Lecture 26: Connections to Algebraic Number theory II

1) Unique factorization for ideals, cont'd
2) Class group.

[N] Sec 1.3, Sec 1.6.

1) Unique factorization for ideals, cont'd

1.0) Reminder.

Recall (Sec 1.1 of Lec 25) 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 $\mathfrak{p}_1,\dots \mathfrak{p}_k$ unique up to permutation $|$ $I=\mathfrak{p}_1\dots\mathfrak{p}_k$.

Here is a tool from last time. Set $K=\operatorname{Frac}(A)$. For ideals $I,J\subset A$ w. $I,J\neq\{0\}$, define:

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

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

We have proved:

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

Corollary: $\mathfrak{p}\mathfrak{p}^{-1}=A$ & for any ideal $I\subset\mathfrak{p}$ we have $I\mathfrak{p}^{-1}\subset A$ (hence $I\mathfrak{p}^{-1}$ is an ideal).

Proof: $I\mathfrak{p}^{-1}\subset\mathfrak{p}\mathfrak{p}^{-1}$ b/c $I\subset\mathfrak{p}$ & $\mathfrak{p}\mathfrak{p}^{-1}\subset A$ by definition of $\mathfrak{p}^{-1}$. By Proposition, $\mathfrak{p}\subsetneq\mathfrak{p}\mathfrak{p}^{-1}$ and since $\mathfrak{p}$ is maximal, $\mathfrak{p}\mathfrak{p}^{-1}=A$. $\square$

1.1) Proof of Theorem

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

Take $I':=I\mathfrak{p}^{-1}$. By Corollary I' is an ideal & by Proposition $I'\supsetneq I$. By the choice of I, $I'=\mathfrak{p}_1\ldots\mathfrak{p}_\ell$ for some primes $\mathfrak{p}_1,\ldots\mathfrak{p}_\ell\Rightarrow$ $I'\mathfrak{p}=\mathfrak{p}_1\ldots\mathfrak{p}_\ell\mathfrak{p}$. So the following claim yields the proof of existence.

Claim: $I=I'\mathfrak{p}$.

Proof of Claim: $I'\mathfrak{p}=(I\mathfrak{p}^{-1})\mathfrak{p}=[\sum_j a_j b_j c_j \mid a_j\in I, b_j\in\mathfrak{p}^{-1}, c_j\in\mathfrak{p}]=$ $I(\mathfrak{p}^{-1}\mathfrak{p})=[\mathfrak{p}^{-1}\mathfrak{p}=A$ by Corollary$]=I$ $\square$

Uniqueness: suppose $\mathfrak{p}_1\ldots\mathfrak{p}_\ell=\mathfrak{q}_1\ldots\mathfrak{q}_k$, 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. $i=\ell$. Then we have $\mathfrak{p}_1\ldots\mathfrak{p}_\ell\mathfrak{p}_\ell^{-1}=\mathfrak{q}_1\ldots\mathfrak{q}_k\mathfrak{q}_k^{-1}$, ideals in A by Corollary.

We claim that $\forall$ ideal $I\subset A$ we have $(I\mathfrak{p})\mathfrak{p}^{-1}=I$ – this is proved as Claim & is left as an exercise. So we get

$$\mathfrak{p}_1\ldots\mathfrak{p}_{\ell-1}=\mathfrak{p}_1\ldots\mathfrak{p}_\ell\mathfrak{p}_\ell^{-1}=\mathfrak{q}_1\ldots\mathfrak{q}_k\mathfrak{q}_k^{-1}=\mathfrak{q}_1\ldots\mathfrak{q}_{k-1}.$$

Now we can proceed by induction on ℓ – cancelling out factors. $\square$

2) Class groups

An important consequence of Thm in Sec 1.0 is that it paves a way to "measure" the failure of being a UFD for a Dedekind domain, A, via the so called class group, $Cl(A)$.

2.1) Fractional ideal.

Definition: By a fractional ideal for A we mean a finitely generated submodule of $\mathrm{Frac}(A)$. We say that a fractional ideal is principal if it's generated by one element.

For example, the ideals are exactly the fractional ideals contained in A.

Lemma: Every fractional ideal I is contained in a principal one, hence is isomorphic to an ideal of A (as an A-module).

Proof: Let $I = \mathrm{Span}_A\left(\frac{a_1}{b_1}, \dots, \frac{a_k}{b_k}\right)$ w. $\frac{a_i}{b_i} \in \mathrm{Frac}(A)$. Then $I \subset A\beta$ w. $\beta = \prod_{i=1}^{k} \frac{1}{b_i}$. The map $\alpha \mapsto \alpha\beta^{-1}$ embeds I into A, identifying I w. ideal. $\square$

2.2) Group structure

Let $FI(A)$ denote the set of nonzero fractional ideals for A (not the common notation). Let $PFI(A)$ denote the subset of all (nonzero) principal fractional ideals.

For $I, J \in FI(A)$ we set
$IJ := \{\sum_{i=1}^{k} \alpha_i \beta_i \mid k \in \mathbb{Z}_{>0},\ \alpha_i \in I,\ \beta_i \in J\}$, $J^{-1} := \{\alpha \in \mathrm{Frac}(A) \mid \alpha J \subset A\}$

Lemma: IJ & J^{-1} are fractional ideals, principal if I & J are.
Proof:
We will prove that $J^{-1} \in FI(A)$, everything else is an exercise. To show that J^{-1} is an A-submodule is also an exercise. To show J^{-1} is finitely generated, pick $\alpha \in J \setminus \{0\}$. We have $\beta \in J^{-1} \Rightarrow \alpha\beta \in A \Leftrightarrow \beta \in A\alpha^{-1}$. So $J^{-1} \subset A\alpha^{-1}$ and is finitely generated as a submodule in a finitely generated module. $\square$

Theorem: The operation $(I, J) \mapsto IJ$ turns $FI(A)$ into an abelian group with unit A and inverse given by $I \mapsto I^{-1}$.

Proof: It is immediate to check that the product is associative, commutative & has A as a unit (exercise). It remains to show $II^{-1} = A$. Note that $\forall \alpha \in \mathrm{Frac}(A) \setminus \{0\}$, we have $(\alpha I)^{-1} = \alpha^{-1} I^{-1}$ so we can assume $I \subset A$. Note that $II^{-1} \subset A$. Thx to Thm in Sec 1.0, we can write $I = \mathfrak{p}_1 \dots \mathfrak{p}_k$ for maximal ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_k \subset A$. We prove $II^{-1} = A$ by induction on k. The base, $k=1$, is Corollary in Sec. 1.0.

In the general case, set $\mathfrak{p} := \mathfrak{p}_k$, $J = I\mathfrak{p}^{-1}$. By Claim in Section 1.1, $I = J\mathfrak{p}$. The uniqueness part of Thm shows $J = \mathfrak{p}_1 \dots \mathfrak{p}_{k-1}$. Therefore, we can apply the inductive assumption to see that $JJ^{-1}=A$. Note that $IJ^{-1}\mathfrak{p}^{-1}=JJ^{-1}\mathfrak{p}\mathfrak{p}^{-1}=A \Rightarrow J^{-1}\mathfrak{p}^{-1}\subset I^{-1} \Rightarrow$ $II^{-1}\supset IJ^{-1}\mathfrak{p}^{-1}=A$. Hence, $II^{-1}=A$ finishing the proof. $\square$

Note that $PFI(A)\subset FI(A)$ is a subgroup.

Definition: The class group of A is $FI(A)/PFI(A)$.

Lemma: TFAE:

(a) A is UFD.

(b) A is PID.

(c) $Cl(A)=\{0\}$.

Proof: (a)$\Rightarrow$(b): Thx to Thm in Sec 1.0, it's enough to show $\forall$ maximal ideal $\mathfrak{p}$ is principal. Pick $a\in\mathfrak{p}$, and decompose it into the product of prime elements: $a=p_1\ldots p_k$. Then $\exists i \mid p_i\in\mathfrak{p}$. Since (p_i) is a nonzero prime, (p_i) is a maximal ideal so $\mathfrak{p}=(p_i)$ finishing the proof.

(b)$\Leftrightarrow$(c): is an exercise (use that any fractional ideal is isomorphic to an ideal as an A-module, Lemma in Sec 2.1), and (b)$\Rightarrow$(a) is standard. $\square$

So, $Cl(A)$ measures how far A is from being UFD/PID.

2.3) Bonus: Class groups of rings of algebraic integers.

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.

2.4) Bonus: Class groups of algebras of functions on smooth affine curves.

Another class of Dedekind domains is the algebras $\mathbb{F}[X]$, where $\mathbb{F}$ is an algebraically closed field & $X\subset\mathbb{F}^n$ is an irreducible algebraic subset, which is a "smooth curve" (to be elaborated on in a bonus lecture). The class group of $\mathbb{F}[X]$ behaves very differently from the case of algebraic integers (e.g. if it's nonzero, then it's not finitely generated). We'll discuss more of this in the remaining bonus lecture.

2.5) Bonus: Generalization - Picard group.

One question is how to generalize $Cl(A)$ from the case when A is a Dedekind domain to the case of more general rings. There are two possible generalizations:

- The class group $Cl(A)$ that makes sense for general normal Noetherian domain A that measures the failure of A to be a UFD, and is a more direct generalization.
- The Picard group $Pic(A)$ that makes sense for a general ring (and even generalizes to noncommutative rings), that looks quite differently but coincides with $Cl(A)$ for "regular domains" of which Dedekind domains are a special case.

The group $Pic(A)$ nicely connects to our study of tensor products, and, to an extent, to Category theory, so we are going to sketch necessary definitions. We say that an A-module M is invertible $\exists$ an A-module M' s.t. $M' \otimes_A M \simeq A$. Let $Pic(A)$ be the set of isomorphism classes of invertible A-modules. The tensor product operation makes $Pic(A)$ into an abelian group.

Here's a categorical significance of $Pic(A)$. Tensoring with an A-module gives a functor $A\text{-Mod} \to A\text{-Mod}$. This functor is a category equivalence (see Bonus to Lec 13) iff M is invertible. Moreover, all category equivalences of A-Mod preserving a suitable structure (the A-linear structure, a variant of the additive structure, see Bonus to Lec 18) come from tensoring w. an invertible module. Oversimplifying a bit, one can say that $Pic(A)$ is the group of symmetries of the A-linear category A-Mod.