Math 210C Lecture 9 Notes

Daniel Raban

April 19, 2019

1 Factorization of Ideals in Dedekind Domains and Discrete Valuation Rings

1.1 Unique factorization of fractional ideals in Dedekind domains

If $\mathfrak{a} \subseteq A$ is an ideal, we define $\mathfrak{a}^{-1} = \{b \in Q(A) : \mathfrak{b}\mathfrak{a} \subseteq A\}$.

Lemma 1.1. *If A is a Dedekind domain and $\mathfrak{p}$ is a maximal ideal, then $\mathfrak{p}\mathfrak{p}^{-1} = A$.*

If we can prove unique factorization of fractional ideals into primes in Dedekind domains, then we can get this result for all ideals.

Theorem 1.1. *Let A be a Dedekind domain, and let $\mathfrak{a} \subseteq Q(A)$ be a fractional ideal of A. There exist $k \geq 0$, distinct nonzero primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k$, and nonzero integers $r_1, \dots, r_k \in \mathbb{Z}$ such that $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$. This factorization is unique up to ordering. Moreover, $\mathfrak{a}$ is an ideal if and only if all $r_i > 0$.*

Proof. Let $\mathfrak{a} \subseteq A$ be a nonzero ideal. Work by induction on m such that there exist maximal $\mathfrak{q}_1, \dots, q_m$ with $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{a}$. Then $m = 0 \iff \mathfrak{a} = A$. Suppose $m \geq 1$. Then there exists a maximal ideal $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. A lemma from before gives us that $\mathfrak{p} = \mathfrak{q}_m$ without loss of generality. Then $\mathfrak{q}_1 \cdots \mathfrak{q}_{m-1} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq A$ by definition of $\mathfrak{p}^{-1}$. By induction on m, there is a factorization of $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$. So $\mathfrak{a} = \mathfrak{a}A = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}\mathfrak{p}$. So we have the factorization.

If $\mathfrak{a} \subseteq Q(A)$ is a fractional ideal, then there is a $d \in A \setminus \{0\}$ such that $f\mathfrak{a} \subseteq A$. Then $(d) = \mathfrak{p}_1^{r_1} \cdots p_k^{r_k}$, $d\mathfrak{a} = \mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_\ell^{s_\ell}$, and $\mathfrak{a} = (d)^{-1}$. Then $d\mathfrak{a} = (\mathfrak{p}_1 \cdots \mathfrak{p}_k^{r_k})^{-1}\mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_k^{s_k}$. So we again have the factorization.

Uniqueness: Let $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k} = \mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_\ell^{s_\ell}$ with $r_i, s_J \in \mathbb{Z}$. Multiply through so that all $r_i, s_j > 0$ and $\mathfrak{p}_j, \mathfrak{q}_i$ are distinct (those that are left). Now both sides equal some ideal $\mathfrak{b} \subseteq A$. Write $\mathfrak{b} = P_1^{t_1} \cdots P_m^{t_m}$. Let $t = \sum_i t_i$ be minimal among all factorizations with this $\mathfrak{b}$. If $t = 0$, then $m = 0$, and $\mathfrak{b} = A$ (so we are done). If $t > 0$, then $\mathfrak{r}_m \supseteq \mathfrak{b}$, so $\mathfrak{r}_m$ equals some $\mathfrak{Q}_j$ in any other factorization $Q_1^{u_1} \cdots Q_n^{u_n}$ of $\mathfrak{b}$ (by the same lemma from earlier). We get a contradiction. So the factorization of $\mathfrak{b}$ is unique, which means the factorization of $\mathfrak{a}$ is unique. $\square$

1.2 Groups of fractional ideals

Corollary 1.1. *Let A be a Dedekind domain. Then $I(A)$, the set of fractional ideals of A is a group under $\cdot$.*

Definition 1.1. $P(A) \leq I(A)$ is the subgroup of **principal fractional ideals**. $\mathrm{Cl}(A) = I(A)/P(A)$ is the **class group** of A.

Lemma 1.2. $\mathrm{Cl}(A)$ *is trivial if and only if A is a PID.*

Proof. If $\mathrm{Cl}(A)$ is trivial, then every fractional ideal is principal, so every ideal is principal. If A is a PID, then any $\mathfrak{a} \in I(A)$ can be written as $\mathfrak{b}\mathfrak{c}^{-1}$ for ideals $\mathfrak{b}, \mathfrak{c}$ of A. Then $\mathfrak{b} = (b)$ and $\mathfrak{c} = c$, so $\mathfrak{a} = (bc^{-1})$. $\square$

For a number field K, $I_K = I(O_K)$, $P_K = P(O_K)$. We write $\mathrm{Cl} = \mathrm{CL}(O_K) = I_K/P_K$. Here is a theorem that is beyond the scope of this course.

Theorem 1.2. Cl_K *is finite.*

Example 1.1. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $O_K = \mathbb{Z}[\sqrt{-5}]$. Let $\mathfrak{a} = (2, 1+\sqrt{-5})$. Then $N_{K/\mathbb{Q}}(2) = 4$, and $N_{K/\mathbb{Q}}(1+\sqrt{-5}) = 6$. If $\mathfrak{a} = (a)$, then $a = 2x + (1+\sqrt{-5})y$, so $N_{K/\mathbb{Q}}(a) = (2x + (1+\sqrt{-5})y)(2x + (1-\sqrt{-5})y) = 4x^2 + 2xy + 6y^2 \in (2)$. We have $N_{K/\mathbb{Q}}(a) \mid 4, 6$, since a generates $\mathfrak{a}$. So $N_{K/\mathbb{Q}}(a) = \pm 2$. But $N_{K/\mathbb{Q}}(a+b\sqrt{-5}) = a^2+5b^2 \neq 2$, since a, b are integers. So $\mathfrak{a}$ is not principal. In fact, $[\mathfrak{a}]$ generates $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$.

Theorem 1.3. *A Dedekind domain is a UFD if and only if it is a PID.*

Proof. PIDs are UFDs in general. Assume A is a UFD and Dedekind domain. If $\mathfrak{p} \subseteq A$ is maximal, it is also minimal (since A has Krull dimension ≤ 1). A is a UFD, so $\mathfrak{p} = (f)$, where f is irreducible. If $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k} = uf_1^{r_1} \cdots f_k^{r_k}$ where f_i is irreducible and $\mathfrak{p}_i = (f_i)$. $\square$

1.3 Discrete Valuation Rings

Definition 1.2. A **discrete valuation ring** (or **DVR**) is a PID with exactly one nonzero prime ideal.

Lemma 1.3. *Let A be PID. The following are equivalent:*

1. *A is a DVR.*
2. *A has a unique nonzero maximal ideal.*
3. *A has a unique nonzero irreducible element up to multiplication by units.*

Definition 1.3. A generator π of the maximal ideal of a DVR is called a **uniformizer**.

The lemma says that this is well-defined, up to units.

Proposition 1.1. *Let A be a domain. Then A is a DVR if and only if A is a local Dedekind domain that is not a field.*

Proof. DVRs are PIDs, so the are Dedekind domains. Then DVRs are local. Let A be a local Dedekind domain which is not a field, and let $(0) \neq \mathfrak{p} \subseteq A$ be a maximal ideal. If $\mathfrak{a} \subseteq A$ is an ideal, then unique factorization gives $\mathfrak{a} = \mathfrak{p}^n$ for some $n \geq 1$. Take $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $\mathfrak{p} = (\pi)$, since (π) must be a power of $\mathfrak{p}$. Then $\mathfrak{a} = \mathfrak{p}^n = (\pi^n)$. So A is a PID and hence a DVR. □

Theorem 1.4. *If A is a noetherian domain, then A is Dedekind if and only if $A_\mathfrak{p}$ is a DVR for all nonzero prime ideals $\mathfrak{p}$ of A.*

Proof. ($\implies$): This follows from the proposition.

($\impliedby$): Let $A' = \bigcap_{\mathfrak{p} \neq 0} A_\mathfrak{p} \subseteq Q(A)$. Then $A \subseteq A'$, and we want to show that $A = A'$. If $c/d \in A'$, with $c, d \in A \setminus \{0\}$, then consider the fractional ideal $\mathfrak{a} = \{a \in A : ac \in (d)\}$. For each $\mathfrak{p}$, $c/d = r/d$, where $r \in A$ and $s \in A \setminus \mathfrak{p}$. Then $sc = rd \in (d)$, so $s \in \mathfrak{a}$. Then $\mathfrak{a} \not\subseteq \mathfrak{p}$ for all $\mathfrak{p}$ maximal, which means that $\mathfrak{a} = A$. So $c/d \in A$. So $A' = A$. □

We will finish the proof next time.