Lecture 25: Connections to Algebraic Number theory

1) Dedekind domains.
2) Unique factorization for ideals.

Refs: [V], Section 9.3; [N] Sec 1.3.

1) Dedekind domains.

1.1) Definition and main example.

Let A be a Noetherian domain.

Definition: We say A is a **Dedekind domain** if
- it's normal (Sec 1 of Lec 22), i.e. $\overline{A}^{Frac(A)} = A$.
- & every nonzero prime ideal is maximal.

Example: PID $\Rightarrow$ Dedekind. Indeed, every PID is tautologically Noetherian & is a UFD, hence normal (Sec 1.1 of Lec 22). As we have remarked in Sec 1 of Lec 7, every nonzero prime ideal in a PID is maximal

The following is the main result of this section, a reason why Dedekind domains are important for Number theory.

Theorem: Every ring of algebraic integers (= integral closure $\overline{\mathbb{Z}}^L$ of $\mathbb{Z}$ in a finite extension L of $\mathbb{Q}$, Sec 2 of Lec 21) is Dedekind.

Side remark: Dedekind domains are also important in Algebraic geometry: algebras of functions on "smooth affine curves" are Dedekind. More on this in a bonus later.

1.2) Finiteness of integral closures.

The main part of the proof of Thm is to show that $\overline{\mathbb{Z}}^L$ is finite over $\mathbb{Z}$ (a.k.a. finitely generated abelian group). We will consider a more general situation.

Let A be a domain, $K = \mathrm{Frac}(A)$, $K \subset L$ finite field extension.

Proposition: Suppose A is Noetherian and normal & $\operatorname{char} K = 0$. Then $\overline{A}^L$ is a finite A-algebra.

Applying this to $A = \mathbb{Z}$ (so $K = \mathbb{Q}$), get

Corollary: $\overline{\mathbb{Z}}^L$ is finite over $\mathbb{Z}$ (and hence Noetherian).

Side remark: Proposition is true in the cases when A is a domain that is a finitely generated algebra over $\mathbb{Z}$ or over a field ([E], Thm 4.14) or when A is a Dedekind domain (a special case of [E], Thm 11.13), but not true just under the Noetherian assumption.

Proof of Proposition:

Let $\dim_K L = n$. Every element $\alpha \in L$ gives a K-linear operator $m_\alpha : L \to L$, $\ell \mapsto \alpha \ell$. So for $\alpha \in L$ it makes sense to speak about $tr(\alpha) := tr(m_\alpha) \in K$.

Step 1: We claim that for $\alpha \in \bar{A}^L$ we have $tr(\alpha) \in A$.

Let $f(x) \in A[x]$ be a monic polynomial w $f(\alpha) = 0$. Choose an algebraic extension $\tilde{L}$ of L where $f(x)$ decomposes into linear factors. All eigenvalues of m_α are roots of $f(x)$, hence are integral over A. Therefore $tr(\alpha)$ – the sum of eigenvalues – is integral over A. But $tr(\alpha) \in K$ and, since A is normal, we see $tr(\alpha) \in A$.

Step 2: For $\alpha, \beta \in L$ define $(\alpha, \beta) := tr(\alpha\beta)$. This is a symmetric K-bilinear form $L \times L \to K$. We claim that $(\cdot,\cdot)$ is nondegenerate: $\forall\, u \in L\ \exists u' \in L \mid tr(uu') \neq 0$. In fact, for $u \in L \setminus \{0\}$ $\exists\, m > 0$ s.t. $(u, u^{m-1}) = tr(u^m) \neq 0$. Indeed, let $u_1 = u, u_2, \dots, u_k$ be the pairwise distinct eigenvalues of m_u (elements of some finite extension $\tilde{L}$ of L) w. multiplicities $d_1, \dots d_k$. Then $tr(u^m) = \sum_{i=1}^{k} d_i u_i^m$.

Consider equations $\sum_{i=1}^{k} u_i^m d_i$ for $m = 1, \dots k$. We view them as the system of linear equations on $d_1, \dots d_k$ w. matrix $X = (u_i^m)_{i,m=1}^{k}$. We claim that $\det(X) \neq 0$. We have $\det(X) = \prod_{i=1}^{k} u_i \cdot \prod_{i<j} (u_i - u_j) \neq 0$. By our convention, $u_i \neq u_j$ for $i \neq j$ so the 2nd factor is nonzero. Also $u \neq 0 \Rightarrow m_u$ is invertible $\Rightarrow u_i \neq 0\ \forall i$, so $\prod_{i=1}^{k} u_i \neq 0$. We conclude that $d_1 = \dots = d_n = 0$ (in $\tilde{L}$), which is impossible: $d_i \in \mathbb{Z}_{>0}$ &

char $\tilde{L}=0$. This contradiction shows $tr(u^m)\neq 0$ for some m, hence $(\cdot,\cdot)$ is non-degenerate.

Step 3: Pick an orthonormal basis $\ell_1, \ldots \ell_n$. We claim $\exists\, a_1, \ldots a_n \in A$ s.t. $\tilde{\ell}_i := a_i \ell_i \in \bar{A}^L$: if $f \in K[x]$, $f(x) = x^m + \sum_{i=0}^{m-1} b_i x^i$ is s.t. $f(\ell_i)=0$, then $\exists\, a_i$ s.t. $\tilde{f}(x) = x^m + \sum_{i=0}^{m-1} b_i a_i^{m-i} x^i \in A[x]$ & $\tilde{f}(a_i\ell_i)=0$. Set $\tilde{\ell}^i = a_i^{-1}\ell_i$ so that $(\tilde{\ell}_i, \tilde{\ell}^j) = \delta_{ij}$. Let $M := \mathrm{Span}_A(\tilde{\ell}^1, \ldots, \tilde{\ell}^n)$.

Claim: $\bar{A}^L \subset M$

This will finish this step b/c A is Noetherian & M is finitely generated over A.

To prove the claim note that, since ℓ_i is an orthonormal basis, $\forall\, \alpha \in L \Rightarrow \alpha = \sum_{i=1}^n (\alpha, \ell_i)\ell_i = \sum_{i=1}^n (\alpha, \tilde{\ell}_i)\tilde{\ell}^i$. We need to show that $(\alpha, \tilde{\ell}_i) \in A$ for $\alpha \in \bar{A}^L$. But $\tilde{\ell}_i \in \bar{A}^L \Rightarrow \alpha\tilde{\ell}_i \in \bar{A}^L$ & $(\alpha, \tilde{\ell}_i) = tr(\alpha\tilde{\ell}_i) \in A$ by Step 1. $\square$

1.3) Proof of Theorem

It remains to show that every nonzero prime ideal $\mathfrak{p} \subset A$ is max'l $\Leftrightarrow$ the domain $A/\mathfrak{p}$ is a field. Since A is integral$/\mathbb{Z}$, Prob 4 in HW6 shows $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$. Besides $\mathfrak{p} \cap \mathbb{Z}$ is prime ideal in $\mathbb{Z}$ (spec. case of 6) in Prob 4 of HW1) so $\exists$ prime p s.t. $\mathfrak{p} \cap \mathbb{Z} = (p)$. So the action of $\mathbb{Z}$ on $A/\mathfrak{p}$ factors through $\mathbb{Z}/p\mathbb{Z}$, hence $A/\mathfrak{p}$ is a vec.

tor space over $\mathbb{Z}/\mathfrak{p}\mathbb{Z}$. Next $A = \mathrm{Span}_{\mathbb{Z}}(a_1, \dots a_k)$ for some a_i (Cor. in Sec 1.2) $\Rightarrow A/\mathfrak{p} = \mathrm{Span}_{\mathbb{Z}/p\mathbb{Z}}(a_i + \mathfrak{p} \mid i = 1, \dots k) \Rightarrow \dim_{\mathbb{Z}/p\mathbb{Z}} A/\mathfrak{p} < \infty \Rightarrow$ $|A/\mathfrak{p}| < \infty$. Every finite domain is a field (exercise: hint – an injective map from a finite set to itself is a bijection) $\square$

2) Unique factorization for ideals.

Our next goal is to prove the following theorem going back to Dedekind.

Theorem: Let A be a Dedekind domain & $I \subset A$ a nonzero ideal. Then $\exists$ prime ideals $\mathfrak{p}_1, \dots \mathfrak{p}_k$ unique up to permutation s.t. $I = \mathfrak{p}_1 \dots \mathfrak{p}_k$.

In other words, the unique factorization, which may fail on the level of elements always holds on the level of ideals.

Today, we do some preparation for the proof. Here's a weaker version of the theorem.

Lemma: Let A be Noetherian & $I \subset A$ be a nonzero ideal. Then $\exists$ nonzero prime ideals $\mathfrak{p}_1 \dots \mathfrak{p}_n \subset A$ s.t. $I \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$.

Proof:

Let X be the set of all I for which the claim fails. If $X \neq \emptyset$, then $\exists$ max'l w.r.t. inclusion $I \in X$ (b/c A is Noetherian). Then I isn't prime $\Rightarrow \exists\, I_1, I_2 \supsetneq I$ w. $I_1 I_2 \subset I$. Then $I_j \in X$ leading to contradiction (exercise). $\square$

In the proof we will need the inverses of ideals.

Let A be a Dedekind domain & $K = \mathrm{Frac}(A)$. For ideals $I, J \subset A$ w. $I, J \neq \{0\}$, define:

$$J^{-1} = \{x \in K \mid xI \subset A\},\ IJ^{-1} = \{\sum_{i=1}^{k} a_i b_i \mid a_i \in I,\ b_i \in J^{-1}\}.$$

Exercise: J^{-1} & IJ^{-1} are A-submodules of K & $J^{-1} = AJ^{-1}$.

The following proposition is the main ingredient for the theorem.

Proposition: We have $I \subsetneq I\mathfrak{p}^{-1}$ for every prime $\mathfrak{p}$.

Proof: Since $A \subset \mathfrak{p}^{-1}$, we have $I \subset I\mathfrak{p}^{-1}$. We need to show $I \neq I\mathfrak{p}^{-1}$.

Case 1: $I = A$: we need to find an element in $\mathfrak{p}^{-1} \setminus A$. Take $a \in \mathfrak{p} \setminus \{0\}$. By Lemma, $\exists$ prime ideals $\mathfrak{p}_1, .., \mathfrak{p}_n \subset A$ w. $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset (a)$, we can assume that $\prod_{i \neq j} \mathfrak{p}_i \not\subset (a)$ $\forall j = 1, .. n$ (otherwise just remove $\mathfrak{p}_j$). Since $a \in \mathfrak{p}$, we have $\mathfrak{p}_1 \cdots \mathfrak{p}_n (\subset (a)) \subset \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\mathfrak{p}_i \subset \mathfrak{p}$ for some i, w.l.o.g. assume $i = n$. But every nonzero prime ideal is maximal, incl. $\mathfrak{p}_n \Rightarrow \mathfrak{p}_n = \mathfrak{p}$. Take $b \in \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} \setminus (a) \Rightarrow a^{-1}b \in K \setminus A$. But $b\mathfrak{p} \subset \mathfrak{p}_1 \cdots \mathfrak{p}_{n-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \subset (a) \Leftrightarrow a^{-1}b\mathfrak{p} \subset A \Leftrightarrow a^{-1}b \in \mathfrak{p}^{-1}$. We see that $\mathfrak{p}^{-1} \neq A$.

Case 2 – general. Assume $I\mathfrak{p}^{-1} = I$. Take $y \in \mathfrak{p}^{-1} \setminus A$. Then $yI \subset I\mathfrak{p}^{-1} = I$ so we have an A-linear endomorphism $\varphi : I \to I$,

$a \mapsto ya$. Since I is a fin. gen'd A-module, the Cayley-Hamilton lemma (see Sec 1.1 of Lec 20 & Lemma 2 in Sec 1.3 of Lec 21) shows $\exists$ monic $f \in A[x]$ w. $f(\varphi)=0$. But $f(\varphi): I \to I$ is given by $a \mapsto f(y)a$. Take $a \neq 0 \rightsquigarrow f(y)=0$. Since A is integrally closed in K, $y \in A$. Contradiction. $\square$