Binary Quadratic Form

Yu-Hsuan Huang Che-Jui Chang Guan-Ting Chen

National Chiao Tung University

National Tsing Hua University

January 12, 2020

Binary Quadratic Form

Definition (binary quadratic form)

A binary quadratic form f is defined as

$$[a, b, c] := ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y],$$

with non-square discriminant $\Delta_f := b^2 - 4ac$ and $\gcd(a, b, c) = 1$. One could rewrite $f = [a, b, c]$ as a matrix, i.e.

$$f(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

denoted $f \sim \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$.

Binary Quadratic Form

Corollary

Suppose $\mathcal{B}_\Delta := \{f : \Delta_f = \Delta\}$. *Then the map* $\mathrm{SL}_2(\mathbb{Z}) \times \mathcal{B}_\Delta \to \mathcal{B}_\Delta$ *defined by*

$$\alpha f \mapsto \tilde{f}(x, y) = f\left(\begin{pmatrix} x & y \end{pmatrix} \alpha\right),$$

is a group action. For $f, g \in \mathcal{B}_\Delta$*, we say* $f \sim g$ *are equivalent forms iff they falls in the same orbit.*

In the matrix point of view one would have,

$$\alpha[a, b, c] \sim \alpha \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \alpha^T.$$

United Quadratic Form

Definition (United Quadratic Form)

Two quadratic forms $f_1 = [a_1, b_1, c_1], f_2 = [a_2, b_2, c_2]$ with same discriminant Δ are said to be united if and only if $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$.

Proposition

For united $[a_1, b_1, c_1], [a_2, b_2, c_2]$, there exists $B, C \in \mathbb{Z}$ that

$$[a_1, b_1, c_1] \sim [a_1, B, a_2 C],$$
$$[a_2, b_2, c_2] \sim [a_2, B, a_1 C].$$

United Quadratic Form

Proof.

Consider $\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}[a,b,c] \sim \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \alpha a + \frac{b}{2} \\ \alpha a + \frac{b}{2} & \alpha^2 a + b\alpha + c \end{pmatrix} \sim [a, 2\alpha a + b, \alpha^2 a + b\alpha + c]$. We first solve for possible $B \in \mathbb{Z}$.

$$\begin{aligned}
& \exists \alpha_i, B, 2\alpha_i a_i + b_i = B, \text{ for } i = 1 \text{ or } 2 \\
\iff & \exists B, b_i = B \mod 2a_i, \text{ for } i = 1 \text{ or } 2 \\
\iff & \exists \alpha, 2\alpha a_1 + b_1 = b_2 \mod 2a_2 \\
\iff & \exists \alpha, \alpha a_1 = \frac{b_2 - b_1}{2} \mod a_2 \\
\iff & d := \gcd(a_1, a_2) | \frac{b_2 - b_1}{2}.
\end{aligned}$$

United Quadratic Form

Proof.

Since we have,

$$\begin{aligned}
&\Delta = b_i^2 - 4a_ic_i, \text{ for } i = 1 \text{ or } 2 \\
\Rightarrow &(b_2 - b_1)(b_2 + b_1) = b_2^2 - b_1^2 = 4(a_2c_2 - a_1c_1) = 0 \mod d \\
\Rightarrow &\gcd\left(d, \frac{b_2 + b_1}{2}\right) = 1, \text{ thus } d | \frac{b_2 - b_1}{2}, \text{ by the united condition.} \\
\Rightarrow &\exists \alpha, B, 2\alpha a_i + b_i = B, \text{ for } i = 1 \text{ or } 2, \text{ by above.}
\end{aligned}$$

Let α, B, t be a (varying) instantiate of above and $B_0 \in \mathbb{N}$ be the unique one $< \ell := \mathrm{lcm}(2a_1, 2a_2) = \frac{2a_1a_2}{d}$ that

$$B = B_0 + t\ell.$$

United Quadratic Form

Proof.

Define C_i satisfying $\begin{pmatrix} 1 & 0 \\ \alpha_i & 1 \end{pmatrix} [a_i, b_i, c_i] = [a_i, B, a_{\bar{i}} C_i]$, since $B^2 - 4a_1 a_2 C_i = \Delta$ for any i, we actually have $C_1 = C_2$, in another word, $C := C_i = \frac{B^2 - \Delta}{4a_1 a_2}$. Therefore it suffices to find B such that C is integer, or equivalently, $B^2 = \Delta \mod 4a_1 a_2$. Recall that we already have

$$\begin{aligned} B &= b_i \mod 2a_i & \Rightarrow B = b_i \mod 2 \text{ thus } 2 | B \pm b_i \\ \Rightarrow B^2 &= b_i^2 \mod 4a_i & \Rightarrow B^2 = b_i^2 \mod 2\ell. \end{aligned}$$

Then we have,

$$\begin{aligned} & B^2 = \Delta \mod 4a_1 a_2 \\ \Longleftrightarrow\ & \Delta - B_0^2 - 2t\ell B_0 = \Delta - B_0^2 - 2t\ell B_0 - t^2\ell^2 = 0 \mod 4a_1 a_2 (= 2d\ell) \\ \Longleftrightarrow\ & \frac{\Delta - B_0^2}{2\ell} = tB_0 \mod d \end{aligned}$$

United Quadratic Form

Proof.

Finally, since,

$$\gcd(B_0, d) = \gcd(B, d) = \gcd(d, b_1) = \gcd(d, \frac{b_1 + b_2}{2}) = 1,$$

we have

$$t = \frac{\Delta - B_0^2}{2\ell} \cdot B_0^{-1} \mod d,$$

as a feasible solution.

$\square$

Form Representation

Proposition

Given any binary form f we have the equivalence,

$$\{f(x,y) : \gcd(x,y) = 1\} = \{a \in \mathbb{Z} : \exists b, c, [a,b,c] \sim f\}.$$

Proof.

Given primitive representation $a = f(x,y)$ *with* $f \sim \begin{pmatrix} a_0 & b_0 \\ b_0 & c_0 \end{pmatrix}$.

Pick $\alpha = \begin{pmatrix} x & * \\ y & * \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ *so that* $\begin{pmatrix} x \\ y \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, *then*

$$a = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a_0 & b_0 \\ b_0 & c_0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix} \alpha^T \begin{pmatrix} a_0 & b_0 \\ b_0 & c_0 \end{pmatrix} \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Therefore

$$\alpha^T \begin{pmatrix} a_0 & b_0 \\ b_0 & c_0 \end{pmatrix} \alpha = \begin{pmatrix} a & * \\ * & * \end{pmatrix} \sim [a, *, *].$$

Form Representation

Proof.

Conversely, when given $\alpha^T[a, b, c] = f$ for $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, suppose

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \alpha \begin{pmatrix} x \\ y \end{pmatrix},$$

where $\gcd(x, y) = 1$, then we have

$$a = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} \alpha^T \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \alpha \begin{pmatrix} x \\ y \end{pmatrix}.$$

Therefore f primitively generates a. $\square$

Form Representation

Proposition

Given any primitive form f and $M \in \mathbb{Z} - \{0\}$, then f primitively represents some integer that is co-prime to M.

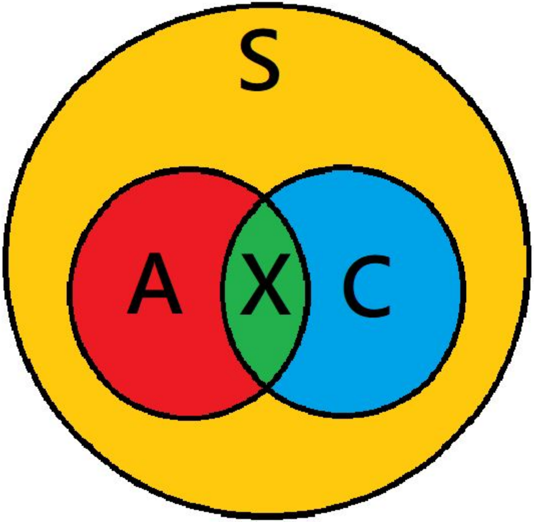
Proof.

Suppose $f = [a, b, c]$, $P_n := \{q \text{ prime}, q|n\}$ be the collection of prime factors of n and $\Pi_\Omega := \prod_{n\in\Omega} n$ be the product of elements in Ω. First we partition,

$$
\begin{aligned}
P_M &= A \sqcup C \sqcup X \sqcup S, \\
A &= (P_a - P_c) \cap P_M, \\
C &= (P_c - P_a) \cap P_M, \\
X &= (P_a \cap P_c) \cap P_M, \\
S &= P_M - A - C - X.
\end{aligned}
$$

We claim that $f(\Pi_A, \Pi_{C\sqcup S})$ is co-prime with M.

Form Representation



Form Representation

Proof.

Note that $f(\Pi, \Pi_{C \sqcup S}) = a\Pi_A^2 + b\Pi_A\Pi_{C \sqcup S} + c\Pi_{C \sqcup S}^2$. First of all,

$$p \in A \Rightarrow f(\Pi_A, \Pi_{C \sqcup S}) = c\Pi_{C \sqcup S}^2 \neq 0 \mod p,$$
$$p \in C \sqcup S \Rightarrow f(\Pi_A, \Pi_{C \sqcup S}) = a\Pi_A^2 \neq 0 \mod p.$$

For $p \in X$, since $p|a, c$ we have $f(\Pi_A, \Pi_{C \sqcup S}) = b\Pi_A\Pi_{C \sqcup S} \mod p$. Since A, C, S, X are disjoint, Π_A and $\Pi_{C \sqcup S}$ are not divisible by p. Also since $[a, b, c]$ is primitive, we have $p \nmid b$ and $b\Pi_A\Pi_{C \sqcup S} \neq 0 \mod p$. This concludes the proof. □

Corollary

Given a form $[a, b, c]$ and arbitrary $M \in \mathbb{Z} - \{0\}$ then there exists $[a', b', c'] \sim [a, b, c]$ that $\gcd(a', M) = 1$.

Form Composition

Definition

Given two united forms $f_1 = [a_1, b_1, c_1], f_2 = [a_2, b_2, c_2]$, write

$$[a_1, b_1, c_1] \sim [a_1, B, a_2 C]$$
$$[a_2, b_2, c_2] \sim [a_2, B, a_1 C]$$

for some $B, C \in \mathbb{Z}$, Then we define

$$f_1 \circ f_2 := [a_1 a_2, B, C]$$

We'll show that the class of all quadratic forms of a fixed discriminant with this composition form an abelian group.

Well-definedness

One of the non-trivial results is the well-definedness of the composition $\circ$. That is,

Proposition

If f_1 and f_2 are united and f_3 and f_4 are united for which $f_1 \sim f_3$ and $f_2 \sim f_4$, then

$$f_1 \circ f_2 \sim f_3 \circ f_4.$$

Well-definedness

One of the non-trivial results is the well-definedness of the composition $\circ$. That is,

Proposition

If f_1 and f_2 are united and f_3 and f_4 are united for which $f_1 \sim f_3$ and $f_2 \sim f_4$, then

$$f_1 \circ f_2 \sim f_3 \circ f_4.$$

To show that, we need the following lemma:

Lemma

Two forms $[a_1, b_1, c_1]$ and $[a_2, b_2, c_2]$ of the same discriminant are equivalent if and only if there exists integers α and γ can be found such that

$$\begin{cases} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 & = a_2 \\ 2a_1\alpha + (b_1 + b_2)\gamma & \equiv 0 \mod 2a_2 \\ (b_1 - b_2)\alpha + 2c_1\gamma & \equiv 0 \mod 2a_2 \end{cases}$$

Proof of Lemma

$$\text{Claim: }\begin{cases} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 & = a_2 \\ 2a_1\alpha + (b_1+b_2)\gamma & \equiv 0 \mod 2a_2 \\ (b_1-b_2)\alpha + 2c_1\gamma & \equiv 0 \mod 2a_2 \end{cases}$$

Proof.

Since $[a_1, b_1, c_1] \sim [a_2, b_2, c_2]$, there exists $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a_1 & \frac{b_1}{2} \\ \frac{b_1}{2} & c_1 \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}^t = \begin{pmatrix} a_2 & \frac{b_2}{2} \\ \frac{b_2}{2} & c_2 \end{pmatrix}$$

Thus we have the equations

$$\begin{cases} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 & = a_2 \\ \alpha\delta - \gamma\beta & = 1 \\ (b_1\alpha + 2c_1\gamma)\delta + (b_1\gamma + 2a_1\alpha)\beta & = b_2 \end{cases}$$

Proof of Lemma

$$\text{Claim: }\begin{cases} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 & = a_2 \\ 2a_1\alpha + (b_1 + b_2)\gamma & \equiv 0 \mod 2a_2 \\ (b_1 - b_2)\alpha + 2c_1\gamma & \equiv 0 \mod 2a_2 \end{cases}$$

Proof.

We can solve δ and β from the last two equations:

$$\begin{cases} 2a_1\alpha + (b_1 + b_2)\gamma = 2a_2\delta \\ (b_1 - b_2)\alpha + 2c_1\gamma = -2a_2\beta \end{cases}$$

This gives us the desired relation.

The opposite direction is simply reversal of the process above. $\square$

Well-definedness

Now we can prove the following proposition:

Proposition

If f_1 and f_2 are united and f_3 and f_4 are united for which $f_1 \sim f_3$ and $f_2 \sim f_4$, then

$$f_1 \circ f_2 \sim f_3 \circ f_4.$$

Proof.

We may assume

$$\begin{aligned} f_1 &= [a_1, B, a_2 C], & f_2 &= [a_2, B, a_1 C], \\ f_3 &= [m_1, N, m_2 L], & f_4 &= [m_2, N, m_1 L] \end{aligned}$$

Then

$$\begin{aligned} f_1 \circ f_2 &= [a_1 a_2, B, C] \\ f_3 \circ f_4 &= [m_1 m_2, N, L] \end{aligned}$$

Well-definedness

Proof (Cont.)

From the previous lemma, there exists x_1, x_2, y_1, y_2 so that

$$\begin{cases} a_1 x_1^2 + B x_1 y_1 + a_2 C y_1^2 & = m_1 \\ 2a_1 x_1 + (B+N) y_1 & \equiv 0 \mod 2m_1 \\ (B-N) x_1 + 2a_2 C y_1 & \equiv 0 \mod 2m_1 \end{cases}$$

and

$$\begin{cases} a_2 x_2^2 + B x_2 y_2 + a_1 C y_2^2 & = m_2 \\ 2a_2 x_2 + (B+N) y_2 & \equiv 0 \mod 2m_2 \\ (B-N) x_2 + 2a_1 C y_2 & \equiv 0 \mod 2m_2 \end{cases}$$

Well-definedness

Proof (Cont.)

From the previous lemma, there exists x_1, x_2, y_1, y_2 so that

$$\begin{cases} a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2 & = m_1 \\ 2a_1x_1 + (B+N)y_1 & \equiv 0 \mod 2m_1 \\ (B-N)x_1 + 2a_2Cy_1 & \equiv 0 \mod 2m_1 \end{cases}$$

and

$$\begin{cases} a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2 & = m_2 \\ 2a_2x_2 + (B+N)y_2 & \equiv 0 \mod 2m_2 \\ (B-N)x_2 + 2a_1Cy_2 & \equiv 0 \mod 2m_2 \end{cases}$$

It suffices to find integers X and Y such that

$$\begin{cases} a_1a_2X^2 + BXY + CY^2 & = m_1m_2 & (1) \\ 2a_1a_2X + (B+N)Y & \equiv 0 \mod 2m_1m_2 & (2) \\ (B-N)X + 2CY & \equiv 0 \mod 2m_1m_2 & (3) \end{cases}$$

Well-definedness

Proof (Cont.)

Let

$$\begin{cases} X & = x_1 x_2 - C y_1 y_2 \\ Y & = a_1 x_1 y_2 + a_2 y_1 x_2 + B y_1 y_2 \end{cases}.$$

Then (1) can be proved by pure computation:

Well-definedness

Proof (Cont.)

Let

$$\begin{cases} X &= x_1x_2 - Cy_1y_2 \\ Y &= a_1x_1y_2 + a_2y_1x_2 + By_1y_2 \end{cases}.$$

Then (1) can be proved by pure computation:

$$\begin{aligned} m_1m_2 &= (a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2)(a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2) \\ &= a_1a_2x_1^2x_2^2 + a_1Bx_1^2x_2y_2 + a_1^2Cx_1^2y_2^2 + Ba_2x_1x_2^2y_1 + B^2x_1x_2y_1y_2 \\ &\quad + a_1BCx_1y_1y_2^2 + a_2^2Cx_2^2y_1^2 + a_2BCx_2y_1^2y_2 + a_1a_2C^2y_1^2y_2^2 \end{aligned}$$

$$\begin{cases} a_1a_2X^2 &= a_1a_2x_1^2x_2^2 - 2a_1a_2Cx_1x_2y_1y_2 + a_1a_2C^2y_1^2y_2^2 \\ BXY &= -a_1BCx_1y_1y_2^2 - a_2BCx_2y_1^2y_2 + Ba_2x_1x_2^2y_1 \\ &\quad + a_1Bx_1^2x_2y_2 - B^2Cy_1^2y_2^2 + B^2x_1x_2y_1y_2 \\ cY^2 &= 2a_2BCx_2y_1^2y_2 + 2a_1BCx_1y_1y_2^2 + a_2^2Cx_2^2y_1^2 \\ &\quad + 2a_1a_2Cx_1x_2y_1y_2 + a_1^2Cx_1^2y_2^2 + B^2Cy_1^2y_2^2 \end{cases}$$

Well-definedness

Proof (Cont.)

For equation (2), we use $N^2 - 4m_1m_2L = B^2 - 4a_1a_2C$, and get

$$
\begin{aligned}
&(a_1x_1 + \frac{B+N}{2}y_1)(a_2x_2 + \frac{B+N}{2}y_2) \\
=&a_1a_2x_1x_2 + \frac{B+N}{2}a_1x_1y_2 + \frac{B+N}{2}a_2y_1x_2 + \frac{B^2+2BN+N^2}{4}y_1y_2 \\
\equiv&a_1a_2(x_1x_2 - Cy_1y_2) + \frac{B+N}{2}(a_1x_1y_2 + a_2y_1x_2 + By_1y_2) \mod m_1m_2 \\
\equiv&a_1a_2X + \frac{B+N}{2}Y \mod m_1m_2
\end{aligned}
$$

Hence

$$2a_1a_2X + (B+N)Y \equiv 0 \mod 2m_1m_2$$

Well-definedness

Proof (Cont.)

The last equation (3) can also be proved by computation. Let

$$U = (B - N)X/2 + CY,$$

then under modulo $m_1 m_2$, we get

$$\begin{aligned}
0 &\equiv [(B-N)x_1/2 + a_2 C y_1][a_2 x_2 + (B+N)y_2/2] \equiv a_2 U \\
0 &\equiv [a_1 x_2 + (B+N)y_1/2][(B-N)x_2/2 + a_1 C y_2] \equiv a_1 U \\
0 &\equiv [(B-N)x_1/2 + a_2 C y_1][(B-N)x_2/2 + a_1 C y_2] \equiv (B-N)U/2 \\
0 &\equiv C[a_1 x_2 + (B+N)y_1/2][a_2 x_2 + (B+N)y_2/2] \equiv (B+N)U/2
\end{aligned}$$

Since we assume the forms are united, $\gcd(a_1, a_2, B) = 1$. Thus

$$U \equiv 0 \mod m_1 m_2$$

as desired. □

Abelian Group

Now we've shown that $\circ$ is a well-defined binary operator on the forms of a fixed discriminant. In fact, the composition $\circ$ gives us a group structure! Specifically, we have the following theorem.

Abelian Group

Now we've shown that $\circ$ is a well-defined binary operator on the forms of a fixed discriminant. In fact, the composition $\circ$ gives us a group structure! Specifically, we have the following theorem.

Theorem

Under composition, the classes of forms of a fixed discriminant form an abelian group.

Abelian Group

Now we've shown that $\circ$ is a well-defined binary operator on the forms of a fixed discriminant. In fact, the composition $\circ$ gives us a group structure! Specifically, we have the following theorem.

Theorem

Under composition, the classes of forms of a fixed discriminant form an abelian group.

Proof.

It's easy to see that $\circ$ is commutative and associative. Further, for any forms $(1, b_1, c_1)$ and (a_2, b_2, c_2) we have

$$(1, b_1, c_1) \circ (a_2, b_2, c_2) \sim (1, b_2, a_2 c_2) \circ (a_2, b_2, c_2) \sim (a_2, b_2, c_2).$$

Abelian Group

Now we've shown that $\circ$ is a well-defined binary operator on the forms of a fixed discriminant. In fact, the composition $\circ$ gives us a group structure! Specifically, we have the following theorem.

Theorem

Under composition, the classes of forms of a fixed discriminant form an abelian group.

Proof.

It's easy to see that $\circ$ is commutative and associative. Further, for any forms $(1, b_1, c_1)$ and (a_2, b_2, c_2) we have

$$(1, b_1, c_1) \circ (a_2, b_2, c_2) \sim (1, b_2, a_2 c_2) \circ (a_2, b_2, c_2) \sim (a_2, b_2, c_2).$$

Finally, we note that for any form (a, b, c) we have

$$(a, b, c) \circ (a, -b, c) \sim (a, b, c) \circ (c, b, a) \sim (ac, b, 1) \sim (1, -b, ac).$$

$\square$

Some Definitions

Let

$$
\begin{aligned}
d \neq 1 &\text{ be a square-free integer} \\
\mathcal{O}_d &= \mathbb{Z}^{int}(\mathbb{Q}(\sqrt{d})) \\
\Delta_d = \Delta(\mathcal{O}_d) &= \begin{cases} d & \text{, if } d \equiv 1 \mod 4 \\ 4d & \text{, if } d \equiv 2, 3 \mod 4 \end{cases}
\end{aligned}
$$

For $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, let

$$
\begin{aligned}
\bar{\alpha} &= a - b\sqrt{d} \\
N(\alpha) = N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) &= \alpha\bar{\alpha} = a^2 - db^2
\end{aligned}
$$

Main Theorem

Let $\mathcal{B}^+_{\Delta_d} = \begin{cases} \mathcal{B}_{\Delta_d} & \text{, if } \Delta_d > 0 \\ \{[a,b,c] \in \mathcal{B}_{\Delta_d} | a > 0\} & \text{, if } \Delta_d < 0 \end{cases}$

$\Rightarrow \mathcal{B}^+_{\Delta_d}/\sim = \begin{cases} \mathcal{B}_{\Delta_d}/\sim & \text{, if } \Delta_d > 0 \\ \text{a subgroup of } \mathcal{B}_{\Delta_d}/\sim \text{ of index } 2 & \text{, if } \Delta_d < 0 \end{cases}$

Let $Cl^+_d = \mathcal{I}(\mathcal{O}_d)/\mathcal{P}^+(\mathcal{O}_d)$, (narrow class group)

where $\mathcal{P}^+(\mathcal{O}_d) = \{(\alpha) | \alpha \in \mathbb{Q}(\sqrt{d}) \text{ with } N(\alpha) > 0\}$

If $\mathtt{I}, \mathtt{J}$ in same class of Cl^+_d, we denote $\mathtt{I} \overset{+}{\sim} \mathtt{J}$

Theorem

$Cl^+_d \simeq \mathcal{B}^+_{\Delta_d}/\sim$

Some Facts

- Suppose K is a number field and $K/\mathbb{Q}$ is galois then for p is prime in $\mathbb{Z}$, we have $(p) = p\mathcal{O}_K = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$

  $$\Rightarrow \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma(\mathfrak{P}_1) = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{ef} = (p)^f = (p^f) = (\|\mathfrak{P}_1\|)$$

  $$\Rightarrow \prod_{\sigma \in Gal(K/\mathbb{Q})} \sigma(\mathtt{I}) = (\|\mathtt{I}\|), \text{ for integral ideal } \mathtt{I} \neq (0) \text{ of } \mathcal{O}_K$$

- Suppose K is a number field, define the content $\mathcal{C}_f$ of a polynomial $f \in \mathcal{O}_K[x_1, \cdots, x_m]$ to be the ideal which generated by coefficients of f. Then

  $$\mathcal{C}_{fg} = \mathcal{C}_f \mathcal{C}_g, \text{ for all } f, g \in \mathcal{O}_K[x_1, \cdots, x_m]$$

- $SL_2(\mathbb{Z}) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle$

from Cl_d^+ to $\mathcal{B}_{\Delta_d}^+/\sim$

For non-zero integral ideal $\mathtt{I}$ of $\mathcal{O}_d$ with integral basis $\{\alpha_1, \alpha_2\}$,
we know $\alpha_1\bar{\alpha_2} - \alpha_2\bar{\alpha_1} = \pm\|\mathtt{I}\|\sqrt{\Delta_d}$,
we choose to order the basis so that $\alpha_1\bar{\alpha_2} - \alpha_2\bar{\alpha_1} = \|\mathtt{I}\|\sqrt{\Delta_d}$
now let

$$\begin{aligned} f_{\alpha_1,\alpha_2} &= \frac{1}{\|\mathtt{I}\|}[\alpha_1 x + \alpha_2 y][\bar{\alpha_1}x + \bar{\alpha_2}y] \\ &= \frac{\alpha_1\bar{\alpha_1}}{\|\mathtt{I}\|}x^2 + \frac{\alpha_1\bar{\alpha_2} + \alpha_2\bar{\alpha_1}}{\|\mathtt{I}\|}xy + \frac{\alpha_2\bar{\alpha_2}}{\|\mathtt{I}\|}y^2 \end{aligned}$$

Note that $\alpha_1\bar{\alpha_1}, \alpha_1\bar{\alpha_2} + \alpha_2\bar{\alpha_1}, \alpha_2\bar{\alpha_2} \in \mathbb{Z}$

Since $(\alpha_1\bar{\alpha_1}, \alpha_1\bar{\alpha_2} + \alpha_2\bar{\alpha_1}, \alpha_2\bar{\alpha_2}) = (\alpha_1, \alpha_2)(\bar{\alpha_1}, \bar{\alpha_2}) = (\|\mathtt{I}\|)$

$\Rightarrow \frac{\alpha_1\bar{\alpha_1}}{\|\mathtt{I}\|}, \frac{\alpha_1\bar{\alpha_2}+\alpha_2\bar{\alpha_1}}{\|\mathtt{I}\|}, \frac{\alpha_2\bar{\alpha_2}}{\|\mathtt{I}\|} \in \mathbb{Z}$ and $(\frac{\alpha_1\bar{\alpha_1}}{\|\mathtt{I}\|}, \frac{\alpha_1\bar{\alpha_2}+\alpha_2\bar{\alpha_1}}{\|\mathtt{I}\|}, \frac{\alpha_2\bar{\alpha_2}}{\|\mathtt{I}\|}) = (1)$

Since $[\frac{\alpha_1\bar{\alpha_2}+\alpha_2\bar{\alpha_1}}{\|\mathtt{I}\|}]^2 - 4\frac{\alpha_1\bar{\alpha_1}}{\|\mathtt{I}\|}\frac{\alpha_2\bar{\alpha_2}}{\|\mathtt{I}\|} = [\frac{\alpha_1\bar{\alpha_2}-\alpha_2\bar{\alpha_1}}{\|\mathtt{I}\|}]^2 = \Delta_d$

hence $f_{\alpha_1,\alpha_2} \in \mathcal{B}_{\Delta_d}^+$

from Cl_d^+ to $\mathcal{B}^+_{\Delta_d}/\sim$

Now if $(\alpha_1, \alpha_2) = \lambda \mathtt{I}'$ for some $\lambda \in \mathbb{Q}(\sqrt{d})$ with $N(\lambda) > 0$ and integral ideal $\mathtt{I}'$, write $\mathtt{I}' = (\beta_1, \beta_2)$ with $\beta_1\bar\beta_2 - \beta_2\bar\beta_1 = \|\mathtt{I}\|\sqrt{\Delta_d}$

$$\Rightarrow \exists \gamma \in GL_2(\mathbb{Z}) \text{ s.t. } \begin{pmatrix} \lambda\beta_1 \\ \lambda\beta_2 \end{pmatrix} = \gamma \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} \lambda\beta_1 & \bar\lambda\bar\beta_1 \\ \lambda\beta_2 & \bar\lambda\bar\beta_2 \end{pmatrix} = \gamma \begin{pmatrix} \alpha_1 & \bar\alpha_1 \\ \alpha_1 & \bar\alpha_1 \end{pmatrix}$$

$$\Rightarrow N(\lambda)[\beta_1\bar\beta_2 - \beta_2\bar\beta_1] = \det(\gamma)[\alpha_1\bar\alpha_2 - \alpha_2\bar\alpha_1]$$

$$\Rightarrow \gamma \in SL_2(\mathbb{Z}) \text{ and } N(\lambda)\|\mathtt{I}'\| = \|\mathtt{I}\|$$

Write $f_{\beta_1,\beta_2} = \frac{1}{\|\mathtt{I}'\|}\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} \begin{pmatrix} \bar\beta_1 & \bar\beta_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

$$= \frac{1}{\|\mathtt{I}'\| N(\lambda)} \begin{pmatrix} x & y \end{pmatrix} \gamma \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \begin{pmatrix} \bar\alpha_1 & \bar\alpha_2 \end{pmatrix} \gamma^T \begin{pmatrix} x \\ y \end{pmatrix}$$

$= \gamma f_{\alpha_1,\alpha_2}$, hence $f_{\alpha_1,\alpha_2} \sim f_{\beta_1,\beta_2}$

from $\mathcal{B}^+_{\Delta_d}/\sim$ to Cl^+_d

For $f = [a, b, c] \in \mathcal{B}^+_{\Delta_d}$, let

$$\mathtt{I}_f = t_f(a, \frac{b - \sqrt{\Delta_d}}{2}), \text{ where } t_f = \begin{cases} 1 & \text{, if } a > 0 \\ \sqrt{\Delta_d} & \text{, if } a < 0 \end{cases}$$

Note that if $d \equiv 1 \mod 4$ then $\Delta_d = d$ and b is odd, and if $d \equiv 2, 3 \mod 4$ then $\Delta_d = 4d$ and b is even

$\Rightarrow \mathtt{I}_f$ is an integral ideal of $\mathcal{O}_d$

Since
$[ax + \frac{b-\sqrt{\Delta_d}}{2}y][ax + \frac{b+\sqrt{\Delta_d}}{2}y] = a^2x^2 + abxy + \frac{b^2-\Delta_d}{4}y^2 = af$

$\Rightarrow (\left\|(a, \frac{b-\sqrt{\Delta_d}}{2})\right\|) = (a)$, and so $\left\|(a, \frac{b-\sqrt{\Delta_d}}{2})\right\| = |a|$

$\Rightarrow N(t_f)[a\frac{b+\sqrt{\Delta_d}}{2} - a\frac{b-\sqrt{\Delta_d}}{2}] = N(t_f)a\sqrt{\Delta_d}$

$$= |N(t_f)| \left\|(a, \frac{b-\sqrt{\Delta_d}}{2})\right\| \sqrt{\Delta_d} = \|\mathtt{I}_f\| \sqrt{\Delta_d}$$

Thus, $\{t_f a, t_f\frac{b-\sqrt{\Delta_d}}{2}\}$ is an integral basis of $\mathtt{I}_f$

from $\mathcal{B}^+_{\Delta_d}/\sim$ to Cl^+_d

If $f' = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} f = [a+b+c, b+2c, c]$

then $\mathtt{I}_{f'} = t_{f'}(a+b+c, \frac{b+2c-\sqrt{\Delta_d}}{2})$

Note that $\begin{pmatrix} a+b+c \\ \frac{b+2c-\sqrt{\Delta_d}}{2} \end{pmatrix} = \frac{1}{a}[a+\frac{b+\sqrt{\Delta_d}}{2}] \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ \frac{b-\sqrt{\Delta_d}}{2} \end{pmatrix}$

Let $\lambda = \frac{1}{a}[a+\frac{b+\sqrt{\Delta_d}}{2}]\frac{t_{f'}}{t_f}$, we have $N(\lambda) = \frac{[a+b+c]N(t_{f'})}{aN(t_f)} > 0$

Since $\mathtt{I}_{f'} = \lambda \mathtt{I}_f$

$\Rightarrow \mathtt{I}_{f'} \overset{+}{\sim} \mathtt{I}_f$

from $\mathcal{B}^+_{\Delta_d}/\sim$ to Cl^+_d

Now if $f' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} f = [c, -b, a]$

then $\mathtt{I}_{f'} = t_{f'}(c, \frac{-b-\sqrt{\Delta_d}}{2})$

Note that $\begin{pmatrix} c \\ \frac{-b-\sqrt{\Delta_d}}{2} \end{pmatrix} = \frac{1}{a}[\frac{b+\sqrt{\Delta_d}}{2}] \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a \\ \frac{b-\sqrt{\Delta_d}}{2} \end{pmatrix}$

Let $\lambda = \frac{1}{a}[\frac{b+\sqrt{\Delta_d}}{2}]\frac{t_{f'}}{t_f}$, we have $N(\lambda) = \frac{cN(t_{f'})}{aN(t_f)} > 0$

Since $\mathtt{I}_{f'} = \lambda \mathtt{I}_f$

$\Rightarrow \mathtt{I}_{f'} \overset{+}{\sim} \mathtt{I}_f$

Thus, for all $f, f' \in \mathcal{B}^+_{\Delta_d}$, $f \sim f'$ implies $\mathtt{I}_f \overset{+}{\sim} \mathtt{I}_{f'}$

Check Bijective

Given $g = [a, b, c] \in \mathcal{B}^+_{\Delta_d}$

$\Rightarrow \mathtt{I}_g = t_g(a, \frac{b-\sqrt{\Delta_d}}{2})$

$\Rightarrow f_{t_g a, t_g \frac{b-\sqrt{\Delta_d}}{2}} = \frac{N(t_g)}{\|\mathtt{I}_g\|}[ax + \frac{b-\sqrt{\Delta_d}}{2}y][ax + \frac{b+\sqrt{\Delta_d}}{2}]$

$= \frac{N(t_g)}{|N(t_g)|} \frac{a}{\left\|(a, \frac{b-\sqrt{\Delta_d}}{2})\right\|} g = \frac{N(t_g)}{|N(t_g)|} \frac{a}{|a|} g = g$

Given $\mathsf{J} = (\alpha_1, \alpha_2)$, where $\alpha_1\bar{\alpha_2} - \alpha_2\bar{\alpha_1} = \|\mathsf{J}\| \sqrt{\Delta_d}$

$\Rightarrow f_{\alpha_1,\alpha_2} = \frac{\alpha_1\bar{\alpha_1}}{\|\mathsf{J}\|}x^2 + \frac{\alpha_1\bar{\alpha_2}+\alpha_2\bar{\alpha_1}}{\|\mathsf{J}\|}xy + \frac{\alpha_2\bar{\alpha_2}}{\|\mathsf{J}\|}y^2$

$\Rightarrow \mathtt{I}_{f_{\alpha_1,\alpha_2}} = t_{f_{\alpha_1,\alpha_2}}(\frac{\alpha_1\bar{\alpha_1}}{\|\mathsf{J}\|}, \frac{\alpha_1\bar{\alpha_2}+\alpha_2\bar{\alpha_1}-\|\mathsf{J}\|\sqrt{\Delta_d}}{2\|\mathsf{J}\|}) = \frac{\bar{\alpha_1} t_{f_{\alpha_1,\alpha_2}}}{\|\mathsf{J}\|}(\alpha_1, \alpha_2)$

$\Rightarrow \mathtt{I}_{f_{\alpha_1,\alpha_2}} \overset{+}{\sim} \mathsf{J}$

Check Isomorphic

Given $f_1 = [a_1, B, a_2 C], f_2 = [a_2, B, a_1 C] \in \mathcal{B}^+_{\Delta_d}$

$\Rightarrow \mathtt{I}_{f_1} = t_{f_1}(a_1, \frac{B-\sqrt{\Delta_d}}{2}), \mathtt{I}_{f_2} = t_{f_2}(a_2, \frac{B-\sqrt{\Delta_d}}{2})$

Note that $(a_1, \frac{B-\sqrt{\Delta_d}}{2})(a_2, \frac{B-\sqrt{\Delta_d}}{2})$

$$= (a_1 a_2) + \frac{B-\sqrt{\Delta_d}}{2}(a_1) + \frac{B-\sqrt{\Delta_d}}{2}(a_2) + (B\frac{B-\sqrt{\Delta_d}}{2} - a_1 a_2 C)$$

$$= (a_1 a_2) + \frac{B-\sqrt{\Delta_d}}{2}(a_1) + \frac{B-\sqrt{\Delta_d}}{2}(a_2) + \frac{B-\sqrt{\Delta_d}}{2}(B)$$

$$= (a_1 a_2, \frac{B-\sqrt{\Delta_d}}{2})$$

Therefore $\mathtt{I}_{f_1}\mathtt{I}_{f_2} = t_{f_1} t_{f_2}(a_1 a_2, \frac{B-\sqrt{\Delta_d}}{2}) = \frac{t_{f_1 \circ f_2}}{t_{f_1} t_{f_2}} \mathtt{I}_{f_1 \circ f_2}$

Since $\frac{t_{f_1 \circ f_2}}{t_{f_1} t_{f_2}} = \begin{cases} \frac{1}{\Delta_d} & \text{, if } a_1 < 0 \text{ and } a_2 < 0 \\ 1 & \text{, otherwise} \end{cases}$

$\Rightarrow \mathtt{I}_{f_1 \circ f_2} \overset{+}{\sim} \mathtt{I}_{f_1}\mathtt{I}_{f_2}$

Thus, $Cl^+_d \simeq \mathcal{B}^+_{\Delta_d} / \sim$

References

- Duncan A. Buell, *Binary Quadratic Forms*, Springer-Verlag, 1989
- Erich Hecke, *Lectures on the Theorem of Algebraic Number*, Springer, 1981