Ideal Class Groups [1]

David Ang

LSGNT

Short introductory talk

Wednesday, 6 October 2021

[1] of number fields

Diophantine equations!

Consider *Mordell's equation*

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

Diophantine equations!

Consider *Mordell's equation*

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

- Consider $y^2 = x^3 - 1$.

Diophantine equations!

Consider *Mordell's equation*

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

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

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: $y = 0$.

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.

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 $\mathbb{Z}[i]$,

$$(y + i)(y - i) = x^3$$

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 $\mathbb{Z}[i]$,

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

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 $\mathbb{Z}[i]$,

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

  Otherwise

  $$p \mid y \pm i$$

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 $\mathbb{Z}[i]$,

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

  Otherwise

  $$p \mid y \pm i \overset{\mathrm{Nm}}{\Longrightarrow} \mathrm{Nm}(p) \mid y^2 + 1 = x^3$$

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 $\mathbb{Z}[i]$,

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

Otherwise

$$p \mid y \pm i \overset{\mathrm{Nm}}{\Longrightarrow} \mathrm{Nm}(p) \mid y^2 + 1 = x^3$$

$$\Downarrow$$

$$p \mid 2i$$

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 $\mathbb{Z}[i]$,

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

  Otherwise

  $$\begin{array}{ccc} p \mid y \pm i & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(p) \mid y^2 + 1 = x^3 \\ \Downarrow & & \\ p \mid 2i & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(p) \mid 4 \end{array}$$

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 $\mathbb{Z}[i]$,

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

  Otherwise

  $$\begin{array}{ccc} p \mid y \pm i & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(p) \mid y^2 + 1 = x^3 \\ \Downarrow & & \qquad\qquad \Longrightarrow \mathrm{Nm}(p) = 1 \\ p \mid 2i & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(p) \mid 4 \end{array}$$

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 $\mathbb{Z}[i]$,

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

  Otherwise

  $$\begin{array}{ccccc} p \mid y \pm i & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(p) \mid y^2 + 1 = x^3 & & \\ \Downarrow & & & \Longrightarrow & \mathrm{Nm}(p) = 1 \ \lightning \\ p \mid 2i & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(p) \mid 4 & & \end{array}$$

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 $\mathbb{Z}[i]$,

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

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 $\mathbb{Z}[i]$,

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

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

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 $b = \pm 1$.

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 $\mathbb{Z}[i]$,

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

  Let
  $$y + i = (a + bi)^3 = a(a^2 - 3b^2) + b(3a^2 - b^2)i.$$
  Then $b = \pm 1$.
  - $b = 1 \implies 3a^2 = 2$ ↯

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 $\mathbb{Z}[i]$,

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

  Let

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

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

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 $\mathbb{Z}[i]$,

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

  Let

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

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

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

Diophantine equations!

Consider *Mordell's equation*

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

- Consider $y^2 = x^3 - 1$. Idea: use UF of $\mathbb{Z}[i]$ and $\mathrm{Nm} : \mathbb{Z}[i] \to \mathbb{N}$.
- Consider $y^2 = x^3 - 5$.

Diophantine equations!

Consider *Mordell's equation*

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

- Consider $y^2 = x^3 - 1$. Idea: use UF of $\mathbb{Z}[i]$ and $\mathrm{Nm} : \mathbb{Z}[i] \to \mathbb{N}$.
- Consider $y^2 = x^3 - 5$. In $\mathbb{Z}[\sqrt{-5}]$,

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

Diophantine equations!

Consider *Mordell's equation*

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

- Consider $y^2 = x^3 - 1$. 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,

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

Diophantine equations!

Consider *Mordell's equation*

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

- Consider $y^2 = x^3 - 1$. 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,

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

Furthermore, can define norm on ideals.

Diophantine equations!

Consider *Mordell's equation*

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

- Consider $y^2 = x^3 - 1$. 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,

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

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

The ideal class group...

Let K be a number field,

The ideal class group...

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

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

The ideal class group...

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

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

Examples

- $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$,

The ideal class group...

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

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

Examples

- $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$,
- $K = \mathbb{Q}(i)$ and $\mathcal{O}_K = \mathbb{Z}[i]$, or

The ideal class group...

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

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

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 $\omega = \frac{1+\sqrt{-3}}{2}$.

The ideal class group...

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

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

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.

The ideal class group...

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

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

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...

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

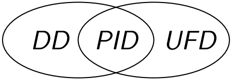
$$\mathcal{O}_K = \{x \in K \mid \exists f \in \mathbb{Z}[X] \text{ monic, } f(x) = 0\}.$$

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

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

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 $\langle 2, 1+\sqrt{-5}\rangle \trianglelefteq \mathcal{O}_K$

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 $\langle 2, 1+\sqrt{-5}\rangle \trianglelefteq \mathcal{O}_K$ has ideal norm

$$\mathrm{Nm}(\langle 2, 1+\sqrt{-5}\rangle) = \#(\mathbb{Z}[\sqrt{-5}]/\langle 2, 1+\sqrt{-5}\rangle)$$

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 $\langle 2, 1+\sqrt{-5}\rangle \trianglelefteq \mathcal{O}_K$ has ideal norm

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

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 $\langle 2, 1+\sqrt{-5}\rangle \trianglelefteq \mathcal{O}_K$ has ideal norm

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

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 $\langle 2, 1+\sqrt{-5}\rangle \trianglelefteq \mathcal{O}_K$ has ideal norm

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

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 $\langle 2, 1+\sqrt{-5}\rangle \trianglelefteq \mathcal{O}_K$ has ideal norm

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

Fact

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

The ideal class group...

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

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

The ideal class group...

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

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

This is an abelian group under ideal multiplication, with identity $\langle 1 \rangle$ and

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

The ideal class group...

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

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

This is an abelian group under ideal multiplication, with identity $\langle 1 \rangle$ and

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

It has a subgroup of *principal fractional ideals*

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

The ideal class group...

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

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

This is an abelian group under ideal multiplication, with identity $\langle 1 \rangle$ and

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

It has a subgroup of *principal fractional ideals*

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

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

The ideal class group...

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

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

This is an abelian group under ideal multiplication, with identity $\langle 1 \rangle$ and

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

It has a subgroup of *principal fractional ideals*

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

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

Theorem

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

The ideal class group...

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

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

This is an abelian group under ideal multiplication, with identity $\langle 1 \rangle$ and

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

It has a subgroup of *principal fractional ideals*

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

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

Theorem

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

Proof.

Geometry of numbers gives *Minkowski's bound* $\mathrm{M}_K \in \mathbb{R}_{>0}$.

$\square$

The ideal class group...

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

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

This is an abelian group under ideal multiplication, with identity $\langle 1\rangle$ and

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

It has a subgroup of *principal fractional ideals*

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

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

Theorem

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

Proof.

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

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.

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 $\langle 2, 1 + \sqrt{-5} \rangle \in \mathcal{I}(K)$ is not principal.

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 $\langle 2, 1 + \sqrt{-5} \rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1 + \sqrt{-5} \rangle^2 = \langle 2 \rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$.

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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 $\langle 2, 1 + \sqrt{-5} \rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1 + \sqrt{-5} \rangle^2 = \langle 2 \rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1 - \sqrt{-5} \rangle = \langle \frac{1-\sqrt{-5}}{2} \rangle \cdot \langle 2, 1 + \sqrt{-5} \rangle$.

Consider $y^2 = x^3 - 5$.

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

Consider $y^2 = x^3 - 5$. Check: x odd.

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 \overset{\mathrm{Nm}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 \overset{\mathrm{Nm}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}$$

Otherwise

$$\mathfrak{p} \mid \langle y \pm \sqrt{-5}\rangle$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 \overset{\mathrm{Nm}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}$$

Otherwise

$$\mathfrak{p} \mid \langle y \pm \sqrt{-5}\rangle \overset{\mathrm{Nm}}{\Longrightarrow} \mathrm{Nm}(\mathfrak{p}) \mid y^2 + 5 = x^3$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 \overset{\mathrm{Nm}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}$$

Otherwise

$$\mathfrak{p} \mid \langle y \pm \sqrt{-5}\rangle \overset{\mathrm{Nm}}{\Longrightarrow} \mathrm{Nm}(\mathfrak{p}) \mid y^2+5 = x^3$$

$$\Downarrow$$

$$\mathfrak{p} \mid \langle 2\sqrt{-5}\rangle$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 \overset{\mathrm{Nm}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}$$

Otherwise

$$\begin{array}{ccc} \mathfrak{p} \mid \langle y \pm \sqrt{-5}\rangle & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(\mathfrak{p}) \mid y^2 + 5 = x^3 \\ \Downarrow & & \\ \mathfrak{p} \mid \langle 2\sqrt{-5}\rangle & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(\mathfrak{p}) \mid 20 \end{array}$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 \overset{\mathrm{Nm}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}$$

Otherwise

$$\begin{array}{lcl} \mathfrak{p} \mid \langle y \pm \sqrt{-5}\rangle & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(\mathfrak{p}) \mid y^2 + 5 = x^3 \\ \Downarrow & & \qquad\qquad \Longrightarrow \mathrm{Nm}(\mathfrak{p}) = 1, 5 \\ \mathfrak{p} \mid \langle 2\sqrt{-5}\rangle & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(\mathfrak{p}) \mid 20 \end{array}$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 \overset{\mathrm{Nm}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}$$

Otherwise

$$\begin{array}{lcll} \mathfrak{p} \mid \langle y \pm \sqrt{-5}\rangle & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(\mathfrak{p}) \mid y^2+5 = x^3 & \\ \Downarrow & & & \Longrightarrow \mathrm{Nm}(\mathfrak{p}) = 1, 5 \ \lightning \\ \mathfrak{p} \mid \langle 2\sqrt{-5}\rangle & \overset{\mathrm{Nm}}{\Longrightarrow} & \mathrm{Nm}(\mathfrak{p}) \mid 20 & \end{array}$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

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

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

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

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

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

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

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

$$\langle y \pm \sqrt{-5}\rangle = \langle a \pm b\sqrt{-5}\rangle^3$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 \overset{\mathrm{Nm}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}$$

$$\overset{\mathrm{DD}}{\Longrightarrow} \langle y \pm \sqrt{-5}\rangle \text{ ideal cubes.}$$

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

$$\langle y \pm \sqrt{-5}\rangle = \langle a \pm b\sqrt{-5}\rangle^3 \implies y \pm \sqrt{-5} = (a \pm b\sqrt{-5})^3$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

$$\begin{aligned}\langle y+\sqrt{-5}\rangle\langle y-\sqrt{-5}\rangle = \langle x\rangle^3 &\overset{\mathrm{Nm}}{\implies} \langle y \pm \sqrt{-5}\rangle \text{ coprime ideals}\\ &\overset{\mathrm{DD}}{\implies} \langle y \pm \sqrt{-5}\rangle \text{ ideal cubes.}\end{aligned}$$

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

$$\begin{aligned}\langle y \pm \sqrt{-5}\rangle = \langle a \pm b\sqrt{-5}\rangle^3 &\implies y \pm \sqrt{-5} = (a \pm b\sqrt{-5})^3\\ &\implies \ldots\end{aligned}$$

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 $\langle 2, 1+\sqrt{-5}\rangle \in \mathcal{I}(K)$ is not principal. However $\langle 2, 1+\sqrt{-5}\rangle^2 = \langle 2\rangle$, so $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Cl}(K)$. In fact $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, for instance $\langle 3, 1-\sqrt{-5}\rangle = \langle \frac{1-\sqrt{-5}}{2}\rangle \cdot \langle 2, 1+\sqrt{-5}\rangle$.

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

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

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

$$\begin{aligned} \langle y \pm \sqrt{-5}\rangle = \langle a \pm b\sqrt{-5}\rangle^3 &\Longrightarrow y \pm \sqrt{-5} = (a \pm b\sqrt{-5})^3 \\ &\Longrightarrow \dots \\ &\Longrightarrow \lightning \end{aligned}$$

What's next?

- Quadratic forms and form class group

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

What's next?

- Quadratic forms and form class group

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

- Picard group and algebraic K-theory

$$\mathrm{Cl}(K) \cong \mathrm{Pic}(\mathrm{Spec}(\mathcal{O}_K)) \qquad \mathrm{K}_0(\mathcal{O}_K) \cong \mathbb{Z} \oplus \mathrm{Cl}(K)$$

What's next?

- Quadratic forms and form class group

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

- Picard group and algebraic K-theory

$$\mathrm{Cl}(K) \cong \mathrm{Pic}(\mathrm{Spec}(\mathcal{O}_K)) \qquad \mathrm{K}_0(\mathcal{O}_K) \cong \mathbb{Z} \oplus \mathrm{Cl}(K)$$

- Idele class group and class field theory

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

What's next?

- Quadratic forms and form class group

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

- Picard group and algebraic K-theory

$$\mathrm{Cl}(K) \cong \mathrm{Pic}(\mathrm{Spec}(\mathcal{O}_K)) \qquad \mathrm{K}_0(\mathcal{O}_K) \cong \mathbb{Z} \oplus \mathrm{Cl}(K)$$

- Idele class group and class field theory

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

- Elliptic curves and Tate-Shafarevich group

$$\mathrm{Cl}(K) \cong Ш(K)$$

What's next?

- Quadratic forms and form class group

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

- Picard group and algebraic K-theory

$$\mathrm{Cl}(K) \cong \mathrm{Pic}(\mathrm{Spec}(\mathcal{O}_K)) \qquad \mathrm{K}_0(\mathcal{O}_K) \cong \mathbb{Z} \oplus \mathrm{Cl}(K)$$

- Idele class group and class field theory

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

- Elliptic curves and Tate-Shafarevich group

$$\mathrm{Cl}(K) \cong Ш(K)$$

- Class number one problem and Cohen-Lenstra heuristics

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