PACIFIC JOURNAL OF MATHEMATICS
Vol. 22, No. 1, 1967

REMARK ON A PROBLEM OF NIVEN AND ZUCKERMAN

R. T. BUMBY AND E. C. DADE

An integer of an algebraic number field K is called irreducible if it has no proper integer divisors in K. Every integer of K can be written as a product of irreducible integers, usually in many different ways. Various problems have been inspired by this lack of unique factorization. This paper studies the question: When are the irreducible integers of K determined by their norms? Attention is confined to the case in which K is a quadratic field. With this assumption it is possible to give a complete answer in terms of the ideal class group of K and the nature of the units of K.

The fields sought in this problem are those quadratic fields K (with $N: K \to Q$ denoting the norm) which satisfy

Property N: *If α is an irreducible integer of K and β is another integer of K such that $N\alpha = N\beta$, then β is also irreducible.*

In many cases Property N can be studied by looking at the class group H of K. However the study is complicated by the existence of quadratic number fields K satisfying:

(1) *K is real and $N\varepsilon = +1$, for every unit ε of K.*

When K satisfies (1), we are forced to consider an extended class group H' of K defined as follows:

Two nonzero fractional ideals $\mathfrak{a}, \mathfrak{b}$ are said to be *strongly equivalent* if $\mathfrak{a} \cdot \mathfrak{b}^{-1} = (\gamma)$ is a principal ideal generated by an element γ of positive norm. This is clearly an equivalence relation. The strong equivalence classes form the group H' under the usual multiplication. There are two strong equivalence classes of principal ideals: the class σ consisting of all principal ideals (α) such that one, and hence all, generators of (α) have negative norm; and the identity class 1 of principal ideals (α) all of whose generators have positive norm. Clearly $\sigma^2 = 1$, and the class group H is naturally isomorphic to $H'/\langle\sigma\rangle$.

If K does not satisfy (1), notice that H', as defined above, and the class group H coincide.

In any case, if $\mathfrak{p}$ is any prime ideal of K and $\mathfrak{p}'$ is the conjugate prime ideal, then $\mathfrak{p} \cdot \mathfrak{p}' = (N\mathfrak{p})$. But $N(N\mathfrak{p}) = (N\mathfrak{p})^2 > 0$. So

(2) *$\mathfrak{p}$ and $\mathfrak{p}'$ lie in inverse strong equivalence classes.*

Our main result is

THEOREM. *Let K be a quadratic number field. Then K satisfies property N if and only if:*

(a) *H has exponent* 2

or (b) *H is odd*

or (c) *K satisfies* (1) *and the* 2*-Sylow subgroup of H' is cyclic*

Proof. First we assume that one of (a), (b), and (c) holds. If K does not satisfy property N then there exist an irreducible integer α and a reducible integer β such that $N\alpha = N\beta$. Let $(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_t$, where the $\mathfrak{p}_i$ are prime ideals. Since $N\beta = N\alpha$, the ideal (β) must equal $\mathfrak{q}_1 \cdots \mathfrak{q}_t$, where, for each i, either $\mathfrak{q}_i$ is $\mathfrak{p}_i$, or $\mathfrak{q}_i$ is $\mathfrak{p}'_i$. But $\beta = \gamma \cdot \delta$, where γ, δ are nonunit integers. Hence we may assume:

$$(\gamma) = \mathfrak{q}_1 \cdots \mathfrak{q}_s\,, \quad (\delta) = \mathfrak{q}_{s+1} \cdots \mathfrak{q}_t\,, \quad \text{where } 1 \leqq s < t\,.$$

Let e_i be $+1$ if $\mathfrak{q}_i = \mathfrak{p}_i$ and -1 if $\mathfrak{q}_i = \mathfrak{p}'_i$. By (2) there are numbers ε, ζ in K such that:

(3) $(\varepsilon) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$, $(\zeta) = \mathfrak{p}_{s+1}^{e_{s+1}} \cdots \mathfrak{p}_t^{e_t}$, *and* (γ), (δ) *are strongly equivalent to* (ε), (ζ), *respectively.*

In case (a), $\mathfrak{p}_i^{e_i}$ is equivalent to $\mathfrak{p}_i$. Therefore (3) implies that $\mathfrak{p}_1 \cdots \mathfrak{p}_s = (\eta)$ is a principal ideal. Clearly η is an integer and a proper divisor of α, contradicting its irreducibility.

In any case, if $e_1 = \cdots = e_s$, then $\mathfrak{p}_1 \cdots \mathfrak{p}_s$ is principal, and we arrive at a contradiction. Therefore we may assume

(4) $e_1 = \cdots = e_r = +1\,,\ e_{r+1} = \cdots = e_s = -1\,,$ *where* $1 \leqq r < s\,,$
and $e_{s+1} = \cdots = e_u = +1\,,\ e_{u+1} = \cdots = e_t = -1\,,$ *where* $s < u < t\,.$

Define the integral ideals $\mathfrak{a}, \mathfrak{b}$ by:

$$\mathfrak{a} = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)(\mathfrak{p}_{s+1} \cdots \mathfrak{p}_u)$$
$$\mathfrak{b} = (\mathfrak{p}_{r+1} \cdots \mathfrak{p}_s)(\mathfrak{p}_{u+1} \cdots \mathfrak{p}_t)\,.$$

By (4), both $\mathfrak{a}$ and $\mathfrak{b}$ are proper integral ideals. By (3), $\mathfrak{a} \cdot \mathfrak{b}^{-1} = (\varepsilon\zeta)$ is strongly equivalent to $(\gamma \cdot \delta) = (\beta)$. Since $N\beta = N\alpha$, the ideals (α), (β) are strongly equivalent. Therefore $\mathfrak{a} \cdot \mathfrak{b}^{-1}$ is strongly equivalent to $(\alpha) = \mathfrak{a} \cdot \mathfrak{b}$. So:

(5) $\mathfrak{b}^2 = (\mathfrak{a} \cdot \mathfrak{b})(\mathfrak{a} \cdot \mathfrak{b}^{-1})^{-1} = (\lambda)$, *where* $N\lambda > 0$.

In case (b), this implies that $\mathfrak{b}$ is principal. Hence α has a proper divisor.

In case (c), the only strong equivalence classes of orders dividing 2 are 1 and σ. By (5), $\mathfrak{b}$ must lie in one of them. So it is principal, and α has a proper divisor.

In each of the three cases, α must have a proper divisor, contradicting its irreducibility. So K must satisfy property N.

Now suppose that K satisfies property N. We first show that H' cannot contain an element π satisfying:

(6) *π has even order $2n > 2$ and, if K satisfies* (1), *then* $\pi^n \neq \sigma$.

Suppose such a π exists. By Dirichlet's theorem there exists a prime ideal $\mathfrak{p}$ in the class π (or, if K satisfies (1), in the class $\pi\langle\sigma\rangle$). Evidently $\mathfrak{p}^{2n} = (\alpha)$ is generated by an irreducible element α satisfying $N\alpha = p^{2n}$, where $p = N\mathfrak{p}$. But $p^{2n} = N(p^n)$, and, since $n > 1$, $p^n = p \cdot p^{n-1}$ is reducible. This contradicts property N. So no π satisfying (6) can exist.

Suppose K does not satisfy (1). It follows immediately from (6) that, if H has even order, then it must have exponent 2. So one of (a) or (b) must hold.

Now we assume that K satisfies (1). Then H' cannot contain elements τ, ρ satisfying:

(7) $\tau^{2^m} = \sigma$, *where* $m \geqq 2$, *and* $\rho^2 = 1$, $\rho \notin \langle\sigma\rangle$.

Suppose τ, ρ exist. Choose prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ in the classes $\tau\langle\sigma\rangle$, $\tau^{-1}\rho\langle\sigma\rangle$, respectively. Then $\mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$ lies in the strong equivalence class 1. So it is a principal ideal (α), where $N\alpha = p_1^2 p_2^2 = N(p_1 p_2)$ and $p_i = N\mathfrak{p}_i$, $i = 1, 2$. By property N, α must be reducible. One of its proper divisors must generate an ideal from the list: $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_1^2, \mathfrak{p}_1 \cdot \mathfrak{p}_2$. But these lie in the classes $\tau\langle\sigma\rangle, \tau^{-1}\rho\langle\sigma\rangle, \tau^2\langle\sigma\rangle, \rho\langle\sigma\rangle$, respectively. By (7), none of these classes is $\langle\sigma\rangle$. So none of the ideals in our list can be principal. This contradiction shows that τ, ρ cannot exist.

Now we can finish the proof. Assume that the 2-Sylow subgroup S of H' is not cyclic. Choose an element $\tau \in S$ of largest possible order such that $\sigma \in \langle\tau\rangle$. Then $\langle\tau\rangle$ is a direct factor of S. Let S' be a complementary subgroup. Since $S' \cap \langle\sigma\rangle = \{1\}$, no element of S' can have order greater than 2 (by (6)). S' must contain some element $\rho \neq 1$, since S is not cyclic. If H' contains an element $\omega \neq 1$ of odd order, then $\pi = \rho \cdot \omega$ satisfies (6), which is impossible. So $H' = S$ is a 2-group. If $\sigma = \tau^{2^m}$, where $m \geqq 2$, then τ, ρ satisfy (7), which is impossible. So $\sigma = \tau^2$ or τ. Therefore

$$H = S/\langle\sigma\rangle \cong S' \times (\langle\tau\rangle/\langle\sigma\rangle) \textit{ has exponent } 2.$$

We conclude that, if K satisfies (1) and property N, then (a) or (c) must hold.

A simple modification of the above argument shows that the irreducible integers α of a quadratic number field K are determined by the absolute values $|N\alpha|$ of their norms if and only if the class group H is of type (a) or (b) in the theorem above.

The problem considered in this paper was raised by Niven and Zuckerman in [2]. A more general form of this problem was treated by other methods in [1].

BIBLIOGRAPHY

1. R. T. Bumby, *Irreducible integers in Galois Extensions*, Pacific J. Math. (to appear).
2. I. Niven and H. S. Zuckerman, *On the lack of unique factorization in quadratic fields*, Oral presentation at American Mathematical Society Symposium on Number Theory, Pasadena, November 1963.

Received August 22, 1966.

RUTGERS, THE STATE UNIVERSITY
CALIFORNIA INSTITUTE OF TECHNOLOGY