Lecture 5:

HW #2 Due Wed Feb 11.

Ch2 # 22, 27, 29, 30

Ch3 # 4 and others to be assigned

Last time: $(\mathcal{O}_K, +) \cong \mathbb{Z}^n$ where $n = [K:\mathbb{Q}]$

Goal: restoring unique factorization for $\mathcal{O}_K$.

Motivation (from HW): $K = \mathbb{Q}(\sqrt{-5})$

$$2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$ all factors irreducible.

Take norms: $4 \cdot 9 = 6 \cdot 6$

Kummer (ideal #'s): β_1, β_2, of norm 2

β_3, β_4 of norm 3

$$6 = \underbrace{(\beta_1\beta_2)}_{2}\underbrace{(\beta_3\beta_4)}_{3} = \underbrace{(\beta_1\beta_3)}_{1+\sqrt{-5}}\underbrace{(\beta_2\beta_4)}_{1-\sqrt{-5}}$$

Dedekind reformulated as

$I \subseteq R$ is an ideal if $a+b \in I$ when $a, b \in I$

$\uparrow$ ring and $ra \in I$ when $r \in R$, $a \in I$

I = those "regular numbers" divisible by some "ideal number".

Ex: $\beta_1 \leftrightarrow \{2, 1+\sqrt{-5}, 3+\sqrt{-5}, 4, \dots\} \subseteq \mathcal{O}_K$ $\swarrow$ principle ideal gen by 2.

$2 \leftrightarrow \{2, 4, 2+2\sqrt{-5}, \dots\} = \{2\cdot\alpha \mid \alpha \in \mathcal{O}_K\} = \langle 2 \rangle$

$I \cdot J = \{ \sum_{\ell=1}^{m} i_\ell j_\ell \mid i_\ell \in I \text{ and } j_\ell \in J \}$

$I | J$ is defined to mean $I \supseteq J$

If R is an integral domain, then

$$\begin{array}{ccc} R \setminus \{0\} & \longrightarrow & \begin{array}{c}\text{non-zero} \\ \text{ideals} \\ \text{of } R\end{array} \\ r & \longmapsto & \langle r \rangle \end{array}$$

respects $\cdot$ and $|$,

kernel is $R^\times$

image is $\left\{\begin{array}{c}\text{principal} \\ \text{ideals}\end{array}\right\}$

This Week's

Goal: Every ideal $\mathfrak{a}$ in $\mathcal{O}_K$ (other than (0) and (1)) has a unique factorization $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k$ into prime ideals.

Ex: $(6) = \mathfrak{p}_1^2 \mathfrak{p}_3 \mathfrak{p}_4$ where $\mathfrak{p}_1 = \langle 2, 1+\sqrt{-5} \rangle$

$\mathfrak{p}_3 = \langle 3, 1+\sqrt{-5} \rangle$, $\mathfrak{p}_4 = \langle 3, 1-\sqrt{-5} \rangle$

[On to background...]

Def: A ring R is Noetherian if every nonempty set S of ideals has a maximal elt (w.r.t. inclusion)

[$\Leftrightarrow$ every ideal is finitely generated

$\Leftrightarrow$ every increasing seq of ideals is eventually constant]

Note: Equiv, no ideal is infinitely divisible.

Ex: $\mathbb{Z}$, $\mathbb{Q}[x_1, \dots, x_n]$; Non Ex: $\mathbb{Q}[x_1, x_2, \dots\dots]$

Ex: $\mathcal{O}_K$, K a number field

Pf: $(\mathcal{O}_K, +)$ is finitely generated.

Def: R (int domain) is integrally closed in its field of fractions $K = \{\frac{\alpha}{\beta} \mid \alpha, \beta \in R\}$ if whenever $k \in K$ is a root of a monic poly in $R[x]$ then $k \in R$.

Ex: $R = \mathbb{Z}$, $K = \mathbb{Q}$, by Gauss's Lemma.

Non Ex: $R = \mathbb{Z}[\sqrt{5}]$, $K = \mathbb{Q}(\sqrt{5}) \leftarrow \left\{ \frac{a+b\sqrt{5}}{c+d\sqrt{5}} \,\middle|\, a,b,c,d \in \mathbb{Z} \right\}$

$\rho = \frac{1+\sqrt{5}}{2}$ is a root of $x^2 - x - 1 = 0$ but not in R.

Ex: K a number field, $R = \mathcal{O}_K$.
Then R is int closed in K ($\cong$ field of fractions)
Ex.

Pf: Suppose $k \in K$ is a root of a monic poly $f(x) \in \mathcal{O}_K[x]$.
Then
$$\prod \sigma_i(f(x)) \qquad \sigma_i : K \hookrightarrow \overline{\mathbb{Q}} \text{ embeddings}$$
is a monic poly in $\mathbb{Z}[x]$ with k as a root.
So $k \in \mathcal{O}_K$. ∎

Def: An int domain R is a Dedekind domain if it is Noetherian, int. closed, and every prime ideal is maximal.

Ex: $\mathcal{O}_K$, K a number field
$\mathbb{C}[X]$, $X \subseteq \mathbb{C}^2$ a nonsingular curve

Point: Dedekind domains have unique factorization of ideals. More "natural" notion than a P.I.D.

Pf that $\mathcal{O}_K$ is Dedekind: $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime ideal.

$\mathfrak{p} \cap \mathbb{Z}$ is a non-zero prime ideal in $\mathbb{Z}$

if $\alpha \in \mathfrak{p}$, sat $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$
where $a_i \in \mathbb{Z}$, $a_0 \neq 0$. $\Longrightarrow a_0 \in \mathfrak{p} \cap \mathbb{Z}$.

$\mathcal{O}_K/\mathfrak{p}$ is an extension of $\mathbb{Z}/\mathfrak{p}\cap\mathbb{Z} \cong \mathbb{F}_{p^n}$ by adjoining algebraic elts; its a finite integral domain, hence a field. So $\mathfrak{p}$ is maximal. ∎