Math 430 Tom Tucker
NOTES FROM CLASS 09/20/21

There were some questions about the proof of unique factorization in Dedekind domains. I went over that the beginning, and also here's something very similar to get the flavor of these types of arguments.

Theorem 7.1. *Suppose that R is Dedekind. Then every ideal in R can be generated by two elements.*

Proof. Let I be an ideal of R and let $x \in I$. Then $R/(x)$ is a direct sum of rings of the form $R_{\mathfrak{p}}/R_{\mathfrak{p}}\mathfrak{p}^e$. All such rings have only principal ideal so any ideal of $R/(x)$ is principal. Let $\varphi : R \longrightarrow R/(x)$ and let $\varphi(y)$ generate $\varphi(I)$. Then $I = Rx + Ry$. □

We make the following definitions

$$\mathbf{F}(R) \text{ is the set of invertible fractional ideals of } R$$

$$\mathbb{P}(R) \text{ is the set of principal fractional ideals of } R$$

and

$$\mathrm{Pic}(R) = \mathbf{F}(R)/\mathbb{P}(R).$$

$\mathrm{Pic}(R)$ is called the Picard group of R.

We will show that if R is a DVR, then all of the fractional ideals of R are invertible. We'll also want a few facts about invertible ideals.

Lemma 7.2. *Let J be a finitely generated fractional ideal of an integral domain R with field of fractions K and let S be a multiplicative set S in R not containing 0. Then $S^{-1}R(R : J) = (S^{-1}R : S^{-1}RJ)$.*

Proof. Since $xJ \subseteq R$ implies that $\frac{x}{s}J \subseteq S^{-1}R$ for any $s \in S$ it is clear that $S^{-1}R(R : J) \subseteq (S^{-1}R : S^{-1}RJ)$. To get the reverse inclusion, let $y \in (S^{-1}R : S^{-1}RJ)$ and let $m_1, \ldots, m_n$ generate J as an R-module. Since $yS^{-1}RJ \subseteq S^{-1}R$, we must have $ym_i \subset S^{-1}R$, so we can write $ym_i = r_i/s_i$ where $r_i \in R$ and $s_i \in S$. Since $(s_1 \cdots s_n y)m_i = (\prod_{j \neq i} s_j)r_i \in R$, this means that $s_1 \cdots s_n y \in (R : J)$. Thus, $y \in S^{-1}R(R : J)$. □

A note on definitions: Fractional ideals are not generally always assume to be finitely generated.

All invertible ideals are automatically finitely generated, though.

Lemma 7.3. *Let J be a fractional ideal of an integral domain R. Then J is invertible $\Leftrightarrow$ J is finitely generated and $R_{\mathfrak{m}}J$ is an invertible fractional ideal of $R_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of R.*

Proof. ($\Rightarrow$) Let J be an invertible ideal ideal of R. Then we can write

$$\sum_{i=1}^{k} n_i m_i = 1$$

with $n_i \in (R : J)$. Since $n_i J \in R$ for each i, we can write any $y \in J$ as $\sum_{i=1}^{k}(n_i y)m_i = y$, so the m_i generate J. Hence, J is finitely generated. Let $\mathfrak{m}$ be a maximal ideal of R. Since we can write $J(R : J) = R$ we must have $R_\mathfrak{m}(J(R : J)) = R_\mathfrak{m}$, so $(R_\mathfrak{m}J)(R_\mathfrak{m}(R : J)) = R_\mathfrak{m}$, so $R_\mathfrak{m}J$ is invertible

($\Leftarrow$) For any ideal J, we can form $J(R : J) \subseteq R$ (not necessarily equal to R). This will be an ideal I of R. Let $\mathfrak{m}$ be a maximal ideal of R. Since J is finitely generated by assumption, we can apply the Lemma immediately above to obtain $(R_\mathfrak{m} : R_\mathfrak{m}J) = R_\mathfrak{m}(R : J)$. Hence, we have $R_\mathfrak{m}J(R : J) = R_\mathfrak{m}$. Thus the ideal $I = J(R : J)$ is not contained in any maximal ideal of R. Thus, $I = R$ and J is invertible. □

Theorem 7.4. *Let R be a a local integral domain of dimension 1. Then R is a DVR $\Leftrightarrow$ every nonzero ideal (note: I didn't say fractional ideal) of R is invertible.*

Proof. ($\Rightarrow$) If J is a fractional ideal, then $xJ \subset R$ for some $x \in R$. Hence $xJ = Ra$ for some $a \in R$ since a DVR is PID. Thus, $J = Rax^{-1}$. Clearly $(R : J) = Ra^{-1}x$ and $J(R : J) = 1$, so J is invertible.

($\Leftarrow$) Since every nonzero ideal $I \subset R$ is invertible, every ideal of R is finitely generated, so R is Noetherian. Now, it will suffice to show that every nonzero ideal in R is a power of the maximal ideal $\mathfrak{m}$ of R. The set of ideals I of R that are not a power of $\mathfrak{m}$ (note: we consider R to $\mathfrak{m}^0$, so the unit ideal is considered to be a power of $\mathfrak{m}$) has a maximal element if it is not empty. Then $(R : \mathfrak{m})I \neq I$ since if $(R : \mathfrak{m})I = I$, then $\mathfrak{m}I = I$ which means that $I = 0$ by Nakayama's Lemma (note that R must be Noetherian since all fractional ideals are invertible). Since $(R : \mathfrak{m})I \supseteq I$ (since $1 \in (R : \mathfrak{m})$), this means that $(R : \mathfrak{m})I$ is strictly larger than I, and is thus a power of $\mathfrak{m}$, so $(R : \mathfrak{m})I\mathfrak{m}$ is also a power of $\mathfrak{m}$.

□

Now, we have the global counterpart.

Theorem 7.5. *Let R be a integral domain of dimension 1. Then R is a Dedekind domain $\Leftrightarrow$ every fractional ideal of R is invertible.*

Proof. ($\Rightarrow$) Let J be a fractional ideal of R. Then, for every maximal ideal $\mathfrak{m}$, it is clear that $R_\mathfrak{m}J$ is a fractional ideal of $R_\mathfrak{m}$. Since $R_\mathfrak{m}$ is a DVR, $R_\mathfrak{m}J$ must be therefore be invertible for every maximal ideal

$\mathfrak{m}$. Moreover, J must be finitely generated since there is an $x \in K$ for which xJ is an ideal of R and every ideal of R is finitely generated since R is Noetherian. Therefore, J must be invertible by a Lemma 7.3.

($\Leftarrow$) Since every ideal of R is invertible, every ideal of R is finitely generated, so R is Noetherian. So it's enough to show that $R_{\mathfrak{p}}$ is a DVR for all nozero primes $\mathfrak{p}$. Let J be an ideal of $R_{\mathfrak{p}}$ and let $I = J \cap R$. Then I is invertible so $R_{\mathfrak{p}} I = J$ is invertible by Lemma 7.3.. Thus $R_{\mathfrak{p}}$ is a DVR by Theorem 7.4.

□

Let's show that not only can every ideal I of a Dedekind domain R be factored uniquely, but so can every fractional ideal J of a Dedekind domain. Since every nonzero prime is invertible in R, we can write $\mathfrak{p}^{-1} = (R : \mathfrak{p})$ for maximal $\mathfrak{p}$ (by the way nonzero prime means the same thing as maximal in a 1-dimensional integral domain of course).

Proposition 7.6. *Let R be a Dedekind domain. Then every fractional ideal J of R has a unique factorization as*

$$J = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$$

with all the $e_i \neq 0$.

Proof. To see that J has some factorization as above we note xJ is an ideal I in R. So if we factor Rx and I and write $J = (x)^{-1} I$, we have a factorization. To see that the factorization is unique we write

$$I = (\prod_{i=1}^{n} \mathfrak{p}_i^{e_i})(\prod_{j=1}^{m} \mathcal{Q}_j^{-f_j})$$

with all the e_i and f_j positive and no $\mathcal{Q}_j$ equal to any $\mathfrak{p}_i$. Let $I = \prod_{j=1}^{m} \mathcal{Q}_j^{f_j}$ Then JI^2 is an ideal of R with $JI^2 = (\prod_{i=1}^{n} \mathfrak{p}_i^{e_i})(\prod_{j=1}^{m} \mathcal{Q}_j^{f_j})$. Since I^2 has a unique factorization and so does JI^2, so must J have a unique factorization. □

Back to showing that $\mathcal{O}_K$ is Dedekind. All we need is to do is show that $\mathcal{O}_K$ is Noetherian and one-dimensional. For R-modules (R a ring), it is easy to see that M satisfies the Noetherian ascending chain condition if and only if every submodule of M is finitely generated (as an R-module).

Proposition 7.7. *Let R be a ring, let M' and M'' be Noetherian R-modules and let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of R-modules. Then M is Noetherian.

Proof. We denote the map from M' into M as i and the map from M to M'' as ϕ. It will suffice to show that every submodule N of M is finitely generated. Since $\phi(N)$ is a submodule N of M'' it is finitely generated by, say, $x_1, \dots, x_m$. Since $N \cap i(M')$, which we denote as N', is a submodule of $i(M')$, it is finitely generated by, say, $y_1, \dots, y_n$. For each x_i, let $z_i \in N$ have the property that $\phi(z_i) = x_i$ and let N'' be the module they generate in N. Then N is generated by $y_1, \dots, y_n, z_1, \dots, z_m$ since given any $t \in N$ we can write $\phi(t) = \sum_{i=1}^{m} r_i \phi(z_i)$, so

$$\phi(t) - \sum_{i=1}^{m} r_i z_i \in N \cap i(M),$$

and $N = N' + N''$. □

Corollary 7.8. *Let A be a Noetherian ring and let M be a finitely generated A-module. Then M is a Noetherian A-module*

Proof. We proceed by induction on the number of generators of M as an A-module. If M has one generator, then it is isomorphic to some quotient of A, so we're done. Otherwise, let $x_1, \dots, x_n$ generate M and write

$$0 \longrightarrow Rx_n \longrightarrow M \longrightarrow M/(Rx_n) \longrightarrow 0.$$

Then $M/(Rx_n)$ is generated by the images of $x_1, \dots, x_{n-1}$, so must be Noetherian by the inductive hypothesis. By the Lemma above, M must be Noetherian. □

Corollary 7.9. *Let A be a Noetherian ring and let $B \supseteq A$ be finitely generated as an A-module. Then B is a Noetherian ring.*

Proof. By the corollary above, B is a Noetherian A-module, so every ideal of B is finitely generated as an A-module, hence also as a B-module. □

What's the problem in general then for showing that $\mathcal{O}_L$ is Dedekind for L a number field? The big problem is showing that it is $\mathcal{O}_L$ is finitely generated as a $\mathbb{Z}$-module.

Definition 7.10. We say that M a is Noetherian R-module if for any ascending chain of R-submodules

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq \dots$$

there is an N such that $M_i = M_j$ for all $i, j \geq N$.