Math 210B. Dedekind domains

In class we define a *Dedekind domain* to be an integrally closed noetherian domain A of dimension 1, and we saw several natural examples going beyond the case of PID's. Most importantly, we discussed examples illustrating that a local Dedekind domain is necessarily a PID; i.e., the local Dedekind domains are exactly the local PID's that are not fields. These are called *discrete valuation rings*. In this handout, we prove the preceding fact about local Dedekind domains along with some other basic facts about Dedekind domains and we compute some prime-ideal factorizations in a cubic integer ring.

1. Local Dedekind domains

Let R be a local Dedekind domain. We aim to show that R is a PID. In fact, we will show something more specific, as follows. Consider its nonzero maximal ideal $\mathfrak{m}$. Since $\mathfrak{m}$ is finitely generated as an R-module (as R is noetherian), $\mathfrak{m} \neq \mathfrak{m}^2$ due to Nakayama's Lemma. Thus, we can pick $t \in \mathfrak{m} - \mathfrak{m}^2$.

We shall prove that $\mathfrak{m} = (t)$ and that every nonzero element of R has the form $t^e u$ for a unique $e \geq 0$ and $u \in R^\times$ (see the first two lemmas below). Let's see that this implies R is a PID. Since every ideal in R is finitely generated, as R is noetherian, we just have to show that for any nonzero $a_1, \ldots, a_n \in R$, the ideal $(a_1, \ldots, a_n)$ is principal. We have $a_j = t^{e_j} u_j$ for $e_j \geq 0$ and $u_j \in R^\times$ for each j, so for $e := \min_j e_j \geq 0$ clearly $(a_j) = (t^{e_j}) \subset (t^e)$ for all j with equality for some j. Thus, $(a_1, \ldots, a_n) = (t^e)$ is principal as desired.

We now proceed in two steps, the first being:

Lemma 1.1. *The maximal ideal $\mathfrak{m}$ is equal to (t).*

Proof. Since R is a local domain with dimension 1, its primes (0) and $\mathfrak{m}$ are the only primes (anything else would lie strictly between these and so violate that $\dim R = 1$! Thus, for any nonzero $a \in R$, the local quotient $R/(a)$ therefore has only one prime, namely $\mathfrak{m}/(a)$, so it is local noetherian of dimension 0, which is to say a local artinian ring. In particular, its maximal ideal $\mathfrak{m}/(a)$ is *nilpotent*, say with vanishing Nth power. This says $\mathfrak{m}^N \subset (a)$.

Applying the preceding to $a = t$, we can pick a least $e \geq 0$ (in fact, $e \leq N$) such that $\mathfrak{m}^e \subset (t)$; obviously $e \geq 1$ (since $(t) \subset \mathfrak{m}$). The aim is to prove $e = 1$, so we assume $e \geq 2$ and seek a contradiction. The minimality of e implies that $\mathfrak{m}^{e-1} \not\subset (t)$, so there exists $r \in \mathfrak{m}^{e-1}$ such that $r \notin (t)$. Note that $\mathfrak{m}(r) \subset \mathfrak{m}\mathfrak{m}^{e-1} = \mathfrak{m}^e \subset (t)$, so we have the containments of ideals

$$\mathfrak{m} \subset \{x \in R \,|\, xr \in (t)\} \subsetneq R,$$

where the second containment is strict because it doesn't contain 1 (as $r \notin (t)$ by design of r). But the only ideals between the *maximal* $\mathfrak{m}$ and the entire local ring R are $\mathfrak{m}$ and R (why?), so this forces

$$\mathfrak{m} = \{x \in R \,|\, xr \in (t)\}.$$

It follows that for the fraction $a := r/t \notin R$ (recall $r \notin (t)$!) we have

$$\mathfrak{m} = \{x \in R \,|\, ax \in R\}.$$

Note in particular that the R-submodule $a\mathfrak{m}$ of $\mathrm{Frac}(R)$ is actually contained in R, so it is an *ideal* of R (as ideals of R are exactly R-submodules of R by another name).

We claim that the ideal $a\mathfrak{m}$ of R is not equal to the unit ideal R, so then it must be contained in the unique (!) maximal ideal $\mathfrak{m}$ (i.e., a-multiplication preserves $\mathfrak{m}$). If to the contrary $a\mathfrak{m} = R$ then since $a = r/t$ we would have $t \in r\mathfrak{m}$. But $r \in \mathfrak{m}^{e-1}$ with $e - 1 \geq 1$ (as we are assuming $e \geq 2$), so $r \in \mathfrak{m}$. This would give $t \in r\mathfrak{m} \subset \mathfrak{m}^2$, contradicting how t was originally chosen. Thus, indeed the ideal $a\mathfrak{m}$ of R is a proper ideal, so it is contained in $\mathfrak{m}$.

To finally reach a contradiction (given the earlier assumption $e \geq 2$), we shall exploit at last that R is integrally closed (which has not yet been used). The element $a = r/t \in \mathrm{Frac}(R)$ does not belong to R, so it cannot be integral over R (as R is integrally closed in its own fraction field). But we just saw that a-multiplication preserves the nonzero finitely generated R-module $\mathfrak{m}$. We shall use this latter property to exhibit a as the root of a monic polynomial over R, contradicting that we have seen a cannot be integral over R.

Let $\phi : \mathfrak{m} \to \mathfrak{m}$ be the R-linear map $x \mapsto ax$ (this "makes sense" as an endomorphism of the R-module $\mathfrak{m}$ because of what we have shown about a). As a linear endomorphism of a finitely generated R-module, we know from the handout on generalized Cayley-Hamilton that ϕ satisfies a monic polynomial relation over R. That is,

$$\phi^n + c_{n-1}\phi^{n-1} + \cdots + c_1\phi + c_0 = 0$$

in $\mathrm{End}_R(\mathfrak{m})$ for some $n > 0$ and $c_0, \ldots, c_{n-1} \in R$. Applying this relation any $x \in \mathfrak{m}$, this says that

$$a^n x + c_{n-1}a^{n-1}x + \cdots + c_1 ax + c_0 x = 0$$

in $\mathfrak{m}$ for all $x \in \mathfrak{m}$. But we can pick $x \in \mathfrak{m} - \{0\}$ and so may cancel x in that relation (as R is a domain), yields $f(a) = 0$ in R for $f = T^n + c_{n-1}T^{n-1} + \cdots + c_1 T + c_0 \in R[T]$. This is an integral relation for a over R, which we saw is not possible. ∎

Next, we describe a general nonzero element of R in terms of t:

Lemma 1.2. *If $a \in R$ is nonzero then $a = t^e u$ for a unique $e \geq 0$ and $u \in R^\times$.*

Proof. As at the start of the preceding proof, since $a \neq 0$ we have $\mathfrak{m}^N \subset (a)$ for some $N \geq 0$. Consider $e \geq 0$ such that $a \in \mathfrak{m}^e$ (e.g., $e = 0$ works). We must have $e \leq N$. Indeed, if not then $e \geq N + 1$, so $\mathfrak{m}^N \subset (a) \subset \mathfrak{m}^e \subset \mathfrak{m}^{N+1} \subset \mathfrak{m}^N$, forcing $\mathfrak{m}^N = \mathfrak{m}^{N+1}$. Thus, $\mathfrak{m}^N = (0)$ by Nakayama's Lemma, an absurdity since R is a domain and $\mathfrak{m} \neq 0$. Since $e \leq N$, we can pick a largest e such that $a \in \mathfrak{m}^e = (t^e)$, so $a/t^e \in R - (t) = R - \mathfrak{m}$. Since R is local, $R - \mathfrak{m} = R^\times$. This says exactly that $a = t^e u$ with $u \in R^\times$.

Suppose $a = t^{e'}u'$ for some $e' \geq 0$ and $u' \in R^\times$. We will show $e' = e$, so then $u' = u$ by cancellation. Since $t^{e'}u' = t^e u$, if $e' < e$ or $e' > e$ then by cancellation of the power with the smaller exponent we see that $t^{|e-e'|} \in R^\times$, an absurdity since t is a nonunit and $|e - e'| \geq 1$. ∎

2. Unique factorization in ideals

The central property of Dedekind domains is that their nonzero ideals admit a "unique factorization" property which replaces the UFD condition (and literally recovers the UFD property in the PID case; in HW7 you show that a Dedekind domain is a PID if and only if it is a UFD, in contrast with higher-dimensional rings such as $k[x, y]$ for a field k). This ultimately rests on the fact that local Dedekind domains are discrete valuation rings. The starting point is:

Lemma 2.1. *Let R be a domain with maximal ideal $\mathfrak{m}$, and let $M = \mathfrak{m}R_\mathfrak{m}$ be the maximal ideal of $R_\mathfrak{m}$. Then $R \cap M^e = \mathfrak{m}^e$ for any $e \geq 0$.*

The role of the domain condition is to ensure that the natural map $R \to R_\mathfrak{m}$ is injective, so the intersection $R \cap M^e$ makes sense.

Proof. Elements of $R - \mathfrak{m}$ have unit image in $R/\mathfrak{m}^e$ since they have unit image in the field $R/\mathfrak{m}$, so the natural map

$$R/\mathfrak{m}^e \to (R/\mathfrak{m}^e)_\mathfrak{m} \simeq R_\mathfrak{m}/M^e$$

is an isomorphism of R-modules (and of rings). The R-module annihilator of the right side is $R \cap M^e$ and of the left side is $\mathfrak{m}^e$. ∎

Now we aim to prove the unique factorization theorem:

Theorem 2.2. *Let J be a nonzero ideal in a Dedekind domain A. There is a unique finite product expression $J = \prod_\mathfrak{m} \mathfrak{m}^{e_\mathfrak{m}}$ with exponents $e_\mathfrak{m} \geq 0$ that are positive for at most finitely many $\mathfrak{m}$.*

Proof. Given such a factorization for J, for every maximal ideal $\mathfrak{m}$ of A we have $J_\mathfrak{m} = JA_\mathfrak{m} = M^{e_\mathfrak{m}}$ for the maximal ideal $M = \mathfrak{m}A_\mathfrak{m}$ of $A_\mathfrak{m}$. Since $M^{e+1} \neq M^e$ (by Nakayama's Lemma, due to the non-vanishing and finite generation of M as a module over the local ring $A_\mathfrak{m}$, or because $A_\mathfrak{m}$ is a discrete valuation ring), the ideal M^e determines e for any $e \geq 0$. This establishes the uniqueness: the localization $J_\mathfrak{m}$ as an ideal of $A_\mathfrak{m}$ determines $e_\mathfrak{m}$ for every $\mathfrak{m}$.

For existence, consider the quotient ring A/J. This is a 0-dimensional noetherian ring, so its primes are all maximal and minimal. But a noetherian ring has only finitely many minimal primes (corresponding to the irreducible components of the prime spectrum), so A/J has only finitely many maximal ideals. These have the form $\mathfrak{m}_1/J, \ldots, \mathfrak{m}_n/J$ for maximal ideals $\mathfrak{m}_i$ of A containing J.

For each i, $JA_{\mathfrak{m}_i}$ is a nonzero proper ideal of the discrete valuation ring $A_{\mathfrak{m}_i}$, so it is generated by a unit multiple of some power of a uniformizer. Intrinsically, this says that

$$JA_{\mathfrak{m}_i} = (\mathfrak{m}_i A_{\mathfrak{m}_i})^{e_i} = \mathfrak{m}_i^{e_i} A_{\mathfrak{m}_i}$$

for some $e_i \geq 1$. By the local product decomposition of 0-dimensional noetherian rings in HW6 Exercise 5(ii), we have a natural isomorphism of A-algebras

$$A/J \simeq \prod_i (A/J)_{\mathfrak{m}_i/J} = \prod_i A_{\mathfrak{m}_i}/JA_{\mathfrak{m}_i} \simeq \prod_i A_{\mathfrak{m}_i}/\mathfrak{m}_i^{e_i} A_{\mathfrak{m}_i} \simeq \prod_i A/\mathfrak{m}_i^{e_i}.$$

Now compute the annihilator ideal on both sides: the left side gives J and the right side gives $\cap_i \mathfrak{m}_i^{e_i}$, and this intersection is $\prod \mathfrak{m}_i^{e_i}$ by the Chinese Remainder Theorem. ■

Although the converse to the implication "PID ⇒ UFD" fails for higher-dimensional noetherian UFD's (e.g., $k[t_1, \ldots, t_n]$ for $n > 1$), it holds in the Dedekind case:

Corollary 2.3. *If A is a Dedekind domain that is a UFD then it is a PID.*

Proof. Since every nonzero proper ideal in A is a product of finitely many maximal ideals by the preceding theorem, it suffices to show that each maximal ideal $\mathfrak{m}$ of A is prime. Pick a nonzero $a \in \mathfrak{m}$. By the UFD property, we can write $a = \pi_1 \cdots \pi_n$ for irreducible π_j. Since $\mathfrak{m}$ is prime, some π_j must belong to $\mathfrak{m}$ since a does. But the UFD property implies that for any irreducible $\pi \in A$ the ideal (π) is *prime*, yet the nonzero primes of A are maximal since A is a 1-dimensional domain, so the inclusion $(\pi_j) \subset \mathfrak{m}$ of ideals is an equality. ■

Remark 2.4. Here is an amusing consequence of unique factorization: for a Dedekind domain A, a pair of nonzero ideals J and J' satisfy $J \subset J'$ if and only if $J = IJ'$ for a nonzero ideal I of A (as if we were working in a PID!). The implication "⇐" is true in any commutative ring, so the interesting fact is the converse.

To prove this, suppose $J \subset J'$. Thus, for all maximal ideals $\mathfrak{m}$ of A we have $J_{\mathfrak{m}} \subset J'_{\mathfrak{m}}$ as ideals of the discrete valuation ring $A_{\mathfrak{m}}$. In other words, if $e_{\mathfrak{m}}$ and $e'_{\mathfrak{m}}$ denote the multiplicities with which $\mathfrak{m}$ appears in the prime ideal factorization of J and J' respectively and if $M = \mathfrak{m}A_{\mathfrak{m}}$ is the maximal ideal of $A_{\mathfrak{m}}$ then $M^{e_{\mathfrak{m}}} \subset M^{e'_{\mathfrak{m}}}$, so clearly $e_{\mathfrak{m}} \geq e'_{\mathfrak{m}}$ (hint: $M = t_{\mathfrak{m}} A_{\mathfrak{m}}$ for a nonzero nonunit $t_{\mathfrak{m}}$). Hence, it makes sense to define

$$I = \prod_{\mathfrak{m}} \mathfrak{m}^{e'_{\mathfrak{m}} - e_{\mathfrak{m}}}$$

(in the sense that the exponents are non-negative, and all but finitely many vanish) and then $J'I$ and J coincide since they have the same factorization as a finite product of maximal ideals of A.

3. A non-quadratic example

In class we discussed how to factorize $p\mathscr{O}_K$ into a product of prime ideals for a positive prime $p \in \mathbf{Z}$ and a number field K such that $\mathscr{O}_K$ is monogenic over $\mathbf{Z}$. We also gave out some such K with degree 2 over $\mathbf{Q}$. Let's now explore a cubic number field.

Let $K = \mathbf{Q}(\alpha)$ with $\alpha^3 + 10\alpha + 1 = 0$. The cubic polynomial $f = X^3 + 10X + 1 \in \mathbf{Z}[X]$ is irreducible over $\mathbf{Q}$ because it does not have a rational root, and $\mathbf{Z}[\alpha]$ is an order in $\mathscr{O}_K$. A direct calculation shows $\mathrm{disc}(\mathbf{Z}[\alpha]/\mathbf{Z}) = -4027$, and this is prime. Hence, $\mathscr{O}_K = \mathbf{Z}[\alpha]$ is monogenic and so our prime factorization technique is applicable.

Consider $p = 2$. Since

$$X^3 + 10X + 1 \equiv (X+1)(X^2 + X + 1) \bmod 2$$

is the irreducible factorization in $\mathbf{F}_2[X]$, by using the obvious lifts of these monic irreducibles to $\mathbf{Z}[X]$ we get that $2\mathscr{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ for prime ideals $\mathfrak{P}_1 = (2, \alpha + 1)$ and $\mathfrak{P}_2 = (2, \alpha^2 + \alpha + 1)$, with respective residue fields $\mathbf{F}_2$ and $\mathbf{F}_4$.

Next, consider $p = 4027$. In this case, one finds

$$X^3 + 10X + 1 \equiv (X + 2215)^2(X + 3624) \bmod 4027$$

in $\mathbf{F}_{4027}[X]$. Using the obvious lifts of these monic linear factors to $\mathbf{Z}[X]$, we get $4027\mathscr{O}_K = \mathfrak{Q}_1^2\mathfrak{Q}_2$ for primes $\mathfrak{Q}_1 = (4027, \alpha + 2215)$ and $\mathfrak{Q}_2 = (4027, \alpha + 3624)$. Both $\mathfrak{Q}_i$'s have residue field $\mathbf{F}_{4027}$.