Geometry of Numbers

Let $K/\mathbb{Q}$ a number field, $\mathcal{O}_K$ the ring of integers. Recall that

$$\mathcal{F} = \{ \mathfrak{f} \subseteq \mathcal{O}_K : \exists a \in \mathcal{O}_K \text{ s.t. } \{0\} \neq a\mathfrak{f} \trianglelefteq \mathcal{O}_K \}.$$

We have two operations on $\mathcal{F}$ by

$$\mathfrak{f} + \mathfrak{g} = \mathcal{O}_K\text{-submodule generated by } \mathfrak{f} \cup \mathfrak{g},$$

$$\mathfrak{f} \cdot \mathfrak{g} = \mathcal{O}_K\text{-submodule generated by } \{ab : a \in \mathfrak{f}, b \in \mathfrak{g}\}.$$

We are interested in understanding the multiplication.

Corollary of prime factorization

$(\mathcal{F}, \mathcal{O}_K, \cdot)$ is an abelian group and $\mathcal{P} = \{a \cdot \mathcal{O}_K : a \in K^\times\}$ is a subgroup.

Definition

The class group of K is the group $Cl(K) := \mathcal{F}/\mathcal{P}$

Theorem:

Let $K/\mathbb{Q}$ a #-field, then $|Cl(K)| < \infty$

Remark: There are versions of the above valid for K a finite extension of $\mathbb{F}_q(T)$. The more general argument (with a weaker conclusion that what we will obtain) can be found in the lecture notes.

Standing assumption

$K/\mathbb{Q}$ is a number field, $\mathcal{O}_K$ is the maximal order, $d = [K:\mathbb{Q}]$.

Recall: Let $\underline{a} \triangleleft \mathcal{O}_K$ non-zero, then $\underline{a}$ is a lattice and

$$[\mathcal{O}_K : \underline{a}]^2 = \frac{\Delta(\underline{a})}{\Delta(\mathcal{O}_K)} < \infty$$

where Δ was the discriminant of the lattice:

$$\Delta(\underline{a}) = \det(\sigma_i(\omega_j))^2,$$

where $(\sigma_1, \dots, \sigma_d)$ is an enumeration of $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ and $(\omega_1, \dots, \omega_d)$ is a $\mathbb{Z}$-basis of $\underline{a}$.

We assume throughout that $\sigma_1, \dots, \sigma_{r_1}$ are real, $\sigma_{r_1}, \dots, \sigma_{r_1+r_2}$ are complex, and $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$.

We let $\sigma_\infty : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the induced geometric embedding.

Lemma:

Let $z \in \mathcal{O}_K$, then $[\mathcal{O}_K : z.\mathcal{O}_K] = |Nr_{K/\mathbb{Q}}(z)|$

Proof: Note that $z.\mathcal{O}_K = [\times z]_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathcal{O}_K$. Hence

$$[\mathcal{O}_K : z.\mathcal{O}_K] = |\det([\times z]_{K/\mathbb{Q}})| = |Nr_{K/\mathbb{Q}}(z)|.$$

Definition (Norm of an ideal)

Let $\underline{a} \triangleleft \mathcal{O}_K$ non-zero, then $Nr(\underline{a}) = [\mathcal{O}_K : \underline{a}]$. We set $Nr(\{0\}) = 0$.

Proposition

(i) Let $\underline{a}, \underline{b} \triangleleft \mathcal{O}_K$, then $Nr(\underline{a}.\underline{b}) = Nr(\underline{a}) Nr(\underline{b})$

(ii) Let $p \in \mathbb{Z}$ a non-zero prime, $\mathfrak{p} \in Spec_p(\mathcal{O}_K)$. Then

$$Nr(\mathfrak{p}) = p^{f_{\mathfrak{p}|p}}.$$

Proof (ii) $Nr(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}] = |\mathcal{O}_K/\mathfrak{p}| = |k_{\mathfrak{p}}| = p^{\dim_{\mathbb{F}_p}(k_{\mathfrak{p}})} = p^{f_{\mathfrak{p}|p}}$.

(i) Suppose that $\underline{a}, \underline{b} \triangleleft \mathcal{O}_K$ are coprime, then

$$\mathcal{O}_K/\underline{a}.\underline{b} \overset{\text{CRT}}{\cong} \mathcal{O}_K/\underline{a} \oplus \mathcal{O}_K/\underline{b}.$$

Hence it suffices to show that $Nr(\mathfrak{p}^m) = Nr(\mathfrak{p})^m$ for all $\mathfrak{p} \in Spec(\mathcal{O}_K)$ non-zero.

We do this by induction. Suppose the claim was proven for $m \in \mathbb{N}$. Note that the sequence

$$0 \longrightarrow \underbrace{\mathfrak{p}^m/\mathfrak{p}^{m+1}}_{\cong k_{\mathfrak{p}}} \longrightarrow \mathcal{O}_K/\mathfrak{p}^{m+1} \longrightarrow \mathcal{O}_K/\mathfrak{p}^m \longrightarrow 0$$

is exact. Hence

$$\left|\mathcal{O}_K/\mathfrak{p}^{m+1}\right| = \left|\mathcal{O}_K/\mathfrak{p}^m\right| \cdot \left|\mathfrak{p}^m/\mathfrak{p}^{m+1}\right| = Nr(\mathfrak{p}^m) \cdot |k_{\mathfrak{p}}|$$

$$= Nr(\mathfrak{p})^m \, p^{f_{\mathfrak{p}|p}} \overset{(i)}{=} Nr(\mathfrak{p})^{m+1}.$$

$\blacksquare$

Definition: Let $\mathfrak{f} \in \mathcal{F}$ and $\mathfrak{a}, \mathfrak{b} \triangleleft \mathcal{O}_K$ s.t. $\mathfrak{f} = \mathfrak{b}^{-1} \cdot \mathfrak{a}$. Then $Nr(\mathfrak{f}) = Nr(\mathfrak{b})^{-1} Nr(\mathfrak{a})$.

Exercise: Show that this well-defined.

Proposition

Let $X \geq 1$. Then $|\{\mathfrak{a} \triangleleft \mathcal{O}_K : \mathrm{Nr}(\mathfrak{a}) \leq X\}| < \infty$.

Proof: Note that $\mathrm{Nr}(\underline{\mathfrak{a}}) = \prod_{\mathfrak{p} | \underline{\mathfrak{a}}} \mathrm{Nr}(\mathfrak{p})^{v_{\mathfrak{p}}(\underline{\mathfrak{a}})}$. If $\mathrm{Nr}(\underline{\mathfrak{a}}) \leq X$, then for all $\mathfrak{p} | \underline{\mathfrak{a}}$, we have that $\mathrm{Nr}(\mathfrak{p}) \leq X$. Since $\mathrm{Nr}(\mathfrak{p})$ is a power of the prime p generating $\mathfrak{p} \cap \mathbb{Z}$, any ideal of norm $\leq X$ is generated by ideals lying above primes $\leq X$. There are only finitely many such primes and for each, the number of primes above is uniformly bounded by the degree formula: $|\mathrm{Spec}_p(\mathcal{O}_K)| \leq d$. Hence every ideal is a product of primes varying among $\leq \pi(X) d$ prime ideals in $\mathcal{O}_K$. Each such prime has norm at least 2 and, hence, $v_{\mathfrak{p}}(\underline{\mathfrak{a}}) \leq \frac{\log X}{\log 2}$. $\boxtimes$

Geometry of numbers

Recall: · A subgroup $\Lambda < \mathbb{R}^d$ is discrete $\Leftrightarrow$ Λ is a free $\mathbb{Z}$-module of rank $r \leq n$ with a $\mathbb{Z}$-basis linearly independent over $\mathbb{R}$.

- A fundamental domain for $\Lambda \curvearrowright \mathbb{R}^d$ is a (measurable) subset $F \subseteq \mathbb{R}^d$ s.t.
$$\mathbb{R}^d = \bigsqcup_{v \in \Lambda} (F + v)$$
- If $\mathcal{B} = (v_1, \dots, v_r)$ is a $\mathbb{Z}$-basis of the discrete subgroup $\Lambda < \mathbb{R}^d$ and if $v_{r+1}, \dots, v_d \in \mathbb{R}^d$ are chosen so that $(v_1, \dots, v_d)$ is an $\mathbb{R}$-basis of $\mathbb{R}^d$, then
$$\mathcal{C} = \left\{ \sum_{i=1}^{d} \alpha_i v_i : \alpha_1, \dots, \alpha_r \in [0,1), \alpha_{r+1}, \dots, \alpha_d \in \mathbb{R} \right\}$$
is a fundamental domain for $\Lambda \curvearrowright \mathbb{R}^d$.
- The volume of a fundamental domain for $\Lambda \curvearrowright \mathbb{R}^d$ only depends on Λ. It is called the covolume.
- A (geometric) lattice $\Lambda < \mathbb{R}^d$ is a discrete subgroup of rank d.
- A discrete subgroup $\Lambda < \mathbb{R}^d$ is a lattice iff the covolume is finite.
- Let $\Lambda' < \Lambda < \mathbb{R}^d$ lattices. Then $\operatorname{covol}(\Lambda') = \operatorname{covol}(\Lambda)[\Lambda : \Lambda']$.

Exercise: Show that
$$\operatorname{covol}(\sigma_\infty(\mathfrak{f})) = 2^{-r_2} |\operatorname{disc}(\mathcal{O}_K)|^{\frac{1}{2}} \operatorname{Nr}(\mathfrak{f}).$$

Theorem (Minkowski's 1^{st} theorem)

Let $\Lambda < \mathbb{R}^d$ a lattice, $V \subseteq \mathbb{R}^d$ measurable s.t. $\mathrm{vol}(V) > \mathrm{covol}(\Lambda)$. Then

$$(V - V) \cap \Lambda \neq \{0\},$$

i.e., $\exists\, v_1, v_2 \in V$ s.t. $v_1 - v_2 \in \Lambda - \{0\}$.

Proof: We will show that there are distinct $\lambda_1, \lambda_2 \in \Lambda$ and $x \in P$ s.t.

$$x \in V - \lambda_i$$

Let $v_i \in V$ s.t. $v_i \in \lambda_i + P$. Then $v_1 \neq v_2$ since $(\lambda_1 + P) \cap (\lambda_2 + P) = \emptyset$ and

$$v_1 - v_2 = \lambda_1 + x - \lambda_2 - x = \lambda_1 - \lambda_2 \in \Lambda - \{0\}.$$

How do we find x, λ_1, λ_2?

$$\mathrm{vol}(P) < \mathrm{vol}(V) = \sum_{\lambda \in \Lambda} \mathrm{vol}((P + \lambda) \cap V) = \sum_{\lambda \in \Lambda} \mathrm{vol}(\overbrace{P \cap (V - \lambda)}^{\subseteq P}).$$

Since the sets on the right hand side are subsets of P but since the sum of the volumes exceeds the volume of P, they are not disjoint, i.e., $\exists\, \lambda_1 \neq \lambda_2 \in \Lambda$ s.t.

$$\emptyset \neq (P \cap (V - \lambda_1)) \cap (P \cap (V - \lambda_2)) = P \cap ((V - \lambda_1) \cap (V - \lambda_2)).$$

$\square$

Theorem (Minkowski's 2^{nd} theorem)

Let $\Lambda < \mathbb{R}^d$ a lattice, $V \subseteq \mathbb{R}^d$ compact convex symmetric (around 0). If
$$\mathrm{vol}(V) \geq 2^d \,\mathrm{covol}(\Lambda),$$
then $V \cap \Lambda \neq \{0\}$

Proof: Assume $\mathrm{vol}(V) > 2^d \,\mathrm{covol}(\Lambda)$, then $\mathrm{vol}(\frac{1}{2}V) > \mathrm{covol}(\Lambda)$ and, hence, there are $v_1, v_2 \in V$

V is symmetric

s.t. $\frac{1}{2}v_1 + \frac{1}{2}v_2 \in \Lambda - \{0\}$. Since V is convex, the claim follows.

Now suppose that V is compact and $\mathrm{vol}(V) = 2^d \,\mathrm{covol}(\Lambda)$. Let $V_m = (1 + \frac{1}{m})V$. Hence, for all $m \in \mathbb{N}$ $\exists\, v_m \in V_m \cap \Lambda - \{0\}$. Since $V_1 \supseteq V_m$, since V_1 is compact, and since Λ is discrete, the set $\{v_m : m \in \mathbb{N}\}$ is finite. Hence there is $v \in \{v_m : m \in \mathbb{N}\}$ s.t. $v \in V_m$ for ∞-many m. Since $V_1 \supseteq V_2 \supseteq V_3 \supseteq \ldots$, $v \in \bigcap_{m \in \mathbb{N}} V_m = V$.

Proposition

$\exists C_K$ depending only on r_1 and d s.t. the following is true.

$$\forall \mathfrak{a} \triangleleft \mathcal{O}_K \ \exists a \in \mathfrak{a} - \{0\} \quad |\mathrm{Nr}_{K/\mathbb{Q}}(a)| \leq C_K |\mathrm{disc}(\mathcal{O}_K)|^{\frac{1}{2}} \mathrm{Nr}(\mathfrak{a})$$

Proof: Let $K_\infty := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ viewed as an $\mathbb{R}$-algebra and let $\|\cdot\| : K_\infty \longrightarrow [0,\infty)$ be the norm defined by

$$(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \longmapsto \sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=1}^{r_2} |z_j| .$$

Let $B_t = \{v \in K_\infty : \|v\| \leq t\}$. Then B_t is convex, compact, symmetric, and

$$\mathrm{vol}(B_t) = \mathrm{vol}(B_1)\, t^d = \frac{2^{r_1} \left(\frac{\pi}{2}\right)^{r_2}}{d!} t^d$$

(cf. Samuel, Ch. IV, Appendix).

Choose t s.t. $\mathrm{vol}(B_t) = 2^d \operatorname{covol}(\sigma_\infty(\mathfrak{a}))$, then

$$\sigma_\infty(\mathfrak{a}) \cap B_t \neq \{0\}.$$

Let $a \in \mathfrak{a} - \{0\}$ s.t. $\sigma_\infty(a) \in B_t$, then

$$|\mathrm{Nr}_{K/\mathbb{Q}}(a)| = \left(\left(\prod_{i=1}^{d} |\sigma_i(a)| \right)^{\frac{1}{d}} \right)^d \leq \left(\frac{1}{d} \sum_{i=1}^{d} |\sigma_i(a)| \right)^d = \left(\frac{1}{d} \|\sigma_\infty(a)\| \right)^d \leq \left(\frac{t}{d} \right)^d$$

$$t^d = \frac{\mathrm{vol}(B_t)}{\mathrm{vol}(B_1)}$$

$$= \frac{2^d}{d^d} \frac{\operatorname{covol}(\sigma_\infty(\mathfrak{a}))}{\mathrm{vol}(B_1)} = \frac{2^{d-r_1} d!}{d^d} \left(\frac{2}{\pi} \right)^{r_2} \cdot 2^{-r_2} |\mathrm{disc}(\mathcal{O}_K)|^{\frac{1}{2}} \mathrm{Nr}(\mathfrak{a}).$$

$\blacksquare$

Theorem

$|Cl(K)|$ is finite.

Lemma

Given $\underline{a} \lhd \mathcal{O}_K$ non-zero. There is a bijection

$$(\underline{a}-\{0\})/\mathcal{O}_K^\times \xrightarrow{\varphi} \{\underline{b} \lhd \mathcal{O}_K : [\underline{b}] = [\underline{a}^{-1}]\}.$$

such that for all $a \in \underline{a}-\{0\}$ we have

$$|Nr_{K|\mathbb{Q}}(a)| = Nr(\varphi(a))\,Nr(\underline{a}).$$

Proof: Consider the map $a \in \underline{a}-\{0\} \longmapsto a.\mathcal{O}_K.\underline{a}^{-1} =: \varphi(a)$. This is well-defined by unique factorization and, indeed, constant on $\mathcal{O}_K^\times$-orbits. We have

$$[\underline{a}].[\varphi(a)] = [a.\mathcal{O}_K] = [\mathcal{O}_K],$$

i.e., $[\varphi(a)] = [\underline{a}^{-1}]$. If $\varphi(a) = \varphi(a')$, then $\varphi(a)\underline{a} = \varphi(a')\underline{a}$, thus $a' \in a\mathcal{O}_K^\times$, i.e., φ is injective on $\mathcal{O}_K^\times$-orbits in $\underline{a}-\{0\}$. Now suppose that $\underline{b} \lhd \mathcal{O}_K$ such that $[\underline{b}] = [\underline{a}^{-1}]$, i.e., there is $b \in K-\{0\}$ s.t. $\underline{b}.\underline{a} = b.\mathcal{O}_K$. Since $\underline{b}.\underline{a} \lhd \mathcal{O}_K$, we know that $b \in \mathcal{O}_K$. Moreover, $\underline{a} \mid b.\mathcal{O}_K$ implies $b \in \underline{a}-\{0\}$. Hence $\underline{b} = b.\mathcal{O}_K.\underline{a}^{-1} = \varphi(b)$, i.e., φ is onto. ∎

Theorem

There exists $M_K > 0$ and for every $x \in Cl(K)$ there exists $\underline{b} \lhd \mathcal{O}_K$ s.t.

$$\underline{b} \in x \quad \text{and} \quad Nr(\underline{b}) \leq M_K .$$

In particular, $Cl(K)$ is finite (since $|\{\underline{a} \lhd \mathcal{O}_K : Nr(\underline{a}) \leq M_K\}| < \infty$).

Proof: For every $\underline{a} \lhd \mathcal{O}_K$ there exists $a \in \underline{a} - \{0\}$ s.t. $|Nr(a)| \leq C_K |disc(\mathcal{O}_K)|^{\frac{1}{2}} Nr(\underline{a})$.

Let $\underline{b} = a \cdot \mathcal{O}_K \cdot \underline{a}^{-1}$, then $Nr(\underline{b}) \leq C_K |disc(\mathcal{O}_K)|^{\frac{1}{2}}$ and $[\underline{b}] = [\underline{a}^{-1}]$.

Since $[\underline{a}]^{-1} = [\underline{a}^{-1}]$ and since inversion is a bijection on $Cl(K)$, i.e., $\forall x \in Cl(K) \, \exists \underline{a} \lhd \mathcal{O}_K$ s.t. $x = [\underline{a}]^{-1}$, this proves the claim. $\square$

Corollaries (exercises)

- Minkowski's bound: Let $x \in Cl(K)$, then there is $\mathfrak{a} \in x$ an ideal in $\mathcal{O}_K$ s.t.

$$Nr(\mathfrak{a}) \leq \frac{d!}{d^d}\left(\frac{4}{\pi}\right)^{r_2} |disc(\mathcal{O}_K)|^{\frac{1}{2}}.$$

- $\forall d \in \mathbb{N}\ \forall \varepsilon > 0\ \exists C_\varepsilon > 0\ \forall K/\mathbb{Q}$ #-field of degree d

$$|Cl(K)| \leq C_\varepsilon |disc(K)|^{\frac{1}{2}+\varepsilon}.$$

- Hermite-Minkowski: Let $K/\mathbb{Q}$ a #-field of degree d, then

$$|disc(K)| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{[K:\mathbb{Q}]-1}.$$

In particular, no finite extension of $\mathbb{Q}$ is totally unramified.