Class Groups of Quadratic Forms

Wilson Chen
chenzhuoxun0324@gmail.com

Euler Circle

July 12, 2022

Binary Quadratic Forms

- $f(x, y) = ax^2 + bxy + cy^2$, where a, b, and c are integers
- primitive if the integers a, b, and c are relatively prime
- f represents an integer n if $f(x, y) = n$ has an integer solution
- a form is positive definite if it represents only positive integers

Some Definitions

Ring

$< R, +, \bullet >$ is a ring if:
1.) $< \mathrm{R}, + >$ is an abelian group
2.) $< R, \bullet >$ is closed, well-defined and associative
3.)The distributive law holds:

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ where } a, b, c \in R$$

Quotient Ring

If $S < R$ then the quotient ring $R/S = \{r + S \mid r \in R\}$ $< \mathrm{R/S}, \oplus, \odot >$
- Define $\oplus$ as:

$$(a + S) \oplus (b + S) = (a + b) + S$$

- Define $\odot$ as:

$$(a + S) \odot (b + S) = (a \bullet b) + S$$

Some Definitions

Ideals

We say that I is an ideal of R if:
1.) $I > R$
2.) for any $i \in I$ and $r \in R$, we have $i \bullet r, r \cdot i \in I$
In other words, if $I < R$ for every $r \in R$ then $r * I \subseteq I$ and $I * r \subseteq I$

Isomorphism

If ϕ is a bijection then ϕ is an isomorphism and we say that rings R and S are isomorphic.

kernel

The kernel of a ring homomorphism $\phi : R \to S$, denoted ker ϕ, is the set of $r \in R$ such that $\phi(r) = 0$.

Ideals

Principal Ideals

If R is a commutative ring with unity and $a \in R$, the ideal $\{ar | r \in R\}$ is the principal ideal generated by a.

Fractional Ideals

Let R be a commutative domain and K its field of fractions. A fractional ideal of R is an R module I contained in K, such that for a certain non zero $a \in \bar{R}$ we have $aI \subset R$.

Algebraic Number Theory

Number Fields

A number field K is a field containing $\mathbb{Q}$ as a subfield which is a finite-dimensional $\mathbb{Q}$-vector space. The degree of K is its dimension.

Order of a Number Field

An order of an algebraic number field K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ which is also a $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

Bijection

We denote $\mathfrak{I}(R)/\mathfrak{P}(R)$ by $Cl(R)$.$Cl(R)$ is called the ideal class group of R. Let $\mathfrak{P}^{+}(R) = \{\alpha R; \alpha \in K, N_{K/\mathbb{Q}}(\alpha) > 0\}$. $\mathfrak{P}^{+}(R)$ is a subgroup of $\mathfrak{P}(R)$. We denote $\mathfrak{F}(R)/\mathfrak{P}^{+}(R)$ by $Cl^{+}(R)$. If K is a imaginary quadratic field, $Cl(R) = Cl^{+}(R)$. We can establish a bijection between $Cl^{+}(\mathbb{Q}(\sqrt{-D}))$ and the set of equivalence classes of primitive binary quadratic forms of discriminant D.

Class Groups as principal/fractionals

Let K be a number field, and let J_K denote the multiplicative group of fractional ideals of $\mathcal{O}_K$. Let P_K denote the multiplicative group of principal fractional ideals: those of the form $(x) = x\mathcal{O}_K$ for some $x \in K$. As J_K is abelian, we can now define the class group to be the quotient

$$\mathrm{Cl}_K := J_K / P_K$$

The elements of Cl_K are called classes.

The Minkowski's Theorem

Theorem

Let $S \subseteq \mathbb{R}^n$ be a convex set containing 0 which is centrally symmetric .
Let L be a lattice with mesh d. If either
(a) The volume of S exceeds $2^n d$, or
(b) The volume of S equals $2^n d$ and S is compact,
then S contains a nonzero lattice point of L.

The Minkowski bound

Thorem

Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be any nonzero ideal. Then there exists $0 \neq \alpha \in \mathfrak{a}$ such that

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|} \cdot \mathrm{N}(\mathfrak{a})$$

Computation of Class Group

Let $K = \mathbb{Q}(\sqrt{-14})$

1) $\lambda_K \sim 4.764$

2)

p	$T^2 + 14 \bmod p$	(p)
2	T^2	$\mathfrak{p}_2^2$
3	$(T-1)(T+1)$	$\mathfrak{p}_3\mathfrak{p}_3'$

3) $\mathfrak{p}_2^2 \sim 1, \mathfrak{p}_2 \sim \mathfrak{p}_2^{-1}$ $\mathfrak{p}_3\mathfrak{p}_3' \sim 1, \mathfrak{p}_3' \sim \mathfrak{p}_3^{-1}$.

4) $a^2 + 14b^2 = 2$ and $a^2 + 14b^2 = 3$ have no integral solutions.

5) $\mathrm{N}_{K/\mathbb{Q}}(2 + \sqrt{-14}) = 18 = 2 \cdot 3^2$.

Computation of Class Group

6) $2+\sqrt{-14}$ is not a multiple of 3 $\longrightarrow \mathfrak{p}_2\mathfrak{p}_3^2 \sim 1 \longrightarrow \mathfrak{p}_3^2 \sim \mathfrak{p}_2^{-1} \sim \mathfrak{p}_2,$

7) the class group of K is generated by $[\mathfrak{p}_3]$.

8) $\mathfrak{p}_2$ is nonprincipal and $\mathfrak{p}_2^2 \sim 1, [\mathfrak{p}_3]$ has order 4. Thus, the class group of K is cyclic of order 4 .

9) Thus we know there are 4 equivalence classes of binary quadratic forms of discriminant 14, and they form $\mathbb{Z}_4$

More Computation

Example $K = \mathbb{Q}(\sqrt{-65})$

1) $\mathcal{O}_K = \mathbb{Z}[\sqrt{-65}]$

2) $\lambda_K \sim 10.26$

3) $(2) = \mathfrak{p}_2^2, (3) = \mathfrak{p}_3\mathfrak{p}_3', (5) = \mathfrak{p}_5^2$, and $(7) = \mathfrak{p}_7$

4) $[\mathfrak{p}_7]$ is trivial $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$

5) none of $\mathfrak{p}_2, \mathfrak{p}_3$, or $\mathfrak{p}_5$ are principal

6) $(4 + \sqrt{-65}) = \mathfrak{p}_3^4$

7) $[\mathfrak{p}_5] = [\mathfrak{p}_2]^{-1} [\mathfrak{p}_3]^2$

8)$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{Cl}(K)$ 9) $\mathfrak{p}_2\mathfrak{p}_3^2 = (\alpha)$

10) $\mathrm{Cl}(K) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Heegner Number

Definition

A positive integer n is a Heegner number if the ring of integers of $\mathbb{Q}(\sqrt{-n})$ has unique prime factorization. In fact, $n = 163$ is the largest number for which $\mathbb{Q}(\sqrt{-n})$ has trivial class group. The complete list is $1, 2, 3, 7, 11, 19, 43, 67, 163$.

Thank You For Listening!

Thank you so much for your time. If you have any questions, please feel free to email me, post your question on the discord channel or send me a DM! If you are interested in this topic and want to discover more about abstract algebra, please read my paper!!!