Ideal class groups [1]

Introductory presentation

David Kurniadi Angdinata

London School of Geometry and Number Theory

Wednesday, 6 October 2021

[1] of number fields

Diophantine equations!

Consider *Mordell's equation*

$$y^2 = x^3 + n, \qquad n \in \mathbb{Z}.$$

- Consider $y^2 = x^3 - 1$. Solution: $(1, 0)$.

  Claim: $y = 0$. Check: x odd. In $\mathbb{Z}[i]$,

  $$(y+i)(y-i) = x^3 \overset{\text{Nm}}{\Longrightarrow} y \pm i \text{ coprime} \overset{\text{UFD}}{\Longrightarrow} y \pm i \text{ cubes}.$$

  Let
  $$y + i = (a+bi)^3 = a(a^2 - 3b^2) + b(3a^2 - b^2)i.$$

  Then $b = \pm 1$.
  - $b = 1 \implies 3a^2 = 2$, contradiction.
  - $b = -1 \implies 3a^2 = 0 \implies y = 0$.

  Idea: use UF of $\mathbb{Z}[i]$ and $\text{Nm} : \mathbb{Z}[i] \to \mathbb{N}$.

Diophantine equations!

Consider *Mordell's equation*

$$y^2 = x^3 + n, \qquad n \in \mathbb{Z}.$$

- Consider $y^2 = x^3 - 1$. Solution: $(1, 0)$.

  Idea: use UF of $\mathbb{Z}[i]$ and $\mathrm{Nm} : \mathbb{Z}[i] \to \mathbb{N}$.
- Consider $y^2 = x^3 - 5$. In $\mathbb{Z}[\sqrt{-5}]$,

  $$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

  However, on ideals,

  $$(6) = (2, 1 + \sqrt{-5}) \cdot (2, 1 - \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}).$$

  Furthermore, can define norm on ideals. Conclusion: consider ideals.

The ideal class group...

Let K be a number field, and let $\mathcal{O}_K$ be its *ring of integers*,

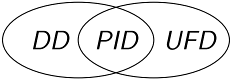
$$\mathcal{O}_K = \{x \in K : \exists f \in \mathbb{Z}[X] \text{ monic}, \ f(x) = 0\}.$$

Examples

- $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$,
- $K = \mathbb{Q}(i)$ and $\mathcal{O}_K = \mathbb{Z}[i]$, or
- $K = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O}_K = \mathbb{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-3}}{2}$.

Fact

$\mathcal{O}_K$ is a Dedekind domain. Every DD has UF into prime ideals.



The ideal class group...

The *ideal norm* is

$$\mathrm{Nm}(I) = \#(\mathcal{O}_K/I), \qquad I \trianglelefteq \mathcal{O}_K.$$

Example

If $K = \mathbb{Q}(\sqrt{-5})$, then $(2, 1+\sqrt{-5}) \trianglelefteq \mathcal{O}_K$ has ideal norm

$$\begin{aligned}\mathrm{Nm}((2, 1+\sqrt{-5})) &= \#(\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5})) \\ &= \#(\mathbb{Z}[X]/(2, 1+X, 5+X^2)) \\ &= \#(\mathbb{F}_2[X]/(1+X, 1+X^2)) = 2.\end{aligned}$$

Fact

$$\mathrm{Nm}(I \cdot J) = \mathrm{Nm}(I)\,\mathrm{Nm}(J), \qquad \mathrm{Nm}((x)) = \mathrm{Nm}(x) = \prod_{\sigma : K \to \overline{K}} \sigma(x).$$

The ideal class group...

Consider the set of non-zero *fractional ideals* of $\mathcal{O}_K$,

$$\mathcal{I}(K) = \{x^{-1}I \subseteq K : x \in \mathcal{O}_K^\times,\ I \trianglelefteq \mathcal{O}_K\} \setminus \{(0)\}.$$

This is an abelian group under ideal multiplication, with identity (1) and

$$I^{-1} = \{x \in K : xI \subseteq \mathcal{O}_K\}, \qquad I \in \mathcal{I}(K).$$

It has a subgroup of *principal fractional ideals*

$$\mathcal{P}(K) = \{(x) \in \mathcal{I}(K) : x \in K^\times\} \leq \mathcal{I}(K).$$

The quotient is the *ideal class group* $\mathrm{Cl}(K)$.

Theorem

$\mathrm{Cl}(K)$ *is finite.*

Proof.

Geometry of numbers gives *Minkowski's bound* $M_K \in \mathbb{R}_{>0}$. Every $[I] \in \mathrm{Cl}(K)$ has a representative $I \trianglelefteq \mathcal{O}_K$ with $\mathrm{Nm}(I) \leq M_K$. □

The ideal class group...

Examples

- If $K = \mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, then $\mathrm{Cl}(K) = 1$, since $\mathcal{O}_K$ is a PID.
- If $K = \mathbb{Q}(\sqrt{-5})$, then $\mathrm{Cl}(K) \neq 1$, since $(2, 1+\sqrt{-5}) \in \mathcal{I}(K)$ is not principal. However $(2, 1+\sqrt{-5})^2 = (2)$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $(3, 1-\sqrt{-5}) = (\frac{1-\sqrt{-5}}{2}) \cdot (2, 1+\sqrt{-5})$.

Consider $y^2 = x^3 - 5$. Check: x odd. In $\mathbb{Z}[\sqrt{-5}]$,

$$\begin{aligned}(y+\sqrt{-5})(y-\sqrt{-5}) = (x)^3 &\overset{\text{Nm}}{\Longrightarrow} (y \pm \sqrt{-5}) \text{ coprime ideals} \\ &\overset{\text{DD}}{\Longrightarrow} (y \pm \sqrt{-5}) \text{ ideal cubes.}\end{aligned}$$

Since $3 \nmid \# \mathrm{Cl}(\mathbb{Q}(\sqrt{-5}))$,

$$\begin{aligned}(y \pm \sqrt{-5}) = (a \pm b\sqrt{-5})^3 &\implies y \pm \sqrt{-5} = (a \pm b\sqrt{-5})^3 \\ &\implies \dots \\ &\implies \text{contradiction}\end{aligned}$$

What's next?

- Quadratic forms and form class group

$$\mathrm{Cl}(\mathbb{Q}(\sqrt{n})) \cong \mathrm{Cl}(\Delta_{\mathbb{Q}(\sqrt{n})})$$

- Picard group and algebraic K-theory

$$\mathrm{Cl}(K) \cong \mathrm{Pic}(\mathrm{Spec}(\mathcal{O}_K)) \qquad K_0(\mathcal{O}_K) \cong \mathbb{Z} \oplus \mathrm{Cl}(K)$$

- Idele class group and class field theory

$$C^1(K) \twoheadrightarrow \mathrm{Cl}(K) \qquad \mathrm{Cl}(K) \cong \mathrm{Gal}(H(K)/K)$$

- Elliptic curves and Tate–Shafarevich group

$$\mathrm{Cl}(K) \cong Ш(K)$$

- Class number one problem and Cohen–Lenstra heuristics

$$\mathrm{Prob}(\mathrm{Cl}(\mathbb{Q}(\sqrt{p})) = 1 \mid p > 0 \text{ prime}) \approx \tfrac{3}{4}$$