Lecture 13: Connections to Algebraic Number theory

1) Unique factorization for ideals, cont'd
2) Noether normalization lemma.

[N] Sec 1.3, Sec 1.6.

1) Unique factorization for ideals, cont'd

1.0) Reminder.

Recall (Sec 1.1 of Lec 13) that a Dedekind domain is a normal Noetherian domain where every nonzero prime ideal is maximal. Our goal in this section is to prove

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 $| \ I = \mathfrak{p}_1 \ldots \mathfrak{p}_k$.

1.1) Fractional ideals.

This is the first tool we need to prove the theorem.

Definition: A *fractional ideal* for A is a finitely generated nonzero A-submodule of $K := \mathrm{Frac}(A)$.

Special cases: 1) $\forall \alpha \in K \setminus \{0\}$, $A\alpha = \{a\alpha \mid a \in A\}$ is a fractional ideal (called *principal*).

2) the nonzero ideals in A = the fractional ideals contained in A.

We'll need two operations on fractional ideals

Lemma: Let $I, J \subset K$ be fractional ideals. Then

$IJ := \{\sum_i a_i b_i \mid a_i \in I, b_i \in J\}$

$J^{-1} = \{a \in K \mid aJ \subset A\}$

are fractional ideals

Proof: we'll give a proof for J^{-1} leaving the case of IJ as an exercise (hint: this is similar to product of ideals, Sec 1 of Lec 2).

If $a, b \in J^{-1}$ & $c \in A$, then $a+b, ca \in J^{-1}$. Also $0 \in J^{-1}$. So, J^{-1} is an A-submodule. To show it's finitely generated, let $\alpha \in J \setminus \{0\}$. Then $a \in J^{-1} \Rightarrow a\alpha \in A \Rightarrow a \in A\alpha^{-1} \Rightarrow J \subset A\alpha^{-1}$. Since A is Noetherian, J is fin. gen'd. $\square$

Rem: We have $(IJ)L = I(JL)$, $IJ = JI$ & $AI = I$ by construction

Example: Let $A = \mathbb{Z}[\sqrt{-5}]$, $J = (2, 1+\sqrt{-5})$. Then $J^{-1} = \{\alpha \in \mathbb{Q}(\sqrt{-5}) \mid 2\alpha, (1+\sqrt{-5})\alpha \in A\} = \{a + b\sqrt{-5} \mid 2a, 2b \in \mathbb{Z};\ a+b \in \mathbb{Z}\} = \frac{1}{2}J$.

1.2) Auxiliary results

Last time we've proved:

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

The proof of Thm is based on the following claim:

Proposition: Let $J, \mathfrak{p} \subset A$ be nonzero ideals s.t. $\mathfrak{p}$ is maximal. Then
1) $J\mathfrak{p}^{-1} \supsetneq J$
2) $\mathfrak{p}\mathfrak{p}^{-1} = A$ & $J\mathfrak{p}^{-1} \subseteq A$ for $J \subseteq \mathfrak{p}$.
3) $J = \mathfrak{p}(J\mathfrak{p}^{-1})$
4) If $J' \subset A$ is an ideal w. $J = \mathfrak{p}J' \Rightarrow J' = J\mathfrak{p}^{-1}$

Proof:

1): $A \subset \mathfrak{p}^{-1} \Rightarrow J \subset J\mathfrak{p}^{-1}$. WTS $J \neq J\mathfrak{p}^{-1}$. This is the main part of the proof.

Case 1: $J = A$: we need to find an element in $A\mathfrak{p}^{-1} \setminus A = \mathfrak{p}^{-1} \setminus A$.
Take $a \in \mathfrak{p} \setminus \{0\}$. By Lemma, $\exists$ prime ideals $\mathfrak{p}_1, \dots \mathfrak{p}_n \neq \{0\} \mid \mathfrak{p}_1 \dots \mathfrak{p}_n \subset (a)$, we can assume that $\prod_{i \neq j} \mathfrak{p}_i \not\subset (a)$ $\forall j = 1, \dots n$ (else we remove $\mathfrak{p}_j$).

Since $a \in \mathfrak{p}$, we have $\mathfrak{p}_1 \dots \mathfrak{p}_n (\subset (a)) \subset \mathfrak{p}$. 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 $b \in \mathfrak{p}_1 \dots \mathfrak{p}_{n-1} \setminus (a) \Rightarrow a^{-1}b \in K \setminus A$.
But $b\mathfrak{p} \subset \mathfrak{p}_1 \dots \mathfrak{p}_{n-1}\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_n \subset (a) \Leftrightarrow a^{-1}b\mathfrak{p} \subset A \Leftrightarrow a^{-1}b \in \mathfrak{p}^{-1} \Rightarrow \mathfrak{p}^{-1} \neq A$.

Case 2: general J. Assume $J\mathfrak{p}^{-1} = J$. Take $y \in \mathfrak{p}^{-1} \setminus A$. Then $yJ \subset J\mathfrak{p}^{-1} = J \rightsquigarrow$ A-linear map $\varphi: J \to J$, $a \mapsto ya$. Since J is a fin. gen'd A-module, the Cayley-Hamilton type lemma (Sec 1.1 of Lec 11 applied to $M := J$ $I = A$) shows $\exists$ monic $f \in A[x]$ w. $f(\varphi) = 0$. But $f(\varphi): J \to J$ is given by $a \mapsto f(y)a$. Take $a \neq 0 \rightsquigarrow$ $f(y) = 0 \Rightarrow y \in \overline{A}^K$. But $\overline{A}^K = A$. Contradiction w. $y \notin A$. $\square$ of 1)

2): Note that $J\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset A$ (exercise). Since $\mathfrak{p}$ is maximal &

1), $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \Rightarrow \mathfrak{p}\mathfrak{p}^{-1} = A$. $\square$ of 2).

3) $\mathfrak{p}(J\mathfrak{p}^{-1}) = $ [Remark in Sec 1.1] $= J(\mathfrak{p}\mathfrak{p}^{-1}) = [2)] = JA = J$ $\square$ of 3)

4) Assume $J = \mathfrak{p}J' \Rightarrow J\mathfrak{p}^{-1} = \mathfrak{p}J'\mathfrak{p}^{-1} = J'\mathfrak{p}\mathfrak{p}^{-1} = [\mathfrak{p}\mathfrak{p}^{-1} = A] = J'$ $\square$ of 4)

1.3) Proof of Theorem

Existence: assume the contrary: there's a nonzero ideal $J \subset A$ that is not a product of primes. Since A is Noetherian we can choose J to be maximal w. this property. We can find a maximal ideal $\mathfrak{p}$ s.t. $J \subset \mathfrak{p}$.

Take $J' := J\mathfrak{p}^{-1}$. By 1) of Prop'n, $J \subsetneq J'$, by 2) $J' \subset A$ & by 3), $J = \mathfrak{p}J'$. By the choice of J, $J' = \mathfrak{p}_1 \ldots \mathfrak{p}_\ell$ for some primes $\mathfrak{p}_1, \ldots \mathfrak{p}_\ell \Rightarrow$ $J = \mathfrak{p}\mathfrak{p}_1 \ldots \mathfrak{p}_\ell$. Contradiction w. choice of J.

Uniqueness: Let $J = \mathfrak{p}_1 \ldots \mathfrak{p}_\ell = \mathfrak{q}_1 \ldots \mathfrak{q}_k$, where $\mathfrak{p}_1, \ldots \mathfrak{p}_\ell, \mathfrak{q}_1, \ldots, \mathfrak{q}_k$ are maximal ideals. Since $\mathfrak{p}_1 \ldots \mathfrak{p}_\ell = \mathfrak{q}_1 \ldots \mathfrak{q}_k \subset \mathfrak{q}_k$ & $\mathfrak{q}_k$ is prime $\Rightarrow \mathfrak{p}_i \subset \mathfrak{q}_k \Rightarrow \mathfrak{p}_i = \mathfrak{q}_k$ for some i. W.l.o.g. $i = \ell$. By 4) of Proposition, $\mathfrak{p}_1 \ldots \mathfrak{p}_{\ell-1} = J\mathfrak{p}_\ell^{-1} = \mathfrak{q}_1 \ldots \mathfrak{q}_{k-1}$ & we argue by induction on ℓ. $\square$

1.4) Class group

Let FI be the set of all fractional ideals & PFI be the subset of all principal fractional ideals. The product of fractional ideals equips FI with an abelian group structure (the inverse is J^{-1} –

to check $JJ^{-1}=A$ one reduces to the case when $J\subset A$ using $J\subset A_\alpha$ for some α, then applies the theorem & $\mathfrak{p}\mathfrak{p}^{-1}=A$). FPI is a subgroup.

The quotient $Cl(A):=FI/PFI$ is called the class group of A. It, roughly speaking, measures how far A is from being a PID.

Bonus discussion

Much is known about the class groups of the rings of algebraic integers - and yet much is not known.

The following is Theorem 6.3 in [N], Chapter I.

Theorem: Let L be a finite extension of $\mathbb{Q}$. Then $|Cl(\overline{\mathbb{Z}}^L)|<\infty$.

To get a better understanding of $Cl(\overline{\mathbb{Z}}^L)$ is an important problem in Number theory, even for $L=\mathbb{Q}(\sqrt{d})$ (which goes back to Gauss), where even some basic things are not known. For a survey of recent developments one can check

A. Bhand, M.R. Murty "Class numbers of quadratic fields", Hardy-Ramanujan journal 42 (2019), 1-9.

2) Noether normalization lemma.

We now switch gears & prove an important result about finite extensions of rings.

Recall that a finitely generated field extension is a finite ext'n of a purely transcendental one. Here's an analog for rings.

Theorem (Noether). Let $\mathbb{F}$ be a field, A a fin. generated $\mathbb{F}$-algebra. Then $\exists\, m \geq 0$ & $\mathbb{F}$-algebra inclusion $\mathbb{F}[x_1, \ldots x_m] \hookrightarrow A$ s.t A is finite over $\mathbb{F}[x_1, \ldots x_m]$

We'll only prove this when $\mathbb{F}$ is infinite, where a proof is easier. For a general case, see [E], Lemma 13.2 & Theorem 13.3.

Key lemma: Assume $\mathbb{F}$ is infinite, $F \in \mathbb{F}[x_1, \ldots x_n]$ is nonzero. Then $\exists$ $\mathbb{F}$-linear combinations $y_1, \ldots, y_{n-1}$ of variables $x_1 \ldots x_n$ s.t. $\mathbb{F}[x_1, \ldots x_n]/(F)$ is finite over $\mathbb{F}[y_1, \ldots, y_{n-1}]$.

Proof of lemma:

$F = f_0 + \ldots + f_k$, f_i is homogeneous of $\deg = i$, $f_k \neq 0$.

Special case: $a := f_k(0, \ldots, 0, 1) \neq 0$. Note that a is the coeff't of x_n^k in f_k, so in F, & $F = a x_n^k + \sum_{i=0}^{k-1} g_i(x_1, \ldots x_{n-1}) x_n^i$, where $g_i \in \mathbb{F}[x_1, \ldots x_{n-1}]$, Replacing F w. $a^{-1}F$, can assume F is monic as an element in $\mathbb{F}[x_1, \ldots x_{n-1}][x_n]$. By Example 2 in Sec 2.2 of Lec 10, $\mathbb{F}[x_1, \ldots x_n]/(F)$ is finite over $\mathbb{F}[x_1, \ldots x_{n-1}]$ and we set $y_i := x_i$.

General case: $\mathbb{F}$ is infinite & $f_k \neq 0 \Rightarrow \exists\, a_1, \ldots, a_n \in \mathbb{F} \mid f_k(a_1, \ldots a_n) \neq 0$ (exercise, hint: view F as an element of $\mathbb{F}[x_1, \ldots x_{n-1}][x_n]$ & induct on n).

Pick invertible $\varphi \in \mathrm{Mat}_{n \times n}(\mathbb{F})$ s.t

$$\varphi \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Consider $F^{\varphi} = F \circ \varphi$ as a function $\mathbb{F}^n \to \mathbb{F}$ (polynomial obtained from F by linear change of variables). Then $f_k^{\varphi}(0, \dots, 0, 1) = f_k(a_1, \dots a_n) \neq 0$.

So $\mathbb{F}[x_1, \dots x_n]/(F^{\varphi})$ is finite over $\mathbb{F}[x_1, \dots x_{n-1}]$, hence

$\wr\!\uparrow \varphi$, linear change of variables.

$\mathbb{F}[x_1, \dots x_n]/(F)$ is finite over $\mathbb{F}[y_1, \dots y_{n-1}]$ w.

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \varphi^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$\square$

Proof of Thm: Pick minimal possible m s.t. $\exists\ \varphi: \mathbb{F}[x_1, \dots x_m] \to A$ & A is finite over $\mathbb{F}[x_1, \dots, x_m]$. Such m exists b/c A is finitely generated, hence a quotient of $\mathbb{F}[x_1, \dots x_n]$ for some n. It remains to prove the following:

Claim: φ is injective.

Proof of claim:

Assume the contrary: $\exists\ F \in \ker \varphi$, $F \neq 0$. By Key Lemma $\mathbb{F}[x_1, \dots x_m]/(F)$ is finite over $\mathbb{F}[y_1, \dots y_{m-1}]$ & A is finite over $\mathbb{F}[x_1, \dots x_m]/(F)$ (b/c φ factors through $\mathbb{F}[x_1, \dots x_m]/(F)$).
By Lemma 1 in Section 2.3 in Lecture 10 A is finite over $\mathbb{F}[y_1, \dots, y_{m-1}]$. Contradiction w. choice of m. $\square$