FACTORIZATION IN QUADRATIC RINGS

By Hubert S. Butts and Gordon Pall

1. Introduction. In this paper we consider the problem of determining the number of factorizations of an ideal in a ring with unity in a quadratic number field as a product of two ideals with given norms, and we also consider the same problem for algebraic integers of the ring rather than ideals (questions of a related nature are considered in [4] and [1]). Denote by R the field of rational numbers, by Z the ring of rational integers, by Δ a nonsquare element of Z such that $\Delta \equiv 0$ or $1 \pmod 4$, and set $\omega = (\epsilon + \sqrt{\Delta})/2$ ($\epsilon = 0$ or 1 according as Δ is even or odd). Let K denote the field $R(\sqrt{\Delta})$, $D_\Delta = \{a + b\omega \mid a, b \text{ in } Z\}$, and denote by D the set of algebraic integers in K. Let s be the largest rational integer such that $\Delta_0 = \Delta/s^2$ is an integer $\equiv 0$ or $1 \pmod 4$. The principal ideal sD is called the conductor of the domain D_Δ—it is the g.c.d. of the set of ideals in D_Δ which are also ideals in D. If A and B are ideals in D_Δ, then the ideal $A + B = \{\alpha + \beta \mid \alpha \text{ in } A, \beta \text{ in } B\}$ is the g.c.d. of A and B. An ideal A in D_Δ is said to be prime to the conductor, or briefly, *s-prime*, if $A + sD = D_\Delta$ [2; 129] and [6; 351]. If A is an ideal in D_Δ, then $\bar{A}$ denotes the ideal $\{\bar{\alpha} \mid \alpha \in A\}$ where $\bar{\alpha}$ denotes the quadratic conjugate of α. For s-prime ideals $N(A) = A\bar{A}$ is a principal ideal (a), where a can be taken to be the positive rational integer which gives the number of residue classes of D_Δ modulo A. Furthermore, for s-prime ideals, $N(AB) = N(A)N(B)$, $\overline{AB} = \bar{A}\cdot\bar{B}$, $\overline{A + B} = \bar{A} + \bar{B}$, and if $A \supset B$, then there is an ideal C such that $AC = B$. The largest rational integer d such that $A = (d)A'$ with A' an ideal in D_Δ is called the *divisor of* A. If A is s-prime, and $A = BC$, then B and C are s-prime.

2. Factorization of ideals in D_Δ. The main result is Theorem 1.

Lemma 1. *Let A be s-prime, $A \neq (0)$, $N(A) = (bc)$ where b and c are positive rational integers. Let d denote the divisor of A and set $e = (d, b, c)$. Then if $c \in A$ the number of factorizations*

$$A = BC, \quad \text{with} \quad N(B) = (b) \quad \text{and} \quad N(C) = (c), \tag{1}$$

is equal to the number of ideals H such that $N(H) = (e)$.

Proof. We prove that if $c \in A$, then $e = b$. Indeed, if $c \in A$, then there exists an ideal Q such that $AQ = (c)$ and therefore

$$A\bar{A} = (b)(c) = (b)AQ, \qquad \bar{A} = (b)Q, \qquad A = (b)\bar{Q}.$$

It follows that $(c) \subset A \subset (b)$, $b \mid c$, $b \mid d$, and $e = b$.

Received May 9, 1966. This work was supported in part by National Science Foundation grants GP 6467 and GP 3956.