11. Finiteness of the ideal class group

Recall from last week: K = number field

$I \in \mathcal{J}(K)$ fract. ideal

Then $I \subset K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^n$, $n = [K : \mathbb{Q}]$

is a lattice

$$\mathrm{Norm}(I) = \underset{\text{index}}{[\mathcal{O}_K : I]} = \frac{\mathrm{Vol}(I)}{\mathrm{Vol}(\mathcal{O}_K)}$$

in the case $I \subset \mathcal{O}_K$: $[\mathcal{O}_K : I] = |\mathcal{O}_K / I|$

Vol = volume, unique up to multiplication by a positive constant

If $\Lambda \subset \mathbb{R}^n$ is a lattice, then

$$\mathrm{Vol}(\Lambda) = \mathrm{Vol}(\mathbb{R}^n/\Lambda) = \mathrm{Vol}(F),$$

where F = fund. domain for Λ.

We have shown: $\forall d > 0$ $\exists$ only finitely many ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $\mathrm{Norm}(\mathfrak{a}) < d$ (Proposition 10.2)

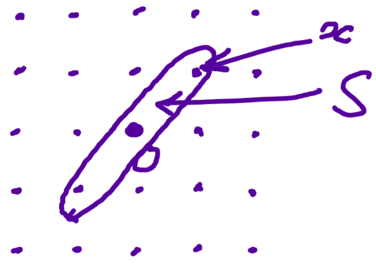
<u>Prop 11.1</u> Let $\Lambda \subset \mathbb{R}^n$ be a lattice, $S \subset \mathbb{R}^n$ a bounded, convex open set, s.t. $0 \in S$, and S is symmetric.

(symmetric means $x \in S \Leftrightarrow -x \in S$)

Assume $Vol(S) \geq 2^n Vol(\Lambda)$. Then

$\exists\, 0 \neq x \in \overline{S} \cap \Lambda$

closure of S



Proof Case 1: $Vol(S) > 2^n Vol(\Lambda)$

Notation: $\lambda \in \mathbb{R}$ then $\lambda S = \{\lambda x \mid x \in S\}$

$$Vol(\lambda S) = \lambda^n Vol(S)$$

Consider the map $f: \frac{1}{2} S \xrightarrow[\text{projection}]{} \mathbb{R}^n / \Lambda$

If f is injective, then

$$\underbrace{Vol\left(\tfrac{1}{2} S\right)}_{2^{-n} Vol(S)} \leq Vol(\mathbb{R}^n/\Lambda) = Vol(\Lambda)$$

$2^{-n} Vol(S)$ — contradiction

$\Rightarrow f$ is not injective $\Rightarrow \exists\, x_1 \neq x_2 \in S$

s.t. $f(\frac{1}{2} x_1) = f(\frac{1}{2} x_2) \Rightarrow \exists\, y \in \Lambda$, s.t.

$$\frac{1}{2} x_1 = \frac{1}{2} x_2 + y \Rightarrow \frac{1}{2}(x_1 - x_2) = y$$

S - symmetric $\Rightarrow -x_2 \in S$

S - convex $\Rightarrow x = \frac{1}{2}(x_1 - x_2) \in S$

then $0 \neq x \in S \cap \Lambda \subset \overline{S} \cap \Lambda$

Case 2: $Vol(S) = 2^n Vol(\Lambda)$

For $\lambda > 1$ $\quad Vol(\lambda S) > 2^n Vol(\Lambda)$

$\Rightarrow$ by case 1 $\quad \exists\, x \in (\lambda S \cap \Lambda) \setminus \{0\}$

Let $\lambda_n = 1 + \frac{1}{n}$, $\quad 0 \neq x_n \in \lambda_n S \cap \Lambda$

$\forall n \quad x_n \in \underbrace{(2S \cap \Lambda) \setminus \{0\}}_{\text{a finite set}}$

$\Rightarrow \exists\, x \in \Lambda \setminus \{0\}$ s.t. $x = x_n$ for infinitely many n

$\Rightarrow x \in \lambda S \quad \forall \lambda > 1$

$\Rightarrow \frac{1}{\lambda} x \in S; \quad \frac{1}{\lambda} x \xrightarrow[\lambda \to 1]{} x \Rightarrow x \in \overline{S}$

We conclude: $\quad x \in \overline{S} \cap \Lambda \setminus \{0\}$ $\quad \square$

To compute volumes of ideals, we will choose special coordinates in $K \otimes_{\mathbb{Q}} \mathbb{R}$

<u>The $\mathbb{R}$-algebra structure on $K \otimes_{\mathbb{Q}} \mathbb{R}$</u>

By the primitive element theorem

$$K \simeq \frac{\mathbb{Q}[X]}{(f)} \quad \text{where } f \in \mathbb{Q}[X] \text{ irred.}$$

$\deg(f) = n = [K : \mathbb{Q}]$

$$K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \frac{\mathbb{Q}[X]}{(f)} \otimes_{\mathbb{Q}} \mathbb{R} = \frac{\mathbb{R}[X]}{(f)}$$

In $\mathbb{R}[X]$ $\quad f = \prod_{i=1}^{r_1} f_i \cdot \prod_{j=1}^{r_2} g_j$, where

$\deg(f_i) = 1$, $\quad \deg(g_j) = 2 \Rightarrow r_1 + 2r_2 = n$

f_i, g_j all pairwise coprime, irreducible

$$\overset{CRT}{\Longrightarrow} \quad \frac{\mathbb{R}[x]}{(f)} \simeq \prod_{i=1}^{r_1} \underbrace{\frac{\mathbb{R}[x]}{(f_i)}}_{\mathbb{R}} \times \prod_{j=1}^{r_2} \underbrace{\frac{\mathbb{R}[x]}{(g_j)}}_{\mathbb{C}}$$

We get the isomorphism of $\mathbb{R}$-algebras

$$K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

Recall: $\exists\, n = [K:\mathbb{Q}]$ embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$ (Prop. 3.1, lecture 2)

<u>Lemma</u> $\left\{ \begin{array}{l} \text{field embeddings} \\ \sigma : K \hookrightarrow \mathbb{C} \end{array} \right\} \simeq \left\{ \begin{array}{l} \mathbb{R}\text{-algebra homomorph.} \\ \gamma : K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C} \end{array} \right\}$

<u>Proof</u> Construct mutually inverse maps between these two sets:

$$(\sigma : K \hookrightarrow \mathbb{C}) \longmapsto (\gamma : K \otimes \mathbb{R} \to \mathbb{C})$$
$$\gamma(a \otimes x) = \sigma(a) \cdot x$$

In the other direction

$$(\gamma : K \otimes \mathbb{R} \to \mathbb{C}) \longmapsto (\sigma : K \hookrightarrow \mathbb{C})$$
$$\sigma(x) = \gamma(x \otimes 1) \qquad \square$$

Let us construct n different $\mathbb{R}$-algebra homomorphisms $\gamma_i : K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C}$

$$\begin{array}{c} K \otimes_{\mathbb{Q}} \mathbb{R} \\ \wr| \\ \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \end{array}$$

1) $\pi_i : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \mathbb{R}$ projection onto the i-th factor
$i = 1 \dots r_1$

$$\begin{tikzcd} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \arrow[r, "\pi_i"] \arrow[rr, bend right, "\gamma_i"'] & \mathbb{R} \arrow[r, hook] & \mathbb{C} \end{tikzcd}$$

2) $\pi_i : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \mathbb{C}$ projection
$i = r_1 + 1, \dots, r_1 + r_2$

$\gamma_i(x) = \pi_i(x)$, $\quad i = r_1 + 1, \dots, r_1 + r_2$
$\gamma_{i+r_2}(x) = \overline{\pi_i(x)}$, $\quad i = r_1 + 1, \dots, r_1 + r_2$

$\Rightarrow$ we get r_1 real embeddings
$\sigma_i : K \hookrightarrow \mathbb{C}$ $\quad \mathrm{Im}(\sigma_i) \subset \mathbb{R}$
and r_2 pairs of complex-conjugate embeddings σ_i, $\sigma_{i+r_2} = \overline{\sigma_i}$, $i = r_1 + 1, \dots, r_1 + r_2$
$n = r_1 + 2r_2 \Rightarrow$ these are all embeddings
$K \hookrightarrow \mathbb{C}$

Identify $K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^{r_1 + 2r_2}$
$(x_1 \dots x_{r_1}, z_1 \dots z_{r_2}) \mapsto (x_1 \dots x_{r_1}, \mathrm{Re}\, z_1, \mathrm{Im}\, z_1 \dots)$

Then $\forall x \in K$ as an element of $\mathbb{R}^{r_1 + 2r_2}$ has coordinates
$(\sigma_1(x), \dots, \sigma_{r_1}(x), \mathrm{Re}\, \sigma_{r_1+1}(x), \mathrm{Im}\, \sigma_{r_1+1}(x), \dots)$

Proposition 11.2 In these coordinates

$$\mathrm{Vol}(\mathcal{O}_K) = 2^{-r_2} |d_K|^{1/2}$$

discriminant of K

Proof $\mathcal{O}_K = \langle e_1, \dots, e_n \rangle$ basis

Recall that $d_K = (\det B)^2$, where

$B = (b_{ij})$, $b_{ij} = \sigma_j(e_i)$ (see Prop. 6.4 lecture 5)

Consider the matrix A with i-th row:

$(\sigma_1(e_i), \dots, \sigma_{r_1}(e_i), \mathrm{Re}\,\sigma_{r_1+1}(e_i), \mathrm{Im}\,\sigma_{r_1+1}(e_i), \dots, \mathrm{Re}\,\sigma_{r_1+r_2}(e_i), \mathrm{Im}\,\sigma_{r_1+r_2}(e_i))$

Transform A into B by the following operations on columns:

1) add column $j+1$ to column j, $j = r_1+1, r_1+3, \dots$

$\rightsquigarrow$ get a matrix A' with $\sigma_j(e_i)$ in column $j = r_1+1, r_1+3, \dots$

2) multiply column j by -2 and add column $j-1$, for $j = r_1+2, r_1+4, \dots$

$\rightsquigarrow$ get matrix A'' with $\sigma_j(e_i)$ in columns $j = r_1+1, r_1+3, \dots$

with $\overline{\sigma_j(e_i)}$ in columns $j = r_1+2, r_1+4, \dots$

$$\mathrm{Vol}(\mathcal{O}_K) = |\det A| = |\det A'| = 2^{-r_2} |\det A''| =$$

$$= 2^{-r_2} |\det B| = 2^{-r_2} |d_K|^{\frac{1}{2}}$$

because $A'' = B$ up to permutation of columns $\square$

<u>Def</u> for $x = (x_1 \ldots x_{r_1}, x_{r_1+1}, \ldots, x_{r_1+2r_2}) \in \mathbb{R}^{r_1+2r_2}$

define $N(x) = \prod_{i=1}^{r_1} x_i \cdot \prod_{j=1}^{r_2} (x_{r_1+2j-1}^2 + x_{r_1+2j}^2)$

Note: if $x \in K \hookrightarrow \mathbb{R}^n$, then

$$N(x) = \prod_{i=1}^{r_1} \sigma_i(x) \cdot \prod_{j=r_1+1}^{r_1+r_2} \underbrace{|\sigma_j(x)|^2}_{\sigma_j(x)\cdot\overline{\sigma_j(x)}} = N_{K/\mathbb{Q}}(x)$$

is the norm of x.

<u>Thm 11.3</u> Let K be a number field with discriminant d_K, that has r_1 real and r_2 pairs of complex-conj. embeddings into $\mathbb{C}$.

1) $\exists$ a constant C_{r_1,r_2} depending on r_1, r_2, s.t. $\forall$ ideal class of K contains an integral ideal of Norm $\leq C_{r_1,r_2} \cdot |d_K|^{\frac{1}{2}}$

2) $Cl(K)$ is finite.

<u>Proof</u> 1) Choose arbitrary convex, symmetric, bounded open subset $S \subset \mathbb{R}^n$, s.t. $0 \in S$ (e.g. the unit ball). Define

$$M = \sup_{x \in S} |N(x)|, \quad \text{where}$$

N is the function difined above.

S is bonded, N continuous $\Rightarrow M < +\infty$

Let $I \in \mathcal{J}(K)$, then

$$\mathrm{Norm}(I^{-1}) \overset{\text{Prop. 10.3}}{=} \frac{\mathrm{Vol}(I^{-1})}{\mathrm{Vol}(\sigma_K)}$$

$$\Rightarrow \mathrm{Vol}(I^{-1}) = \mathrm{Vol}(\sigma_K) \cdot \mathrm{Norm}(I^{-1}) = \frac{\mathrm{Vol}(\sigma_K)}{\mathrm{Norm}(I)}$$

$$\overset{\text{Prop. 11.2}}{\Longrightarrow} \quad \mathrm{Vol}(I^{-1}) = \frac{2^{-r_2}|d_K|^{\frac{1}{2}}}{\mathrm{Norm}(I)} \qquad (*)$$

Let $\lambda = 2 \cdot \left(\frac{\mathrm{Vol}(I^{-1})}{\mathrm{Vol}(S)} \right)^{1/n}$

$$\mathrm{Vol}(\lambda S) = \lambda^n \mathrm{Vol}(S) = 2^n \mathrm{Vol}(I^{-1})$$

$$\overset{\text{Prop. 11.1}}{\Longrightarrow} \quad \exists\ 0 \neq x \in I^{-1} \cap \overline{\lambda S}$$

$$x \in \overline{\lambda S} \Rightarrow |N_{K/\mathbb{Q}}(x)| = |N(x)| \leq \lambda^n M$$

Consider $\quad x \cdot I = \sigma \subset \sigma_K \quad$ because $x \in I^{-1}$

$[I] = [\mathfrak{a}]$ in $Cl(K)$

$$\mathrm{Norm}(\mathfrak{a}) \overset{\text{Prop 10.1}}{=} |N_{K/\mathbb{Q}}(x)| \cdot \mathrm{Norm}(I) \leq \lambda^n M \,\mathrm{Norm}(I)$$

$$\overset{\text{def. of } \lambda}{=} \quad 2^n \frac{\mathrm{Vol}(I^{-1})}{\mathrm{Vol}(S)} \cdot M \cdot \mathrm{Norm}(I)$$

$$\overset{(*)}{=} \quad 2^n \frac{2^{-r_2} |d_K|^{1/2}}{\mathrm{Norm}(I) \cdot \mathrm{Vol}(S)} \cdot M \cdot \mathrm{Norm}(I)$$

$$\overset{n = r_1 + 2r_2}{=} \quad 2^{r_1 + r_2} \frac{|d_K|^{1/2} \cdot M}{\mathrm{Vol}(S)}$$

Let $C_{r_1, r_2} = 2^{r_1 + r_2} \dfrac{M}{\mathrm{Vol}(S)}$

– depends on r_1, r_2 and the choice of S

2) $\forall$ element in $Cl(K)$ is represented by $\mathfrak{a} \subset \mathcal{O}_K$ with $\mathrm{Norm}(\mathfrak{a}) \leq C_{r_1, r_2} |d_K|^{1/2}$ by part 1. By Prop. 10.2 $\exists$ only fin. many such ideals $\Rightarrow$ $Cl(K)$ is finite $\square$