Lecture 6: Factorization of ideals

Last time:

Dedekind domain: int domain which is Noetherian, integrally closed, and every prime ideal is maximal.

Goal Thm: $\mathcal{O}$ a Dedekind domain. Every ideal

$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n$ where $\mathfrak{p}_i$ are prime, unique up to order.

[discuss in context of divisibility]

Not obvious as don't know

$$\mathfrak{a} \text{ not prime} \Rightarrow \mathfrak{a} = \mathfrak{b}\mathfrak{c}$$

$$\mathfrak{b} \mid \mathfrak{a} \Rightarrow \mathfrak{a} = \mathfrak{b}\mathfrak{c}$$

$\mathfrak{a}$ may not be a prod of primes but at least divides one

Lemma $\mathfrak{a} \neq 0$ an ideal of $\mathcal{O}$. Then

$\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$ where $\mathfrak{p}_i$ are prime.

Pf: $\mathcal{M} = \{\text{ideals not sat this}\}$. Let $\mathfrak{a} \in \mathcal{M}$ be maximal. As $\mathfrak{a}$ isn't prime, there are $b_1, b_2 \notin \mathfrak{a}$ with $b_1 b_2 \in \mathfrak{a}$. Idea: If $\mathfrak{a} = (b_1 b_2)$ then $\mathfrak{a} = (b_1)(b_2)\ldots$

Let $\mathfrak{a}_i = (b_i) + \mathfrak{a}$, which is not in $\mathcal{M}$ as $\mathfrak{a}_i \supsetneq \mathfrak{a}$.

But then

$$\mathfrak{a} \supseteq \mathfrak{a}_1 \mathfrak{a}_2 \supseteq \begin{pmatrix}\text{prod of}\\ \text{primes}\end{pmatrix}\begin{pmatrix}\text{prod of}\\ \text{primes}\end{pmatrix} = \begin{pmatrix}\text{prod of}\\ \text{primes}\end{pmatrix},$$

contradicting that $\mathfrak{a} \in \mathcal{M}$. ∎

Lemma: $\mathfrak{p}$ a prime ideal of $\mathcal{O}$. Set

$$\mathfrak{p}^{-1} = \{ k \in K \mid k\mathfrak{p} \subseteq \mathcal{O} \}$$

Closed under $+$, mult by elts of $\mathcal{O}$. "Fractional Ideal"

Ex: $\mathcal{O} = \mathbb{Z}$, $\mathfrak{p} = \langle 2 \rangle$, $\mathfrak{p}^{-1} = \{ \frac{a}{2} \mid a \in \mathbb{Z} \}$, $(6)\mathfrak{p}^{-1} = (3) \neq (6)$

Then $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ for all ideals $\mathfrak{a} \neq 0$.

[means $\{ \sum a_i p_i \mid a_i \in \mathfrak{a}, p_i \in \mathfrak{p}^{-1} \}$]

Motivation: If $\mathfrak{p} \mid \mathfrak{a}$, then $\mathfrak{a}\mathfrak{p}^{-1}$ is an ideal of $\mathcal{O}$, strictly containing $\mathfrak{a} \Rightarrow$ progress.

Proof: Claim: $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Pick $a \neq 0$ in $\mathfrak{p}$. Find primes $\mathfrak{p}_i$ so that
$\mathfrak{p} \supseteq (a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$ where n minimal.

Now $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i as if not take $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ and observe $a_1 \cdots a_n \in \mathfrak{p}$. As prime ideals are maximal, must have $\mathfrak{p} = \mathfrak{p}_i$. Say $\mathfrak{p} = \mathfrak{p}_1$. Pick $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_n \setminus (a)$, so $\frac{b}{a} \notin \mathcal{O}$. But $\frac{b}{a} \in \mathfrak{p}^{-1}$ as $\frac{b}{a}\mathfrak{p} = \frac{1}{a} b\mathfrak{p} \subseteq \frac{1}{a}(a) \subseteq \mathcal{O}$.

This proves the claim.

Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}$, with generators $\alpha_1, \dots, \alpha_n$. Assume $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Let $k \in \mathfrak{p}^{-1}$. Will show $k \in \mathcal{O}$. Consider $\vec{\alpha} = (\alpha_1, \dots, \alpha_n) \in K^n$. As $k\alpha_i \in \mathfrak{a}$ for all i, there is $A \in M_n(\mathcal{O})$ such that $k\vec{\alpha} = A\vec{\alpha}$. Thus k is a root of $\mathrm{char}(A)$ a monic poly in $\mathcal{O}[x]$. As $\mathcal{O}$ is integrally closed, $k \in \mathcal{O}$. But then $\mathfrak{p}^{-1} = \mathcal{O}$, contradicting the claim. ▨

<u>Cor</u>: $\mathfrak{p}$ a prime ideal. Then $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

<u>Pf</u>: By lemma, we have $\mathfrak{p} \subsetneq \underbrace{\mathfrak{p}\mathfrak{p}^{-1}}_{\text{ideal}} \subseteq \mathcal{O}$. As prime ideals are maximal, must have $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

<u>Proof of Theorem</u>: <u>Existence</u>: Let $\mathfrak{a}$ be a max elt of

$$\mathcal{M} = \left\{ \begin{array}{l} \text{ideals not } (0) \text{ or } (1) \\ \text{lacking prime decomp.} \end{array} \right\}.$$

Pick a max ideal $\mathfrak{p} \supsetneq \mathfrak{a}$. Now

$$\underset{\text{by Lemma}}{\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$$

as otherwise $\overset{\mathfrak{a}}{\overset{\|}{\mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p}}} = \overset{\mathfrak{p}}{\overset{\|}{\mathfrak{p}\mathfrak{p}^{-1}\mathfrak{p}}}$

So $\mathfrak{a}\mathfrak{p}^{-1}$ is a proper ideal of $\mathcal{O}$ not in $\mathcal{M}$ $\Rightarrow$ has a prime factorization. But then

$$\mathfrak{a} = (\mathfrak{a}\mathfrak{p}^{-1})\mathfrak{p}$$ has one as well, a contradiction ▨

<u>Uniqueness</u>: on HW.