Math 430 Tom Tucker
NOTES FROM CLASS 09/08/21

Earlier we said that we wanted to show that $\mathcal{O}_K$ had many of the same properties as $\mathbb{Z}$. What we will in fact show is that $\mathcal{O}_K$ is something called a *Dedekind domain*. A Dedekind domain is a simple kind of ring. Let us first define an even simpler kind of ring, a *discrete valuation ring*, frequently called a DVR.

Definition 4.1. A discrete valuation on a field K is a surjective homomorphism from K^* onto the additive group of $\mathbb{Z}$ such that

(1) $v(xy) = v(x) + (y)$;

(2) $v(x + y) \geq \min(v(x), v(y))$.

By convention, we say that $v(0) = \infty$.

Remark 4.2. Note that it follows from property 2 that if $v(x) > v(y)$, then $v(x + y) = v(y)$. To prove this we note that $v(-x) = v(x)$ and $v(y) = v(-y)$, so we have

$$v(y) \geq \min(v(x + y), v(-x)) \geq v(x + y)$$

since $v(x) > v(y)$. Since $v(x+y) \geq \min(v(x), v(y))$ also, we must have $v(x + y) = v(y)$.

Example 4.3. Let v_p be the p-adic valuation on $\mathbb{Q}$. That is to say that $v_p(a)$ is the largest power dividing a for $a \in \mathbb{Z}$ and $v_p(a/b) = v_p(a) - v_p(b)$ for $a, b \in \mathbb{Z}$.

Definition 4.4. A discrete valuation R ring is a set of the form

$$\{a \in K \mid v(a) \geq 0\}$$

How can we identify a DVR? The following will help.

A couple remarks first:

(1) If I and J are principal then so is IJ. In particular, any power of a principal ideal is principal.

(2) Notation: for any ideal I of R, we say $I^0 = R$.

Proposition 4.5. *Let R be a Noetherian local domain of dimension 1 with maximal ideal $\mathcal{M}$ and with $R/\mathcal{M} = k$ its residue field. Then the following are equivalent*

(1) *R is a DVR;*
(2) *R is integrally closed;*
(3) *$\mathcal{M}$ is principal;*

(4) *there is some $\pi \in R$ such that every element $a \in R$ can be written uniquely as $u\pi^n$ for some unit u and some integer $n \geq 0$;*
(5) *every nonzero ideal is a power of $\mathcal{M}$.*

Proof. ($1 \Rightarrow 2$) Suppose that $b \in K \setminus R$. Then $v(b) < 0$, so for any monic polynomial in b with coefficients in R, we have

$$v(b^n + a_n b^{n-1} + \cdots + a_0) = v(b^n) < 0,$$

which means that $b^n + a_n b^{n-1} + \cdots + a_0 \neq 0$.

($2 \Rightarrow 3$) Let $a \in \mathcal{M}$. There is some n for which $\mathcal{M}^n \subseteq (a)$ (by "weak factorization" in Noetherian rings) but $\mathcal{M}^{n-1}$ is not contained in (a) (note $n-1$ could be zero). Let $b \in \mathcal{M}^{n-1} \setminus (a)$ and let $x = a/b$. We can show that $\mathcal{M} = Rx$. This is equivalent to showing that $x^{-1}\mathcal{M} = R$. Note that since (b) is not in (a), $b/a = x^{-1}$ cannot be in R. Hence, it cannot be integral over R. By Cayley-Hamilton, $x^{-1}\mathcal{M} \neq \mathcal{M}$ since $\mathcal{M}$ is finitely generated as an R-module and $x^{-1} \notin R$ and R is integrally closed. Since $x^{-1}\mathcal{M}$ is an R-module and $x^{-1}\mathcal{M} \subseteq R$ (this follows from the fact that $b\mathcal{M} \subseteq \mathcal{M}^n \subseteq (a)$), this means that $x^{-1}\mathcal{M}$ is an ideal of R not contained in $\mathcal{M}$. So $x^{-1}\mathcal{M} = R$, as desired.

($3 \Rightarrow 4$) Let π generate $\mathcal{M}$. Now, let $a \in R$. We define $w(a)$ to be the smallest n for which $\mathcal{M}^n \subseteq Ra$; such an n exists by "weak factorization" in Noetherian rings. We will show by induction that that a can be written as $u\pi^{w(a)}$ for some unit u. The case $w(a) = 0$ is trivial, since $w(a) = 0$ means a is a unit. If $w(a) \geq 1$, then $a \in \mathcal{M}$. Then we can write $a = \pi b$ for some b. Since, any element in $\mathcal{M}^n$, which is simply the set of $z\pi^n$ for $z \in R$, can be written as xa for some $x \in R$, any element $z\pi^{w(a)-1}$ in $\mathcal{M}^{w(a)-1}$ can be written as xb for that same x. Hence $w(b) \leq w(a) - 1$. By the same reasoning, $w(b) \geq w(a) - 1$. Hence $w(b) = w(a) - 1$. So we can write b uniquely as $u\pi^{w(b)}$ for some unit u, which gives $a = u\pi^{w(a)}$ uniquely.

($4 \Rightarrow 5$) Let I be an ideal of R. Since I is finitely generated, it has generators $m_1, \ldots, m_n$ which can all be written as $u_i \pi^{t_i}$. Then the i for which t_i is smallest will generate I from above.

($5 \Rightarrow 1$) Let $a \in R$. Then $Ra = \mathcal{M}^n$ for some unique n. Letting $v(a) = n$ gives the desired valuation.

□

Example 4.6. The ideal $\mathcal{P}$ generated by 2 and $\sqrt{5} - 5$ in $\mathbb{Z}[\sqrt{5}]$ is prime but $\mathbb{Z}[\sqrt{5}]_{\mathcal{P}}$ is not a DVR. More on this later.

Definition 4.7. Dedekind domain is a Noetherian domain R such that $R_{\mathcal{P}}$ is a DVR for every nonzero prime $\mathcal{P}$ of R.

The ideal structure is a bit more complicated than that of a DVR. Recall that in any noetherian ring R for every ideal I we can write $\prod_{i=1}^{n} \mathcal{P}_i \subseteq I$ with $\mathcal{P}_i \supseteq I$. We'll prove that in a Dedekind domain we can write get an inequality and get it uniquely.

One more thing: we'll want to work in Noetherian domains of (Krull) dimension 1 more generally, as you'll see later. So we'll try to state results for them when possible.

To understand how to factorize an ideal I, we'll want to understand R/I. To help us with this we'll want the Chinese remainer theorem.

The Chinese remainder theorem really consists of writing 1 in a lot of different ways. Let's prove the following easy Lemma.

Lemma 4.8. *Let I and J be ideals in R. Suppose that $I + J = 1$. Then*

(1) *$I \cap J = IJ$; and*
(2) *for any positive integers m, n, we have $I^m + J^n = 1$.*

Proof. Since $I + J = 1$, we can write $a + b = 1$ for $a \in I$ and $b \in J$. Now 1. follows from the fact that for if $x \in I \cap J$, then $x = (a + b)x = ax + bx \in IJ$, so $I \cap J \subseteq IJ$. The reverse inclusion $IJ \cup I \cap J$ is obvious. To prove 2., we simply write $(a + b)^{2(m+n)} = 1$, and note that the expansion of $(a + b)^{2(m+n)}$ consists entirely of elements in either $I^{m+n} \subseteq I^m$ or $J^{m+n} \subseteq J^n$. □

Lemma 4.9. *Let I and J be ideals of R and suppose that $I + J = 1$. Then the natural map*

$$\phi : R \longrightarrow R/I \oplus R/J$$

is surjective with kernel IJ.

Proof. The kernel is $I \cap J$ which equals IJ from the Lemma above. Now, to see that it is surjective, write $a + b = 1$ with $a \in I$ and $b \in J$. Then $b = 1 - a$ and $\phi(b) = (1, 0)$ and $\phi(a) = (0, 1)$. Since $\phi(R)$ is clearly a $R/I \oplus R/J$ module and $R/I \oplus R/J$ is generated by $(1, 0)$ and $(0, 1)$ as an $R/I \oplus R/J$ module, ϕ must be surjective. □