The Ideal Class Group

Def Let k be a number field. The **class group** $Cl(k)$ (or C_k) of k is the group of fractional ideals modulo the principal fractional ideals (a) with $a \in k$.

Prop Let k be a number field, $B \in \mathbb{Z}_{>0}$. There are only finitely many integral ideals $\mathfrak{a} \subseteq \mathcal{O}_k$ with $N_k(\mathfrak{a}) \leq B$.

Proof $\mathfrak{a}$ is a subgroup of $\mathcal{O}_k$, and $|\mathcal{O}_k/\mathfrak{a}| \leq B$. In general, if G is a finitely generated abelian group, there are finitely many subgroups S such that $|G/S| \leq B$, since the subgroups of index dividing n must contain nG and G/nG is finite. Then we can take $n = [1, 2, \dots, B]$. ∎

Let k be a number field. Recall that there are n embeddings $k \hookrightarrow \overline{\mathbb{Q}}$, where $n = [k:\mathbb{Q}]$. Of those embeddings, some may be real, and some may be complex. The complex embeddings come in pairs of conjugate embeddings. We will say that there are r real embeddings and s pairs of complex embeddings, and write $n = r+2s$.

Ex For $\mathbb{Q}(\sqrt{2})$, $n = r = 2$. For $\mathbb{Q}(\sqrt[3]{2})$, $n = 3$, $r = 1$, $s = 1$. For $\mathbb{Q}(i)$, $n = 2$, $s = 1$.

Thm (Finiteness of the Class Group) Let k be a number field with $[k:\mathbb{Q}] = n = r+2s$ as above. There is a constant $C_{r,s}$ depending only on r, s such that every ideal class of $\mathcal{O}_k$ contains an integral ideal of norm at most $C_{r,s}\sqrt{|d_k|}$, where $d_k = \operatorname{disc}_k$.

In fact, one can take $C_{r,s} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$.

Notation $M_k = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d_k|}$ is called the **Minkowski constant**.

Coro C_k is finite.

Ex Let $k = \mathbb{Q}(\sqrt{10})$, $\mathcal{O}_k = \mathbb{Z}[\sqrt{10}]$. Then $n = 2$, $s = 0$, $r = 2$, $|d_k| = 40$.

$M_k = \left(\frac{4}{\pi}\right)^0 \cdot \frac{2!}{2^2}\sqrt{40} = \sqrt{10} = 3.16\ldots$

Finiteness of the class group implies that every ideal class has a representative that is an integral ideal of norm 1, 2, or 3.

We have that $x^2 - 10 \equiv x^2 \pmod 2$, $2\mathcal{O}_k = (2, \sqrt{10})^2$. If $(2, \sqrt{10}) = (\alpha)$ were principal, we would have $|N_k(\alpha)| = 2$ but $a^2 - 10b^2 = \pm 2$ has no solution (look modulo 5). Then $(2, \sqrt{10})$ is a nontrivial element of order 2 and $2 \mid |C_k|$.

For norm 3, $x^2 - 10 \equiv (x-1)(x+1) \pmod 3$, $3\mathcal{O}_k = (3, -1+\sqrt{10})(3, 1+\sqrt{10})$

If either of them were principal, the equation $a^2-10b^2=\pm 3$ would have an integer solution. But again, this is impossible modulo 5.

Let $(3,-1+\sqrt{10})(4+\sqrt{10}) = (12+3\sqrt{10}, 6+3\sqrt{10})$
$(3,1+\sqrt{10})(2+\sqrt{10}) = (6+3\sqrt{10}, 12+3\sqrt{10})$

$\Rightarrow (3,1+\sqrt{10}) \sim (3,-1+\sqrt{10})$ We have that every ideal is equivalent to either (1) (class of order 1), $(2,\sqrt{10})$ (class of order 2), $(3,1+\sqrt{10})$ (class of order 2)

C_K is a group of at most 3 elements, with at least one element of order $2 \Rightarrow |C_K| \leq 2$.

Indeed, $(2,\sqrt{10})(3,1+\sqrt{10}) = (6, 3\sqrt{10}, 2+2\sqrt{10}, 10+\sqrt{10}) \sim (6, 3\sqrt{10}, 2+2\sqrt{10}, -2+\sqrt{10})$
$\sim (6, 3\sqrt{10}, -2+\sqrt{10}) \sim (3\sqrt{10}, -2+\sqrt{10}) \sim (-2+\sqrt{10})$
$\uparrow 2+2\sqrt{10} = 3\sqrt{10}-(-2+\sqrt{10})$ $\uparrow 6 = 3\sqrt{10}-3(-2+\sqrt{10})$ $\leftarrow 3\sqrt{10} = (5+\sqrt{10})(-2+\sqrt{10})$ $\#$

The strategy for the proof of the theorem is to start with a nonzero ideal $\mathcal{O}_K$ and show that there is a $a \in K$, a very small in norm, such that $a\mathcal{O}_K$ is integral. Then $N_K(a\mathcal{O}_K)$ will be small

Def A subset S of $\mathbb{R}^n$ is called **convex** if whenever $x, y \in S$, the line connecting x and y is contained in S.

S is called **symmetric about the origin** if whenever $x \in S$, then $-x \in S$

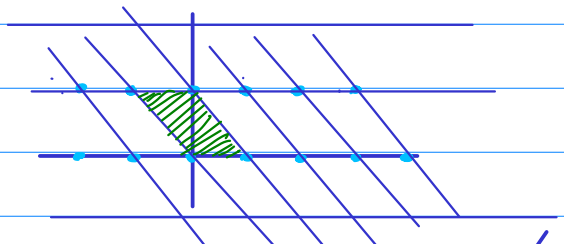
Def An **n-dimensional lattice** in $\mathbb{R}^n$ is a subgroup of the form $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_m$ with $v_1, \ldots, v_m$ linearly independent vectors.

$\{v_1, \ldots, v_m\}$ is called a **basis** for Λ.

A **fundamental parallelotope** is a set of the form

$$\phi = \left\{ \sum_{i=1}^{m} a_i v_i \;\middle|\; a_i \in \mathbb{R},\ 0 \leq a_i < 1 \right\}$$

Ex $\Lambda = \mathbb{Z}(1,0) \oplus \mathbb{Z}(-1,2) \subseteq \mathbb{R}^2$



Let $n=m$. The **volume** of Λ is defined to be the volume of ϕ and is computed by $\det(v_1, \ldots, v_m)$ and is independent of the choice of the basis. It is denoted by $\mathrm{Vol}(\mathbb{R}^n/\Lambda)$

Lemma (Minkowski-Blichfeld) Let $\Lambda \subseteq \mathbb{R}^n$ be an n-dimensional lattice Let S be a bounded, convex, closed subset of $\mathbb{R}^n$, symmetric about the origin. If $\mathrm{Vol}(S) \geq 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda)$, then S contains a nonzero element

of Λ

Proof First assume that $\mathrm{Vol}(S) > 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda)$. Take the map $\frac{1}{2}S \xrightarrow{\pi} \mathbb{R}^n/\Lambda$. If this map is injective, then $\frac{1}{2^n}\mathrm{Vol}(S) = \mathrm{Vol}\left(\frac{S}{2}\right) \leq \mathrm{Vol}(\mathbb{R}^n/\Lambda)$ contradiction. Then π is not injective, $\exists\, p_1, p_2 \in S$ $p_1 \neq p_2$ such that $\frac{1}{2}(p_1-p_2) \in \Lambda$. Since S is symmetric about the origin and convex, $\frac{1}{2}(p_1-p_2) \in S \Rightarrow \frac{1}{2}(p_1-p_2) \in S \cap \Lambda$ and $\frac{1}{2}(p_1-p_2) \neq 0$

Now assume that $\mathrm{Vol}(S) = 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda)$ for all $\varepsilon > 0$ $\exists\, 0 \neq Q_\varepsilon \in \Lambda \cap (1+\varepsilon)S$ since $\mathrm{Vol}((1+\varepsilon)S) > \mathrm{Vol}(S) = 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda)$. If $\varepsilon < 1$, then $Q_\varepsilon \in \Lambda \cap 2S$, which is finite since $2S$ is bounded and Λ is discrete. Hence there is a subsequence of Q_ε that converges in $\Lambda \cap 2S$, leading to $Q \in \Lambda \cap S$. $\#$

Lemma If Λ_2 is an n-dimensional sublattice of Λ_1, then Λ_1/Λ_2 is a finite group and $\mathrm{Vol}(\mathbb{R}^n/\Lambda_2) = \mathrm{Vol}(\mathbb{R}^n/\Lambda_1)\,|\Lambda_1/\Lambda_2|$

Proof Let $H \leq G$ free abelian groups of the same rank. Then $\exists\, \beta_1, \dots, \beta_n$ such that $G \cong \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$, $H \cong \mathbb{Z}d_1\beta_1 \oplus \cdots \oplus \mathbb{Z}d_n\beta_n$ for some $d_i \in \mathbb{Z}_{>0}$. Then $|G/H| = d_1 \cdots d_n$. $\#$

Fix a number field K with $\sigma_1, \dots, \sigma_r$ real embeddings and $\tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}$ complex embeddings.

Let $\varphi : K \longrightarrow \mathbb{R}^n$ be

$$\varphi(x) = (\sigma_1(x), \sigma_2(x), \dots, \sigma_r(x), \mathrm{Re}(\tau_1(x)), \mathrm{Im}(\tau_1(x)), \dots, \mathrm{Re}(\tau_s(x)), \mathrm{Im}(\tau_s(x)))$$

Lemma The image of $\mathcal{O}_K$ by φ is an n-dimensional lattice $\Lambda_{\mathcal{O}_K}$ with $\mathrm{Vol}(\mathbb{R}^n/\Lambda_{\mathcal{O}_K}) = \frac{1}{2^s}\,|\mathrm{disc}(K)|^{\frac{1}{2}}$

Proof Fix $\alpha_1, \dots, \alpha_n$ be an integral basis of $\mathcal{O}_K$. Then $\varphi(\alpha_1), \dots, \varphi(\alpha_n)$ generates $\varphi(\mathcal{O}_K)$. We need to see that they are linearly independent over $\mathbb{R}$.

$$\begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \mathrm{Re}\tau_1(\alpha_1) & \mathrm{Im}\tau_1(\alpha_1) & \cdots & \mathrm{Re}\tau_s(\alpha_1) & \mathrm{Im}\tau_s(\alpha_1) \\ \vdots & & & & & & & \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \mathrm{Re}\tau_1(\alpha_n) & \mathrm{Im}\tau_1(\alpha_n) & \cdots & \mathrm{Re}\tau_s(\alpha_n) & \mathrm{Im}\tau_s(\alpha_n) \end{vmatrix}$$

$$\longrightarrow \quad C_{r+1+2k} \longrightarrow C_{r+1+2k} + i\,C_{r+2+2k} \quad \longrightarrow$$

$$C_{r+2+2k} \longrightarrow C_{r+1+2k} - 2i\,C_{r+2+2k}$$

$$= \frac{1}{|(-2i)^s|} \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1(\alpha_1)} & \cdots & \tau_s(\alpha_1) & \overline{\tau_s(\alpha_1)} \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau_1(\alpha_n)} & \cdots & \tau_s(\alpha_n) & \overline{\tau_s(\alpha_n)} \end{vmatrix}$$

$= \frac{1}{2^s} |\text{disc } k|^{1/2} \neq 0$. Therefore, we get a full lattice and

$$\text{Vol}\left(\mathbb{R}^n / \varphi(\mathcal{O}_k)\right) = \frac{1}{2^s}\sqrt{|d_k|} \quad \#$$

Remark If $\mathfrak{A}$ is a fractional ideal of $\mathcal{O}_k$ we can extend the norm in the obvious way. For instance, if $\mathfrak{A} = \mathfrak{P}_1 \cdots \mathfrak{P}_n (\mathfrak{q}_1 \cdots \mathfrak{q}_m)^{-1}$

$$N_k(\mathfrak{A}) = N_k(\mathfrak{P}_1 \cdots \mathfrak{P}_n) N(\mathfrak{q}_1 \cdots \mathfrak{q}_n)^{-1}$$

Lemma If $\mathfrak{A}$ is a fractional ideal of $\mathcal{O}_k$, then $\varphi(\mathfrak{A})$ is a lattice in $\mathbb{R}^n$ and $\text{Vol}\left(\mathbb{R}^n / \varphi(\mathfrak{A})\right) = \frac{1}{2^s}\sqrt{|d_k|}\, N_k(\mathfrak{A})$.

Proof: First suppose that $\mathfrak{A}$ is integral. $\varphi(\mathcal{O}_k)$ is a rank n abelian group and it spans $\mathbb{R}^n$. By a previous Lemma, there is $a \in \mathfrak{A}$, $a \neq 0$ such that $a\mathcal{O}_k \subseteq \mathfrak{A} \subseteq \mathcal{O}_k$. So $\varphi(\mathfrak{A})$ is an n-dimensional lattice in $\mathbb{R}^n$. Choose a basis $\{\beta_1, \ldots, \beta_n\}$ of $\mathcal{O}_k$ such that $\{d_1\beta_1, \ldots, d_n\beta_n\}$ is a basis of $\mathfrak{A}$, $d_i \in \mathbb{Z}$.

$$N_k(\mathfrak{A}) = |\mathcal{O}_k/\mathfrak{A}| = |d_1 \cdots d_n| = |\varphi(\mathcal{O}_k)/\varphi(\mathfrak{A})|$$

$$\text{Vol}\left(\mathbb{R}^n/\varphi(\mathfrak{A})\right) = \text{Vol}\left(\mathbb{R}^n/\varphi(\mathcal{O}_k)\right) \left|\varphi(\mathcal{O}_k)/\varphi(\mathfrak{A})\right| =$$

$$\text{Vol}\left(\mathbb{R}^n/\varphi(\mathcal{O}_k)\right) N_k(\mathfrak{A}) = \frac{1}{2^s}\sqrt{|d_k|}\, N_k(\mathfrak{A})$$

Now if $\mathfrak{A}$ is a fractional ideal $\exists a \in \mathcal{O}_k$ such that $a\mathfrak{A}$ is integral then $N_k(\mathfrak{A}) = N_k(a^{-1}) N_k(a\mathfrak{A})$

$$\text{Vol}\left(\mathbb{R}^n/\varphi(\mathfrak{A})\right) = \text{Vol}\left(\mathbb{R}^n/\varphi(a^{-1}a\mathfrak{A})\right) = N_k(a^{-1})\,\text{Vol}\left(\mathbb{R}^n/\varphi(a\mathfrak{A})\right)$$

$$= N_k(a^{-1}) \frac{1}{2^s}\sqrt{|d_k|}\, N_k(a\mathfrak{A}) = N_k(\mathfrak{A}) \frac{1}{2^s}\sqrt{|d_k|} \quad \#$$

Proof of Thm Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ be defined by

$$f(x_1, \ldots, x_n) = |x_1 \cdots x_r (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{r+2s-1}^2 + x_{r+2s}^2)|$$

If $x \in k$ $f(\varphi(x)) = |N_{k/\mathbb{Q}}(x)|$ and $f(ax_1, \ldots, ax_n) = |a|^n f(x_1, \ldots, x_n)$

Let $S \subseteq \mathbb{R}^n$ be fixed, closed, bounded, convex, symmetric about the origin, with positive volume. Since S is compact,

$M = \max\{ f(x) \mid x \in S \}$ is well-defined

Let $\mathfrak{A}$ be a fractional ideal of $\mathcal{O}_k$. We want to find $a \in \mathfrak{A}^{-1}$ so that $a\mathfrak{A}$ is integral with small norm. The Lemma implies

$c = \text{Vol}\left(\mathbb{R}^n/\varphi(\mathfrak{A}^{-1})\right) = \frac{1}{2^s}\sqrt{|d_k|}\, N_k(\mathfrak{A})^{-1}$. Take $\lambda = \left(\frac{c}{\text{Vol}(S)}\right)^{1/n} \cdot 2$

Then $\text{Vol}(\lambda S) = \lambda^n \text{Vol}(S) = \frac{2^n c}{\text{Vol}(S)} \cdot \text{Vol}(S) = 2^n \text{Vol}\left(\mathbb{R}^n/\varphi(\mathfrak{A}^{-1})\right)$

Then there is

$b \neq 0$, $b \in \varphi(\mathfrak{A}^{-1}) \cap \lambda S$: Let $a \in \mathfrak{A}^{-1}$ be such that $\varphi(a) = b$, then

$|N_{k/\mathbb{Q}}(a)| \leq \lambda^n M$; since $\lambda^n M$ is the largest value of f on λS.

SINCE $a \in \mathfrak{a}^{-1}$, THEN $a\mathfrak{a} \subseteq \mathcal{O}_K$ AND

$$N_K(a\mathfrak{a}) = |N_{K/\mathbb{Q}}(a)|\, N_K(\mathfrak{a}) \le \lambda^h H\, N_K(\mathfrak{a}) \le 2^h \frac{c}{\mathrm{Vol}(S)} H\, N_K(\mathfrak{a}) =$$

$$= 2^h \frac{2^{r+s}\sqrt{|d_K|}}{\mathrm{Vol}(S)} H = 2^{r+s}\sqrt{|d_K|}\, \frac{H}{\mathrm{Vol}(S)}$$

THE THEOREM IS COMPLETED IF WE CAN FIND S SATISFYING ALL OF THAT

LEMMA: THE SET

$$S = \{(x_1,\dots,x_n) \mid |x_1| + \dots + |x_r| + 2\left(\sqrt{x_{r+1}^2+x_{r+2}^2} + \dots + \sqrt{x_{n-1}^2+x_n^2}\right) \le n\}$$

IS CLOSED, BOUNDED, CONVEX, SYMMETRIC ABOUT THE ORIGIN, AND

$$\mathrm{Vol}(S) = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s, \quad H = 1$$

PROOF: S IS CONVEX:

$$|x_1 t + y_1(1-t)| \le t|x_2| + (1-t)|y_2|$$

$$\sqrt{(tx_{r+1}+(1-t)y_{r+1})^2 + (tx_{r+2s+1}+(1-t)y_{r+2s+1})^2} \le t\sqrt{x_{r+1}^2+x_{r+2s+1}^2} + (1-t)\sqrt{y_{r+1}^2+y_{r+2s+1}^2}$$

(SQUARE TWICE TO FINISH THIS PART)

WE HAVE $|f(a)| \le 1$ BY THE ARITHMETIC–GEOMETRIC MEAN INEQUALITY

$$a_1 \cdots a_n \le \left(\frac{a_1+\dots+a_n}{n}\right)^n \text{ FOR } a_i \ge 0, \text{ EQUALITY IF } a_1 = \dots = a_n.$$

FINALLY, LET $\mathrm{Vol}(S) = V_{r,s}(n)$

NOTICE $V_{r,s}(t) = t^{r+2s} V_{r,s}(1)$

IF $r>0$, $V_{r,s}(1) = 2\int_0^1 V_{r-1,s}(1-x)\,dx = 2\int_0^1 (1-x)^{r+2s-1}\,dx\; V_{r-1,s}(1) = \frac{2}{r+2s} V_{r-1,s}(1) =$

$$\dots = \frac{2^r}{(r+2s)\cdots(1+2s)} V_{0,s}(1)$$

WHEN $s>0$, $r=0$, $V_{0,s}(1) = \iint_{x^2+y^2 \le \frac{1}{4}} V_{0,s-1}\left(1-2\sqrt{x^2+y^2}\right)dx\,dy = \int_0^{2\pi}\int_0^{\frac{1}{2}} V_{0,s-1}(1-2\rho)\rho\,d\rho\,d\theta$

$$= 2\pi \int_0^{1/2} (1-2\rho)^{2(s-1)}\rho\,d\rho\; V_{0,s-1}(1) = \frac{\pi}{2}\int_0^1 u^{2(s-1)}(1-u)\,du\; V_{0,s-1}(1) =$$

$$= \frac{\pi}{2}\left(\frac{1}{2s-1} - \frac{1}{2s}\right) V_{0,s-1}(1) = \frac{\pi}{2\cdot 2s(2s-1)} V_{0,s-1}(1) = \dots = \frac{\pi^s}{2^s (2s)!} V_{0,0}(1).$$

WE HAVE

$V_{0,1}(1) = \frac{\pi}{4}$ AND $V_{1,0}(1) = 2 = 2V_{0,0}(1) \Rightarrow V_{0,0}(1) = 1.$

$$\Rightarrow V_{r,s}(n) = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s \quad \#\#$$

COROLLARY: LET $K \neq \mathbb{Q}$ BE A NUMBER FIELD. THEN $|d_K| > 1$

PROOF: BY THE THEOREM, WE HAVE $1 \le \sqrt{|d_K|}\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$

THUS, $\sqrt{|d_K|} \ge \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!} \Rightarrow \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!} > 1$ BY INDUCTION.

($n = r+2s \Rightarrow s \le n/2$)

$n=2$,

$$\left(\frac{\pi}{4}\right)^{3/2} \cdot \frac{2^2}{2!} = \frac{\pi}{4}\cdot 2 > 1$$

$$\left(\frac{\pi}{4}\right)^{\frac{n+1}{2}} \frac{(n+1)^{n+1}}{(n+1)!} = \left(\frac{\pi}{4}\right)^{\frac{1}{2}} \left(\frac{n+1}{n}\right)^n \left(\frac{\pi}{4}\right)^{\frac{n}{2}} \frac{n^n}{n!} > \left(\frac{\pi}{4}\right)^{\frac{1}{2}} \left(\frac{n+1}{n}\right)^n > 1$$

DEF: LET k BE A NUMBER FIELD. THE ORDER OF C_k IS CALLED THE CLASS NUMBER OF k AND IS DENOTED BY h_k.

ALGEBRAIC CONJECTURE: THERE ARE INFINITELY MANY NUMBER FIELDS WITH $|C_k|=1$

EX IT SEEMS THAT $k=\mathbb{Q}(\sqrt{d})$ $d>1$ HAS INFINITELY MANY d's WITH $h_k=1$. (COHEN-LENSTRA)

EX FOR $d<0$, ONLY $d=-3,-4,-7,-8,-11,-19,-43,-67,-163$ YIELD $h_k=1$

STRATEGY FOR COMPUTING h_k

① FIND $M_k=\sqrt{|d_k|}\left(\frac{4}{\pi}\right)^s\frac{n!}{n^n}$

② FIND ALL $\mathfrak{P}\subseteq\mathcal{O}_k$ THAT LIE ABOVE $p\in\mathbb{N}$, $p\leq M_k$

③ FIND THE GROUP GENERATED BY THE $[\mathfrak{P}]$.

EX FOR $\mathbb{Q}(\sqrt{5})$, $n=2$, $r=2$, $s=0$, $d_k=5$, $M_k=\sqrt{5}\left(\frac{4}{\pi}\right)^0\frac{2!}{2^2}<2$ $\Rightarrow$ ALL IDEALS ARE PRINCIPAL, $h_k=1$.

FOR $\mathbb{Q}(\sqrt{-6})$, $n=2$, $r=0$, $s=1$, $d_k=-24$, $M_k=\sqrt{24}\left(\frac{4}{\pi}\right)^1\frac{2!}{2^2}\sim 3.1$

WE LOOK FOR PRIMES LYING OVER 2 AND 3.

$x^2+6\equiv x^2 \pmod{2,3}$ $\Rightarrow$ $(2)=(2,\sqrt{-6})^2$, $(3)=(3,\sqrt{-6})^2$

$\Rightarrow$ $(2,\sqrt{-6})$, $(3,\sqrt{-6})$ HAVE ORDER 2.

IF $(2,\sqrt{-6})=(a+b\sqrt{-6})$ $\Rightarrow$ $2=N_k(2,\sqrt{-6})=a^2+6b^2$ NO SOLUTIONS. THE SAME WORKS FOR $(3,\sqrt{-6})$. THEN, THEY ARE NO PRINCIPAL. NOTICE

$(2,\sqrt{-6})(3,\sqrt{-6})=(6,2\sqrt{-6},3\sqrt{-6},-6)=(6,\sqrt{-6})=(\sqrt{-6})$ $\Rightarrow$ THE CLASSES ARE INVERSE TO EACH OTHER $\Rightarrow$ $Cl(k)=\langle(2,\sqrt{-6})\rangle=\mathbb{Z}/2\mathbb{Z}$

THE UNIT GROUP

DEF THE GROUP OF UNITS U_k ASSOCIATED TO A NUMBER FIELD k IS THE GROUP OF ELEMENTS OF $\mathcal{O}_k$ THAT HAVE AN INVERSE IN $\mathcal{O}_k$

THM (DIRICHLET) THE GROUP U_k IS OF THE FORM

$$U_k\simeq\mathbb{Z}^{r+s-1}\oplus T,$$

WHERE T IS A FINITE CYCLIC GROUP CONSISTING OF THE ROOTS OF UNITY IN k

EX IN THE REAL QUADRATIC CASE, $n=r=2$, $s=0$, $r+s-1=1$. THEN WE HAVE $U=\{\pm u^k \mid k\in\mathbb{Z}\}$ FOR SOME u. WE NORMALIZE BY TAKING THE SMALLEST $u>1$, CALLED THE FUNDAMENTAL UNIT.

EX IN $\mathbb{Z}[\sqrt{2}]$, $u=1+\sqrt{2}$ IN $\mathbb{Z}[\sqrt{31}]$, $u=1520+273\sqrt{31}$

WE PROVE THE THEOREM BY DEFINING A MAP $\Psi: U_k\longrightarrow\mathbb{R}^{r+s}$ AND SHOWING THAT $\ker\Psi$ IS FINITE AND THE IMAGE IS A LATTICE IN A HYPERPLANE

IN $\mathbb{R}^{r+s}$.

PROP LET k BE A NUMBER FIELD AND $a \in \mathcal{O}_k$. THEN a IS A UNIT IFF $N_{k/\mathbb{Q}}(a) = \pm 1$

PROOF: WE HAVE $a \in \mathcal{O}_k \iff a^{-1} \in \mathcal{O}_k$ $\quad 1 = N_{k/\mathbb{Q}}(a) N_{k/\mathbb{Q}}(a^{-1})$, $N_{k/\mathbb{Q}}(a) \in \mathbb{Z}$, $N_{k/\mathbb{Q}}(a^{-1}) \in \mathbb{Z}$

$\Rightarrow N_{k/\mathbb{Q}}(a) = \pm 1$

CONVERSELY, SUPPOSE $N_{k/\mathbb{Q}}(a) = \pm 1$, $a \in \mathcal{O}_k$. WRITE

$$\pm 1 = N_{k/\mathbb{Q}}(a) = \prod_{\substack{\sigma \text{ EMBEDDINGS} \\ \sigma \neq id}} \sigma(a) = a \prod_{\substack{\sigma \text{ EMBEDDINGS} \\ \sigma \neq id}} \sigma(a) \Rightarrow$$

$$a^{-1} = \pm \prod_{\substack{\sigma \text{ EMBEDDINGS} \\ \sigma \neq id}} \sigma(a) \in \overline{\mathbb{Z}} \cap k \subset \mathcal{O}_k \Rightarrow a \in \mathcal{O}_k^{\times} \quad \#$$

REMARK THE PROPOSITION IS FALSE IF WE REPLACE $\mathcal{O}_k$ BY k.

$x^2 - \frac{1}{2}x + 1$ HAS ROOTS $\frac{1 \pm \sqrt{-15}}{4} \in k \setminus \mathcal{O}_k$; $N_{k/\mathbb{Q}}\left(\frac{1 \pm \sqrt{-15}}{4}\right) = 1$

LET k BE A NUMBER FIELD. RECALL $[k:\mathbb{Q}] = n = r+2s$. DEFINE THE LOG MAP $\Psi: \mathcal{O}_k^{\times} \longrightarrow \mathbb{R}^{r+s}$

$$\Psi(a) = \left(\log|\sigma_1(a)|, \dots, \log|\sigma_r(a)|, \log|\tau_1(a)|, \dots, \log|\tau_s(a)|\right)$$

LEMMA WE HAVE $\operatorname{Im}\Psi \subseteq H$ WHERE

$$H = \left\{(x_1, \dots, x_{r+s}) \in \mathbb{R}^{r+s} \,\middle|\, x_1 + \dots + x_r + 2x_{r+1} + \dots + 2x_{r+s} = 0\right\}$$

PROOF: IF $a \in \mathcal{O}_k^{\times}$, THEN $1 = |N_{k/\mathbb{Q}}(a)| = \prod_{i=1}^{r} |\sigma_i(a)| \prod_{i=1}^{s} |\tau_i(a)|^2$, THEN TAKE THE LOGARITHM TO CONCLUDE #

LEMMA: THE KERNEL OF Ψ CONSISTS OF THE ROOTS OF UNITY OF k AND IT IS A FINITE CYCLIC GROUP.

PROOF: CLEARLY THE ROOTS OF UNITY IN k ARE INCLUDED IN $\ker\Psi$

WE HAVE $\Psi(\ker\Psi) \subseteq \Psi\left(\{a \in \mathcal{O}_k \mid |\sigma_i(a)| = |\tau_j(a)| = 1 \ \forall i,j\}\right) \subseteq \Psi(\mathcal{O}_k) \cap S$

SINCE $\Psi(\mathcal{O}_k)$ IS A LATTICE AND S IS A COMPACT SET OF FINITE VOLUME, $\Psi(\mathcal{O}_k) \cap S$ IS FINITE. THEREFORE $\ker\Psi$ IS A FINITE GROUP AND THERE IS m = THE EXPONENT OF $\ker\Psi$. (ALL ELEMENTS $x \in \ker\Psi$ SATISFY $x^m = 1$)

SINCE A POLYNOMIAL OF $\deg = m$ OVER k CAN HAVE AT MOST m ROOTS, WE GET THAT $\ker\Psi$ HAS AT MOST ORDER m AND THEREFORE IT IS CYCLIC. #

LEMMA THE IMAGE $\Psi: \mathcal{O}_k^{\times} \longrightarrow \mathbb{R}^{r+s}$ IS DISCRETE.

PROOF: LET X BE A CLOSED BOUNDED SUBSET OF $\mathbb{R}^{r+s}$. WE WANT TO SHOW THAT $\Psi(\mathcal{O}_k^{\times}) \cap X$ IS FINITE. SINCE X IS BOUNDED, $\forall u \in T = \Psi^{-1}(X) \subseteq \mathcal{O}_k^{\times}$ THE COORDINATES OF $\Psi(u)$ ARE BOUNDED, SINCE $\exp$ IS CONTINUOUS SO

$\log|\sigma_i(a)| \le M \Rightarrow |\sigma_i(a)| \le e^M$ AND $\log|\tau_i(a)| \le M \Rightarrow |\mathrm{Re}(\tau_i(a))|, |\mathrm{Im}(\tau_i(a))| \le |\tau_i(a)| \le e^M$

THUS $\psi(\Sigma)$ IS A BOUNDED SUBSET OF $\psi(\mathcal{O}_K)$ WHICH IS A LATTICE IN $\mathbb{R}^n$ $\Rightarrow$ $\psi(\Sigma)$ FINITE. ALSO ψ IS INJECTIVE $\Rightarrow$ Σ FINITE $\Rightarrow$ $\psi(U_K)\cap X \subseteq \psi(\Sigma)\cap X$ IS FINITE, #

LEMMA Δ DISCRETE SUBGROUP $\Gamma \subseteq \mathbb{R}^n$ IS A LATTICE.

PROOF WE HAVE THAT $\forall x \in M$, $\exists U_x$ OPEN SUCH THAT $U_x \cap \Gamma = \{x\}$

LET V BE THE SUBSPACE OF $\mathbb{R}^n$ SPANNED BY M. IT HAS $\dim = m \le n$.

LET $\{u_1,\dots,u_m\}$ BE A BASIS OF V, $u_i \in \Gamma$. LET $\Lambda = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_m \subseteq V$

LET $\phi = \{a_1u_1+\cdots+a_mu_m \mid a_i \in \mathbb{R},\ 0 \le a_i < 1\}$ BE THE FUNDAMENTAL PARALLELOTOPE.

CONSIDER Γ/Λ. LET $\{\gamma_i\} \subseteq \Gamma$ BE REPRESENTATIVES OF COSETS. SINCE Λ IS FULL IN V, $\phi+\tilde{\gamma}$ FOR $\tilde{\gamma}\in\Lambda$ COVER V. WRITE $\gamma_i = \mu_i + \tilde{\gamma}_i$ WITH $\mu_i \in \phi$, $\tilde{\gamma}_i \in \Lambda$

NOW $\mu_i \in \gamma_i - \tilde{\gamma}_i \in \Gamma \cap \phi \subseteq \Gamma \cap \overline{\phi}$, WHICH IS FINITE SINCE $\overline{\phi}$ IS CLOSED AND BOUNDED AND Γ IS DISCRETE. THIS MEANS THAT THERE ARE FINITELY MANY γ_i'S AND $|\Gamma/\Lambda| < \infty$. THUS $\exists M$ SUCH THAT $M\Gamma \subseteq \Lambda$ AND THAT $\Lambda \subseteq \Gamma \subseteq \frac{1}{M}\Lambda \Rightarrow \Gamma$ IS A FREE ABELIAN GROUP OF RANK m AND THEREFORE A LATTICE #

LEMMA LET $n \in \mathbb{Z}_{\ge 2}$, $\omega_1,\dots,\omega_n \in \mathbb{R}$ NOT ALL EQUAL. LET $A,B \in \mathbb{R}_{>0}$. $\exists d_1,\dots,d_n \in \mathbb{R}_{>0}$ SUCH THAT $|\omega_1\log(d_1)+\cdots+\omega_n\log(d_n)| > B$ AND $d_1\cdots d_n = A$

PROOF WITHOUT LOSS OF GENERALITY, WE CAN ASSUME $\omega_1 \neq 0$. $\exists \omega_j$ SUCH THAT $\omega_j \neq \omega_1$. BY REORDERING, ASSUME $j=2$. SET $d_3 = \cdots = d_n = 1$ TAKE $d_1, d_2 > 0$ WITH $d_1d_2 = A$ WE HAVE

$$|\omega_1\log(d_1)+\cdots+\omega_n\log(d_n)| = |\omega_1\log(d_1)+\omega_2\log(d_2)| = |\omega_1\log(d_1)+\omega_2\log(A/d_1)|$$
$$= |(\omega_1-\omega_2)\log(d_1)+\omega_2\log A| \to \infty \text{ AS } d_1 \to \infty$$

THEN WE CAN CHOOSE d_1 AS REQUIRED #

PROOF OF DIRICHLET'S THM THE IMAGE OF $\psi(U_K)$ IS DISCRETE AND THEREFORE A LATTICE. WE WANT TO PROVE THAT IT SPANS H. LET W BE THE $\mathbb{R}$-SPAN OF $\psi(U_K)$. W IS A SUBSPACE OF H. THEN THE ORTHOGONAL COMPLEMENTS WITH RESPECT TO THE DOT PRODUCT SATISFY $H^\perp \subseteq W^\perp$. WE WILL PROVE $W^\perp \subseteq H^\perp$ BY PROVING THAT $(H^\perp)^c \subseteq (W^\perp)^c$

Let $z=(z_1,\dots,z_{r+s})\notin H^+$. Define $f:K^*\to\mathbb{R}$

$f(x)=z_1\log|\sigma_1(x)|+\cdots+z_{r+s}\log|\sigma_{r+s}(x)|$

Then $f(U_K)=\{0\}\iff z\in\omega^\perp$. We will show that $z\notin\omega^\perp$ by showing that $f(U_K)\neq\{0\}$.

Let $A=\left(\frac{2}{\pi}\right)^s\sqrt{|d_K|}$. Choose $c_1,\dots,c_r,e_1,\dots,e_s\in\mathbb{R}_{>0}$ such that

$c_1\cdots c_r(e_1\cdots e_s)^2=A$

Let $S=\{(x_1,\dots,x_n)\in\mathbb{R}^n \mid |x_i|\le c_i \ 1\le i\le r,\ |x_i^2+x_{i+1}^2|\le e_{i-r}^2 \ r+1\le i\le r+2s-1\}$

S closed, bounded, convex, symmetric about the origin. Its dimension is $r+2s$

$\mathrm{Vol}(S)=\prod_{i=1}^{r}(2c_i)\prod_{i=1}^{s}(\pi e_i^2)=2^r\pi^s A=2^{n-s}\sqrt{|d_K|}$

By Minkowski-Bliechfeldt, since we have that

$\mathrm{Vol}(S)=\frac{2^n}{2^s}\sqrt{|d_K|}=2^n\left(\frac{\sqrt{|d_K|}}{2^s}\right)=2^n\,\mathrm{Vol}\left(\mathbb{R}^n/\varphi(\mathcal{O}_K)\right)$

Thus, there is $x\neq0$, $x\in S\cap\varphi(\mathcal{O}_K)$. Let $a\in\mathcal{O}_K$, $\varphi(a)=x$

Then $\varphi(a)\in S\Rightarrow|\sigma_i(a)|\le c_i \ i=1,\dots,r$ $|\tau_i(a)|\le e_i \ i=1,\dots,s$

Then $|N_{K/\mathbb{Q}}(a)|=\left|\prod_{i=1}^{r}\sigma_i(a)\right|\prod_{i=1}^{s}|\tau_i(a)|^2\le c_1\cdots c_r e_1^2\cdots e_s^2=A$

Since $a\in\mathcal{O}_K$, $a\neq0$, then $|N_{K/\mathbb{Q}}(a)|\ge1$

If $|\sigma_i(a)|<\frac{c_i}{A}$, $1\le|N_{K/\mathbb{Q}}(a)|<c_1\cdots\frac{c_i}{A}\cdots c_r(e_1\cdots e_s)^2=\frac{A}{A}=1$ contradiction

If $|\tau_i(a)|^2<\frac{1}{A}e_{i-r}^2$ also leads to a contradiction

Thus, $\frac{c_i}{|\sigma_i(a)|}\le A$, $\left(e_{i-r}\frac{1}{|\tau_i(a)|}\right)^2\le A$

Let $b_1,\dots,b_m$ be generators for the finitely many nonzero principal ideals of $\mathcal{O}_K$ of norm $\le A$

Since $|N_{K/\mathbb{Q}}(a)|\le A$, we have $(a)=(b_j)$ for some j so $\exists u\in\mathcal{O}_K$ such that $a=ub_j$.

Let $t=t_{c_1\cdots c_r e_1\cdots e_s}=z_1\log(c_1)+\cdots+z_r\log(c_r)+z_{r+1}\log(e_1)+\cdots+z_{r+s}\log(e_s)$

We have $|f(u)-t|=|f(a)-f(b_j)-t|\le|f(b_j)|+|t-f(a)|$

$=|f(b_j)|+|z_1(\log c_1-\log|\sigma_1(a)|+\cdots+z_{r+s}(\log e_s-\log|\tau_s(a)|)|$

$=|f(b_j)|+\left|z_1\log\left(\frac{c_1}{|\sigma_1(a)|}\right)+\cdots+\frac{z_{r+s}}{2}\log\left(\frac{e_s}{|\tau_s(a)|}\right)^2\right|$

$\le\underbrace{|f(b_j)|+\log A\left(\sum_{i=1}^{r}|z_i|+\frac{1}{2}\sum_{i=r+1}^{r+s}|z_i|\right)}_{B_j}$

Take $B=\max_j B_j$. It does not depend on the choice of c_i's and e_i's (it only depends on z and K)

We then have $|f(u)-t|\le B$

IF WE CHOOSE $C_1 \cdots C_r (e_1 - e_s)^2 = A$, $|t_{C_1,\ldots,C_r,e_1,\ldots,e_s}| > B$, THIS IMPLIES

$|f(u)| > 0 \Rightarrow f(U_K) \neq 0 \Rightarrow z \notin W^\perp \Rightarrow W^\perp \subsetneq H^\perp \Rightarrow W^\perp = H^\perp \Rightarrow W = H$.

THIS CAN BE ACHIEVED SINCE

$$t = z_1 \log(\varepsilon_1) + \cdots + z_{r+s} \log(\varepsilon_s)$$
$$= z_1 \log(\varepsilon_1) + \cdots + z_r \log(\varepsilon_r) + \tfrac{1}{2} z_{r+1} \log(\varepsilon_1^2) + \cdots + \tfrac{1}{2} z_{r+s} \log(\varepsilon_s^2)$$
$$= w_1 \log(d_1) + \cdots + w_r \log(d_r) + w_{r+1} \log(d_{r+1}) + \cdots + w_{r+s} \log(d_{r+s})$$

THE CONDITION $z \notin H^\perp$ IMPLIES THAT THE w_i ARE NOT ALL EQUAL #

THE DISTRIBUTION OF IDEALS IN NUMBER FIELDS

LET K BE A NUMBER FIELD, $[K:\mathbb{Q}] = n$, $t \in \mathbb{R}_{>0}$

$i(t) = \#\{\mathfrak{a} \text{ IDEAL OF } \mathcal{O}_K \mid N_K(\mathfrak{a}) \leq t\}$

LET C BE A CLASS OF INTEGRAL IDEALS IN C_K AND

$i_C(t) = \#\{\mathfrak{a} \in C \mid N_K(\mathfrak{a}) \leq t\}$

THUS $i(t) = \sum_C i_C(t)$

THM THERE IS A NUMBER $\alpha(K)$ DEPENDING ON $\mathcal{O}_K$ BUT INDEPENDENT OF C SUCH THAT $i_C(t) = \alpha(K) t + O(t^{1-\frac{1}{n}})$

COR $i(t) = h_K \alpha(K) t + O(t^{1-\frac{1}{n}})$

IDEA OF THE PROOF COUNT IDEALS IN C BY COUNTING ELEMENTS OF A CERTAIN IDEAL

FIX $\mathfrak{b} \in C^{-1}$. THERE IS A ONE-TO-ONE CORRESPONDENCE

$$\left\{ \begin{array}{l} \text{IDEALS } \mathfrak{a} \in C \\ N_K(\mathfrak{a}) \leq t \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{PRINCIPAL IDEALS } (\alpha) \subseteq \mathfrak{b} \\ N_K(\alpha) \leq t N_K(\mathfrak{b}) \end{array} \right\}$$

$$\mathfrak{a} \longleftrightarrow \mathfrak{a}\mathfrak{b} = (\alpha)$$

COUNTING $(\alpha) \subseteq \mathfrak{b}$ IS LIKE COUNTING $\alpha \in \mathfrak{b}$ UP TO A UNIT. IF $|U_K|$ IS FINITE, THIS IS EASIER.

PROOF OF THE IMAGINARY QUADRATIC CASE. WE HAVE THAT $\ell(\mathcal{O}_K)$ IS A LATTICE IN $\mathbb{R}^2$, AND $N_K(\alpha) = |\alpha|^2$. WE WANT TO COUNT THE NUMBER OF NONZERO POINTS OF $\ell(\mathfrak{b})$ IN THE CIRCLE OF RADIUS $\sqrt{t N_K(\mathfrak{b})}$ CENTERED AT 0. LET ϕ THE FUNDAMENTAL PARALLELOTOPE FOR $\ell(\mathfrak{b}) \subseteq \mathbb{R}^2$. CONSIDER TRANSLATES OF ϕ CENTERED AT POINTS OF $\ell(\mathfrak{b})$. THE NUMBER OF $\alpha \in \mathfrak{b}$ WITH $|\alpha| \leq \rho = \sqrt{t N_K(\mathfrak{b})}$ IS APPROXIMATED BY THE NUMBER OF TRANSLATES OF ϕ THAT ARE CONTAINED IN THE CIRCLE, NAMELY $\frac{\pi \rho^2}{\mathrm{Vol}(\phi)} = \frac{\pi t N_K(\mathfrak{b})}{\mathrm{Vol}(\phi)}$. LET $i^-(\rho)$ BE THE NUMBER OF COPIES OF ϕ THAT LIE ENTIRELY IN THE CIRCLE OF RADIUS ρ

LET $i^+(\rho)$ BE THE NUMBER OF COPIES OF ϕ THAT INTERSECT THE CIRCLE OF

RADIUS ρ. LET $n(\rho)$ BE THE NUMBER OF POINTS IN THE CIRCLE. THEN

$$n^-(\rho) \le n(\rho) \le n^+(\rho)$$

ALGEBRAIC NUMBER THEORY $x^n+y^n=z^n$ M. LALÍN

IF δ DENOTES THE LONGEST DIAGONAL OF ϕ, THEN $n^+(\rho) \le n^-(\rho+\delta)\ \forall \rho$

THUS $n^+(\rho-\delta) \le n(\rho) \le n^-(\rho+\delta) \Rightarrow$

$$\pi(\rho-\delta)^2 \le n^+(\rho-\delta)\,\mathrm{Vol}(\phi) \le n(\rho)\,\mathrm{Vol}(\phi) \le n^-(\rho+\delta)\,\mathrm{Vol}(\phi) \le \pi(\rho+\delta)^2$$

$$\Rightarrow n(\rho)\,\mathrm{Vol}(\phi) = \pi\rho^2 + \gamma(\rho) \quad \text{WITH} \quad |\gamma(\rho)| \le 2\pi\delta\rho + \delta^2\pi$$

USING $|U_K|\, i_c(t) = n\left(\sqrt{t N_K(\mathfrak{b})}\right) - 1$ ← WE DON'T COUNT NONZERO POINTS

$$i_c(t) = \frac{\pi t N_K(\mathfrak{b})}{|U_K|\,\mathrm{Vol}(\phi)} + \varepsilon(t) \qquad \frac{\varepsilon(t)}{\sqrt{t}} \text{ BOUNDED AS } t\to\infty \Rightarrow \varepsilon(t) = O(\sqrt{t})$$

SINCE $\mathrm{Vol}(\phi) = \frac{1}{2}\sqrt{|d_K|}\,N_K(\mathfrak{b}) \Rightarrow i_c(t) = \dfrac{2\pi t}{|U_K|\sqrt{|d_K|}} + O(\sqrt{t})$

WE TAKE $\alpha = \dfrac{2\pi}{|U_K|\sqrt{|d_K|}}$ (THIS IS $\dfrac{\pi}{\sqrt{|d_K|}}$ UNLESS $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$) //

MORE GENERALLY, LET $U_K \cong V \oplus T$ WHERE $V \cong \mathbb{R}^{r+s-1}$. THEN

$$V \subseteq U_K \subseteq \mathcal{O}_K^\times \xhookrightarrow{\varphi} (\mathbb{R}^+)^r \times (\mathbb{C}^\times)^s \xrightarrow{\log} \mathbb{R}^{r+s} \qquad \Psi = \log\circ\varphi$$

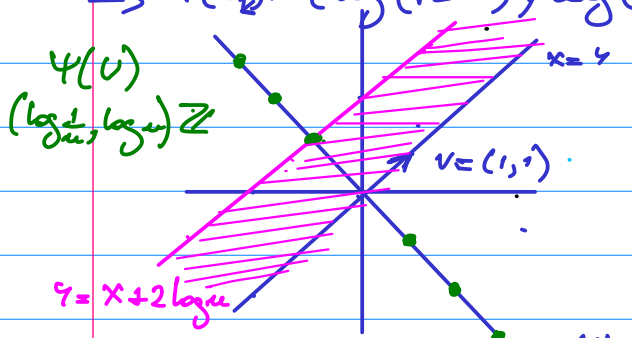
$$a \longmapsto (\sigma_1(a), \dots, \sigma_r(a), \tau_1(a), \dots, \tau_s(a))$$

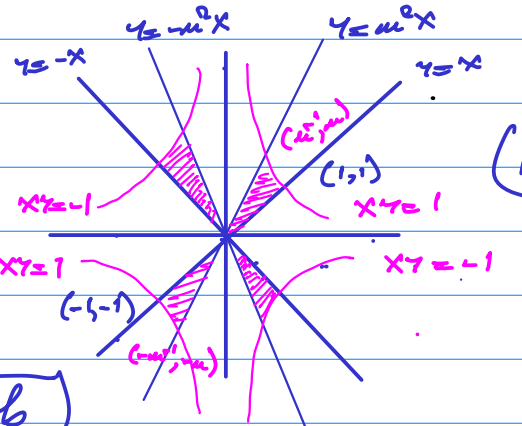
$$(x_1, \dots, x_r, z_1, \dots, z_s) \longmapsto (\log|x_1|, \dots, \log|x_r|, \log|z_1|, \dots, \log|z_s|)$$

TAKE $D = \log^{-1}(\phi \oplus \mathbb{R}v)$, WHERE ϕ IS A FUNDAMENTAL DOMAIN FOR $\Psi(V)$ AND $v \in \mathbb{R}^{r+s} \setminus H$. IF WE COUNT ELEMENTS IN $\varphi(\mathfrak{b}) \cap D$ OF NORM UP TO $t N_K(\mathfrak{b})$, WE WILL GET $|T|\, i_c(t)$

IDEA OF THE PROOF OF THE REAL QUADRATIC CASE TAKE, FOR EXAMPLE, $\mathbb{Q}(\sqrt{2})$. THEN $\Psi(U_K) \subseteq \{x+y=0\} \subseteq \mathbb{R}^2$ $\quad U_K = \{\pm(1+\sqrt{2})^k \mid k \in \mathbb{R}\}$

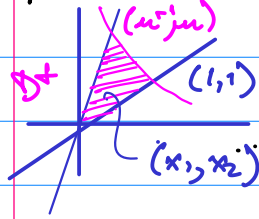
$$\Rightarrow \Psi(U_K) = \left(\log(\sqrt{2}-1), \log(\sqrt{2}+1)\right)\mathbb{Z}$$





THE GOAL IS TO LOOK AT $\varphi(\mathfrak{b}) \cap D(\sqrt{t N_K \mathfrak{b}})$

THE MAP $\log:(\mathbb{R}^\times)^2 \to \mathbb{R}^2$ IS $\Psi(a+b\sqrt{2}) = \left(\log|a-b\sqrt{2}|, \log|a+b\sqrt{2}|\right)$



$$x_1 = t e^{s\omega_1} \qquad (\omega_1,\omega_2) = \left(\log(\sqrt{2}-1), \log(\sqrt{2}+1)\right)$$

$$x_2 = t e^{s\omega_2} \qquad \begin{vmatrix} \frac{\partial x_1}{\partial t} & \frac{\partial x_1}{\partial s} \\ \frac{\partial x_2}{\partial t} & \frac{\partial x_2}{\partial s} \end{vmatrix} = \begin{vmatrix} e^{s\omega_1} & \omega_1 t e^{s\omega_1} \\ e^{s\omega_2} & \omega_2 t e^{s\omega_2} \end{vmatrix} = (\omega_2-\omega_1) t e^{s(\omega_1+\omega_2)} = (\omega_2-\omega_1)t$$

$$0 \le t \le 1 \qquad 0 \le s \le 1$$

We have $\mathrm{Vol}(D(i)) = 4\,\mathrm{Vol}(\mathcal{D}^+) = 4\int_{\mathcal{D}^+} dx_1 dx_2 = 4\int_0^1\int_0^1 t(\omega_2-\omega_1)\,dt\,ds$

$= 2(\omega_2-\omega_1) = 2\log\left(\frac{\sqrt{2}+1}{\sqrt{2}-1}\right) = 2\log u^2 = 4\log u$

Then $i_c(\mathfrak{k}) \sim \frac{4\log u \cdot h_{\mathfrak{k}}(\mathfrak{b})}{|T|\,\mathrm{Vol}(\mathcal{O})} = \frac{4\log u \cdot h_{\mathfrak{k}}(\mathfrak{b})}{|T|\sqrt{|d_{\mathfrak{k}}|}\,N_{\mathfrak{k}}(\mathfrak{b})}$

$\alpha(\mathfrak{k}) = \frac{4\log u}{|T|\sqrt{|d_{\mathfrak{k}}|}}$ #

For the general case, $\alpha(\mathfrak{k}) = \frac{2^{r+s}\,\pi^s\,\mathrm{Reg}(C_{\mathfrak{k}})}{|T|\sqrt{|d_{\mathfrak{k}}|}}$

If $\{v_1,\dots,v_{r+s-1}\}$ is a $\mathbb{Z}$-basis for the lattice $\Psi(V)$, then the regulator $\mathrm{Reg}(C_{\mathfrak{k}})$ is the absolute value of the determinant obtained by deleting any column from the matrix of rows $v_1,\dots,v_{r+s-1}$.