

# Pacific Journal of Mathematics

**REMARK ON A PROBLEM OF NIVEN AND ZUCKERMAN**

RICHARD THOMAS BUMBY AND EVERETT C. DADE

## 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  $N: K \rightarrow \mathbb{Q}$  denoting the norm) which satisfy

*Property N:* If  $\alpha$  is an irreducible integer of  $K$  and  $\beta$  is another integer of  $K$  such that  $N\alpha = N\beta$ , then  $\beta$  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  $\varepsilon$  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  $\mathfrak{a}\mathfrak{b}^{-1} = (\gamma)$  is a principal ideal generated by an element  $\gamma$  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  $\sigma$  consisting of all principal ideals  $(\alpha)$  such that one, and hence all, generators of  $(\alpha)$  have negative norm; and the identity class  $1$  of principal ideals  $(\alpha)$  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  $\mathfrak{p}\mathfrak{p}' = (N\mathfrak{p})$ . 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  $\alpha$  and a reducible integer  $\beta$  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  $(\beta)$  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  $\gamma, \delta$  are nonunit integers. Hence we may assume:

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

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  $\varepsilon, \zeta$  in  $K$  such that:

$$(3) \quad (\varepsilon) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}, \quad (\zeta) = \mathfrak{p}_{s+1}^{e_{s+1}} \cdots \mathfrak{p}_t^{e_t}, \quad \text{and } (\gamma), (\delta) \text{ are strongly equivalent to } (\varepsilon), (\zeta), \text{ respectively.}$$

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  $\eta$  is an integer and a proper divisor of  $\alpha$ , 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

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

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  $(\alpha), (\beta)$  are strongly equivalent. Therefore  $\mathfrak{a} \cdot \mathfrak{b}^{-1}$  is strongly equivalent to  $(\alpha) = \mathfrak{a} \cdot \mathfrak{b}$ . So:

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

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

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

In each of the three cases,  $\alpha$  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  $\pi$  satisfying:

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

Suppose such a  $\pi$  exists. By Dirichlet's theorem there exists a prime ideal  $\mathfrak{p}$  in the class  $\pi$  (or, if  $K$  satisfies (1), in the class  $\pi\langle\sigma\rangle$ ). Evidently  $\mathfrak{p}^{2n} = (\alpha)$  is generated by an irreducible element  $\alpha$  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  $\pi$  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  $\tau, \rho$  satisfying:

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

Suppose  $\tau, \rho$  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  $(\alpha)$ , 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  $N$ ,  $\alpha$  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  $\tau, \rho$  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  $\sigma = \tau^{2m}$ , where  $m \geq 2$ , then  $\tau, \rho$  satisfy (7), which is impossible. So  $\sigma = \tau^2$  or  $\tau$ . Therefore

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

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  $\alpha$  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

# PACIFIC JOURNAL OF MATHEMATICS

## EDITORS

H. SAMELSON

Stanford University  
Stanford, California

J. P. JANS

University of Washington  
Seattle, Washington 98105

J. DUGUNDJI

University of Southern California  
Los Angeles, California 90007

RICHARD ARENS

University of California  
Los Angeles, California 90024

## ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSIDA

## SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA  
CALIFORNIA INSTITUTE OF TECHNOLOGY  
UNIVERSITY OF CALIFORNIA  
MONTANA STATE UNIVERSITY  
UNIVERSITY OF NEVADA  
NEW MEXICO STATE UNIVERSITY  
OREGON STATE UNIVERSITY  
UNIVERSITY OF OREGON  
OSAKA UNIVERSITY  
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY  
UNIVERSITY OF TOKYO  
UNIVERSITY OF UTAH  
WASHINGTON STATE UNIVERSITY  
UNIVERSITY OF WASHINGTON  
\* \* \*  
AMERICAN MATHEMATICAL SOCIETY  
CHEVRON RESEARCH CORPORATION  
TRW SYSTEMS  
NAVAL ORDNANCE TEST STATION

Charles A. Akemann, <i>Some mapping properties of the group algebras of a compact group</i> .....	1
A. V. Boyd, <i>Note on a paper by Uppuluri</i> .....	9
Thomas Craig Brown, <i>A semigroup union of disjoint locally finite subsemigroups which is not locally finite</i> .....	11
Richard Thomas Bumby and Everett C. Dade, <i>Remark on a problem of Niven and Zuckerman</i> .....	15
James Calvert, <i>An integral inequality with applications to the Dirichlet problem</i> .....	19
Jack Gary Ceder and Terrance Laverne Pearson, <i>On products of maximally resolvable spaces</i> .....	31
William Guignard Faris, <i>The product formula for semigroups defined by Friedrichs extensions</i> .....	47
Robert S. Freeman, <i>Closed operators and their adjoints associated with elliptic differential operators</i> .....	71
Thomas Lee Hayden, <i>The extension of bilinear functionals</i> .....	99
Gloria Conyers Hewitt, <i>Limits in certain classes of abstract algebras</i> .....	109
Tilla Weinstein, <i>The dilatation of some standard mappings</i> .....	117
Mitsuru Nakai, <i>On Evans' kernel</i> .....	125
Ernest Levane Roetman, <i>On the biharmonic wave equation</i> .....	139
Malcolm Jay Sherman, <i>Operators and inner functions</i> .....	159
Walter Laws Smith, <i>On the weak law of large numbers and the generalized elementary renewal theorem</i> .....	171
A. J. Ward, <i>On H-equivalence of uniformities: The Isbell-Smith problem</i> .....	189