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

$$F(\mathbf{x}) = a_0 x_1^n + a_1 x_1^{n-1} x_2 + \cdots + a_{n-1} x_1 x_2^{n-1} + a_n x_2^n ,$$

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.