Remarks about class groups.

1. They control unique factorization.
2. They control the abelian extensions of K.
   (Class field theory). $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$
3. We know which imaginary quadratic fields have $h_K = 1$.
   $\| \; |Cl(\mathcal{O}_K)|$

   Statistics of size are still an open problem
   (Cohen-Lenstra heuristics)
4. For real quadratic fields we expect but don't know that ∞'ly many have class # 1.
5. Class numbers $\mathbb{Q}(\sqrt{p})$ Known $h_K = 1 \iff p \leq 19$
   p prime.

Units K is a number field, what is $\mathcal{O}_K^\times$ (multiplicative units in $\mathcal{O}_K$)?
(U_K).

(The other part of factorization...)

Recall $\alpha \in \mathcal{O}_K$ is a unit $\iff N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Example: In $\mathbb{Q}(\sqrt{m})$ $m \equiv 2$ or $3 \bmod 4$.
Units in $\mathbb{Z}[\sqrt{m}]$ $\leftrightarrow$ solution in $\mathbb{Z}^2$ to $a^2 - b^2 m = \pm 1$

$N_{\mathbb{Q}(\sqrt{m})}(a + b\sqrt{m})$

E.g. $\mathbb{Q}(\sqrt{-17})$ $\rightsquigarrow$ $a^2 + 17b^2 = \pm 1$.

$\Rightarrow b = 0$, $a = \pm 1$

Units in $\mathbb{Z}[\sqrt{-17}]$ are ± 1.

In general if $m < 0$ there only finitely many solutions (usually just ± 1).

(in particular roots of unity)

E.g. $\mathbb{Q}(\sqrt{5})$ $\quad a^2 - 5b^2 = \pm 1$

$a = 1 \quad b = 1 \quad \rightsquigarrow -4$

$a = 2 \quad b = 0 \quad \rightsquigarrow 4$.

$\frac{1+\sqrt{5}}{2}$ is in $\mathcal{O}_K$ $\quad K = \mathbb{Q}(\sqrt{5})$.

and its norm is -1.

Infinite order.

Theorem: $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$

$\mu(K)$: roots of unity in K

r = # of real embeddings

s = # of complex embeddings / 2

E.g. $K = \mathbb{Q}(\sqrt{m})$ $\quad m < 0 \Rightarrow r = 0, s = 1$

$\mathcal{O}_K^\times = \mu(K)$.

$K = \mathbb{Q}(\sqrt{m})$ $\quad m > 0 \Rightarrow r = 2, s = 0$.

$\mathcal{O}_K^\times = \mu(K) \times \mathbb{Z}$

ζ $= \{\pm 1\} \times \mathbb{Z}$.

In particular applies to $Q(\sqrt{5}) = K$

$\Rightarrow$ $\mathcal{O}_K^\times = \{\pm 1\} \times \langle \frac{1+\sqrt{5}}{2} \rangle$.

"fundamental unit"

Know $\mathcal{O}_{K,\text{tors}}^\times = \mu(K)$ and is cyclic of finite order.

To show f.g. of rank $\leq r+s-1$:

$\sigma_1, \dots, \sigma_r$ embeddings $K \hookrightarrow \mathbb{R}$

$\tau_1, \dots, \tau_s$ embeddings $K \hookrightarrow \mathbb{C}$

One per equivalence class w/ complex conjugation

$$L: \mathcal{O}_K^\times \longrightarrow \mathbb{R}^{r+s}$$
$$\alpha \longmapsto (\log|\sigma_1(\alpha)|, \log|\sigma_2(\alpha)|, \dots, 2\log|\tau_1(\alpha)|, \dots 2\log|\tau_s(\alpha)|)$$

Observations: • This is a homomorphism.

• Image is contained in $x_1 + x_2 + \dots + x_{r+s} = 0$.

($N(\alpha) = \pm 1 \cdot |N(\alpha)| = 1$.

expand as a product, take $\log$)

• Kernel is $\mu(K)$. (exercise last week)

$L: \mathcal{O}_K^\times / \mu(K) \hookrightarrow$ Real vector space of dimension $r+s-1$.

If we can show this is a lattice, then we get $\mathcal{O}_K^\times$ f.g. with rank $\leq r+s-1$.

Need to show intersection some open ball around zero has finitely many elements.
(Follows from $\mathcal{O}_K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$ as a lattice)

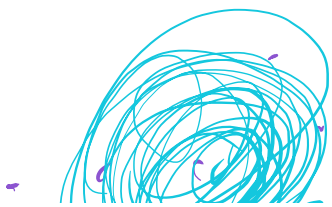
Most interesting part: producing enough units to see the rank is $r+s-1$.

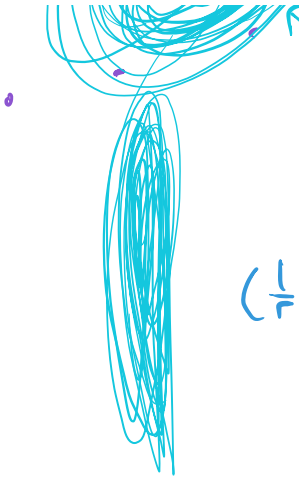
We'll show for $K = \mathbb{Q}(\sqrt{m})$ $m > 0$.
(Why does $a^2 - b^2 m = \pm 1$ have a solution with $b \neq 0$).

Idea: Use Minkowski's theorem + idea of pigeonhole guess & check.

$\mathcal{O}_K \hookrightarrow \mathbb{R}^2$ is a lattice (volume f.d. is $\sqrt{\Delta_K}$),

Take T to be any convex symmetric set with area big enough that Minkowski's theorem guarantees it contains a point of $\mathcal{O}_K$.





T $\mathcal{O}_K$

N is bounded on T

$N(x,y) = xy \leq M$

$\left(\frac{1}{r}, r\right) \cdot T$ then has same value and the same norm bound, still symmetric & convex.

$\left(\frac{1}{n}, n\right) \cdot T$ contains a number $\alpha_n \in \mathcal{O}_K$. $n \in \mathbb{N}$ of norm $\leq M$.

There are only finitely many principal ideals $I_1, \dots, I_{8K}$ of Norm $\leq M$.

$I_1 = (\beta_1) \quad \dots \quad I_{8K} = (\beta_K)$.

$\beta_i = (x_i, y_i)$

$\uparrow$ minimal x-coordinate.

α_n for $n \gg 0$ is not equal to β_i for any i.

but $\alpha_n = (\beta_i)$ for some i.

$\frac{\alpha_n}{\beta_i}$ is a unit. ($\neq \pm 1$) of infinite order.