Math 154. Unique factorization in Dedekind domains

1. Background

In class we defined a *Dedekind domain* to be a noetherian domain A that is integrally closed in its fraction field F such that (i) all nonzero prime ideals $\mathfrak{p}$ of A are maximal, and (ii) there exist nonzero maximal ideals.

The condition (ii) is really the same as the condition $A \neq F$. One direction is clear: if A has a nonzero proper ideal (e.g., a nonzero maximal ideal) then A contains a nonzero nonunit, so it is not a field (i.e., $A \neq F$). Conversely, suppose $A \neq F$, so A contains a nonzero nonunit a. Then the ideal (a) of A generated by a is a *proper* ideal. But in *any* noetherian ring, a proper ideal I always lies in a maximal ideal! Indeed, if I is not maximal then it is strictly contained in a proper ideal I', and if I' is not maximal then it is strictly contained in a proper ideal I''', and so on. The noetherian condition on A implies that this process actually must end at some point, which is to say that we reach a maximal ideal that in turn contains the original I!

In this handout, we wish to explain the rest of the proof of unique factorization of nonzero proper ideals into products of finitely many prime ideals (up to rearrangement of the factors) in any such A. In class we proved two key lemmas, and we'll see below that those two lemmas form the technical heart of the argument. Let's recall the two lemmas:

Lemma 1.1. *Any nonzero proper ideal $\mathfrak{a}$ in A contains a finite product $\prod_{i=1}^{n} \mathfrak{p}_i$ for maximal ideals $\mathfrak{p}_i$ ($n \geq 1$).*

Lemma 1.2. *For every maximal ideal $\mathfrak{p}$ of A, the A-submodule*

$$\widetilde{\mathfrak{p}} = \{y \in F \mid y\mathfrak{p} \subseteq A\}$$

satisfies $\mathfrak{p}\widetilde{\mathfrak{p}} = A$.

We recall that the proof of Lemma 1.1 used the noetherian condition and maximality of nonzero prime ideals in an essential way, and the proof of Lemma 1.2 used Lemma 1.1 and integral closedness of A. So already we have used all the key features of the definition of a Dedekind domain. The rest of the argument will be a kind of formal game with these two lemmas.

2. Uniqueness

Uniqueness of prime factorization (granting existence!) will be a quick application of the "cancellation" process provided by Lemma 1.2, much like the proof of the uniqueness aspect of prime factorization in $\mathbf{Z}$:

Proposition 2.1. *If a nonzero proper ideal $\mathfrak{a}$ of A admits two expressions $\prod_{i=1}^{n} \mathfrak{p}_i$ and $\prod_{j=1}^{m} \mathfrak{q}_j$ as products of maximal ideals then necessarily $m = n$ and $\{\mathfrak{p}_i\}$ is a permutation of $\{\mathfrak{q}_j\}$.*

Proof. We proceed by induction on $\min(n, m)$. First suppose the minimum is 1, so by relabeling we may assume $n = 1$. Thus, $\mathfrak{a} = \mathfrak{p}_1$ is a maximal ideal. Consider the expression $\mathfrak{a} = \prod \mathfrak{q}_j$. This is clearly contained in $\mathfrak{q}_1$, so the maximal ideal $\mathfrak{a}$ is contained in the proper ideal $\mathfrak{q}_1$. This forces $\mathfrak{a} = \mathfrak{q}_1$ (so $\mathfrak{p}_1 = \mathfrak{q}_1$). Multiplying the equality $\mathfrak{q}_1 = \mathfrak{a} = \prod_{j=1}^{m} \mathfrak{q}_j$ by $\widetilde{\mathfrak{q}}_1$ gives (by Lemma 1.2 with $\mathfrak{p} = \mathfrak{q}_1$) that $A = \prod_{j=2}^{m} \mathfrak{q}_j$. But this is absurd if $m > 1$, since in such cases the right side lies in $\mathfrak{q}_2$, which is a proper ideal! This settles the case $\min(n, m) = 1$.

Now suppose $\min(n, m) > 1$, and again by symmetry we may assume $n \leq m$. We have

$$\mathfrak{p}_1 \supseteq \prod \mathfrak{p}_i = \prod \mathfrak{q}_j.$$

But we saw in class that if a product of several ideals is contained in a prime ideal then at least one of the given ideals must itself be contained in the prime ideal. (Review the argument if you can't reconstruct it.) Thus, some $\mathfrak{q}_{j_0}$ is contained in $\mathfrak{p}_1$. This is a containment relation among maximal ideals, hence an equality! Relabeling the $\mathfrak{q}$'s, we may assume $j_0 = 1$, which is to say $\mathfrak{p}_1 = \mathfrak{q}_1$.

Letting $\mathfrak{p}$ denote this common maximal ideal, we multiply the equality $\prod \mathfrak{p}_i = \prod \mathfrak{q}_j$ by $\widetilde{\mathfrak{p}}$ and apply Lemma 1.2 (and the "associativity" and "commutativity" of our multiplication operation on pairs of A-submodules of F) to "cancel" the prime ideal $\mathfrak{p}_1 = \mathfrak{q}_1$ to obtain $\prod_{i>1} \mathfrak{p}_i = \prod_{j>1} \mathfrak{q}_j$. This is an equality between a product of $n - 1$ maximal ideals and a product of $m - 1$ maximal ideals, and $\min(n - 1, m - 1) = \min(n, m) - 1$.

Thus, induction now applies to conclude the argument. (Note how the argument constructs the required permutation of factors in the uniqueness statement, at the step where we relabeled to get $j_0 = 1$.) ■

3. Existence

It remains to improve Lemma 1.1 to an equality rather than a containment. For this, the trick is to show that a containment relation $\mathfrak{a} \subseteq \mathfrak{b}$ among nonzero proper ideals in the Dedekind A is the same as a divisibility relation $\mathfrak{b}|\mathfrak{a}$ in the sense of nonzero ideals; i.e., $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for some nonzero ideal $\mathfrak{c}$ in A. Some motivation for this comes from the fact that in any domain R we have $(a) \subseteq (b)$ if and only if $a \in (b)$, which is to say $a = bc$ for some $c \in R$, and this is the same as $(a) = (b)(c)$ for some $c \in R$ (since a unit ambiguity in relating a to bc can be absorbed by replacing c with the corresponding unit multiple without affecting the ideal (c)). In particular, in a PID we see that containment among ideals is the same as a divisibility relation (in the correct direction), best remembered by thinking about the relation between (2) and (10) in $\mathbf{Z}$.

We are going to prove that this property of PID carries over to any Dedekind domain, But beware that in more general domains it is false! For instance, $R = \mathbf{Z}[\sqrt{5}]$ is not a PID, and it is not even Dedekind (since the ring of integers of $\mathbf{Q}(\sqrt{5})$ is slightly bigger), and on HW5 you'll show that despite the containment $2R \subseteq \mathfrak{p} := (2, 1 + \sqrt{5})$ in R we do *not* have $2R = \mathfrak{p}\mathfrak{b}$ for any ideal $\mathfrak{b}$ of R. Here is the key lemma, done "one prime at a time":

Lemma 3.1. *Let $\mathfrak{p}$ be a maximal ideal of A and $\mathfrak{a}$ a nonzero ideal of A. Then $\mathfrak{a} \subseteq \mathfrak{p}$ if and only if $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ for some ideal $\mathfrak{b}$ of A. Moreover, $\mathfrak{a}$ is strictly contained in any such $\mathfrak{b}$.*

Proof. The implication "$\Leftarrow$" is easy (since $\mathfrak{b} \subseteq A$). For the converse, define the A-submodule $\mathfrak{b} := \widetilde{\mathfrak{p}}\mathfrak{a}$ in F. This is an A-submodule of $\widetilde{\mathfrak{p}}\mathfrak{p} = A$ (Lemma 1.2!), so $\mathfrak{b}$ is really an ideal of A. But then

$$\mathfrak{p}\mathfrak{b} = (\mathfrak{p}\widetilde{\mathfrak{p}})\mathfrak{a} = A\mathfrak{a} = \mathfrak{a}$$

where we have again used Lemma 1.2.

It remains to show that for any such expression $\mathfrak{p}\mathfrak{b}$ for $\mathfrak{a}$, necessarily $\mathfrak{a} \neq \mathfrak{b}$. Suppose to the contrary that $\mathfrak{b} = \mathfrak{a}$, so $\mathfrak{a} = \mathfrak{p}\mathfrak{a}$. Then multiplying both sides by $\widetilde{\mathfrak{p}}$ gives (by Lemma 1.2) that $\widetilde{\mathfrak{p}}\mathfrak{a} = \mathfrak{a}$, so all elements of $\widetilde{\mathfrak{p}}$ lie in $\mathrm{Hom}_A(\mathfrak{a}, \mathfrak{a})$. But we saw in class (using Exercise 2 on HW5) that this Hom-module viewed in terms of fraction-multiplication within F is actually equal to A! Thus, we'd get that $\widetilde{\mathfrak{p}} \subseteq A$. However, in class we showed that in fact $\widetilde{\mathfrak{p}}$ is strictly bigger than A. ■

Now we're ready to construct the factorization of a nonzero proper ideal $\mathfrak{a}$ of A into a finite product of maximal ideals. The argument we will use is similar to the proof that a PID is a UFD. As we noted at the start of this handout, $\mathfrak{a}$ lies in *some* maximal ideal $\mathfrak{p}$ (using that A is noetherian). By Lemma 3.1, we can therefore write $\mathfrak{a} = \mathfrak{p}\mathfrak{a}'$ where $\mathfrak{a}'$ strictly contains $\mathfrak{a}$. If $\mathfrak{a}' = A$ then we're done. Otherwise $\mathfrak{a}'$ is a (nonzero) proper ideal, and by running through the preceding argument with $\mathfrak{a}'$ in place of $\mathfrak{a}$ we get $\mathfrak{a}' = \mathfrak{p}'\mathfrak{a}''$ for a maximal ideal $\mathfrak{p}'$ and an ideal $\mathfrak{a}''$ that strictly contains $\mathfrak{a}'$.

If $\mathfrak{a}'' = A$ then we are done: $\mathfrak{a} = \mathfrak{p}\mathfrak{a}' = \mathfrak{p}\mathfrak{p}'$. Otherwise $\mathfrak{a}''$ is a (nonzero) proper ideal and hence $\mathfrak{a}'' = \mathfrak{p}''\mathfrak{a}'''$ for a maximal ideal $\mathfrak{p}''$ and an ideal $\mathfrak{a}'''$ that strictly contains $\mathfrak{a}''$ (and $\mathfrak{a} = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''\mathfrak{a}'''$). Continuing in this way, each time the process does not reach the unit ideal, we pick up another maximal ideal factor and increase our strictly rising chain of ideals in A (i.e., $\mathfrak{a} \subsetneq \mathfrak{a}' \subsetneq \mathfrak{a}'' \subsetneq \dots$). Since A is noetherian, this process cannot go on forever! Thus, eventually we must reach the unit ideal and so have arrived at a factorization of $\mathfrak{a}$ into a product of finitely many maximal ideals of A. This completes the proof of the existence of a prime ideal factorization of every nonzero proper ideal of the Dedekind domain A (and the uniqueness up to rearrangement has been proved above).

4. Applications

To finish, we now record two interesting consequences of the above considerations. The first is a generalization of Lemma 3.1 that is analogous to a result already seen for principal ideals in UFD's:

Proposition 4.1. *If A is a Dedekind domain and $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals of A then $\mathfrak{a} \subseteq \mathfrak{b}$ if and only if $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for an ideal $\mathfrak{c}$ of A. Such an ideal $\mathfrak{c}$ is moreover uniquely determined.*

Proof. If $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for some ideal $\mathfrak{c}$ of A then clearly $\mathfrak{a}$ is contained in $\mathfrak{b}$. Conversely, if such a containment holds then to find $\mathfrak{c}$ we may assume that $\mathfrak{b}$ is a proper ideal (as otherwise we can take $\mathfrak{c} = \mathfrak{a}$). Thus, as for any proper ideal in A, $\mathfrak{b}$ is contained in a maximal ideal $\mathfrak{p}$. Since $\mathfrak{p}$ contains $\mathfrak{b}$ and hence contains $\mathfrak{a}$, by two applications of Lemma 3.1 we can write $\mathfrak{a} = \mathfrak{p}\mathfrak{a}'$ and $\mathfrak{b} = \mathfrak{p}\mathfrak{b}'$ for nonzero ideals $\mathfrak{a}'$ and $\mathfrak{b}'$ in A. Applying multiplication by $\widetilde{\mathfrak{p}}$ to the containment

$$\mathfrak{p}\mathfrak{a}' = \mathfrak{a} \subseteq \mathfrak{b} = \mathfrak{p}\mathfrak{b}'$$

then yields $\mathfrak{a}' \subseteq \mathfrak{b}'$ as ideals in A.

Now consider the unique prime ideals factorizations of $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}'$, and $\mathfrak{b}'$ (unique up to rearrangement, of course). Clearly the *number* of prime ideal factors of $\mathfrak{a}'$ (counted with multiplicity!) is strictly one less than the number for $\mathfrak{a}$, and likewise for $\mathfrak{b}'$ in relation to $\mathfrak{b}$. Thus, if we proceed by induction on the maximum of the number of prime ideal factors of $\mathfrak{a}$ and $\mathfrak{b}$, then this number if smaller for the pair of ideals $\mathfrak{a}'$ and $\mathfrak{b}'$, so by induction we must have $\mathfrak{a}' = \mathfrak{b}'\mathfrak{c}$ for some ideal $\mathfrak{c}$ of A. Multiplying both sides by $\mathfrak{p}$ then gives

$$\mathfrak{a} = \mathfrak{p}\mathfrak{a}' = \mathfrak{p}\mathfrak{b}'\mathfrak{c} = \mathfrak{b}\mathfrak{c}$$

as desired.

Finally, to show that $\mathfrak{c}$ is uniquely determined, consider a hypothetical equality of ideals $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ in A for some unknown $\mathfrak{c}$. Passing to prime ideal factorizations of all three of these ideals, with $\mathfrak{a}$ and $\mathfrak{b}$ known, we see that (i) the prime ideal factors of $\mathfrak{b}$ must be among those of $\mathfrak{a}$, appearing with multiplicity not exceeding the multiplicity in the prime ideal factorization of $\mathfrak{a}$, and (ii) there is exactly one possibility for the prime ideal factorization of $\mathfrak{c}$: its prime ideal factors are only among the ones of $\mathfrak{a}$, and they appear with multiplicity (possibly 0) given by the multiplicity in $\mathfrak{a}$ minus the multiplicity of the same prime ideal factor in $\mathfrak{b}$. This proves that there is at most one possibility for $\mathfrak{c}$, establishing the desired uniqueness. ■

Proposition 4.2. *Let A be a Dedekind domain. Then A is a PID if and only if it is a UFD.*

This result is specific to Dedekind domains: $\mathbf{Q}[x, y]$ is a UFD but not a PID (and also it is not Dedekind: the ideal (x) is nonzero and prime but not maximal).

Proof. Every PID is a UFD, so the interesting direction is the converse: assuming A is a UFD, we seek to show that it is a PID. For this we will use the prime ideal factorization in Dedekind domains. Since every nonzero proper ideal is a product of finitely many maximal ideals, to establish the PID property it suffices to show that all maximal ideals $\mathfrak{p}$ of A are principal! Pick a nonzero element $\alpha \in \mathfrak{p}$, so $(\alpha) \subseteq \mathfrak{p}$. We may assume that this containment is strict (or else we are done). Thus, by Lemma 3.1, $(\alpha) = \mathfrak{p}\mathfrak{b}$ for some nonzero ideal $\mathfrak{b}$ of A, and $\mathfrak{b}$ is a proper ideal (why?). Consider the resulting prime ideal factorization $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$ for some maximal ideals $\mathfrak{p}_j$ $(2 \leq j \leq n)$. This gives

$$(\alpha) = \mathfrak{p} \prod_{j=2}^{n} \mathfrak{p}_j.$$

But A is a UFD, so $\alpha = \pi_1 \cdots \pi_m$ for irreducible elements $\pi_i \in A$, and hence

$$(\alpha) = (\pi_1) \cdots (\pi_m).$$

The UFD property implies that the nonzero principal ideals (π_i) are *prime* ideals. (Warning: this fails in non-UFD's! Recall for instance that in the non-UFD $R = \mathbf{Z}[\sqrt{-5}]$ we have that 3 is irreducible but $3R$ is not prime since it contains the element $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but contains neither of $1 \pm \sqrt{-5}$.) Thus, the two above expressions for (α) as a product involve entirely (nonzero) prime ideals on the right side! The uniqueness of prime ideal factorization therefore implies that the prime ideal factor $\mathfrak{p}$ of (α) must be one of the (π_i)'s, so $\mathfrak{p}$ is principal. ■