Annals of Mathematics, **159** (2004), 217–250

Higher composition laws I: A new view on Gauss composition, and quadratic generalizations

By Manjul Bhargava

1. Introduction

Two centuries ago, in his celebrated work *Disquisitiones Arithmeticae* of 1801, Gauss laid down the beautiful law of composition of integral binary quadratic forms which would play such a critical role in number theory in the decades to follow. Even today, two centuries later, this law of composition still remains one of the primary tools for understanding and computing with the class groups of quadratic orders.

It is hence only natural to ask whether higher analogues of this composition law exist that could shed light on the structure of other algebraic number rings and fields. This article forms the first of a series of four articles in which our aim is precisely to develop such "higher composition laws". In fact, we show that Gauss's law of composition is only one of at least fourteen composition laws of its kind which yield information on number rings and their class groups.

In this paper, we begin by deriving a general law of composition on $2\times2\times2$ cubes of integers, from which we are able to obtain Gauss's composition law on binary quadratic forms as a simple special case in a manner reminiscent of the group law on plane elliptic curves. We also obtain from this composition law on $2 \times 2 \times 2$ cubes four further new laws of composition. These laws of composition are defined on 1) binary cubic forms, 2) pairs of binary quadratic forms, 3) pairs of quaternary alternating 2-forms, and 4) senary (six-variable) alternating 3-forms.

More precisely, Gauss's theorem states that the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of a given discriminant D has an inherent group structure. The five other spaces of forms mentioned above (including the space of $2 \times 2 \times 2$ cubes) also possess natural actions by special linear groups over $\mathbb{Z}$ and certain products thereof. We prove that, just like Gauss's space of binary quadratic forms, each of these group actions has the following remarkable properties. First, each of these six spaces possesses only a single polynomial invariant for the corresponding group action, which we call the *discriminant*. This discriminant invariant is found to take only values that

are 0 or 1 (mod 4). Second, there is a natural notion of *projectivity* for elements in these spaces, which reduces to the notion of primitivity in the case of binary quadratic forms. Finally, for each of these spaces L, the set $\mathrm{Cl}(L;D)$ of orbits of projective elements having a fixed discriminant D is naturally equipped with the structure of a finite abelian group.

The six composition laws mentioned above all turn out to have natural interpretations in terms of ideal classes of quadratic rings. We prove that the law of composition on $2\times 2\times 2$ cubes of discriminant D gives rise to groups isomorphic to $\mathrm{Cl}^+(S)\times\mathrm{Cl}^+(S)$, where $\mathrm{Cl}^+(S)$ denotes the narrow class group of the quadratic order S of discriminant D. This interpretation of the space of $2\times 2\times 2$ cubes then specializes to give the narrow class group in Gauss's case and in the cases of pairs of binary quadratic forms and pairs of quaternary alternating 2-forms, and yields roughly the 3-part of the narrow class group in the case of binary cubic forms. Finally, it gives the trivial group in the case of six-variable alternating 3-forms, yielding the interesting consequence that, for any fundamental discriminant D, there is exactly one integral senary 3-form $E\in\wedge^3\mathbb{Z}^6$ having discriminant D (up to $\mathrm{SL}_6(\mathbb{Z})$-equivalence).

We note that many of the spaces we derive in this series of articles were previously considered over algebraically closed fields by Sato-Kimura [7] in their monumental work classifying prehomogeneous vector spaces. Over other fields such as the rational numbers, these spaces were again considered in the important work of Wright-Yukie [9], who showed that generic rational orbits in these spaces correspond to étale extensions of degrees 1, 2, 3, 4, or 5. Our approach differs from previous work in that we consider orbits over the integers $\mathbb{Z}$; as we shall see, the integer orbits have an extremely rich structure, extending Gauss's work on the space of binary quadratic forms to various other spaces of forms.

The organization of this paper is as follows. Section 2 forms an extended introduction in which we describe, in an elementary manner, the above-mentioned six composition laws and the elegant properties which uniquely determine them. In Section 3 we describe how to rephrase these six composition laws in the language of ideal classes of quadratic orders, when the discriminant is nonzero; we use this new formulation to provide proofs of the assertions of Section 2 as well as to gain an understanding of the nonprojective elements of these spaces in terms of nonprojective ideal classes. In Section 4, we conclude by discussing the mysterious relationship between our composition laws and the exceptional Lie groups.

Remarks on terminology and notation. An n-ary k-ic form is a homogeneous 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 will denote by $(\mathrm{Sym}^k\mathbb{Z}^n)^*$ the $\binom{n+k-1}{k}$-dimensional lattice of n-ary

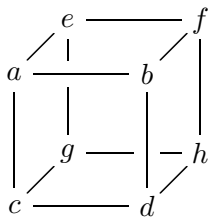
k-ic forms with integer coefficients. The reason for the "$*$" is that there is also a sublattice $\mathrm{Sym}^k\mathbb{Z}^n$ corresponding to the forms $f : \mathbb{Z}^n \to \mathbb{Z}$ satisfying $f(\xi) = F(\xi, \dots, \xi)$ for some symmetric multilinear function $F : \mathbb{Z}^n \times \cdots \times \mathbb{Z}^n \to \mathbb{Z}$ (classically called the "polarization" of f). Thus, for example, $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ is the space of binary quadratic forms $f(x, y) = ax^2+bxy+cy^2$ with $a, b, c \in \mathbb{Z}$, while $\mathrm{Sym}^2\mathbb{Z}^2$ is the subspace of such forms where b is even, i.e., forms corresponding to integral symmetric matrices $\left[\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right]$. Analogously, $(\mathrm{Sym}^3\mathbb{Z}^2)^*$ is the space of integer-coefficient binary cubic forms $f(x, y) = ax^3+bx^2y+cxy^2+dy^3$, while $\mathrm{Sym}^3\mathbb{Z}^2$ is the subspace of such forms with b and c divisible by 3. Finally, one also has the space $\wedge^k\mathbb{Z}^n$ of n-ary alternating k-forms, i.e., multilinear functions $\mathbb{Z}^n \times \cdots \times \mathbb{Z}^n \to \mathbb{Z}$ that change sign when any two variables are interchanged.

2. Quadratic composition and $2 \times 2 \times 2$ cubes of integers

In this section, we discuss the space of $2 \times 2 \times 2$ cubical integer matrices, modulo the natural action of $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$, and we describe the six composition laws (including Gauss's law) that can be obtained from this perspective. No proofs are given in this section; we postpone them until Section 3.

2.1. *The fundamental slicings.* Let $\mathcal{C}_2$ denote the space $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. Since $\mathcal{C}_2$ is a free abelian group of rank 8, each element of $\mathcal{C}_2$ can be represented as a vector (a, b, c, d, e, f, g, h) or, more naturally, as a cube of integers

(1)



.

Here, if we denote by $\{v_1, v_2\}$ the standard basis of $\mathbb{Z}^2$, then the element of $\mathcal{C}_2$ described by (1) is

$$\begin{array}{ccccccccc} & av_1\otimes v_1\otimes v_1 & + & bv_1\otimes v_2\otimes v_1 & + & cv_2\otimes v_1\otimes v_1 & + & dv_2\otimes v_2\otimes v_1 \\ + & ev_1\otimes v_1\otimes v_2 & + & fv_1\otimes v_2\otimes v_2 & + & gv_2\otimes v_1\otimes v_2 & + & hv_2\otimes v_2\otimes v_2\,; \end{array}$$

but the cubical representation is both more intuitive and more convenient and hence we shall always identify $\mathcal{C}_2$ with the space of $2 \times 2 \times 2$ cubes of integers.

Now a cube of integers $A \in \mathcal{C}_2$ may be partitioned into two 2×2 matrices in essentially three different ways, corresponding to the three possible slicings of a cube—along three of its planes of symmetry—into two congruent parallelepipeds. More precisely, the integer cube A given by (1) can be partitioned

into the 2×2 matrices

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

or into

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

or

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

Our action of Γ is defined so that, for any $1 \leq i \leq 3$, an element $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ in the i^{th} factor of $\mathrm{SL}_2(\mathbb{Z})$ acts on the cube A by replacing (M_i, N_i) by $(rM_i + sN_i, tM_i + uN_i)$. The actions of these three factors of $\mathrm{SL}_2(\mathbb{Z})$ in Γ commute with each other; this is analogous to the fact that row and column operations on a rectangular matrix commute. Hence we obtain a natural action of Γ on $\mathcal{C}_2$.

Now given any cube $A \in \mathcal{C}_2$ as above, let us construct a binary quadratic form $Q_i = Q_i^A$ for $1 \leq i \leq 3$, by defining

$$Q_i(x, y) = -\mathrm{Det}(M_i x - N_i y).$$

Then note that the form Q_1 is invariant under the action of the subgroup $\{\mathrm{id}\} \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \subset \Gamma$, because this subgroup acts only by row and column operations on M_1 and N_1 and hence does not change the value of $-\mathrm{Det}(M_1 x - N_1 y)$. The remaining factor of $\mathrm{SL}_2(\mathbb{Z})$ acts in the standard way on Q_1, and it is well-known that this action has exactly one polynomial invariant[1], namely the discriminant $\mathrm{Disc}(Q_1)$ of Q_1 (see, e.g., [6]). Thus the unique polynomial invariant for the action of $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ on its representation $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ is given simply by $\mathrm{Disc}(Q_1)$. Of course, by the same reasoning, $\mathrm{Disc}(Q_2)$ and $\mathrm{Disc}(Q_3)$ must also be equal to this same invariant up to scalar factors. A symmetry consideration (or a quick calculation!) shows that in fact $\mathrm{Disc}(Q_1) = \mathrm{Disc}(Q_2) = \mathrm{Disc}(Q_3)$; we denote this common value simply by $\mathrm{Disc}(A)$. Explicitly, we find

$$\begin{aligned}\mathrm{Disc}(A) = {} & a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 \\ & -2(abgh + cdef + acfh + bdeg + aedh + bfcg) + 4(adfg + bceh).\end{aligned}$$

[1]We use throughout the standard abuse of terminology "has one polynomial invariant" to mean that the corresponding polynomial invariant ring is generated by one element.

2.2. *Gauss composition revisited.* We have seen that every cube A in $\mathcal{C}_2$ gives three integral binary quadratic forms Q_1^A, Q_2^A, Q_3^A all having the same discriminant. Inspired by the group law on elliptic curves, let us define an addition axiom on the set of (primitive) binary quadratic forms of a fixed discriminant D by declaring that, for all triplets of primitive quadratic forms Q_1^A, Q_2^A, Q_3^A arising from a cube A of discriminant D,

THE CUBE LAW. *The sum of Q_1^A, Q_2^A, Q_3^A is zero.*

More formally, we consider the free abelian group on the set of primitive binary quadratic forms of discriminant D modulo the subgroup generated by all sums $[Q_1^A] + [Q_2^A] + [Q_3^A]$ with Q_i^A as above.

One basic and beautiful consequence of this axiom of addition is that forms that are $\mathrm{SL}_2(\mathbb{Z})$-equivalent automatically become "identified", for the following reason. Suppose that $\gamma = \gamma_1 \times \mathrm{id} \times \mathrm{id} \in \Gamma$, and that A gives rise to the three quadratic forms Q_1, Q_2, Q_3. Then $A' = \gamma A$ gives rise to the three quadratic forms Q_1', Q_2, Q_3, where $Q_1' = \gamma_1 Q_1$. Now the Cube Law implies that the sum of Q_1, Q_2, Q_3 is zero, and also that the sum of Q_1', Q_2, Q_3 is zero. Therefore Q_1 and Q_1' become identified, and thus we may view the Cube Law as descending to a law of addition on $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of forms of a given discriminant.

In fact, with an appropriate choice of identity, this simple relation imposed by the Cube Law turns the space of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D into a group! More precisely, for a binary quadratic form Q let us use $[Q]$ to denote the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of Q. Then we have the following theorem.

THEOREM 1. *Let D be any integer congruent to 0 or $1 \pmod 4$, and let $Q_{\mathrm{id},D}$ be any primitive binary quadratic form of discriminant D such that there is a cube A_0 with $Q_1^{A_0} = Q_2^{A_0} = Q_3^{A_0} = Q_{\mathrm{id},D}$. Then there exists a unique group law on the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D such that*:

(a) *$[Q_{\mathrm{id},D}]$ is the additive identity*;

(b) *For any cube A of discriminant D such that Q_1^A, Q_2^A, Q_3^A are primitive, we have*

$$[Q_1^A] + [Q_2^A] + [Q_3^A] = [Q_{\mathrm{id},D}].$$

Conversely, given Q_1, Q_2, Q_3 with $[Q_1] + [Q_2] + [Q_3] = [Q_{\mathrm{id},D}]$, there exists a cube A of discriminant D, unique up to Γ-equivalence, such that $Q_1^A = Q_1$, $Q_2^A = Q_2$, and $Q_3^A = Q_3$.

The most natural choice of identity element in Theorem 1 is

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

in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$. That $Q_{\mathrm{id},D}$ satisfies the condition required of it follows from the triply-symmetric cubes

(3)

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

whose three associated quadratic forms are all given by $Q_{\mathrm{id},D}$ (as defined by (2)).

Indeed, if the identity element $Q_{\mathrm{id},D}$ is given as in (2), then the group law defined by Theorem 1 is equivalent to Gauss composition! Thus Theorem 1 gives a very short and simple description of Gauss composition; namely, it implies that the group defined by Gauss can be obtained simply by considering the free group generated by all primitive quadratic forms of a given discriminant D, modulo the relation $Q_{\mathrm{id},D} = 0$ and modulo all relations of the form $Q_1^A + Q_2^A + Q_3^A = 0$ where Q_1^A, Q_2^A, Q_3^A form a triplet of primitive quadratic forms arising from a cube A of discriminant D.

In Section 3.3 we give a proof of Theorem 1, and of its equivalence with Gauss composition, using the language of ideal classes. An alternative proof, not using ideal classes, is given in the appendix.

We use $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ to denote the lattice of integer-valued binary quadratic forms[2], and we use $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$ to denote the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D equipped with the above group structure.

2.3. *Composition of* $2\times2\times2$ *cubes.* Theorem 1 actually implies something stronger than Gauss composition: not only do the primitive binary quadratic forms of discriminant D form a group, but the cubes of discriminant D—that give rise to triples of primitive quadratic forms—themselves form a group.

To be more precise, let us say a cube A is *projective* if the forms Q_1^A, Q_2^A, Q_3^A are primitive, and let us denote by $[A]$ the Γ-equivalence class of A. Then we have the following theorem.

[2]Gauss actually considered only the sublattice $\mathrm{Sym}^2\mathbb{Z}^2$ of binary forms whose corresponding symmetric matrices have integer entries. From the modern point of view, however, it is more natural to consider the "dual lattice" $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ of binary quadratic forms having integer coefficients. This is the point of view we adopt.

THEOREM 2. *Let D be any integer congruent to* 0 *or* 1 (mod 4), *and let $A_{\mathrm{id},D}$ be the triply-symmetric cube defined by* (3). *Then there exists a unique group law on the set of* Γ*-equivalence classes of projective cubes A of discriminant D such that*:

(a) $[A_{\mathrm{id},D}]$ *is the additive identity*;

(b) *For $i = 1, 2, 3$, the maps $[A] \mapsto [Q_i^A]$ yield group homomorphisms to* $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$.

We note again that other identity elements could have been chosen in Theorem 2. However, for concreteness, we choose $A_{\mathrm{id},D}$ as in (3) once and for all, since this choice determines the choice of identity element in all other compositions (including Gauss composition).

Theorem 2 is easily deduced from Theorem 1. In fact, addition of cubes may be defined in the following manner. Let A and A' be any two projective cubes having discriminant D; since $([Q_1^A] + [Q_1^{A'}]) + ([Q_2^A] + [Q_2^{A'}]) + ([Q_3^A] + [Q_3^{A'}]) = [Q_{\mathrm{id},D}]$ in $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$, the existence of a cube A'' with $[Q_i^{A''}] = [Q_i^A] + [Q_i^{A'}]$ for $1 \le i \le 3$ and its uniqueness up to Γ-equivalence follows from the last part of Theorem 1. We define the composition of $[A]$ and $[A']$ by setting $[A] + [A'] = [A'']$.

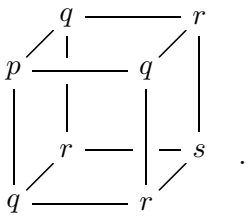
We denote the set of Γ-equivalence classes of projective cubes of discriminant D, equipped with the above group structure, by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$.

2.4. *Composition of binary cubic forms.* The above law of composition on cubes also leads naturally to a law of composition on ($\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of) integral binary cubic forms $px^3 + 3qx^2y + 3rxy^2 + sy^3$. For just as one frequently associates to a binary quadratic form $px^2 + 2qxy + ry^2$ the symmetric 2×2 matrix

$$\begin{bmatrix} p & q \\ q & r \end{bmatrix},$$

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

(4)



.

Using $\mathrm{Sym}^3\mathbb{Z}^2$ to denote the space of binary cubic forms with triplicate central coefficients, the above association of $px^3+3qx^2y+3rxy^2+sy^3$ with the cube (4) corresponds to the natural inclusion

$$\iota : \mathrm{Sym}^3\mathbb{Z}^2 \to \mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2$$

of the space of triply-symmetric cubes into the space of cubes.

We call a binary cubic form $C(x,y)=px^3+3qx^2y+3rxy^2+sy^3$ *projective* if the corresponding triply-symmetric cube $\iota(C)$ given by (4) is projective. In this case, the three forms $Q_1^{\iota(C)}$, $Q_2^{\iota(C)}$, $Q_3^{\iota(C)}$ are all equal to the *Hessian*

$$H(x,y)=(q^2-pr)x^2+(ps-qr)xy+(r^2-qs)y^2=-\frac{1}{36}\begin{vmatrix} C_{xx} & C_{xy}\\ C_{yx} & C_{yy}\end{vmatrix}; \tag{5}$$

hence C is projective if and only if H is primitive, i.e., if $\gcd(q^2-pr,\ ps-qr, r^2-qs)=1$.

The preimages of the identity cubes (3) under ι are given by

$$C_{\mathrm{id},D}=3x^2y+\frac{D}{4}y^3 \quad \text{or} \quad C_{\mathrm{id},D}=3x^2y+3xy^2+\frac{D+3}{4}y^3 \tag{6}$$

in accordance with whether $D\equiv 0 \pmod 4$ or $D\equiv 1 \pmod 4$. Denoting the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of $C\in\mathrm{Sym}^3\mathbb{Z}^2$ by $[C]$, we have the following theorem.

THEOREM 3. *Let D be any integer congruent to 0 or 1 modulo 4, and let $C_{\mathrm{id},D}$ be given as in (6). Then there exists a unique group law on the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of projective binary cubic forms C of discriminant D such that*:

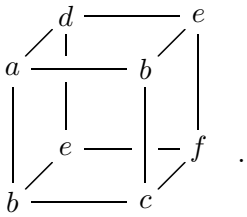
(a) *$[C_{\mathrm{id},D}]$ is the additive identity*;

(b) *The map given by $[C]\mapsto[\,\iota(C)\,]$ is a group homomorphism to $\mathrm{Cl}(\mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2; D)$.*

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

2.5. *Composition of pairs of binary quadratic forms.* The group law on binary cubic forms of discriminant D was obtained by imposing a symmetry condition on the group of $2\times 2\times 2$ cubes of discriminant D, and determining that this symmetry was preserved under the group law. Rather than imposing a threefold symmetry, one may instead impose only a twofold symmetry. This leads to cubes taking the form

(7)



.

That is, these cubes can be sliced (along a certain fixed plane) into two 2×2 symmetric matrices and therefore can naturally be viewed as a pair of binary quadratic forms $(ax^2 + 2bxy + cy^2, dx^2 + 2exy + fy^2)$.

If we use $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$ 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 (7) corresponds to the natural inclusion map

$$\jmath : \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2 \to \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2.$$

The preimages of the identity cubes $A_{\mathrm{id},D}$ under $\jmath$ are seen to be

(8)
$$B_{\mathrm{id},D} = \left(2xy, x^2 + \frac{D}{4}y^2\right) \quad \text{or} \quad B_{\mathrm{id},D} = \left(2xy + y^2, x^2 + 2xy + \frac{D+3}{4}y^2\right)$$

in accordance with whether $D \equiv 0$ or $1 \pmod 4$. Denoting the $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-class of $B \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$ by $[B]$, we have the following theorem.

THEOREM 4. *Let D be any integer congruent to 0 or 1 modulo 4, and let $B_{\mathrm{id},D}$ be given as in* (8)*. Then there exists a unique group law on the set of $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$-equivalence classes of projective pairs of binary quadratic forms B of discriminant D such that*:

(a) $[B_{\mathrm{id},D}]$ *is the additive identity*;

(b) *The map given by* $[B] \mapsto [\jmath(B)]$ *is a group homomorphism to* $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$.

The set of $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-equivalence classes of projective pairs of binary quadratic forms having a fixed discriminant D, equipped with the above group structure, is denoted by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D)$.

The groups $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D)$, however, are not new. Indeed, we have imposed our symmetry condition on cubes so that, for such an element $B \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2 \hookrightarrow \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, the last two associated quadratic forms Q_2^B and Q_3^B are equal, while the first, Q_1^B, is (possibly) different. Therefore the map

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D) \to \mathrm{Cl}\left((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\right),$$

taking twofold symmetric projective cubes $B \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$ to their third associated quadratic form Q_3^B, yields an isomorphism of groups.[3]

2.6. *Composition of pairs of quaternary alternating* 2*-forms.* Instead of imposing conditions of symmetry, one may impose conditions of *skew-symmetry* on cubes using a certain "fusion" process. To define these skew-symmetrizations, let us view our original space $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ as the space of $\mathbb{Z}$-trilinear maps $L_1 \times L_2 \times L_3 \to \mathbb{Z}$, where L_1, L_2, L_3 are $\mathbb{Z}$-modules of rank 2 (namely, the $\mathbb{Z}$-duals of the three factors $\mathbb{Z}^2$ in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$). Then given such a trilinear map

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

in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, one may naturally construct another $\mathbb{Z}$-trilinear map

$$\bar{\phi} : L_1 \times (L_2 \oplus L_3) \times (L_2 \oplus L_3) \to \mathbb{Z}$$

that is skew-symmetric in the second and third variables; this map $\bar{\phi} = \mathrm{id} \otimes \wedge_{2,2}(\phi)$ is given by

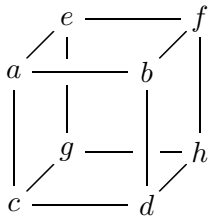
$$\bar{\phi}\,(r, (s,t), (u,v)) = \phi(r,s,v) - \phi(r,u,t).$$

Thus we have a natural $\mathbb{Z}$-linear mapping

$$\mathrm{id} \otimes \wedge_{2,2} : \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \to \mathbb{Z}^2 \otimes \wedge^2(\mathbb{Z}^2 \oplus \mathbb{Z}^2) = \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4 \tag{9}$$

taking $2\times2\times2$ cubes to pairs of alternating 2-forms in four variables. Explicitly, in terms of fixed bases for L_1, L_2, L_3, this mapping is given by

(10)



$$\to \left(\begin{bmatrix} & & a & b \\ & & c & d \\ -a & -c & & \\ -b & -d & & \end{bmatrix}, \begin{bmatrix} & & e & f \\ & & g & h \\ -e & -g & & \\ -f & -h & & \end{bmatrix} \right).$$

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ as before, and set $\Gamma' = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$. Then it is clear from our description that two elements in the same Γ-equivalence class in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ will map by (9) (or (10)) to the same Γ'-equivalence class in $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$. More remarkably, as we will prove in Section 3.6, the map (9) is *surjective on the level of equivalence classes*; that is,

[3]That these two spaces $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ and $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$ carry similar information is a reflection of the fact that, in the language of prehomogeneous vector spaces, $\mathrm{Sym}^2\mathbb{Z}^2$ is a *reduced form* of the space $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$, i.e., is the smallest space that can be obtained from $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$ by what are called "castling transforms" (cf. [7]).

any element $v \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ can be transformed by an element of Γ' to lie in the image of (9) or (10). We say that an element $F \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ is *projective* if it is Γ'-equivalent to $(\mathrm{id} \otimes \wedge_{2,2})(A)$ for some projective cube A.

Now to any pair $F = (M, N) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ of alternating 4×4 matrices, one can naturally associate a binary quadratic form $Q = Q^F$ given by

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

where, as is customary, we choose the sign of the Pfaffian so that

$$\mathrm{Pfaff}\left(\begin{bmatrix} & I \\ -I & \end{bmatrix}\right) = +1.$$

We obtain therefore an SL_2-equivariant map

$$\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4 \to (\mathrm{Sym}^2\mathbb{Z}^2)^*. \tag{11}$$

One easily checks that the coefficients of the covariant $Q(x, y)$ give a complete set of polynomial invariants for the action of $\mathrm{SL}_4(\mathbb{Z})$ on $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$. Hence 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 $\Gamma' = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$, namely

$$\mathrm{Disc}(\mathrm{Pfaff}(Mx - Ny)).$$

We call this unique, degree 4 invariant the *discriminant* $\mathrm{Disc}(F)$ of F. It is evident from the explicit formula (10) that the linear map (9) is discriminant-preserving.

Since the mapping (9) is surjective on the level of equivalence classes, and the Γ-equivalence classes of projective cubes having discriminant D form a group, we might suspect that the Γ'-equivalence classes of projective elements in $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ having discriminant D also possess a natural composition law. In fact, this is the case; denoting by $[F]$ the Γ'-equivalence class of F, we have the following theorem.

THEOREM 5. *Let D be any integer congruent to 0 or 1 modulo 4, and let $F_{\mathrm{id},D} = \mathrm{id} \otimes \wedge_{2,2}(A_{\mathrm{id},D})$. Then there exists a unique group law on the set of Γ'-equivalence classes of projective pairs of quaternary alternating 2-forms F of discriminant D such that*:

(a) $[F_{\mathrm{id},D}]$ *is the additive identity*;

(b) *The map given by* $[A] \mapsto [\mathrm{id} \otimes \wedge_{2,2}(A)]$ *is a group homomorphism from* $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D)$;

(b′) *The map given by* $[F] \mapsto [Q^F]$ *is a group homomorphism to* $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$.

In fact, either (b) or (b′) would be sufficient in Theorem 5 to specify the desired group structure. We denote the set of Γ'-equivalence classes of

projective pairs of quaternary alternating 2-forms of discriminant D, equipped with the above group structure, by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D)$.

We will prove Theorem 5 in Section 3.6 in terms of modules over quadratic orders. In particular, we will prove the following (somewhat unexpected) group isomorphism:

THEOREM 6. *For all discriminants D, the map*

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D) \to \mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$$

defined by $[F] \mapsto [Q^F]$ is an isomorphism of groups.[4]

2.7. *Composition of senary alternating 3-forms.* Finally, rather than imposing only a double skew-symmetry, we may impose a triple skew-symmetry. This leads to the space $\wedge^3\mathbb{Z}^6$ of alternating 3-forms in six variables, as follows. For any trilinear map

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

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

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

given by

$$\begin{aligned}\bar{\phi}\left((r_1, r_2, r_3), (s_1, s_2, s_3), (t_1, t_2, t_3)\right) &= \mathrm{Det}_\phi(r, s, t) \\ &= \sum_{\sigma \in S_3} (-1)^\sigma \, \phi(r_{\sigma(1)}, s_{\sigma(2)}, t_{\sigma(3)}).\end{aligned}$$

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

$$\wedge_{2,2,2} : \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \to \wedge^3(\mathbb{Z}^2 \oplus \mathbb{Z}^2 \oplus \mathbb{Z}^2) = \wedge^3\mathbb{Z}^6, \tag{12}$$

taking $2 \times 2 \times 2$ cubes to senary alternating 3-forms.

By construction, it is clear that two elements in the same Γ-equivalence class in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ will map under $\wedge_{2,2,2}$ to the same $\mathrm{SL}_6(\mathbb{Z})$-equivalence class in $\wedge^3\mathbb{Z}^6$. Moreover, we will find in Section 3.7 that the map (12) is *surjective on the level of equivalence classes*, i.e., every element $v \in \wedge^3\mathbb{Z}^6$ is $\mathrm{SL}_6(\mathbb{Z})$-equivalent to some vector in the image of (12).

The space $\wedge^3\mathbb{Z}^6$ also has a unique polynomial invariant for the action of $\mathrm{SL}_6(\mathbb{Z})$, which we call the *discriminant*. This discriminant again has degree 4, and one checks that the map (12) is discriminant-preserving.

[4]Despite the isomorphism, the spaces $\mathrm{Sym}^2\mathbb{Z}^2$ and $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ are *not* related by so-called "castling transforms", i.e., $\mathrm{Sym}^2\mathbb{Z}^2$ is not a reduced form of $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$. (Compare footnote [3] at the end of Section 2.5.)

We say that an element $E \in \wedge^3\mathbb{Z}^6$ is *projective* if it is $\mathrm{SL}_6(\mathbb{Z})$-equivalent to $\wedge_{2,2,2}(A)$ for some projective cube A. Because the projective classes of cubes in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ of discriminant D possess a group law, and the map (12) is surjective on equivalence classes, we may reasonably expect that (as in the case of $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$) the projective classes in $\wedge^3\mathbb{Z}^6$ of discriminant D should also turn into a group, defined by a pair of conditions (a) and (b) analogous to those presented in Theorems 1–5. This is indeed the case.

However, as we will prove in Section 3.7 from the point of view of modules over quadratic orders, this resulting group $\mathrm{Cl}(\wedge^3\mathbb{Z}^6; D)$ always consists of exactly one element! Thus it becomes rather unnecessary to state a theorem for $\wedge^3\mathbb{Z}^6$ akin to Theorems 1–5. Instead, we have the following theorem.

THEOREM 7. *Let D be any integer congruent to 0 or 1 modulo 4. Then the set $\mathrm{Cl}(\wedge^3\mathbb{Z}^6; D)$ consists only of the single element $[E_{\mathrm{id},D}] = [\wedge_{2,2,2}(A_{\mathrm{id},D})]$. If furthermore D is a fundamental discriminant,*[5] *then all six-variable alternating 3-forms with discriminant D are projective, and hence up to $\mathrm{SL}_6(\mathbb{Z})$-equivalence there is exactly one senary alternating 3-form of discriminant D.*

To summarize Section 2, we have natural, discriminant-preserving arrows

$$\begin{array}{ccccc}
\mathrm{Sym}^3\mathbb{Z}^2 & \longrightarrow & \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2 & \longrightarrow & \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 \\
 & & \downarrow & & \downarrow \\
 & & (\mathrm{Sym}^2\mathbb{Z}^2)^* & \longleftarrow & \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4 \\
 & & & & \downarrow \\
 & & & & \wedge^3\mathbb{Z}^6
\end{array}$$

leading to the group homomorphisms

$$\begin{array}{ccccc}
\mathrm{Cl}(\mathrm{Sym}^3\mathbb{Z}^2; D) & \longrightarrow & \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2; D) & \longrightarrow & \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; D) \\
 & & \downarrow & & \downarrow \\
 & & \mathrm{Cl}\left((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\right) & \longleftarrow & \mathrm{Cl}(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4; D) \\
 & & & & \downarrow \\
 & & & & \mathrm{Cl}(\wedge^3\mathbb{Z}^6; D)
\end{array}$$

where the central two arrows to $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$ are in fact isomorphisms, and the bottom group $\mathrm{Cl}(\wedge^3\mathbb{Z}^6; D)$ is trivial.

[5]Recall that an integer D is called a *fundamental discriminant* if it is square-free and 1 (mod 4) or it is four times a square-free integer that is 2 or 3 (mod 4). Asymptotically, $6/\pi^2 \approx 61\%$ of all discriminants are fundamental.

3. Relations with ideal classes in quadratic orders

The integral orbits of the six spaces discussed in the previous section each have natural interpretations in terms of quadratic orders.

3.1. *The parametrization of quadratic rings.* In the first four papers of this series, we will be interested in studying commutative rings $\mathcal{R}$ with unit whose underlying additive group is $\mathbb{Z}^n$ for $n = 2, 3, 4$, and 5; such rings are called *quadratic*, *cubic*, *quartic*, and *quintic* rings respectively.[6] The prototypical example of such a ring is, of course, an order in a number field of degree at most 5. To any such ring of rank n we may attach the *trace* function $\mathrm{Tr} : \mathcal{R} \to \mathbb{Z}$, which assigns to an element $\alpha \in \mathcal{R}$ the trace of the endomorphism $\mathcal{R} \xrightarrow{\times\alpha} \mathcal{R}$. The *discriminant* $\mathrm{Disc}(\mathcal{R})$ of such a ring $\mathcal{R}$ is then defined as the determinant $\det(\mathrm{Tr}(\alpha_i\alpha_j)) \in \mathbb{Z}$, where $\{\alpha_i\}$ is any $\mathbb{Z}$-basis of $\mathcal{R}$.

It is a classical fact, due to Stickelberger, that a ring having finite rank as a $\mathbb{Z}$-module must have discriminant congruent to 0 or 1 (mod 4). In the case of rank 2, this is easy to see: such a ring must have $\mathbb{Z}$-basis of the form $\langle 1, \tau\rangle$, where τ satisfies a quadratic $\tau^2 + r\tau + s = 0$ with $r, s \in \mathbb{Z}$. The discriminant of this ring is then computed to be $r^2 - 4s$, which is congruent to 0 or 1 modulo 4.

Conversely, given any integer $D \equiv 0$ or 1 (mod 4) there is a unique quadratic ring $S(D)$ having discriminant D (up to isomorphism), given by

$$S(D) = \begin{cases} \mathbb{Z}[x]/(x^2) & \text{if } D = 0, \\ \mathbb{Z} \cdot (1,1) + \sqrt{D}(\mathbb{Z} \oplus \mathbb{Z}) & \text{if } D \geq 1 \text{ is a square}, \\ \mathbb{Z}[(D + \sqrt{D})/2] & \text{otherwise;} \end{cases} \tag{13}$$

explicitly, $S(D)$ has $\mathbb{Z}$-basis $\langle 1, \tau\rangle$ where multiplication is determined by the law

$$\tau^2 = \frac{D}{4} \quad \text{or} \quad \tau^2 = \frac{D-1}{4} + \tau \tag{14}$$

in accordance with whether $D \equiv 0$ (mod 4) or $D \equiv 1$ (mod 4).[7]

Therefore, if we denote by $\mathbb{D}$ the set of elements of $\mathbb{Z}$ that are congruent to 0 or 1 (mod 4), we may say that *isomorphism classes of quadratic rings are parametrized by* $\mathbb{D}$.

There is a slight problem with this latter parametrization, however, in that all quadratic rings have two automorphisms, whereas, at least as stated, corresponding elements of $\mathbb{D}$ do not. As a result, the above construction

[6] In subsequent articles, we will turn our attention to noncommutative rings.

[7] This case distinction, which will persist throughout the paper, could be avoided by writing $S(D)$ as $\mathbb{Z} + \mathbb{Z}\tau$ where τ is the root of $\tau^2 - D\tau + \frac{D^2-D}{4} = 0$, or of any quadratic $\tau^2 + r\tau + s = 0$ with $r^2 - 4s = D$; but then one would also have the variables r, s, or D in all the formulas, so we have preferred instead to fix the choice $r \in \{0, 1\}$.

parametrizes quadratic rings up to isomorphism, but this isomorphism is not canonical. One natural way to rectify this situation is to eliminate the extra automorphism by considering not quadratic rings, but *oriented quadratic rings*, i.e., quadratic rings S in which a specific choice of isomorphism $\bar{\pi} : S/\mathbb{Z} \to \mathbb{Z}$ has been made.[8] Alternatively, a quadratic ring $S = S(D)$ is oriented once a specific choice of $\sqrt{D}$ is made; in this case, the corresponding map $\bar{\pi} : S/\mathbb{Z} \to \mathbb{Z}$ is obtained as follows. One observes that the choice of $\sqrt{D}$ determines a natural projection $\pi : S \to \mathbb{Z}$, given by the formula

$$\pi(x) = \mathrm{Tr}(x/\sqrt{D}) = \frac{x - x'}{\sqrt{D}},$$

where we have used x' to denote the image of x under the nontrivial automorphism of the underlying *unoriented* quadratic ring. The map π evidently has kernel $\mathbb{Z}$, and so $\pi : S \to \mathbb{Z}$ descends to an isomorphism $\bar{\pi} : S/\mathbb{Z} \to \mathbb{Z}$ as desired.

Since an oriented quadratic ring does not have any automorphisms, any two oriented quadratic rings of the same discriminant are canonically isomorphic. Thus it will be convenient to assume all quadratic rings to be oriented, and we will use the notation $S(D)$ to denote the unique oriented quadratic ring of discriminant D. We may now state an improved version of the above parametrization as follows:

THEOREM 8. *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*

$$D \leftrightarrow S(D)\,,$$

where $D = \mathrm{Disc}(S(D))$.

A further important feature of oriented quadratic rings is that one may speak of *oriented bases*. If S is any oriented quadratic ring, then a basis $\langle 1, \tau \rangle$ of S is positively oriented if $\pi(\tau) > 0$. A basis $\langle \alpha, \beta \rangle$ of any given rank 2 submodule of $K = S \otimes \mathbb{Q}$ has positive orientation if the change-of-basis matrix taking the positively oriented basis $\langle 1, \tau \rangle$ to $\langle \alpha, \beta \rangle$ has positive determinant (alternatively, if $\pi(\alpha'\beta) > 0$). In general, a $\mathbb{Z}$-basis $\langle \alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_n, \beta_n \rangle$ of a rank $2n$ submodule of K^n has positive orientation if it can be obtained as a transformation of the $\mathbb{Q}$-basis

$$\begin{aligned}\langle (1,0,\ldots,0), (\tau,0,\ldots,0),\ (0,1,\ldots,0), (0,\tau,\ldots,0),\ \ldots \\ \ldots,\ (0,0,\ldots,1), (0,0,\ldots,\tau) \rangle\end{aligned}$$

[8] Note that $S/\mathbb{Z} \cong \wedge^2 S$ via the map $x \mapsto 1 \wedge x$; hence an *orientation* of S may also be viewed as a choice of $\mathbb{Z}$-module isomorphism $\bar{\pi} : \wedge^2 S \to \mathbb{Z}$.

of K^n by a matrix of positive determinant. Any other basis is said to be *negatively oriented*.

Finally, we say that a quadratic ring is *nondegenerate* if its discriminant is nonzero, i.e., if it is not isomorphic to the (degenerate) quadratic ring $S(0)$. Similarly, we say that an element $v \in L$—where L is any one of the six spaces $(\mathrm{Sym}^2\mathbb{Z}^2)^*$, $\mathbb{Z}^2\otimes\mathbb{Z}^2\otimes\mathbb{Z}^2$, $\mathrm{Sym}^3\mathbb{Z}^2$, $\mathbb{Z}^2\otimes\mathrm{Sym}^2\mathbb{Z}^2$, $\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4$, or $\wedge^3\mathbb{Z}^6$ introduced in Section 2—is *nondegenerate* if its discriminant $\mathrm{Disc}(v)$ is nonzero. In the forthcoming sections, we show that the orbits of nondegenerate elements in these six spaces may be completely classified in terms of certain special types of ideal classes in nondegenerate quadratic rings. We begin by recalling briefly the classical case of binary quadratic forms.

3.2. *The case of binary quadratic forms.* As is well-known, the group $\mathrm{Cl}\big((\mathrm{Sym}^2\mathbb{Z}^2)^*; D\big)$ is almost, but not quite the same as, the ideal class group of the unique quadratic order S of discriminant D. To make up for the slight discrepancy, it is necessary to introduce the notion of *narrow class group*, which may be defined as the group $\mathrm{Cl}^+(S)$ of *oriented ideal classes*. More precisely, an *oriented ideal* is a pair (I, ε), where I is any (fractional) ideal of S in $K = S \otimes \mathbb{Q}$ having rank 2 as a $\mathbb{Z}$-module, and $\varepsilon = \pm 1$ gives the *orientation* of I. Multiplication of oriented ideals is defined componentwise, and the norm of an oriented ideal (I, ε) is defined to be $\varepsilon\cdot|L/I|\cdot|L/S|^{-1}$, where L is any lattice in K containing both S and I. For an element $\kappa \in K$, the product $\kappa \cdot (I, \varepsilon)$ is defined to be the ideal $(\kappa I, \mathrm{sgn}(N(\kappa))\varepsilon)$. Two oriented ideals (I_1, ε_1) and (I_2, ε_2) are said to be in the same *oriented ideal class* if $(I_1, \varepsilon_1) = \kappa \cdot (I_2, \varepsilon_2)$ for some invertible $\kappa \in K$.

With these notions, 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* $((\kappa), \mathrm{sgn}(N(\kappa)))$). The elements of this group are thus the invertible oriented ideal classes. In practice, we shall denote an oriented ideal (I, ε) simply by I, with the orientation $\varepsilon = \varepsilon(I)$ on I being understood.[9]

We may now state the precise relation between equivalence classes of binary quadratic forms and ideal classes of quadratic orders.

THEOREM 9. *There is a canonical bijection between the set of nondegenerate* $\mathrm{SL}_2(\mathbb{Z})$*-orbits on the space* $(\mathrm{Sym}^2\mathbb{Z}^2)^*$ *of integer-valued binary quadratic forms, and the set of isomorphism classes of pairs* (S, I)*, where* S *is a nondegenerate oriented quadratic ring and* I *is a (not necessarily invertible) oriented*

[9]Traditionally, the narrow class group is considered only for quadratic orders S of positive discriminant, and is defined as the group of invertible ideals of S modulo the subgroup of invertible principal ideals that are generated by elements of positive norm. We prefer our definition here since it gives the correct notion also when $D < 0$.

ideal class of S. Under this bijection, the discriminant of a binary quadratic form equals the discriminant of the corresponding quadratic ring.

Restricting the above result to the set of primitive quadratic forms, and noting that, in the above bijection, primitive binary quadratic forms correspond to invertible ideal classes, we obtain the following group isomorphism.

THEOREM 10. *The bijection of Theorem* 9 *restricts to a correspondence*

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

which is an isomorphism of groups.

We remark—although it will not be used in this paper—that the usual (as opposed to narrow) ideal class group may be obtained as the set of $\mathrm{GL}_2(\mathbb{Z})$-(rather than $\mathrm{SL}_2(\mathbb{Z})$-) equivalence classes of primitive binary quadratic forms, except that we must then let an element $\alpha \in \mathrm{GL}_2(\mathbb{Z})$ act on a form Q by $Q \mapsto \frac{1}{\det(\alpha)} \cdot \alpha Q$.

Theorem 9 is known in the indefinite case, while the general definite case follows easily from the known case of positive definite quadratic forms. We will give proofs of Theorems 9 and 10 in a more general context in the next section.

3.3. *The case of $2 \times 2 \times 2$ cubes.* We now turn to the general case of $2 \times 2 \times 2$ cubes. Before stating the result, we make some definitions. Let S be the quadratic ring of discriminant D, and let $K = S \otimes \mathbb{Q}$ be the corresponding quadratic algebra over $\mathbb{Q}$. 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 ideals 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 must have $N(\kappa_1\kappa_2\kappa_3) = 1$.) For example, if S is Dedekind, then an equivalence class of balanced triples means simply a triple of narrow ideal classes whose product is the principal class. Our main result on $2 \times 2 \times 2$ cubes is then as follows:

THEOREM 11. *There is a canonical bijection between the set of nondegenerate Γ-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.*

Proof. For a balanced triple (I_1, I_2, I_3) of ideals of an oriented quadratic order $S = S(D)$ as in the theorem, we first show how to construct a corresponding $2 \times 2 \times 2$ cube. In accordance with whether $D = \mathrm{Disc}(S)$ is congruent to 0

or 1 (mod 4), let $\langle 1, \tau \rangle$ be a positively oriented basis of S such that $\tau^2 - \frac{D}{4} = 0$ or $\tau^2 - \tau + \frac{1-D}{4} = 0$ respectively. Let $\langle \alpha_1, \alpha_2 \rangle$, $\langle \beta_1, \beta_2 \rangle$, and $\langle \gamma_1, \gamma_2 \rangle$ denote $\mathbb{Z}$-bases of the ideals I_1, I_2, and I_3 respectively, where the basis for each I_j is chosen to be oriented the same as or different than $\langle 1, \tau \rangle$ in accordance with whether $\varepsilon(I_j) = +1$ or -1. Since by hypothesis the product $I_1 I_2 I_3$ is contained in S, we may write

$$\alpha_i \beta_j \gamma_k = c_{ijk} + a_{ijk} \tau \tag{15}$$

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 $2 \times 2 \times 2$ cube. In terms of the projection map $\pi : S \to \mathbb{Z}$ discussed in Section 3.1, we have $a_{ijk} = \pi(\alpha_i \beta_j \gamma_k)$, or in more coordinate-free terms, $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ represents the trilinear mapping $I_1 \times I_2 \times I_3 \to \mathbb{Z}$ given by the formula $(x, y, z) \mapsto \pi(xyz)$.

It is clear from construction that changing $\langle \alpha_1, \alpha_2 \rangle$, $\langle \beta_1, \beta_2 \rangle$, $\langle \gamma_1, \gamma_2 \rangle$ to some other set of (appropriately oriented) bases for I_1, I_2, I_3, via an element $T \in \Gamma$, would simply transform A into an equivalent cube via that same element T. Hence the Γ-equivalence class of A is independent of our choice of bases for I_1, I_2, and I_3. Furthermore, it is clear that if the balanced triple (I_1, I_2, I_3) is replaced by an equivalent triple, our cube A does not change. Hence we have a well-defined map from balanced triples of ideal classes in a quadratic ring to Γ-orbits in $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$.

It remains to show that this mapping $(S, (I_1, I_2, I_3)) \to A$ is in fact a bijection; that is, we wish to show that for any given cube A there is *exactly one* pair $(S, (I_1, I_2, I_3))$ up to equivalence that yields the element A via the above map.

To this end, let us fix a cube $A = (a_{ijk})$, and consider the system (15), which currently consists mostly of indeterminates. We show that all these indeterminates are in fact essentially determined by A.

First, we claim that the ring S is determined by A, for which it suffices to show that $\mathrm{Disc}(S)$ is determined. To see this, we observe that the system of equations (15) implies the following identity:

$$\mathrm{Disc}(A) = N(I_1)^2 N(I_2)^2 N(I_3)^2 \cdot \mathrm{Disc}(S). \tag{16}$$

This identity may be proven as follows. Suppose $S = S(D) = \mathbb{Z} + \mathbb{Z}\tau$ with τ chosen as before (with D an indeterminate). Let us begin by considering the simplest case, with $I_1 = I_2 = I_3 = S$, $\alpha_1 = \beta_1 = \gamma_1 = 1$, and $\alpha_2 = \beta_2 = \gamma_2 = \tau$. In this case, the cube $A = (a_{ijk})$ in (15) is none other than the identity cube $A_{\mathrm{id},D}$ given by (3). For this cube, we have $\mathrm{Disc}(A) = D = \mathrm{Disc}(S)$, proving the identity in this special case.

Now suppose I_1 is changed to a general fractional S-ideal having $\mathbb{Z}$-basis $\langle \alpha_1, \beta_1 \rangle$. Then there is a transformation $T \in \mathrm{SL}_2(\mathbb{Q})$ taking the old basis $\langle 1, \tau \rangle$ to the new basis $\langle \alpha_1, \beta_1 \rangle$, and so the new A in (15) is obtained by transforming

$A_{\mathrm{id},D}$ by $T \times \{e\} \times \{e\} \in \Gamma$. The quadratic form Q_2^A (or Q_3^A) is thus seen to multiply by a factor of $\det(T) = N(I_1)$, so that the discriminant of A becomes multiplied by a factor of $N(I_1)^2$. In a similar manner, if I_2 and I_3 are also changed to general S-ideals, this will introduce factors of $N(I_2)^2$ and $N(I_3)^2$ in (16), thus proving the identity for general I_1, I_2, I_3.

Now by assumption we have $N(I_1)N(I_2)N(I_3) = 1$, so that

$$\mathrm{Disc}(A) = \mathrm{Disc}(S), \tag{17}$$

and hence S is indeed determined by A to be $S(\mathrm{Disc}(A))$.

Next, by the associativity and commutativity of S, we must have

$$\alpha_i\beta_j\gamma_k \cdot \alpha_{i'}\beta_{j'}\gamma_{k'} = \alpha_{i'}\beta_j\gamma_k \cdot \alpha_i\beta_{j'}\gamma_{k'} = \alpha_i\beta_{j'}\gamma_k \cdot \alpha_{i'}\beta_j\gamma_{k'} = \alpha_i\beta_j\gamma_{k'} \cdot \alpha_{i'}\beta_{j'}\gamma_k \tag{18}$$

for all $1 \le i, i', j, j', k, k' \le 2$. Expanding out these identities using (15), and then equating all coefficients of 1 and τ, yield 18 (linear and quadratic) equations in the eight variables c_{ijk} in terms of the a_{ijk}. We find that this system, together with the condition $N(I_1)N(I_2)N(I_3) > 0$, has a unique solution, given by

$$\begin{aligned} c_{ijk} = {} & (i'-i)(j'-j)(k'-k) \\ & \cdot\big[a_{i'jk}a_{ij'k}a_{ijk'} + \tfrac{1}{2}a_{ijk}(a_{ijk}a_{i'j'k'} - a_{i'jk}a_{ij'k'} - a_{ij'k}a_{i'jk'} - a_{ijk'}a_{i'j'k})\big] \\ & - \tfrac{1}{2}\, a_{ijk}\, \varepsilon \end{aligned}$$

with $\{i, i'\} = \{j, j'\} = \{k, k'\} = \{1, 2\}$, and where $\varepsilon = 0$ or 1 in accordance with whether $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$. A quick congruence check shows that the solutions for the c_{ijk} are necessarily integral! Therefore, the c_{ijk}'s in (15) are also uniquely determined by the cube A.

We must still determine the existence of $\alpha_i, \beta_j, \gamma_k \in S$ yielding the desired a_{ijk} and c_{ijk}'s in (15). It is clear that the pair (α_1, α_2) (similarly (β_1, β_2), (γ_1, γ_2)) is uniquely determined—up to a nonzero scaling factor in K—by the equations (15). For example, given any fixed $1 \le j, k \le 2$ for which $c_{1jk} + a_{1jk}\tau$ and $c_{2jk} + a_{2jk}\tau$ are invertible in K, we have

$$\alpha_1\beta_j\gamma_k(c_{2jk} + a_{2jk}\tau) = \alpha_2\beta_j\gamma_k(c_{1jk} + a_{1jk}\tau), \tag{19}$$

so the ratio $\alpha_1 : \alpha_2$ is determined, and we may let, e.g., $\alpha_1 = c_{1jk} + a_{1jk}\tau$ and $\alpha_2 = c_{2jk} + a_{2jk}\tau$. That this ratio $\alpha_1 : \alpha_2$ as determined by (19) is independent of j, k (up to a constant factor) follows from the associative laws (18) that have been forced upon the system (15). The pair (β_1, β_2) can be similarly determined up to scalars in K, and then (γ_1, γ_2) is completely determined by (α_1, α_2) and (β_1, β_2). Hence the triple (I_1, I_2, I_3) is completely determined up to equivalence.

Thus we must show only that the $\mathbb{Z}$-modules $I_1 = \langle \alpha_1, \alpha_2 \rangle$, $I_2 = \langle \beta_1, \beta_2 \rangle$, $I_3 = \langle \gamma_1, \gamma_2 \rangle$ as determined above actually form ideals of S. In fact, it is

possible to determine the precise S-module structures of I_1, I_2, I_3. Let Q_1, Q_2, Q_3 be the three quadratic forms associated to A as in Section 2.1, where we write $Q_i = p_i x^2 + q_i xy + r_i y^2$. Then a short calculation using explicit expressions for $\alpha_i, \beta_j, \gamma_k$ as above shows that

$$\begin{array}{rcl} \tau \cdot \alpha_1 &=& \frac{q_1+\varepsilon}{2} \cdot \alpha_1 \;+\; p_1 \cdot \alpha_2, \\ -\tau \cdot \alpha_2 &=& r_1 \cdot \alpha_1 \;+\; \frac{q_1-\varepsilon}{2} \cdot \alpha_2 \end{array} \tag{20}$$

where again $\varepsilon = 0$ or 1 in accordance with whether $D \equiv 0$ or $1 \pmod 4$, and where the module structures of $I_2 = \langle \beta_1, \beta_2 \rangle$ and $I_3 = \langle \gamma_1, \gamma_2 \rangle$ are given analogously in terms of the forms Q_2 and Q_3 respectively. In particular, we conclude that I_1, I_2, I_3 are indeed ideals of S.

We have now determined all the indeterminates in (15), having started only with the value of the cube A. It follows that there is exactly one pair $(S, (I_1, I_2, I_3))$ up to equivalence that yields the cube A under the mapping $(S, (I_1, I_2, I_3)) \to A$; this completes the proof. □

Note that the above discussion makes the bijection of Theorem 11 very precise. Given a quadratic ring S and a balanced triple (I_1, I_2, I_3) of ideals in S, the corresponding cube $A = (a_{ijk})$ is obtained from equations (15). Conversely, given a cube $A \in \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$, the ring S is determined by (17); bases for the ideal classes I_1, I_2, I_3 in S are obtained from (15), and the S-module structures of I_1, I_2, and I_3 are given by (20).

Let us define a balanced triple (I_1, I_2, I_3) of ideals of S to be *projective* if I_1, I_2, I_3 are projective as S-modules. Then there is a natural group law on the set of equivalence classes of projective balanced triples of ideals of a ring S. Namely, for any two such balanced triples (I_1, I_2, I_3) and (I_1', I_2', I_3'), define their composition to be the (balanced) triple $(I_1 I_1', I_2 I_2', I_3 I_3')$. This group of equivalence classes of projective balanced triples is naturally isomorphic to $\mathrm{Cl}^+(S) \times \mathrm{Cl}^+(S)$, via the map $(I_1, I_2, I_3) \to (I_1, I_2)$.

Restricting Theorem 11 to the set of projective elements of $\mathcal{C}_2$, and noting that projective cubes give rise to balanced triples of projective ideals, yields the following group isomorphism.

THEOREM 12. *The bijection of Theorem* 11 *restricts to a correspondence*

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

which is an isomorphism of groups.

That primitive binary quadratic forms and projective ideal classes are in one-to-one correspondence (the case of Gauss) is of course recovered as a special case. Indeed, a short calculation shows that the norm forms of I_1, I_2, I_3 as given by Theorem 11 are simply Q_1^A, Q_2^A, Q_3^A, which are the three quadratic forms associated to A. Thus we have also proved Theorems 1, 2, 9, and 10.

3.4. *The case of binary cubic forms.* In this section, we obtain the analogue of Theorem 11 for binary cubic forms.

THEOREM 13. *There is a canonical bijection between the set of nondegenerate* $\mathrm{SL}_2(\mathbb{Z})$*-orbits on the space* $\mathrm{Sym}^3\mathbb{Z}^2$ *of binary cubic forms, and the set of equivalence classes of triples* (S, I, δ)*, where* S *is a nondegenerate oriented quadratic ring,* I *is an ideal of* S*, and* δ *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, δ) *and* (S', I', δ') *are equivalent if there is an isomorphism* $\phi : S \to S'$ *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.*

Proof. Given a triple (S, I, δ) as in the theorem, we first show how to construct the corresponding binary cubic form $C(x, y)$. Let $S = \mathbb{Z} + \mathbb{Z}\tau$ as before, and let $I = \mathbb{Z}\alpha + \mathbb{Z}\beta$ with $\langle \alpha, \beta \rangle$ positively oriented. In analogy with (15), we may write

$$\begin{aligned} \alpha^3 &= \delta\,(\,c_0 + a_0\tau\,), \\ \alpha^2\beta &= \delta\,(\,c_1 + a_1\tau\,), \\ \alpha\beta^2 &= \delta\,(\,c_2 + a_2\tau\,), \\ \beta^3 &= \delta\,(\,c_3 + a_3\tau\,), \end{aligned} \tag{21}$$

for some eight integers a_i and c_i. Then $C(x, y) = a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3$ is our desired binary cubic form.

In terms of the map $\pi : S \to \mathbb{Z}$ discussed in Section 3.1, $C(x, y) = \pi\big((\alpha x + \beta y)^3\big)$, so we can give a basis-free description of C as the map $\xi \mapsto \pi(\xi^3)$ from I to $\mathbb{Z}$. From this it is clear that changing $\langle \alpha, \beta \rangle$ to some other basis for I, via an element $T \in \mathrm{SL}_2(\mathbb{Z})$, simply changes $C(x, y)$ (via the natural $\mathrm{SL}_2(\mathbb{Z})$-action on $\mathrm{Sym}^3\mathbb{Z}^2$) by that same element T. Hence the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of $C(x, y)$ is independent of our choice of basis for I. Conversely, any binary cubic form $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $C(x, y)$ can be obtained from (S, I, δ) in the manner described above simply by changing the basis for I appropriately. Finally, it is clear that triples equivalent to (S, I, δ) yield the identical cubic forms $C(x, y)$ under the above map.

It remains to show that this map from the set of equivalence classes of triples (S, I, δ) to the set of equivalence classes of binary cubic forms $C(x, y)$ is in fact a bijection.

To this end, fix a binary cubic form $C(x, y)$, and consider the system (21), which again consists mostly of indeterminates. We show that these indeterminates are essentially determined by the form $C(x, y)$.

First, the ring S is completely determined. To see this, we use the system of equations (21) to obtain the identity

$$\mathrm{Disc}(C) = N(I)^6 N(\delta)^{-2} \cdot \mathrm{Disc}(S),$$

just as (16) was obtained from (15). By assumption $N(\delta) = N(I)^3$, so

$$\mathrm{Disc}(C) = \mathrm{Disc}(S). \tag{22}$$

Thus $\mathrm{Disc}(S)$, and hence the ring S itself, is determined by the binary cubic form C.

The associativity and commutativity of S implies $(\alpha^2\beta)^2 = \alpha^3 \cdot \alpha\beta^2$ and $(\alpha\beta^2)^2 = \alpha^2\beta \cdot \beta^3$. Expanding these identities using (21), we obtain two linear and two quadratic equations in c_0, c_1, c_2, c_3. Assuming the basis $\langle \alpha, \beta \rangle$ of I has positive orientation, we find that this system of four equations for the c_i has exactly one solution, given by

$$\begin{aligned} c_0 &= \tfrac{1}{2}(2a_1^3 - 3a_0a_1a_2 + a_0^2a_3 - \varepsilon\, a_0), \\ c_1 &= \tfrac{1}{2}(a_1^2a_2 - 2a_0a_2^2 + a_0a_1a_3 - \varepsilon\, a_1), \\ c_2 &= -\tfrac{1}{2}(a_1a_2^2 - 2a_1^2a_3 + a_0a_2a_3 + \varepsilon\, a_2), \\ c_3 &= -\tfrac{1}{2}(2a_2^3 - 3a_1a_2a_3 + a_0a_3^2 + \varepsilon\, a_3), \end{aligned}$$

where as usual $\varepsilon = 0$ or 1 in accordance with whether $D \equiv 0$ or 1 modulo 4. (Again, the solutions for the $\{c_i\}$ are necessarily integral.) Thus the c_i's in (21) are also uniquely determined by the binary cubic form C.

An examination of the system (21) shows that we must have

$$\alpha : \beta = (c_1 + a_1\tau) : (c_2 + a_2\tau) \tag{23}$$

in S, and hence α and β are uniquely determined up to a scalar factor in $S \otimes \mathbb{Q}$. Once α and β are fixed, the system (21) then determines δ uniquely, and if α, β are each multiplied by an element $\kappa \in S \otimes \mathbb{Q}$, then δ scales by a factor of κ^3. Thus we have produced the unique triple up to equivalence that yields the form C under the mapping $(S, I, \delta) \to C$.

To see that this object (S, I, δ) is a valid triple in the sense of Theorem 13, we must only check that I, currently given as a $\mathbb{Z}$-module, is actually an ideal of S. In fact, using (23) one can calculate the module structure of I explicitly in terms of C; it is given by (20), where $\alpha_1 = \alpha$, $\alpha_2 = \beta$, and

$$p_1 = a_1^2 - a_0a_2, \quad q_1 = a_0a_3 - a_1a_2, \quad r_1 = a_2^2 - a_1a_3. \tag{24}$$

This completes the proof. □

The above discussion gives very precise information about the bijection of Theorem 13. Given a triple (S, I, δ), the corresponding cubic form $C(x, y)$ is obtained from equations (21). Conversely, given a cubic form $C(x, y) \in \mathrm{Sym}^3\mathbb{Z}^2$, the ring S is determined by (22); a basis for the ideal class I is obtained from (23), and the S-module structure of I is given by (20) and (24).

Restricting Theorem 13 to the set of classes of projective binary cubic forms now yields the following group isomorphism; here, we use $\mathrm{Cl}_3(S(D))$ to denote the group of ideal classes having order dividing 3 in $\mathrm{Cl}(S(D))$.

COROLLARY 14. *Let $S(D)$ denote the quadratic ring of discriminant D. Then there is a natural surjective group homomorphism*

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

which sends a binary cubic form C to the $S(D)$-module I, where $(S(D), I, \delta)$ is a triple corresponding to C as in Theorem 13. *Moreover, the cardinality of the kernel of this homomorphism is $|U/U^3|$, where U denotes the group of units in $S(D)$.*

The special case where D corresponds to the ring of integers in a quadratic number field deserves special mention.

COROLLARY 15. *Suppose D is the discriminant of a quadratic number field K. Then there is a natural surjective homomorphism*

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

where $\mathrm{Cl}_3(K)$ denotes the exponent 3*-part of the ideal class group of the ring of integers in K. The cardinality of the kernel is equal to*

$$\begin{cases} 1 & \text{if } D < -3; \quad \text{and} \\ 3 & \text{if } D \geq -3. \end{cases}$$

This last result was stated by Eisenstein [4], except that his assertion omitted the factor of 3 in the case of positive D, a mistake which was corrected by Arndt and Cayley later in the 19th century.

3.5. *The case of pairs of binary quadratic forms.* Just as the case of binary cubic forms was obtained by imposing a threefold symmetry on balanced triples (I_1, I_2, I_3) of a quadratic ring S, the case of pairs of binary quadratic forms can be handled by imposing a twofold symmetry. The method of proof is similar; we simply state the result.

THEOREM 16. *There is a canonical bijection between the set of nondegenerate $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$-orbits on the space $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2$, 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 of 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.*

The map taking a projective balanced triple (I_1, I_3, I_3) to the third ideal I_3 corresponds to the isomorphism of groups stated at the end of Section 2.5.

3.6. *The case of pairs of quaternary alternating* 2*-forms.* The two spaces of Section 2 resulting from the "fusion" process, namely $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^4$ and $\wedge^3\mathbb{Z}^6$, turn out to correspond to modules of higher rank. Let S again be an oriented quadratic ring and $K = S \otimes \mathbb{Q}$ the corresponding quadratic $\mathbb{Q}$-algebra. A *rank* n *ideal* of S is an S-submodule of K^n having rank $2n$ as a $\mathbb{Z}$-module. Two rank n ideals are said to be in the same *rank* n *ideal class* if they are isomorphic as S-modules (equivalently, if there exists an element $\lambda \in \mathrm{GL}_n(K)$ mapping one to the other).[10] As in Section 3.2, we speak also of *oriented* (or *narrow*) rank n ideals. As in the case of rank 1, the norm of an oriented rank n ideal M is defined to be the usual norm $|L/M| \cdot |L/S|^{-1}$ times the orientation $\varepsilon(M) = \pm 1$ of M, where L denotes any lattice in K^n containing both S^n and M.

There is a canonical map, denoted "det", from $(K^n)^n$ to K, given by taking the determinant. For a rank n ideal $M \subseteq K^n$ of S, we use $\mathrm{Det}(M)$ to denote the ideal in S generated by all elements of the form $\det(x_1, \ldots, x_n)$ where $x_1, \ldots, x_n \in M$. For example, if M is a decomposable rank n ideal, i.e., if $M \cong I_1 \oplus \cdots \oplus I_n \subseteq K^n$ for some ideals $I_1, \ldots, I_n$ in S, then $\mathrm{Det}(M)$ is simply the product ideal $I_1 \cdots I_n$. It is known that, up to a scalar factor in K, the function Det depends only on the S-module structure of M and not on the particular embedding of M into K^n.

Let us call a k-tuple of oriented S-ideals $M_1, \ldots, M_k$, of ranks $n_1, \ldots, n_k$ respectively, *balanced* if $\mathrm{Det}(M_1) \cdots \mathrm{Det}(M_k) \subseteq S$ and $N(M_1) \cdots N(M_k) = 1$. Furthermore, two such balanced k-tuples $(M_1, \ldots, M_k)$ and $(M_1', \ldots, M_k')$ are said to be *equivalent* if there exist elements λ_1, ..., λ_k in $\mathrm{GL}_{n_1}(K)$, ..., $\mathrm{GL}_{n_k}(K)$ respectively such that $M_1' = \lambda_1 M_1$, ..., $M_k' = \lambda_k M_k$. (In particular, we must have $N(\det(\lambda_1) \cdots \det(\lambda_k)) = 1$.) Note that these definitions of balanced and equivalent naturally extend those given in Section 3.3 for triples of rank 1 ideals.

Armed with these notions, we may present our theorem regarding the space of pairs of quaternary alternating 2-forms:

THEOREM 17. *There is a canonical bijection between the set of nondegenerate* $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$*-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 is equal to the discriminant of the corresponding quadratic ring.*

Proof. Given a pair $(S, (I, M))$ as in the theorem, we first show how to construct a corresponding pair of quaternary alternating 2-forms. Let $\langle 1, \tau \rangle$ be

[10] As is the custom, ideals and ideal classes are implied to be rank 1 unless explicitly stated otherwise.

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 $\mathbb{Z}$-bases for the oriented S-ideals I and M respectively. By hypothesis, we may write

$$\alpha_i \det(\beta_j, \beta_k) = c_{jk}^{(i)} + a_{jk}^{(i)} \tau \tag{25}$$

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.

By construction, it is clear that changing the bases for I and M by an element $T \in \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$ simply changes F by that same element T. Thus the $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_4(\mathbb{Z})$-equivalence class of F is well-defined.

We wish to show that the mapping $(S, (I, M)) \to F$ is in fact a bijection. To this end, let us fix an element $F \in \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^4$, and consider the system (25), which currently consists mostly of indeterminates. We show again that essentially all constants in the system are uniquely determined by F.

First we claim the ring S is determined by F. This follows by deriving the following identity:

$$\mathrm{Disc}(F) = N(I)^2 N(M)^2 \cdot \mathrm{Disc}(S).$$

Since $N(I)N(M) = 1$, we conclude that

$$\mathrm{Disc}(F) = \mathrm{Disc}(S) \tag{26}$$

and hence $S = S(\mathrm{Disc}(F))$ is indeed determined by F.

To show that the constants $c_{jk}^{(i)}$ are determined, we require the following determinental identity, which states that

$$\det(v_1, v_3) \cdot \det(v_2, v_4) = \det(v_1, v_2) \cdot \det(v_3, v_4) + \det(v_1, v_4) \cdot \det(v_2, v_3)$$

for any four vectors v_1, v_2, v_3, v_4 in the coordinate plane (this is a special case of the classical "Plücker relations"). As this identity holds over any ring, we may write

$$\begin{aligned} \alpha_i \det(\beta_k, \beta_m) \cdot \alpha_j \det(\beta_\ell, \gamma_n) = {} & \alpha_{i'} \det(\beta_k, \beta_\ell) \cdot \alpha_{j'} \det(\beta_m, \gamma_n) \\ & + \alpha_{i''} \det(\beta_k, \beta_n) \cdot \alpha_{j''} \det(\beta_\ell, \gamma_m) \end{aligned} \tag{27}$$

for $i,j \in \{1,2\}$ and $k,\ell,m,n \in \{1,2,3,4\}$, and (i',j') and (i'',j'') are any ordered pairs each equal to (i,j) or (j,i). This leads to 94 linear and quadratic equations in the $c_{jk}^{(i)}$'s, in terms of the $a_{jk}^{(i)}$'s. This system, together with the condition $N(I)N(M) > 0$, turns out to have a unique solution, given by

$$\begin{aligned} c_{jk}^{(i)} = (i - i') \Big[& a_{jk}^{(i')} \mathrm{Pfaff}(F_i) \\ & - \tfrac{1}{2} a_{jk}^{(i)} \big(\mathrm{Pfaff}(F_1 + F_2) - \mathrm{Pfaff}(F_1) - \mathrm{Pfaff}(F_2) \big) \Big] \; - \; \tfrac{1}{2} \, a_{jk}^{(i)} \, \varepsilon \end{aligned}$$

where $\{i,i'\}=\{1,2\}$, and $\varepsilon = 0$ or 1 in accordance with whether $D \equiv 0$ or 1 (mod 4). Thus the (integers) $c_{jk}^{(i)}$ in (25) are also uniquely determined by A.

We claim that the $\mathbb{Z}$-modules I and M are now determined. First, we observe that the ratio $\alpha_1 : \alpha_2$ is uniquely determined by

$$\alpha_1 : \alpha_2 = (c_{jk}^{(1)} + a_{jk}^{(1)}\tau) : (c_{jk}^{(2)} + a_{jk}^{(2)}\tau), \tag{28}$$

for $j,k \in \{1,2,3,4\}$; these equalities are implied by the system (25). That the ratio on the right side of (28) is independent of j,k follows from the relations (27) that have been imposed on the system. Hence α_1, α_2 are uniquely determined up to a scalar factor in K. (For example, if $c_{12}^{(i)} + a_{12}^{(i)}\tau$ are independent over K for $i = 1,2$, we may simply set $\alpha_i = c_{12}^{(i)} + a_{12}^{(i)}\tau$ for $i = 1,2$.) Once we have chosen $\alpha_1, \alpha_2 \in S$ with the required ratio, the values of $\det(\beta_j, \beta_k)$ are completely determined by the system (25). Moreover, because of the relations (27) that have been imposed on the system, these values of $\det(\beta_j, \beta_k)$ satisfy the Plücker relations required of them; hence the values of $\beta_1, \beta_2, \beta_3, \beta_4$ are uniquely determined as elements in K^2 up to a factor of $\mathrm{SL}_2(K)$. An explicit embedding $M \hookrightarrow K \oplus K$ can easily be computed in terms of the constants $c_{jk}^{(i)}$ and $a_{jk}^{(i)}$ if desired.

It remains only to verify that the $\mathbb{Z}$-modules $I = \langle \alpha_1, \alpha_2 \rangle$ and $M = \langle \beta_1, \beta_2, \beta_3, \beta_4 \rangle$ are in fact modules over S. Using an explicit embedding $I \hookrightarrow S$, or otherwise, one finds the S-module structure of I is given by (20), where the constants p_1, q_1, r_1 are defined by

$$-\mathrm{Pfaff}(F_1 x - F_2 y) = p_1 x^2 + q_1 xy + r_1 y^2. \tag{29}$$

Similarly, if we write

$$\tau \cdot \beta_i = \sum_{j=1}^{4} t_{ij} \beta_j,$$

then the module structure of M is given by

$$t_{ij} \;=\; \tbinom{i\,j\,k\,\ell}{1\,2\,3\,4}\left(a_{i\ell}^{(1)} a_{ik}^{(2)} - a_{ik}^{(1)} a_{i\ell}^{(2)}\right) \tag{30}$$

for $\{i,j,k,\ell\} = \{1,2,3,4\}$, and

$$t_{ii} \;=\; \tfrac{1}{2} \sum_{\substack{j,k,\ell \\ k<\ell}} \tbinom{i\,j\,k\,\ell}{1\,2\,3\,4}\left(a_{k\ell}^{(1)} a_{ij}^{(2)} - a_{ij}^{(1)} a_{k\ell}^{(2)}\right) \;+\; \tfrac{1}{2}\,\varepsilon \tag{31}$$

where $\binom{i\,j\,k\,\ell}{1\,2\,3\,4}$ denotes the sign of the permutation (i,j,k,ℓ) of $(1,2,3,4)$, and $\varepsilon = 0$ or 1 in accordance with whether $D \equiv 0$ or 1 (mod 4). As all structural coefficients t_{ij} are seen to be integral, this completes the proof. □

Again, the proof gives very precise information on the bijection of Theorem 17. Given a pair $(S,(I,M))$, the corresponding pair of 4×4 skew-symmetric matrices is obtained from equations (25). Conversely, given an element $\{a_{jk}^{(i)}\}\in\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4$, the ring S is determined by (26), while explicit embeddings of $I\hookrightarrow S$ and $M\hookrightarrow K\oplus K$ may be obtained using (28) and (25). Finally, the module structures of I and M are given by equations (20), (29), (30), and (31) respectively.

It is interesting to consider the map

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

of Section 2.6 in light of Theorems 11 and 17. We find that it corresponds to the map

$$(S,(I_1,I_2,I_3))\to(S,(I_1,I_2\oplus I_3)), \tag{32}$$

which takes balanced triples of ideal classes of S to balanced pairs of ideal classes of S having ranks 1 and 2 respectively. In other words, the fusion operation of Section 2.6 literally fuses together the ideals I_2 and I_3 by direct sum.

On the other hand, it is a theorem of H. Bass [1] that if $\mathcal{R}$ is a ring in which every ideal is generated by two elements, then every torsion-free module over $\mathcal{R}$ is a direct sum of rank 1 modules. In particular, any torsion-free module M over a quadratic order S is a direct sum of ideal classes of rank 1. Hence the map given by (32) is actually surjective onto the set of eligible pairs $(S,(I,M))$. We have proved the surjectivity assertion of Section 2.6: every element of $F\in\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4$ is integrally equivalent to $\mathrm{id}\otimes\wedge_{2,2}(A)$ for some cube A.

Let us now restrict Theorem 17 to the projective classes in $\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4$. Such classes correspond to pairs $(S,(I,M))$ in which I and M are projective S-modules satisfying $I\cdot\mathrm{Det}(M)=S$. The cancellation theorem of Serre [8] states that a projective module of rank k over a dimension 1 ring S is uniquely determined by its determinant. It follows in view of Serre's theorem that any projective pair $(S,(I,M))$ is of the form $(S,(I,S\oplus I^{-1}))$, and hence the mapping

$$\mathrm{Cl}(\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4;D)\to\mathrm{Cl}(S(D)),$$

sending $(S(D),I,M)$ to $(S(D),I)$, is an isomorphism of groups. Alternatively, the map

$$\mathrm{Cl}(\mathbb{Z}^2\otimes\wedge^2\mathbb{Z}^4;D)\to\mathrm{Cl}\left((\mathrm{Sym}^2\mathbb{Z}^2)^*;D\right),$$

which sends a pair (F_1,F_2) of alternating 4×4 matrices to the binary quadratic form $-\mathrm{Pfaff}(F_1x-F_2y)$, yields an isomorphism of groups. This proves Theorems 5 and 6.

3.7. *The case of senary alternating* 3*-forms.* Finally, we obtain the analogue of Theorem 17 for the space $\wedge^3\mathbb{Z}^6$. We show that fusing together the three ideals I_1, I_2, I_3 in Theorem 11 leads to the parametrization of certain rank three modules over quadratic orders.

THEOREM 18. *There is a canonical bijection between the set of nondegenerate* $\mathrm{SL}_6(\mathbb{Z})$*-orbits 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.*

Proof. Given a pair (S, M) as in the theorem, we first show how to construct a corresponding senary alternating 3-form. Let again $\langle 1, \tau\rangle$ be a $\mathbb{Z}$-basis for S, and suppose $\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\rangle$ is a positively oriented $\mathbb{Z}$-basis for the S-module M. By the hypothesis that M is balanced, we may write

$$\det(\alpha_i, \alpha_j, \alpha_k) = c_{ijk} + a_{ijk}\tau \tag{33}$$

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 $E = \{a_{ijk}\}_{1\le i,j,k\le 6} \in \wedge^3\mathbb{Z}^6$ is then our desired senary alternating 3-form.

It is clear that changing the chosen $\mathbb{Z}$-basis of M via an element $T \in \mathrm{SL}_6(\mathbb{Z})$ simply changes E by that same element T. Hence the $\mathrm{SL}_6(\mathbb{Z})$-equivalence class of E is well-defined.

We wish to show that the mapping $(S, M) \to E$ is in fact a bijection. To this end, let us fix an element $E \in \wedge^3\mathbb{Z}^6$, and consider the system (33), which consists mostly of indeterminates. We show that all constants in the system are essentially determined by E.

First the ring S is determined by E. This follows by first deriving the following identity:

$$\mathrm{Disc}(E) = N(M)^2 \cdot \mathrm{Disc}(S).$$

Since $N(M) = 1$, it follows that

$$\mathrm{Disc}(E) = \mathrm{Disc}(S) \tag{34}$$

and hence $S = S(\mathrm{Disc}(E))$ is indeed determined by E.

To proceed further, we require the following three-dimensional analogue of the determinantal identity of Section 3.6; we have

$$\begin{aligned}&\det(v_1, v_2, v_3)\cdot\det(v_4, v_5, v_6) + \det(v_1, v_2, v_5)\cdot\det(v_3, v_4, v_6)\\ =\,&\det(v_1, v_2, v_4)\cdot\det(v_3, v_5, v_6) + \det(v_1, v_2, v_6)\cdot\det(v_3, v_4, v_5)\end{aligned}$$

for any six vectors $v_1, v_2, v_3, v_4, v_5, v_6$ in three-space (this, again, is a special case of the Plücker relations). As this identity holds over any ring, we may write

$$\begin{aligned}(35)\qquad &\det(\alpha_i,\alpha_j,\alpha_k)\cdot\det(\alpha_\ell,\alpha_m,\alpha_n)+\det(\alpha_i,\alpha_j,\alpha_m)\cdot\det(\alpha_k,\alpha_\ell,\alpha_n)\\ &=\det(\alpha_i,\alpha_j,\alpha_\ell)\cdot\det(\alpha_k,\alpha_m,\alpha_n)+\det(\alpha_i,\alpha_j,\alpha_n)\cdot\det(\alpha_k,\alpha_\ell,\alpha_m)\end{aligned}$$

for all $i,j,k,\ell,m,n\in\{1,2,3,4,5,6\}$. This leads to a system of 135 nontrivial linear and quadratic equations for the c_{ijk}'s in terms of the a_{ijk}'s. This system, together with the condition that the basis $\alpha_1,\dots,\alpha_6$ is positively oriented, has a unique solution given by

$$\begin{aligned}c_{ijk} = &\sum_{s,t,u}\tbinom{i\,j\,k\,s\,t\,u}{1\,2\,3\,4\,5\,6}\,a_{ijs}a_{jkt}a_{iku}\\ &-\tfrac{1}{2}\,a_{ijk}\sum_{\substack{s,t,u,v,w,x\\ |\{i,j,k\}\cap\{s,t,u\}|\geq 2\\ s<t<u,\ v<w<x}}\tbinom{s\,t\,u\,v\,w\,x}{1\,2\,3\,4\,5\,6}\,a_{stu}a_{vwx}\ -\ \tfrac{1}{2}\,a_{ijk}\,\varepsilon\end{aligned}$$

where $\binom{i\,j\,k\,\ell\,m\,n}{1\,2\,3\,4\,5\,6}$ denotes the sign of the permutation (i,j,k,ℓ,m,n) of $(1,2,3,4,5,6)$, and $\varepsilon=0$ or 1 in accordance with whether $D\equiv 0$ or 1 (mod 4). Thus the (integers) c_{ijk} in (33) are also uniquely determined by E.

We claim that the $\mathbb{Z}$-module M is now determined. Indeed, the values of all determinants $\det(\alpha_i,\alpha_j,\alpha_k)$ are determined by (33). Moreover, these determinants satisfy the Plücker relations required of them as a result of (35). It follows that the values of $\alpha_1,\dots,\alpha_6$ are uniquely determined as elements of K^3 up to a factor in $\mathrm{SL}_3(K)$. An explicit embedding $M\hookrightarrow K\oplus K\oplus K$ can easily be computed in terms of the constants c_{ijk} and a_{ijk} if desired.

It remains only to verify that the $\mathbb{Z}$-module $M=\langle\alpha_1,\dots,\alpha_6\rangle$ is in fact a module over S. If we write

$$\tau\cdot\alpha_i=\sum_{j=1}^{6}t_{ij}\alpha_j,$$

then using an explicit embedding $M\hookrightarrow K^3$ as above, or otherwise, one finds

$$(36)\qquad t_{ij}\ =\ \sum_{\substack{k,\ell,m,n\\ k<\ell,\,m<n\\ k<m}}\tbinom{i\,j\,k\,\ell\,m\,n}{1\,2\,3\,4\,5\,6}\,a_{ik\ell}a_{imn}$$

for $i\neq j$, and

$$(37)\qquad t_{ii}\ =\ -\tfrac{1}{2}\sum_{\substack{j,k,\ell,m,n\\ j<k,\,\ell<m<n}}\tbinom{i\,j\,k\,\ell\,m\,n}{1\,2\,3\,4\,5\,6}\,a_{ijk}a_{\ell mn}\ +\ \tfrac{1}{2}\,\varepsilon,$$

where again $\varepsilon\in\{0,1\}$ with $D\equiv\varepsilon$ (mod 4). As all values of t_{ij} are seen to be integers, this completes the proof. □

The proof makes the bijection of Theorem 18 very precise. Given a pair (S, M), the corresponding senary alternating 3-form is obtained from equations (33). Conversely, given an element $\{a_{ijk}\} \in \wedge^3\mathbb{Z}^6$, the ring S is determined by (34), an explicit embedding of $M \hookrightarrow K^3$ may be obtained from (33), and the S-module structure of M is determined by equations (36) and (37).

Let us re-examine the natural "fusion" map

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

of Section 2.7. In terms of Theorems 11 and 18, it corresponds to the map

$$(S, (I_1, I_2, I_3)) \to (S, I_1 \oplus I_2 \oplus I_3), \tag{38}$$

which sends balanced triples of ideal classes of S to a single balanced ideal class of rank 3. Thus, the triple-fusion operation $\wedge_{2,2,2}$ of Section 2.7 literally fuses together all three rank 1 ideal classes I_1, I_2, I_3 into a single rank 3 ideal class M.

On the other hand, if follows again from Bass's theorem [1] that any rank 3 ideal class over a quadratic ring S is a direct sum of rank 1 ideal classes. Hence the map (38) is actually surjective onto the set of all pairs (S, M). Therefore, we have proved the surjectivity assertion of Section 2.7: every element of $\wedge^3\mathbb{Z}^6$ is integrally equivalent to $\wedge_{2,2,2}(A)$ for some cube A.

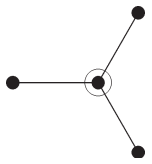
Last but not least, let us restrict Theorem 18 to the set of projective classes in $\wedge^3\mathbb{Z}^6$ of discriminant D. By Serre's theorem, any projective pair (S, M) must actually take the form $(S, S \oplus S \oplus S)$; hence $\mathrm{Cl}(\wedge^3\mathbb{Z}^6; D)$ consists of only one element. If, moreover, S is a maximal order (i.e., if D is a fundamental discriminant), then any torsion-free module over S is projective, and so all pairs (S, M) are projective. We conclude that if D is a fundamental discriminant, then up to integer equivalence, there is exactly one element of $\wedge^3\mathbb{Z}^6$ having discriminant D. We have proven Theorem 7.

4. Higher composition laws and exceptional groups

The composition laws we have presented in Sections 2 and 3 turn out to be closely related to certain exceptional Lie groups. To be precise, let G be a Lie group and P be a maximal parabolic of G. Write $P = LU$, where L is the Levi factor and U is the unipotent radical at P. Then the group L acts naturally (by conjugation) on the abelianized unipotent radical $W = U/[U, U]$. For appropriate choices of G and P, we find that we obtain precisely the spaces W underlying our composition laws.

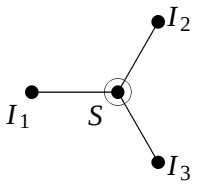
For example, the first case we considered in Section 2 was the space of $2 \times 2 \times 2$ cubes. Let G denote the exceptional Lie group of type D_4, and let

P denote the maximal parabolic corresponding to the central vertex of D_4:



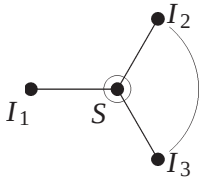
When this central vertex is removed, what remains are three isolated vertices, and hence the Levi L at P is $L = \mathrm{SL}_2 \times \mathrm{SL}_2 \times \mathrm{SL}_2$. In addition, a calculation shows that W, the abelianized unipotent radical at P, is precisely the space of $2 \times 2 \times 2$ cubes.

As we discovered in Section 3, the three factors of SL_2 in L act on the bases of three ideals I_1, I_2, and I_3 respectively in some quadratic order S (where the three ideals sum to zero). This suggests that we ought to label the vertices of the Dynkin diagram of D_4 in the following manner:

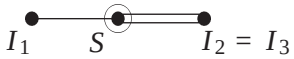


In particular, we see that the outer automorphisms of D_4 act by permuting the triple (I_1, I_2, I_3) of ideals in S.

Next, let us see what happens when we impose certain symmetry and skew-symmetry conditions, as we did in Sections 2 and 3. First, we would like to impose the symmetry condition that identifies I_2 with I_3, so that $I_2 = I_3$. On the level of Dynkin diagrams, then, we perform the identification

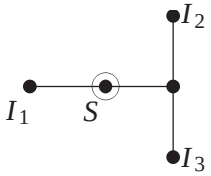


to yield



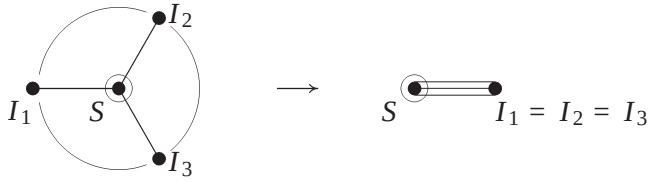
and we have obtained the Dynkin diagram B_3. Thus the composition law corresponding to pairs of binary quadratic forms, as discussed in Sections 2.5 and 3.5, arises from the group B_3, where the parabolic P corresponds again to the central vertex.

If, instead of identifying them, we fuse together the ideals I_2 and I_3 by direct sum, this corresponds at the level of Dynkin diagrams to fusing the vertices labelled I_2 and I_3 in the diagram of D_4 with an additional vertex; this yields:



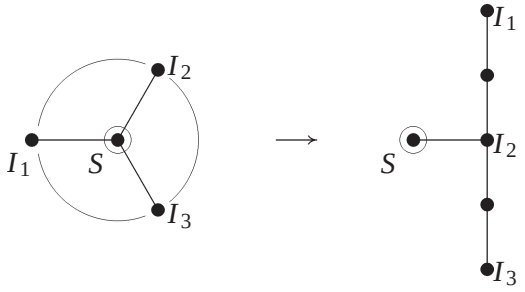
and we have obtained the Dynkin diagram D_5. Hence the composition law on pairs of quaternary alternating 2-forms, as discussed in Sections 2.6 and 3.6, arises in this sense from the group D_5, where P again is the maximal parabolic corresponding to the (circled) vertex labelled S.

Let us now identify all three ideals I_1, I_2, I_3. This corresponds, on the level of Dynkin diagrams, to the triple identification



yielding the Dynkin diagram G_2. Thus the composition law on binary cubic forms, discussed in Sections 2.4 and 3.4, arises in this sense from the Lie group G_2.

Finally, if we fuse together all three ideals I_1, I_2, I_3 by direct sum, this means we take all the outer vertices of the Dynkin diagram D_4 and fuse them together with vertices in between, to obtain



and this is the Dynkin diagram E_6. That is, the composition of alternating 3-forms in six variables, discussed in Sections 2.7 and 3.7, is related in this way to the exceptional Lie group E_6.

Our discussion above shows, in sum, that quadratic composition stems essentially from the triply-symmetric Dynkin diagram of the Lie group D_4, together with its parabolic subgroup corresponding to the central vertex.

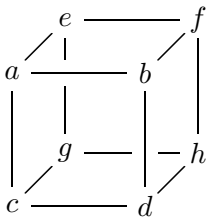
Are there a Lie group and parabolic that might lead to cubic composition laws? The answer, remarkably, is yes. This question (and its answer) will be treated fully in the next article.

Appendix: Equivalence of the cube law and Gauss composition

The most elementary way to see the equivalence of the Cube Law and Gauss composition is probably via the definition of Gauss composition due to Dirichlet [3]. In this appendix, we show how Dirichlet composition can be derived in a very natural and simple manner from the Cube Law.

Suppose we have a projective cube

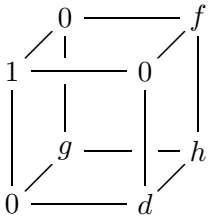
(39)



.

Since the cube is projective, the greatest common divisor of its entries is 1. Therefore, by applying elements of $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$, we may obtain an entry "1" in the $(1,1,1)$ position; that is, we may find an equivalent cube with $a = 1$ in (39). This "1" entry can then be used to clear out the three adjacent entries in the cube, i.e., we may arrange for $b = c = e = 0$. Thus we see that any projective cube can be transformed by an element of Γ to some cube of the form

(40)



.

Let us write down the three quadratic forms Q_1, Q_2, Q_3 associated to the cube (40). We have

$$\begin{aligned} Q_1 &= -dx^2 + hxy + fgy^2 \\ Q_2 &= -gx^2 + hxy + dfy^2 \\ Q_3 &= -fx^2 + hxy + dgy^2. \end{aligned} \tag{41}$$

Now the Cube Law declares that $[Q_1] + [Q_2] = -[Q_3]$, and therefore

$$[-dx^2 + hxy + fgy^2] + [-gx^2 + hxy + dfy^2] = [dgx^2 + hxy - fy^2].$$

This is precisely Dirichlet composition.

Acknowledgments. This article is based on Chapters 1 and 2 of the author's Ph.D. thesis [2] at Princeton University. I am extremely grateful to my advisor Professor A. Wiles and to Professor P. Sarnak for all their enthusiasm, encouragement, and guidance during this work. I am also very thankful to Professors P. Deligne, B. Gross, H. W. Lenstra, J-P. Serre and especially D. Zagier for their careful reading and for many helpful comments on earlier versions of this manuscript.

I extend my gratitude to the Hertz Foundation for funding this work, and to the Clay Mathematics Institute for their subsequent support.

Clay Mathematics Institute, Cambridge, MA
Princeton University, Princeton, NJ
E-mail address: bhargava@math.princeton.edu

References

[1] H. Bass, Torsion free and projective modules, *Trans. Amer. Math. Soc.* **102** (1962), 319–327.

[2] M. Bhargava, Higher Composition Laws, Ph.D. Thesis, Princeton University, June 2001.

[3] P. G. L. Dirichlet, *Zahlentheorie*, 4th. edition, Vieweg Brunswick, 1894.

[4] G. Eisenstein, Théorèmes sur les formes cubiques et solution d'une équation du quatrième degré indéterminées, *J. reine angew. Math.* **27** (1844), 75–79.

[5] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[6] D. Hilbert, *Theory Of Algebraic Invariants*, Engl. trans. by R. C. Laubenbacher, Cambridge University Press, 1993.

[7] M. Sato and T. Kimura, A classification of irreducible prehomogeneous vector spaces and their relative invariants, *Nagoya Math. J.* **65** (1977), 1–155.

[8] J-P. Serre, Modules projectifs et espaces fibrés à fibre vectorielle, *Séminaire Dubreil-Pisot* 1957/58, no. 23.

[9] D. J. Wright and A. Yukie, Prehomogeneous vector spaces and field extensions, *Invent. Math.* **110** (1992), 283–314.

(Received November 13, 2001)