE THE IDEAL CLASS MONOID!**

field, and we will show this, or at least deduce the finiteness from the more standard finiteness of the Picard group of a maximal order, a result we alluded to before.

In particular, for any order in a number field we can consider its **class number** $h(\mathcal{O})$, which is the cardinality of $\operatorname{Pic}(\mathcal{O})$. When $\mathcal{O} = \mathcal{O}_K$ is the maximal order $\operatorname{Pic}(\mathcal{O}_K)$ is often denoted $\operatorname{Cl}(\mathcal{O}_K$ or even $\operatorname{Cl}(K)$, and similarly one often writes simply $h(K)$ for $\# \operatorname{Pic}(\mathcal{O}_K)$ and calls this quantity the **class number of the number field** K.

After a lengthy motivation, let us repeat the definition more crisply in a more general context: for any integral domain R, the Picard group $\operatorname{Pic}(R)$ is the quotient by the group $J(R)$ of **invertible** fractional ideals of R by the subgroup of principal fractional ideals of R. Equivalently, it is the quotient of the monoid of ideals I of R for which there exists an ideal J such that $IJ = (\alpha)$ by the submonoid of principal ideals. The elements of $\operatorname{Pic}(R)$ are usually called ideal classes, with the proviso that they are the equivalence classes not of all ideals in R but only of the "good" (invertible) ideals of R.

This brings us to the key problem: our general definition of $\operatorname{Pic}(R)$ for an arbitrary domain is no more difficult than that of $\operatorname{Pic}(R)$ for a Dedekind domain – in fact it's easier, because for the latter we used the theorem that all ideals of a Dedekind domain are invertible, whereas for an arbitrary ring our definition tells us to just stick with the invertible ones, no matter what. However unless we can acquire some clues as to which ideals – other than principal ones! – are "good" in our domain R, we don't seem to have much hope of understanding or computing $\operatorname{Pic}(R)$.

In complete generality, this does indeed seem to be a stumper (no doubt many substantial papers in commutative algebra have been written on various cases), but for the class of orders $\mathcal{O}$ in number fields – and in fact for the more general class of "almost Dedekind rings" to be introduced sohrtly – we can do much better. In particular, there is a beautiful formula which relates the Picard group of a nonmaximal order to the Picard group of its integral closure (i.e., the full ring of integers).

Exercise 2.3.5:[6] a) Let Q^G be its group of units, and put $Q^B = Q \setminus Q^G$, the set of nonunits. Show that $Q^B Q^B \subset Q^B$ (i.e., Q^B is a sub-semigroup of M) and $Q^B Q^G \subset Q^B$ (once you go bad, there's no turning back).
b) More generally, let M be a commutative monoid and $q : M \rightarrow Q$ be a monoid homomorphism. Define $G_q(M)$ – the q-good guys of M – to be $q^{-1}(Q^G)$ and $B_q(M)$ – the q-bad guys of M – to be $q^{-1}(Q^B)$. Show that again the good guys form a submonoid, the bad guys form a subsemigroup, and $G_q(M) \cdot B_q(M) \subset B_q(M)$.
c) Apply this with $M = I(R)$ the monoid of all integral ideals of a domain R, $Q = Q(R) = I(R)/\sim$ the ideal class monoid, and q the natural quotient map, to conclude: the invertible ideals of R form a submonoid, the noninvertible ideals form a subsemigroup, and invertible times noninvertible is noninvertible.

In the case of $R = \mathbb{Z}[\sqrt{-3}]$, we have our one bad prime $\mathfrak{p}_2$, and it looks to me that the subsemigroup of "bad" (noninvertible) ideals is precisely the set $\mathfrak{p}_2^a$ (i.e.,

[6] Note that, perhaps contrary to appearances, this Exercise is almost trivial.

I have not stopped to give a formal proof...) Thus all the other ideals are "good." But in fact this is still not ideal (so to speak!), because the monoid of all the good guys has a complicated structure: indeed we have the good ideal $2R$ which does not factor uniquely into primes (recall this is because it has norm a power of 2, and hence it could only factor into powers of the bad prime $\mathfrak{p}$, which would mean it isn't good). Every other prime ideal of R is principal, and as above this implies that every ideal of odd norm is principal and factors uniquely into principal primes.

So we see that there is a *second* dichotomy that is complicating the picture: apart from "good" (invertible) and "bad" (noninvertible) there is also factorizable into primes versus non-factorizable. Let's call an ideal which factors into primes **lawful** and an ideal which doesn't **chaotic**. Therefore the ideal $2R$ is *chaotic good*, which is fine for it but we would in fact rather restrict our attention to the *lawful good* ideals. In this case we see that every ideal which is prime to $2R$ is lawful good. Noting that $2R$ is precisely the *conductor* of the order $\mathbb{Z}[\sqrt{-3}]$, this gives us a clue as to what may be going on in general. Here are some basic facts that we shall be able to establish for any order $\mathcal{O}$ in a number field:

(I) The ideals which are prime to the conductor $\mathfrak{f}(\mathcal{O})$ are lawful good.

(II) Every good ideal is equivalent in $\operatorname{Pic}(\mathcal{O})$ to a lawful good ideal, i.e., if I is an invertible $\mathcal{O}$-ideal, there exists a principal $\mathcal{O}$-ideal (α) such that $(\alpha)I$ is coprime to the conductor $\mathfrak{f}$. (Thus so long as we are interested in the Picard group, we can restrict our attention to lawful good ideals.)

(III) Every lawful good ideal factors uniquely into a product of (necesarily lawful!) good prime ideals.

(IV) A prime ideal is bad iff it is not coprime to $\mathfrak{f}$: in particular only finitely many primes are bad.

In summary, if we just restrict our attention to ideals which are coprime to the conductor, then for all practical purposes our nonmaximal order $\mathcal{O}$ is as good as a Dedekind ring. (In some rough sense we are just throwing away the finite set of primes which are not coprime to the conductor, but we are not literally restricting to the corresponding Zariski open subset (i.e., the nonsingular locus): if we did that then $\operatorname{Pic}(\mathcal{O})$ would be a certain localization of the ideal class group of the maximal order – in particular, a smaller group. Wait and see what actually happens!)

But rather than stopping to prove these facts now, we will recast the situation in an even more general context and give the theorems there.

Project: Let $\mathcal{O}$ be an order (possibly nonmaximal) in a number field K.
a) Show that the ideal class monoid $Q(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\sim$ is finite.
b) Compute the ideal class monoid explicitly for some non-maximal orders (quadratic orders would, of course, be the natural place to start, and probably to finish, unless you have some specific ambitions in the case of higher degree). Can you say anything about which finite commutative monoids might arise as ideal class

monoids?

Comments: I don't know how this will turn out. In fact I do not have a proof that the ideal class monoid of an order is always finite, so it is conceivable that it isn't. (That would be much more interesting....) In the case of a maximal order the statement reduces to the assertion that the ideal class *group* of a number field is finite, which is well-known to be both true and nontrivial. My guess is that the proof of this will adapt to the case of nonmaximal orders, the key step being to show that there exists an N depending only on $\mathcal{O}$ such that every ideal in $\mathcal{O}$ is equivalent to an ideal of norm at most N. Therefore this project is a good opportunity for someone who has not had a chance to go through the proof of this basic finiteness result – one of the best ways to make sure you're paying attention throughout the proof of the result is to have the goal of adapting it to prove a different result.

4. The Picard group of an almost Dedekind ring

In this section I am unabashedly following [Neuk, $\S I.12$]. Moreover, some proofs are omitted for now (and were omitted in the lectures.)

Let R be a domain which is Noetherian, one-dimensional, but possibly not integrally closed. Let $\tilde{R}$ be the integral closure of R in its quotient field; by the Krull-Akizuki theorem (Theorem 2), $\tilde{R}$ is a Dedekind domain. It therefore makes some sense to call R a **pre-Dedekind domain**.

We will need to recall the notion of localization of a domain R at a multiplicatively closed subset S of R (i.e., a subset containing 1 and not containing 0 such that $S \cdot S = S$). This is a mild generalization of the quotient field construction: we define R_S to be the set of elements of the quotient field F of the form $\frac{a}{s}$ with $s \in S$. One immediately checks that we have inclusions $R \subset R_S \subset K$. Note that for an ideal I of R, the complement $R \setminus I$ is multiplicatively closed iff I is a prime ideal. So if $\mathfrak{p}$ is prime, we define $R_\mathfrak{p}$ to be the localization at the multiplicative subset $R \setminus \mathfrak{p}$, i.e., we allow as denominators any element not in $\mathfrak{p}$. (The switch to the complement looks confusing at first, but recall that $0 \in \mathfrak{p}$, so we could not really mean to localize at $\mathfrak{p}$.) Note that we recover the usual quotient field construction by localizing at the prime ideal (0). If $\mathfrak{p}$ is any nonzero prime ideal, then the localized ring $R_\mathfrak{p}$ has the nonzero ideal $\mathfrak{p}R_\mathfrak{p}$ as its unique *maximal* ideal, so is a so-called **local ring** (and not a field).

If M is an R-module, then we can also localize R at an arbitrary subset S; one can either give a similar direct construction or construe this as $M_S := R_S \otimes_R M$. When I is an ideal of R, I_S can be viewed as the pushed forward ideal IR_S of R_S.

Theorem 20. *(pre-Dedekind Chinese Remainder Theorem) Let I be an ideal in the pre-Dedekind domain R. Then*

$$R/I \cong \bigoplus_{\mathfrak{p} \in \mathcal{P}} R_\mathfrak{p}/IR\mathfrak{p} \cong \bigoplus_{\mathfrak{p} \supset I} R_\mathfrak{p}/IR_\mathfrak{p}.$$

Theorem 21. *Let R be a Noetherian domain. A fractional ideal I is invertible iff for all maximal ideals $\mathfrak{p}$, $I_\mathfrak{p} = IR_\mathfrak{p}$ is a principal fractional ideal of $R_\mathfrak{p}$.*

Remark: In other words, a fractional ideal of R is invertible iff it is a rank one locally free (= projective, since R is Noetherian) module.

Proof: If I is invertible, there exists J such that $IJ = \alpha R$, so that $1 = \sum_{i=1}^{r} a_i b_i$ with $a_i \in I,\ b_i \in J$. (Note $IJ = R$ implies $a_i b_i \in R$ for all i.) Moreover not all products $a_i b_i$ can lie in the proper ideal $\mathfrak{p}R_{\mathfrak{p}}$. So after reordering we may assume that $a_1 b_1$ is a unit in the local ring $R_{\mathfrak{p}}$. We claim that $I_{\mathfrak{p}}$ is the principal fractional ideal $a_1 R_{\mathfrak{p}}$. Indeed, $a_1 \in I \subset I_{\mathfrak{p}}$, and for $x \in I_{\mathfrak{p}}$, we have $xb_1 \in I_{\mathfrak{p}} J = R_{\mathfrak{p}}$, so $x = xb_1(b_1 a_1)^{-1} a_1 \in a_1 R_{\mathfrak{p}}$.

Conversely, assume that for all $\mathfrak{p}$ the ideal $I_{\mathfrak{p}} = IR_{\mathfrak{p}} = a_{\mathfrak{p}} R_{\mathfrak{p}}$ for some $a_{\mathfrak{p}} \in K^{\times}$. We must show that the fractional ideal $I^* = \{x \in K \mid x\mathfrak{I} \subset R\}$ is the inverse to $\mathfrak{I}$. Our worry is that II^* is too small, i.e., there exists a maximal ideal $\mathfrak{p}$ such that $II^* \subset \mathfrak{p}$. Let $a_1, \ldots, a_n$ be a set of generators for I. Since $a_i \in a_{\mathfrak{p}} R_{\mathfrak{p}}$, we may write it as $a_i = a_{\mathfrak{p}} \frac{b_i}{s_i}$ with $b_i \in R$, $s_i \in R \setminus \mathfrak{p}$. Let us, as usual, clear denominators: put $s = s_1 \cdots s_n$, so that $sa_i \in a_{\mathfrak{p}} R$ for all i, so that $sa_{\mathfrak{p}}^{-1} I \subset R$, and therefore $sa_{\mathfrak{p}}^{-1} \in I^*$. Therefore $s = sa_{\mathfrak{p}}^{-1} a_{\mathfrak{p}} \in I^* I \subset \mathfrak{p}$, contradiction.

Exercise 2.4.1*: a) Let I and J be invertible fractional ideals in the Noetherian domain R. Show that the product fractional ideal IJ is isomorphic, as an R-module, to $I \otimes_R J$. (Hint: there is an obvious map; show that it becomes an isomorphism after localizing at every maximal ideal, which is enough to show that it is an isomorphism.)
b) Show that the inverse fractional ideal I^* is isomorphic to the R-module $\operatorname{Hom}_R(I, R)$.
c) Conclude that $\operatorname{Pic}(R) = \operatorname{Pic}(\operatorname{Spec} R)$ in the sense of algebraic geometry.

Recall that for any domain R we are denoting the invertible fractional ideals by $J(R)$ and the principal fractional ideals by $\operatorname{Prin}(R)$, and the set of nonzero prime ideals by $\mathcal{P}$.

Proposition 22. *Let R be a pre-Dedekind domain. Then the mapping $I \mapsto (IR_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{P}}$ induces an isomorpism of commutative groups*

$$J(R) \xrightarrow{\sim} \bigoplus_{\mathfrak{p} \in \mathcal{P}} \operatorname{Prin}(R_{\mathfrak{p}}).$$

Modding out by globally principal fractional ideals, we get an isomorphism

$$\operatorname{Pic}(R) \xrightarrow{\sim} \left(\bigoplus_{\mathfrak{p} \in \mathcal{P}} \operatorname{Prin}(R_{\mathfrak{p}}) \right) / \operatorname{Prin}(R).$$

Comment: If R is actually a Dedekind domain, then each localization $R_{\mathfrak{p}}$ is a discrete valuation ring, in which the only fractional ideals are integral powers of the principal ideal generated by a uniformizing element $\pi_{\mathfrak{p}}$: $I = (\pi_{\mathfrak{p}})^n$ for $n \in \mathbb{Z}$. Therefore $\operatorname{Prin}(R_{\mathfrak{p}}) \cong \mathbb{Z}$, and we are in fact recovering (or rather, "proving") the unique factorization of fractional ideals into primes. The idea is that if R is only *pre*-Dedekind, then there will be some bad primes $\mathfrak{p}$ such that the one-dimensional Noetherian local ring $R_{\mathfrak{p}}$ is not a DVR (equivalently: it is singular, it is not integrally closed, it is not a PID), and then the situation is more delicate. The strategy will be to compare $\operatorname{Pic}(R)$ with the Picard group $\operatorname{Pic}(\tilde{R})$ of its normalization. This will go smoothly (so to speak) if, and only if, we make the following additional assumption:

Definition: An **almost Dedekind ring** is a one-dimensional Noetherian domain R such that its integral closure $\tilde{R}$ is finitely generated as an R-module.[7]

In our intended application to orders in a number field, $\tilde{R}$ is finitely generated as a $\mathbb{Z}$-module, so it is certainly finitely generated as an R-module. The other important case where this holds is when R is the coordinate ring $k[C]$ of an affine, geometrically integral but possibly singular algebraic curve C over an arbitrary field k. (The fact that finiteness of integral closure does not hold in general is one of the great nightmares of abstract commutative algebra. It does not seem helpful to give an example here, but see e.g. [Kap].

Henceforth we work with an arbitrary almost Dedekind ring R. The first thing that this buys us is that if I is any proper ideal of R, then its pushforward $\tilde{I} := I\tilde{R}$ is a proper ideal of $\tilde{R}$. Indeed, WLOG we may assume that $I = \mathfrak{p}$ is a maximal ideal, and then if $\mathfrak{p}\tilde{R} = \tilde{R}$, then the same holds after tensoring up to $R_{\mathfrak{p}}$: $\frac{\tilde{R}_{\mathfrak{p}}}{\mathfrak{p}\tilde{R}_{\mathfrak{p}}} = 0$, so we are taking a finitely generated (aha!) module over a local ring, modding out by the maximal ideal of that ring, and getting zero. By Nakayama's Lemma, we must have had $\tilde{R} \otimes R_{\mathfrak{p}} = 0$, which is absurd, since the last object is a subring of the quotient field of $\tilde{R}$.

For any prime $\mathfrak{p}$ of R, we may push it forward and then factor it in $\tilde{R}$:

$$\mathfrak{p}\tilde{R} = P_1^{e_1} \cdots P_r^{e_r}.$$

This shows that there is at least one, and only finitely many, prime ideals of $\tilde{R}$ lying over a given prime ideal of R.

Definition: $\mathfrak{f} = \{a \in \tilde{R} \mid a\tilde{R} \subset R\}$, the **conductor** of R. This is at the same time an ideal of $\tilde{R}$ and an ideal of R, and indeed is characterized as the largest such ideal.

Proposition 23. *Since $\tilde{R}$ is finitely generated as an R-module, we have $\mathfrak{f} \neq 0$.*

Exercise 2.4.2: Prove Proposition 23.

In particular, only finitely many prime ideals of $\tilde{R}$ contain $\mathfrak{f}$, hence the same is true for prime ideals in R. These are our bad primes, in the following sense:

Proposition 24. *A prime ideal $\mathfrak{p}$ of R contains the conductor iff the localization $R_{\mathfrak{p}}$ is singular, i.e., is not a DVR. If $\mathfrak{p}$ does not contain the conductor, then $\tilde{\mathfrak{p}} = \mathfrak{p}\tilde{R}$ is a prime ideal of $\tilde{R}$.*

Proof: ...

In other words, the pullback map $\operatorname{Spec}\tilde{R} \to \operatorname{Spec}(R)$ is a bijection outside the finite set of primes which lie over the conductor.

[7] After writing these notes and lecturing on them, I discovered that algebraists already use the term "almost Dedekind ring" for a rather more exotic (non-Noetherian) type of domain. I doubt that confusion will result from this.

Proposition 25. *a) There is an exact sequence*

$$1 \to \frac{\tilde{R}^{\times}}{R^{\times}} \to \bigoplus_{\mathfrak{p} \in \operatorname{Spec} R} \tilde{R}_{\mathfrak{p}^{\times}}/R_{\mathfrak{p}}^{\times} \to \operatorname{Pic} R \to \operatorname{Pic} \tilde{R} \to 1.$$

b) We have

$$\bigoplus_{\mathfrak{p} \in \operatorname{Spec} R} \tilde{R}_{\mathfrak{p}}^{\times}/R_{\mathfrak{p}}^{\times} \cong (\tilde{R}/\mathfrak{f})^{\times})/(R/\mathfrak{f})^{\times}.$$

Corollary 26. *Let $\mathcal{O}$ be an order in the algebraic number field K, with maximal order $\mathcal{O}_K$ and conductor $\mathfrak{f}$. Then the groups $\mathcal{O}_K^{\times}/\mathcal{O}^{\times}$ and $\operatorname{Pic}(\mathcal{O})$ are finite, one one has*

$$\# \operatorname{Pic}(\mathcal{O}) = \frac{\# \operatorname{Pic}(\mathcal{O}_K)}{[\mathcal{O}_K^{\times} : \mathcal{O}^{\times}]} \frac{\#(\mathcal{O}_K/\mathfrak{f})^{\times}}{\#(\mathcal{O}/\mathfrak{f})^{\times}}.$$

References

[Cla65] L. Claborn, *Dedekind domains and rings of quotients.* Pacific Journal, 1965.

[Cla66] L. Claborn, *Every abelian group is a class group.* Pacific Journal, 1966.

[Dino] D. Lorenzini, *An invitation to arithmetic geometry*, AMS.

[Kap] I. Kaplansky, *Commutative rings.* University of Chicago Press, 1974.

[Neuk] J. Neukirch, *Algebraic number theory*, Springer.

[ZS] O. Zariski and P. Samuel, *Commutative Algebra: Volume I.* Springer Graduate Texts in Mathematics 28.