Math 568 Tom Tucker
NOTES FROM CLASS 9/24

A note on definitions: Fractional ideals are not generally always assume to be finitely generated. So here's what we have from last time with this convention.

Lemma 7.1. *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 $m_1, \dots, m_n$ 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, $y \in S^{-1}R(R : J)$. □

All invertible ideals are automatically finitely generated, though.

Lemma 7.2. *Let J be a fractional ideal of an integral domain R. Then J is invertible $\Leftrightarrow$ J is finitely generated and $R_{\mathcal{M}}J$ is an invertible fractional ideal of $R_{\mathcal{M}}$ for every maximal ideal $\mathcal{M}$ 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 $\mathcal{M}$ be a maximal ideal of R. Since we can write $J(R : J) = R$ we must have $R_{\mathcal{M}}(J(R : J)) = R_{\mathcal{M}}$, so $(R_{\mathcal{M}}J)(R_{\mathcal{M}}(R : J)) = R_{\mathcal{M}}$, so $R_{\mathcal{M}}J$ 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 $\mathcal{M}$ be a maximal ideal of R. Since J is finitely generated by assumption, we can apply the Lemma immediately above to obtain $(R_{\mathcal{M}} : R_{\mathcal{M}}J) = R_{\mathcal{M}}(R : J)$. Hence, we have $R_{\mathcal{M}}J(R : J) = R_{\mathcal{M}}$. Thus the ideal $I = J(R : J)$ is not contained in any maximal ideal of R. Thus, $I = R$ and J is invertible. □

Theorem 7.3. *Let R be a a local integral domain of dimension 1. Then R is a DVR $\Leftrightarrow$ every nonzero 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 $\mathcal{M}$ of R. The set of ideals I of R that are not a power of $\mathcal{M}$ (note: we consider R to $\mathcal{M}^0$, so the unit ideal is considered to be a power of $\mathcal{M}$) has a maximal element if it is not empty. Taking such a maximal element I, we see that $(R : \mathcal{M})I$ must not be invertible since if it had an inverse J, then $\mathcal{M}J$ would be an inverse for I. On the other hand, $(R : \mathcal{M})I \neq I$ since if $(R : \mathcal{M})I = I$, then $\mathcal{M}I = I$ which means that $I = 0$ by Nakayama's Lemma. Since $(R : \mathcal{M})I \supseteq I$ (since $1 \in (R : \mathcal{M})$), this means that $(R : \mathcal{M})I$ is strictly larger than I, contradicting the maximality of I. □

Now, we have the global counterpart.

Theorem 7.4. *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 $\mathcal{M}$, it is clear that $R_{\mathcal{M}}J$ is a fractional ideal of $R_{\mathcal{M}}$. Since $R_{\mathcal{M}}$ is a DVR, $R_{\mathcal{M}}J$ must be therefore be invertible for every maximal ideal $\mathcal{M}$. 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 7.2.

($\Leftarrow$) Since every ideal of R is invertible, every ideal of R is finitely generated, so R is Noetherian. Let $\mathcal{M}$ be a maximal ideal of R and let I be a nonzero ideal in $R_{\mathcal{M}}$. Then $I \cap R$ is invertible, so I is invertible. Thus, $R_{\mathcal{M}}$ is a DVR as desired.

□

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 $\mathcal{P}^{-1} = (R : \mathcal{P})$ for maximal $\mathcal{P}$ (by the way nonzero prime means the same thing as maximal in a 1-dimensional integral domain of course).

Proposition 7.5. *Let R be a Dedekind domain. Then every fractional ideal J of R has a unique factorization as*

$$J = \prod_{i=1}^{n} \mathcal{P}_i^{e_i}$$

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

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

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

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. It is integrally closed and we alter one of the Lemmas above to show that it is one-dimensional. Here is the proof of that.

Lemma 7.6. *Let A be an integral domain that is not a field. Suppose that B is integral over A. Then B is not a field.*

Proof. Since A is not a field, there is some $x \in A$ such that $x^{-1} \notin A$. We will show that x^{-1} is not integral over A and therefore cannot be in B. Suppose that x^{-1} was integral over A. Then we would have

$$x^{-n} + a_{n-1}x^{-n+1} + \cdots + a_0 = 0$$

with $a_i \in A$. But then we would have

$$x^{-1} = -(a_{n-1} + \ldots a_0 x^{n-1}) \in A,$$

a contradiction. □

Proposition 7.7. *Let A and B be integral domains with $A \subset B$ and B integral over A. Suppose that A is 1-dimensional. Then B is 1-dimensional.*

Proof. First, note that B cannot be 0-dimensional since it cannot be a field by the lemma above. We have seen before $\dim B \leq 1$ so our proof is done. □

So all we need to do is show that $\mathcal{O}_L$ is Noetherian for a number field L (a number field is a finite extension of $\mathbb{Q}$). We'll show something a little more general. We'll show the following.

Theorem 7.8. *Let A be a Dedekind domain with field of fractions K. Let L be a finite separable extension of A. Then the integral closure B of A in L is a Dedekind domain.*

From some work we've done, all we'll have to do is show that B is contained in a finitely generated A-module. We'll use something called a dual basis, the existence of which is proven using the separable basis theorem.

The separable basis theorem. Here is the basic set-up for today. Let L be a finite algebraic extension of degree n over K. Since L is a vector space over K and multiplication by an element x in L preserves the K-structure of L, we see that

$$r_x : z \mapsto xz$$

is a K-linear invertible map from L to L. Given a basis $m_1, \ldots, m_n$ for L over K, we can write

$$r_x m_i = \sum_{i=1}^{n} a_{ij} m_j$$

for $m_1, \ldots, m_n$. We have the usual definitions for the norm and trace of r_x below

$$\mathrm{T}_{L/K}(x) := \mathrm{T}_{L/K}(r_x) = \sum_{i=1}^{n} a_{ii}$$
$$\mathrm{N}_{L/K}(x) := \mathrm{N}_{L/K}(r_x) = \det([a_{ij}]).$$

In other words, if r_x gives the matrix M, then the trace is the sum of the diagonal elements and the norm is the product of the diagonal elements. It turns out that this definition doesn't depend on the choice of basis. This is a standard fact from linear algebra. It follows from the fact that for any matrix $n \times n$ M and any invertible $n \times n$ matrix U, we have

$$\mathrm{T}_{L/K}(M) = \mathrm{T}_{L/K}(UMU^{-1})$$

and

$$\mathrm{N}_{L/K}(M) = \mathrm{N}_{L/K}(UMU^{-1}).$$