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 $m$. Since $m$ is finitely generated as an $R$-module (as $R$ is noetherian), $m \neq m^2$ due to Nakayama’s Lemma. Thus, we can pick $t \in m - m^2$.

We shall prove that $m = (t)$ and that every nonzero element of $R$ has the form $t^n u$ 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 $(a_j) = (t^e) \subset (t^e)$ 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 $m$ is equal to $(t)$.

Proof. Since $R$ is a local domain with dimension 1, its primes $(0)$ and $m$ 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 $m/(a)$, so it is local noetherian of dimension 0, which is to say a local artinian ring. In particular, its maximal ideal $m/(a)$ is nilpotent, say with vanishing $N$th power. This says $m^N \subset (a)$.

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

$$m \subset \{ x \in R \mid xr \in (t) \} \subset R,$$

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

$$m = \{ x \in R \mid xr \in (t) \}.$$

It follows that for the fraction $a := r/t \not\in R$ (recall $r \not\in (t)$!) we have

$$m = \{ x \in R \mid ax \in R \}.$$

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

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 $a = r/t \in \text{Frac}(R)$ 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 $m$. 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 $R$. 1
Let $\phi : m \to m$ be the $R$-linear map $x \mapsto ax$ (this “makes sense” as an endomorphism of the $R$-module $m$ 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 $\phi$ 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 $\text{End}_R(m)$ for some $n > 0$ and $c_0, \ldots, c_{n-1} \in R$. Applying this relation any $x \in m$, this says that

$$a^n x + c_{n-1}a^{n-1}x + \cdots + c_1ax + c_0x = 0$$

in $m$ for all $x \in m$. But we can pick $x \in m - \{0\}$ and so may cancel $x$ in that relation (as $R$ is a domain), yields $f(a) = 0$ in $R$ for $f = T^n + c_{n-1}T^{n-1} + \cdots + c_1T + c_0 \in R[T]$. 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 $a = t^eu$ 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 $m^N \subset (a)$ for some $N \geq 0$. Consider $e \geq 0$ such that $a \in m^e$ (e.g., $e = 0$ works). We must have $e \leq N$. Indeed, if not then $e \geq N + 1$, so $m^N \subset (a) \subset m^e \subset m^{N+1} \subset m^N$, forcing $m^N = m^{N+1}$. Thus, $m^N = (0)$ by Nakayama’s Lemma, an absurdity since $R$ is a domain and $m \neq 0$. Since $e \leq N$, we can pick a largest $e$ such that $a \in m^e = (t^e)$, so $a/t^e \in R - (t) = R - m$. Since $R$ is local, $R - m = R^\times$. This says exactly that $a = t^eu$ 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 $t^{e'}u' = t^eu$, if $e' < e$ or $e' > e$ then by cancellation of the power with the smaller exponent we see that $t^{e-e'}u \in R^\times$, 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 $m$, and let $M = mR_m$ be the maximal ideal of $R_m$. Then $R \cap M^e = m^e$ for any $e \geq 0$.

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

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

$$R/m^e \to (R/m^e)_m \simeq R_m/M^e$$

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 $m^e$.

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 $J = \prod_m m^{e_m}$ with exponents $e_m \geq 0$ that are positive for at most finitely many $m$.

**Proof.** Given such a factorization for $J$, for every maximal ideal $m$ of $A$ we have $J_m = JA_m = M^{e_m}$ for the maximal ideal $M = mA_m$ of $A_m$. Since $M^{e_{m+1}}$ is not $M^e$ (by Nakayama’s Lemma, due to the non-vanishing and finite generation of $M$ as a module over the local ring $A_m$, or because $A_m$ is a discrete valuation ring), the ideal $M^e$ determines $e$ for any $e \geq 0$. This establishes the uniqueness: the localization $J_m$ as an ideal of $A_m$ determines $e_m$ for every $m$. 


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 $m_1/J, \ldots, m_n/J$ for maximal ideals $m_i$ of $A$ containing $J$.

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

$$JA_{m_i} = (m_iA_{m_i})^{e_i} = m_i^{e_i}A_{m_i},$$

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

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

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

Although the converse to the implication “PID $\Rightarrow$ 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 $m$ of $A$ is prime. Pick a nonzero $a \in m$. By the UFD property, we can write $a = \pi_1 \cdots \pi_n$ for irreducible $\pi_j$. Since $m$ is prime, some $\pi_j$ must belong to $m$ since $a$ does. But the UFD property implies that for any irreducible $\pi \in A$ the ideal $(\pi)$ is prime, yet the nonzero primes of $A$ are maximal since $A$ is a 1-dimensional domain, so the inclusion $(\pi_j) \subset m$ 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 $J = JJ'$ for a nonzero ideal $I$ of $A$ (as if we were working in a PID!). The implication “$\Leftarrow$” 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 $m$ of $A$ we have $J_m \subset J'_m$ as ideals of the discrete valuation ring $A_m$. In other words, if $e_m$ and $e'_m$ denote the multiplicities with which $m$ appears in the prime ideal factorization of $J$ and $J'$ respectively and if $M = mA_m$ is the maximal ideal of $A_m$ then $M^{e_m} \subset M^{e'_m}$, so clearly $e_m \geq e'_m$ (hint: $M = t_mA_m$ for a nonzero nonunit $t_m$). Hence, it makes sense to define

$$I = \prod_m m^{e'_m - e_m}$$

(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 $p\mathcal{O}_K$ into a product of prime ideals for a positive prime $p \in \mathbb{Z}$ and a number field $K$ such that $\mathcal{O}_K$ is monogenic over $\mathbb{Z}$. We also gave out some such $K$ with degree 2 over $\mathbb{Q}$. Let’s now explore a cubic number field.

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

Consider $p = 2$. Since

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

we have $2\mathcal{O}_K = (2)\mathcal{O}_K = \mathcal{O}_K$. Moreover, $p\mathcal{O}_K$ is a product of prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ with $\mathfrak{p}_1^{e_1}$, $\mathfrak{p}_2^{e_2}$, and $\mathfrak{p}_3^{e_3}$ such that $2 = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$ and $2\mathcal{O}_K = (2)$.

For each prime $\mathfrak{p}$ above 2, let $f_{\mathfrak{p}}$ be the quadratic polynomial $f_{\mathfrak{p}}(X)$ such that $f_{\mathfrak{p}}(X)$ is monic and $\mathfrak{p}f_{\mathfrak{p}}(X)$ is irreducible. Then $\mathfrak{p}^{e_{\mathfrak{p}}}f_{\mathfrak{p}}(X) \equiv 0 \mod 2$. Since $2 = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$, we have $2 = 2\mathfrak{p}_1^{e_{\mathfrak{p}}_1}\mathfrak{p}_2^{e_{\mathfrak{p}}_2}\mathfrak{p}_3^{e_{\mathfrak{p}}_3}$, and hence $e_{\mathfrak{p}}_1 = e_{\mathfrak{p}}_2 = e_{\mathfrak{p}}_3 = 1$.

Thus, $2\mathcal{O}_K = (2)\mathcal{O}_K = \mathcal{O}_K$. Moreover, $p\mathcal{O}_K$ is a product of prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ with $\mathfrak{p}_1^{e_1}$, $\mathfrak{p}_2^{e_2}$, and $\mathfrak{p}_3^{e_3}$ such that $2 = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$ and $2\mathcal{O}_K = (2)$.
is the irreducible factorization in $\mathbb{F}_2[X]$, by using the obvious lifts of these monic irreducibles to $\mathbb{Z}[X]$ we get that $2\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ for prime ideals $\mathfrak{P}_1 = (2, \alpha + 1)$ and $\mathfrak{P}_2 = (2, \alpha^2 + \alpha + 1)$, with respective residue fields $\mathbb{F}_2$ and $\mathbb{F}_4$.

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

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

in $\mathbb{F}_{4027}[X]$. Using the obvious lifts of these monic linear factors to $\mathbb{Z}[X]$, we get $4027\mathcal{O}_K = \Omega_1^2\Omega_2$ for primes $\Omega_1 = (4027, \alpha + 2215)$ and $\Omega_2 = (4027, \alpha + 3624)$. Both $\Omega_i$'s have residue field $\mathbb{F}_{4027}$. 