Class groups.

Recall: Dedekind domain is a UFD $\leftrightarrow$ it's a PID.

Class group will measure the failure to be a PID.

Def'n: • The group of fractional ideals in a DD A is the free abelian group generated by the prime ideals

• The group of nonzero finitely generated A-submodules of $K = \mathrm{Frac}(A)$.

M_1, M_2 are f.g. submodules, then $M_1 \cdot M_2$ gives the group law.

$(a,b) \cdot (c,d) = (ac, bc, ad, bd)$.

To get inverses:

1) Clear denominators $\rightsquigarrow$ for any M, $\exists\ s \in K$ s.t. $(s)M \subseteq A$.

i.e. $(s)M$ is an ideal.

2) If I an ideal, write $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$

take $a \in I$

$$(a) = \mathfrak{p}_1^{e_1+b_1} \cdots \mathfrak{p}_m^{e_m+b_m} \mathfrak{q}_1^{h_1} \cdots \mathfrak{q}_s^{h_s}.$$

$$\Updownarrow$$

$$(a) = I\, \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_m^{b_m} \mathfrak{q}_1^{h_1} \cdots \mathfrak{q}_s^{h_1}.$$

$$(1) = (a)^{-1}(a) = I \left(\mathfrak{p}_1^{b_1} \cdots \cdots \mathfrak{q}_s^{h_1}\right)/a$$

$Cl(A) =$ Fractional ideals / Principal (fractional) ideals.

↑ Every class contains an actual ideal.

trivial $\Leftrightarrow$ ideal is principal.

$Cl(A)$ is trivial $\Leftrightarrow$ A is a PID $\Leftrightarrow$ A is a UFD.

Remark: Fractional ideals $\leftrightarrow$ Cartier divisors on $\operatorname{Spec} A$.

Big result in a minute: If K is a #-field, then $Cl(\mathcal{O}_K)$ is finite and effectively computable.

Example: $A = \mathbb{C}[x,y]/(y^2 - x^3 - x)$ then $Cl(A)$ is infinite. (this one $\cong \mathbb{C}/\mathbb{Z}+\mathbb{Z}i$).

- If A is the integral closure of $\mathbb{F}_q[t]$ in a finite extension of $\mathbb{F}_q(t)$ the $Cl(A)$ is finite.

The size of an ideal:

K a # field and for I an ideal in $\mathcal{O}_K$,

$$N(I) = |\mathcal{O}_K / I|.$$

Note: if $I = (a)$ $N(I) = |N(a)|$.

if $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}$ then

$$N(I) = \prod \mathfrak{p}_i^{e_i f_i}$$ where $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$

p_i prime #.

Theorem: (Minkowski's bound). Let $[K : \mathbb{Q}] = n$ and let Δ_K = discriminant of

Then any class in $Cl(\mathcal{O}_K)$ is represented by an ideal I of $\mathcal{O}_K$ s.t. $N(I) \leq \underbrace{\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}}_{B_K} |\Delta_K|^{1/2}$.

$s = \frac{1}{2}$ # of embeddings $K \hookrightarrow \mathbb{C}$ that don't factor through $\mathbb{R}$.

Corollary: $Cl(\mathcal{O}_K)$ is finite.

Corollary: There is no unramified extension of $\mathbb{Q}$.

PF: p ramifies in $K \Leftrightarrow p \mid \Delta_K$.

$$\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} < 1$$

(I.e. $\operatorname{Spec} \mathbb{Z}$ is simply connected).

Example: Quadratic Fields $K = \mathbb{Q}(\sqrt{m})$. m squarefree

$m < 0$ $m \equiv 1 \bmod 4 \rightsquigarrow s = 1$, $\Delta_K = m$. $n = 2$

$$B_K = \frac{4}{\pi}\frac{2}{4}\sqrt{m} = \frac{2}{\pi}\sqrt{m}.$$

(e.g. if $m = -3$, this is < 2, so class group is trivial).

$m < 0$ $m \equiv 3 \bmod 4 \rightsquigarrow B_K = \frac{4}{\pi}\sqrt{m}$.

$m > 0$ $m \equiv 1 \bmod 4 \rightsquigarrow s = 0$

$$B_K = \frac{1}{2}\sqrt{m}.$$

(e.g. if $m = 5$ get class)

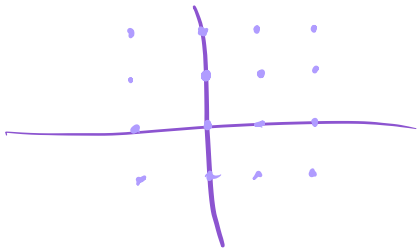
number 1 1.

$M>0$ $M \equiv 3$ and $4 \rightsquigarrow B_K = \sqrt{M}$.

Proof for imaginary quadratic fields: $K = \mathbb{Q}(\sqrt{-m})$ $m>0$,

$\mathcal{O}_K \subseteq \mathbb{C}$.

e.g. if $M=-1$
$\mathcal{O}_K = \mathbb{Z}[i]$.



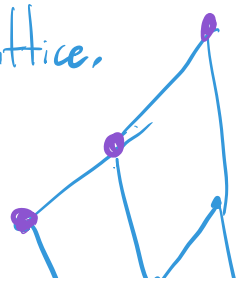
Lemma: It suffices to show that for any ideal $I \subseteq \mathcal{O}_K$
$\exists\ a \in I$ s.t. $N(a) \leq B_K N(I)$.

Pf: Let $x \in Cl(\mathcal{O}_K)$ and let I be
an ~~principal~~ ideal representing x^{-1}.
Then take $a \in I$ s.t. $N(a) \leq B_K N(I)$
Corrected after recording
$a = \frac{(a)}{I} \cdot I$.

$\frac{(a)}{I}$ represents $(I)^{-1}$ in $Cl(A)$.

$N\left(\frac{(a)}{I}\right) = N(a)/N(I) \leq B_K$.

I a nonzero ideal $\Rightarrow$
$I \subseteq \mathcal{O}_K \subseteq \mathbb{C}$ is a lattice.



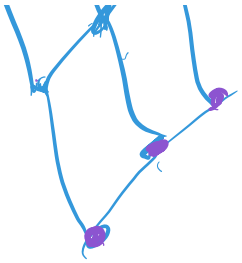
the point is $\mathcal{O}_K/I$ is finite.
$\Rightarrow$ structure theory of f.g.
ab. groups $\Rightarrow$ ∃ a basis

e_1, e_2 for $\mathcal{O}_K$

and integers d_1 d_2 with

$d_1 e_1$ $d_2 e_2$ a basis for I

(as a $\mathbb{Z}$-module)



Q: If I have a lattice of area A, how close to the origin is the smallest non-zero lattice point?

Theorem If a lattice $L \subseteq \mathbb{R}^n$ has volume V and D is a convex, symmetric (bounded) region in $\mathbb{R}^n$ of volume $\geq 2^n V$ then $L \cap D \neq \{(0)\}$!

Pf: Take a fundamental parallelopiped ($F = \hat{\sum_{i=1}^{n}} a_i e_i$, $0 \leq a_i \leq 1$, e_i are a basis for L)

$\mathrm{Vol}(F) = V$.

$$\mathbb{R}^n = \bigcup_{\lambda \in L} \lambda + F$$

$$\left(\tfrac{1}{2}D\right) = \bigcup_{\lambda \in L} (\lambda + F) \cap \left(\tfrac{1}{2}D\right)$$

$$\mathrm{Vol}\left(\tfrac{1}{2}D\right) = \sum \mathrm{Vol}\left((\lambda + F) \cap \left(\tfrac{1}{2}D\right)\right)$$

S_λ

can think of S_λ as a subset of F by translation

$$\tfrac{1}{2^n}\mathrm{Vol}(D) = \sum \mathrm{Vol}(S_\lambda)$$

$$\mathrm{Vol}(F) \leq \sum \mathrm{Vol}(S_\lambda).$$

↯ suppose actually strict.

Then $S_{\lambda_1} \cap S_{\lambda_2} \neq \emptyset$. $\lambda_1 \neq \lambda_2$

$\exists\ x \in S_{\lambda_1} \cap S_{\lambda_2}$.

i.e, $x+\lambda_1$ and $x+\lambda_2$ are both in $\frac{1}{2}D$.

$x+\lambda_1$ and $-x-\lambda_2$ are both in $\frac{1}{2}D$

(by convexity) $\frac{x+\lambda_1+(-x-\lambda_2)}{2}$ in $\frac{1}{2}D$

$\lambda_1-\lambda_2$ in D.

Minkowski for $K \subseteq \mathbb{Q}(\sqrt{-m})$, $m>0$ squarefree.

$I \subseteq \mathcal{O}_K$. $N(I) = |\mathcal{O}_K/I|$.

$\mathrm{Vol}(I) = \mathrm{Vol}(\mathcal{O}_K)\cdot N(I)$.

$\mathcal{O}_K = \mathbb{Z}+\mathbb{Z}\sqrt{-m}$ $\rightsquigarrow$ $\mathrm{Vol} = \sqrt{m} = \frac{1}{2}|\Delta_K|^{\frac{1}{2}}$

or $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{-m}}{2}\right)$ $\rightsquigarrow$ $\mathrm{Vol} = \frac{\sqrt{m}}{2} = \frac{1}{2}|\Delta_K|^{\frac{1}{2}}$.

$$\mathrm{Vol}(|z| \le t) = \pi t^2$$

Need this to be $4\cdot \mathrm{Vol}(I) = 4N(I)\frac{1}{2}|\Delta_K|^{\frac{1}{2}}$

$$\pi t^2 = 4N(I)\tfrac{1}{2}|\Delta_K|^{\frac{1}{2}}$$

$$t^2 = \frac{4}{\pi}\tfrac{1}{2}|\Delta_K|^{\frac{1}{2}}N(I)$$

$\S$

Get an element in I with $\mathrm{Norm} \le B_K N(I)$.

The general case:

- Choose a good symmetric domain for this theorem

$[K:\mathbb{Q}] = n$

- Relate $\sqrt{|\text{discriminant}|}$ to the volume of $\mathcal{O}_K$.

$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}^s \times \mathbb{R}^{n-2s}$

But living where?

Use that both transform by $|\det|$

Check what $\sim$ is

the ratio is on $\mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \cdots$

$\langle 1, i \rangle \times \langle 1, i \rangle \times \cdots \times \langle 1 \rangle \times \langle 1 \rangle \times \langle 1 \rangle \cdots$

Pick one adapted to AM-GM inequality.

$$S_t = \sum_{i=1}^{s} 2|z_i| + \sum_{j=s+1}^{n} |r_j| \leq t$$