Lecture 8: Norms of ideals

<u>Reminder</u>: HW due Wednesday.

<u>Change</u>: Office hour on Tuesday 2-3 (+ Mon 10-11)

<u>Last time</u>:

<u>Thm</u>: $\mathcal{O}$ a Dedekind domain. Then every ideal $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_n$ with $\mathfrak{p}_i$ prime, unique up to order.

<u>Goal</u>: Splitting of primes in extensions

$$\begin{array}{ll} \mathbb{Q}(i) \supseteq \mathbb{Z}[i] & (5) = (2+i)(2-i), \ (3) \text{ is prime} \\ \quad | & \\ \mathbb{Q}(i) \supseteq \mathbb{Z} & \end{array}$$

K a number field, $\mathcal{O}_K$ integers in K.

For $\mathfrak{a} \neq 0$ an ideal of $\mathcal{O}_K$, define its norm by

$$\mathcal{N}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] \in \mathbb{N}$$

[Book uses $\|\mathfrak{a}\|$ instead.]

<u>Makes sense</u>: By HW, $(\mathfrak{a}, +) \cong \mathbb{Z}^n \cong (\mathcal{O}_K, +)$ and thus by HW the index is finite.

Suppose $\mathfrak{a} = (\alpha)$. Then

$$\mathcal{N}(\mathfrak{a}) = |\mathcal{N}_{K/\mathbb{Q}}(\alpha)|$$

Pf: Let $\omega_1, \omega_2, \dots, \omega_n$ be an integral basis for $\mathcal{O}_K$.

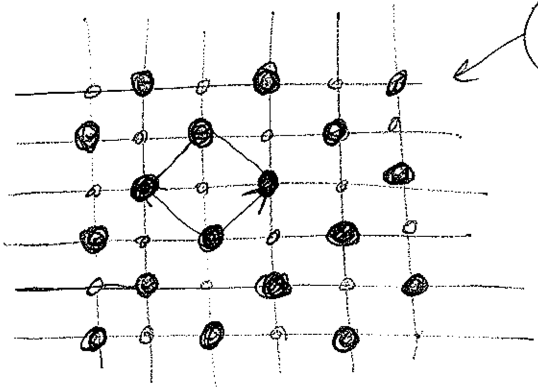
Let A be the matrix of $T_\alpha : K \to K$, $k \mapsto k\alpha$ with respect to $\{\omega_1, \dots, \omega_n\}$.

By def, $N_{K/\mathbb{Q}}(\alpha) = \det A$. Now the i^{th} column of A expresses $\alpha\omega_i$ in terms of $\{\omega_1, \dots, \omega_n\}$, and $\{\alpha\omega_1, \dots, \alpha\omega_n\}$ are a $\mathbb{Z}$-basis for $\mathfrak{a}$. So the column span of $A = \mathfrak{a} \subseteq \mathcal{O}_K \cong \mathbb{Z}^n$. Then

$$[\mathcal{O}_K : \mathfrak{a}] = |\det A| = |N_{K/\mathbb{Q}}(\alpha)|. \qquad \blacksquare$$

<u>Example:</u>

$K = \mathbb{Q}(i)$



$(\mathbb{Z}[i], +) \cong \mathbb{Z}^2$

$\mathfrak{a} = (1+i)$

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$\det A = 2 = [\mathcal{O}_K : \mathfrak{a}] = N(1+i)$$

<u>Expect:</u> N should be multiplicative

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})\, N(\mathfrak{b})$$

Follows from:

<u>Prop</u>: If $\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_n^{v_n}$ is the prime factorization of an ideal in $\mathcal{O}_K$, then $N(\mathfrak{a}) = \prod N(\mathfrak{p}_i)^{v_i}$.

Pf: By the Chinese Remainder Theorem:

$$\mathcal{O}_K/\mathfrak{a} \cong \mathcal{O}_K/\mathfrak{p}_1^{v_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_n^{v_n}$$

since $\underbrace{\mathfrak{p}_i^{v_i} + \mathfrak{p}_j^{v_j}}_{\gcd} = \mathcal{O}_K$. Thus $[\mathcal{O}_K : \mathfrak{a}] = \prod [\mathcal{O}_K : \mathfrak{p}_i^{v_i}]$, so we've reduced to the case $\mathfrak{a} = \mathfrak{p}^v$. Consider $\mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \cdots \supsetneq \mathfrak{p}^v$ properly by unique factorization.

Now $V = \mathfrak{p}^k/\mathfrak{p}^{k+1}$ is a module (= vector space) over $F = \mathcal{O}_K/\mathfrak{p}$. <u>Claim</u>: $\dim_F V = 1$

Let $\alpha \in \mathfrak{p}^k \setminus \mathfrak{p}^{k+1}$. Will show $F\alpha = V$. Let $\mathfrak{b} = (\alpha) + \mathfrak{p}^{k+1}$. Then $\mathfrak{p}^k \supseteq \mathfrak{b} \supsetneq \mathfrak{p}^{k+1}$ which forces $\mathfrak{p}^k = \mathfrak{b}$, as otherwise $\mathcal{O} \supsetneq \mathfrak{p}^{-k}\mathfrak{b} \supsetneq \mathfrak{p}$, contradicting maximality of $\mathfrak{p}$. So $F\alpha = V$, proving the Claim.

Thus

$$[\mathcal{O}_K : \mathfrak{p}^\nu] = [\mathcal{O} : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{\nu-1} : \mathfrak{p}^\nu]$$

$$= |F|^\nu = \mathcal{N}(\mathfrak{p})^\nu \quad \text{as desired.} \quad \blacksquare$$

[Skip ahead to next page if short on time.]

Ex: $K = \mathbb{Q}(\zeta)$, where ζ is a p^{th} root of unity. If $\lambda = 1-\zeta$, then (λ) is a ideal of norm p, hence prime. Moreover $(p) = (\lambda)^{p-1}$

Proof: $\phi_p(X) = \dfrac{X^p - 1}{X-1} = X^{p-1} + \cdots + X + 1 = \prod_{k=1}^{p-1} (X - \zeta^k)$

Then $\phi_p(1) = p = \prod_{K=1}^{p-1} (1-\zeta^k) = \mathcal{N}_{K/\mathbb{Q}}(\lambda) = \mathcal{N}((\lambda))$

Moreover, as ideals $(1-\zeta^k) = (1-\zeta)$ because

$$1-\zeta^k = \varepsilon_k(1-\zeta) \text{ where } \varepsilon_k = 1 + \zeta + \cdots + \zeta^{k-1} \in \mathcal{O}_K$$

and ε_k is a unit: If $k'k \equiv 1 \bmod p$ then

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1-(\zeta^k)^{k'}}{1-\zeta^k} = 1 + \zeta^k + \cdots + (\zeta^k)^{k'-1} \in \mathcal{O}_K.$$

Thus $(p) = (\lambda)^{p-1}$. $\blacksquare$

Combining Fields: $\mathcal{O}_{KL} \supseteq \mathcal{O}_K \mathcal{O}_L$

$$\begin{tikzcd}[column sep=small]
 & KL \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash, "m"'] & & L \arrow[dl, dash, "n"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Thm: If $[KL:\mathbb{Q}] = mn$

then $\mathcal{O}_{KL} = \frac{1}{d}\mathcal{O}_K \mathcal{O}_L$

where $d = \gcd(\Delta_K, \Delta_L)$.

When $d = 1$, $\Delta_{KL} = \Delta_K^n \Delta_L^m$.

Pf: See text.

If time remains, discuss $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ as lead in to Friday's class.