Annals of Mathematics, **159** (2004), 865–886

Higher composition laws II: On cubic analogues of Gauss composition

By Manjul Bhargava

1. Introduction

In our first article [2] we developed a new view of Gauss composition of binary quadratic forms which led to several new laws of composition on various other spaces of forms. Moreover, we showed that the groups arising from these composition laws were closely related to the class groups of orders in quadratic number fields, while the spaces underlying those composition laws were closely related to certain exceptional Lie groups. In this paper, our aim is to develop analogous laws of composition on certain spaces of forms so that the resulting groups yield information on the class groups of orders in *cubic* fields; that is, we wish to obtain genuine "cubic analogues" of Gauss composition.

The fundamental object in our treatment of quadratic composition [2] was the space of $2 \times 2 \times 2$ cubes of integers. In particular, Gauss composition arose from the three different ways of slicing a cube A into two 2×2 matrices M_i, N_i $(i = 1, 2, 3)$. Each such pair (M_i, N_i) gives rise to a binary quadratic form $Q_i^A(x, y) = Q_i(x, y)$, defined by $Q_i(x, y) = -\mathrm{Det}(M_i x + N_i y)$. The Cube Law of [2] declares that as A ranges over all cubes, the sum of $[Q_1]$, $[Q_2]$, $[Q_3]$ is zero. It was shown in [2] that the Cube Law gives a law of addition on binary quadratic forms that is equivalent to Gauss composition. Various other invariant-theoretic constructions using the space of $2 \times 2 \times 2$ cubes led to several new composition laws on other spaces of forms. Furthermore, we showed that each of these composition laws gave rise to groups that are closely related to the class groups of orders in quadratic fields.

Based on the quadratic case described above, our first inclination for the cubic case might be to examine $3 \times 3 \times 3$ cubes of integers. A $3 \times 3 \times 3$ cube C can be sliced (in three different ways) into three 3×3 matrices L_i, M_i, N_i $(i = 1, 2, 3)$. We may therefore obtain from C three ternary cubic forms $f_1(x, y, z), f_2(x, y, z), f_3(x, y, z)$, defined by

$$f_i(x, y, z) = -\mathrm{Det}(L_i x + M_i y + N_i z).$$

We may declare a cubic analogue of the "Cube Law" of [2] by demanding that $[f_1] + [f_2] + [f_3] = [f]$ for some appropriate $[f]$.

This procedure does in fact yield a law of composition on ternary cubic forms, and gives the desired group structure on the norm forms of ideal classes in cubic rings.[1] The only problem is that it gives us a bit more than we want, for the norm form of an ideal class in a cubic ring is always a *decomposable form*, i.e., one that decomposes into linear factors over $\bar{\mathbb{Q}}$. On the other hand, our group law arising from $3 \times 3 \times 3$ cubes gives a law of composition not just on decomposable forms, but on general ternary cubic forms. Since our interest in composition laws here is primarily for their connection with class groups, we should like to "slice away" a part of the space of $3 \times 3 \times 3$ cubes somehow so as to extract only the part of the space corresponding to ideal classes.

How this slicing should occur becomes apparent upon examination of how cubic rings are parametrized. Since cubic rings do not correspond to ternary cubic forms, but rather to binary cubic forms (as was shown by Delone-Faddeev [4]), this indicates that we should perhaps slice away one layer of the $3 \times 3 \times 3$ cube to retain only a $2 \times 3 \times 3$ box of integers, so that the one $\mathrm{SL}_3 \times \mathrm{SL}_3$-invariant is a binary cubic form, while the other two dimensions might then correspond to ideal classes in the associated cubic ring.

This space of $2 \times 3 \times 3$ boxes does indeed turn out to be exactly what is needed for a cubic analogue of Gauss's theory. There is again a natural composition law on this space, and we prove that the groups obtained via this law of composition are isomorphic to the class groups of cubic orders. In addition, by applying the symmetrization and skew-symmetrization processes as introduced in [2], we obtain two further cubic laws of composition. These composition laws are defined on 1) pairs of ternary quadratic forms, and 2) pairs of senary (six-variable) alternating 2-forms. In the case of pairs of ternary quadratic forms, we show that the corresponding groups are equal roughly to the 2-parts of the ideal class groups of cubic rings. In the case of pairs of senary alternating 2-forms, we show that the corresponding groups are trivial.

The three spaces of forms mentioned above were considered over algebraically closed fields in the monumental work of Sato-Kimura [9] classifying prehomogeneous vector spaces. Over other fields such as the rational numbers, these spaces were again considered in the important work of Wright and Yukie [12]. In particular, they indicated that—at least over a field F—there is a strong analogy between the space of $2 \times 3 \times 3$ matrices and Gauss's space of binary quadratic forms. Specifically, they showed that nondegenerate orbits in this space of matrices over F—under the natural action of $\mathrm{GL}_2(F) \times \mathrm{GL}_3(F) \times \mathrm{GL}_3(F)$—correspond bijectively with étale cubic extensions L of F, while the corresponding point stabilizers are closely related to

[1] Here, f must be taken to be the norm form of the "inverse different" ideal of the desired cubic ring. (In fact, the same is true also in the quadratic case, but since the ideal class of the inverse different is always trivial, this was not visible in the construction.)

the group $\mathrm{GL}_1(L)$. This is in direct analogy with the space of binary quadratic forms over F, where $\mathrm{GL}_2(F)$-orbits correspond to étale quadratic extensions K of F, while point stabilizers are essentially given by $\mathrm{GL}_1(K)$. In the current paper we obtain a full integral realization of their observation and analogy over fields. As in Gauss's original work [6], we consider here orbits over the integers $\mathbb{Z}$; as we shall see, these integer orbits have an extremely rich structure, leading to analogues of Gauss composition corresponding to orders and ideal classes in cubic fields.

We also determine the precise point stabilizers in $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ of the elements in the space of $2 \times 3 \times 3$ integer matrices. Just as stabilizers in $\mathrm{GL}_2(\mathbb{Z})$ of integer points in the space of binary quadratic forms correspond to the unit groups of orders in quadratic fields, we prove that generic stabilizers in $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ of points in the space of $2 \times 3 \times 3$ integer boxes correspond to the unit groups of orders in cubic fields. We similarly determine the stabilizers over $\mathbb{Z}$ of the other two spaces of forms indicated above, again in terms of the unit groups of orders in cubic fields.

This article is organized as follows. Each of the three spaces of forms mentioned above possesses a natural action by a product of linear groups over $\mathbb{Z}$. In Section 2, we classify the orbits of this group action explicitly in terms of ideal classes of cubic orders, whenever the unique invariant for this group action (which we call the *discriminant*) does not vanish. In Section 3, we discuss the composition laws that then arise on the orbits of these three spaces, and we describe the resulting groups in terms of ideal class groups of cubic rings. Finally, the work contained herein was motivated in part by staring at Dynkin diagrams of appropriate exceptional Lie groups; this still mysterious connection with the exceptional groups is discussed in Section 4.

2. Cubic composition and $2 \times 3 \times 3$ boxes of integers

In this section we examine the natural action of the group $\bar{\Gamma} = \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ on the space $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$, which we may naturally identify with the space of $2 \times 3 \times 3$ integer matrices. As such matrices have a bit less symmetry than the $2 \times 2 \times 2$ cubes of [2], there is essentially only one slicing of interest, namely, the one which splits a $2 \times 3 \times 3$ box into two 3×3 submatrices. Hence we will also identify the space $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ of $2 \times 3 \times 3$ integer boxes with the space of pairs (A, B) of 3×3 integer matrices.

2.1. *The unique* Γ*-invariant* $\mathrm{Disc}(A, B)$. In studying the orbits of $\bar{\Gamma} = \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ on pairs (A, B) of 3×3 matrices, it suffices to restrict the $\bar{\Gamma}$-action to the subgroup $\Gamma = \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$, since $(-I_2, -I_3, I_3)$ and $(-I_2, I_3, -I_3)$ in $\bar{\Gamma}$ act trivially on all pairs (A, B). Moreover, unlike $\bar{\Gamma}$, the group Γ acts faithfully.

We observe that the action of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ on its 18-dimensional representation $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ has just a single polynomial invariant.[2] Indeed, the action of $\mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ on $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ has four independent invariants, namely the coefficients of the binary cubic form

$$f(x, y) = \mathrm{Det}(Ax - By). \tag{1}$$

The group $\mathrm{GL}_2(\mathbb{Z})$ acts on the cubic form $f(x, y)$, and it is well-known that this action has exactly one polynomial invariant (see, e.g., [7]), namely the discriminant $\mathrm{Disc}(f)$ of f. Hence the unique $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$-invariant on $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ is given by $\mathrm{Disc}(\mathrm{Det}(Ax - By))$. We call this fundamental invariant the *discriminant* of (A, B), and denote it by $\mathrm{Disc}(A, B)$. If $\mathrm{Disc}(A, B)$ is nonzero, we say that (A, B) is a *nondegenerate* element of $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$. Similarly, we call a binary cubic form f *nondegenerate* if $\mathrm{Disc}(f)$ is nonzero.

2.2. *The parametrization of cubic rings.* The parametrization of cubic orders by integral binary cubic forms was first discovered by Delone and Faddeev in their famous treatise on cubic irrationalities [4]; this parametrization was refined recently to general cubic rings by Gan-Gross-Savin [5] and by Zagier (unpublished). Their construction is as follows. Given a cubic ring R (i.e., any ring free of rank 3 as a $\mathbb{Z}$-module), let $\langle 1, \omega, \theta \rangle$ be a $\mathbb{Z}$-basis for R. Translating ω, θ by the appropriate elements of $\mathbb{Z}$, we may assume that $\omega \cdot \theta \in \mathbb{Z}$. We call a basis satisfying the latter condition *normalized*, or simply *normal*. If $\langle 1, \omega, \theta \rangle$ is a normal basis, then there exist constants $a, b, c, d, \ell, m, n \in \mathbb{Z}$ such that

$$\begin{array}{rcl} \omega\theta &=& n \\ \omega^2 &=& m + b\omega - a\theta \\ \theta^2 &=& \ell + d\omega - c\theta. \end{array} \tag{2}$$

To the cubic ring R with multiplication table as above, we associate the binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Conversely, given a binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, form a potential cubic ring having multiplication laws (2). The values of ℓ, m, n are subject to the associative law relations $\omega\theta \cdot \theta = \omega \cdot \theta^2$ and $\omega^2 \cdot \theta = \omega \cdot \omega\theta$, which when multiplied out using (2), yield a system of equations possessing the unique solution $(n, m, \ell) = (-ad, -ac, -bd)$, thus giving

$$\begin{array}{rcl} \omega\theta &=& -ad \\ \omega^2 &=& -ac + b\omega - a\theta \\ \theta^2 &=& -bd + d\omega - c\theta. \end{array} \tag{3}$$

If follows that any binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, via the recipe (3), leads to a unique cubic ring $R = R(f)$.

[2] As in [2], we use the convenient phrase "single polynomial invariant" to mean that the polynonomial invariant ring is generated by one element.

Lastly, one observes by an explicit calculation that changing the $\mathbb{Z}$-basis $\langle \omega, \theta \rangle$ of $R/\mathbb{Z}$ by an element of $\mathrm{GL}_2(\mathbb{Z})$, and then renormalizing the basis in R, transforms the resulting binary cubic form $f(x, y)$ by that same element of $\mathrm{GL}_2(\mathbb{Z})$.[3] Hence an isomorphism class of cubic ring determines a binary cubic form uniquely up to the action of $\mathrm{GL}_2(\mathbb{Z})$. It follows that isomorphism classes of cubic rings are parametrized by integral binary cubic forms modulo $GL_2(\mathbb{Z})$-equivalence.

One finds by a further calculation that the discriminant of a cubic ring $R(f)$ is precisely the discriminant of the binary cubic form f. We summarize this discussion as follows:

THEOREM 1 ([4],[5]). *There is a canonical bijection between the set of* $\mathrm{GL}_2(\mathbb{Z})$*-equivalence classes of integral binary cubic forms and the set of isomorphism classes of cubic rings, by the association*

$$f \leftrightarrow R(f).$$

Moreover, $\mathrm{Disc}(f) = \mathrm{Disc}(R(f))$.

We say a cubic ring is *nondegenerate* if it has nonzero discriminant (equivalently, if it is an order in an étale cubic algebra over $\mathbb{Q}$). The discriminant equality in Theorem 1 implies, in particular, that nondegenerate cubic rings correspond bijectively with equivalence classes of nondegenerate integral binary cubic forms.

2.3. *Cubic rings and* $2 \times 3 \times 3$ *boxes of integers.* In this section we classify the nondegenerate Γ-orbits on $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ in terms of ideal classes in cubic rings. Before stating the result, we recall some definitions. As in [2], we say that a pair (I, I') of (fractional) R-ideals in $K = R \otimes \mathbb{Q}$ is *balanced* if $II' \subseteq R$ and $N(I)N(I') = 1$. Furthermore, two such balanced pairs (I_1, I_1') and (I_2, I_2') are called *equivalent* if there exists an invertible element $\kappa \in K$ such that $I_1 = \kappa I_2$ and $I_1' = \kappa^{-1} I_2'$. For example, if R is a Dedekind domain then an equivalence class of balanced pairs of ideals is simply a pair of ideal classes that are inverse to each other in the ideal class group.

THEOREM 2. *There is a canonical bijection between the set of nondegenerate* Γ*-orbits on the space* $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ *and the set of isomorphism classes of pairs* $(R, (I, I'))$*, where* R *is a nondegenerate cubic ring and* (I, I') *is an equivalence class of balanced pairs of ideals of* R*. Under this bijection, the discriminant of an integer* $2 \times 3 \times 3$ *box equals the discriminant of the corresponding cubic ring.*

[3] In basis-free terms, the binary cubic form f represents the mapping $R/\mathbb{Z} \to \wedge^3 R \cong \mathbb{Z}$ given by $\xi \mapsto 1 \wedge \xi \wedge \xi^2$, making this transformation property obvious.

Proof. Given a pair of balanced R-ideals I and I', we first show how to construct a corresponding pair (A, B) of 3×3 integer matrices. Let $\langle 1, \omega, \theta \rangle$ denote a normal basis of R, and let $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and $\langle \beta_1, \beta_2, \beta_3 \rangle$ denote any $\mathbb{Z}$-bases for the ideals I and I' having the same orientation as $\langle 1, \omega, \theta \rangle$. Then since $II' \subseteq R$, we must have

$$\alpha_i \beta_j = c_{ij} + b_{ij}\omega + a_{ij}\theta \tag{4}$$

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

By construction, it is clear that changing $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ or $\langle \beta_1, \beta_2, \beta_3 \rangle$ to some other basis of I or I' via a matrix in $\mathrm{SL}_3(\mathbb{Z})$ would simply transform A and B by left or right multiplication by that same matrix. Similarly, a change of basis from $\langle 1, \omega, \theta \rangle$ to another normal basis $\langle 1, \omega', \theta' \rangle$ of R is completely determined by a unique element $\left(\begin{smallmatrix} r & s \\ u & v \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, where

$$\begin{aligned} \omega' &= q + r\omega + s\theta \\ \theta' &= t + u\omega + v\theta \end{aligned}$$

for some integers q, t. It is easily checked that this change of basis transforms (A, B) by the same element $\left(\begin{smallmatrix} r & s \\ u & v \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$. Conversely, any pair of 3×3 matrices in the same Γ-orbit as (A, B) can actually be obtained from $(R, (I, I'))$ in the manner described above, simply by changing the bases for R, I, and I' appropriately.

Next, suppose (J, J') is a balanced pair of ideals of R that is equivalent to (I, I'), and let κ be the invertible element in $R \otimes \mathbb{Q}$ such that $J = \kappa I$ and $J' = \kappa^{-1} I'$. If we choose bases for I, I', J, J' to take the form $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$, $\langle \beta_1, \beta_2, \beta_3 \rangle$, $\langle \kappa\alpha_1, \kappa\alpha_2, \kappa\alpha_3 \rangle$, and $\langle \kappa'\beta_1, \kappa'\beta_2, \kappa'\beta_3 \rangle$ respectively, then it is immediate from (4) that $(R, (I, I'))$ and $(R, (J, J'))$ will yield identical elements (A, B) in $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$. It follows that the association $(R, (I, I')) \to (A, B)$ is a well-defined map even on the level of equivalence classes.

It remains to show that our mapping $(R, (I, I')) \to (A, B)$ from the set of equivalence classes of pairs $(R, (I, I'))$ to the space $(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3)/\Gamma$ is in fact a bijection. To this end, let us fix the 3×3 matrices $A = (a_{ij})$ and $B = (b_{ij})$, and consider the system (4), which at this point consists mostly of indeterminates. We show in several steps that these indeterminates are in fact essentially determined by the pair (A, B).

First, we claim that the ring structure of $R = \langle 1, \omega, \theta \rangle$ is completely determined. Indeed, let us write the multiplication in R in the form (3), with unknown integers a, b, c, d, and let $f = ax^3 + bx^2y + cxy^2 + dy^3$. We claim that the system of equations (4) implies the following identity:

$$\mathrm{Det}(Ax - By) = N(I)N(I') \cdot (ax^3 + bx^2y + cxy^2 + dy^3). \tag{5}$$

To prove this identity, we begin by considering the simplest case, where we have $I = I' = R$, with identical $\mathbb{Z}$-bases $\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \langle \beta_1, \beta_2, \beta_3 \rangle = \langle 1, \omega, \theta \rangle$. In this case, from the multiplication laws (3) we see that the pair (A, B) in (4) is given by

$$(A, B) = \left(\begin{bmatrix} & & 1 \\ & -a & \\ 1 & & -c \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & b & \\ & & d \end{bmatrix} \right). \tag{6}$$

For this (A, B), one finds that indeed $\mathrm{Disc}(Ax - By) = ax^3 + bx^2y + cxy^2 + dy^3$, proving the identity in this special case.

Now suppose that I and I' are changed to general fractional ideals of R, having $\mathbb{Z}$-bases $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and $\langle \beta_1, \beta_2, \beta_3 \rangle$ respectively. Then there exist transformations T, $T' \in \mathrm{SL}_3(\mathbb{Q})$ taking $\langle 1, \omega, \theta \rangle$ to the new bases $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and $\langle \beta_1, \beta_2, \beta_3 \rangle$ respectively, and so the new (A, B) in (4) may be obtained by transforming the pair of matrices on the right side of (6) by left multiplication by T and by right multiplication by T'. The binary cubic form $\mathrm{Det}(Ax - By)$ is therefore seen to multiply by a factor of $\det(T)\det(T') = N(I)N(I')$, proving identity (5) for general I and I'.

Now by assumption we have $N(I)N(I') = 1$, so identity (5) implies

$$\mathrm{Det}(Ax - By) = f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3; \tag{7}$$

thus the matrices A and B do indeed determine $f(x, y)$ and hence the ring R.

Next, we show that the quantities c_{ij} in (4) are also completely determined by A and B. By the associative law in R, we have nine equations of the form

$$(\alpha_i \beta_j)(\alpha_{i'} \beta_{j'}) = (\alpha_i \beta_{j'})(\alpha_{i'} \beta_j), \tag{8}$$

for $1 \le i, i', j, j' \le 3$. Expanding these identities out using (4), (3), and (7), and then equating the coefficients of 1, ω, and θ, yields a system of 18 linear and 9 quadratic equations in the 9 indeterminates c_{ij} in terms of a_{ij} and b_{ij}. We find that this system has exactly one (quite pretty) solution, given by

$$c_{ij} = \sum_{i' < i'',\, j' < j''} \left(\begin{smallmatrix} i & i' & i'' \\ 1 & 2 & 3 \end{smallmatrix}\right) \left(\begin{smallmatrix} j & j' & j'' \\ 1 & 2 & 3 \end{smallmatrix}\right) \begin{vmatrix} a_{ij} & a_{ij'} \\ a_{i'j} & a_{i'j'} \end{vmatrix} \cdot \begin{vmatrix} b_{ij} & b_{ij''} \\ b_{i''j} & b_{i''j''} \end{vmatrix} \tag{9}$$

where $\left(\begin{smallmatrix} r & s & t \\ 1 & 2 & 3 \end{smallmatrix}\right)$ denotes the sign of the permutation (r, s, t) of $(1, 2, 3)$. (Note that the solutions for the $\{c_{ij}\}$ are necessarily integral, since they are polynomials in the a_{ij} and b_{ij}!) Thus the c_{ij}'s are also uniquely determined by (A, B).

We still must determine the existence of $\alpha_i, \beta_j \in R$ yielding the desired a_{ij}, b_{ij}, and c_{ij}'s in (4). An examination of the system (4) shows that we have

$$\alpha_1 : \alpha_2 : \alpha_3 = c_{1j} + b_{1j}\omega + a_{1j}\theta : c_{2j} + b_{2j}\omega + a_{2j}\theta : c_{3j} + b_{3j}\omega + a_{3j}\theta, \tag{10}$$

for any $1 \le j \le 3$. That the ratio on the right-hand side of (10) is independent of the choice of j follows from the identities (8) that we have forced on the

system (4). Thus the triple $(\alpha_1, \alpha_2, \alpha_3)$ is uniquely determined up to a factor in K^*. Once the basis $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ of I is chosen, then the basis $\langle \beta_1, \beta_2, \beta_3 \rangle$ for I' is given directly from (4), since the c_{ij}, b_{ij}, and a_{ij} are known. Therefore the pair (I, I') is uniquely determined up to equivalence.

To see that this object $(R, (I, I'))$ as determined above forms a valid pair in the sense of Theorem 2, we must only check that I and I', currently given only as $\mathbb{Z}$-modules in K, are actually fractional ideals of R. In fact, using explicit embeddings of I and I' into K, or by examining (4) directly, one can calculate the exact R-module structures of I' and I explicitly in terms of (A, B); these module structures are too beautiful to be left unmentioned.

Given a matrix M, let us use M_i to denote the i-th column of M and $|M|$ to denote the determinant of M. Then the R-module structure of I' is given by

$$\begin{aligned}
-\omega \cdot \alpha_1 &= |B_1A_2A_3| \cdot \alpha_1 + |A_1B_1A_3| \cdot \alpha_2 + |A_1A_2B_1| \cdot \alpha_3 \\
-\omega \cdot \alpha_2 &= |B_2A_2A_3| \cdot \alpha_1 + |A_1B_2A_3| \cdot \alpha_2 + |A_1A_2B_2| \cdot \alpha_3 \\
-\omega \cdot \alpha_3 &= |B_3A_2A_3| \cdot \alpha_1 + |A_1B_3A_3| \cdot \alpha_2 + |A_1A_2B_3| \cdot \alpha_3 \\
-\theta \cdot \alpha_1 &= |A_1B_2B_3| \cdot \alpha_1 + |B_1A_1B_3| \cdot \alpha_2 + |B_1B_2A_1| \cdot \alpha_3 \\
-\theta \cdot \alpha_2 &= |A_2B_2B_3| \cdot \alpha_1 + |B_1A_2B_3| \cdot \alpha_2 + |B_1B_2A_2| \cdot \alpha_3 \\
-\theta \cdot \alpha_3 &= |A_3B_2B_3| \cdot \alpha_1 + |B_1A_3B_3| \cdot \alpha_2 + |B_1B_2A_3| \cdot \alpha_3,
\end{aligned} \tag{11}$$

while the R-module structure of I is given analogously in terms of the rows of A and B rather than the columns. It is evident that all the structure coefficients above are integers, and this concludes the proof of Theorem 2. □

Our discussion makes the bijection of Theorem 2 very precise. Given a cubic order R and a balanced pair (I, I') of ideals in R, the corresponding element $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ is obtained from the set of equations (4). Conversely, given an element $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$, the ring R is determined by (3) and (7); bases for the ideal classes I and I' of R may be obtained from (10) and (4), and the R-module structures of I and I' are given by (11).

Note that the algebraic formulae in the proof of Theorem 2 could be used to extend the bijection also to *degenerate* orbits, i.e., orbits where the discriminant is zero. Such orbits correspond to cubic rings R of discriminant zero, together with a balanced pair of R-modules I, I' having rank 3 over $\mathbb{Z}$. The condition of "balanced", however, becomes even harder to understand in the degenerate case! To avoid such technicalities we have stated the result only in the primary cases of interest, namely those involving nondegenerate orbits and rings.[4]

[4]It is an interesting question to formulate a module-theoretic definition of "balanced" that applies over any ring, and that is functorial (i.e., respects extension by scalars). This would allow one to directly extend Theorem 2 both to degenerate orbits and to orbits over an arbitrary commutative ring.

The proof of Theorem 2 not only gives a complete description of the nondegenerate orbits of the representation of Γ on $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ in terms of cubic rings, but also allows us to precisely determine the point stabilizers. We have the following

COROLLARY 3. *The stabilizer in* Γ *of a nondegenerate element* $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ *is given by the semidirect product*

$$\mathrm{Aut}(R) \ltimes U^+(R_0),$$

where $(R, (I, I'))$ *is the pair corresponding to* (A, B) *as in Theorem* 2, $R_0 = \mathrm{End}_R(I) \cap \mathrm{End}_R(I')$ *is the intersection of the endomorphism rings of* I *and* I', *and* $U^+(R_0)$ *denotes the group of units of* R_0 *having positive norm.*

Note that if I, I' are projective R-modules, then $R_0 = R$, so that the stabilizer of (A, B) in Γ is simply $\mathrm{Aut}(R) \ltimes U^+(R)$. This is in complete analogy with Gauss's case of binary quadratic forms, where generic stablizers are given by the groups of units of positive norm in the corresponding quadratic endomorphism rings.

Proof. The proof of Theorem 2 shows that an element (A, B) uniquely determines the multiplication table of R, in terms of some basis $\langle 1, \omega, \theta \rangle$. Elements of $\mathrm{GL}_2(\mathbb{Z})$ that send this basis to another basis $\langle 1, \omega', \theta' \rangle$ with the identical multiplication table evidently correspond to elements of $\mathrm{Aut}(R)$. Once this automorphism has been fixed, the system of equations (10) then uniquely determines the triples $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$ up to factors $\kappa, \kappa^{-1} \in K^*$. It follows that an element $T \times T' \in \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ acting on the bases $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and $\langle \beta_1, \beta_2, \beta_3 \rangle$ of I and I' respectively will preserve (10) if and only if $T\alpha_i = \kappa\alpha_i$ and $T'\beta_j = \kappa^{-1}\beta_j$. In other words, T acts as multiplication by a unit κ in the endomorphism ring of I, while T' acts as the inverse $\kappa^{-1} \in \mathrm{End}_R(I')$ on I'. This is the desired conclusion. □

2.4. *Cubic rings and pairs of ternary quadratic forms.* Just as we were able to impose a symmetry condition on $2 \times 2 \times 2$ matrices to obtain information on the exponent 3-parts of class groups of quadratic rings ([2, §2.4]), we can impose a symmetry condition on $2 \times 3 \times 3$ matrices to yield information on the exponent 2-parts of class groups of cubic rings. The "symmetric" elements in $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ are precisely the elements of $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$, i.e., pairs (A, B) of symmetric 3×3 integer matrices, or equivalently, pairs (A, B) of integral ternary quadratic forms. The cubic form invariant f and the *discriminant* $\mathrm{Disc}(A, B)$ of (A, B) may be defined in the identical manner; we have $f(x, y) = \mathrm{Det}(Ax - By)$ and $\mathrm{Disc}(A, B) = \mathrm{Disc}(\mathrm{Det}(Ax - By))$. Again, we say an element $(A, B) \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$ is *nondegenerate* if $\mathrm{Disc}(A, B)$ is nonzero.

The precise correspondence between nondegenerate pairs of ternary quadratic forms and ideal classes "of order 2" in cubic rings is then given by the following theorem.

THEOREM 4. *There is a canonical bijection between the set of nondegenerate* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$*-orbits on the space* $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$ *and the set of equivalence classes of triples* (R, I, δ)*, where* R *is a nondegenerate cubic ring,* I *is an ideal of* R*, and* δ *is an invertible element of* $R \otimes \mathbb{Q}$ *such that* $I^2 \subseteq (\delta)$ *and* $N(\delta) = N(I)^2$*. (Here two triples* (R, I, δ) *and* (R', I', δ') *are equivalent if there exists an isomorphism* $\phi : R \to R'$ *and an element* $\kappa \in R' \otimes \mathbb{Q}$ *such that* $I' = \kappa\phi(I)$ *and* $\delta' = \kappa^2\phi(\delta)$*.) Under this bijection, the discriminant of a pair of ternary quadratic forms equals the discriminant of the corresponding cubic ring.*

Proof. For a triple (R, I, δ) as above, we first show how to construct a corresponding pair (A, B) of ternary quadratic forms. Let $\langle 1, \omega, \theta \rangle$ denote a normal basis of R, and let $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ denote a $\mathbb{Z}$-basis of the ideal I having the same orientation as $\langle 1, \omega, \theta \rangle$. Since by hypothesis I is an ideal whose square is contained in $\delta \cdot R$, we must have

$$\alpha_i\alpha_j = \delta\,(\,c_{ij} + b_{ij}\omega + a_{ij}\theta\,) \tag{12}$$

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

The matrices A and B can naturally be viewed as quadratic forms on the lattice $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3$. Hence changing $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ to some other basis of I, via an element of $\mathrm{SL}_3(\mathbb{Z})$, would simply transform (A, B) (via the natural $\mathrm{SL}_3(\mathbb{Z})$-action) by that same element. Also, just as in Theorem 2, a change of the basis $\langle 1, \omega, \theta \rangle$ to another normal basis by an element of $\mathrm{GL}_2(\mathbb{Z})$ transforms (A, B) by that same element. We conclude that our map from equivalence classes of triples (R, I, δ) to equivalence classes of pairs (A, B) of ternary quadratic forms is well-defined.

To show that this map is a bijection, we fix the pair $A = (a_{ij})$ and $B = (b_{ij})$ of ternary quadratic forms, and then show that these values determine all the indeterminates in the system (12). First, to show that the ring R is determined, we assume that R has multiplication given by the equations in (3) for unknown integers a, b, c, d, and as in the proof of Theorem 2, we derive from (12) the identity

$$\begin{aligned} \mathrm{Det}(Ax - By) &= N(I)^2 N(\delta)^{-1} \cdot (ax^3 + bx^2y + cxy^2 + dy^3) \\ &= ax^3 + bx^2y + cxy^2 + dy^3, \end{aligned} \tag{13}$$

where we have used the hypothesis that $N(\delta) = N(I)^2$. It follows as before that the ring R is determined by the pair (A, B).

Next we use the associative law in R to show that the constants c_{ij} in the system (12) are uniquely determined. We have three identities of the form $(\delta^{-1}\alpha_1^2)(\delta^{-1}\alpha_2^2) = (\delta^{-1}\alpha_1\alpha_2)^2$, and three more of the form $(\delta^{-1}\alpha_1^2)(\delta^{-1}\alpha_2\alpha_3) = (\delta^{-1}\alpha_1\alpha_2)(\delta^{-1}\alpha_1\alpha_3)$. Expanding out all six of these using (3) and (12), and then equating the coefficients of 1, ω, and θ, yields a system of 18 linear and quadratic equations in the six indeterminates $c_{11}, c_{22}, c_{33}, c_{12}, c_{13}, c_{23}$. This system in the c_{ij} has a unique solution, given again by (9).

Now an examination of the system (12) shows that we have

$$\alpha_1 : \alpha_2 : \alpha_3 = c_{1j} + b_{1j}\omega + a_{1j}\theta : c_{2j} + b_{2j}\omega + a_{2j}\theta : c_{3j} + b_{3j}\omega + a_{3j}\theta \,, \tag{14}$$

and the latter ratio is independent of the choice of $j \in \{1, 2, 3\}$. Thus the triple $(\alpha_1, \alpha_2, \alpha_3)$ is uniquely determined up to a factor in R. Regardless of how the triple $(\alpha_1, \alpha_2, \alpha_3)$ is scaled, this then determines δ uniquely up to a square factor in R.

Finally, to see that this object (R, I, δ) is really a valid triple in the sense of Theorem 4, we must only check that I is an ideal of R. Again, the R-module structure of I can be determined explicitly in terms of (A, B), and is given by (11). This completes the proof of Theorem 4. □

The proof gives very precise information about the bijection of Theorem 4. Given a triple (R, I, δ), the corresponding pair (A, B) of ternary quadratic forms is obtained from equations (12). Conversely, given an element $(A, B) \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$, the ring R is determined by (3) and (13); a basis for the ideal class I may be obtained from (14), and the R-module structure of I is given by (11).

Again, we may determine precisely the point stabilizers:

COROLLARY 5. *The stabilizer in* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ *of a nondegenerate element* $(A, B) \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$ *is given by the semidirect product*

$$\mathrm{Aut}(R) \ltimes U_2^+(R_0),$$

where (R, I) *is the pair corresponding to* (A, B) *as in Theorem* 4, $R_0 = \mathrm{End}_R(I)$ *is the endomorphism ring of* I, *and* $U_2^+(R_0)$ *denotes the group of units of* R_0 *having order dividing* 2 *and positive norm.*

Note that $\mathrm{Aut}(R)$ is contained in the symmetric group S_3, while $U_2^+(R)$ must be contained in the Klein-four group K_4. It follows that the stabilizers occurring in Corollary 5 are contained in the *finite group* $S_3 \ltimes K_4 = S_4$. This is consistent with the results of Sato-Kimura [9] and Wright-Yukie [12] over fields.

If I is projective over R, then $R_0 = R$ so that the stabilizer of (A, B) is simply given by $\mathrm{Aut}(R) \ltimes U_2^+(R)$. Corollary 5 may be proven in a manner similar to Corollary 3, and so we omit the proof.

2.5. *Cubic rings and pairs of senary alternating 2-forms.* As in [2], rather than a symmetry condition we may impose instead a skew-symmetry condition on $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ using the "fusion" operator of [2, Section 2.6]. More precisely, if we realize elements of the space $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ as pairs of skew-symmetric 6×6 matrices $(\mathcal{A}, \mathcal{B})$, then there is a natural map

$$\mathrm{id} \otimes \wedge_{3,3} : \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \to \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6 \tag{15}$$

defined by sending

$$(A, B) \mapsto \left(\begin{bmatrix} & A \\ -A^t & \end{bmatrix}, \begin{bmatrix} & B \\ -B^t & \end{bmatrix} \right). \tag{16}$$

The resulting skew-symmetrized space $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ has a natural action by the group $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_6(\mathbb{Z})$, and this group action again possesses a unique polynomial invariant. Indeed, a complete set of invariants for the action of $\mathrm{SL}_6(\mathbb{Z})$ on $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ is given by the four coefficients of the binary cubic form

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

and so the unique $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_6(\mathbb{Z})$-invariant is given by $\mathrm{Disc}(\mathrm{Pfaff}(\mathcal{A}x - \mathcal{B}y))$, which we again call the *discriminant* $\mathrm{Disc}(\mathcal{A}, \mathcal{B})$ of $(\mathcal{A}, \mathcal{B})$. It is evident from the explicit formula (16) that the map (15) is discriminant-preserving. As usual, we say an element in $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ is *nondegenerate* if it has nonzero discriminant.

Consistent with the pattern laid down in [2], the fused space $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ leads to the parametrization of certain rank 2 modules over cubic rings. Suppose R is any nondegenerate cubic ring, and let $K = R \otimes \mathbb{Q}$. As in [2], we consider rank 2 modules M over R as equipped with explicit embeddings into $K \oplus K$, i.e., as *rank* 2 *ideals*. Moreover, we say a rank 2 ideal $M \subseteq K \oplus K$ is *balanced* if $\mathrm{Det}(M) \subseteq R$ and $N(M) = 1$. Finally, two such rank 2 ideals are *equivalent* if one can be mapped to the other via an element of $\mathrm{SL}_2(K)$. Our parametrization result is then as follows:

THEOREM 6. *There is a canonical bijection between the set of nondegenerate* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_6(\mathbb{Z})$*-orbits on the space* $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$*, and the set of isomorphism classes of pairs* (R, M)*, where* R *is a nondegenerate cubic ring and* M *is an equivalence class of balanced ideals of* R *having rank* 2*. Under this bijection, the discriminant of a pair of senary alternating* 2*-forms is equal to the discriminant of the corresponding cubic ring.*

Proof. Given a pair (R, M) as in the theorem, we first show how to construct a corresponding pair of senary alternating 2-forms. Let again $\langle 1, \omega, \theta \rangle$ be a normal basis for R, and let $\langle \alpha_1, \alpha_2, \ldots, \alpha_6 \rangle$ denote an appropriately oriented $\mathbb{Z}$-basis for the rank 2 ideal M. By hypothesis, we may write

$$\det(\alpha_i, \alpha_j) = c_{ij} + b_{ij}\omega + a_{ij}\theta \tag{17}$$

for some 45 integers c_{ij}, b_{ij}, a_{ij} satisfying

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

for all $i, j \in \{1, 2, \ldots, 6\}$. Let $\mathcal{A}$ and $\mathcal{B}$ denote the 6×6 matrices (a_{ij}) and (b_{ij}) respectively. Then $(\mathcal{A}, \mathcal{B})$ represents our desired pair of senary alternating 2-forms.

By construction, it is clear that changing the basis for M by an element of $\mathrm{SL}_6(\mathbb{Z})$ simply transforms $(\mathcal{A}, \mathcal{B})$ by that same element. Hence the $\mathrm{SL}_6(\mathbb{Z})$-equivalence class of $(\mathcal{A}, \mathcal{B})$ is well-defined.

We wish to show that the mapping $(R, M) \to (\mathcal{A}, \mathcal{B})$ is in fact a bijection. To this end, let us fix an element $(\mathcal{A}, \mathcal{B}) \in \mathbb{Z}^2 \otimes \wedge^2 \mathbb{Z}^6$, and consider the system (17), which currently consists mostly of indeterminates. We show that essentially all constants in this system are uniquely determined by $(\mathcal{A}, \mathcal{B})$.

First we claim the ring R is determined by $(\mathcal{A}, \mathcal{B})$. To show this, we assume (3), and derive from (17) the identity

$$\begin{aligned} \mathrm{Pfaff}(\mathcal{A}x - \mathcal{B}y) &= N(M) \cdot (ax^3 + bx^2y + cxy^2 + dy^3) \\ &= ax^3 + bx^2y + cxy^2 + dy^3, \end{aligned} \tag{18}$$

where we have used the hypothesis that $N(M) = 1$. It follows, as in the proof of Theorem 2, that the ring R is determined by the pair $(\mathcal{A}, \mathcal{B})$.

To show that the constants c_{ij} are determined, we use the identity

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

which holds for any four vectors v_1, v_2, v_3, v_4 in the coordinate plane (a special case of the Plücker relations). Since this identity holds over any ring, we have in R the relations

$$\det(\alpha_i, \alpha_k) \cdot \det(\alpha_j, \alpha_\ell) = \det(\alpha_i, \alpha_j) \cdot \det(\alpha_k, \alpha_\ell) + \det(\alpha_i, \alpha_\ell) \cdot \det(\alpha_j, \alpha_k) \tag{19}$$

for $i, j, k, \ell \in \{1, 2, \ldots, 6\}$. Expanding out these relations using (17), and equating the coefficients of 1, ω, and θ, leads to 45 linear and quadratic equations in the c_{ij}'s, in terms of the a_{ij}'s and b_{ij}'s. This system turns out to have a unique solution, given by

$$c_{ij} = -\sum_{k,\ell,m,n} \tbinom{i\,j\,k\,\ell\,m\,n}{1\,2\,3\,4\,5\,6} \, \mathrm{Pfaff}(\mathcal{A}_{ijkl}) \cdot \mathrm{Pfaff}(\mathcal{B}_{ijmn}), \tag{20}$$

where we use $\binom{i\,j\,k\,\ell\,m\,n}{1\,2\,3\,4\,5\,6}$ to denote the sign of the permutation (i, j, k, ℓ, m, n) of $(1, 2, 3, 4, 5, 6)$. Thus the (integers) c_{ij} in (17) are also uniquely determined by $(\mathcal{A}, \mathcal{B})$.

We claim that the $\mathbb{Z}$-module M is now determined. Indeed, the values of all determinants $\det(\alpha_i, \alpha_j)$ are determined by (17). Moreover, these determinants satisfy the Plücker relations required of them as a result of (19). It follows that the values of $\alpha_1, \ldots, \alpha_6$ are uniquely determined as elements of

K^2 up to a constant factor in $\mathrm{SL}_2(K)$. An explicit embedding $M \hookrightarrow K \oplus K$ can easily be computed in terms of the constants c_{jk}, b_{jk}, and a_{jk} if desired.

It remains only to verify that M, determined only as a $\mathbb{Z}$-module above, is in fact a module over R. The R-module structure of M can be determined explicitly from (17), and is again too beautiful to be left unmentioned.

To state the result, we require some simple notation. Let $\mathcal{X}$ and $\mathcal{Y}$ denote any two 6×6 skew-symmetric matrices, and let $r_{ij,\mathcal{Y}}(\mathcal{X})$ denote the matrix obtained by replacing the i-th row and column of $\mathcal{X}$ by the j-th row and column of $\mathcal{Y}$, with the exception of the (i,i)-entry which is set equal to zero (to maintain skew-symmetry). For example,

$$r_{24,\mathcal{B}}(\mathcal{A}) = \begin{bmatrix} 0 & b_{14} & a_{13} & a_{14} & a_{15} & a_{16} \\ b_{41} & 0 & b_{43} & b_{44} & b_{45} & b_{46} \\ a_{31} & b_{34} & 0 & a_{34} & a_{35} & a_{36} \\ a_{41} & b_{44} & a_{43} & 0 & a_{45} & a_{46} \\ a_{51} & b_{54} & a_{53} & a_{54} & 0 & a_{56} \\ a_{61} & b_{64} & a_{63} & a_{64} & a_{65} & 0 \end{bmatrix}.$$

If we use $\mathrm{Pf}_{ij,Y}(\mathcal{X})$ to denote the Pfaffian of $r_{ij,\mathcal{Y}}(\mathcal{X})$, then the R-module structure of M is given as follows. We have for any $i \in \{1, 2, \ldots, 6\}$:

$$\begin{aligned} -\omega \cdot \alpha_i &= \sum_{j=1}^{6} \mathrm{Pf}_{ij,\mathcal{A}}(\mathcal{B})\, \alpha_j \\ -\theta \cdot \alpha_i &= \sum_{j=1}^{6} \mathrm{Pf}_{ij,\mathcal{B}}(\mathcal{A})\, \alpha_j\,. \end{aligned} \tag{21}$$

As all module coefficients are clearly integers, this completes the proof. □

Again, the proof gives very precise information about the bijection of Theorem 6. Given a pair (R, M) as in the theorem, the corresponding pair $(\mathcal{A}, \mathcal{B}) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ is obtained from equations (17). Conversely, given an element $(\mathcal{A}, \mathcal{B}) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$, the ring R is determined by (3) and (18); a basis for the rank 2 ideal M may be obtained from (17), and the R-module structure of M is given by (21).

The point stabilizers are given by the following corollary.

Corollary 7. *The stabilizer in* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_6(\mathbb{Z})$ *of a nondegenerate element* $(\mathcal{A}, \mathcal{B}) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ *is given by the semidirect product*

$$\mathrm{Aut}(R) \ltimes \mathrm{End}_R(M),$$

where (R, M) *is the pair corresponding to* $(\mathcal{A}, \mathcal{B})$ *as in Theorem* 6 *and* $\mathrm{End}_R(M)$ *denotes the subgroup of elements in* $\mathrm{SL}_2(R \otimes \mathbb{Q})$ *mapping* M *into* M.

If M is a projective R-module, then $\mathrm{End}(M)$ is simply $\mathrm{SL}_2(R)$, so that the stabilizer of $(\mathcal{A}, \mathcal{B})$ in this case is $\mathrm{Aut}(R) \ltimes \mathrm{SL}_2(R)$. It is again interesting to compare with the results of Sato-Kimura [9] and Wright-Yukie [12] over fields, who show that the connected component of the identity element of the stabilizer of a nondegenerate point in the representation of $\mathrm{GL}_2(K) \times \mathrm{SL}_6(K)$ on $K^2 \otimes \wedge^2 K^6$ (K a field) is $\mathrm{SL}_2(L)$, where L is an étale degree 3 extension of K. Corollary 7 may be proved in a manner similar to Corollary 3.

3. Resulting composition laws

In this section, we describe natural composition laws on $2 \times 3 \times 3$ boxes of integers, pairs of integral ternary quadratic forms, and pairs of senary alternating 2-forms. These composition laws may be viewed as cubic analogues of the composition laws presented in [2].

3.1. *Composition of* $2 \times 3 \times 3$ *integer matrices.* Define a pair of 3×3 matrices $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ to be *projective* if, in the corresponding pair $(R, (I, I'))$ (as in Section 2.3), the ideals I and I' are projective (i.e., invertible) as R-modules. Given a binary cubic form f, let $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$ denote the set of all elements $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3$ such that $\mathrm{Det}(Ax - By) = f(x, y)$. Then the group $G = \mathrm{SL}_3(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \subset \Gamma$ acts naturally on the set $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$.

Our work in Section 2 now shows that, for a given binary cubic form f, there is a natural group law on the set of G-orbits of projective elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$. This law of composition is most easily defined as follows. Let (A_1, B_1) and (A_2, B_2) be any two elements of $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)/G$, and let $(R(f), (I_1, I_1'))$ and $(R(f), (I_2, I_2'))$ be the corresponding pairs as constructed in Theorem 2. Define the composition of (A_1, B_1) and (A_2, B_2) to be the unique element $(A_3, B_3) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)/G$ corresponding to the pair $(R(f), (I_1 I_2, I_1' I_2'))$. It is then clear that this yields a group law on the desired set. We denote the resulting group by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f)$.

It is in fact simple to see what this group is. Since in the projective case the pair (I, I') is balanced if and only if I' is the inverse of I in the ideal class group, we may forget I' completely in the correspondence and we are left with simply with the class group $\mathrm{Cl}(R(f))$ of $R(f)$. Thus we may state

THEOREM 8. *There is a natural group isomorphism*

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f) \xrightarrow{\sim} \mathrm{Cl}(R(f)),$$

which sends an element $(A, B) \in \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$ *to the ideal class* I *in the cubic ring* $R = R(f)$, *where* $(R, (I, I'))$ *is the pair corresponding to* (A, B) *as in Theorem* 2.

The whole situation may thus be viewed as a cubic analogue of Gauss's theory of composition for binary quadratic forms and its relation to ideal classes of quadratic orders. Indeed, the analogy is quite strong:

- In the case of binary quadratic forms, the unique SL_2-invariant is the discriminant D, which classifies orders in quadratic fields. The primitive classes having a fixed value of D form a group under a certain natural composition law. This group is naturally isomophic to the narrow class group of the corresponding quadratic order.

- In the case of $2 \times 3 \times 3$ integer boxes, the unique $\mathrm{SL}_3 \times \mathrm{SL}_3$-invariant is the cubic form f, which classifies orders in cubic fields. The projective classes having a fixed value of f form a group under a certain natural composition law. This group is naturally isomorphic to the ideal class group of the corresponding cubic order.

If $f(x,y) = ax^3+bx^2y+cxy^2+dy^3$ is a given cubic form, then the identity element of $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f)$ (i.e., the *principal class*) is given by

$$(A,B) = \left(\begin{bmatrix} & & 1 \\ & -a & \\ 1 & & -c \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & b & \\ & & d \end{bmatrix} \right), \tag{22}$$

as was computed in the course of the proof of Theorem 2. One checks that indeed $\mathrm{Det}(Ax - By) = ax^3 + bx^2y + cxy^2 + dy^3$ for this pair (A,B).

3.2. *Composition of pairs of ternary quadratic forms.* Define a pair of ternary quadratic forms $(A,B) \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$ to be *projective* if in the corresponding triple (R,I,δ) (as in Section 2.4), the ideal I is projective as an R-module. Given a binary cubic form f, let $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3(f)$ denote the set of all elements $(A,B) \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3$ such that $\mathrm{Det}(Ax - By) = f(x,y)$; the group $\mathrm{SL}_3(\mathbb{Z})$ acts naturally on the set $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3(f)$.

As before there is a natural composition law on the set of projective elements of $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2(f)/\mathrm{SL}_3(\mathbb{Z})$ which turns this set of orbits into a finite abelian group. This composition law is most easily defined as follows. Let (A_1,B_1) and (A_2,B_2) be any two elements of $\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3(f)/\mathrm{SL}_3(\mathbb{Z})$, and let $(R(f),I_1,\delta_1)$ and $(R(f),I_2,\delta_2)$ be the corresponding triples as constructed in Theorem 4. The composition of (A_1,B_1) and (A_2,B_2) is then defined to be the unique element $(A_3,B_3) \in \mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3(f)/\mathrm{SL}_3(\mathbb{Z})$ corresponding to the triple $(R(f),I_1I_2,\delta_1\delta_2)$. It is clear that this does in fact yield a group law on the desired set. We denote the resulting groups by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f)$.

The natural inclusion

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^2 \to \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \tag{23}$$

corresponds, in terms of the bijections laid down in Theorems 2 and 4, to the

mapping

$$(R, I, \delta) \to (R, (I, I\delta^{-1})). \tag{24}$$

The latter mapping makes sense because if (R, I, δ) is a valid triple in the sense of Theorem 4, then $(I, I\delta^{-1})$ is a balanced pair of ideals of R and hence satisfies the conditions of Theorem 2.

As in the quadratic case, the restriction to symmetric classes isolates a certain arithmetic part of the class group of the corresponding order. In the current case, if $R(f)$ is the cubic ring corresponding to the cubic form f, then there is a natural map from $\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f)$ onto the subgroup $\mathrm{Cl}_2(R(f))$ of ideal classes of order dividing 2 in $\mathrm{Cl}(R(f))$. More precisely, we have

THEOREM 9. *There is a natural surjective group homorphism*

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f) \twoheadrightarrow \mathrm{Cl}_2(R),$$

which takes a pair (A, B) of ternary quadratic forms to the R-module I; here (R, I, δ) is a triple corresponding to (A, B) as in Theorem 4. The cardinality of the kernel of this homomorphism is $|U_R/\{U_R^2, \pm 1\}|$, where U_R denotes the group of units of R.

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

COROLLARY 10. *Suppose f corresponds to the ring of integers in a cubic field K. Then there is a natural surjective homomorphism*

$$\mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f) \twoheadrightarrow \mathrm{Cl}_2(K),$$

where $\mathrm{Cl}_2(K)$ denotes the exponent 2-part of the class group of the ring of integers in K. The cardinality of the kernel is equal to

$$\begin{cases} 2 & \text{if } K \otimes \mathbb{R} \cong \mathbb{R} \oplus \mathbb{C}; \quad \text{and} \\ 4 & \text{if } K \otimes \mathbb{R} \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}. \end{cases}$$

3.3. *Composition of pairs of senary alternating 2-forms.* Finally, let us return to the tensorial inclusion

$$\mathrm{id} \otimes \wedge_{3,3} : \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \to \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6 \tag{25}$$

described in Section 2.5. In light of Theorems 2 and 4, we find that this inclusion corresponds to the mapping

$$(R, (I, I')) \to (R, (I, I \oplus I')). \tag{26}$$

This makes sense because the direct sum of a balanced pair of ideals is a single balanced ideal of rank 2. That is, the fusion operator $\mathrm{id} \otimes \wedge_{3,3}$ literally fuses together two ideals I and I' of a cubic ring R into a single rank 2 ideal M.

As in Sections 3.1 and 3.2, let us define a pair of forms $(\mathcal{A},\mathcal{B}) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ to be *projective* if in the corresponding pair (R, M) (as in Section 2.5), the rank 2 ideal M is projective as an R-module. By a theorem of Serre [10], any projective rank 2 ideal class over a Noetherian, dimension one domain is a direct sum of rank 1 ideal classes. Therefore, in view of the description (26), we see that the map (25) must be *surjective at the level of projective equivalence classes*; i.e., any projective element of $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ is $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_6(\mathbb{Z})$-equivalent to an element in the image of (25).[5]

For a binary cubic form f, let $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6(f)$ denote the set of all elements $(\mathcal{A},\mathcal{B}) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ such that $\mathrm{Pfaff}(\mathcal{A}x - \mathcal{B}y) = f(x, y)$. As in all previous cases, one may expect that the group law on the set of projective elements in $\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3(f)$ induces a group law on the set of projective elements in $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6(f)$, via the map (25). This is indeed the case, and we denote the resulting group by $\mathrm{Cl}(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6; f)$. However, the second part of Serre's theorem [10] states that a projective module of rank k over a dimension 1 ring R is uniquely determined by its determinant. It follows that any projective pair (R, M) arising in Theorem 4 must actually take the form $(R, R \oplus R)$. Hence there is always exactly one projective element in $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$, up to $\mathrm{SL}_3(\mathbb{Z})$-equivalence, whose cubic form invariant is equal to f! Thus we may state:

THEOREM 11. *The group* $\mathrm{Cl}(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6; f)$ *is trivial for all cubic forms* f. *In particular, if* f *corresponds to the ring of integers in a cubic field*[6]*, then there is only one element* $(\mathcal{A},\mathcal{B}) \in \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$, *up to* $\mathrm{SL}_6(\mathbb{Z})$*-equivalence, whose binary cubic form invariant* $\mathrm{Det}(\mathcal{A}x - \mathcal{B}y)$ *is* $f(x, y)$. *This unique element is given by* $\mathrm{id} \otimes \wedge_{3,3}(A, B)$, *where* (A, B) *is as in* (22).

Therefore, the space $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$ is in a sense the cubic analogue of the quadratic composition space $\wedge^3\mathbb{Z}^6$ (see [2, Th. 7]).

In summary, we have natural inclusions

$$\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3 \to \mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3 \to \mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$$

leading to the group homomorphisms

$$\begin{array}{ccccc} \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathrm{Sym}^2\mathbb{Z}^3; f) & \to & \mathrm{Cl}(\mathbb{Z}^2 \otimes \mathbb{Z}^3 \otimes \mathbb{Z}^3; f) & \to & \mathrm{Cl}(\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6; f) \\ \downarrow & & \wr\| & & \wr\| \\ \mathrm{Cl}_2(R) & \hookrightarrow & \mathrm{Cl}(R) & \twoheadrightarrow & \{1\}. \end{array}$$

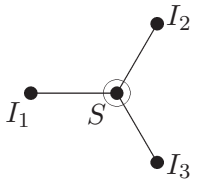
[5] We are unsure as to whether the latter statement is true without the assumption of projectivity.

[6] It is known that a proportion of $\frac{\zeta(4)}{\zeta(2)\zeta(3)} \approx 55\%$ of irreducible cubic forms f satisfy this condition ([3, Lemma 5].)

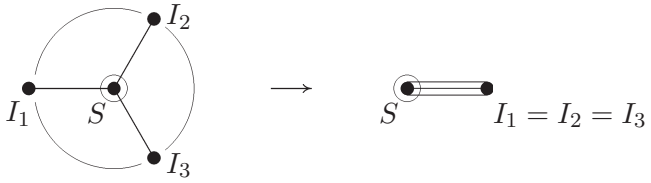
4. Cubic composition and exceptional groups

As in the case of quadratic composition [2], the theory of cubic composition is closely connected to certain exceptional Lie groups. Let G be any Lie group, and let $P = LU$ be a maximal parabolic with Levi factor L and unipotent radical U. Then the group L acts naturally by conjugation on the abelianized unipotent radical $W = U/[U,U]$. A complete classification of all representations (L, W) arising in this fashion was given by Rubenthaler in [8] (see also Vinberg [11]).

In [2], we showed how appropriate choices of G and P gave rise to the various representations W underlying our quadratic composition laws. To be more precise, we observed that if G is the exceptional Lie group D_4, with P the parabolic corresponding to the central vertex of D_4, then the resulting representation of L on W is essentially $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ acting on $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. Moreover, we proved that the orbits of this action correspond to pairs $(S, (I_1, I_2, I_3))$, where S is a quadratic ring, (I_1, I_2, I_3) forms a balanced triple of ideals of S, and the three factors of $\mathrm{SL}_2(\mathbb{Z})$ act on the bases of the ideals I_1, I_2, I_3 respectively. This led to a labelling of the Dynkin diagram of D_4 as follows:

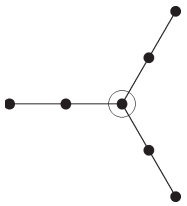


By applying symmetry and skew-symmetry ("fusion") processes, we obtained various other Dynkin diagrams and corresponding quadratic composition laws. For example, dividing by the full symmetry group S_3 led to the diagram



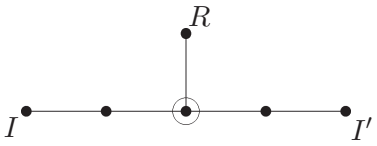
of G_2, where the condition "(I_1, I_2, I_3) balanced" turned into the condition "$I^3 \sim 1$ in the class group of S" (at least in the projective case), while the space $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ of $2 \times 2 \times 2$ integer cubes turned into the space $\mathrm{Sym}^3\mathbb{Z}^2$ of integral binary cubic forms after the symmetrization.

Thus quadratic composition was seen to stem essentially from the triply-symmetric Dynkin diagram of D_4. Judging from the quadratic case, to obtain a theory of cubic composition we then might want a Dynkin diagram of the form



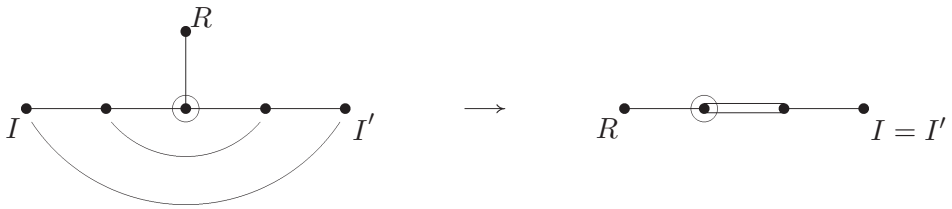
Unfortunately, a group with the above Dynkin diagram does not exist. If, however, we cut short one of the legs of this diagram, we do obtain a genuine Dynkin diagram, namely that of the group E_6. (This corresponds to the "slicing" we performed in the introduction.) Taking again the parabolic P of E_6 corresponding to the central vertex, we indeed find that the Levi factor is $L = \mathrm{GL}_2 \times \mathrm{GL}_3 \times \mathrm{GL}_3$, and the abelianized unipotent radical W is the space of $2 \times 3 \times 3$ boxes, the subject of Sections 2.3 and 3.1.

As shown in Section 2.3, the GL_2 factor of L acts on the basis of a cubic ring R, while the two SL_3 factors act on the bases of two ideals I and I' of R (where I and I' are balanced). This suggests that we should label the Dynkin diagram of E_6 as follows:



which is the cubic analogue of the diagram of D_4. The outer automorphism of E_6 of course acts by interchanging the pair of ideals (I, I') of R.

As with the quadratic case, we may impose a symmetry condition on the situtation, and identify the ideals I and I'; this corresponds to the identification



yielding the Dynkin diagram for F_4, where in the projective case the condition "(I, I') balanced" turns into the condition "$I^2 \sim 1$ in the class group of R" after the symmetrization. Thus the composition law on pairs of ternary quadratic forms, discussed in Sections 2.4 and 3.2, arises in this sense from the exceptional group F_4.

Finally, if instead of identifying them we fuse together the two ideals I and I', this corresponds at the level of Dynkin diagrams to joining the pairs

of vertices labelled I and I' with an additional added vertex (labelled "$\oplus$" in the diagram below). This yields

It is somewhat mysterious, however, where the row of five vertices labelled $I \oplus I'$ should be connected to the circled vertex. There are two choices, indicated in the picture above by dotted lines, each of which gives the Dynkin diagram of E_7. Either way, one finds that the representation of the Levi subgroup on the abelianized unipotent radical for the indicated choice of maximal parabolic does indeed yield the correct representation of $\mathrm{GL}_2 \times \mathrm{SL}_6$ on $\mathbb{Z}^2 \otimes \wedge^2\mathbb{Z}^6$. That is, the composition law on pairs of senary alternating 2-forms, as discussed in Sections 2.5 and 3.3, arises in this way from the group E_7, where the condition "the pair of rank 1 ideals (I, I') is balanced" for E_6 turns into the condition "the rank 2 ideal M is balanced" on E_7 following the skew-symmetrization.

In sum, we see that cubic composition essentially stems from the doubly-symmetric Dynkin diagram of E_6.

Acknowledgments. This article is based on Chapter 3 of the author's Ph.D. thesis [1] 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 kind correspondence and numerous 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] M. Bhargava, *Higher Composition Laws*, Ph.D. Thesis, Princeton University, June 2001.

[2] ———, Higher composition laws I: A new view on Gauss composition, and quadratic generalizations, *Ann. of Math.* **158** (2004), 217–250.

[3] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.

[4] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs **10**, A.M.S., Providence, RI, 1964.

[5] W.-T. Gan, B. H. Gross, and G. Savin, Fourier coefficients of modular forms on G_2, *Duke Math. J.* **115** (2002), no. 1, 105–169.

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

[7] D. Hilbert, *Theory Of Algebraic Invariants* (Engl. trans. by R. C. Laubenbacher), Cambridge Univ. Press, Cambridge, 1993.

[8] H. Rubenthaler, Espaces préhomogènes de type parabolique, in *Lectures on Harmonic Analysis on Lie Groups and Related Topics* (Strasbourg, 1979), 189–221, Lectures in Math. **14**, Kinokuniya Book Store, Tokyo, 1982.

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

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

[11] È. B. Vinberg, The classification of nilpotent elements of graded Lie algebras, *Soviet Math. Dokl.* **16** (1975), no. 6, 1517–1520.

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

(Received December 10, 2002)