Gauss Composition

Pan Jing Bin

Binary Quadratic Forms

We want to study the $SL_2(\mathbb{Z})$-equivalence classes of integer binary quadratic forms

$$ax^2 + bxy + cy^2.$$

The binary quadratic form is **primitive** if $\gcd(a, b, c) = 1$.

Form Class Group

If f and g are two primitive binary quadratic forms of a given discriminant D, then there exist $A, A', B, C \in \mathbb{Z}$ such that

$$f \sim [A, B, CA'] \text{ and } g \sim [A', B, CA].$$

We define the **composition** of f and g to be the $SL_2(\mathbb{Z})$-equivalence class containing the form $[AA', B, C]$.

This is the **form class group** of discriminant D.

Quadratic Rings

We also want to study **quadratic rings**, which are commutative rings with unity whose additive group is isomorphic to $\mathbb{Z}^2$.

Examples :

1. $\mathbb{Z} \times \mathbb{Z}$.
2. $\mathbb{Z}[i]$ (The Gaussian Integers).

Trace, Norm and Discriminant

If R is a quadratic ring and α is an element of R, then the map $\varphi_{\times\alpha} : R \to R$ defined by

$$\varphi_{\times\alpha}(\gamma) = \alpha \cdot \gamma$$

is R-linear.

By fixing a $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2\}$, the map $\varphi_{\times\alpha}$ can be represented by a 2×2 matrix with coefficients in $\mathbb{Z}$.

The **trace** and **norm** of α is defined to be the trace and determinant of the corresponding matrix.

Trace, Norm and Discriminant

Let $\{\alpha_1, \alpha_2\}$ be any $\mathbb{Z}$-basis of a quadratic ring R. Define the **discriminant** of R by

$$\text{disc}(R) = \det\left(\begin{pmatrix} Tr(\alpha_1\alpha_1) & Tr(\alpha_1\alpha_2) \\ Tr(\alpha_2\alpha_1) & Tr(\alpha_2\alpha_2) \end{pmatrix}\right).$$

Working definition :

Every quadratic ring R has a $\mathbb{Z}$-basis of the form $\{1_R, x\}$, where x satisfies an integer quadratic equation

$$x^2 + rx + s = 0$$

for some $r, s \in \mathbb{Z}$. Then $\text{disc}(R) = r^2 - 4s$.

Regular Basis

We can morph the $\mathbb{Z}$-basis $\{1, x\}$ into an even "nicer" basis $\{1_R, \tau\}$, where

$$\tau^2 - \frac{D}{4} = 0 \quad \text{or} \quad \tau^2 - \tau + \frac{1-D}{4} = 0$$

in accordance to whether $D \equiv 0$ or $1 \pmod 4$.

We call this a regular basis for R.

Notation : For any $\alpha_1, \alpha_2 \in R$, we let $\langle \alpha_1, \alpha_2 \rangle$ denote the subset

$$\left\{ x \cdot \alpha_1 + y \cdot \alpha_2 \mid x, y \in \mathbb{Z} \right\}.$$

Classification of Quadratic Rings

Theorem

If R and S are two quadratic rings of the same discriminant, then $R \cong S$ as rings. We let $S(D)$ denote the unique quadratic ring of discriminant D.

Concrete constructions for $S(D)$ are given by

$$S(D) = \begin{cases} \mathbb{Z}[x] \,/\, (x^2) & \text{if } D = 0 \\ \mathbb{Z} \cdot (1,1) + \sqrt{D}(\mathbb{Z} \oplus \mathbb{Z}) & \text{if } D \geq 1 \text{ is a perfect square} \\ \mathbb{Z}[(D + \sqrt{D})/2] & \text{otherwise.} \end{cases}$$

Localisation

To an quadratic ring $S(D)$, we define the localisation $K(D) = S(D) \otimes_{\mathbb{Z}} \mathbb{Q}$. If $\{\alpha_1, \alpha_2\}$ is a $\mathbb{Z}$-basis for $S(D)$, then every element in $K(D)$ is of the form

$$x \cdot \alpha_1 + y \cdot \alpha_2$$

for some $x, y \in \mathbb{Q}$.

The notion of **norm** on $S(D)$ can easily be extended to $K(D)$ as follows :

$$N^{K(D)}\left(\frac{p_1}{q} \cdot \alpha_1 + \frac{p_2}{q} \cdot \alpha_2\right) = \frac{1}{q^2} \cdot N^{S(D)}(p_1 \cdot \alpha_1 + p_2 \cdot \alpha_2).$$

Oriented Fractional Ideals

A **fractional ideal** I of $S(D)$ is a $S(D)$-submodule of $K(D)$ such that there exists $r \in S(D)$ satisfying

1. r is **invertible** in $K(D)$.
2. $rI \subseteq S(D)$.

The element r can be thought of as clearing the denominators of I, hence the name fractional ideal.

Any fractional ideal must also be a free $\mathbb{Z}$-module having rank 0, 1 or 2. Here we are only interested in studying the case of rank 2.

An **oriented fractional ideal** is a pair (I, ϵ), where I is a fractional ideal of $S(D)$ of **rank** 2 as a $\mathbb{Z}$-module and $\epsilon = \pm 1$ indicates the orientation of I.

Oriented Fractional Ideals

Multiplication of oriented fractional ideals is done component wise. If $k \in K(D)$ is an **invertible** scalar, define

$$k \cdot (I, \epsilon) = \Big(kI,\ \epsilon \cdot \operatorname{sgn}\big(N(k)\big) \Big).$$

For simplicity, we will denote (I, ϵ) simply by I and let $\operatorname{sgn}(I) = \epsilon$ denote the orientation.

Orientation of the ring

Problem : For every quadratic ring $S(D)$, there are exactly two different choices of τ for the regular basis $\{1, \tau\}$. Intuitively, this corresponds to the fact that

$$x^2 - \frac{D}{4} = 0 \text{ or } x^2 - x + \frac{1-D}{4} = 0$$

has two distinct roots.

Example : The $\mathbb{Z}$-bases $\{1, i\}$ and $\{1, -i\}$ are both regular bases for $\mathbb{Z}[i]$, the quadratic ring of discriminant -4.

We have $\langle 1, i \rangle = \langle 1, -i \rangle$ but the change-of-basis matrix is

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \notin SL_2(\mathbb{Z}).$$

This will cause problems later on when we try to relate ideals to $SL_2(\mathbb{Z})$-equivalence classes of binary quadratic forms.

Orientation

The Solution :

We first fix a choice of τ. This induces a natural projection map $S(D) \to S(D)$ given by

$$\pi(a + b\tau) = b.$$

An **oriented quadratic ring** is a pair $(S(D), \pi)$.

Example : When $S(D) = \mathbb{Z}[i]$, We may choose $\tau = i$. The projection map π then becomes

$$\pi(a + bi) = b.$$

Then $\left(\mathbb{Z}[i], \pi\right)$ is an oriented quadratic ring.

Oriented bases

A regular basis $\{1, \tau\}$ is **positively oriented** if $\pi(\tau) > 0$ and **negatively oriented** otherwise.

Example : $\{1, i\}$ is positively oriented and $\{1, -i\}$ is negatively oriented.

In general, every oriented quadratic ring has a unique positively oriented regular basis and a unique negatively oriented regular basis.

We generalise to arbitrary Z-bases as follows : The $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2\}$ for an oriented fractional ideal I is **positively oriented** if the change-of-basis matrix from the positively oriented regular basis $\{1, \tau\}$ has positive determinant.

How it solves the problem : If $\{\alpha_1, \alpha_2\}$ and $\{\beta_1, \beta_2\}$ are **similarly oriented** $\mathbb{Z}$-bases for an ideal I, then the change-of-basis matrix have determinant 1.

Remark : From this point onwards all quadratic rings $S(D)$ are assumed to be oriented.

Narrow Class Group

An oriented fractional ideal I is **invertible** if there exists an oriented fractional ideal J such that $IJ = S(D)$.

Two oriented fractional ideals I and J are **narrowly equivalent** if there exists **invertible** $k \in K(D)$ such that $I = kJ$.

For a quadratic ring $S(D)$, the set of narrow-equivalence classes of invertible oriented fractional ideals of $S(D)$ forms a group under multiplication of ideals. This is known as the **narrow class group**.

Norm of an ideal

Problem : Need a way to measure the 'size' of the ideal.

For an oriented fractional ideal I, define the **norm** of I by

$$N(I) = \mathrm{sgn}(I) \cdot \frac{|M/I|}{|M/S(D)|}$$

where M is any oriented fractional ideal in $K(D)$ containing both I and $S(D)$.

Correspondence Between Quadratic Forms and Classes of Ideals

The main theorem is divided into two parts.

Theorem (First part)

Let D be a non-zero *integer congruent to* 0 *or* 1 *modulo* 4*. There is a bijection between the set of $SL_2(\mathbb{Z})$-equivalence classes of binary quadratic forms of discriminant D and the set of narrow-equivalence classes of oriented fractional ideals of $S(D)$.*

Correspondence Between Quadratic Forms and Classes of Ideals

Let I be an oriented fractional ideal. Let $\{\alpha_1, \alpha_2\}$ be a $\mathbb{Z}$-basis for I, where the orientation of $\{\alpha_1, \alpha_2\}$ follows the orientation of I. In this bijection, we associate I with the binary quadratic form

$$\frac{N(\alpha_1 x + \alpha_2 y)}{N(I)}$$

where x and y are integer variables.

This can be written as

$$\frac{N(\alpha_1)x^2 + \left[N(\alpha_1 + \alpha_2) - N(\alpha_1) - N(\alpha_2)\right]xy + N(\alpha_2)y^2}{N(I)}.$$

Correspondence Between Quadratic Forms and Classes of Ideals

To a binary quadratic form $f = [A, B, C]$, we associate f to the oriented fractional ideal

$$\left(\langle A, b_B + \tau \rangle, \ \mathrm{sgn}(A) \right),$$

where $\{1, \tau\}$ is the positively oriented regular basis for $S(D)$ and

$$b_B = \begin{cases} B/2 & \text{if } D \equiv 0 \pmod 4 \\ (B-1)/2 & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Remark : The value of C is usually completely determined by the formula $B^2 - 4AC = D$.

When D is a perfect square, then we may have $A = 0$. Those cases need to be handled separately.

Correspondence Between Quadratic Forms and Classes of Ideals

Alternatively, some authors adopt the following bijection instead :

$$\langle \alpha_1, \alpha_2 \rangle \mapsto \frac{N(\alpha_1 x - \alpha_2 y)}{N(I)}$$

and

$$[A, B, C] \mapsto \left(\left\langle A, b_{-B} + \tau \right\rangle, \ \mathrm{sgn}(A) \right).$$

Isomorphism Between Form Class Group and Narrow Class Group

We now focus on primitive binary quadratic forms and invertible oriented fractional ideals.

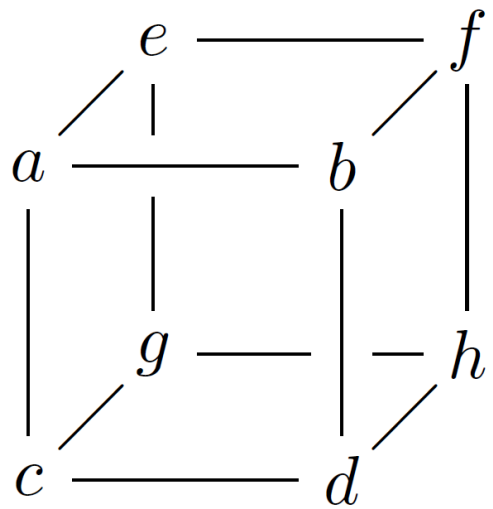
Theorem (Second part)

Under this bijection, primitive binary quadratic forms get mapped to invertible oriented fractional ideals and vice versa. Furthermore, the bijection restricts to a group isomorphism between the form class group of discriminant D and the narrow class group of $S(D)$.

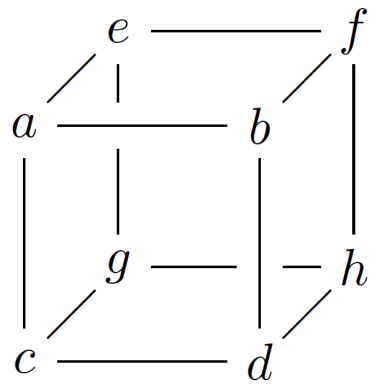
Bhargava's Cube

We now change our setting to $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, the free $\mathbb{Z}$-module of rank 8. Every element can be written in the form (a, b, c, d, e, f, g, h).

We associate it with the cube of integers



.



Since the cube has three different symmetries, there are three different ways to partition the cube, namely

$$M_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \; N_1 = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

or

$$M_2 = \begin{bmatrix} a & c \\ e & g \end{bmatrix}, \; N_2 = \begin{bmatrix} b & d \\ f & h \end{bmatrix}$$

or

$$M_3 = \begin{bmatrix} a & e \\ b & f \end{bmatrix}, \; N_3 = \begin{bmatrix} c & g \\ d & h \end{bmatrix}.$$

Associated Binary Quadratic Forms

Given a cube X, we can construct three binary quadratic forms by setting

$$Q_i^X(x, y) = -\det(M_i x - N_i y).$$

The cube X is **projective** if Q_1^X, Q_2^X and Q_3^X are all primitive.

The discriminant of Q_1^X, Q_2^X and Q_3^X are all equal. We define the **discriminant** of X by

$$\mathrm{disc}(X) = \mathrm{disc}(Q_1^X) = \mathrm{disc}(Q_2^X) = \mathrm{disc}(Q_3^X).$$

Group Action

We define an analogous group action on the cube :

An element

$$\left(\begin{bmatrix} r_1 & s_1 \\ t_1 & u_1 \end{bmatrix}, \begin{bmatrix} r_2 & s_2 \\ t_2 & u_2 \end{bmatrix}, \begin{bmatrix} r_3 & s_3 \\ t_3 & u_3 \end{bmatrix} \right)$$

of the group $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ act on the cube by replacing (M_i, N_i) with $(r_i M_i + s_i N_i, t_i M_i + u_i N_i)$ for each $i \in \{1, 2, 3\}$.

Associated Binary Quadratic Forms

Key proposition : Γ-equivalent cubes correspond to $SL_2(\mathbb{Z})$-equivalent forms and vice versa.

Let X be a cube. If X is transformed by the action of some element in Γ, then the three associated binary quadratic forms Q_1^X, Q_2^X and Q_3^X will all be transformed by the action of some element in $SL_2(\mathbb{Z})$.

Conversely, if Q_1^X, Q_2^X and Q_3^X are transformed to Q_1', Q_2' and Q_3' by some element in $SL_2(\mathbb{Z})$, then there exist a transformation of X to Y by some element in Γ such that

$$Q_1^Y = Q_1' \quad \text{and} \quad Q_2^Y = Q_2' \quad \text{and} \quad Q_3^Y = Q_3'.$$

Constructing The Group Law on Primitive Forms

First start with the free group on the set of all primitive forms of discriminant D.

Define the cube law by setting

$$Q_1^X + Q_2^X + Q_3^X = 0$$

for every projective cube X.

If the cube X give rise to Q_1, Q_2, Q_3, then we may transform X (by the Γ-action) to another cube X', which gives rise to Q_1', Q_2, Q_3, where Q_1' is $SL_2(\mathbb{Z})$-equivalent to Q_1. The cube law dictates that

$$Q_1 + Q_2 + Q_3 = 0 \quad \text{and} \quad Q_1' + Q_2 + Q_3 = 0.$$

Thus Q_1 and Q_1' become identified.

Constructing The Group Law on Primitive Forms

Key proposition : For any two primitive forms f and g of discriminant D, there exist a projective cube X, unique up to Γ-equivalence, such that $Q_1^X = f$ and $Q_2^X = g$. (This is tricky to prove)

Next, we choose a suitable identity element $Q_{\mathrm{id,D}}$.

Additional condition : There exist a cube X such that

$$Q_1^X = Q_2^X = Q_3^X = Q_{\mathrm{id,D}}.$$

We declare $Q_{\mathrm{id,D}} = 0$.

Reason : There exist a cube X such that $Q_1^X = Q_2^X = Q_{\mathrm{id,D}}$. By the cube law,

$$Q_3^X = 0.$$

If Q_3^X and $Q_{\mathrm{id,D}}$ are not $SL_2(\mathbb{Z})$-equivalent, then we would have 'identified more than we should'.

Remark : We use $\overline{f}$ to denote the $SL_2(\mathbb{Z})$-equivalence class containing f.

For any primitive form f, there exists a cube A such that $Q_1^A = Q_{\mathrm{id,D}}$ and $Q_2^A = f$. The cube law dictates that $Q_1^A + Q_2^A + Q_3^A = 0$ and $Q_{\mathrm{id,D}} = 0$ so

$$-\overline{f} = \overline{Q_3^A}.$$

Then for any two primitive forms f and g, there exists a cube A' such that $Q_1^{A'} = f$ and $Q_2^{A'} = g$. Define

$$\overline{f} + \overline{g} = -\overline{Q_3^{A'}}.$$

Main Theorem

Theorem (Manjul Bhargava)

Let D be any integer congruent to 0 or 1 modulo 4. Let $Q_{id,D}$ be any primitive binary quadratic form of discriminant D such that there exists a cube X_0 satisfying $Q_1^{X_0} = Q_2^{X_0} = Q_3^{X_0} = Q_{id,D}$. Then there exists a unique group law on the set of $SL_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D satisfying

1. *$\overline{Q_{id,D}}$ is the additive identity.*
2. *For any projective cube X of discriminant D, we have*

$$\overline{Q_1^X} + \overline{Q_2^X} + \overline{Q_3^X} = \overline{Q_{id,D}}.$$

Conversely, given Q_1, Q_2, Q_3 with $\overline{Q_1} + \overline{Q_2} + \overline{Q_3} = \overline{Q_{id,D}}$, there exists a cube X, unique up to Γ-equivalence, such that $Q_1^X = Q_1$, $Q_2^X = Q_2$ and $Q_3^X = Q_3$.

Equivalence with Gauss composition

When we choose

$$A_{\mathrm{id},D} = \begin{array}{ccc} 1 & \text{———} & 0 \\ | \diagdown & | & | \diagdown \\ 0 & \text{———} & 1 \\ | & | & | \\ | & 0 \text{ ——} & | - D/4 \\ | \diagdown & | & | \diagdown \\ 1 & \text{———} & 0 \end{array} \quad \text{or} \quad A_{\mathrm{id},D} = \begin{array}{ccc} 1 & \text{———} & 1 \\ | \diagdown & | & | \diagdown \\ 0 & \text{———} & 1 \\ | & | & | \\ | & 1 \text{ ——} & | - (D+3)/4 \\ | \diagdown & | & | \diagdown \\ 1 & \text{———} & 1 \end{array},$$

the three associated quadratic forms simply become

$$Q_{\mathrm{id,D}} = \begin{cases} x^2 - \dfrac{D}{4}y^2 & \text{if } D \equiv 0 \pmod 4 \\ x^2 - xy + \dfrac{1-D}{4}y^2 & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

In this case, the group law is precisely Gauss composition.

Composition of $2 \times 2 \times 2$ cubes

The group law on quadratic forms induces a natural group law on the set of Γ-equivalence classes of projective cubes.

Sketch of construction :

Let X and Y be two projective cubes of discriminant D. By the cube law,

$$(\overline{Q_1^X} + \overline{Q_1^Y}) + (\overline{Q_2^X} + \overline{Q_2^Y}) + (\overline{Q_3^X} + \overline{Q_3^Y}) = \overline{Q_{\mathrm{id,D}}}.$$

Theorem (Second part)

Conversely, given Q_1, Q_2, Q_3 with $\overline{Q_1} + \overline{Q_2} + \overline{Q_3} = \overline{Q_{id,D}}$, there exists a cube X, unique up to Γ-equivalence, such that $Q_1^X = Q_1$, $Q_2^X = Q_2$ and $Q_3^X = Q_3$.

There exist a cube Z, unique up to Γ-equivalence, satisfying

$$\overline{Q_i^Z} = \overline{Q_i^X} + \overline{Q_i^Y} \text{ for all } i \in \{1, 2, 3\}.$$

Composition of $2 \times 2 \times 2$ cubes

Define the composition of $[X]$ and $[Y]$ (denoted by $+_c$) by

$$[X] +_c [Y] = [Z].$$

Remark : $[X]$ denotes the Γ-equivalence class of the cube X.

Composition of $2 \times 2 \times 2$ cubes

$$A_{\mathrm{id},D} = \begin{array}{ccc} 1 & \text{———} & 0 \\ | \diagdown & & | \diagdown \\ 0 & \text{———} & 1 \\ | & & | \\ & 0 \text{ ——} & | - D/4 \\ & \diagdown & \diagdown \\ 1 & \text{———} & 0 \end{array} \quad \text{or} \quad A_{\mathrm{id},D} = \begin{array}{ccc} 1 & \text{———} & 1 \\ | \diagdown & & | \diagdown \\ 0 & \text{———} & 1 \\ | & & | \\ & 1 \text{ ——} & | - (D+3)/4 \\ & \diagdown & \diagdown \\ 1 & \text{———} & 1 \end{array}$$

Theorem (Manjul Bhargava)

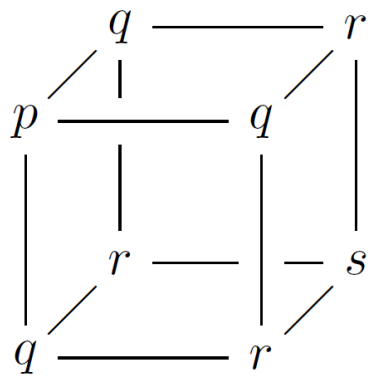
Let D be any integer congruent to 0 or 1 modulo 4. Then there exists a unique group law on the set of Γ-equivalence classes of projective cubes of discriminant D such that

1. $[A_{id,D}]$ *is the additive identity.*
2. *For $i = 1, 2, 3$, the maps $[X] \mapsto \overline{Q_i^X}$ yield group homomorphisms to the form class group of discriminant D.*

Further Generalisations

The group structure on $2 \times 2 \times 2$ projective cubes allows Gauss composition to be generalised to higher dimensions.

An example : A **binary cubic form** $px^3 + 3qx^2y + 3rxy^2 + sy^3$ can be naturally associated with the **triply-symmetric** cube



.

To a binary cubic form C, we use $\iota(C)$ to denote the corresponding cube.

Further Generalisations

Notions on cubes can then be 'carried over' to binary cubic forms :

1. A binary cubic form C is **projective** if $\iota(C)$ is projective.
2. Two binary cubic forms C_1 and C_2 are $SL_2(\mathbb{Z})$-**equivalent** $\iota(C_1)$ and $\iota(C_2)$ are Γ-equivalent.
3. The **discriminant** of a binary cubic form C is the discriminant of $\iota(C)$.

By definition ι induces a natural bijection between the $SL_2(\mathbb{Z})$-equivalence class of projective binary cubic forms and the Γ-equivalence classes of projective cubes which contains a triply-symmetric cube.

Further Generalisations

Rough idea : The group structure on cubic forms 'follow' the group structure on triply-symmetric cubes.

1. Given any two projective cubic forms C_1 and C_2, first show that the Γ-equivalence class of

$$\left[\iota(C_1)\right] +_c \left[\iota(C_2)\right]$$

must also contain a triply-symmetric cube X.

2. We then define their composition (denoted by $\bullet$) by

$$\overline{C_1} \bullet \overline{C_2} = \overline{\iota^{-1}(X)}.$$

Further Generalisations

Under the bijection ι, the preimages of the identity cube $A_{\mathrm{id,D}}$ are

$$C_{\mathrm{id,D}} = \begin{cases} 3x^2y + \dfrac{D}{4}y^3 & \text{if } D \equiv 0 \pmod 4 \\ 3x^2y + 3xy^2 + \dfrac{D+3}{4}y^3 & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

Theorem (Manjul Bhargava)

Let D be any integer congruent to 0 or 1 modulo 4. Then there exists a unique group law on the set of $SL_2(\mathbb{Z})$-equivalence classes of projective binary cubic forms C of discriminant D such that

1. $\overline{C_{id,D}}$ *is the additive identity.*
2. *The map given by* $\overline{C} \mapsto [\iota(C)]$ *is a group homomorphism.*