

# Pacific Journal of Mathematics

**IRREDUCIBLE INTEGERS IN GALOIS EXTENSIONS**

RICHARD THOMAS BUMBY

## IRREDUCIBLE INTEGERS IN GALOIS EXTENSIONS

R. T. BUMBY

**We start from the question: When are the irreducible integers of a number field determined by their norms? Attention is centered on the case in which the word "norm" is taken to mean the relative norm of a Galois extension. In this case we are able to show that the ideal class group, as a module over the Galois group, is severely limited by this condition. The restriction of this question to (relatively) quadratic extensions has special properties which are studied in further detail. The homological methods which are in the background of our study become very useful in the study of quadratic extensions.**

As in [1], we say that the extension  $K/k$  satisfies Property  $N$  when: if  $\alpha$  is an irreducible integer of  $K$  and  $\beta$  is another integer of  $K$  such that  $N_{K/k}\alpha = N_{K/k}\beta$ , then  $\beta$  is irreducible.

The norm from  $K$  to  $k$  induces another map, also called  $N_{K/k}$ , from the ideals of  $K$  to the ideals of  $k$ . Ideals can be written uniquely as a product of prime ideals. If  $K/k$  is a Galois extension, the ideals having the same norm as a given prime ideal  $\mathfrak{P}$  are the images  $\mathfrak{P}^\rho$  of  $\mathfrak{P}$  under the action of the various automorphisms  $\rho$  of the Galois group. The norm of  $\mathfrak{P}$  is a power of a prime ideal  $P$  of  $k$ , and any ideal of  $K$  whose norm is divisible by  $P$  must itself be divisible by one of the  $\mathfrak{P}^\rho$ . Thus if  $\mathfrak{A}$  and  $\mathfrak{B}$  are ideals of  $K$  and  $N_{K/k}\mathfrak{A} = N_{K/k}\mathfrak{B}$ , then

$$\begin{aligned}\mathfrak{A} &= \mathfrak{P}_1 \dots \mathfrak{P}_r \\ \mathfrak{B} &= \mathfrak{P}_1^{\rho_1} \dots \mathfrak{P}_r^{\rho_r}.\end{aligned}$$

We shall assume that we are given a fixed Galois extension of number fields  $K/k$  which we wish to test for having Property  $N$ . For this purpose, we assume that we have integers  $\alpha$  and  $\beta$  in  $K$  having the same norm and that  $\beta = \gamma\delta$  with  $\gamma$  and  $\delta$  integers of  $K$ , neither of which is a unit. To prove Property  $N$  we must show that  $\alpha$  is also reducible. From  $N\alpha = N\beta$ , it follows that  $N(\alpha) = N(\beta)$ . Thus we may write

$$\begin{aligned}(\gamma) &= \prod_{\rho \in \mathcal{G}} \mathfrak{A}_\rho \\ (\delta) &= \prod_{\rho \in \mathcal{G}} \mathfrak{B}_\rho \\ (\alpha) &= \prod_{\rho \in \mathcal{G}} (\mathfrak{A}_\rho \mathfrak{B}_\rho)^\rho \\ (\beta) &= \prod_{\rho \in \mathcal{G}} (\mathfrak{A}_\rho \mathfrak{B}_\rho).\end{aligned}$$

Some of the  $\mathfrak{A}_\rho, \mathfrak{B}_\rho$  may be the unit ideal.

If we wish to prove Property  $N$  we must show that this allows us to write  $(\alpha)$  as a product of two principal ideals, neither of which is the unit ideal. The most direct way to do this would be to rearrange the factors  $\mathfrak{A}_\rho$  and  $\mathfrak{B}_\rho$  which are given to us. *There is no other way to prove Property  $N$ .* Each ideal class contains primes; so if we replace  $\mathfrak{A}_\rho$  and  $\mathfrak{B}_\rho$  by prime ideals in the same ideal class (or the unit ideal if we start with a principal  $\mathfrak{A}_\rho$  or  $\mathfrak{B}_\rho$ ), the only factors of the ideal replacing  $(\alpha)$  are products of these ideals. Such a product will be called a *block*.

There is the possibility that  $N(\alpha) = N(\beta)$  while  $N\alpha$  is not equal to the norm of any element of  $(\beta)$ . If  $\alpha$  and  $\beta$  are elements of  $K$ , then  $N(\alpha) = N(\beta)$  if  $N\alpha/N\beta$  is a unit of  $k$ . Only if this ratio is the norm of a unit of  $K$  will  $\alpha$  have the same norm as a generator of  $(\beta)$ . Changing  $\mathfrak{A}_\rho$  to  $t\mathfrak{A}_\rho (t \in K)$  replaces  $\beta$  by  $t\beta$  and  $\alpha$  by  $t^o\alpha$ . Thus  $N\alpha/N\beta$  is multiplied by  $Nt^o/Nt = 1 = N1$ . The only restriction placed on our solution of this problem by working with  $N\alpha$  instead of  $N(\alpha)$  is the limitation of the possible classes of  $\mathfrak{A}_\rho, \mathfrak{B}_\rho$ . Let us formulate the requirement on the ideal class group  $H$  of  $K$ . For convenience  $H$  will be written additively, and the induced action of the Galois group  $G$  will be denoted by left multiplication.

**THEOREM 1.** *The extension  $K/k$  does not have property  $N$  if and only if we can find  $c_\rho, d_\rho \in H$  for all  $\rho \in G$  such that*

(i) *not all  $c_\rho$  are 0*

(ii) *not all  $d_\rho$  are 0*

(iii)  $\sum_\rho c_\rho = 0$

(iv)  $\sum_\rho d_\rho = 0$

(v) *if  $\mathfrak{C}_\rho$  is an ideal in the class  $c_\rho + d_\rho$  for each  $\rho \in G$ , then  $\prod_{\rho \in G} (\mathfrak{C}_\rho / \mathfrak{C}_\rho)$  is a principal fractional ideal having a generator of norm 1.*

(vi) *no "block" of  $\sum_\rho \rho c_\rho + \sum_\rho \rho d_\rho$  has sum 0 unless either it or its complement consists entirely of 0 terms.*

**REMARKS.** The discussion preceding the statement of the theorem amounts to a proof. It should be noted that the condition in (v) was shown to be independent of the representative  $\mathfrak{C}_\rho$  of the ideal class  $c_\rho + d_\rho$ . The somewhat mysterious property (v) has a nice interpretation in terms of homological algebra. (Iwasawa [2] is a helpful reference here.) Let  $E$  denote the group of units in  $K$ ,  $I$  the group of ideals of  $K$ , and  $H$  the ideal class group. The group  $P$  of principal ideals can be thought of either as the kernel of the map  $I \rightarrow H$  or as  $K^*/E$ . This gives two exact sequences

$$\begin{aligned} 0 &\rightarrow E \rightarrow K^* \rightarrow P \rightarrow 0 \\ 0 &\rightarrow P \rightarrow I \rightarrow H \rightarrow 0 \end{aligned}$$

in which the objects are  $G$  modules. By composing connecting homomorphisms of the cohomology sequences of these exact sequences, we get a map  $\eta: H^{-2}(G, H) \rightarrow H^0(G, E)$ . This is the map that we constructed explicitly in the discussion preceding the theorem. In fact, one verifies that the condition that  $N(\alpha) = N(\beta)$  is precisely the condition that  $\langle c_\rho + d_\rho \rangle$  be a  $(-2)$ -cocycle, and (v) states that this cocycle must represent a class in the kernel of  $\eta$ .

2. Basic calculations.

PROPOSITION 1. If  $G$  acts trivially on  $H$  or if  $H = Z_2 \oplus Z_2$ , then property  $N$  holds.

*Proof.* In the first case, the norm completely determines the classes of the ideal factors of a number. Thus the question of reducibility depends only on the norm. In the second case, it is easily verified that there are only three types of irreducible elements (cf. Rogers [3]): (a) primes, (b)  $\mathfrak{P}_1\mathfrak{P}_2$  where  $\mathfrak{P}_1 \sim \mathfrak{P}_2$ , (c)  $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$  where no two of  $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$  are equivalent. If the ideal factors are replaced by conjugates in any way that leaves the product principal, then the product will be of the same type—hence irreducible.

These choices for  $H$  will be called “type  $I$ ”.

On the other hand if we can construct  $c_\rho$  and  $d_\rho$  satisfying (i)–(vi) of the previous section, then we can not have property  $N$ . If  $c_\rho + d_\rho$  has the form given in Table 1, (v) will hold. This is easy to verify by direct calculation; but, of course, Table 1 simply gives the form of the  $(-2)$ -coboundaries.

Table 1.

$\rho \in G$	1	$\sigma$	$\tau$	$\sigma\tau$	other
$[x; \sigma, \tau]_\rho$	$-\tau x$	$\tau x$	$x$	$-x$	0

If it happens that the elements  $1, \sigma, \tau, \sigma\tau$  fail to be distinct, then the appropriate value for  $[x; \sigma, \tau]_\rho$  is the sum of all the quantities associated with the names of  $\rho$ .

Our first goal is to determine which actions of single elements of  $G$  are compatible with Property  $N$ .

PROPOSITION 2. Property  $N$  implies that for all  $\rho \in G$  either  $(1 + \rho + \rho^2)H$  or  $(1 - \rho^2)H$  is zero.

*Proof.* We have the following choices for  $c_\rho, d_\rho$  based on  $c + d = [x; \sigma, \sigma]$ .

Table 2.

$\rho \in G$	1	$\sigma$	$\sigma^2$	Other
$c_\rho$	$x$	0	$-x$	0
$d_\rho$	$-(1 + \sigma)x$	$(1 + \sigma)x$	0	0
$c_\rho + d_\rho$	$-\sigma x$	$(1 + \sigma)x$	$-x$	0

To prove Property *N*, we must show that some proper block of  $[x] + [-(1 + \sigma)x] + [\sigma(1 + \sigma)x] + [-\sigma^2x]$  must have sum zero. It suffices to look at the blocks of length one and those of length two which contain the first term; the other blocks are negatives of these. Thus Property *N* requires that one of the following must be zero:  $x, -(1 + \sigma)x, \sigma(1 + \sigma)x, -\sigma^2x, -\sigma x, (1 + \sigma + \sigma^2)x, (1 - \sigma^2)x$ . But all are nonzero if  $(1 + \sigma + \sigma^2)x$  and  $(1 - \sigma^2)x$  are. Finally, an abelian group cannot be a union of two proper subgroups, so either  $1 - \sigma^2$  or  $1 + \sigma + \sigma^2$  annihilates all of  $H$ .

PROPOSITION 3. Property *N* implies that for all  $\rho \in G$ , either (a)  $(1 + \rho)H = 0$ , or (b)  $(1 - \rho)H = 0$ , or (c)  $\ker(1 + \rho) = \ker(1 - \rho)$  and the order of  $H$  is a power of 2.

*Proof.* We construct somewhat more complicated choices for  $c_\rho$  and  $d_\rho$  given by Table 3. These are also based on  $c + d = [x; \sigma, \sigma]$ .

Table 3.

$\rho \in G$	1	$\sigma$	$\sigma^2$	other
$c_\rho$	$-y$	$y$	0	0
$d_\rho$	$-\sigma x + y$	$(1 + \sigma)x - y$	$-x$	0
$c_\rho + d_\rho$	$-\sigma x$	$(1 + \sigma)x$	$-x$	0

The five nonzero terms of which the blocks will be built are:  $-y, \sigma y, -\sigma x + y, \sigma(1 + \sigma)x - \sigma y, -\sigma^2x$ . To construct a counterexample to Property *N*, we need only verify that no block has sum zero, and we may confine our attention to the blocks of length one (listed above) and all blocks of length two. The blocks of length two are:  $(\sigma - 1)y, -\sigma x, (1 + \sigma)(\sigma x - y), -\sigma^2x - y, -\sigma x + (1 + \sigma)y, \sigma(1 + \sigma)x, -\sigma^2x + \sigma y, \sigma^2x + (1 - \sigma)y, -\sigma(\sigma + 1)x + y, \sigma(x - y)$ . As in the proof of Proposition 2, this list can be shortened. The abridged list is:

$$(\sigma - 1)y, (\sigma + 1)x, (1 + \sigma)(\sigma x - y), \sigma^2x + y, \sigma x - (1 + \sigma)y, \sigma^2x + (1 - \sigma)y, -\sigma(\sigma + 1)x + y, x - y, (1 + \sigma)x - y.$$

If neither  $(1 + \sigma)H$  nor  $(1 - \sigma)H$  is zero, there will certainly be values for  $x$  and  $y$  so that  $(\sigma - 1)y$  and  $(\sigma + 1)x$  are nonzero. We must now look at the other terms of our list to see what might force one of them to be zero.

If it is possible to find  $x$  with  $(1 + \sigma)x \neq 0$  and  $(1 - \sigma)x = 0$ , we can simplify our list further. For if  $(1 - \sigma)y \neq 0$ , we also have  $(1 - \sigma)(y + ux) \neq 0$ , hence  $y + ux \neq 0$  for any  $u$ . Similarly, if we have  $(1 - \sigma)y \neq 0$  and  $(1 + \sigma)y = 0$ , the list is simplified. If we have both, the list completely evaporates.

Thus, if  $\ker(1 + \sigma) \not\subseteq \ker(1 - \sigma)$  and  $\ker(1 - \sigma) \not\subseteq \ker(1 + \sigma)$ , we have a counterexample to Property  $N$ .

If  $\ker(1 + \sigma) \subset \ker(1 - \sigma)$  properly, we want to choose  $x \in \ker(1 - \sigma)$  with  $(1 + \sigma)x \neq 0$ , and  $y \in H$  with  $(1 - \sigma)y \neq 0$ . We must then consider  $(1 + \sigma)(\sigma x - y)$ ,  $\sigma x - (1 + \sigma)y = x - (1 + \sigma)y$ , and

$$\sigma^2 x + (1 - \sigma)y = x + (1 - \sigma)y .$$

If we have  $(1 + \sigma)(\sigma x - y) = 0$ , then we also have

$$0 = (1 - \sigma)(\sigma x - y) = (\sigma - 1)y .$$

But this is assumed nonzero already! Thus, for any  $y \in H$ , not in  $\ker(1 - \sigma)$ , the elements  $(\sigma + 1)y$  and  $(\sigma - 1)y$  must exhaust the elements of  $\ker(1 - \sigma)$  which are not in  $\ker(1 + \sigma)$  whenever we have Property  $N$ . This leaves only the possibilities that  $\ker(1 - \sigma) = Z_3$  and  $\ker(1 + \sigma) = 0$ , or  $\ker(1 - \sigma) = Z_4$  and  $\ker(1 + \sigma) = Z_2$  since the difference between the orders of these groups is at most 2 and all elements of order 2 in the larger are in the smaller (also we are assuming that they are *not* equal). In both of these possibilities, Property  $N$  requires that  $(\sigma + 1)y + (\sigma - 1)y = 0$  and  $y$  not be of order 2. This is impossible.

If  $\ker(1 - \sigma) \subset \ker(1 + \sigma)$  properly, we want to choose  $y \in \ker(1 + \sigma)$  with  $(1 - \sigma)y \neq 0$  and  $x \in H$  with  $(1 + \sigma)x \neq 0$ . As above, we get a counterexample to Property  $N$  in this case if we can choose  $y \neq (1 + \sigma)x, \sigma(1 + \sigma)x$ . Again we find that Property  $N$  can only hold when  $\ker(1 + \sigma) = Z_4$  and  $\ker(1 - \sigma) = Z_2$ , or  $\ker(1 + \sigma) = Z_3$  and  $\ker(1 - \sigma) = 0$ . Also  $(1 + \sigma)H = \ker(1 + \sigma)$ . With the aid of Proposition 2 we discover that this is not consistent with Property  $N$ .

This leaves  $\ker(1 + \sigma) = \ker(1 - \sigma)$ . Every element of this common kernel is of order 2, hence  $(1 + \sigma)$  and  $(1 - \sigma)$  are both isomorphisms on the  $p$ -Sylow components of  $H$  for  $p > 2$ . By Proposition 2 such a subgroup must be annihilated by  $1 + \sigma + \sigma^2$  if we have Property  $N$ . Using the list constructed from Table 3, we find that the group must have order at most 8. This leaves only  $H = Z_7$  with  $\sigma$  being multiplication by 2 or  $-3$ . A closer look shows that  $x = 1$ ,

$y = 5$  gives a counter-example when  $\sigma = 2$ . This concludes the proof of Proposition 3.

**THEOREM 2.** *If  $K/k$  satisfies Property N, and if there is  $\rho \in G$  such that neither  $(1 - \rho)H$  nor  $(1 + \rho)H$  is trivial, and if  $H$  is not  $Z_2 \oplus Z_2$ , then  $H$  must have the form  $Z_2 \oplus \cdots \oplus Z_2$  or*

$$Z_4 \oplus Z_2 \oplus \cdots \oplus Z_2,$$

and the kernels of  $(1 - \rho)$  and  $(1 + \rho)$  for all  $\rho \in G$  have index at most 2 in  $H$ . If  $H$  contains any elements of order 4, then every  $\ker(1 - \rho)$  must contain all elements of order 2.

*Proof.* Proposition 3 tells us that  $H$  must have order  $2^n$  for some  $n$  when the hypotheses of the theorem are met. If we consider the subgroup  $H_1$  of  $H$  consisting of all elements of order 2, Proposition 2 tells us that we must have either  $(1 + \rho + \rho^2)H_1 = 0$  or  $(1 - \rho^2)H_1 = 0$  for all  $\rho \in G$ .

In the first case  $H_1$  must be a direct sum of a number of copies of  $Z_2 \oplus Z_2$  with  $\rho$  acting by permuting the nonzero elements. If there is more than one copy of this module, Table 3 produces a counter-example easily.

If we have  $(1 - \rho^2)H_1 = 0$ , we use Table 3 to search for a counterexample with both  $x$  and  $y$  in  $H_1$  but not in  $(1 + \rho)H_1$ . It is easy to see that we find what we are looking for whenever  $\ker(1 + \rho)$  is of index greater than 2.

Now suppose that there are elements of order 4 in  $H$ . If we assume  $x$  of order 4 and  $y$  of order 2 in Table 3, we find that Property N requires either  $(1 - \sigma)y$ ,  $y - \sigma(1 + \sigma)x$ , or  $y - (1 + \sigma)x$  to be zero. This is inconsistent with the possibility that  $(1 + \sigma + \sigma^2)H = 0$ , so we may assume that  $(1 - \sigma^2)H = 0$ . Thus  $(1 + \sigma)H \subseteq \ker(1 - \sigma) = \ker(1 + \sigma)$ , so Property N implies  $(1 - \sigma)H_1 = 0$ . Since  $(1 - \sigma^2)H = 0$  and  $\ker(1 + \sigma) = \ker(1 - \sigma) = H_1$ ,  $H$  must have exponent 4. If there were two elements of order 4 in  $H$  whose difference was also of order 4, there would be a counterexample to Property N given by Table 3 with these elements in the role of  $x$  and  $y$ . This completes the proof of the theorem.

This theorem allows certain possibilities for  $H$  if we have Property N. These possible choices will be said to be of type II if they are not of type I. All other  $G$  modules will be said to be of type III. Thus if  $H$  is of type (I, II, III) we (always, sometimes, never) have property N.

**FINAL REMARK.** Having the form of  $H$  written out so clearly it

is a simple matter to find all subgroups of the automorphism group of  $H$  composed of elements which all satisfy this theorem. If

$$H \cong Z_2 \oplus Z_2 ,$$

we get the full automorphism group. If  $H \cong Z_4 \oplus Z_2 \oplus \dots \oplus Z_2$ , we get the group of all automorphisms which reduce to the identity on  $H_1$ . If  $H \cong Z_2 \oplus \dots \oplus Z_2$  there are two types: those for which all  $1 + \rho$  have a common kernel, and those for which they have a common image. For all other groups we have  $\{\pm 1\}$ . Except for  $H \cong Z_2 \oplus Z_2$ , the admissible automorphisms form an abelian group of exponent 2. In particular, if  $G$  has no subgroup of index 2, the converse of Proposition 1 holds.

3. Further results. In the last section we found that certain choices for  $H$  as a  $G$  module ensure Property  $N$ , and we also found some severe limitations on  $H$  if we were to have Property  $N$ . The latter conditions were based on a collection of examples which satisfied condition (v) for structural reasons. More complicated examples can be constructed, but further study does not seem practical at this time. We concentrate instead on the case  $G = Z_2$ .

For  $G = Z_2$ , the only coboundaries are of the form  $[x; \rho, \rho]$ , where  $\rho$  is the nontrivial element of  $G$ . We can thus determine easily all counterexamples to Property  $N$  for which  $c + d$  is a coboundary. The result is easily stated.

**THEOREM 3.** *If  $H$  belongs to class II, no coboundary can be the  $(c + d)$  of a counterexample to Property  $N$ , but every nonbounding cocycle does give rise to a counterexample. Thus when  $G = Z_2$ , the map  $H^{-2}(G, H) \rightarrow H^0(G, E)$  must be a monomorphism if we have Property  $N$  and  $H$  of type II.*

*Proof.* The study of Property  $N$  is reduced to looking at

$$\begin{aligned} c_1 &= y & c_\rho &= -y \\ d_1 &= -(z + y) & d_\rho &= (z + y) \end{aligned}$$

where  $\rho z = z$ .  $(c + d)$  is a boundary when  $z \in (1 + \rho)H$ . Property  $N$  is equivalent to one of the following being zero:

$$y, -(z + y), -\rho y, \rho(z + y), -z, (1 - \rho)y, \rho z + (1 + \rho)y .$$

If  $H$  is of class II, this means that either  $(1 - \rho)y = 0$  or  $z \in (1 + \rho)H$ . In class II, we can always find  $y$  with  $(1 - \rho)y \neq 0$  so we have the theorem.

This result can be used to show that when  $G = Z_2$  and  $G$  does



not act trivially on  $H$ , Property  $N$  implies that not too many primes ramify in the extension  $K/k$ . We sketch the proof using the notation of [2]. The mapping  $H^{-2}(G, H) \rightarrow H^0(G, E)$  factors through  $H^{-1}(G, U/E)$ . The map  $\alpha: H^{-2}(G, H) \rightarrow H^{-1}(G, U/E)$  is onto, so both it and the map  $\beta: H^{-1}(G, U/E) \rightarrow H^0(G, E)$  must be monomorphisms for Property  $N$  to hold. But  $\beta$  is a monomorphism if and only if  $\gamma: H^{-1}(G, E) \rightarrow H^{-1}(G, U)$  is onto. The rank of  $H^{-1}(G, U)$  is equal to the number of ramified primes, and the rank of  $H^{-1}(G, E)$  is bounded by the rank of the subgroup of  $E$  consisting of the units of  $K$  whose norm in  $k$  is 1. Thus the rank of  $H^{-1}(G, E)$  can be bounded by a quantity depending only on  $k$ . This bound must then be a bound on the number of ramified primes if we have Property  $N$  and  $G$  does not act trivially on  $H$ .

If  $k = Q$ ,  $(\rho + 1)H = 0$ , so case III never arises. Case I requires  $H$  to be of exponent 2. In studying case II by the method just outlined, we find many pleasant surprises:  $\alpha$  is always an isomorphism, and  $\gamma$  is always a monomorphism. Thus Property  $N$  is equivalent to the number of ramified primes being equal to (it can not be less than) the rank of  $H^{-1}(G, E)$ . This rank is 1 unless  $K$  is a real field all of whose units have norm +1. (cf. [1] condition (1)), in which case it is 2. Thus we have Property  $N$  for  $K = Q(\sqrt{D})$ ,  $k = Q$  in the following cases.

One ramified prime:  $D = -1, \pm 2$ ,  $p, -q$  (where  $p \equiv 1 \pmod{4}$  and  $q \equiv -1 \pmod{4}$  are positive primes).

Two ramified primes:  $D = 2p, pp', q, 2q, qq'$ . Of these, the last three never have units of norm  $-1$ , so they always have Property  $N$ . In the first two cases we find that exactly one of the forms

$$\begin{aligned} pp^*x^2 - y^2 \\ px^2 - p^*y^2 \\ p^*x^2 - py^2 \end{aligned}$$

represents  $+1$  ( $p^*$  stands for 2 or  $p'$ ). If the second or third represents  $+1$  then there is no unit of norm  $-1$  and we have Property  $N$ . If the first represents  $+1$  then we can have Property  $N$  only if  $H$  is of exponent 2. If  $(p^*/p) = -1$ , then only the first form can represent  $+1$ . But in this case the 2-Sylow subgroup has exponent 2. Thus we have Property  $N$  only if there are no elements of odd order in  $H$ . If  $(p^*/p) = +1$ ,  $H$  must be of type II, so Property  $N$  depends only on which of the three forms represents  $+1$ .

Thus we have a somewhat different version of the results obtained in [1].

## BIBLIOGRAPHY

1. R. T. Bumby and E. C. Dade, *Remark on a problem of Niven and Zuckerman*
2. K. Iwasawa, *A note on the group of units of an algebraic number field*, Journ. Math. pures et appl. (9) **35** (1956), 189-192.
3. K. Rogers, *A combinatorial problem in abelian groups*, Proc. Camb. Phil. Soc. (3) **59** (1963), 559-562.

Received August 22, 1966. This work was begun while the author was supported by a grant from the Rutgers Research Council and completed with the help of National Science Foundation grant GP-4368.



# 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

---

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced). The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, Richard Arens at the University of California, Los Angeles, California 90024.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

---

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is \$8.00; single issues, \$3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$4.00 per volume; single issues \$1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 7-17, Fujimi 2-chome, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

# Pacific Journal of Mathematics

Vol. 22, No. 2

February, 1967

Paul Frank Baum, <i>Local isomorphism of compact connected Lie groups</i> . . . .	197
Lowell Wayne Beineke, Frank Harary and Michael David Plummer, <i>On the critical lines of a graph</i> . . . . .	205
Larry Eugene Bobisud, <i>On the behavior of the solution of the telegraphist's equation for large velocities</i> . . . . .	213
Richard Thomas Bumby, <i>Irreducible integers in Galois extensions</i> . . . . .	221
Chong-Yun Chao, <i>A nonimbedding theorem of nilpotent Lie algebras</i> . . . . .	231
Peter Crawley, <i>Abelian <math>p</math>-groups determined by their Ulm sequences</i> . . . . .	235
Bernard Russel Gelbaum, <i>Tensor products of group algebras</i> . . . . .	241
Newton Seymour Hawley, <i>Weierstrass points of plane domains</i> . . . . .	251
Paul Daniel Hill, <i>On quasi-isomorphic invariants of primary groups</i> . . . . .	257
Melvyn Klein, <i>Estimates for the transfinite diameter with applications to conformal mapping</i> . . . . .	267
Frederick M. Lister, <i>Simplifying intersections of disks in Bing's side approximation theorem</i> . . . . .	281
Charles Wisson McArthur, <i>On a theorem of Orlicz and Pettis</i> . . . . .	297
Harry Wright McLaughlin and Frederic Thomas Metcalf, <i>An inequality for generalized means</i> . . . . .	303
Daniel Russell McMillan, Jr., <i>Some topological properties of piercing points</i> . . . . .	313
Peter Don Morris and Daniel Eliot Wulbert, <i>Functional representation of topological algebras</i> . . . . .	323
Roger Wolcott Richardson, Jr., <i>On the rigidity of semi-direct products of Lie algebras</i> . . . . .	339
Jack Segal and Edward Sandusky Thomas, Jr., <i>Isomorphic cone-complexes</i> . . . . .	345
Richard R. Tucker, <i>The <math>\delta^2</math>-process and related topics</i> . . . . .	349
David Vere-Jones, <i>Ergodic properties of nonnegative matrices. I</i> . . . . .	361