Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 46 (2000)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ARITHMETIC OF BINARY CUBIC FORMS
Autor: HOFFMAN, J. William / MORALES, Jorge
DOI: https://doi.org/10.5169/seals-64795

L'Enseignement Mathématique, t. 46 (2000), p. 61–94

ARITHMETIC OF BINARY CUBIC FORMS

by J. William HOFFMAN and Jorge MORALES

ABSTRACT. This paper explores a connection between the theory of binary cubic forms and binary quadratic forms that was first discovered for forms over $\mathbf{Z}$ by Eisenstein. We generalize Eisenstein's theory to cubic forms over an arbitrary integral domain of characteristic not 2 or 3 using Kneser's Clifford algebra interpretation of the composition of quadratic forms.

1. INTRODUCTION

An important problem of number theory is the classification of binary n-forms

$$F(\mathbf{x}) = a_0x_1^n + a_1x_1^{n-1}x_2 + \cdots + a_{n-1}x_1x_2^{n-1} + a_nx_2^n\,,$$

where the coefficients a_i are integers, up to $\mathbf{SL}_2(\mathbf{Z})$-equivalence.

In *Disquisitiones Arithmeticæ* Gauss presented a systematic theory for $n = 2$, based in part on earlier researches of Fermat, Euler, Lagrange and Legendre. Recall that a composition of two binary quadratic forms q and q' is a quadratic form q'' such that there exists a bilinear map $B\colon \mathbf{Z}^2 \times \mathbf{Z}^2 \to \mathbf{Z}^2$ with the property $q''(B(\mathbf{x},\mathbf{y})) = q(\mathbf{x})q'(\mathbf{y})$. One of the most remarkable discoveries of Gauss is that the set of $\mathbf{SL}_2(\mathbf{Z})$-equivalence classes of binary primitive quadratic forms of given discriminant D is a finite abelian group with respect to composition of quadratic forms. This group was later interpreted by Dedekind in terms of ideal class groups.

F. G. Eisenstein in his first paper [6] showed a remarkable connection between the theory of binary cubic forms ($n = 3$) and the theory of binary quadratic forms ($n = 2$). This connection is as follows:

To every binary cubic form of the type

$$F(\mathbf{x}) = a_0x_1^3 + 3a_1x_1^2x_2 + 3a_2x_1x_2^2 + a_3x_2^3 \qquad (a_i \in \mathbf{Z}), \tag{1}$$

Eisenstein associates a quadratic form

$$q_F(\mathbf{x}) = Ax_1^2 + Bx_1x_2 + Cx_2^2, \tag{2}$$

where $A = a_1^2 - a_0a_2$, $B = a_1a_2 - a_0a_3$ and $C = a_2^2 - a_1a_3$. Eisenstein [7] calls q_F the *determining form* of F (*'determinierende Form'*). He shows that the correspondence $F \mapsto q_F$ commutes with the natural action of the group $\mathbf{SL}_2(\mathbf{Z})$ by linear substitution and therefore takes classes of cubic forms to classes of quadratic forms. Notice that q_F is essentially the Hessian of F.

It is natural to fix a nonzero integer $D \equiv 0$ or $1 \bmod 4$ and ask for all cubic forms F such that q_F has discriminant D, in other words, for all solutions of the quartic equation (hence the title of the paper [6])

$$\begin{aligned} D &= a_0^2a_3^2 - 3a_1^2a_2^2 + 4a_0a_2^3 + 4a_1^3a_3 - 6a_0a_1a_2a_3 \\ &= B^2 - 4AC \end{aligned} \tag{3}$$

in integers a_0, a_1, a_2, a_3. Note that the discriminant D of q_F is related to the discriminant $\delta(F)$ of F (as in [12, Chap. V, §9]) by

$$\delta(F) = -27D. \tag{4}$$

Eisenstein observes that from one solution of (3) one can obtain infinitely many solutions by taking its translations under the action of $\mathbf{SL}_2(\mathbf{Z})$. The orbits of this action are the essentially different solutions to (3).

He states without proof in [6] that if $D = 4d$ with d square-free, and $q(\mathbf{x})$ is a primitive quadratic form of discriminant D, then there exists a cubic form F as in (2) such that $q_F = q$ if and only if "the triplication of $q(\mathbf{x})$ gives the principal class", that is, if and only if $q(\mathbf{x})$ is an element of 3-torsion in the class group of binary quadratic forms of discriminant D. He also asserts that when $q(\mathbf{x})$ is an element of 3-torsion, there is only one class of cubic forms F with $q_F = q$. The latter assertion turned out not to be completely correct as stated when $D > 0$, for in this case there are in fact three nonequivalent cubic forms F with $q_F = q$ (see Example 7.2). This was noticed by Arndt [1], Pepin [13], Cayley [3] and Hermite [8].

In a second paper [7], Eisenstein proves his assertions for the case when $D = -4p$, where p a positive prime congruent to 3 mod 4. A key point in

Eisenstein's proofs of these results is a syzygy that he found connecting the fundamental covariants of a binary cubic form F. Let

$$G_F(\mathbf{x}) = \frac{1}{3}\begin{vmatrix} \partial F/\partial x_1 & \partial F/\partial x_2 \\ \partial q_F/\partial x_1 & \partial q_F/\partial x_2 \end{vmatrix}. \tag{5}$$

One has the polynomial identity (essentially in [7, §5]) relating F, q_F and G_F:

$$4q_F(\mathbf{x})^3 = G_F(\mathbf{x})^2 - DF(\mathbf{x})^2, \tag{6}$$

where D is the discriminant of q_F. It is worth noting that the graded ring of covariants of binary cubic forms (over a field of characteristic 0) is generated by F, q_F, D, G_F and that (6) generates the ideal of relations among these (cf. [15, 3.4.3]).

Let T_F and T_{G_F} be the symmetric trilinear forms such that

$$T_F(\mathbf{x},\mathbf{x},\mathbf{x}) = F(\mathbf{x}) \qquad \text{and} \qquad T_{G_F}(\mathbf{x},\mathbf{x},\mathbf{x}) = G_F(\mathbf{x})$$

(note that the middle coefficients of F and G_F are divisible by 3). One verifies the identity, equivalent to (6),

$$4q_F(\mathbf{x})q_F(\mathbf{y})q_F(\mathbf{z}) = T_{G_F}(\mathbf{x},\mathbf{y},\mathbf{z})^2 - DT_F(\mathbf{x},\mathbf{y},\mathbf{z})^2. \tag{7}$$

Suppose now that q_F is primitive (i.e., the GCD of its coefficients is 1). Assume also that $D = 4d$ for an integer $d \neq 0$. Since the form $X^2 - dY^2$ is the unit element in the group of primitive quadratic forms of discriminant D, the identity (7) shows that q_F is an element of 3-torsion for composition of quadratic forms. To see this it is enough to divide by 4 throughout in (7), observing that T_{G_F} will have integer coefficients, all divisible by 2 since D is a multiple of 4. A similar argument can be given when $D \equiv 1 \pmod 4$ (or see Proposition 5.9 for a general statement).

In this paper, we generalize Eisenstein's theory to cubic forms over any integral domain R of characteristic not 2 or 3. In order to extend Eisenstein's determining form (2) to the case of projective, not necessarily free, R-modules we need to allow quadratic forms with values in arbitrary projective R-modules of rank one. Thus Kneser's theory of binary quadratic mappings [11] provides the appropriate setting.

In Section 2 we explain Kneser's Clifford algebra description of the composition law for binary quadratic forms and mappings. We restate some of his results and give a natural interpretation in flat cohomology of his exact sequence relating the class groups of binary quadratic forms and binary quadratic mappings.

In Section 3 we generalize Eisenstein's notion of determining form to any integral domain R of characteristic not 2 or 3 and introduce the concept of a *cubic C-form* that plays a central role in the rest of the paper.

In Section 4 we use a natural Lie algebra representation to characterize the cubic C-forms (Theorem 4.5). This allows us to use the formalism of derivations.

In Section 5 we give necessary and sufficient conditions on a module M to admit cubic C-forms F with primitive determining mapping and we classify these forms (Theorem 5.1 and Theorem 5.2). These results are roughly the analogues of Eisenstein's theorems. We also discuss the relation between the notions of C-equivalence and ordinary (R-) equivalence and give an application to counting cubic forms over finite fields.

In the special case where R is a PID, we obtain a statement (Theorem 5.10) that closely parallels Eisenstein's theory. These results were known, modulo language, to Eisenstein [6] and [7], Arndt [1], Pepin [13], Cayley [3] and Hermite [8] in the case where $R = \mathbf{Z}$. The more specific classical results over $\mathbf{Z}$ concerning class numbers are deduced in Corollaries 5.11 and 5.12.

The main result for PID's (Theorem 5.10) can be summarized as follows: Let $q = ax_1^2+bx_1x_2+cx_2^2$ be a primitive quadratic form with $D = b^2-4ac \neq 0$. Let $C = C^+(q)$ be the even Clifford algebra of q and let $\tau \in C$ be such that $\tau^2 = D$. Then there exists a cubic form $F(\mathbf{x})$ in the shape of (1), with $a_i \in R$ such that $q_F = q$ (q_F as in (2)) if and only if the triplication of q in the sense of composition is trivial. Furthermore, when this condition is satisfied, the cubic forms in the fiber of the map $F \mapsto q_F$ above q can be written uniquely as $F' = aF + bG_F$, where F is a fixed form with $q_F = q$, the form G_F is the cubic covariant defined in (5), and the coefficients a and b are in the field of fractions of R and are such that $a + b\tau$ is a unit of C satisfying[1]) $a^2 - Db^2 = 1$. The $\mathbf{SL}_2(R)$-equivalence class of F' is determined uniquely by the class of $a + b\tau$ in $C^\times/C^{\times 3}$.

In Section 6, we show that the flat cohomology group $H^1_{\text{fl}}(\operatorname{Spec} C, \mu_3)$ acts simply transitively on the set of isomorphism classes of cubic C-forms with primitive determining mapping (Theorem 6.1). We also show that the main classification theorem of Section 5 can be interpreted in terms of a Kummer exact sequence in flat cohomology.

In Section 7 we show how to represent C-forms as scaled cubic trace forms and give applications to explicit computations over $\mathbf{Z}$.

---

[1]) In fact, defining $F' = aF + bG_F$ for arbitrary a and b, one has the identity $q_{F'} = (a^2 - Db^2)\, q_F$, which was apparently discovered by Hermite (see his letter to Cayley, [8])

A final remark: Gauss' theory of binary quadratic forms led to two major developments: the theory of number fields on the one hand, and the theory of quadratic forms in more than two variables on the other. The arithmetic of forms of higher degree over $\mathbf{Z}$ seems to have been largely neglected. In modern times Shintani revived interest in the arithmetic of cubic forms by introducing a family of Dirichlet series that depend on class numbers of cubic forms, and have good analytic properties (analytic continuation and functional equations). This work has been reinterpreted in the language of adèles by Wright [16]. For a general introduction to arithmetic problems concerning forms of higher degree, see [9].

We would like to thank J. Hurrelbrink and S. Weintraub for helpful discussions concerning this work.

CONTENTS

2. BINARY QUADRATIC MAPPINGS

We shall assume throughout this section that the ground ring R is an integral domain of characteristic not 2. The fraction field of R will be denoted by K.

A *binary quadratic form* is a pair (M, q) such that M is a projective R-module of rank two and $q: M \to R$ is a mapping such that $q(a\mathbf{x}) = a^2 q(\mathbf{x})$, $a \in R$, $\mathbf{x} \in M$, and such that $b(\mathbf{x}, \mathbf{y}) := q(\mathbf{x} + \mathbf{y}) - q(\mathbf{x}) - q(\mathbf{x})$ is R-bilinear. The form q is said to be *primitive* if the ideal generated by $q(M)$ is R. A morphism $(M, q) \to (M', q')$ is an R-linear mapping $f: M \to M'$ such that $q = q' \circ f$. If $M = R^2$ is the free module, we will often omit reference to M.

Let C be a quadratic R-algebra in the sense of [11], that is, an R-algebra, which as an R-module is projective of rank two, and such that $R1 \subset C$ is a direct factor of C as R-modules. Locally over $\operatorname{Spec} R$, such an algebra C is isomorphic with an algebra of the form

$$R[t]/(t^2 + bt + c), \qquad (b, c \in R).$$

Let $n\colon C \to R$ and $t\colon C \to R$ be the norm and the trace maps of C. It is easy to see that C possesses a unique nontrivial R-automorphism $x \mapsto \bar{x}$ satisfying $t(x) = x + \bar{x}$ and $n(x) = x\bar{x}$.

When $R = \mathbf{Z}$, for each nonzero integer $D \equiv 0$ or $1 \pmod 4$, we shall denote by C_D the unique quadratic $\mathbf{Z}$-algebra of discriminant D.

The notion of a *form of type* C was introduced by Kneser [11] and will play an important role in this paper.

DEFINITION 2.1. Let M be a projective C-module of rank 1. We say that a quadratic form $q\colon M \to R$ is *of type* C if it satisfies

$$q(c\mathbf{x}) = n(c)q(\mathbf{x}) \tag{8}$$

for all $\mathbf{x} \in M$, $c \in C$. A C-morphism $(M, q) \to (M', q')$ is a C-linear mapping $f\colon M \to M'$ such that $q = q' \circ f$.

Recall that the Clifford algebra $C(M, q)$ is the quotient of the tensor algebra $T_R(M)$ by the ideal generated by $\mathbf{x}\otimes\mathbf{x} - q(\mathbf{x})1$ for all $\mathbf{x} \in M$. The *even Clifford algebra*, $C^+(M, q)$, is the subalgebra generated by tensors of even degree, and is easily seen to be a quadratic R-algebra. Also, M is identified with the odd part of the Clifford algebra (i.e., generated by tensors of odd degree), and the map $C^+(M, q) \times M \to M$ induced by multiplication in $C(M, q)$ makes M into a $C^+(M, q)$-module. The formation of the Clifford algebra commutes with localization on $\operatorname{Spec} R$.

In the special case when $M = R^2$ we can describe $C^+(M, q)$ explicitly: Let $\{e_1, e_2\}$ be a basis of R^2 relative to which $q = ax_1^2 + bx_1x_2 + cx_2^2$. Then $e_1^2 = a$, $e_2^2 = c$, $e_1e_2 + e_2e_1 = b$ in the Clifford algebra of q. Thus if $\omega = -e_1e_2$ we have

$$C^+(q) = R[\omega] = R[x]/(x^2 + bx + ac).$$

PROPOSITION 2.2 ([11, Proposition 1]).

1. *Let (M,q) be a primitive quadratic form and $C = C^+(M,q)$ its even Clifford algebra. Then M becomes a projective C-module of rank one, and (M,q) is a quadratic form of type C.*

2. *Let C be a quadratic R-algebra and (M,q) be a nonzero quadratic form of type C. Then there exists a unique homomorphism of R-algebras*

$$\phi\colon C^+(M,q) \to C$$

satisfying $\phi(u)\mathbf{x} = u\mathbf{x}$ for $u \in C^+(M,q)$ and $\mathbf{x} \in M$. Furthermore, ϕ is an isomorphism if and only if q is primitive.

If q is a binary form over $\mathbf{Z}$ of discriminant D, then $C^+(M,q)$ is the unique quadratic algebra C_D over $\mathbf{Z}$ of discriminant D. If moreover q is primitive, then q is of type C_D. Thus all the primitive forms of discriminant D are of type C_D.

Kneser showed [11, Theorem 3] that the set $G(C)$ of primitive binary forms of type C modulo C-isomorphism forms a group for composition, which generalizes Gauss' theory for binary quadratic forms over $\mathbf{Z}$. The group law on $G(C)$ is explicitly given as follows: The composition of (M,q) and (M',q') is the form $(M \otimes_C M', q'')$, where $q''(\mathbf{x} \otimes \mathbf{y}) = q(\mathbf{x})q'(\mathbf{y})$. The neutral element is clearly (C,n).

The relation between C-isomorphism and R-isomorphism of quadratic forms is explained by the following proposition. Recall that an algebra over a field is *étale* if it is a product of separable extension fields of that field.

PROPOSITION 2.3. *Let C be a quadratic R-algebra, and suppose that $C \otimes K$ is an étale K-algebra. Let (M,q) and (M',q') be nonzero quadratic forms of type C. Then every R-isomorphism $f\colon (M,q) \to (M',q')$ is either C-linear or C-sesquilinear.*

Proof. By extending scalars to K, it will suffice to prove our proposition for the case when $R = K$. The map f will induce an isomorphism of the even Clifford algebras $C^+(M,q) \to C^+(M',q')$. These algebras are canonically isomorphic with C by Proposition 2.2, and hence f induces an automorphism f_* of the K-algebra C satisfying $f(c\mathbf{x}) = f_*(c)f(\mathbf{x})$. By hypothesis C is an étale algebra over K, so its only K-automorphisms are the identity and the canonical conjugation. Thus $f_*(c)$ is either c or $\bar{c}$ for all $c \in C$, which completes the proof. □

Note that the proposition is false if $C \otimes K$ is not étale, as can be easily seen by taking $C = R[t]/(t^2)$ with the norm form.

Let (M, q) be a nonzero binary quadratic form over R. Suppose that it is of type C, and let $C_1^\times$ be the subgroup of the units of C with $n(c) = 1$. Then we obtain a natural homomorphism (l_c = multiplication by c in M):

$$\begin{aligned} C_1^\times &\longrightarrow \mathbf{SO}(M, q) \\ c &\longmapsto l_c \end{aligned} \tag{9}$$

where $\mathbf{SO}(M, q) \subset \mathrm{Aut}_R(M)$ is the subgroup of R-automorphisms fixing q and having determinant 1.

COROLLARY 2.4. *With the above hypotheses, and assuming that $C \otimes K$ is an étale K-algebra, the map (9) is an isomorphism.*

Proof. Since M is projective of rank one over C, the map $c \to l_c$ is an isomorphism $C \simeq \mathrm{End}_C(M)$; thus it is enough to show that the elements of $\mathbf{SO}(M, q)$ are C-linear.

Let $f \in \mathbf{SO}(M, q)$. It is sufficient to show the C-linearity of f locally; so we may assume $M = C$ and $q = an$ with $a \in C^\times$.

The canonical conjugation σ of C preserves q and has determinant -1. Suppose now that f is C-sesquilinear. Then $f\sigma$ is C-linear, i.e. $f\sigma = l_c$ for some $c \in C^\times$ which must satisfy $n(c) = \det(l_c) = 1$, since l_c preserves q. Thus $\det(f) = -1$, contrary to our hypothesis. Hence, by Proposition 2.3, the map f must be C-linear. □

To define an analogue of Eisenstein's determining form (2) for general rings, we shall need the more general notion of binary quadratic mapping.

A *binary quadratic mapping* over R is a triple (M, q, N) where M is a projective R-module of rank two, N is a projective R-module of rank one and $q: M \to N$ is a map such that $q(a\mathbf{x}) = a^2 q(\mathbf{x})$ and $b(\mathbf{x}, \mathbf{y}) = q(\mathbf{x} + \mathbf{y}) - q(\mathbf{x}) - q(\mathbf{y})$ is R-bilinear.

A morphism $(M, q, N) \to (M', q', N')$ is a pair (f, g) of R-linear maps

$$f: M \to M' \qquad \text{and} \qquad g: N \to N'$$

such that $q'f = gq$. We say that (M, q, N) is *primitive* if $Rq(M) = N$. If N is free over R, then choosing a basis $\mathbf{n}$ of N we can write $q(\mathbf{x}) = Q(\mathbf{x})\mathbf{n}$. Then (M, Q) is a quadratic form in the previous sense. Note however that in this case (M, q, N) is isomorphic to (M', q', N') as quadratic mappings if and only if there exists a unit $u \in R^\times$ such that $(M, Q) \simeq (M', uQ')$ as quadratic forms.

Hence we can think of a quadratic mapping over R as defining a family of quadratic forms up to similarity equivalence, locally on a covering of $\operatorname{Spec} R$, and glued together in an obvious sense.

In the case $R = \mathbf{Z}$ every projective module is free, so that a quadratic mapping in this case is the same thing as a quadratic form, but up to similarity equivalence as above. This differs therefore from the usual theory, based on $\mathbf{SL}_2(\mathbf{Z})$-equivalence, but this difference is easily accounted for (see the discussion for PIDs in Section 5).

Let C be a quadratic algebra and assume that M is a projective C-module of rank 1. A quadratic mapping (M, q, N) is of *type* C if q satisfies the identity (8).

In order to have an analogue of Proposition 2.2 we need a definition of the even Clifford algebra in the context of quadratic mappings. The (total) Clifford algebra of a quadratic mapping (as opposed to a quadratic form) cannot be defined. The reason is that the Clifford algebra is not a functor for similarities of quadratic forms. As Kneser observed, the *even* Clifford algebra is a functor for similarities of quadratic forms. We can define directly the even Clifford algebra for quadratic mappings as follows:

DEFINITION 2.5. Let (M, q, N) be a quadratic mapping. The *even Clifford algebra* $C^+(M, q, N)$ is the quotient of the tensor algebra

$$T_R(N^* \otimes M \otimes M),$$

where $N^* = \operatorname{Hom}_R(N, R)$, by the ideal generated by

$$(10) \qquad \begin{cases} \lambda \otimes \mathbf{x} \otimes \mathbf{x} - \lambda(q(\mathbf{x})) \\ (\lambda \otimes \mathbf{x} \otimes \mathbf{y}) \otimes (\mu \otimes \mathbf{y} \otimes \mathbf{z}) - \lambda(q(\mathbf{y}))\ \mu \otimes \mathbf{x} \otimes \mathbf{z} \end{cases}$$

$(\lambda, \mu \in N^*,\ \mathbf{x}, \mathbf{y}, \mathbf{z} \in M)$.

One verifies easily that the above definition depends only on the isomorphism class of (M, q, N). For a similar construction, see [10, Ch. II, Section 8]. Note that the second defining relation can also be written as

$$(\lambda \otimes \mathbf{x} \otimes \mathbf{y}) \otimes (\mu \otimes \mathbf{y} \otimes \mathbf{z}) - \mu(q(\mathbf{y}))\ \lambda \otimes \mathbf{x} \otimes \mathbf{z}.$$

This is because $\lambda(u)\mu(v) = \lambda(v)\mu(u)$ on N since the difference is an alternating bilinear form, which must vanish since N has rank 1. We also need to define a $C^+(M, q, N)$-module structure on M; this is not completely obvious since the total Clifford algebra is no longer available. We begin with a lemma:

LEMMA 2.6. *Let Q be a quadratic form on M and let B be the associated bilinear form. Then*

$$B(\mathbf{x},\mathbf{y})\mathbf{z} - B(\mathbf{z},\mathbf{x})\mathbf{y} + B(\mathbf{y},\mathbf{z})\mathbf{x} \equiv 0 \pmod{2M}$$

for all $\mathbf{x},\mathbf{y},\mathbf{z} \in M$.

Proof. Let C be the Clifford algebra of Q. The expression

$$\sum_{\sigma} \operatorname{sign}(\sigma)\mathbf{x}_{\sigma 1}\mathbf{x}_{\sigma 2}\mathbf{x}_{\sigma 3}\,, \tag{11}$$

where σ runs over all permutations of $\{1,2,3\}$, defines an alternating R-trilinear map $M^3 \to C$. Since M has rank 2 over R, we have $\wedge^3 M = 0$; thus the expression (11) is identically zero. The lemma follows from the identity $\mathbf{x}_i\mathbf{x}_j + \mathbf{x}_j\mathbf{x}_i = B(\mathbf{x}_i,\mathbf{x}_j)$ in the Clifford algebra. □

We can now define a $C^+(M,q,N)$-module structure on M as follows:

$$(\lambda \otimes \mathbf{x} \otimes \mathbf{y}) \cdot \mathbf{z} = \tfrac{1}{2}[\lambda(b(\mathbf{x},\mathbf{y}))\mathbf{z} - \lambda(b(\mathbf{z},\mathbf{x}))\mathbf{y} + \lambda(b(\mathbf{y},\mathbf{z}))\mathbf{x}]\,. \tag{12}$$

Note that dividing by 2 in (12) makes sense in M by virtue of Lemma 2.6 applied to $Q = \lambda \circ q$, $B = \lambda \circ b$, and the fact that R is an integral domain of characteristic not 2. To see that this is a well-defined module we need:

LEMMA 2.7. *The definition* (12) *is compatible with the defining relations* (10) *for* $C^+(M,q,N)$.

Proof. This is straightforward for the first relation. For the second relation of (10), we can, without loss of generality, extend scalars from R to its fraction field K. We prove that the second relation vanishes when applied to an element $\mathbf{w} \in M$. If the vectors $\mathbf{z}$ and $\mathbf{y}$ are linearly dependent, say $\mathbf{z} = a\mathbf{y}$ for $a \in K$, then the second relation is a consequence of the first, so we may assume that $\mathbf{z}$ and $\mathbf{y}$ are linearly independent. In this case it is enough to consider the subcases (a) $\mathbf{w} = \mathbf{y}$, (b) $\mathbf{w} = \mathbf{z}$, since now $\mathbf{y}$, $\mathbf{z}$ forms a basis of M. The case (b) is easily seen by direct computation of both sides. In case (a), applying $(\lambda \otimes \mathbf{x} \otimes \mathbf{y}) \otimes (\mu \otimes \mathbf{y} \otimes \mathbf{z})$ to $\mathbf{y}$, we get

$$\tfrac{1}{4}\big(2\mu(b(\mathbf{y},\mathbf{z}))\,\lambda(b(\mathbf{y},\mathbf{y}))\,\mathbf{x} - \mu(b(\mathbf{y},\mathbf{y}))\,\lambda(b(\mathbf{x},\mathbf{y}))\,\mathbf{z} + \mu(b(\mathbf{y},\mathbf{y}))\,\lambda(b(\mathbf{z},\mathbf{x}))\,\mathbf{y} - \mu(b(\mathbf{y},\mathbf{y}))\,\lambda(b(\mathbf{y},\mathbf{z}))\,\mathbf{x}\big)\,.$$

In the last three terms in this formula, we may exchange λ and μ, using the identity $\lambda(u)\mu(v) = \lambda(v)\mu(u)$. The expression then reduces to

$$\tfrac{1}{2}\lambda(q(\mathbf{y}))\big(\mu(b(\mathbf{x},\mathbf{z}))\,\mathbf{y} - \mu(b(\mathbf{y},\mathbf{x}))\,\mathbf{z} + \mu(b(\mathbf{z},\mathbf{y}))\,\mathbf{x}\big)$$

which is exactly the proposed identity. □

It is important to note that in the case of a quadratic form, as opposed to a quadratic mapping, (12) really defines the usual module structure given by multiplication in the Clifford algebra of the form. Namely, the expression in (12) equals $\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z}$ in that algebra. We leave this verification to the reader (hint: use (11) and the fact that $\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z} = \mathbf{z} \otimes \mathbf{y} \otimes \mathbf{x}$ in the Clifford algebra of a binary quadratic form).

Locally on $\mathrm{Spec}(R)$, where both M and N are free, the choice of trivializations of these modules reduces a quadratic mapping to a quadratic form well-defined up to scalar multiples by a local unit. The even Clifford algebra as we have defined it is isomorphic on this open set to the Clifford algebra of this quadratic form, and the module structure as we have defined it coincides with the module structure given by multiplication in the Clifford algebra of the locally defined form. In fact, we can define the even Clifford algebra and the module structure by taking these locally defined objects and gluing them together, which provides an alternative construction.

Here is the analogue of Proposition 2.2 for quadratic mappings:

PROPOSITION 2.8.

1. *If* (M, q, N) *is primitive, then* M *is a projective* $C = C^+(M, q, N)$*-module of rank one and* q *is of type* C.

2. *Let* (M, q, N) *be a nonzero quadratic mapping of type* C, *and let* $C^+(M, q, N)$ *be its even Clifford algebra. Then there exists a unique homomorphism of* R*-algebras* $\phi\colon C^+(M, q, N) \to C$ *satisfying* $\phi(u)\mathbf{x} = u\mathbf{x}$ *for* $u \in C^+(M, q, N)$ *and* $\mathbf{x} \in M$. *Furthermore,* ϕ *is an isomorphism if and only if* q *is primitive.*

We shall omit the proof, since it is essentially rephrasing the proof given in [11, Proposition 1].

REMARK 2.9. Proposition 2.3 also holds for quadratic mappings. This can be easily seen by extending the scalars to K.

M. Kneser [11, Section 6] shows that the set $H(C)$ of isomorphism classes of primitive binary quadratic mappings (M, q, N) of type C forms a group for composition, the neutral element being (C, n, R). Note that the equivalence relation here is C-equivalence: an isomorphism is a pair (f, g) as before, but with f a C-linear isomorphism. He also showed that $H(C)$ is isomorphic to the group $\mathrm{Pic}(C)$ via the canonical map $(M, q, N) \mapsto M$.

We compare the group $G(C)$ of C-isomorphism classes of primitive quadratic forms of type C and the group $H(C)$ above by means of the canonical group homomorphism $G(C) \to H(C)$ induced by the correspondence $(M,q) \mapsto (M,q,R)$. M. Kneser (*op. cit.*) showed that this map fits into an exact sequence

$$0 \longrightarrow R^{\times}/n(C^{\times}) \longrightarrow G(C) \longrightarrow H(C) \xrightarrow{n} \operatorname{Pic}(R). \tag{13}$$

In the classical case of a quadratic $\mathbf{Z}$-algebra C of discriminant D, the sequence (13) was essentially known to Dedekind. Since $\operatorname{Pic}(\mathbf{Z}) = 0$ and $\mathbf{Z}^{\times} = \{\pm 1\}$, the sequence (13) shows that the group $G(C)$ is the narrow class group of C if $D > 0$, and it is $\{\pm 1\}\times$ the class group of C if $D < 0$ (the sign corresponding to positive and negative definite forms). In either case, it differs from the ideal class group $\operatorname{Pic}(C)$ at most by a cyclic factor of order 2.

It is worth noticing that the exact sequence above has a natural interpretation in flat cohomology. Let $\pi\colon \operatorname{Spec} C \to \operatorname{Spec} R$ be the natural morphism. Let $\mathcal{G} = \operatorname{Aut}_C(C,n)$ and $\mathcal{H} = \operatorname{Aut}_C(C,n,R)$ as group schemes over $\operatorname{Spec} R$. One sees immediately that $\mathcal{H} = \pi_*\mathbf{G}_m$, where $\mathbf{G}_m$ is the multiplicative group scheme, and that $\mathcal{G}$ is the kernel of the norm map $n\colon \pi_*\mathbf{G}_m \to \mathbf{G}_m$. From the short exact sequence of group schemes over $\operatorname{Spec} R$

$$0 \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow \mathbf{G}_m \longrightarrow 0,$$

we obtain the long exact sequence (see [14, Chap. III, §4])

$$0 \to R^{\times}/n(C^{\times}) \to H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathcal{G}) \to H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathcal{H}) \xrightarrow{n} H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathbf{G}_m),$$

where the flat topology is understood. The group $G(C)$ [respectively $H(C)$] can be identified with $H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathcal{G})$ [respectively $H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathcal{H})$] by interpreting quadratic forms [respectively quadratic mappings] as torsors for $\mathcal{G}$ [respectively $\mathcal{H}$] in the flat topology.

Note that there is a natural isomorphism

$$H^1_{\mathrm{fl}}(\operatorname{Spec} R, \pi_*\mathbf{G}_m) = H^1_{\mathrm{fl}}(\operatorname{Spec} C, \mathbf{G}_m),$$

so we also have $H(C) = \operatorname{Pic}(C)$ (compare [11, Proposition 2]).

3. CUBIC FORMS

We shall assume henceforth that the ground ring R is an integral domain of characteristic not dividing 6. The field of fractions of R will be denoted by K as previously.

Let M be a projective R-module of rank 2, and let $M^* = \mathrm{Hom}_R(M, R)$ be its dual. Consider the symmetric algebra

$$\mathrm{Sym}_R(M^*) = \bigoplus_n \mathrm{Sym}_R^n(M^*).$$

In this paper, a binary n-form is a pair (M, F), where M is a projective R-module of rank 2, and $F \in \mathrm{Sym}_R^n(M^*)$. A morphism $(M, F) \to (M', F')$ is an R-linear map $\phi: M \to M'$ such that $F'\phi = F$.

DEFINITION 3.1. An element $F \in \mathrm{Sym}_R^n(M^*)$ will be called a *Gaussian n-form* if there is a symmetric n-linear form $T: M \times \cdots \times M \to R$ with $F(\mathbf{x}) = T(\mathbf{x}, \ldots, \mathbf{x})$.

The set of Gaussian n-forms is a submodule of $\mathrm{Sym}_R(M^*)$ and will be denoted by $S^n(M^*)$. The module $\mathrm{Sym}^n(M^*)$ is projective of rank $n+1$ over R. If no binomial symbol $\binom{n}{i}$ is zero in R for $0 < i < n$, then $S^n(M^*)$ is also a projective R-module of rank $n+1$. If each of these binomial symbols is invertible in R then $S^n(M^*) = \mathrm{Sym}_R^n(M^*)$. Note that for any R-homomorphism $M \to M'$, the induced map $\mathrm{Sym}_R^n(M'^*) \to \mathrm{Sym}_R^n(M^*)$ sends $S^n(M'^*)$ to $S^n(M^*)$.

In this section we shall concentrate on binary cubic forms ($n = 3$). Unless otherwise stated all the binary cubic forms we shall consider are assumed to be Gaussian forms.

Let $F \in S^3(M^*)$ and let T be the symmetric trilinear form such that $F(\mathbf{x}) = T(\mathbf{x}, \mathbf{x}, \mathbf{x})$. For fixed $\mathbf{x} \in M$ we consider the homomorphism

$$T_{\mathbf{x}}: M \longrightarrow M^*$$
$$\mathbf{y} \longmapsto [\mathbf{z} \to T(\mathbf{x}, \mathbf{y}, \mathbf{z})].$$

Applying the second alternating power functor $\wedge^2$ we get a homomorphism

$$\wedge^2 T_{\mathbf{x}}: \wedge^2 M \to \wedge^2 M^*,$$

thus an element of $\mathcal{D}(M) := \mathrm{Hom}_R(\wedge^2 M, \wedge^2 M^*)$. We define

$$q_F(\mathbf{x}) := \wedge^2 T_{\mathbf{x}}. \tag{14}$$

It is immediate from the definitions that

$$(M, q_F, \mathcal{D}(M)) \tag{15}$$

is a binary quadratic mapping in the sense of Section 2. It is also evident that if (M, F) is isomorphic to (M', F'), then $(M, q_F, \mathcal{D}(M))$ is isomorphic to $(M', q_{F'}, \mathcal{D}(M'))$.

DEFINITION 3.2. The quadratic mapping $(M, q_F, \mathcal{D}(M))$ is called the *determining mapping* of (M, F).

By abuse of language, we shall refer sometimes to q_F as the determining mapping of F, without referring explicitly to the underlying modules M and $\mathcal{D}(M)$.

Over any open subset of $\operatorname{Spec} R$ where M is free, the choice of a local basis $\mathbf{m} = \{\mathbf{m}_1, \mathbf{m}_2\}$ of M allows us to write

$$F(\mathbf{x}) = a_0 x_1^3 + 3a_1 x_1^2 x_2 + 3a_2 x_1 x_2^2 + a_3 x_2^3, \tag{16}$$

where $\mathbf{x} = x_1\mathbf{m}_1 + x_2\mathbf{m}_2$. Let $\mathbf{m}^* = \{\mathbf{m}_1^*, \mathbf{m}_2^*\}$ be the dual basis of M^*. An easy computation gives

$$T_{\mathbf{x}}(\mathbf{m}_1) = (a_0 x_1 + a_1 x_2)\,\mathbf{m}_1^* + (a_1 x_1 + a_2 x_2)\,\mathbf{m}_2^*,$$

$$T_{\mathbf{x}}(\mathbf{m}_2) = (a_1 x_1 + a_2 x_2)\,\mathbf{m}_1^* + (a_2 x_1 + a_3 x_2)\,\mathbf{m}_2^*.$$

In the bases $\mathbf{m}_1 \wedge \mathbf{m}_2$ for $\wedge^2 M$ and $-\mathbf{m}_1^* \wedge \mathbf{m}_2^*$ for $\wedge^2 M^*$ (note the sign change), the determining form q_F is given by

$$\begin{aligned} q_F(\mathbf{x}) &= -\begin{vmatrix} a_0 x_1 + a_1 x_2 & a_1 x_1 + a_2 x_2 \\ a_1 x_1 + a_2 x_2 & a_2 x_1 + a_3 x_2 \end{vmatrix} \\ &= (a_1^2 - a_0 a_2) x_1^2 + (a_1 a_2 - a_0 a_3) x_1 x_2 + (a_2^2 - a_1 a_3) x_2^2, \end{aligned} \tag{17}$$

which shows that (15) coincides locally with Eisenstein's determining form (2).

Now let C be a quadratic R-algebra as in Section 2 and let M be a projective C-module of rank one.

DEFINITION 3.3. Let $F \in S^3(M^*)$ and let T be the symmetric trilinear form associated to F. We will say that F is a *C-form* if $T(c\mathbf{x}, \mathbf{y}, \mathbf{z})$ is symmetric in $\mathbf{x}, \mathbf{y}, \mathbf{z}$ for any $c \in C$.

REMARK 3.4. The above definition makes sense for forms in $S^n(M^*)$ for any n. In particular, one has the notion of a quadratic C-form. This should not be confused with the concept of a quadratic form *of type* C. Indeed, it is easy to see that a quadratic form q is of type C if and only if the symmetric bilinear form b attached attached to q satisfies $b(c\mathbf{x}, \mathbf{y}) = b(\mathbf{x}, \bar{c}\mathbf{y})$; whereas the condition for a C-form reads $b(c\mathbf{x}, \mathbf{y}) = b(\mathbf{x}, c\mathbf{y})$.

We will use throughout the notation

$$M_C^{\otimes 3} = M \otimes_C M \otimes_C M, \quad M_R^{\otimes 3} = M \otimes_R M \otimes_R M .$$

Note that there is a natural epimorphism of R-modules $p\colon M_R^{\otimes 3} \to M_C^{\otimes 3}$. We have the following characterization of C-forms:

LEMMA 3.5. *Let $F \in S^3(M^*)$ and let T be the associated symmetric R-trilinear form, viewed as a linear form on $M_R^{\otimes 3}$. Then F is a C-form if and only if there exists a linear map $\lambda\colon M_C^{\otimes 3} \to R$ such that $T = \lambda \circ p$. Furthermore, the map λ is unique.*

Proof. It is enough to prove the lemma locally, so we assume that M is free over C.

Let $\lambda\colon M_C^{\otimes 3} \to R$ be an R-homomorphism. Write $M = C\mathbf{m}$ for some $\mathbf{m} \in M$ and let $\mathbf{x} = c_1\mathbf{m}$, $\mathbf{y} = c_2\mathbf{m}$, $\mathbf{z} = c_3\mathbf{m}$ with $c_i \in C$.

Then $T(\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z}) = \lambda(c_1c_2c_3(\mathbf{m} \otimes \mathbf{m} \otimes \mathbf{m}))$ is visibly symmetric and satisfies the condition of Definition 3.3.

Conversely, if $T(c\mathbf{x}, \mathbf{y}, \mathbf{z})$ is symmetric then in particular T itself is symmetric ($c = 1$), and hence

$$T(c\,\mathbf{x}, \mathbf{y}, \mathbf{z}) = T(\mathbf{x}, c\mathbf{y}, \mathbf{z}) = T(\mathbf{x}, \mathbf{y}, c\,\mathbf{z}),$$

showing the existence of λ. Uniqueness follows from the fact that p is onto. □

Let $S_C^3(M^*) \subset S^3(M^*)$ be the submodule of cubic C-forms on M. Note that the lemma above can be summarized by saying that the map

$$\begin{aligned} \mathrm{Hom}_R(M_C^{\otimes 3}, R) &\longrightarrow S_C^3(M^*) \\ \lambda &\longmapsto [\mathbf{x} \mapsto \lambda(\mathbf{x} \otimes \mathbf{x} \otimes \mathbf{x})] \end{aligned} \tag{18}$$

is an isomorphism of R-modules.

On the other hand, we also have

LEMMA 3.6. *Let L be any projective C-module of finite rank. Then the map*

$$\begin{aligned} \mathrm{Hom}_C(L, C^*) &\longrightarrow \mathrm{Hom}_R(L, R) \\ f &\longmapsto (\mathbf{x} \mapsto f(\mathbf{x})(1)) \end{aligned} \tag{19}$$

is an isomorphism of C-modules (the dual $P^* = \mathrm{Hom}_R(P, R)$ is made into a C-module by setting $(c\lambda)(x) = \lambda(cx)$ for $\lambda \in P^*$).

Proof. By localization, it is sufficient to prove the lemma when $L = C$, in which case the map is the identity. □

Combining the isomorphisms (18) and (19) with $L = M_C^{\otimes 3}$, we obtain

PROPOSITION 3.7. *The map*

$$\begin{aligned} \mathrm{Hom}_C(M_C^{\otimes 3}, C^*) &\longrightarrow S_C^3(M^*) \\ \phi &\longmapsto [F_\phi : \mathbf{x} \mapsto \phi(\mathbf{x} \otimes \mathbf{x} \otimes \mathbf{x})(1)] \end{aligned} \tag{20}$$

is an isomorphism of R-modules.

Using the isomorphism (20) we give $S_C^3(M^*)$ the C-module structure so that this bijection becomes a C-module isomorphism. Note that

$$T_\phi(\mathbf{x}, \mathbf{y}, \mathbf{z}) := \phi(\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z})(1)$$

is the symmetric trilinear form attached to F_ϕ. Hence the C-module structure on $S_C^3(M^*)$ is given explicitly by

$$(cF)(\mathbf{x}) = T(c\mathbf{x}, \mathbf{x}, \mathbf{x}). \tag{21}$$

LEMMA 3.8. *C^* is an invertible C-module.*

Proof. Locally over $\mathrm{Spec}\, R$, we have $C = R[\omega] = R[x]/(x^2+bx+c)$. Then the R-module C^* is freely generated by λ_1, λ_2, where $\lambda_1(1) = 1$, $\lambda_1(\omega) = 0$, $\lambda_2(1) = 0$, $\lambda_2(\omega) = 1$. One sees that $\omega\lambda_2 = \lambda_1 - b\lambda_2$, so that λ_2 is a local C-module basis of C^*. □

By virtue of (20) and this lemma, $S_C^3(M^*)$ is an invertible C-module.

In the next section we will give alternate characterizations of the cubic C-forms on M, related to their determining mapping.

4. A LIE ALGEBRA REPRESENTATION

Let M be a projective R-module of rank two. Let $G = \mathrm{Aut}_R(M)$ and let $\mathfrak{g} = \mathrm{End}_R(M)$ viewed as a Lie algebra over R.

The group G acts on the right on $\mathrm{Sym}_R(M^*)$ by algebra automorphisms via

$$(F\sigma)(\mathbf{x}) = F(\sigma\mathbf{x})$$

for $F \in \mathrm{Sym}_R(M^*)$ and $\sigma \in G$. Taking the formal derivative at the origin of the associated map

$$G \to \mathrm{Aut}_{R-\mathrm{alg}}(\mathrm{Sym}_R(M^*))$$

we get a representation of Lie algebras

$$\rho\colon \mathfrak{g} \longrightarrow \mathrm{Der}_R(\mathrm{Sym}_R(M^*))\,. \tag{22}$$

The action of G preserves the homogeneous components $\mathrm{Sym}_R^n(M^*)$ and also the submodule $S^n(M^*)$ of Gaussian forms. The same is true for the Lie algebra action of $\mathfrak{g}$.

We shall compute the action of $\mathfrak{g}$ on $S^n(M^*)$ explicitly:

LEMMA 4.1. *Let $F \in S^n(M^*)$ and let T be the associated n-linear form. Then*

$$\rho(g)(F)(\mathbf{x}) = nT(g\mathbf{x}, \mathbf{x}, \ldots, \mathbf{x})$$

for all $g \in \mathfrak{g}$.

Proof. To compute the derivative of $G \to \mathrm{Aut}_R(S^n(M^*))$, we extend the scalars to the "dual numbers" $R[\epsilon]/(\epsilon^2)$. Using the symmetry of T we have

$$F((1 + g\epsilon)\mathbf{x}) = F(\mathbf{x}) + nT(g\mathbf{x}, \mathbf{x}, \ldots, \mathbf{x})\,\epsilon\,,$$

which proves our assertion. □

Let C/R be a quadratic algebra in the sense of Section 2 and let M be an invertible C-module. Then we have a natural map $C \to \mathrm{End}_R(M)$ and we can restrict the representation ρ to C. Note that when R is a field and C is an étale quadratic algebra then the image of C is a Cartan subalgebra $\mathfrak{h}_C$ of $\mathfrak{g}$.

Comparing (22) with equation (21), we see that the C-module structure on $S_C^3(M^*)$ is related to the Lie algebra action by

$$cF = \tfrac{1}{3}\rho(c)F\,. \tag{23}$$

We will make this explicit in a special case that we need:

LEMMA 4.2. *Let $F \in S^3(M^*)$ be a binary cubic form over a field K of characteristic not 2 or 3. Let q_F be its determining form, and $C = C^+(q_F)$ its even Clifford algebra. Let x_1, x_2 be coordinates on the vector space M with respect to a basis $\mathbf{m}_1, \mathbf{m}_2$. Let*

$$\tau = \mathbf{m}_1\mathbf{m}_2 - \mathbf{m}_2\mathbf{m}_1 \in C = C^+(q_F).$$

Note that $\tau^2 = D$ is the discriminant of q_F. Then

$$\rho(\tau) = \frac{\partial q_F}{\partial x_2}\frac{\partial}{\partial x_1} - \frac{\partial q_F}{\partial x_1}\frac{\partial}{\partial x_2},$$

acting on forms of any degree.

Proof. As we have seen,

$$q_F(x_1\mathbf{m}_1 + x_2\mathbf{m}_2) = Px_1^2 + Qx_1x_2 + Rx_2^2,$$

where $P = a_1^2 - a_0a_2$, $Q = a_1a_2 - a_0a_3$, and $R = a_2^2 - a_1a_3$. By direct computation in the Clifford algebra C, we see that

$$\tau\mathbf{m}_1 = Q\mathbf{m}_1 - 2P\mathbf{m}_2$$

$$\tau\mathbf{m}_2 = 2R\mathbf{m}_1 - Q\mathbf{m}_2.$$

Since $\rho(c)$ is a derivation of $\mathrm{Sym}_R(M^*)$, we have

$$\rho(c) = \rho(c)(x_1)\frac{\partial}{\partial x_1} + \rho(c)(x_2)\frac{\partial}{\partial x_2}.$$

Thus $\tau(x_1\mathbf{m}_1 + x_2\mathbf{m}_2) = (Qx_1 + 2Rx_2)\mathbf{m}_1 - (2Px_1 + Qx_2)\mathbf{m}_2$, which gives $\rho(\tau)(x_1) = \partial q_F/\partial x_2$ and $\rho(\tau)(x_2) = -\partial q_F/\partial x_1$. □

COROLLARY 4.3. $\rho(\tau)q_F = 0$ *and*

$$\rho(\tau)F = \begin{vmatrix} \partial F/\partial x_1 & \partial F/\partial x_2 \\ \partial q_F/\partial x_1 & \partial q_F/\partial x_2 \end{vmatrix} \tag{24}$$

$$= 3G_F,$$

where G_F is as in (5).

REMARK 4.4. If we further assume that C is an étale algebra, then as we have remarked, ρ maps C onto a Cartan subalgebra of $\mathrm{End}_K(M) \sim \mathfrak{gl}(2, K)$. This algebra decomposes as

$$\mathfrak{h}_C = \mathfrak{z} \oplus \mathfrak{h}'_C$$

where the first factor is the center, consisting of scalar matrices, and the second factor is the intersection $\mathfrak{h}_C \cap \mathfrak{sl}(2, K)$, consisting of matrices of trace 0. As the formulas in the proof of the preceding lemma show that τ acts on M with trace 0, we see that $\mathfrak{h}'_C = K\tau$.

THEOREM 4.5. *Let C/R be a quadratic algebra such that $C \otimes K$ is étale over K. Let M be a projective rank-one C-module and let $F \in S^3(M^*)$ be such that the determining mapping q_F is not 0. Then the following conditions are equivalent:*

(a) *F is a C-form*

(b) *$(M, q_F, \mathcal{D}(M))$ is of type C*

(c) *$\rho(c)\rho(\overline{c})F = 9n(c)F$ for all $c \in C$.*

Proof. (a)$\Rightarrow$(b). If T is the trilinear form attached to F, then, using the symmetry of $T(c\mathbf{x}, \mathbf{y}, \mathbf{z})$, we have

$$\begin{aligned} q_F(c\mathbf{x}) &= \wedge^2 T(c\mathbf{x}, -, -) \\ &= \wedge^2 (T(\mathbf{x}, c-, -)) \\ &= n(c) \wedge^2 (T(\mathbf{x}, -, -)) \\ &= n(c) q_F(\mathbf{x}) , \end{aligned}$$

which proves the claim. In fact, this implication does not depend on $C \otimes K$ being étale.

It is enough to prove the theorem for the case where $R = K$ is a separably closed field. We can assume in this case $C = K[\sigma]$ with σ satisfying $\sigma^2 = 1$. We will make these assumptions for the rest of the proof.

(b)$\Rightarrow$(c). Let $\{\mathbf{m}_1, \mathbf{m}_2\}$ be a basis of M over K with $\sigma\mathbf{m}_1 = \mathbf{m}_1$ and $\sigma\mathbf{m}_2 = -\mathbf{m}_2$. With respect to this basis, the form q_F, being of type C, must have the shape

$$q_F(\mathbf{x}) = \alpha x_1 x_2 ,$$

where $\alpha \neq 0$. To see that this is so, note that because q_F is of type C, we have $q_F(\sigma\mathbf{m}_1) = n(\sigma)q_F(\mathbf{m}_1) = -q_F(\mathbf{m}_1)$, which shows that $q_F(\mathbf{m}_1) = 0$. One sees similarly that $q_F(\mathbf{m}_2) = 0$. Then the coefficients of $F(\mathbf{x}) = a_0x_1^3 + 3a_1x_1^2x_2 + 3a_2x_1x_2^2 + a_3x_2^3$ satisfy the relations: $a_1^2 - a_0a_2 = 0$, $a_1a_2 - a_0a_3 = \alpha$ and $a_2^2 - a_1a_3 = 0$. Since $\alpha \neq 0$, it follows at once that $a_1 = a_2 = 0$, so F is of the form $F(\mathbf{x}) = \lambda x_1^3 + \mu x_2^3$. Since $q_F \neq 0$ (in fact nondegenerate under the étaleness hypothesis), the algebra C can be identified with the even Clifford algebra $C^+(M, q_F, \mathcal{D}(M))$ by Proposition 2.8. Under that identification we have $\tau = \alpha\sigma$, where τ is defined as in Lemma 4.2. From that lemma we get $\rho(\sigma) = x_1\partial/\partial x_1 - x_2\partial/\partial x_2$, which can be seen directly, since both sides agree on x_1, x_2. Hence $\rho(\sigma)(x_1^{3-i}x_2^i) = (3 - 2i)x_1^{3-i}x_2^i$. In particular, for $F(\mathbf{x}) = \lambda x_1^3 + \mu x_2^3$ we have

$$\rho(\sigma)\rho(\overline{\sigma})F = -\rho(\sigma)^2F = -9F = 9n(\sigma)F .$$

The more general identity $\rho(c)\rho(\bar{c})F = 9n(c)F$ for $c \in C$ follows from this particular case by noting that, from Lemma 4.1, $\rho(1)F = 3F$.

(c)$\Rightarrow$(a). Suppose that $\rho(\sigma)^2F = 9F$. Then F must have the form $F = \lambda x_1^3 + \mu x_2^3$. This is because, as we saw in the discussion above, the monomials $x_1^{3-i}x_2^i$ are eigenvectors for the operator $\rho(\sigma)^2$ with eigenvalue $(3-2i)^2$, which equals 9 only for $i = 0$ and $i = 3$. Hence the associated trilinear form is $T(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \lambda x_1 y_1 z_1 + \mu x_2 y_2 z_2$. Thus $T(\sigma\mathbf{x}, \mathbf{y}, \mathbf{z}) = \lambda x_1 y_1 z_1 - \mu x_2 y_2 z_2$, which is visibly symmetric in $\mathbf{x}, \mathbf{y}, \mathbf{z}$. □

REMARK 4.6. It is interesting to notice that the syzygy (6) can be recovered from Part (c) of Theorem 4.5. Assume for simplicity that $R = K$ is a field and C is an étale K-algebra. Let $\{\mathbf{m}_1, \mathbf{m}_2\}$ be a basis of M. Let $\tau = \mathbf{m}_1\mathbf{m}_2 - \mathbf{m}_2\mathbf{m}_1 \in C = C^+(q_F)$ as in Lemma 4.2. As we noted in Remark 4.4, τ generates the trace 0 part of the Cartan subalgebra defined by C. Using the derivation property and Corollary 4.3, we see $\rho(\tau)(G_F^2 - DF^2) = (2/3)(\rho(\tau)^2F - 9DF)G_F$. From the above theorem, $\rho(\tau)^2F = 9DF$, so this is 0. On the other hand, $\rho(\tau)q_F = 0$, also by Corollary 4.3, which implies that $\rho(\tau)q_F^3 = 0$. Hence both q_F^3 and $G_F^2 - DF^2$ lie in the subspace on weight 0 (for the action of the Cartan subalgebra $\mathfrak{h}'_C \subset \mathfrak{sl}(2, K)$) of $S^6(M^*)$. As $S^6(M^*)$ is an irreducible representation of $\mathfrak{sl}(2, K)$, this is one-dimensional. Hence q_F^3 and $G_F^2 - D_FF^2$ differ by a constant multiple. A priori, this constant could depend on F (e.g., D). That this is not so can be seen by noting that both sides are of the same degree in the coefficients of F.

COROLLARY 4.7. *Let M be a projective R-module of rank 2, and let $F \in S^3(M^*)$.*

(i) *Let $C = C^+(M, q_F, \mathcal{D}(M))$ and suppose that $C \otimes K$ is étale, and that q_F is primitive. Then F is a C-form.*

(ii) *If F is a C-form for a quadratic R-algebra C and $(M, q_F, \mathcal{D}(M))$ is primitive, then $C \cong C^+(M, q_F, \mathcal{D}(M))$.*

Proof. (i) By Proposition 2.8, $(M, q_F, \mathcal{D}(M))$ is of type C. We conclude by Theorem 4.5.

(ii) If F is a C-form, then by Theorem 4.5, the quadratic mapping $(M, q_F, \mathcal{D}(M))$ is type C. But assuming furthermore that $(M, q_F, \mathcal{D}(M))$ is primitive, we see that C is isomorphic with $C^+(M, q_F, \mathcal{D}(M))$ by Proposition 2.8. □

LEMMA 4.8. *Suppose that $C \otimes K$ is étale over K and let (M, F) and (M', F') be cubic C-forms. Assume that the determining mappings $q_F, q_{F'}$ are nonzero. Then every R-linear isomorphism $f\colon (M, F) \to (M', F')$ is either C-linear or C-sesquilinear.*

Proof. The map f will induce an isomorphism of determining quadratic mappings of type C. We conclude by Proposition 2.3. □

5. STRUCTURE OF THE CUBIC C-FORMS

We shall describe below the C-module structure of $S^3_C(M^*)$ and the corresponding C-isomorphism classes.

THEOREM 5.1. *Let M be a rank-one projective C-module. For each $\phi \in \mathrm{Hom}_C(M_C^{\otimes 3}, C^*)$ we define a cubic form by $F_\phi(\mathbf{x}) = \phi(\mathbf{x} \otimes \mathbf{x} \otimes \mathbf{x})(1)$. Then*

(i) *The correspondence $\phi \mapsto F_\phi$ is an isomorphism of C-modules $\mathrm{Hom}_C(M_C^{\otimes 3}, C^*) \to S^3_C(M^*)$.*

(ii) *The determining mapping q_{F_ϕ} is primitive if and only if ϕ is an isomorphism.*

(iii) *Two cubic C-forms F and F_1 on M are equivalent over C if and only if there exists $c \in C^\times$ such that $F_1 = c^3 F$.*

Proof. (i) This is a restatement of Proposition 3.7. The map $\phi \mapsto F_\phi$ is a C-isomorphism by definition of the structure of C-module on $S^3_C(M^*)$ in Section 3.

(ii) It is enough to prove our assertion locally, so we assume that M is free over C. Write $M = C\mathbf{m}$ for some $\mathbf{m} \in M$. Let $\lambda = \phi(\mathbf{m} \otimes \mathbf{m} \otimes \mathbf{m})$. Then we have $\phi(x\mathbf{m} \otimes y\mathbf{m} \otimes z\mathbf{m}) = \lambda(xyz)$. Let $\beta(y\mathbf{m}, z\mathbf{m}) = \lambda(yz)$ and observe that λ is a basis of C^* over C if and only if the symmetric bilinear form β is unimodular. We have

$$\begin{aligned} q_{F_\phi}(x\mathbf{m}) &= n(x) q_{F_\phi}(\mathbf{m}) \\ &= n(x) \wedge^2 \beta . \end{aligned}$$

It follows from this equality that q_{F_ϕ} is primitive if and only if β is unimodular, that is, if and only if ϕ is an isomorphism.

(iii) Let F and F_1 be cubic C-forms on M. Suppose that they are C-isomorphic. Then there exists $c \in C^\times$ such that $F_1 = F \circ l_c$. Let T be the symmetric trilinear form associated to F. Since $T(c\mathbf{x}, c\mathbf{y}, c\mathbf{z}) = T(c^3\mathbf{x}, \mathbf{y}, \mathbf{z})$, we get $F_1 = c^3F$. Conversely, if $F_1 = c^3F$ we may reverse these steps to conclude that $F_1 = F \circ l_c$ □

We shall henceforth denote by $\mathrm{Cubic}_C(M)$ the set of C-isomorphism classes of cubic C-forms on M with primitive determining mapping. Recall that when M is an invertible C-module, there is a *unique* primitive quadratic mapping (M, q, N) of type C on M ([11]). If $F \in \mathrm{Cubic}_C(M)$, then necessarily

$$(M, q_F, \mathcal{D}(M)) = (M, q, N) \text{ in } H(C), \quad \text{and} \quad C = C^+(M, q_F, \mathcal{D}(M)),$$

by Corollary 4.7 (ii); in particular, all members of $\mathrm{Cubic}_C(M)$ have isomorphic determining mappings.

THEOREM 5.2. *Let M be a projective C-module of rank one.*

(i) *The set* $\mathrm{Cubic}_C(M)$ *is nonempty if and only if* $3[M] = [C^*]$ *in* $\mathrm{Pic}(C)$.

(ii) *If* $3[M] = [C^*]$ *in* $\mathrm{Pic}(C)$, *then the group* $C^\times/C^{\times 3}$ *acts simply transitively on the set* $\mathrm{Cubic}_C(M)$.

Proof. (i) By Part (ii) of Theorem 5.1, the module M admits a cubic C-form with primitive determining mapping if and only if there is an isomorphism $M_C^3 \to C^*$.

(ii) Since $M_C^{\otimes 3}$ and C^* are invertible C-modules, $\mathrm{Isom}_C(M_C^{\otimes 3}, C^*)$ is either empty or it is a torsor for $C^\times$ (i.e., a simply transitive $C^\times$-set). It is nonempty if and only if $\mathrm{Cubic}_C(M)$ is nonempty, by Part (i). Suppose this is so, and choose an isomorphism $\phi\colon M_C^3 \to C^*$. Each cubic C-form on M with primitive determining mapping is uniquely of the shape $F_{c\phi}$ with $c \in C^\times$ by Parts (i) and (ii) of Theorem 5.1. By Part (iii) of Theorem 5.1, the form $F_{c\phi}$ will be isomorphic with F_ϕ if and only if $c \in (C^\times)^3$. □

We discuss next the relation between R-isomorphism and C-homomorphism of cubic forms.

Let $\mathrm{Cubic}_R(M)$ be the set of R-isomorphism classes of binary Gaussian cubic forms on M with primitive determining mapping of type C. Set

$$\mathcal{S}_R(C) = \coprod_{[M]} \mathrm{Cubic}_R(M) \quad \text{and} \quad \mathcal{S}(C) = \coprod_{[M]} \mathrm{Cubic}_C(M),$$

where $[M]$ runs over the elements of $\mathrm{Pic}(C)$ satisfying $3[M] = [C^*]$ and $\coprod$ means disjoint union.

The set $\mathcal{S}(C)$ carries a natural involution given by

$$[M,F] \mapsto \overline{[M,F]} := [\overline{M},F],$$

where $\overline{M}$ is defined as follows: $\overline{M} = M$ as R-modules with C acting by $c \cdot \mathbf{x} = \overline{c}\mathbf{x}$, where $c \mapsto \overline{c}$ is the canonical involution of C. This is well-defined because q_F depends only on the R-module structure of M, and it will be of type C for M if and only if it is so for $\overline{M}$ since $n(c) = n(\overline{c})$. Note that $[M,F] = \overline{[M,F]}$ if and only if (M,F) possesses a C-sesquilinear automorphism.

PROPOSITION 5.3. *With the previous notation we have*

(i) $\mathcal{S}_R(C) = \mathcal{S}(C)/\sim$, *where* $\sim$ *identifies* $[M,F]$ *with* $\overline{[M,F]}$.

(ii) *If* $[M] = [\overline{M}]$ *and* $3[M] = [C^*]$, *then* $\mathrm{Cubic}_C(M)$ *has an element* $[M,F_0]$ *fixed under the involution.*

(iii) *If* $[M] \neq [\overline{M}]$ *and* $3[M] = [C^*]$ *in* $\mathrm{Pic}(C)$, *then* $\mathrm{Cubic}_C(M) = \mathrm{Cubic}_R(M)$. *In particular,* $\mathrm{Cubic}_R(M)$ *is a simply transitive* $(C^\times/C^{\times 3})$*-set.*

Proof. (i) Let $\psi\colon (M,F) \to (M',F')$ be an R-isomorphism. Then ψ is an isomorphism of quadratic mappings $(M, q_F, \mathcal{D}(M)) \to (M', F', \mathcal{D}(M'))$. By Proposition 2.3, the map ψ is either C-linear or C-sesquilinear. Hence either $[M,F] = [M',F']$ or $[M,F] = \overline{[M',F']}$.

(ii) We start out with an element $[M,F] \in \mathcal{S}(C)$, which exists by hypothesis on M and by Theorem 5.2(i), and we choose a C-sesquilinear automorphism $\sigma\colon M \to M$. We know by Theorem 5.2 that all the C-forms on M are of the form wF with $w \in C^\times$. In particular $F \circ \sigma = wF$ for some $w \in C^\times$. An easy computation using (21) shows $(wF)\circ\sigma = \overline{w}(F\circ\sigma)$, so $F\circ\sigma^2 = \overline{w}wF$. Since σ^2 is C-linear, it follows from Theorem 5.2 that $\overline{w}w \in C^{\times 3}$. Using the fact that the cohomology of $\mathbf{Z}/2\mathbf{Z}$ with coefficients in a group of odd exponent (in this case $C^\times/C^{\times 3}$ with $\mathbf{Z}/2\mathbf{Z}$ acting via the canonical involution of C) is trivial, we conclude that $w = \overline{u}^{-1}uv^3$ for some $u, v \in C^\times$. Let $F_0 = uF$. By direct computation we have $F_0 \circ \sigma = v^3 F_0$; thus $\overline{[M,F]} = [M, F\circ\sigma] = [M,F]$ as claimed.

(iii) If $[M] \neq [\overline{M}]$, by Part (i), no two distinct elements of $\mathrm{Cubic}_C(M)$ can be identified in $\mathrm{Cubic}_R(M)$, that is, the canonical projection

$$\mathrm{Cubic}_C(M) \to \mathrm{Cubic}_R(M)$$

is a bijection. The second assertion follows from Theorem 5.2. □

COROLLARY 5.4. *Let* $[M] \in \mathrm{Pic}(C)$ *be as in Part (ii) of Theorem 5.3. Let* $[M, F_0] \in \mathrm{Cubic}_C(M)$ *be a the fixed point of the involution. Then the map* $(C^\times / C^{\times 3}) \to \mathrm{Cubic}_C(M)$ *given by* $u \mapsto [M, uF_0]$ *is an isomorphism of* $\mathbf{Z}/2\mathbf{Z}$*-sets. In particular, this correspondence induces a bijection* $\mathrm{Cubic}_R(M) \simeq (C^\times / C^{\times 3})/\sim$, *where* $\sim$ *identifies* c *with* $\bar{c}$.

Proof. By Theorem 5.2, it is enough to show that the map $u \mapsto [M, uF_0]$ commutes with the action of $\mathbf{Z}/2\mathbf{Z}$ via the involutions. Let $\sigma\colon (\bar{M}, F_0) \to (M, F_0)$ be a C-isomorphism and let $u \in C^\times$. Since $(uF_0) \circ \sigma = \bar{u}(F_0 \circ \sigma)$, we have $\overline{[M, uF_0]} = [\bar{M}, uF_0] \overset{\sigma}{=} [M, (uF_0) \circ \sigma] = [M, \bar{u}(F_0 \circ \sigma)] = [M, \bar{u}F_0]$. □

The above proposition applies in particular to the case of fields. We can summarize our results in this case as follows:

PROPOSITION 5.5. *Let* K *be a field of characteristic not 2 or 3. Let* $\mathcal{S}_K$ *be the set of* K*-isomorphism classes of all binary cubic forms over* K *with nonzero discriminant. Then there is a natural partition*

$$\mathcal{S}_K = \coprod_C \mathrm{Cubic}_K(C), \tag{25}$$

where C *ranges over the quadratic étale* K*-algebras and each* $\mathrm{Cubic}_K(C)$ *is in one-to-one correspondence with the quotient of* $C^\times/(C^\times)^3$ *by the involution* $c \mapsto \bar{c}$.

Proof. If K is a field then $\mathrm{Pic}(C) = 0$ for all quadratic K-algebras C. Each cubic form with nonzero discriminant will be a C-form for a unique quadratic étale algebra, namely the even Clifford algebra of its determining form, by Proposition 2.8 and Theorem 4.5. We finish by applying Proposition 5.3. □

As an illustration of these ideas, we prove a result known to L. E. Dickson [5, page 23]:

PROPOSITION 5.6. *Let* $K = \mathbf{F}_q$ *be a finite field with* q *elements, not of characteristic* 2 *or* 3. *Then the number of* $\mathbf{GL}_2(\mathbf{F}_q)$*-equivalence classes of binary cubic forms over* $\mathbf{F}_q$ *with nonzero discriminant is* 3 *if* $q \equiv 2 \mod 3$, *and is* 9 *if* $q \equiv 1 \mod 3$.

Proof. The étale quadratic algebras over $\mathbf{F}_q$ are

1. $C = \mathbf{F}_q \times \mathbf{F}_q$;
2. $C = \mathbf{F}_{q^2}$.

If $q \equiv 2 \bmod 3$, then $C^\times/(C^\times)^3$ is trivial in the first case and is $\mathbf{Z}/3\mathbf{Z}$ in the second case since $q^2 \equiv 1 \bmod 3$. In the second case the involution $c \to \bar{c}$ fixes the identity element of $C^\times/(C^\times)^3$ and interchanges the other two elements, giving 2 orbits on this. This gives $1+2$ orbits in total, so by Proposition 5.5, we have 3 isomorphism classes of binary cubic forms. If $q \equiv 1 \bmod 3$, then $C^\times/(C^\times)^3$ is $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ in the first case and is $\mathbf{Z}/3$ in the second case. In the second case, the Galois involution acts trivially, since $\mathbf{F}_q^\times/(\mathbf{F}_q{}^\times)^3 = C^\times/(C^\times)^3$. This gives 3 orbits. In the first case, the involution flips the two factors, and there are clearly 6 orbits. This gives a total of 9 orbits, and hence 9 cubic forms. □

REMARK 5.7. When $R = K$ is a field of characteristic not 2 or 3, one can give an alternate description of $\mathcal{S}_R$. Since $\mathbf{GL}_2$ acts threefold transitively on $\mathbf{P}^1$, any binary cubic form with nonzero discriminant is equivalent over the separable closure of K with $\Phi = xy(x-y)$. Therefore, by the usual descent yoga, there is a canonical bijection

$$\mathcal{S}_K \simeq H^1(K, \mathrm{Aut}(\Phi)), \tag{26}$$

where $\mathrm{Aut}(\Phi)$ is the K-group scheme of automorphisms of Φ. The structure of $\mathrm{Aut}(\Phi)$ is easily worked out:

$$\mathrm{Aut}(\Phi) = \mu_3 \times S_3,$$

where S_3 is the symmetric group on 3 letters as a trivial Galois module; it corresponds to the stabilizer in $\mathbf{PGL}_2$ of the set of zeros of Φ in $\mathbf{P}^1$.

The signature $S_3 \to \mu_2$ induces a homomorphism $\delta\colon \mathrm{Aut}(\Phi) \to \mu_2$, which in turn induces a map in Galois cohomology

$$\delta_*\colon H^1(K, \mathrm{Aut}(\Phi)) \to H^1(K, \mu_2) = K^\times/K^{\times 2}. \tag{27}$$

Using (4) and the identification (26), we can show that

$$\delta_*(F) = -3D_F \in K^\times/K^{\times 2}.$$

Thus we can interpret the partition (25) as the partition on $H^1(K, \mathrm{Aut}(\Phi))$ given by the fibers of δ_*, the set $\mathrm{Cubic}_K(C)$ corresponding to the fiber $\delta_*^{-1}(-3D)$, where D is the discriminant of C.

When R is a PID we can give a more precise version of Theorem 5.2. In this case, C is a free R-module, and since $R1$ is a direct factor, $C = R \oplus R\omega = R[\omega]$ is a monogenic R-algebra. Therefore C^* is free of rank one over C (see Section 7), so the condition $3[M] = [C^*]$ of Theorem 5.2 reads simply $3[M] = 0$. Furthermore, since $\mathrm{Pic}(R) = 0$, the exact sequence (13) induces an isomorphism

$$G(C)[3] \simeq H(C)[3] = \mathrm{Pic}(C)[3] \tag{28}$$

(note that $R^\times / n(C^\times)$ is an elementary abelian 2-group).

The isomorphism (28) suggests that when R is a PID, it should be possible to use quadratic forms instead of quadratic mappings and develop a theory for binary cubic forms that is completely parallel to Eisenstein's theory over $\mathbf{Z}$. As we mentioned above, any projective R-module is free, so that a quadratic form (M, q) is the same thing as a quadratic form classically understood: a homogeneous polynomial of degree two. If q is of type C then $M = R^2$ becomes an invertible C-module. This C-module is said to be *associated to* q.

We begin by proving an easy technical lemma.

LEMMA 5.8. *Suppose that R is a UFD and let $C = R[t]/(t^2 + bt + c)$. Let $D = b^2 - 4c$ and let ω be the class of t in C. Set $\delta = b + 2\omega$ (note that $\delta^2 = D$) and let $\xi = x + y\delta$ with $x, y \in R$. If $n(\xi) \equiv 0 \pmod{4R}$, then $\xi \equiv 0 \pmod{2C}$.*

Proof. It is enough to prove $x \equiv by \pmod{2R}$. Let $p \in R$ be an irreducible element. For $z \in R - \{0\}$ we denote by $\mathrm{ord}_p(z)$ the largest power of p occurring in the factorization of z. Set $m = \mathrm{ord}_p(x - by)$. If $m < \mathrm{ord}_p(2)$ then, since ord_p is a valuation, $\mathrm{ord}_p(x + by) = \mathrm{ord}_p(x - by + 2by) = m$. Hence $\mathrm{ord}_p(x^2 - b^2y^2) = 2m < \mathrm{ord}_p(4)$, which contradicts our assumption (since $b^2 \equiv D \pmod{4R}$). Therefore $\mathrm{ord}_p(x - by) \geq \mathrm{ord}_p(2)$ for all irreducible p, which proves the lemma. □

Now we can prove:

PROPOSITION 5.9. *Let R be a PID and let F be a cubic form on $M = R^2$ given in the natural basis by (1), with coefficients $a_i \in R$. Suppose that its Eisenstein determining form $q_F(\mathbf{x}) = ax_1^2 + bx_1x_2 + cx_2^2$, as in (2), is primitive of discriminant $D \neq 0$ and let $C := C^+(q_F) = R[t]/(t^2 + bt + ac)$. Then $3[M, q_F] = 0$ in $G(C)$.*

Proof. By the syzygy (7) we have

$$4q_F(\mathbf{x})q_F(\mathbf{y})q_F(\mathbf{z}) = X^2 - DY^2,$$

where X and Y are symmetric R-trilinear forms in $\mathbf{x}, \mathbf{y}, \mathbf{z}$. Applying the lemma to the rings $R' := R[x_1, x_2, y_1, y_2, z_1, z_2]$ and $C' := C \otimes_R R'$ with $\xi = X + \delta Y$ (with δ as in the lemma; the lemma applies since R, hence R', is a UFD), we have

$$q_F(\mathbf{x})q_F(\mathbf{y})q_F(\mathbf{z}) = n(T), \tag{29}$$

where $T = \xi/2 \in C'$, by the lemma. Note that T is symmetric trilinear in $\mathbf{x}, \mathbf{y}, \mathbf{z}$; hence the identity (29) shows that the triplication of q_F is the trivial form, as desired. □

The results below were essentially known in the case $R = \mathbf{Z}$ to Eisenstein [6] and [7], Arndt [1], Pepin [13], Cayley [3] and Hermite [8].

THEOREM 5.10. *Let R be a PID. Let $q = ax_1^2 + bx_1x_2 + cx_2^2$ be a primitive binary quadratic form over R of discriminant $D = b^2 - 4ac \neq 0$. Let $C = C^+(q)$ be the even Clifford algebra of q and let $M := R^2$ be endowed with the natural C-module structure. Let $\tau \in C$ be such that $\tau + \overline{\tau} = 0$ and $\tau^2 = D$. With this notation we have*

(i) *There exists a Gaussian binary cubic form F such that $q_F = q$ (where q_F is given by (2)) if and only if $3[M, q] = 0$ in the group $G(C)$ of C-isomorphism classes of quadratic forms of type C.*

(ii) *If F and F' are Gaussian binary cubic forms with $q_F = q_{F'} = q$, then there exists a unit $c = a + b\tau \in C^\times$ with $n(c) = 1$ such that $F' = cF = aF + bG_F$, where G_F is the cubic covariant defined in (5).*

(iii) *Let two cubic forms F and F' with $q_F = q_{F'} = q$ be given. The following conditions are equivalent:*

  (a) *There exists $d \in C^\times$ with $n(d) = 1$ such that $F' = d^3F$.*

  (b) *There exists $d \in C^\times$ such that $F' = d^3F$.*

  (c) *F and F' are $\mathbf{SL}_2(R)$-equivalent.*

Proof. (i) By Proposition 5.9 the condition $3[M, q] = 0$ is necessary. We shall see that it is sufficient. Suppose $3[M, q] = 0$ in $G(C)$; in particular

$$3[M] = 0 \in \mathrm{Pic}\,(C),$$

thus by virtue of Theorem 5.2, Part (i), there exists a Gaussian cubic form F such that $[M, q_F, R] = [M, q, R]$ in $H(C)$. By Proposition 5.9, the class $[M, q_F]$ is in $G(C)[3]$; hence, by the isomorphism (28), we conclude $[M, q_F] = [M, q]$ in $G(C)$.

(ii) Suppose that $q_F = q_{F'} = q$. $C \otimes K$ is an étale K-algebra since $D \neq 0$. Hence by Corollary 4.7 both F and F' are C-forms and by Theorem 5.2, Part (ii), there exists $c \in C^\times$ such that $F' = cF = (\rho(c)/3)F$ (in the notation of (23)). Writing $c = a + b\tau$ we get $F' = aF + (b/3)(\rho(\tau)F)$. By (24) we have $\rho(\tau)F = 3G_F$ (changing the sign of τ if needed) and direct computation shows $q_{F'} = n(c)q_F$. Thus $n(c) = 1$ as required. Note that in general, the coefficients a, b will have a 2 in the denominator since $\tau = b + 2\omega$ for a generator ω of the algebra C (see Lemma 5.8).

(iii) a)$\Rightarrow$b) is trivial.

b)$\Rightarrow$c). If $F' = d^3F$ with $d \in C^\times$ then, by Part (ii) of Theorem 5.2, F and F' are C-equivalent, the isomorphism being $\mathbf{x} \to d\mathbf{x}$. We have $n(d)^3 = 1$ by the proof of Part (ii) of this theorem, so replacing d by $n(d)d$ we can assume $n(d) = 1$; that is, F and F' are $\mathbf{SL}_2(R)$-equivalent, and this also establishes the implication b)$\Rightarrow$a).

c)$\Rightarrow$a). If $F'(\mathbf{x}) = F(d\mathbf{x})$, where $d \in \mathbf{SL}_2(R)$, then d is in the orthogonal group of $q = q_F = q_{F'}$. Since $\det(d) = 1$, it is in the special orthogonal group of this form, hence given by multiplication by an element $d \in C_1^\times$ by Corollary 2.4. But $F(d\mathbf{x}) = (d^3F)(\mathbf{x})$. □

COROLLARY 5.11. *Now let $R = \mathbf{Z}$, and let D be a nonzero integer congruent to 0 or 1 modulo 4. Let F be an integral Gaussian binary cubic form with primitive determining form of discriminant D.*

(i) *Suppose $D < -3$. If F' is another Gaussian binary cubic form with $q_{F'} = q_F$ then F' is $\mathbf{SL}_2(\mathbf{Z})$-equivalent to F.*

(ii) *Suppose $D > 0$ or $D = -3$. Then there are exactly three $\mathbf{SL}_2(\mathbf{Z})$-equivalence classes of Gaussian binary cubic forms F' such that $q_{F'} = q_F$.*

Proof. We have that $C^+(q_F) = C_D$, the unique quadratic $\mathbf{Z}$-algebra of discriminant D. Note that $(C_D)_1^\times / (C_D)_1^{\times 3}$ is trivial when $D < -3$ and is cyclic of order 3 when $D = -3$ or $D > 0$. The corollary follows immediately from this and Parts (ii) and (iii) of Theorem 5.10. □

COROLLARY 5.12. *Let D be a nonzero integer congruent to 0 or 1 modulo 4. Let $h_3(D)$ be the number of $\mathbf{SL}_2(\mathbf{Z})$-equivalence classes if binary Gaussian cubic forms with primitive determining form of discriminant D. Then $h_3(D) = |\mathrm{Pic}\,(C_D)[3]|$ if $D < -3$ and $h_3(D) = 3|\mathrm{Pic}\,(C_D)[3]|$ if $D = -3$ or $D > 0$.*

Proof. Follows immediately from Corollary 5.11, equation (28) and Part (i) of Theorem 5.10. □

6. Cohomological interpretation

Let $\mathbf{G}_m$ be the multiplicative group regarded as an affine group scheme over $X := \operatorname{Spec} C$ and let $\mu_3 \subset \mathbf{G}_m$ be the kernel of multiplication by 3. All the cohomology groups below are with respect to the flat topology on X.

THEOREM 6.1. *Suppose* $[C^*]$ *is divisible by* 3 *in* $\operatorname{Pic}(C)$. *Then the group* $H^1_{\mathrm{fl}}(X, \mu_3)$ *acts simply transitively on the set* $\mathcal{S}(C)$ *of* C*-equivalence classes of cubic* C*-forms with primitive determining mapping.*

Proof. Recall that the group $H^1_{\mathrm{fl}}(X, \mu_3)$ can be interpreted concretely as the set of isomorphism classes of pairs (L, ψ), where L is an invertible C-module and where $\psi\colon L_C^{\otimes 3} \to C$ is an isomorphism (see Milne [14, Chap. III, §4]). Let $[L, \psi]$ be an element of $H^1_{\mathrm{fl}}(X, \mu_3)$ and let (M, F) be a cubic C-form. By Theorem 5.1, Part (i), we can assume $F = F_\phi$, where $\phi\colon M^{\otimes 3} \to C^*$ is an isomorphism. We define an action of $H^1_{\mathrm{fl}}(X, \mu_3)$ on $\mathcal{S}(C)$ by

$$[L, \psi] \cdot [M, F_\phi] = [L \otimes M, F_{\psi \otimes \phi}], \tag{30}$$

noting that

$$(L \otimes M)_C^{\otimes 3} = L_C^{\otimes 3} \otimes M_C^{\otimes 3} \xrightarrow{\psi \otimes \phi} C \otimes C^* = C^*$$

is an isomorphism. Let us show first that this action is simple. Suppose $[L \otimes M, F_{\psi \otimes \phi}] = [M, F_\phi]$. Then, $L \cong C$. Choosing an isomorphism $L \to C$, we have $\psi(x \otimes y \otimes z) = uxyz$, where $u \in C^\times$. Hence $[M, F_\phi] = [M, F_{u\phi}]$, and by Part (iii) of Theorem 5.1 we conclude that $u = c^3$ for some $c \in C^\times$. But then $c\colon C \to C$ provides an isomorphism of (C, ψ) with $(C, 1)$, thus $[L, \psi] = [C, 1]$.

We show now that the action is transitive. Let $[M_i, F_{\phi_i}]$ $(i = 1, 2)$ be elements of $\mathcal{S}(C)$. Let $M_2^\bullet = \operatorname{Hom}_C(M_2, C)$ and let $\phi_2^\bullet : (C^*)^\bullet \to (M_2^{\otimes 3})^\bullet$ be the dual of ϕ_2. Let $L = M_1 \otimes M_2^\bullet$ and let $\psi = \phi_1 \otimes \phi_2^{\bullet -1}$. One verifies immediately that $[L, \psi] \cdot [M_2, F_{\phi_2}] = [M_1, F_{\phi_1}]$, which proves that the action is transitive. □

Note that, under the hypothesis of (6.1),

$$\mathcal{S}(C) = \coprod_{L \in \mathrm{Pic}\,(C)[3]} \mathrm{Cubic}_C(M_0 \otimes L)$$

where M_0 is any invertible module such that $M_0^{\otimes 3} \cong C^*$. Each $\mathrm{Cubic}_C(M)$ is a torsor for $C^\times/(C^\times)^3$ by Theorem 5.2.

Consider now the short exact sequence of group schemes over X

$$1 \longrightarrow \mu_3 \xrightarrow{i} \mathbf{G}_m \xrightarrow{3} \mathbf{G}_m \longrightarrow 1$$

and the associated Kummer long exact sequence in flat cohomology

$$H^0_{\mathrm{fl}}(X, \mathbf{G}_m) \xrightarrow{3} H^0_{\mathrm{fl}}(X, \mathbf{G}_m) \xrightarrow{\partial} H^1_{\mathrm{fl}}(X, \mu_3) \xrightarrow{i_*} H^1_{\mathrm{fl}}(X, \mathbf{G}_m) \xrightarrow{3} H^1_{\mathrm{fl}}(X, \mathbf{G}_m).$$

Using the canonical isomorphisms (see [14, Chap. III, §4])

$$H^0_{\mathrm{fl}}(X, \mathbf{G}_m) \simeq C^\times, \quad H^1_{\mathrm{fl}}(X, \mathbf{G}_m) \simeq \mathrm{Pic}\,(C)$$

we obtain a short exact sequence

$$1 \to C^\times/C^{\times 3} \xrightarrow{\partial} H^1_{\mathrm{fl}}(X, \mu_3) \xrightarrow{i_*} \mathrm{Pic}\,(C)[3] \to 1. \tag{31}$$

By what we have proved, $\mathcal{S}(C)$ will be empty unless $[C^*]$ is divisible by 3 in $\mathrm{Pic}\,(C)$. By the Kummer sequence, $[C^*]$ is divisible by 3 if and only if

$$\partial[C^*] = 0 \in H^2_{\mathrm{fl}}(X, \mu_3).$$

Assume that this holds and consider the group $H(C)$ of binary quadratic mappings as defined by Kneser in [11]. The determining form construction (14) gives a well-defined map

$$e\colon \mathcal{S}(C) \longrightarrow H(C)$$
$$[M, F] \longmapsto [M, q_F, \mathcal{D}(M)].$$

We fix a "base point" $[M_0, F_0] \in \mathcal{S}(C)$ and we modify the map e slightly so that it becomes a map of pointed sets. We define

$$e'\colon \mathcal{S}(C) \longrightarrow H(C)$$
$$[M, F] \longmapsto e[M, F] - e[M_0, F_0].$$

We also define a map $f\colon H^1_{\mathrm{fl}}(X, \mu_3) \to \mathcal{S}(C)$ by $f(x) = x \cdot [M_0, F_0]$, where $\cdot$ is the action defined in (30). Note that by virtue of Theorem 6.1, the map f is bijective.

With this notation we have a commutative square

$$\begin{array}{ccc} H^1_{\mathrm{fl}}(X, \mu_3) & \xrightarrow{i_*} & \mathrm{Pic}\,(C)[3] \\ \downarrow f & & \uparrow j \\ \mathcal{S}(C) & \xrightarrow{e'} & H(C)[3] \end{array} \tag{32}$$

where $j\colon H(C) \to \mathrm{Pic}\,(C)$ is the natural homomorphism $[M, q, N] \mapsto [M]$. Kneser [11, §6] has shown that j is an isomorphism (see also Section 2), so the two vertical maps in (32) are bijections and the horizontal maps are surjections.

Note that because of the exact sequence (31), the fibers of e' are in one-to-one correspondence with the elements of the group $C^\times/C^{\times 3}$. This is, of course, equivalent to Theorem 5.2, Part (ii).

7. Explicit computations and cubic trace forms

In this section we assume that $A := C \otimes K$ is a quadratic étale algebra over K. In this case the trace form $(x, y) \to \mathrm{Tr}_{A/K}(xy)$ is nondegenerate and gives rise to a natural isomorphism between the codifferent

$$C' = \{x \in A : \mathrm{Tr}_{A/K}(xC) \subset R\}$$

and the dual C^*. If M is a fractional C-ideal with $M^3 \simeq C'$, then, by Theorem 5.1, the cubic forms on M with primitive determining form are given by

$$F_u(\mathbf{x}) = \mathrm{Tr}_{A/K}(ua\mathbf{x}^3)\,, \tag{33}$$

where $a \in A$ is a fixed element with $aM^3 = C'$, and u is a unit of C. Moreover, by Theorem 5.1, two such forms F_u and F_v are C-isomorphic if and only if u and v represent the same element of $C^\times/(C^\times)^3$.

We shall compute explicitly some examples for $R = \mathbf{Z}$ using (33). In this case we have $C = \mathbf{Z}[t]/(f(t))$, where f is a monic degree-two polynomial with distinct roots and coefficients in $\mathbf{Z}$.

Let ω be the class of t in C. It is well-known, and easy to prove, that the codifferent C' is a principal fractional C-ideal generated by $f'(\omega)^{-1}$, where f' is the derivative of f. Hence, $[C^*]$ is trivial in $\mathrm{Pic}\,(C)$ (note that this holds more generally provided $\mathrm{Pic}\,(R) = 0$).

EXAMPLE 7.1. Let $C = \mathbf{Z}[\frac{1+\sqrt{-23}}{2}]$ (note that 23 is the smallest square-free positive integer N such that $A = \mathbf{Q}(\sqrt{-N})$ has class number divisible by 3; in fact $\mathrm{Pic}(C) \simeq \mathbf{Z}/3\mathbf{Z}$ (see [2]). The class group $\mathrm{Pic}(C)$ is generated by the class of

$$M = 2\mathbf{Z} + \omega\mathbf{Z},$$

where $\omega = \frac{1+\sqrt{-23}}{2}$. Thus the three classes of $\mathrm{Pic}(C)$ are represented by the ideals C, M and $\overline{M}$. The quadratic forms attached to C, M and $\overline{M}$ are respectively

$$x_1^2 + x_1x_2 + 6x_2^2, \quad 2x_1^2 + x_1x_2 + 3x_2^2, \quad 2x_1^2 - x_1x_2 + 3x_2^2.$$

One verifies also that $\theta = \omega - 2$ satisfies $M^3 = \theta C$, thus $(1/\theta\sqrt{-23})M^3 = C'$. Hence, by (33), the cubic C-form on M is given by

$$F(\mathbf{x}) = \mathrm{Tr}\left(\frac{\mathbf{x}^3}{\theta\sqrt{-23}}\right),$$

where $\mathbf{x} = 2x_1 + x_2\omega$. Similar computations can be done for $\overline{M}$ (taking $\theta = -1 - \omega$ and the $\mathbf{Z}$-basis $\{2, -1+\omega\}$) and for C (with the basis $\{1, \omega\}$). The following table summarizes the results of these computations:

Module	Cubic Form	Determining Form
M	$-x_1^3 - 3x_1^2x_2 + 3x_1x_2^2 + 2x_2^3$	$2x_1^2 + x_1x_2 + 3x_2^2$
$\overline{M}$	$x_1^3 - 3x_1^2x_2 - 3x_1x_2^2 + 2x_2^3$	$2x_1^2 - x_1x_2 + 3x_2^2$
C	$x_2(3x_1^2 + 3x_1x_2 - 5x_2^2)$	$x_1^2 + x_1x_2 + 6x_2^2$

EXAMPLE 7.2. Let $C = \mathbf{Z}[\sqrt{79}]$. Here also $\mathrm{Pic}(C) \simeq \mathbf{Z}/3\mathbf{Z}$ (see [2]) (in fact 79 is the smallest square-free positive integer N such that $\mathbf{Q}(\sqrt{N})$ has class number divisible by 3).

The class group $\mathrm{Pic}(C)$ is generated by the class of

$$M = 9\mathbf{Z} + (4 + \sqrt{79})\mathbf{Z}.$$

Thus the three classes of $\mathrm{Pic}(C)$ are represented by the ideals C, M and $\overline{M}$. One verifies also that $\alpha = 52 - 5\sqrt{79}$ satisfies $M^3 = \alpha C$, thus $(1/2\alpha\sqrt{79})M^3 = C'$. The fundamental unit of C is $\tau = 80 + 9\sqrt{79}$; hence, by (33), the three nonisomorphic cubic C-forms on M are given by

$$F_{\tau^k}(\mathbf{x}) = \mathrm{Tr}\left(\frac{\tau^k}{2\alpha\sqrt{79}}\mathbf{x}^3\right),$$

where $\mathbf{x} = 9x_1 + (4 + \sqrt{79})x_2$ and $k = -1, 0, 1$. Similar computations can be done for $\overline{M}$ (taking the $\mathbf{Z}$-basis $\{9, -4 + \sqrt{79}\}$) and C (with the natural basis $\{1, \sqrt{79}\}$).

Module	Cubic Forms	Determining Form
M	$-68x_1^3 + 111x_1^2x_2 - 60x_1x_2^2 + 11x_2^3$ $5x_1^3 + 24x_1^2x_2 + 33x_1x_2^2 + 16x_2^3$ $868x_1^3 + 3729x_1^2x_2 + 5340x_1x_2^2 + 2549x_2^3$	$9x_1^2 + 8x_1x_2 - 7x_2^2$
$\overline{M}$	$-868x_1^3 + 3729x_1^2x_2 - 5340x_1x_2^2 + 2549x_2^3$ $-5x_1^3 + 24x_1^2x_2 - 33x_1x_2^2 + 16x_2^3$ $68x_1^3 + 111x_1^2x_2 + 60x_1x_2^2 + 11x_2^3$	$9x_1^2 - 8x_1x_2 - 7x_2^2$
C	$-9x_1^3 + 240x_1^2x_2 - 2133x_1x_2^2 + 6320x_2^3$ $3x_1^2x_2 + 79x_2^3$ $9x_1^3 + 240x_1^2x_2 + 2133x_1x_2^2 + 6320x_2^3$	$x_1^2 - 79x_2^2$

REFERENCES

[1] ARNDT, F. Zur Theorie der binären kubischen Formen. *J. Crelle 53* (1857), 309–321.

[2] BOREVICH, Z. I. and I. R. SHAFAREVICH. *Number Theory.* Academic Press, New York, 1966.

[3] CAYLEY, A. Two letters on cubic forms. *Quarterly Math. J. 1* (1857), 85–87, 90–91 = *Collected Mathematical Papers*, vol. 3, 9–12, Cambridge Univ. Press, 1890.

[4] DICKSON, L. E. *History of the Theory of Numbers, vol. III.* Chelsea, 1952.

[5] —— On invariants and the theory of numbers. *The Madison Colloquium.* Dover Publications, New York, 1966.

[6] EISENSTEIN, G. Théorèmes sur les formes cubiques et solution d'une équation du quatrième degré à quatre indéterminées. *J. Crelle 27* (1844), 75–79 = *Mathematische Werke*, Band I, Chelsea Publ. Co., 1975, 1–5.

[7] —— Untersuchungen über die cubischen Formen mit zwei Variabeln. *J. Crelle 27* (1844), 89–104 = Mathematische Werke, Band I, Chelsea Publ. Co., 1975, 10–25.

[8] HERMITE, C. Lettre à Cayley sur les formes cubiques. *Œuvres*, tome 1, 437–439, Gauthier-Villars, 1905.

[9] IGUSA, J. I. Lectures on Forms of Higher Degree. *Tata Institute Lectures on Mathematics and Physics, vol. 59.* Springer-Verlag, Berlin, Heidelberg, New York, 1978.

[10] KNUS, M.-A., A. MERKURJEV, M. ROST and J.-P. TIGNOL. *The Book of Involutions.* American Mathematical Society Colloquium Publications, vol. 44, 1998.

[11] KNESER, M. Composition of binary quadratic forms. *J. Number Theory 15* (1982), 406–413.

[12] LANG, S. *Algebra.* Addison-Wesley, 1971.

[13] PEPIN, TH. Théorie des fonctions homogènes du troisième degré, à deux variables. *Atti Accad. Pont. Nuovi Lincei 37* (1883), 227–294.

[14] MILNE, J. S. *Étale Cohomology.* Princeton University Press, 1980.

[15] SPRINGER, T. A. *Invariant Theory.* Lecture Notes in Mathematics, vol. 585, Springer-Verlag, 1977.

[16] WRIGHT, D. J. The adelic zeta function associated with the space of binary cubic forms, I: global theory. *Math. Ann. 270* (1985), 503–534.

(Reçu le 3 juin 1999)

J. William Hoffman and Jorge Morales

Louisiana State University
Department of Mathematics
Baton Rouge, LA 70803
USA
e-mail: hoffman@math.lsu.edu
morales@math.lsu.edu