


# Summary on Higher Composition Law and the Density of Discriminants

Jiahe Shen,  js6157@columbia.edu<sup>1</sup>

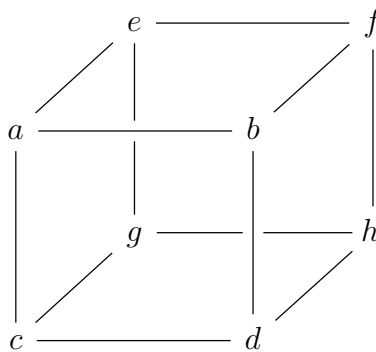
<sup>1</sup>Department of Mathematics, Columbia University

September 23, 2023

## 1 Higher Composition Law I

Some terminology and notations need to know: An  $n$ -ary  $k$ -ic form is a homogenous polynomial in  $n$ -variables of degree  $k$ . For example, a binary quadratic form is a function of the form  $f(x, y) = ax^2 + bxy + cy^2$  for some coefficients  $a, b, c$ . We write  $(\text{Sym}^k \mathbb{Z}^n)^*$  the  $\binom{n+k-1}{k}$ -dimensional lattice of  $n$ -ary  $k$ -ic form with integer coefficients; We write  $\text{Sym}^k \mathbb{Z}^n$  for the sublattice that the coefficient of  $x_1^{e_1} \dots x_n^{e_n} (e_1 + \dots + e_n = k)$  is a multiple of  $\binom{k}{e_1, \dots, e_n}$ . For example,  $(\text{Sym}^3 \mathbb{Z}^2)^*$  is the space of integer-coefficient symmetric binary cubic forms  $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ , while  $\text{Sym}^3 \mathbb{Z}^2$  is the space of such forms with  $b$  and  $c$  divisible by 3. Finally, we also has the space  $\wedge^k \mathbb{Z}^n$  of  $n$ -ary alternating  $k$ -forms, i.e., multilinear functions  $\mathbb{Z}^n \times \dots \times \mathbb{Z}^n \rightarrow \mathbb{Z}$  that change sign when any two variables are interchanged.

Let  $\mathcal{C}_2$  denote the space  $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$  consisting of cubes of integers



Where  $a, b, c, d, e, f, g, h \in \mathbb{Z}$ . A cube of integers  $A \in \mathcal{C}_2$  defined as above can be partitioned into two  $2 \times 2$  matrices in three ways:

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

or into

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

or

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

Define a group action of  $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$  over  $\mathcal{C}_2$  as

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} (M_i, N_i) = (rM_i + sN_i, tM_i + uN_i), \quad \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$$

The element  $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$  lies in the  $i^{\text{th}}$  factor of  $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$  and these three factors commute with each other.

For any cube  $A \in \mathcal{C}_2$ , and  $1 \leq i \leq 3$ , define a binary quadratic form  $Q_i = Q_i^A$  by

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

The form  $Q_1$  is invariant under the action of the subgroup  $\{id\} \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ , and the remaining factor of  $SL_2(\mathbb{Z})$  acts in the standard way on  $Q_1$ . The unique polynomial invariant of this action is  $\text{Disc}(Q_1)$ . Such a conclusion also holds for  $Q_2$  and  $Q_3$ , and it is surprising that  $\text{Disc}(Q_1) = \text{Disc}(Q_2) = \text{Disc}(Q_3)$ , which we also denote as  $\text{Disc}(A)$ . Explicitly, we have

$$\text{Disc}(A) = a^2 h^2 + b^2 g^2 + c^2 f^2 + d^2 e^2 - 2(abgh + cdef + acfh + bdcg + aedh + bfcg) + 4(adfg + bceh)$$

Let  $D \equiv 0, 1 \pmod{4}$ . Inspired by the group law on elliptic curves, we define an addition axiom on the set of (primitive) binary forms  $Q_1^A, Q_2^A, Q_3^A$  arising from a cube  $A$  of discriminant  $D$ ,

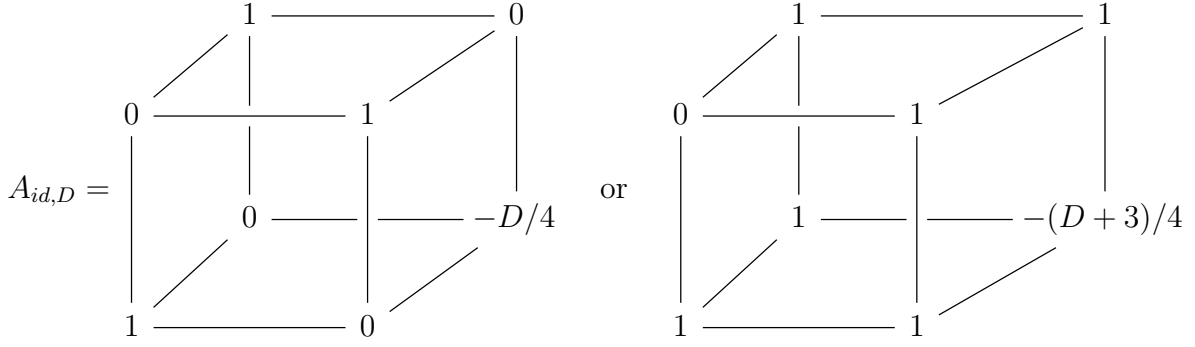
$$Q_1^A + Q_2^A + Q_3^A = 0$$

More formally, we consider the free abelian group on the set of primitive binary quadratic form of discriminant  $D$  modulo the subgroup generated by all sums  $[Q_1^A] + [Q_2^A] + [Q_3^A]$ . Since  $[Q_1] + [Q_2] + [Q_3] = [Q_1'] + [Q_2] + [Q_3] = 0$ , the cube law descends to a law of addition on  $SL_2(\mathbb{Z})$ -equivalence classes of forms of a given discriminant. Also, given  $Q_1, Q_2, Q_3$  with  $[Q_1] + [Q_2] + [Q_3] = 0$ , there exists a cube  $A$  of discriminant  $D$ , unique up to  $\Gamma$ -equivalence, such that  $Q_1 = Q_1^A, Q_2 = Q_2^A, Q_3 = Q_3^A$ .

The natural choice of identity element of composition law is

$$Q_{id,D} = x^2 - \frac{D}{4}y^2 \quad \text{or} \quad Q_{id,D} = x^2 - xy + \frac{1-D}{4}y^2$$

follows from the triply-symmetric cubes



We use  $(\text{Sym}^2\mathbb{Z}^2)^*$  to denote the lattice of integer-valued binary quadratic forms, and we use  $\text{Cl}((\text{Sym}^2\mathbb{Z}^2)^*; D)$  to denote the set of  $SL_2(\mathbb{Z})$ -equivalence classes of primitive binary quadratic forms of discriminant  $D$  equipped with the above group structure.

We say a cube  $A$  is projective if the forms  $Q_1^A, Q_2^A$  and  $Q_3^A$  are primitive.

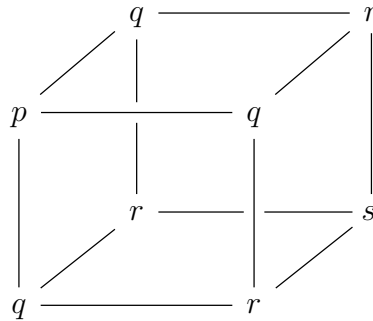
Let  $D$  be any integer congruent to 0 or 1 (mod 4), and let  $A_{id,D}$  be the triply-symmetric cube defined above. Then there exists a unique group law on the set of  $\Gamma$ -equivalence classes of projective cubes  $A$  of discriminant  $D$  such that

- (a)  $[A_{id,D}]$  is the additive identity;
- (b) For  $i = 1, 2, 3$ , the maps  $[A] \mapsto [Q_i^A]$  is a group homomorphism to  $\text{Cl}((\text{Sym}^2\mathbb{Z}^2)^*; D)$ .

In fact, for every projective cubes  $A, A'$ , since  $[Q_1^A] + [Q_1^{A'}] + [Q_2^A] + [Q_2^{A'}] + [Q_3^A] + [Q_3^{A'}] = 0$ , there must exist projective cube  $A''$  such that  $[Q_i^A] + [Q_i^{A'}] = [Q_i^{A''}]$  for  $i = 1, 2, 3$ . We define the composition of  $[A]$  and  $[A']$  by  $[A] + [A'] = [A'']$ .

We denote the set of  $\Gamma$ -equivalence classes of projective cubes of discriminant  $D$ , equipped with the above group structure, by  $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$ .

The above law of composition on cubes also leads naturally to a law of composition on  $SL_2(\mathbb{Z})$ -equivalence classes of integral binary cubic forms  $px^3 + 3qx^2y + 3rxy^2 + sy^3$ . For just as one frequently associates to binary quadratic form  $px^2 + 2qxy + ry^2$  the symmetric  $2 \times 2$  matrix  $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ , one may naturally associate to a binary cubic form  $px^3 + 3qx^2y + 3rxy^2 + sy^3$  the triply symmetric  $2 \times 2 \times 2$  matrix



which gives a natural inclusion  $\iota : \text{Sym}^3\mathbb{Z}^2 \rightarrow \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ . The preimage of the identity cubes under  $\iota$  are given by

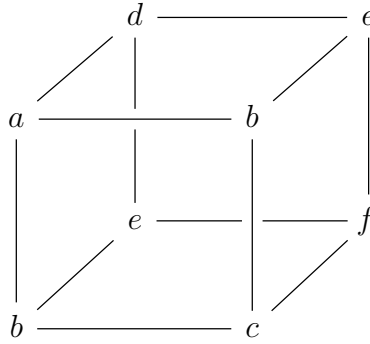
$$C_{id,D} = 3x^2y + \frac{D}{4}y^3 \quad \text{or} \quad C_{id,D} = 3x^2y + 3xy^2 + \frac{D+3}{4}y^3$$

Denoting the  $SL_2(\mathbb{Z})$ -equivalence class of  $C \in \text{Sym}^3\mathbb{Z}^2$  by  $[C]$ . Let  $D$  be any integer congruent to 0 or 1 mod 4, and let  $C_{id,D}$  be defined as above. 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

- (a)  $[C_{id,D}]$  is the additive identity;
- (b) The map given by  $[C] \mapsto [\iota(C)]$  is a group homomorphism to  $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$ .

We denote the set of equivalence classes of projective binary cubic forms of discriminant  $D$  equipped with the above group structure by  $\text{Cl}(\text{Sym}^3\mathbb{Z}^2; D)$ .

Consider the cubes that hold a twofold symmetry



These cubes can be naturally viewed as a pair of binary quadratic forms  $(ax^2 + 2bxy + cy^2, dx^2 + 2exy + fy^2)$ .

If we use  $\mathbb{Z}^2 \otimes \text{Sym}^2\mathbb{Z}^2$  to denote the space of pairs of classically integral binary quadratic forms, then the above association of  $(ax^2 + 2bxy + cy^2, dx^2 + 2exy + fy^2)$  with the cube above corresponds to the natural inclusion map

$$j : \mathbb{Z}^2 \otimes \text{Sym}^2\mathbb{Z}^2 \rightarrow \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$$

The preimage of the identity cubes  $A_{id,D}$  under  $j$  are seen to be

$$B_{id,D} = (2xy, x^2 + \frac{D}{4}y^2) \quad \text{or} \quad B_{id,D} = (2xy + y^2, x^2 + 2xy + \frac{D+3}{4}y^2)$$

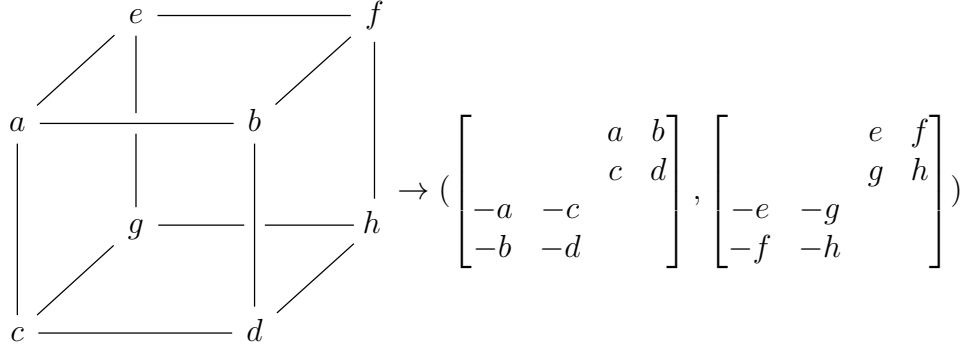
Denoting the  $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ -class of  $B \in \mathbb{Z}^2 \otimes \text{Sym}^2\mathbb{Z}^2$  by  $[B]$ . Let  $D$  be any integer congruent to 0 or 1 mod 4, and let  $B_{id,D}$  be given as above. There exists a unique group law on the set of  $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ -equivalence classes of projective pairs of binary quadratic forms  $B$  of discriminant  $D$  such that

- (a)  $[B_{id,D}]$  is the additive identity;
- (b) The map given by  $[B] \mapsto [j(B)]$  is a group homomorphism to  $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$ .

Consider the natural  $\mathbb{Z}$ -linear mapping

$$id \otimes \wedge_{2,2} : \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \rightarrow \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$$

taking  $2 \times 2 \times 2$  cubes to pairs of alternating 2-forms in four variables



Let  $\Gamma = SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$  as before, and set  $\Gamma' = SL_2(\mathbb{Z}) \times SL_4(\mathbb{Z})$ . For any pair  $F = (M, N) \in \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4$  of alternating  $4 \times 4$  matrices, one can naturally associate a binary quadratic form  $Q = Q^F$  given by

$$-Q(x, y) = \text{Pfaff}(Mx - Ny) = \sqrt{(\det(Mx - Ny))}$$

(Let  $A$  be a  $2n \times 2n$  matrix. A Pfaffian is a polynomial over the entries of  $A$  defined as  $\text{Pfaff}(A) = \frac{1}{2^n n!} \sum_{\sigma \in S_{2n}} \text{sgn}(\sigma) \prod_{i=1}^n a_{\sigma(2i-1), \sigma(2i)}$ . In particular, when  $A$  is skew-symmetric, we have  $\text{Pfaff}(A)^2 = \det(A)$ .)

The space of elements  $(M, N) \in \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4$  possesses a unique polynomial invariant for the action of  $\Gamma' = SL_2(\mathbb{Z}) \times SL_4(\mathbb{Z})$ , namely

$$\text{Disc}(\text{Pfaff}(Mx - Ny))$$

We denote this invariant of  $F$  as  $\text{Disc}(F)$ . Denote  $[F]$  as the  $\Gamma'$ -equivalence class of  $F$ . Let  $D$  be any integer congruent to 0 or 1 mod 4, and let  $F_{id, D} = id \otimes \wedge_{2,2}(A_{id, D})$  be written as

$$\left( \begin{bmatrix} & 0 & 1 \\ & 1 & 0 \\ 0 & -1 & \\ -1 & 0 & \end{bmatrix}, \begin{bmatrix} & 1 & 0 \\ & 0 & -\frac{D}{4} \\ -1 & 0 & \\ 0 & \frac{D}{4} & \end{bmatrix} \right) \text{ or } \left( \begin{bmatrix} & 0 & 1 \\ & 1 & 1 \\ 0 & -1 & \\ -1 & -1 & \end{bmatrix}, \begin{bmatrix} & 1 & 1 \\ & 1 & -\frac{D+3}{4} \\ -1 & -1 & \\ -1 & \frac{D+3}{4} & \end{bmatrix} \right)$$

Then there exists a unique group law on the set of  $\Gamma'$ -equivalence classes of projective pairs of quaternary alternating 2-forms  $F$  of discriminant  $D$  such that:

- (a)  $[F_{id, D}]$  is the additive identity;
- (b) The map given by  $[A] \mapsto [id \otimes \wedge_{2,2}(A)]$  is a group homomorphism from  $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2, D)$ ;
- (c) The map given by  $[F] \mapsto [Q^F]$  is a group homomorphism to  $\text{Cl}((\text{Sym}^2 \mathbb{Z}^2)^*; D)$ .

For any trilinear map

$$\phi : L_1 \times L_2 \times L_3 \rightarrow \mathbb{Z}$$

in  $\mathbb{Z}^2 \times \mathbb{Z}^2 \times \mathbb{Z}^2$ , construct the alternating trilinear map

$$\bar{\phi} = \wedge_{2,2,2}(\phi) : (L_1 \oplus L_2 \oplus L_3)^3 \rightarrow \mathbb{Z}$$

given by

$$\bar{\phi}((r_1, r_2, r_3), (s_1, s_2, s_3), (t_1, t_2, t_3)) = \det_{\phi}(r, s, t) = \sum_{\sigma \in S_3} (-1)^{\sigma} \phi(r_{\sigma(1)}, s_{\sigma(2)}, t_{\sigma(3)})$$

This is an integral alternating 3-form in six variables, and so we obtain a natural  $\mathbb{Z}$ -linear map

$$\wedge_{2,2,2} : \mathbb{Z}^2 \times \mathbb{Z}^2 \times \mathbb{Z}^2 \rightarrow \wedge^3(\mathbb{Z}^2 \oplus \mathbb{Z}^2 \oplus \mathbb{Z}^2) = \wedge^3 \mathbb{Z}^6$$

We say that an element  $E \in \wedge^3 \mathbb{Z}^6$  is projective if it is  $SL_6(\mathbb{Z})$ -equivalent to  $\wedge_{2,2,2}(A)$  for some projective cube  $A$ . The projective classes in  $\wedge^3 \mathbb{Z}^6$  of discriminant  $D$  should also turn into a group. In fact, this group, denote as  $\text{Cl}(\wedge^3 \mathbb{Z}^6; D)$ , always consists of exactly one element, which is  $[E_{id,D}] = [\wedge_{2,2,2}(A_{id,D})]$ .

Now we turn to discover the relations of these composition laws with ideal classes in quadratic orders.

Let  $\mathbb{D}$  be the set of integers congruent to 0 or 1 mod 4. There is a one-to-one correspondence between the set of elements of  $\mathbb{D}$  and the set of isomorphism classes of oriented quadratic rings by the association

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

Where "oriented" means that the specific choice of  $\sqrt{D}$  is already made.

There is a canonical bijection between the set of nondegenerated  $SL_2(\mathbb{Z})$ -orbits on the space  $(\text{Sym}^2 \mathbb{Z}^2)^*$  of integer-valued binary quadratic forms, and the set of isomorphism classes of pairs  $(S, I)$ , where  $S$  is a nondegenerated oriented quadratic ring and  $I$  is a (not necessarily invertible) oriented ideal class of  $S$ . Under this bijection, the discriminant of a binary quadratic form equals the discriminant of the corresponding quadratic ring. Also, this bijection is restricted to a correspondence

$$\text{Cl}((\text{Sym}^2 \mathbb{Z}^2)^*; D) \leftrightarrow \text{Cl}^+(S(D))$$

Here  $\text{Cl}^+(S(D))$  is the narrow ideal class group. To be specific, consider an oriented ideal  $(I, \epsilon)$ .  $I$  is any (fractional) ideal of  $S$  in  $K = S \otimes \mathbb{Q}$  having rank 2 as a  $\mathbb{Z}$ -module, and  $\epsilon = \pm 1$  gives the orientation of  $I$ . For any element  $\kappa \in K$ , the product  $\kappa \cdot (I, \epsilon)$  is defined to be the ideal  $(\kappa I, \text{sgn}(N(\kappa))\epsilon)$ . Two oriented ideals  $(I_1, \epsilon_1)$  and  $(I_2, \epsilon_2)$  are said to be in the same oriented ideal class if  $(I_1, \epsilon_1) = \kappa(I_2, \epsilon_2)$  for some invertible  $\kappa \in K$ . With these notations, the narrow class group can then be defined as the group of invertible oriented ideals modulo multiplication by invertible scalars  $\kappa \in K$ , (equivalently, modulo the subgroup consisting of invertible principal oriented ideals  $((\kappa), \text{sgn}(N(\kappa)))$ .)

We say that a triple  $(I_1, I_2, I_3)$  of oriented ideals of  $S$  is balanced if  $I_1 I_2 I_3 \subseteq S$  and  $N(I_1)N(I_2)N(I_3) = 1$ . Also, we define two balanced triples  $(I_1, I_2, I_3)$  and  $(I'_1, I'_2, I'_3)$  of  $S$  to

be equivalent if  $I_1 = \kappa_1 I'_1, I_2 = \kappa_2 I'_2, I_3 = \kappa_3 I'_3$  for some elements  $\kappa_1, \kappa_2, \kappa_3 \in K$ . In particular, we have  $N(\kappa_1 \kappa_2 \kappa_3) = 1$ . Throughout the paper,  $N(I)$  is the norm of the ideal  $I$ , which is defined as

$$N(I, \epsilon) = \epsilon \frac{|L/I|}{|L/S|}$$

Where  $L$  is any lattice in  $K = S \otimes \mathbb{Q}$  containing both  $S$  and  $I$ . (We sometimes omit the orientation of  $I$  if not necessary.)

There is a canonical bijection between the set of nondegenerate  $\Gamma$ -orbits on the space  $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$  of  $2 \times 2 \times 2$  integer cubes, and the set of isomorphism classes of pairs  $(S, (I_1, I_2, I_3))$ , where  $S$  is a nondegenerate oriented quadratic ring and  $(I_1, I_2, I_3)$  is an equivalence class of balanced triples of oriented ideals of  $S$ . Under this bijection, the discriminant of an integer cube equals the discriminant of the corresponding quadratic ring. Specifically, let  $\langle 1, \tau \rangle$  be a positively oriented basis of  $S$  such that  $\tau^2 - \frac{D}{4} = 0$  or  $\tau^2 - \tau + \frac{1-D}{4} = 0$ . Let  $I_1 = \langle \alpha_1, \alpha_2 \rangle, I_2 = \langle \beta_1, \beta_2 \rangle, I_3 = \langle \gamma_1, \gamma_2 \rangle$  denote the  $\mathbb{Z}$ -basis of the ideals  $I_1, I_2$  and  $I_3$ . We write

$$\alpha_i \beta_j \gamma_k = c_{ijk} + a_{ijk} \tau$$

for some set of sixteen integers  $a_{ijk}$  and  $c_{ijk}$  ( $1 \leq i, j, k \leq 2$ ). Then  $A = (a_{ijk})$  is our desired cube. This bijection is restricted to correspondence

$$\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D) \leftrightarrow \text{Cl}^+(S(D)) \times \text{Cl}^+(S(D))$$

which is an isomorphism of groups.

There is a canonical bijection between the set of nondegenerate  $SL_2(\mathbb{Z})$ -orbits on the space  $\text{Sym}^3 \mathbb{Z}^2$  of binary cubic forms, and the set of equivalence classes of triples  $(S, I, \delta)$ , where  $S$  is a nondegenerate oriented quadratic ring,  $I$  is an ideal of  $S$ , and  $\delta$  is an invertible element of  $S \otimes \mathbb{Q}$  such that  $I^3 \subseteq \delta \cdot S$  and  $N(I)^3 = N(\delta)$ . Here two triples  $(S, I, \delta)$  and  $(S, I', \delta')$  are equivalent if there is an isomorphism  $\phi : S \rightarrow S'$  and an element  $\kappa \in S' \otimes \mathbb{Q}$  such that  $I' = \kappa \phi(I)$  and  $\delta' = \kappa^3 \phi(\delta)$ . Under this bijection, the discriminant of a binary cubic form is equal to the discriminant of the corresponding quadratic ring. Specifically, let  $\tau$  be as before, and  $I = \langle \alpha, \beta \rangle$  with  $\langle \alpha, \beta \rangle$  positively oriented. We write

$$\alpha^3 = \delta(c_0 + a_0 \tau), \alpha^2 \beta = \delta(c_1 + a_1 \tau), \alpha \beta^2 = \delta(c_2 + a_2 \tau), \beta^3 = \delta(c_3 + a_3 \tau)$$

For some eight integers  $a_i$  and  $c_i$ . Then  $C(x, y) = a_0 x^3 + 3a_1 x^2 + 3a_2 xy^2 + a_3 y^3$  is our desired binary cubic form. This bijection restricts to a surjective group homomorphism

$$\text{Cl}(\text{Sym}^3 \mathbb{Z}^2; D) \twoheadrightarrow \text{Cl}_3(S(D))$$

The special case where  $D$  corresponds to the ring of integers in a quadratic number field deserves special mention. Suppose  $D$  is the discriminant of a quadratic number field  $K$ . Then, there is a natural surjective homomorphism

$$\text{Cl}(\text{Sym}^3 \mathbb{Z}^2; D) \twoheadrightarrow \text{Cl}_3(K)$$

There is a canonical bijection between the set of nondegenerate  $SL_2(\mathbb{Z})$ -orbits on the space  $\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^2$ , and the set of isomorphism classes of pairs  $(S, (I_1, I_2, I_3))$ , where  $S$  is a nondegenerate oriented quadratic ring and  $(I_1, I_2, I_3)$  is an equivalence class of balanced triples or oriented ideals of  $S$  such that  $I_2 = I_3$ . Under this bijection, the discriminant of a pair of binary quadratic forms is equal to the discriminant of the corresponding quadratic ring.

There is a canonical bijection between the set of nondegenerate  $SL_2(\mathbb{Z}) \times SL_4(\mathbb{Z})$ -orbits on the space  $\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4$ , and the set of isomorphism classes of pairs  $(S, (I, M))$ , where  $S$  is a nondegenerate oriented quadratic ring and  $(I, M)$  is an equivalence class of balanced pairs of oriented ideals of  $S$  having ranks 1 and 2 respectively. Under this bijection, the discriminant of a pair of quaternary alternating 2-forms equals the discriminant of the corresponding quadratic ring. (See the paper for details and important definitions.) Specifically, let  $\langle 1, \tau \rangle$  be a  $\mathbb{Z}$ -basis for  $S$  as before, and suppose  $\langle \alpha_1, \alpha_2 \rangle$  and  $\langle \beta_1, \beta_2, \beta_3, \beta_4 \rangle$  are appropriately oriented  $\mathbb{Z}$ -basis for the oriented  $S$ -ideals of  $I$  and  $M$  respectively. By hypothesis, we may write

$$\alpha_i \det(\beta_j, \beta_k) = c_{jk}^{(i)} + a_{jk}^{(i)} \tau$$

for some set of 24 constants  $c_{jk}^{(i)}$  and  $a_{jk}^{(i)}$  such that

$$c_{jk}^{(i)} = -c_{kj}^{(i)} \quad \text{and} \quad a_{jk}^{(i)} = -a_{kj}^{(i)}$$

for all  $i \in \{1, 2\}$  and  $j, k \in \{1, 2, 3, 4\}$ . Then the set of constants  $F = \{a_{jk}^{(i)}\} \in \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4$  is our desired pair of quaternary alternating 2-forms. This bijection is restricted to correspondence

$$\text{Cl}(\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4; D) \leftrightarrow \text{Cl}(S(D))$$

which is an isomorphism of groups.

There is a canonical bijection between the set of nondegenerate  $SL_6(\mathbb{Z})$  on the space  $\wedge^3 \mathbb{Z}^6$ , and the set of isomorphism classes of pairs  $(S, M)$ , where  $S$  is a nondegenerate oriented quadratic ring and  $M$  is an equivalence class of balanced ideals of  $S$  having rank 3. Under this bijection, the discriminant of a senary alternating 3-form is equal to the discriminant of the corresponding quadratic ring. Specifically, let  $\langle 1, \tau \rangle$  be a  $\mathbb{Z}$ -basis of  $S$ , and  $\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6 \rangle$  is a positively oriented  $\mathbb{Z}$ -basis for the  $S$ -module  $M$ . By the hypothesis that  $M$  is balanced, we may write

$$\det(\alpha_i, \alpha_j, \alpha_k) = c_{ijk} + a_{ijk} \tau$$

for some set of 40 integers  $\{c_{ijk}\}$  and  $\{a_{ijk}\}$  satisfying

$$c_{ijk} = -c_{jik} = -c_{ikj} = -c_{kji}$$

and

$$a_{ijk} = -a_{jik} = -a_{ikj} = -a_{kji}$$

for all  $i, j, k \in \{1, 2, 3, 4, 5, 6\}$ . The set of constants  $E = \{a_{ijk}\}_{1 \leq i, j, k \leq 6} \in \wedge^3 \mathbb{Z}^6$  is then our desired senary alternating 3-form.



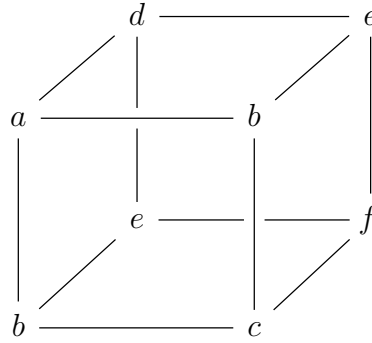
Finally, let us summarize this whole section. We have natural discriminant-preserving arrows

$$\begin{array}{ccc}
 \text{Sym}^3 \mathbb{Z}^2 & \xrightarrow{(1)} & \mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^2 & \xrightarrow{(2)} & \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \\
 & & \downarrow (3) & & \downarrow (4) \\
 & & (\text{Sym}^2 \mathbb{Z}^2)^* & \xleftarrow{(5)} & \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4 \\
 & & & & \downarrow (6) \\
 & & & & \wedge^3 \mathbb{Z}^6
 \end{array}$$

Specifically,

The arrow (1) maps  $px^3 + 3qx^2y + 3rxy^2 + sy^3$  to  $(px^2 + 2qxy + ry^2, qx^2 + 2rxy + sy^2)$ , which is an injective map;

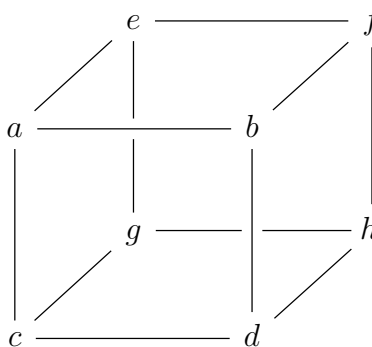
The arrow (2) maps  $(ax^2 + 2bxy + cy^2, dx^2 + 2exy + fy^2)$  to the cube



which is an injective map;

The arrow (3) maps  $(ax^2 + 2bxy + cy^2, dx^2 + 2exy + fy^2)$  to the binary quadratic form  $-\det \begin{pmatrix} ax - dy & bx - ey \\ bx - ey & cx - fy \end{pmatrix} = (b^2 - ac)x^2 + (af + cd - 2be)xy + (e^2 - df)y^2$ ;

The arrow (4) maps the cube



To the pair of alternating 2-form in four variables  $\left( \begin{bmatrix} & a & b \\ -a & -c & d \\ -b & -d & \end{bmatrix}, \begin{bmatrix} & e & f \\ -e & -g & h \\ -f & -h & \end{bmatrix} \right)$ ,

which is an injective map;

The arrow (5) maps the pair  $F = (M, N) \in \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4$  of alternating  $4 \times 4$  matrices to the binary quadratic form given by  $-\text{Pfaff}(Mx - Ny)$ ;

The arrow (6) is also injective; we omit the details here.

These arrows above lead to the group homomorphisms

$$\begin{array}{ccccc}
 \text{Cl}(\text{Sym}^3 \mathbb{Z}^2; D) & \xrightarrow{(1)} & \text{Cl}(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^2; D) & \xrightarrow{(2)} & \text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D) \\
 & & \downarrow (3) & & \downarrow (4) \\
 & & \text{Cl}((\text{Sym}^2 \mathbb{Z}^2)^*; D) & \xleftarrow{(5)} & \text{Cl}(\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4; D) \\
 & & & & \downarrow (6) \\
 & & & & \text{Cl}(\wedge^3 \mathbb{Z}^6; D)
 \end{array}$$

Where arrows (3) and (5) are bijective, arrow (2) is injective, and arrow (4) is surjective, and the group  $\text{Cl}(\wedge^3 \mathbb{Z}^6; D)$  is trivial; Specifically in the language of ideal classes,

The arrow (1) maps  $(S, I, \delta)$  to  $(S, (I_1, I_2, I_2))$ , where  $I_2 = I$ ;

The arrow (2) maps  $(S, (I_1, I_2, I_2))$  to itself, which must be an inclusion;

The arrow (3) maps  $(S, (I_1, I_2, I_2))$  to  $(S, I_1)$ , which is a bijection;

The arrow (4) maps  $(S, (I_1, I_2, I_3))$  to  $(S, (I_1, I_2 \oplus I_3))$ , which is a surjective map;

The arrow (5) maps  $(S, (I, M))$  to  $(S, I)$ , which is a bijection;

The arrow (6) maps  $(S, (I, M))$  to  $(S, I \oplus M)$ , which is actually the zero map.

## 2 Higher Composition Law II

We study the action of the group  $\bar{\Gamma} = GL_2(\mathbb{Z}) \times GL_3(\mathbb{Z}) \times GL_3(\mathbb{Z})$  on the space of  $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$  on the pair of  $3 \times 3$  matrices, i.e. the space of pairs  $(A, B)$  of  $3 \times 3$  integer matrices. In fact, it suffices restrict the  $\bar{\Gamma}$ -action to the subgroup  $\Gamma = GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z})$ , since  $(-I_2, -I_3, I_3)$  and  $(-I_2, I_3, -I_3)$  in  $\bar{\Gamma}$  acts trivially on all pairs  $(A, B)$ . Moreover, the group  $\Gamma$  acts faithfully.

The action of  $SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z})$  on  $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$  has four independent invariants, namely the coefficients of the binary cubic form

$$f(x, y) = \det(Ax - By)$$

The group  $GL_2(\mathbb{Z})$  acts on the cubic form  $f(x, y)$ , and it is well-known that this action has exactly one polynomial invariant, namely the discriminant  $\text{Disc}(f)$  of  $f$ . Hence the unique  $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z}) \times SL_3(\mathbb{Z})$ -invariant on  $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$  is given by  $\text{Disc}(\det(Ax - By))$ . We call this fundamental invariant the discriminant of  $(A, B)$ , and denote it by  $\text{Disc}(A, B)$ .

(Let  $f = ax^3 + bx^2y + cxy^2 + dy^3$  be a binary cubic form. We define its discriminant to be  $\text{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$ . This comes from the symmetric polynomial  $a^4(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$ .)

If  $\text{Disc}(A, B)$  is nonzero, we say that  $(A, B)$  is a nondegenerate element of  $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ . Similarly, we call a binary cubic form  $f$  nondegenerate if  $\text{Disc}(f)$  is nonzero.

The parameterization of cubic ring: Let  $R$  be a cubic ring (i.e., any ring free of rank 3 as a  $\mathbb{Z}$ -module), and  $\langle 1, \omega, \theta \rangle$  be a  $\mathbb{Z}$ -basis for  $R$ . Translating  $\omega, \theta$  by the appropriate elements of  $\mathbb{Z}$ , we may assume that  $\omega \cdot \theta \in \mathbb{Z}$ . We call a basis satisfying the latter condition normalized or simply normal. If  $\langle 1, \omega, \theta \rangle$  is a normal basis, then there exist constants  $a, b, c, d, l, m, n \in \mathbb{Z}$  such that

$$\omega\theta = n, \omega^2 = m + b\omega - a\theta, \theta^2 = l + d\omega - c\theta$$

The associative law relations indicate that  $(n, m, l) = (-ad, -ac, -bd)$ . To the cubic ring with multiplication as above, we associate the binary cubic form  $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ , which implies the following theorem:

There is a canonical bijection between the set of  $GL_2(\mathbb{Z})$ -equivalence classes of integral binary cubic forms and the set of isomorphism classes of cubic rings by the association

$$f \leftrightarrow R(f)$$

Moreover,  $\text{Disc}(f) = \text{Disc}(R(f))$ . Here the discriminant of a free ring of rank  $n$  with  $\mathbb{Z}$ -basis  $\langle \alpha_1 = 1, \alpha_2, \dots, \alpha_n \rangle$  is defined as the determinant of the matrix  $(\text{Tr}(\alpha_i \alpha_j))_{1 \leq i, j \leq n}$ .

The symmetric elements in  $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$  are precisely the elements of  $\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$ , i.e., pairs  $(A, B)$  or symmetric  $3 \times 3$  integer matrices. The cubic form  $f = \det(Ax - By)$  and the discriminant  $\text{Disc}(A, B) = \text{Disc}(f) = \text{Disc}(\det(Ax - By))$  are defined as before. Again, we say an element  $(A, B) \in \mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$  is nondegenerate if  $\text{Disc}(A, B)$  is nonzero. The group  $GL_2(\mathbb{Z}) \otimes SL_3(\mathbb{Z})$  acts naturally over  $\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$ .

Consider the natural map

$$id \otimes \wedge_{3,3} : \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \rightarrow \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6$$

defined by sending

$$(A, B) \mapsto \left( \begin{bmatrix} & A \\ -A^t & \end{bmatrix}, \begin{bmatrix} & B \\ -B^t & \end{bmatrix} \right)$$

The resulting skew-symmetrized space  $\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6$  has a natural action by the group  $GL_2(\mathbb{Z}) \times SL_6(\mathbb{Z})$ , and this group action again possess a unique polynomial invariant. Indeed, a complete set of invariants for the action of  $SL_6(\mathbb{Z})$  on  $\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6$  is given by four coefficients of the binary cubic form

$$f(x, y) = \text{Pfaff}(\mathcal{A}x - \mathcal{B}y)$$

and so the unique  $GL_2(\mathbb{Z}) \times SL_6(\mathbb{Z})$ -invariant is given by  $\text{Disc}(\text{Pfaff}(\mathcal{A}x - \mathcal{B}y))$ , which again call the discriminant of  $(\mathcal{A}, \mathcal{B})$ . As usual, we say  $(\mathcal{A}, \mathcal{B}) \in \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6$  is nondegenerate if it has nonzero discriminant.

Now, let us discover the relations of these above with ideal classes in cubic rings.

Let  $R$  be a cubic ring. We say that a pair  $(I, I')$  of fractional  $R$ -ideals in  $K = R \otimes \mathbb{Q}$  is balanced if  $II' \subseteq R$  and  $N(I)N(I') = 1$ . Two balanced pairs  $(I_1, I'_1)$  and  $(I_2, I'_2)$  are called equivalence if there exists an invertible element  $\kappa \in K$  such that  $I_1 = \kappa I_2$  and  $I'_1 = \kappa^{-1} I'_2$ .

There is a canonical bijection between the set of nondegenerate  $\Gamma$ -orbits on the space  $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$  and the set of isomorphism classes of pairs  $(R, (I, I'))$ , where  $R$  is a nondegenerate cubic ring and  $(I, I')$  is an equivalence class of balanced pairs of ideals in  $R$ . Specifically, let  $\langle 1, \omega, \theta \rangle$  be a normal basis of  $R$ , and let  $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$  and  $\langle \beta_1, \beta_2, \beta_3 \rangle$  denote any  $\mathbb{Z}$ -basis for the ideals  $I$  and  $I'$  having the same orientation as  $\langle 1, \omega, \theta \rangle$ . ("Same orientation" means that the linear transformations that map  $\langle 1, \omega, \theta \rangle$  to  $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$  and  $\langle \beta_1, \beta_2, \beta_3 \rangle$  have positive determinant.) Since  $II' \subseteq R$ , we must have

$$\alpha_i \beta_j = c_{ij} + b_{ij} \omega + a_{ij} \theta$$

for some set of 27 integers  $a_{ij}, b_{ij}$  and  $c_{ij}$ , where  $i, j \in \{1, 2, 3\}$ . Let  $A$  and  $B$  denote the  $3 \times 3$  matrices  $(a_{ij})$  and  $(b_{ij})$  respectively. Then  $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$  is our desired pair of  $3 \times 3$  matrices.

Under this bijection, the discriminant of an integer  $2 \times 3 \times 3$  box equals the discriminant of the corresponding cubic ring. This bijection restricts to correspondence

$$\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f) \leftrightarrow \text{Cl}(R(f))$$

which provides a composition law on the left side and becomes a group isomorphism. In particular, when  $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ , the identity element of  $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f)$  could be written as

$$(A, B) = \left( \begin{bmatrix} & & 1 \\ -a & & \\ 1 & & -c \end{bmatrix}, \begin{bmatrix} & 1 \\ 1 & b \\ & d \end{bmatrix} \right)$$

There is a canonical bijection between the set of nondegenerate  $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ -orbits on the space  $\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$  and the set of equivalence classes of triples  $(R, I, \delta)$ , where  $R$  is a nondegenerate cubic ring,  $I$  is an ideal of  $R$ , and  $\delta$  is an invertible element of  $R \otimes \mathbb{Q}$  such that  $I^2 \subseteq (\delta)$  and  $N(\delta) = N(I)^2$ . Specifically, for a triple  $(R, I, \delta)$  as above, we first show how to construct a corresponding pair  $(A, B)$  of ternary quadratic forms. Let  $\langle 1, \omega, \theta \rangle$  denote a normal basis of  $R$ , and let  $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$  denote a  $\mathbb{Z}$ -basis of the ideal  $I$  having the same orientation as  $\langle 1, \omega, \theta \rangle$ . Since by hypothesis  $I$  is an ideal whose square is contained in  $\delta R$ , we must have

$$\alpha_i \alpha_j = \delta(c_{ij} + b_{ij}\omega + a_{ij}\theta)$$

for some set of integers  $a_{ij}, b_{ij}$  and  $c_{ij}$ . Let  $A = (a_{ij})$  and  $B = (b_{ij})$  denote the  $3 \times 3$  symmetric matrices. Then, the ordered pair  $(A, B) \in \mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3$  is our desired pair of ternary quadratic forms.

Under this bijection, the discriminant of a pair of ternary quadratic forms equals the discriminant of the corresponding cubic ring. This bijection is restricted to a surjective map

$$\text{Cl}(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3; f) \rightarrow \text{Cl}_2(R(f))$$

which provides a composition law on the left side and therefore, becomes a group homomorphism.

We consider rank 2 modules  $M$  over  $R$  that could be embedded into  $K \oplus K$ , here  $K = R \otimes \mathbb{Q}$ . We say a rank 2 ideal  $M \subset K \oplus K$  is balanced if  $\det(M) \subseteq R$  and  $N(M) = 1$ . Two such ideals are equivalent if one could be mapped into the other ideal via an element of  $SL_2(K)$ . There is a canonical bijection between the set of nondegenerate  $GL_2(\mathbb{Z}) \otimes SL_6(\mathbb{Z})$ -orbits on the space  $\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6$ , and the set of isomorphism classes of pairs  $(R, M)$ , where  $R$  is a nondegenerate cubic ring and  $M$  is an equivalence class of balanced pairs having rank 2. As before, this bijection preserves discriminant from both sides. In particular, suppose  $R = \langle 1, \omega, \theta \rangle$ , and  $M = \langle \alpha_1, \dots, \alpha_6 \rangle$  denote an appropriately oriented  $\mathbb{Z}$ -basis. We may write

$$\det(\alpha_i, \alpha_j) = c_{ij} + b_{ij}\omega + a_{ij}\theta$$

for some integers  $c_{ij}, b_{ij}, a_{ij}$  satisfying

$$c_{ij} = -c_{ji}, b_{ij} = -b_{ji}, a_{ij} = -a_{ji}$$

for all  $i, j \in \{1, 2, 3, 4, 5, 6\}$ . Let  $\mathcal{A} = (a_{ij}), \mathcal{B} = (b_{ij})$ , and the pair  $(\mathcal{A}, \mathcal{B})$  is what we want. This fact indicates that the group  $\text{Cl}(\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6; f)$  is trivial for all cubic forms  $f$ . In particular, if  $f$  corresponds to the ring of integers in a cubic field, then there is only one element  $(\mathcal{A}, \mathcal{B}) \in \mathbb{Z}$ , up to  $SL_6(\mathbb{Z})$ -equivalence, whose binary cubic form invariant  $\det(\mathcal{A}x - \mathcal{B}y)$  is  $f(x, y)$ . This unique element is given by  $id \otimes \wedge_{3,3}(A, B)$ , where  $(A, B)$  is the identity element of  $\text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f)$  (see above).

Finally, let us summarize this whole section. We have natural discriminant-preserving inclusions

$$\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3 \rightarrow \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \rightarrow \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6$$

The former arrow maps symmetric matrices  $(A, B)$  to itself; And the latter arrow maps  $(A, B)$  to  $(\begin{bmatrix} & A \\ -A^t & \end{bmatrix}, \begin{bmatrix} & B \\ -B^t & \end{bmatrix})$ .

These arrows above lead to the group homomorphisms

$$\text{Cl}(\mathbb{Z}^2 \otimes \text{Sym}^2 \mathbb{Z}^3; f) \rightarrow \text{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f) \rightarrow \text{Cl}(\mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6; f)$$

Where the former arrow maps  $(R, I, \delta)$  to  $(R, (I, I\delta^{-1}))$ ; The latter arrow maps  $(R, (I, I'))$  to  $(R, (I \oplus I'))$ , which is actually the zero map.

### 3 Higher Composition Law III

The main goal of this paper is to prove the following theorem:

There is a canonical bijection between the set of  $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$ -orbits on the space  $(\text{Sym}^2 \mathbb{Z}^3)^* \otimes \mathbb{Z}^2$  or pairs of integral ternary quadratic forms and the set of isomorphism classes of  $(Q, R)$ , where  $Q$  is a quartic ring and  $R$  is a cubic resolvent ring of  $Q$ .

Here an element  $(g_3, g_2) \in G_{\mathbb{Z}} = GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$  operates by sending  $(A, B)$  to

$$(g_3, g_2)(A, B) = (rg_3Ag_3^t + sg_3Bg_3^t, tg_3Ag_3^t + ug_3Bg_3^t)$$

where we written  $g_2$  as  $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$ .

Furthermore, this bijection also leads to the following corollaries:

(a) There is a canonical bijection between isomorphism classes of nontrivial quartic rings and  $GL_3(\mathbb{Z}) \times GL_2^{\pm 1}(\mathbb{Q})$ -equivalence classes of pairs  $(A, B)$  of integral ternary quadratic forms where  $A$  and  $B$  are linearly independent over  $\mathbb{Q}$ . Here "trivial quartic ring" refers to the ring  $\mathbb{Z} + \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3$  with all  $x_i x_j = 0$ , and  $GL_2^{\pm 1}(\mathbb{Q})$  is the subgroup of  $GL_2(\mathbb{Q})$  having discriminant  $\pm 1$ . This corollary indicates that two pairs of ternary quadratic forms are associated to the same quartic ring if and only if they are related by a transformation in the group  $GL_2^{\pm 1}(\mathbb{Q})$ .

(b) There is a canonical bijection between the primitive quartic rings and  $GL_2(\mathbb{Z}) \times GL_2(\mathbb{Q})$ -equivalence classes of pairs  $(A, B)$  of integral ternary forms where  $A$  and  $B$  are linearly independent over  $\mathbb{Q}$ . Here we define the content of the ring  $Q$  as the maximal integer  $n$  such that there exists a ring  $T$  that satisfies

$$Q = \mathbb{Z} + nT$$

and "primitive" means that the ring has content 1. This corollary states that primitive quartic rings correspond to pairs  $(M, V)$ , where  $M$  is a free  $\mathbb{Z}$ -module of rank 3 and  $V$  is a two-dimensional rational subspace of the (six-dimensional) vector space of  $Q$ -valued quadratic forms on  $M$ . Equivalently, primitive quartic rings  $Q$  correspond to pairs  $(M, \Lambda)$ , where  $\Lambda$  is a maximal two-dimensional lattice of  $\mathbb{Z}$ -valued quadratic forms on  $M$ .

Now let us define the  $S_k$ -closure of a ring of rank  $k$ . Let  $R$  be a ring of rank  $k$  with basis  $\langle \alpha_1 = 1, \dots, \alpha_k \rangle$ . Then the discriminant of  $R$  is defined as the determinant of the matrix  $(\text{Tr}(\alpha_i \alpha_j))_{1 \leq i, j \leq k}$ . Suppose  $R$  has nonzero discriminant, and let  $R^{\otimes k}$  denote the  $k$ th tensor power  $R^{\otimes k} = R \otimes_{\mathbb{Z}} R \otimes_{\mathbb{Z}} \dots \otimes_{\mathbb{Z}} R$  of  $R$ . Then  $R^{\otimes k}$  is seen to be a ring of rank  $k^k$ . Denote by  $I_R$  the ideal in  $R^{\otimes k}$  generated by all elements of the form

$$(x \otimes 1 \otimes \dots \otimes 1) + (1 \otimes x \otimes \dots \otimes 1) + \dots + (1 \otimes 1 \otimes \dots \otimes x) - \text{Tr}(x)$$

and let  $J_R$  denote the  $\mathbb{Z}$ -saturation of the ideal  $I_R$ ; i.e., let

$$J_R = \{r \in R^{\otimes k} : nr \in I_R \text{ for some } n \in \mathbb{Z}\}$$

for  $x \in R$ . The  $S_k$ -closure of a ring  $R$  of rank  $k$  is the ring  $\bar{R}$  given by  $R^{\otimes k}/J_R$ .

To introduce the cubic resolvent of a quartic ring, let us first consider the quadratic resolvent of a For a cubic ring  $R$ , the quadratic resolvent ring  $S^{\text{res}}(R)$  of  $R$  is the unique quadratic ring  $S$  such that  $\text{Disc}(R) = \text{Disc}(S)$ .

Give a cubic ring  $R$ , there is a natural map from  $R$  to its quadratic resolvent ring that preserves discriminants. Indeed, for an element  $x \in R$ , let  $x, x', x''$  denote the  $S_3$ -conjugate of  $x$  in the  $S_3$  closure  $\bar{R}$  of  $R$ . Then the element

$$\tilde{\phi}_{3,2}(x) = \frac{[(x - x')(x' - x'')(x'' - x)]^2 + (x - x')(x' - x'')(x'' - x)}{2}$$

is contained in some quadratic ring, and  $\tilde{\phi}_{3,2}(x)$  has the same discriminant as  $x$ . We define the quadratic invariant ring

$$S^{\text{inv}}(R) = \mathbb{Z}[\{\tilde{\phi}_{3,2}(x) : x \in R\}]$$

We must have  $S^{\text{inv}}(R) \subseteq S$ , and the order will be discussed later. The map  $\tilde{\phi}_{3,2}$  descends to the mapping

$$\phi_{3,2} : R/\mathbb{Z} \rightarrow S/\mathbb{Z}$$

as a map of  $\mathbb{Z}$ -modules, thus well defined as an integral binary cubic form up to  $GL_2(\mathbb{Z}) \times GL_1(\mathbb{Z})$ -equivalence.

Now let us consider the case when  $Q$  is a quartic ring. Define a function  $\tilde{\phi}_{4,3}$  over  $\bar{Q}$  as

$$\tilde{\phi}_{4,3}(x) = xx' + x''x'''$$

And define

$$R^{\text{inv}}(Q) = \mathbb{Z}[\{\tilde{\phi}_{4,3}(x) : x \in Q\}]$$

Here we carry out the definition of the cubic resolvent ring of  $Q$ . A cubic resolvent ring  $R$  of  $Q$  is a cubic ring  $R$  such that  $\text{Disc}(Q) = \text{Disc}(R)$  and  $R \supseteq R^{\text{inv}}(Q)$ . The order will be discussed later. Note that the cubic resolvent ring must exist but might not be unique.

The map  $\tilde{\phi}_{4,3}$  descends to

$$\phi_{4,3} : Q/\mathbb{Z} \rightarrow R/\mathbb{Z}$$

As a map between  $\mathbb{Z}$ -modules, this map is a quadratic map from  $\mathbb{Z}^3$  to  $\mathbb{Z}^2$  and thus corresponds to a pair of integral ternary quadratic forms, well defined up to  $GL_3(\mathbb{Z}) \times GL_2(\mathbb{Z})$ -equivalence. This indicates that isomorphism classes of quartic rings should be parametrized roughly by pairs of integral ternary quadratic forms up to integer equivalence.

Finally, we directly write down the bijection mentioned at the beginning of this section.

On one hand, let  $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$  and  $\langle 1, \omega_1, \omega_2 \rangle$  be bases for  $Q$  and  $R$  respectively such that the map  $\phi_{4,3}$  is given by

$$\phi_{4,3}(t_1\bar{\alpha}_1 + t_2\bar{\alpha}_2 + t_3\bar{\alpha}_3) = B(t_1, t_2, t_3)\bar{\omega}_1 + A(t_1, t_2, t_3)\bar{\omega}_2$$



where  $\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3, \bar{\omega}_1, \bar{\omega}_2$  denote the reductions modulo  $\mathbb{Z}$  of  $\alpha_1, \alpha_2$ . Then the matrices  $(A, B) \in (\text{Sym}^2 \mathbb{Z}^3)^* \otimes \mathbb{Z}^2$  are the pair we want;

On the other hand, suppose we are given the pair  $(A, B) \in (\text{Sym}^2 \mathbb{Z}^3)^* \otimes \mathbb{Z}^2$  of integral ternary quadratic forms. Writing out the pair  $(A, B)$  of ternary quadratic forms as

$$A(x_1, x_2, x_3) = \sum_{1 \leq i, j \leq 3} a_{ij} x_i x_j$$

$$B(x_1, x_2, x_3) = \sum_{1 \leq i, j \leq 3} b_{ij} x_i x_j$$

and letting  $a_{ji} = a_{ij}$  and  $b_{ji} = b_{ij}$ , define the constants  $\lambda_{kl}^{ij} = \lambda_{kl}^{ij}(A, B)$  by

$$\lambda_{kl}^{ij}(A, B) = \begin{vmatrix} a_{ij} & b_{ij} \\ a_{kl} & b_{kl} \end{vmatrix}$$

the  $\lambda_{kl}^{ij}$  thus take up to 15 possible nonzero values up to sign.

Let  $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$  and  $\langle 1, \omega_1, \omega_2 \rangle$  be bases for  $Q$  and  $R$  respectively. We write out the multiplication law of  $Q$  explicitly as

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^3 c_{ij}^k \alpha_k$$

where  $c_{ij}^k \in \mathbb{Z}$  for  $i, j \in \{1, 2, 3\}$  and  $k \in \{0, 1, 2, 3\}$ , then the condition that the basis is normal is equivalent to

$$c_{12}^1 = c_{12}^2 = c_{13}^1 = 0$$

For any permutation  $(i, j, k)$  of  $(1, 2, 3)$ , we have

$$c_{ii}^i = \pm \lambda_{ij}^{ik} + C_i, c_{ii}^j = \pm \lambda_{ik}^{ii}$$

$$c_{ij}^i = \pm \frac{1}{2} \lambda_{jj}^{ik} + \frac{1}{2} C_j, c_{ij}^k = \pm \lambda_{ii}^{jj}$$

where we have used  $\pm$  to denote the sign of the permutation  $(i, j, k)$  of  $(1, 2, 3)$ , and where the constants  $C_i$  are given by

$$C_1 = \lambda_{11}^{23}, C_2 = -\lambda_{22}^{13}, C_3 = \lambda_{33}^{12}$$

Finally, we write the formula for  $c_{ij}^0$ :

$$c_{ij}^0 = \sum_{i=1}^3 (c_{kk}^r c_{ri}^k - c_{ij}^r c_{rk}^k)$$

for any  $k \neq i$ , which ends up the construction of  $Q$ ; We also write out the multiplication law of  $R$  as

$$\omega_1 \omega_2 = -ad, \omega_1^2 = -ac + b\omega_1 - a\omega_2, \omega_2^2 = -bd + d\omega_1 - c\omega_2$$

where the constants  $a, b, c, d$  satisfies

$$ax^3 + bx^2y + cxy^2 + dy^3 = 4 \det(Ax + By)$$

which gives the construction of  $R$ . One could verify that the maps between  $(Q, R)$  and  $(A, B)$  are reciprocal inverse mapping, and  $R = R(A, B)$  is indeed the cubic resolvent of  $Q = Q(A, B)$ . Therefore we are done. Furthermore, the bijection is also discriminant preserving. i.e.,  $\text{Disc}(Q) = \text{Disc}(R) = \text{Disc}(A, B)$ . Here the discriminant of the pair  $(A, B)$  is defined to be

$$\text{Disc}(4 \cdot \det(Ax + By))$$

Notice that this definition is different from the definition appeared in Section 2.

We also define the content  $\text{ct}(A, B)$  of a pair  $(A, B)$  of integral binary forms to be the content of the corresponding quartic ring, i.e.,

$$\text{ct}(A, B) = \text{ct}(Q(A, B)) = \gcd\{\lambda_{kl}^{ij}(A, B)\}$$

We have the following statement that gives the formula for orders:

(a) Let  $R$  be a cubic ring,  $S^{\text{inv}}(R)$  be the quadratic invariant ring of  $R$ , and  $S$  the quadratic resolvent ring of  $R$ . Then  $[S : S^{\text{inv}}(R)] = \epsilon(R)\text{ct}(R)$ , where  $\epsilon(R) = 2$  if  $R = \mathbb{Z} + \text{ct}(R)R_1$  with  $R_1 \otimes \mathbb{Z}^2 \cong \mathbb{Z}_2^3$ , and  $\epsilon(R) = 1$  otherwise. In particular,  $S^{\text{inv}}(R) = S$  if and only if  $R$  is primitive and  $R \otimes \mathbb{Z}^2$  is not isomorphic to  $\mathbb{Z}_2^3$ .

(b) Let  $Q$  be a quartic ring,  $R^{\text{inv}}(Q)$  be the cubic invariant ring of  $Q$ , and  $R$  be any cubic resolvent ring of  $Q$ . Then  $[R : R^{\text{inv}}(Q)] = \text{ct}(Q)$ . In particular,  $R^{\text{inv}}(Q) = R$  if and only if  $Q$  is primitive.

An alternative description of cubic resolvent that does not involve the notion of  $S_k$ -closure: Let  $Q$  be a quartic ring,  $R$  a cubic ring, and  $\xi : \wedge^3(Q/\mathbb{Z}) \rightarrow \wedge^2(R/\mathbb{Z})$  an isomorphism. Then we call a quadratic map  $\phi : Q/\mathbb{Z} \rightarrow R/\mathbb{Z}$  a resolvent mapping if

(a) The identity

$$\xi(x \wedge y \wedge xy) = \phi(x) \wedge \phi(y)$$

holds for all  $x, y \in Q$ ;

(b) The identity

$$[\text{Disc}(\phi)]z = z \wedge z^2$$

holds for all  $z \in R$ . Here  $\text{Disc}(\phi) = \eta \circ \text{disc} \circ \phi$ , and  $\eta = \xi^{*-1} \otimes \xi^{*-1} \otimes \iota$ . See the paper for details.

Let  $Q$  be a quartic ring. A cubic resolvent ring of  $Q$  is a cubic ring  $R$  equipped with an isomorphism  $\xi : \wedge^3(Q/\mathbb{Z}) \rightarrow \wedge^2(R/\mathbb{Z})$  and a resolvent mapping  $\phi : Q/\mathbb{Z} \rightarrow R/\mathbb{Z}$ .

With these definitions, the theorem at the beginning of the section immediately extends to cases of zero discriminant.

A quartic ring  $Q$  with a nonzero discriminant is said to be maximal if it is not a subring of any other quartic ring. (This definition comes from the ring of integers in a number field.)

$Q$  is maximal if and only if it is maximal at every prime  $p$ . If  $Q$  is not maximal at  $p$ , then there exists a  $\mathbb{Z}$ -basis  $\langle 1, \alpha_1, \alpha_2, \alpha_3 \rangle$  of  $Q$  such that at least one of the following is true:

- (1)  $\mathbb{Z} + \mathbb{Z}(\alpha_1/p) + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3$  forms a ring;
- (2)  $\mathbb{Z} + \mathbb{Z}(\alpha_1/p) + \mathbb{Z}(\alpha_2/p) + \mathbb{Z}\alpha_3$  forms a ring;
- (3)  $\mathbb{Z} + \mathbb{Z}(\alpha_1/p) + \mathbb{Z}(\alpha_2/p) + \mathbb{Z}(\alpha_3/p)$  forms a ring.

We can translate the conditions (1)(2)(3) into the conditions respectively on the  $\lambda$ -invariants of  $(A, B)$ :

- (1)  $\lambda_{22}^{11}, \lambda_{23}^{11}, \lambda_{33}^{11}, \lambda_{23}^{12}$  are multiples of  $p$ , and  $\lambda_{12}^{11}, \lambda_{13}^{11}$  are multiples of  $p^2$ ;
- (2)  $\lambda_{22}^{11}, \lambda_{23}^{11}, \lambda_{13}^{12}, \lambda_{23}^{12}, \lambda_{22}^{13}, \lambda_{23}^{22}$  are multiples of  $p$ , and  $\lambda_{12}^{11}, \lambda_{22}^{11}, \lambda_{22}^{12}$  are multiples of  $p^2$ ;
- (3) All the  $\lambda_{kl}^{ij}$ 's are multiples of  $p$ .

Now we want to understand those pairs  $(A, B)$  or integral ternary quadratic forms corresponding to maximal orders in quartic fields. To be specific, we consider pairs  $(A, B)$  or ternary quadratic forms over the  $p$ -adic ring  $\mathbb{Z}_p$  and its residue field  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . The intersection condition of the two conics related to  $A$  and  $B$  actually gives information about whether  $Q$  is maximal at  $p$ . (Here we consider the projective space  $\mathbb{P}_{\mathbb{F}_p}^2$  and view  $A$  and  $B$  as projective curves.) Let  $\mathcal{U}_p$  denote the subset of elements  $(A, B)$  such that  $Q = Q(A, B)$  is maximal at  $p$ . In fact, the measure of  $\mathcal{U}_p$  could be written as

$$\mu(\mathcal{U}_p) = (p-1)^4 p(p+1)^2 (p^2+p+1)(p^3+p^2+2p+1)/p^{12}$$

See the paper for more details that we omit here.

## 4 Higher Composition Law IV

The main goal of this paper is to prove the following theorem:

There is a canonical bijection between the set of  $GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ -orbits on the space of  $\mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$  of quadruples of  $5 \times 5$  skew-symmetric matrices and the set of isomorphism classes of pairs  $(R, S)$ , where  $R$  is a quintic ring and  $S$  is a sextic resolvent ring of  $R$ .

Here an element  $(g_4, g_5) \in G_{\mathbb{Z}} = GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$  operates by sending  $A = (A_1, A_2, A_3, A_4)$  to

$$(g_4, g_5)(A_1, A_2, A_3, A_4)^t = g_4(g_5 A_1 g_5^t, g_5 A_2 g_5^t, g_5 A_3 g_5^t, g_5 A_4 g_5^t)^t$$

Let  $R$  be a quintic ring, and  $\langle 1, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$  be a  $\mathbb{Z}$ -basis of  $R$ . The definition of  $S_5$ -closure  $\bar{R}$  of  $R$  is the same as Section 3.

Consider the six fundamental index 6 subgroups  $M(1), \dots, M(6)$  in  $S_5$ , called the metacyclic subgroups. Each of these subgroups is generated by a 5-cycle and a 4-cycle. For  $M(1) = \langle (12345), (2354) \rangle$ ,  $M(2) = \langle (12354), (3254) \rangle$ , while  $M^{(2+i)}$  ( $1 \leq i \leq 4$ ) is obtained by conjugating  $M^{(2)}$  by the 5-cycle  $(12345)^i$ . These six metacyclic groups form a set of conjugate subgroups.

For simplicity, we shall write  $M = M^{(1)}$ . The ring  $\bar{R}^M$  fixed pointwise by the action of  $M$  is evidently a ring of rank 6 (i.e., a sextic ring), which we call the sextic invariant ring and denote  $S^{\text{inv}}(R)$ . We will be looking for the sextic resolvent ring of  $R$  inside the sextic  $\mathbb{Q}$ -algebra  $S^{\text{inv}}(R) \otimes \mathbb{Q}$ . (Unfortunately, unlike Section 3, the order is not known in this case.)

Let  $\langle x, y \rangle_R = \text{Tr}_{\mathbb{Z}}^R(xy)$  be a symmetric quadratic form on  $R$ , and  $\langle \alpha_0^*, \alpha_1^*, \alpha_2^*, \alpha_3^*, \alpha_4^* \rangle$  denote the dual basis of  $\langle \alpha_0 = 1, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$  with respect to this pairing. We write  $R^*$  for the  $\mathbb{Z}$ -dual of  $R$  with  $\mathbb{Z}$ -basis  $\alpha_0^*, \alpha_1^*, \alpha_2^*, \alpha_3^*, \alpha_4^*$ . A sextic resolvent of  $R$  is a rank 6 sublattice  $S \subset \bar{R}^M \otimes \mathbb{Q}$  such that  $\text{Disc}(S) = (16\text{Disc}(R))^3$ , and such that any one of the following equivalent conditions holds:

(a)  $f(x, y, z) \in \tilde{R}$  for every  $x, y, z \in S$ . Here  $\tilde{R} = \mathbb{Z}\alpha_1^* + \mathbb{Z}\alpha_2^* + \mathbb{Z}\alpha_3^* + \mathbb{Z}\alpha_4^* \subset R^*$  is a sublattice, and  $f : S \times S \times S \rightarrow R^*$  with the form

$$f(x, y, z) = \frac{1}{16\text{Disc}(R)} \begin{vmatrix} x^{(1)} - x^{(2)} & x^{(3)} - x^{(6)} & x^{(4)} - x^{(5)} \\ y^{(1)} - y^{(2)} & y^{(3)} - y^{(6)} & y^{(4)} - y^{(5)} \\ z^{(1)} - z^{(2)} & z^{(3)} - z^{(6)} & z^{(4)} - z^{(5)} \end{vmatrix}$$

Here for  $s \in S$ ,  $s^{(1)}, s^{(2)}, \dots, s^{(6)}$  denote the conjugates of  $s \in \bar{R} \otimes \mathbb{Q}$ , labelled so that they are stabilized by  $M^{(1)}, M^{(2)}, \dots, M^{(6)}$  respectively;

(b) Let  $\langle \beta_0 = 1, \beta_1, \dots, \beta_5 \rangle$  denote a  $\mathbb{Z}$ -basis of  $S$ , and  $S^*$  be the  $\mathbb{Z}$ -dual for  $S$  with dual basis  $\langle \beta_0^*, \beta_1^*, \dots, \beta_5^* \rangle$ . Let  $\tilde{S} = \mathbb{Z}\beta_1^* + \dots + \mathbb{Z}\beta_5^* \subset S^*$  be a sublattice. Then this condition states that  $g(u, v) \in \tilde{R}$  for every  $u, v \in \tilde{S}$ . Here  $g : \tilde{S} \times \tilde{S} \rightarrow \tilde{R}$  has the form

$$g(u, v) = \frac{\sqrt{\text{Disc}(S)}}{48\text{Disc}(R)} \begin{vmatrix} 1 & 1 & 1 \\ u^{(1)} + u^{(2)} & u^{(3)} + u^{(6)} & u^{(4)} + u^{(5)} \\ v^{(1)} + v^{(2)} & v^{(3)} + v^{(6)} & v^{(4)} + v^{(5)} \end{vmatrix}$$

Where  $\sqrt{\text{Disc}(S)}$  is defined analogously to  $\sqrt{\text{Disc}(R)}$ , namely, as  $\det[(\beta_i^{(m)})_{0 \leq i, m-1 \leq 5}]$ ;

- (c)  $\text{Tr}(\alpha \cdot f(x, y, z)) \in \mathbb{Z}$  for every  $\alpha \in R$  and  $x, y, z \in S$ ;  
(d)  $\text{Tr}(\alpha \cdot g(u, v)) \in \mathbb{Z}$  for every  $\alpha \in R$  and  $u, v \in \tilde{S}$ .

Notice that the definition of  $S$  above only gives a lattice structure on  $S$ . However, we could prove that it is actually a ring.

Finally, we directly write down the bijection mentioned at the beginning of this section.

On one hand, let  $\langle 1, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$  and  $\langle 1, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5 \rangle$  be bases for  $Q$  and  $R$  respectively. We keep the notations as above and write

$$g(\beta_i^*, \beta_j^*) = a_{1ij}\alpha_1^* + a_{2ij}\alpha_2^* + a_{3ij}\alpha_3^* + a_{4ij}\alpha_4^*$$

Then the set of forty integers  $A = \{a_{rij}\}_{1 \leq i \leq 4, 1 \leq i < j \leq 5}$  gives the element of  $\mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$  we desired.

On the other hand, suppose we are given  $A = (A_1, A_2, A_3, A_4) = (a_{rij}) \in \mathbb{Z}^4 \otimes \wedge^2 \mathbb{Z}^5$ . For any  $X \in \wedge^2 \mathbb{Z}^5$  and  $1 \leq i \leq 5$ , define the  $i$ th  $4 \times 4$  signed sub-Pfaffian  $Q_i$  of  $X$  to be the  $(-1)^{i+1}$  times the Pfaffian of the  $4 \times 4$  principal submatrix obtained from  $X$  by removing its  $i$ th row and column. Let

$$Q[X] = [Q_1, \dots, Q_5]^t$$

be the column vector of signed  $4 \times 4$  sub-Pfaffians of  $X$ . Let  $Q(X, Y)$  denote the corresponding symmetric bilinear form such that  $Q(X, X) = 2Q(X)$ . To be specific,  $2Q(X, Y) = Q(X + Y, X + Y) - Q(X, X) - Q(Y, Y)$  implies  $Q(X, Y) = Q(X + Y) - Q(X) - Q(Y)$ . For  $i, j, k, l, m \in \{1, 2, 3, 4\}$ , let us use the shorthand

$$\{ijklm\} = Q(A_i, A_j)^t \cdot A_k \cdot Q(A_l, A_m)$$

We write out the multiplication law of  $R$  explicitly as

$$\alpha_i \alpha_j = c_{ij}^0 + \sum_{k=1}^4 c_{ij}^k \alpha_k$$

for  $1 \leq i, j \leq 4$ . The normal basis assumption implies that

$$c_{12}^1 = c_{12}^2 = c_{34}^3 = c_{34}^4 = 0$$

For any permutation  $(i, j, k, l)$  of  $(1, 2, 3, 4)$ , we have

$$\begin{aligned} c_{ij}^k &= \pm \{iiljj\}/4 \\ c_{ii}^j &= \pm \{liiik\} \\ c_{ij}^j - c_{ik}^k &= \pm \{jklji\}/2 \\ c_{ii}^j - c_{ij}^j - c_{ik}^k &= \pm \{ijlki\} \end{aligned}$$

and also the equality

$$c_{ij}^0 = \sum_{i=1}^4 (c_{jk}^r c_{ri}^k - c_{ij}^r c_{rk}^k)$$

for any  $k \neq i$ . This marks the ending of the construction of the multiplication law of  $R$ . And now let us turn to the ring structure of  $S = \langle 1, \beta_1, \dots, \beta_5 \rangle$ :

$$\beta_i \beta_j = d_{ij}^0 + \sum_{k=1}^5 d_{ij}^k \beta_k$$

Define invariants  $D_{ij}^k = D_{ij}^k(A)$  for  $A$  by

$$D_{ij}^k = \frac{1}{2304} \sum [\sigma(il'_1 l'_2 k'_3 l'_3) \sigma(jl''_1 l''_2 k''_3 l''_3) \sigma(k'_1 l_1 l_2 k_3 l_3) \sigma(k''_1 k'_2 k'_4 l'_4 l''_4) \sigma(k_2 k''_2 k_4 k''_4 l_4) \\ \cdot \delta(k, l_1; k_2, l_2; k_3, l_3; k_4, l_4) \delta(k'_1, l'_1; k'_2, l'_2; k'_3, l'_3; k'_4, l'_4) \delta(k''_1, l''_1; k''_2, l''_2; k''_3, l''_3; k''_4, l''_4)]$$

Where we have used  $\sigma(n_1, \dots, n_5)$  to denote the sign of the permutation  $(n_1, \dots, n_5)$  of  $(1, 2, 3, 4, 5)$ , and

$$\delta(i_1, j_1; i_2, j_2; i_3, j_3; i_4, j_4) = \begin{vmatrix} a_{1i_1 j_1} & a_{2i_1 j_1} & a_{3i_1 j_1} & a_{4i_1 j_1} \\ a_{1i_2 j_2} & a_{2i_2 j_2} & a_{3i_2 j_2} & a_{4i_2 j_2} \\ a_{1i_3 j_3} & a_{2i_3 j_3} & a_{3i_3 j_3} & a_{4i_3 j_3} \\ a_{1i_4 j_4} & a_{2i_4 j_4} & a_{3i_4 j_4} & a_{4i_4 j_4} \end{vmatrix}$$

Let

$$\begin{aligned} d_{ij}^k &= D_{ij}^k \\ d_{ii}^j &= D_{ii}^j \\ d_{ij}^j - d_{ik}^k &= D_{ij}^j - D_{ik}^k \\ d_{ii}^i - d_{ij}^j - d_{ik}^k &= D_{ii}^i - D_{ij}^j - D_{ik}^k \end{aligned}$$

Also, we may assume

$$d_{12}^1 = d_{12}^2 = d_{34}^3 = d_{34}^4 = d_{45}^4 = 0$$

And finally, we obtain

$$d_{ij}^0 = \sum_{r=1}^5 (d_{jk}^r d_{ri}^k - d_{ij}^r d_{rk}^k)$$

for any  $k \neq i$ , which gives the construction of  $S$ . One could verify that the maps between  $(R, S)$  and  $A = (A_1, A_2, A_3, A_4)$  are reciprocal reverse mapping, and  $S = S(A)$  is indeed the sextic resolvent of  $R = R(A)$ . Therefore we are done. Furthermore, the bijection is also discriminant preserving, i.e.,  $\text{Disc}(A) = \text{Disc}(R) = \frac{1}{16} \text{Disc}(S)^{1/3}$ . Here the discriminant of  $A$  is defined to be equal to the discriminant of  $R = R(A)$ , and therefore the first = must holds.

Consider the classical resolvent map

$$\psi : R \rightarrow \tilde{S} \times \mathbb{Q}$$

defined by  $\psi(\alpha) = \frac{1}{\sqrt{\text{Disc}(R)}}(\alpha^{(1)}\alpha^{(2)} + \alpha^{(2)}\alpha^{(3)} + \alpha^{(3)}\alpha^{(4)} + \alpha^{(4)}\alpha^{(5)} + \alpha^{(5)}\alpha^{(1)} - \alpha^{(1)}\alpha^{(3)} - \alpha^{(3)}\alpha^{(5)} - \alpha^{(5)}\alpha^{(2)} - \alpha^{(2)}\alpha^{(4)} - \alpha^{(4)}\alpha^{(1)})$ . Let  $t = (t_1, t_2, t_3, t_4) \in \mathbb{Z}^4$  and  $\alpha(t) = t_1\alpha_1 + t_2\alpha_2 + t_3\alpha_3 + t_4\alpha_4 \in R/\mathbb{Z}$ . Then we have the following equation

$$\psi(\alpha(t)) = 4Q_1(t)\tilde{\beta}_1 + \dots + 4Q_5(t)\tilde{\beta}_5$$

Which links the entries of the  $4 \times 4$ -Pfaffians and the resolvent map. Moreover, the image of  $\psi$  lies not only in  $\tilde{S} \otimes \mathbb{Q}$ , but in  $\tilde{S}$  itself! Therefore, the map  $\psi$  also descends to

$$\bar{\psi} : R/\mathbb{Z} \rightarrow \tilde{S}$$

An alternative description of cubic resolvent that does not involve the notion of  $S_k$ -closure: Let  $Q$  be a quintic ring and  $S$  a sextic ring. We call a  $\mathbb{Z}$ -linear map  $\phi : R/\mathbb{Z} \rightarrow \wedge^2(S/\mathbb{Z})$  a sextic resolvent ring if  $R(\phi) = R$  and  $S(\phi) = S$ . (The ring  $R(\phi)$  and  $S(\phi)$  are obtained by the way we already introduced.)

Let  $R$  be a quintic ring. A sextic resolvent ring of  $R$  is a sextic ring  $S$  equipped with a sextic resolvent mapping  $\phi : R/\mathbb{Z} \rightarrow \wedge^2(S/\mathbb{Z})$ .

With these definitions, the theorem at the beginning of the section immediately extends to cases of zero discriminant.

A quintic ring  $R$  with a nonzero discriminant is said to be maximal if it is not a subring of any other quintic ring. (This definition comes from the ring of integers in a number field.)  $R$  is maximal if and only if it is maximal at every prime  $p$ . This part is similar to the quartic case, except that we consider the intersection of the sub-Pfaffians in  $\mathbb{P}_{\mathbb{F}_p}^3$  (and not the skew-symmetric matrices). Let  $\mathcal{U}_p$  denote the subset of elements  $A = (A_1, A_2, A_3, A_4)$  such that  $R = R(A)$  is maximal at  $p$ . In fact, the measure of  $\mathcal{U}_p$  could be written as

$$\mu(\mathcal{U}_p) = (p-1)^8 p^{12} (p+1)^4 (p^2+1)^2 (p^2+p+1)^2 (p^4+p^3+p^2+p+1)(p^4+p^3+2p^2+2p+1)/p^{40}$$

See the paper for more details we omit here.

## 5 The density of discriminants of quartic rings and fields

This section aims to prove theorems 1-5 of the paper. (See the paper for description and details.)

Theorem 1: Let  $N_4^{(i)}(\xi, \eta)$  denote the number of  $S_4$ -quartic fields  $K$  having  $4 - 2i$  real embeddings such that  $\xi < \text{Disc}(K) < \eta$ . Then

$$\lim_{X \rightarrow \infty} \frac{N_4^{(0)}(0, X)}{X} = \frac{1}{48} \prod_p (1 + p^{-2} - p^{-3} - p^{-4})$$

$$\lim_{X \rightarrow \infty} \frac{N_4^{(1)}(0, X)}{X} = \frac{1}{8} \prod_p (1 + p^{-2} - p^{-3} - p^{-4})$$

$$\lim_{X \rightarrow \infty} \frac{N_4^{(2)}(0, X)}{X} = \frac{1}{16} \prod_p (1 + p^{-2} - p^{-3} - p^{-4})$$

Theorem 2: Let  $M_4^{(i)}(\xi, \eta)$  denote the number of quartic orders  $\mathcal{O}$  contained in  $S_4$ -quartic fields having  $4 - 2i$  real embeddings such that  $\xi < \text{Disc}(\mathcal{O}) < \eta$ . Then

$$\lim_{X \rightarrow \infty} \frac{M_4^{(0)}(0, X)}{X} = \frac{\zeta(2)^2 \zeta(3)}{48 \zeta(5)}$$

$$\lim_{X \rightarrow \infty} \frac{M_4^{(1)}(-X, 0)}{X} = \frac{\zeta(2)^2 \zeta(3)}{8 \zeta(5)}$$

$$\lim_{X \rightarrow \infty} \frac{M_4^{(2)}(0, X)}{X} = \frac{\zeta(2)^2 \zeta(3)}{16 \zeta(5)}$$

Theorem 3: Let  $p$  be a fixed prime, and let  $K$  run through all  $S_4$ -quartic fields in which  $p$  does not ramify, the fields being ordered by the size of the discriminants. Let  $K_{24}$  denote the Galois closure of  $K$ . Then the Artin symbol  $(K_{24}/p)$  takes the values  $\langle e \rangle$ ,  $\langle (12) \rangle$ ,  $\langle (123) \rangle$ ,  $\langle (1234) \rangle$ , and  $\langle (12)(34) \rangle$  with relative frequency  $1 : 6 : 8 : 6 : 3$ .

Theorem 4: When ordered by absolute discriminant, a positive proportion (approximately 17.111%) of quartic fields have associated Galois groups  $D_4$ . The remaining 82.889% of quartic fields have Galois group  $S_4$ .

Theorem 5: For a cubic field  $F$ , let  $h_2 * (F)$  denote the size of the exponent-2 part of the class group of  $F$ . Then

$$\lim_{X \rightarrow \infty} \frac{\sum_F h_2^*(F)}{\sum_F 1} = 5/4$$

$$\lim_{X \rightarrow \infty} \frac{\sum_F h_2^*(F)}{\sum_F 1} = 3/2$$

Where the sums range over cubic fields  $F$  having discriminants in the ranges  $(0, X)$  and  $(-X, 0)$  respectively.



Let  $V_{\mathbb{R}}$  denote the space of pairs  $(A, B)$  of ternary quadratic forms over the real numbers. Let  $V_{\mathbb{Z}} \subset V_{\mathbb{R}}$  denote the subset of pairs of integral forms. According to Section 3, there is a canonical bijection between the set of  $G_{\mathbb{Z}} = GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$ -equivalence classes of elements  $(A, B) \in V_{\mathbb{Z}}$  and the set of isomorphism classes of pairs  $(Q, R)$ , where  $Q$  is a quartic ring and  $R$  is a cubic resolvent ring of  $Q$ . Under this bijection, we have  $\text{Disc}(A, B) = \text{Disc}(Q) = \text{Disc}(R)$ .

From the point of view of the statement above, we would like to restrict the elements of  $V_{\mathbb{Z}}$  under consideration to those that are irreducible in an appropriate sense. More precisely, we call a pair  $(A, B)$  of integral ternary quadratic forms in  $V_{\mathbb{Z}}$  absolutely irreducible if

- (a)  $A$  and  $B$  do not possess a common zero as conics in  $\mathbb{P}^2(\mathbb{Q})$ ; and
- (b) the binary cubic form  $f(x, y) = \det(Ax - By)$  is irreducible over  $\mathbb{Q}$ .

Equivalently,  $(A, B)$  is absolutely irreducible if  $A$  and  $B$  possess a common zero in  $\mathbb{P}^2$  having field of definition  $K$ , where  $K$  is a quartic field whose Galois closure has Galois group either  $A_4$  or  $S_4$  over  $\mathbb{Q}$ . Absolutely irreducible elements in  $V_{\mathbb{Z}}$  correspond to  $(Q, R)$  where  $Q$  is an order in either an  $A_4$  or  $S_4$ -quartic field.

The action of  $G_{\mathbb{R}} = GL_2(\mathbb{R}) \times SL_3(\mathbb{R})$  on  $V_{\mathbb{R}}$  has three nondegenerate orbits  $V_{\mathbb{R}}^{(0)}, V_{\mathbb{R}}^{(1)}, V_{\mathbb{R}}^{(2)}$ , where  $V_{\mathbb{R}}^{(i)}$  consists of those elements  $(A, B)$  in  $V_{\mathbb{R}}$  having  $4 - 2i$  common zeros in  $\mathbb{P}^2(\mathbb{R})$ . For  $0 \leq i \leq 2$ , let  $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}$  be the subset of  $V_{\mathbb{R}}^{(i)}$  consisting of integral forms. Let  $N(V_{\mathbb{Z}}^{(i)}; X)$  denote the number of  $G_{\mathbb{Z}}$ -equivalence classes of absolutely irreducible elements  $(A, B) \in V_{\mathbb{Z}}^{(i)}$  and satisfying  $|\text{Disc}(A, B)| < X$ . Then we prove the following theorem, which plays an important role in proving theorem 1-5:

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(0)}; X)}{X} &= \frac{\zeta(2)^2 \zeta(3)}{48} \\ \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(1)}; X)}{X} &= \frac{\zeta(2)^2 \zeta(3)}{8} \\ \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(2)}; X)}{X} &= \frac{\zeta(2)^2 \zeta(3)}{16} \end{aligned}$$

Let  $\mathcal{F}$  denote a fundamental domain for the action of  $G_{\mathbb{Z}}$  on  $G_{\mathbb{R}}$  by left multiplication. We also assume that  $\mathcal{F} \subset G_{\mathbb{R}}$  is semi-algebraic and connected, and that it is contained in a standard Siegel set, i.e.,  $\mathcal{F} \subset N'A'K\Lambda$ . (See the paper for the definition of the sets  $K, A', N', \Lambda$ .)

Next, for  $i = 0, 1, 2$ , let  $n_i$  denote the cardinality of the stabilizer for  $G_{\mathbb{R}}$  of any element  $v \in V_{\mathbb{R}}^{(i)}$ . The group  $G_{\mathbb{R}}$  acts transitively on  $V_{\mathbb{R}}^{(i)}$ . The group of stabilizer for  $v \in V_{\mathbb{R}}^{(i)}$  is respectively  $S_4, C_2 \times C_2, D_4$  for  $i = 0, 1, 2$ , which has order  $n_1 = 24, n_2 = 4, n_3 = 8$ . For any  $V_{\mathbb{R}}^{(i)}$ ,  $\mathcal{F}_v$  will be the union of  $n_i$  fundamental domains for the action of  $G_{\mathbb{Z}}$  on  $V_{\mathbb{R}}^{(i)}$ . Therefore, we view  $\mathcal{F}_v$  as a multiset, and the multiplicity is between 1 and  $n_i$ . It is an important conclusion that the stabilizer in  $G_{\mathbb{Z}}$  of an absolutely irreducible element  $(A, B)$  is always trivial, we conclude that for any  $v \in V_{\mathbb{R}}^{(i)}$ , the product  $n_i \cdot N(V_{\mathbb{Z}}^{(i)}; X)$  is equal to the number of absolutely irreducible integer points in  $\mathcal{F}_v$  having absolute discriminant less than  $X$ .

Thus to estimate  $N(V_{\mathbb{Z}}^{(i)}; X)$ , it suffices to count the number of integer points in  $\mathcal{F}v$  for some  $v \in V_{\mathbb{R}}^{(i)}$ . The number of such integer points can be difficult to count in a single such  $\mathcal{F}v$ , so instead, we average over many  $\mathcal{F}v$  by averaging over certain  $v$  lying in a box  $H$  with measure  $|\text{Disc}(v)|^{-1} dv$ . In this paper we let  $H = \{(A, B) \in V_{\mathbb{R}} : |a_{ij}|, |b_{ij}| \leq 10; |\text{Disc}(A, B)| \geq 1\}$ . (In

fact, any nonempty  $H$  with nonzero volume is okay.) Let  $\Phi = \Phi_H$  denote the characteristics function of  $H$ . Then we have

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{\int_{v \in V^{(i)}} \Phi(v) \cdot \#\{x \in \mathcal{F}v \cap V_{\mathbb{Z}}^{(i)} \text{ abs.irr.} : 0 < |\text{Disc}(x)| < X\} |\text{Disc}(v)|^{-1} dv}{n_i \cdot \int_{v \in V^{(i)}} \Phi(v) |\text{Disc}(v)|^{-1} dv}$$

We chose the measure  $|\text{Disc}(v)|^{-1} dv$  because it is a  $G_{\mathbb{R}}$ -invariant measure. More generally, for any  $G_{\mathbb{Z}}$ -invariant set  $S \subset V_{\mathbb{Z}}$ , we may speak of the number  $N(S; X)$  of irreducible  $G_{\mathbb{Z}}$ -orbits on  $S$  having discriminant less than  $X$ . Then  $N(S; X)$  can be expressed similarly as

$$N(S; X) = \frac{\int_{v \in V^{(i)}} \Phi(v) \cdot \#\{x \in \mathcal{F}v \cap S \text{ abs.irr.} : 0 < |\text{Disc}(x)| < X\} |\text{Disc}(v)|^{-1} dv}{n_i \cdot \int_{v \in V^{(i)}} \Phi(v) |\text{Disc}(v)|^{-1} dv}$$

Then, from lemma 11 to lemma 16 in the paper, we turn to estimates on the not absolutely reducible pairs of  $(A, B)$ . Our result is that the expected number of integral ternary quadratic forms  $(A, B) \in \mathcal{F}v$  such that  $|\text{Disc}(A, B)| < X$ , and  $(A, B)$  is not absolutely irreducible is  $o(X)$  when  $X \rightarrow \infty$ , i.e., most of the pairs  $(A, B) \in \mathcal{F}v$  are absolutely irreducible. Therefore, it suffices to count the number of all the integral points in  $\mathcal{F}v$  with discriminant less than  $X$ , which afterwards could be estimated as the volume of  $\mathcal{R}_X = \mathcal{R}_X(v)$ , the submultiset in  $\mathcal{F}v$  having discriminant less than  $X$ . To sum up,

Let  $v$  take a random variable in  $H \cap V^{(i)}$  uniformly with respect to the measure  $|\text{Disc}(v)|^{-1} dv$ . Then the expected number of absolutely irreducible integral elements in  $\mathcal{R}_X$  is

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i} \text{Vol}(\mathcal{R}_X) + o(X)$$

Then we compute the volume of  $\mathcal{R}_X$ :

$$\frac{1}{n_i} \text{Vol}(\mathcal{R}_X) = \frac{6\pi^3}{n_i} \int_0^{X^{1/6}} t^6 d^\times t \cdot \int_{G_{\mathbb{Z}} \setminus G_{\mathbb{R}}^{\pm 1}} dg = \frac{\zeta(2)^2 \zeta(3)}{2n_i} X$$

Which ends our proof.

Also, due to the work that people have done before, we know that the contributions from the Galois groups  $C_4$ ,  $K_4$ , and  $A_4$  are  $o(X)$ , which are negligible in comparison. Therefore, we write the theorem in the language of quartic rings and cubic resolvents, and it leads to the following theorem:

Let  $M_4^{*(i)}(\xi, \eta)$  denote the number of isomorphism classes of pairs  $(Q, R)$  such that  $Q$  is an order in an  $S_4$ -quartic field with  $4 - 2i$  real embeddings,  $R$  is a cubic resolvent ring of  $Q$ , and  $\xi < \text{Disc}(Q) < \eta$ . Then

$$\lim_{X \rightarrow \infty} \frac{M_4^{*(0)}(0, X)}{X} = \frac{\zeta(2)^2 \zeta(3)}{48}$$

$$\lim_{X \rightarrow \infty} \frac{M_4^{*(1)}(-X, 0)}{X} = \frac{\zeta(2)^2 \zeta(3)}{8}$$

$$\lim_{X \rightarrow \infty} \frac{M_4^{*(2)}(0, X)}{X} = \frac{\zeta(2)^2 \zeta(3)}{16}$$

Actually, it should be "A<sub>4</sub> or S<sub>4</sub> quartic field", but we are allowed to neglect the A<sub>4</sub> part.

The following theorem is also important for our proof. Suppose  $S$  is a subset of  $V_{\mathbb{Z}}^{(i)}$  defined by (possibly infinitely many) congruence conditions. Then

$$\lim_{X \rightarrow \infty} \frac{N(S \cap V^{(i)}; X)}{X} = \frac{\zeta(2)^2 \zeta(3)}{2n_i} \prod_p \mu_p(S)$$

Where  $\mu_p(S)$  denotes the  $p$ -density of  $S$  in  $V_{\mathbb{Z}}$ , and  $n_i = 24, 4, 8$  respectively.

Now, we can start proving theorems 1-5. We omit the details here since they can be found in the paper.

## 6 The density of discriminants of quintic rings and fields

This section aims to prove theorems 1-4 of the paper. (See the paper for description and details.) The techniques we write down are just the same as in the last section.

Theorem 1: Let  $N_5^{(i)}(\xi, \eta)$  denote the number of  $S_5$ -quintic fields  $K$  having  $5 - 2i$  real embeddings such that  $\xi < \text{Disc}(K) < \eta$ . Then

$$\lim_{X \rightarrow \infty} \frac{N_5^{(0)}(0, X)}{X} = \frac{1}{240} \prod_p (1 + p^{-2} - p^{-4} - p^{-5})$$

$$\lim_{X \rightarrow \infty} \frac{N_5^{(1)}(0, X)}{X} = \frac{1}{24} \prod_p (1 + p^{-2} - p^{-4} - p^{-5})$$

$$\lim_{X \rightarrow \infty} \frac{N_5^{(2)}(0, X)}{X} = \frac{1}{16} \prod_p (1 + p^{-2} - p^{-4} - p^{-5})$$

Theorem 2: Let  $M_5^{(i)}(\xi, \eta)$  denote the number of quartic orders  $\mathcal{O}$  contained in  $S_5$ -quintic fields having  $5 - 2i$  real embeddings such that  $\xi < \text{Disc}(\mathcal{O}) < \eta$ . Then there exists a positive constant  $\alpha$  such that

$$\lim_{X \rightarrow \infty} \frac{M_5^{(0)}(0, X)}{X} = \frac{\alpha}{240}$$

$$\lim_{X \rightarrow \infty} \frac{M_5^{(1)}(-X, 0)}{X} = \frac{\alpha}{24}$$

$$\lim_{X \rightarrow \infty} \frac{M_5^{(2)}(0, X)}{X} = \frac{\alpha}{16}$$

In fact, we have  $\alpha = \prod_p \alpha_p$ , where

$$\alpha_p = \frac{p-1}{p} \sum_{[R_p: \mathbb{Z}_p]=5} \frac{1}{|\text{Aut}_{\mathbb{Z}_p}(R_p)| \text{Disc}_p(R_p)}$$

Theorem 3: Let  $p$  be a fixed prime, and let  $K$  run through all  $S_5$ -quartic fields in which  $p$  does not ramify, the fields being ordered by the size of the discriminants. Let  $K_{120}$  be the Galois closure of  $K$ . Then the Artin symbol  $(K_{120}/p)$  taking values  $\langle e \rangle, \langle (12) \rangle, \langle (123) \rangle, \langle (1234) \rangle, \langle (12345) \rangle, \langle (12)(34) \rangle, \langle (12)(345) \rangle$  with relative frequency  $1 : 10 : 20 : 30 : 24 : 15 : 20$ .

Theorem 4: When ordered by absolute discriminant, a density of 100% of quintic fields have associated Galois group  $S_5$ .

Let  $V_{\mathbb{R}}$  denote the space of quadruples  $(A, B, C, D)$  of skew-symmetric over the real numbers. Let  $V_{\mathbb{Z}} \subset V_{\mathbb{R}}$  denote the subset of quadruples of integral forms. According to Section 4, there is a canonical bijection between the set of  $G_{\mathbb{Z}} = GL_4(\mathbb{Z}) \times SL_5(\mathbb{Z})$ -equivalence classes of elements  $(A, B, C, D) \in V_{\mathbb{Z}}$  and the set of isomorphism classes of pairs  $(R, S)$ , where  $R$  is a quintic ring and  $S$  is a sextic resolvent ring of  $Q$ . Under this bijection, we have  $\text{Disc}(A, B, C, D) = \text{Disc}(R) = \frac{1}{16} \text{Disc}(S)^{1/3}$ .

From the point of view of the statement above, we would like to restrict the elements of  $V_{\mathbb{Z}}$  under consideration to those that are irreducible in an appropriate sense. More precisely, we call a quadruple  $(A, B, C, D)$  of integral ternary quadratic forms in  $V_{\mathbb{Z}}$  absolutely irreducible if

(a)  $A, B, C, D$  is irreducible, i.e., it possesses a zero in  $\mathbb{P}^3$  having field of fractions  $K$ , where  $K$  is a quintic field extension of  $\mathbb{Q}$ ;

(b) The fractional field of its associated quintic ring is an  $S_5$ -quintic field. Equivalently, if the fields of definition of its common zeros in  $\mathbb{P}^3$  are  $S_5$ -quintic fields.

Absolutely irreducible elements in  $V_{\mathbb{Z}}$  correspond to  $(R, S)$  where  $R$  is an order in an  $S_5$ -quintic field.

The action of  $G_{\mathbb{R}} = GL_4(\mathbb{R}) \times SL_5(\mathbb{R})$  on  $V_{\mathbb{R}}$  has three nondegenerate orbits  $V_{\mathbb{R}}^{(0)}, V_{\mathbb{R}}^{(1)}, V_{\mathbb{R}}^{(2)}$ , where  $V_{\mathbb{R}}^{(i)}$  consists of those elements  $(A, B, C, D)$  in  $V_{\mathbb{R}}$  having  $5 - 2i$  common zeros in  $\mathbb{P}^3(\mathbb{R})$ . For  $0 \leq i \leq 2$ , let  $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}$  be the subset of  $V_{\mathbb{R}}^{(i)}$  consisting of integral forms. Let  $N(V_{\mathbb{Z}}^{(i)}; X)$  denote the number of  $G_{\mathbb{Z}}$ -equivalence classes of absolutely irreducible elements  $(A, B, C, D) \in V_{\mathbb{Z}}^{(i)}$  and satisfying  $|\text{Disc}(A, B, C, D)| < X$ . Then we prove the following theorem, which plays an important role in proving theorem 1-4:

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(0)}; X)}{X} &= \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{240} \\ \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(1)}; X)}{X} &= \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{24} \\ \lim_{X \rightarrow \infty} \frac{N(V_{\mathbb{Z}}^{(2)}; X)}{X} &= \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{16} \end{aligned}$$

Let  $\mathcal{F}$  denote a fundamental domain for the action of  $G_{\mathbb{Z}}$  on  $G_{\mathbb{R}}$  by left multiplication. We also assume that  $\mathcal{F} \subset G_{\mathbb{R}}$  is semi-algebraic and connected, and that it is contained in a standard Siegel set, i.e.,  $\mathcal{F} \subset N'A'K\Lambda$ . (See the paper for the definition of the sets  $K, A', N', \Lambda$ .)

Next, for  $i = 0, 1, 2$ , let  $n_i$  denote the cardinality of the stabilizer for  $G_{\mathbb{R}}$  of any element  $v \in V_{\mathbb{R}}^{(i)}$ . The group  $G_{\mathbb{R}}$  acts transitively on  $V_{\mathbb{R}}^{(i)}$ . The group of stabilizer for  $v \in V_{\mathbb{R}}^{(i)}$  is respectively  $S_5, S_3 \times C_2, D_4$  for  $i = 0, 1, 2$ , which has order  $n_1 = 120, n_2 = 12, n_3 = 8$ . For any  $V_{\mathbb{R}}^{(i)}$ ,  $\mathcal{F}_v$  will be the union of  $n_i$  fundamental domains for the action of  $G_{\mathbb{Z}}$  on  $V_{\mathbb{R}}^{(i)}$ . Therefore, we view  $\mathcal{F}_v$  as a multiset, and the multiplicity is between 1 and  $n_i$ . It is an important conclusion that the stabilizer in  $G_{\mathbb{Z}}$  of an absolutely irreducible element  $(A, B, C, D)$  is always trivial, we conclude that for any  $v \in V_{\mathbb{R}}^{(i)}$ , the product  $n_i \cdot N(V_{\mathbb{Z}}^{(i)}; X)$  is equal to the number of absolutely irreducible integer points in  $\mathcal{F}_v$  having absolute discriminant less than  $X$ .

Thus to estimate  $N(V_{\mathbb{Z}}^{(i)}; X)$ , it suffices to count the number of integer points in  $\mathcal{F}_v$  for some  $v \in V_{\mathbb{R}}^{(i)}$ . The number of such integer points can be difficult to count in a single such  $\mathcal{F}_v$ , so instead, we average over many  $\mathcal{F}_v$  by averaging over certain  $v$  lying in a box  $H$  with measure  $|\text{Disc}(v)|^{-1} dv$ . In this paper, we let  $H$  be any nonempty  $H$  with nonzero volume. Let  $\Phi = \Phi_H$  denote the characteristics function of  $H$ . Then we have

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{\int_{v \in V^{(i)}} \Phi(v) \cdot \#\{x \in \mathcal{F}_v \cap V_{\mathbb{Z}}^{(i)} \text{ abs.irr.} : 0 < |\text{Disc}(x)| < X\} |\text{Disc}(v)|^{-1} dv}{n_i \cdot \int_{v \in V^{(i)}} \Phi(v) |\text{Disc}(v)|^{-1} dv}$$

We chose the measure  $|\text{Disc}(v)|^{-1}dv$  because it is a  $G_{\mathbb{R}}$ -invariant measure. More generally, for any  $G_{\mathbb{Z}}$ -invariant set  $S \subset V_{\mathbb{Z}}$ , we may speak of the number  $N(S; X)$  of irreducible  $G_{\mathbb{Z}}$ -orbits on  $S$  having discriminant less than  $X$ . Then  $N(S; X)$  can be expressed similarly as

$$N(S; X) = \frac{\int_{v \in V^{(i)}} \Phi(v) \cdot \#\{x \in \mathcal{F}v \cap S \text{ abs.irr.} : 0 < |\text{Disc}(x)| < X\} |\text{Disc}(v)|^{-1} dv}{n_i \cdot \int_{v \in V^{(i)}} \Phi(v) |\text{Disc}(v)|^{-1} dv}$$

Then, from lemma 8 to lemma 14 (except from proposition 12) in the paper, we turn to estimates on the not absolutely irreducible quadruples of  $(A, B, C, D)$ . Our result is that the expected number of integral ternary quadratic forms  $(A, B, C, D) \in \mathcal{F}v$  such that  $|\text{Disc}(A, B, C, D)| < X$ , and  $(A, B, C, D)$  is not absolutely irreducible is  $o(X)$  when  $X \rightarrow \infty$ , i.e., most of the pairs  $(A, B, C, D) \in \mathcal{F}v$  are absolutely irreducible. Therefore, it suffices to count the number of all the integral points in  $\mathcal{F}v$  with discriminant less than  $X$ , which afterwards could be estimated as the volume of  $\mathcal{R}_X = \mathcal{R}_X(v)$ , the submultiset in  $\mathcal{F}v$  having discriminant less than  $X$ . To sum up,

Let  $v$  take a random variable in  $H \cap V^{(i)}$  uniformly with respect to the measure  $|\text{Disc}(v)|^{-1}dv$ . Then the expected number of absolutely irreducible integral elements in  $\mathcal{R}_X$  is

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{n_i} \text{Vol}(\mathcal{R}_X) + o(X)$$

Then we compute the volume of  $\mathcal{R}_X$ :

$$\frac{1}{n_i} \text{Vol}(\mathcal{R}_X) = \frac{20}{n_i} \int_0^{X^{1/40}} t^{40} d^{\times} t \cdot \int_{G_{\mathbb{Z}} \backslash G_{\mathbb{R}}^{\pm 1}} dg = \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{2n_i} X$$

Which ends our proof.

Also, we write the theorem in the language of quintic rings and sextic resolvents, and this lead to the following theorem:

Let  $M_5^{*(i)}(\xi, \eta)$  denote the number of isomorphism classes of pairs  $(R, S)$  such that  $R$  is an order in an  $S_5$ -quintic field with  $5 - 2i$  real embeddings,  $S$  is a sextic resolvent ring of  $Q$ , and  $\xi < \text{Disc}(Q) < \eta$ . Then

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{M_5^{*(0)}(0, X)}{X} &= \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{240} \\ \lim_{X \rightarrow \infty} \frac{M_5^{*(1)}(-X, 0)}{X} &= \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{24} \\ \lim_{X \rightarrow \infty} \frac{M_5^{*(2)}(0, X)}{X} &= \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{16} \end{aligned}$$

The following theorem is also important for our proof. Suppose  $S$  is a subset of  $V_{\mathbb{Z}}^{(i)}$  defined by (possibly infinitely many) congruence conditions. Then

$$\lim_{X \rightarrow \infty} \frac{N(S \cap V^{(i)}; X)}{X} = \frac{\zeta(2)^2 \zeta(3)^2 \zeta(4)^2 \zeta(5)}{2n_i} \prod_p \mu_p(S)$$

Where  $\mu_p(S)$  denotes the  $p$ -density of  $S$  in  $V_{\mathbb{Z}}$ , and  $n_i = 120, 12, 8$  respectively.

Now, we can start proving theorems 1-4. We omit the details here since they can be found in the paper.