1. Introduction

L'Enseignement Mathématique, t. 36 (1990), p. 321-358

THE DISTANCE BETWEEN IDEALS IN THE ORDERS OF A REAL QUADRATIC FIELD

par Pierre KAPLAN and Kenneth S. WILLIAMS [1])

1. INTRODUCTION

The notion of the distance between two equivalent, reduced, primitive ideals of an order in the ring of integers of a real quadratic field was first introduced by Shanks [7] in 1972 in order to develop a more efficient algorithm for computing the fundamental unit of the field, although this notion was already implicit in the work of earlier authors including Lagrange [2]. Shanks used the language of binary quadratic forms to describe the concept of distance. This concept, still described in terms of binary quadratic forms, was made more precise and exploited by Lenstra [4] (1982) and Schoof [6] (1983) in their work on quadratic fields and factorization. In 1986 Williams and Wunderlich [12] gave a treatment of distance in terms of ideals, and used it to develop a simple algorithm for use in the continued fraction factoring algorithm. Parts of their theory have also been used in numerical studies of Eisenstein's problem [9] [11].

The aim of this papers is two-fold. We first give a complete treatment of the basic theory of the distance between equivalent, reduced, primitive ideals in the hope of making this attractive and useful theory better known and more readily available for further research. Our treatment is based mainly on the presentation of Williams and Wunderlich [12], but, in our view, is simpler in some aspects. Our second objective is to define a homomorphism between the ideal class groups of different orders and to apply this theory to compare distances between corresponding ideals in the two orders. The presentation is self-contained in that factorization of ideals in an order of a quadratic field is not needed, nor do we use the theory of the units of a real quadratic field. Indeed the theory of units is a consequence of our presentation, see Corollary 5. We give known results as Propositions and new results as Theorems.

[1]) Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

Throughout this paper, if A is a unitary commutative ring, and $\alpha_1, \alpha_2, \ldots, \alpha_m$ are elements of A, the Z-module generated by $\alpha_1, \alpha_2, \ldots, \alpha_m$ is denoted by $[\alpha_1, \alpha_2, \ldots, \alpha_m]$ and the A-module (ideal) generated by $\alpha_1, \alpha_2, \ldots, \alpha_m$ by $(\alpha_1, \alpha_2, \ldots, \alpha_m)$. The product of the ideals $(\alpha_1, \ldots, \alpha_m)$ and $(\alpha'_1, \ldots, \alpha'_n)$ is the ideal $(\alpha_1\alpha'_1, \ldots, \alpha_i\alpha'_j, \ldots, \alpha_m\alpha'_r)$. If I is an ideal, we often write the product ideal $(\alpha)I$ as αI.

2. Basic definitions

Let K be a quadratic field of discriminant D_0. As D_0 is a discriminant we have $D_0 \equiv 0 \pmod 4$ or $D_0 \equiv 1 \pmod 4$. In §2 and §3 K may be real ($D_0 > 0$) or imaginary ($D_0 < 0$) but in the remaining sections K will be assumed to be real. An element α of K can be written $\alpha = x + y\sqrt{D_0}$, where x and y are rational numbers. The conjugate of α is the element $\bar{\alpha} = x - y\sqrt{D_0}$ of K. The norm of α is the rational number $N(\alpha) = \alpha\bar{\alpha} = x^2 - D_0y^2$. We define the integer ω_0 of K by

$$\omega_0 = \begin{cases} \dfrac{\sqrt{D_0}}{2}, & \text{if } D_0 \equiv 0 \pmod 4, \\ \dfrac{1}{2}(1 + \sqrt{D_0}), & \text{if } D_0 \equiv 1 \pmod 4. \end{cases} \tag{2.1}$$

The ring of integers of K is $O_{D_0} = [1, \omega_0]$. For a positive integer f, we set

$$D = D_0f^2, \omega = \begin{cases} \dfrac{\sqrt{D}}{2}, & \text{if } D \equiv 0 \pmod 4 \\ \dfrac{1}{2}(1 + \sqrt{D}), & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{2.2}$$

and

$$O_D = [1, \omega] = [1, f\omega_0]. \tag{2.3}$$

It is easy to check that O_D is the subring of index f in O_{D_0}, called the order of discriminant D. We note that

$$\omega^2 = \begin{cases} \dfrac{D}{4}, & \text{if } D \equiv 0 \pmod 4, \\ \omega + \dfrac{(D-1)}{4}, & \text{if } D \equiv 1 \pmod 4. \end{cases} \tag{2.4}$$