Lecture 12: Integral & finite algebras III

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

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

1) Dedekind domains.

1.1) Definition and main example.

Let A be a domain.

Definition: We say A is a Dedekind domain if
- A is Noetherian
- it's normal (Sec 2.3 of Lec 11), i.e. $\overline{A}^{Frac(A)} = A$.
- & every nonzero prime ideal is maximal.

Example: PID A is Dedekind. Indeed, $\forall$ PID is tautologically Noetherian & is a UFD, hence normal (Sec 2.3 of Lec 11). Every nonzero prime ideal is of the form (p) for prime $p \in A$. It's maximal: if $(f) \supseteq (p)$, then f divides $p \Rightarrow f = \varepsilon$ or εp for invertible p.

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 $\overline{\mathbb{Z}}^L$ for a finite extension L of $\mathbb{Q}$, Sec 2.2 in Lec 11) is Dedekind.

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 & 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.

1.3) Reminders from Linear algebra

In the proof of the proposition we'll need some constructions from Linear algebra that we recall now.

Let K be a field and V a finite dimensional vector space$/K$.

1.3.1) Bilinear forms

By a bilinear form on V we mean a bilinear map $\beta: V\times V \to K$.
We say β is symmetric if $\beta(u,v)=\beta(v,u)\ \forall\, u,v$, and non-degenerate if $\forall\, u\in V\setminus\{0\}\ \exists\, u'\in V$ s.t. $\beta(u,u')\neq 0$.

Now choose a basis $e_1,\dots e_n\in V$ so that $K^n \xrightarrow{\sim} V$ $((a_1,\dots a_n)\mapsto \sum_{i=1}^n a_i e_i)$
We view elements of V as column vectors. Then every bilinear β is given by $\beta(u,v)=u^T B v$ for unique matrix B ($B=(\beta(e_i,e_j))_{i,j=1}^n$)
We have: β is symmetric $\Leftrightarrow$ B is symmetric; β is non-degenerate $\Leftrightarrow$ B is non-degenerate.

Exercise 1 Let β be non-degenerate & symmetric. Show that:
1) $\exists!$ "dual basis" $e^i, i=1,\dots n$, characterized by $\beta(e_i,e^j)=\delta_{ij}$ (take the columns of B^{-1})
2) $\forall\, v\in V \Rightarrow v=\sum_{i=1}^n (e_i,v)e^i$ (hint: $\beta(v-\sum(e_i,v)e^i, e_i)=0\ \forall\, i$).

1.3.2) Trace

Let $\varphi: V\to V$ be a linear operator. By the trace of φ, $tr(\varphi)$, one means the sum of diagonal entries of the matrix of φ in any basis of V. Equivalently, if $\lambda_1,\dots\lambda_n$ ($n=\dim V$) are eigenvalues of φ with multiplicities, then $tr(\varphi)=\sum_{i=1}^n \lambda_i$.

1.4) 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 $tr(\alpha):=tr(m_\alpha)\in K$. The proof will be in 4 steps.

Step 1: Show that $\alpha \in \bar{A}^L \Rightarrow tr(\alpha) \in A$ (here we use that A is normal).

Step 2: Define $\beta(x,y) = tr(xy)$, a bilinear form $L \times L \to K$. Since $xy = yx \Rightarrow m_x m_y = m_y m_x \Rightarrow \beta$ is symmetric. We'll show that β is non-degenerate (here we use that char $K=0$)

Step 3: We show $\exists$ basis $e_1, \dots e_n$ of L over K lying in $\bar{A}^L$. Thx to Step 2 & 1) of Exercise 1 $\exists$ dual basis $e^1, \dots e^n \in L$.

Step 4: We use 2) of Exercise 1 to show $\bar{A}^L \subset M := Span_A(e^1, \dots, e^n)$ & use that A is Noetherian to conclude $\bar{A}^L$ is a fin. gen'd A-module.

Proof of Step 1: Pick $\alpha \in \bar{A}^L$. Let $f(x) \in A[x]$ be monic s.t. $f(\alpha) = 0 \Rightarrow f(m_\alpha) = 0$ (in $End_K(L)$) $\Rightarrow f(\lambda_i) = 0$ $\forall$ e-values $\lambda_1, \dots \lambda_n$ of m_α (that live in a suitable finite extension $\tilde{L}$ of L) $\Rightarrow \lambda_i \in \bar{A}^{\tilde{L}}$ $\Rightarrow tr(\alpha) = \sum_{i=1}^n \lambda_i \in \bar{A}^{\tilde{L}}$. Since A is normal, $\bar{A}^{\tilde{L}} \cap K = \bar{A}^K = A \Rightarrow$ $tr(\alpha) \in A$.

Proof of Step 2: β is nondegenerate, i.e. $\forall u \in L$ $\exists u' \in L \mid tr(uu') \neq 0$. We'll show a stronger claim: for $u \in L \setminus \{0\}$ $\exists m \geq 0$ s.t. $(u, u^{m-1}) = tr(u^m) \neq 0$.

Indeed, let $u_1, u_2, \dots, u_k$ 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 $\sum_{i=1}^k u_i^m d_i = 0$ for $m = 1, \dots k$. We view them as the system of linear equations on $d_1, \dots d_k$ w. matrix $X = (u_i^m)_{i,m=1}^k$, essentially, the Vandermonde matrix. We have $\det(X)=\prod_{i=1}^{k} u_i \cdot \prod_{i>j}(u_i-u_j)$. 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 $\prod_{i=1}^{k} u_i \neq 0$. So $\det(X)\neq 0$. We conclude that $d_1=\ldots=d_n=0$ (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.

Proof of Step 3: one can choose a basis of L over K lying in $\bar{A}^L$. Pick a basis $\ell_1,\ldots,\ell_n$ of L over K. We claim $\exists\, a_1,\ldots a_n\in A\setminus\{0\}$ s.t. $e_i:=a_i\ell_i\in\bar{A}^L$.

Choose $f\in K[x]$, $f(x)=x^m+\sum_{j=0}^{m-1} b_j x^j$ w. $b_j\in K$ is s.t. $f(\ell_i)=0$. $\forall$ $a_i\in A\setminus\{0\}\Rightarrow 0=a_i^m f(\ell_i)=\tilde{f}(a_i\ell_i)$, where $\tilde{f}=x^m+\sum_{j=0}^{m-1} b_j a_i^{m-j}x^j$. Choose $a_i\in A$ w. $a_i b_j\in A\ \forall j\Rightarrow \tilde{f}\in A[x]$ & is monic $\Rightarrow e_i:=a_i\ell_i\in\bar{A}^L$.

Proof of Step 4: that $\bar{A}^L\subset M=\mathrm{Span}_A(e^i)$ & $\bar{A}^L$ is fin. gen'd.

Pick $a\in\bar{A}^L$. By Exercise 1, $a=\sum_{i=1}^{n}\beta(e_i,a)e^i$. By Step 3, $e_i\in\bar{A}^L$ $\Rightarrow e_i a\in\bar{A}^L$. By Step 1, $\beta(e_i,a)=tr(e_i a)\in A$. So $a\in M\Rightarrow \bar{A}^L\subset M$.

M is finitely generated A-module. Since A is Noetherian, Corollary in Sec 3 of Lec 5, shows M is Noetherian $\Rightarrow \bar{A}^L$ is finitely generated A-module.

1.3) Proof of Theorem

Set $B:=\bar{\mathbb{Z}}^L$. It's a finitely generated $\mathbb{Z}$-module by Proposition & normal by Example 1) in Sec 2.3 of Lec 11.

It remains to show that every nonzero prime ideal $\mathfrak{p} \subset B$ is max'l $\Leftrightarrow$ the domain $B/\mathfrak{p}$ is a field.

Step 1: We claim that $\forall$ nonzero ideal $I \subset B \Rightarrow I \cap \mathbb{Z} \neq \{0\}$. Pick $a \in I \setminus \{0\}$ & let $f \in \mathbb{Z}[x]$ be monic s.t. $f(a)=0$ & has min. deg w. this property; $f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_0$ ($c_i \in \mathbb{Z}$). Note that:

- $c_0 \neq 0$ – otherwise for $g(x) = f(x)/x$ still have $g(a)=0$.
- $c_0 = -a^n - c_{n-1}a^{n-1} - \ldots - c_1 a \in I \Rightarrow 0 \neq c_0 \in I \cap \mathbb{Z}$.

Step 2: Note that $\mathfrak{p} \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$. We have $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$ $\Rightarrow \mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$ is finite set. Since B is finitely generated module over $\mathbb{Z} \Rightarrow B/\mathfrak{p}$ is finitely generated module over $\mathbb{Z}$, hence over $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}) \Rightarrow \exists\, k \in \mathbb{Z}_{>0} \mid (\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}))^k \twoheadrightarrow B/\mathfrak{p} \Rightarrow B/\mathfrak{p}$ is finite as a set. But every domain finite as a set is a field (exercise – hint: every injective map from a finite set to itself is bijective) so $\mathfrak{p}$ is maximal. $\square$

2) Unique factorization for ideals.

Our next goal is to prove the following theorem going back to Dedekind, which also explains why we care about Dedekind domains.

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

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

In the proof we need the following lemma:

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 $J \in X$ (b/c A is Noetherian). Then J isn't prime $\Rightarrow \exists\ J_1, J_2 \supsetneq J$ w. $J_1 J_2 \subset J$. Then $J_j \notin X$ leading to contradiction (exercise). $\square$