Lecture 5:
HW #2 Due Wed Feb 11.
Ch 2 # 22, 27, 29, 30
Ch 3 # 4 and others to be assigned

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

Goal: restoring unique factorisation for \(O_K\).

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

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

Take norms: \(4 \cdot 9 = 6 \cdot 6\)


torem

Kummer (Local #15): \(\beta_1, \beta_2, \text{ of norm } 2\)
\(\beta_3, \beta_4, \text{ of norm } 3\)

\[6 = \left(\frac{\beta_1\beta_2}{2}\right) \left(\frac{\beta_3\beta_4}{3}\right) = \left(\frac{\beta_1\beta_3}{1+\sqrt{-5}}\right) \left(\frac{\beta_2\beta_4}{1-\sqrt{-5}}\right)\]

Dedekind reformulated as

\(I \subseteq \mathcal{O}_K\) is an ideal if \(a + b\sqrt{5} \in I\) whenever \(a, b \in I\)

and \(ra \in I\) whenever \(r \in \mathcal{O}_K, a \in I\)

\(I = \text{ those "regular numbers" divisible by some "ideal numbers" } \)

\(\perp\) principle ideal gen

\(\exists x:\ \beta_1 \leftrightarrow \{2, 1+\sqrt{-5}, 3+\sqrt{-5}, 4, \ldots\} \subseteq \mathcal{O}_K\)

\(\perp\) \(\beta_1 = 2\).

\[2 \leftrightarrow \{2, 4, 2+2\sqrt{-5}, \ldots\} = \{2 \cdot x | x \in \mathcal{O}_K\}^2 = \langle 2 \rangle\]
I \cdot J = \{ \sum_{k=1}^{m} i_k j_k \mid i_k \in I \text{ and } j_k \in J \}

I \mid J \text{ is defined to mean } I \subseteq J

If R is an integral domain, then

\[
R \setminus \{0\} \rightarrow \text{ ideals of } R \text{ respecting } 0 \text{ and } 1,
\]

\[
r \mapsto \langle r \rangle
\]

kernel is \( R^* \)

image is \{ principal ideals \}

This Week's Goal:

Every ideal \( \mathfrak{a} \) in \( \mathcal{O}_K \) (other than \( (0) \) and \( (1) \)) has a unique factorization

\( \mathfrak{a} \mathfrak{a}^{-1} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \)

into prime ideals.

Ex: \( (6) = \mathfrak{p}_1^2 \mathfrak{p}_2 \mathfrak{p}_4 \) 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 (wrt. inclusion)

\( \iff \) every ideal is finitely generated

\( \iff \) every increasing seq of ideals is eventually constant

Note: Equiv, no ideal is infinitely divisible.
Ex: $\mathbb{Z}, \mathbb{Q}[x_1, \ldots, x_n]$; Non Ex: $\mathbb{Q}[x_1, x_2, \ldots]$

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

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

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

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

Non Ex: $R = \mathbb{Z}[(\sqrt{5})]$, $K = \mathbb{Q}(\sqrt{5})$

$p = \frac{1 + \sqrt{5}}{2}$ 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 $K (\approx$ field of fractions $)$

Rf: Suppose $k \in K$ is a root of a nonic poly $f(x) \in \mathcal{O}_K[x]$.

Then $\prod \mathcal{O}_i(f(x)) \in \mathcal{O}_i$ is a nonic poly in $\mathbb{Z}[x]$ with $k$ as a root.

So $k \in \mathcal{O}_K$. 

\[\diamondsuit\]
Def: An integral domain \( R \) is a Dedekind domain if it is Noetherian, int. closed, and every prime ideal is maximal.

Ex: \( \mathbb{Q}_K \), \( K \), a number field, \( \mathbb{C}[x], x \in \mathbb{C}^2 \) a nonsingular curve.

Point: Dedekind domains have unique factorization of ideals, more "natural" notion than a PID.

If that \( \mathbb{Q}_K \) is Dedekind, \( \mathfrak{p} \subseteq \mathbb{Q}_K \) a prime ideal, \( \mathfrak{p} \mathbb{Z} \) is a non-zero prime ideal in \( \mathbb{Z} \) if \( \alpha \in \mathfrak{p} \), sat \( \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0 \) where \( a_i \in \mathbb{Z}, a_0 \neq 0 \). \( \Rightarrow a_0 \in \mathfrak{p} \mathbb{Z} \).

\( \mathbb{Q}_K/\mathfrak{p} \) is an extension of \( \mathbb{Q}_\mathbb{Z}/\mathfrak{p} \mathbb{Z} \cong \mathbb{F}_p^n \) by adjoining algebraic elements; it's a finite integral domain, hence a field. So \( \mathfrak{p} \) is maximal.