1. Introduction

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.