COLLOQUIUM MATHEMATICUM

VOL. LIV 1987 FASC. 2

# CHARACTERIZATION OF IRREDUCIBLE ALGEBRAIC INTEGERS BY THEIR NORMS

BY

G. LETTL (GRAZ)

**1. Preliminaries and main result.** Let $K$ be an algebraic number field and $L$ a finite extension of it. We shall denote by $\mathcal{O}_K$ the ring of integers of $K$, $E_K$ the group of units (i.e., invertible elements of $\mathcal{O}_K$), $\mathcal{C}_K$ the ideal class group of $K$, written additively, and $h_K$ its order.

It is well known that $h_K$ is finite and that $h_K$ is in a certain sense a measure indicating how far $\mathcal{O}_K$ is remote from being a unique factorization domain. $\mathcal{O}_K$ is a unique factorization domain iff $h_K = 1$ and $\mathcal{O}_K$ is a half-factorial domain iff $h_K \leqslant 2$ (see [3]).

Two integers $\alpha, \beta \in \mathcal{O}_K \backslash \{0\}$ are called *associated* ($\alpha \sim \beta$) if $\alpha\beta^{-1} \in E_K$. An integer $\alpha \in \mathcal{O}_K \backslash (E_K \cup \{0\})$ is called *irreducible* if the only integers dividing $\alpha$ are units or integers associated with $\alpha$. If $L/K$ is normal, denote its Galois group by $G$ and the relative norm for $L/K$ of $\alpha \in L$ by $N\alpha \in K$.

DEFINITION 1. The extension $L/K$ has *property* (N*) if the following holds:

For any $\alpha, \beta \in \mathcal{O}_L$ with $N\alpha \sim N\beta$ in $K$, $\alpha$ and $\beta$ are either both irreducible or both not.

If $L/K$ is normal and $h_L = 1$, it is easy to check that (N*) holds. If $L/K$ is not normal, property (N*) does not hold. We will characterize all finite normal extensions of algebraic number fields with property (N*). It will be shown that for an extension $L/K$ property (N*) depends only on the $G$-module structure of the ideal class group $\mathcal{C}_L$. For $n \in N$ set $C_n = Z/nZ$, the cyclic group of order $n$.

The main result is given by

THEOREM 1. *A normal extension $L/K$ with Galois group $G$ has property* (N*) *iff one of the following conditions holds*:

(a) $\mathcal{C}_L \simeq C_2 \oplus C_2$;

(b) *$G$ acts trivially on $\mathcal{C}_L$*;

(c) *$h_L$ is odd and there exists an algebraic number field $L_0$ with*

$$K \subsetneqq L_0 \subsetneqq L \quad \textit{and} \quad [L_0 \colon K] = 2$$

*such that the Galois group* $G_0$ *of* $L/L_0$ *acts trivially on* $\mathscr{C}_L$ *and any* $\sigma \in G \backslash G_0$ *acts on* $\mathscr{C}_L$ *via* $\sigma a = -a$.

From Theorem 1 we immediately obtain

COROLLARY 1. *If* $L/K$ *is normal and* $([L: K], 6) = 1$, *then* $L/K$ *has property* (N*) *iff* $G$ *acts trivially on* $\mathscr{C}_L$.

If $K = Q$ and $L$ is a quadratic number field, (a) in Theorem 1 implies (b), (b) reduces to

$$\mathscr{C}_L \simeq \bigoplus_{i=1}^{k} C_2 \quad \text{with } k \in N,$$

and (c) reduces to "$h_L$ is odd", so we obtain the result mentioned in [2], pp. 17–18.

Bumby and Dade [2] and Bumby [1] considered a similar problem asking when $L/K$ has *property* (N), which means: if $\alpha$ and $\beta$ are integers of $L$ with the same relative norms, then either both are irreducible or both are not. All quadratic number fields with property (N) are characterized in [2], whereas in [1] necessary conditions are given under which property (N) holds for general $L/K$. Of course, property (N*) implies (N).

In the next section we will show how property (N*) depends on the $G$-module structure of $\mathscr{C}_L$.

**2. Translation into a problem of $G$-modules.** Let $G$ be a multiplicative group and $A$ a $G$-module. A non-empty finite family $(a_i)_{i \in I}$ in $A$ is called a *block* if

$$\sum_{i \in I} a_i = 0.$$

A block is called *irreducible* if none of its proper subfamilies is a block.

DEFINITION 2. Let $G$ be a multiplicative group and $A$ a $G$-module. We say that $(G, A)$ has *property* (N*) if for every irreducible block $(a_i)_{i \in I}$ in $A$ and every family $(\sigma_i)_{i \in I}$ in $G$ the following holds: if $(\sigma_i a_i)_{i \in I}$ is a block, then it is irreducible.

The usefulness of Definition 2 will become clear by the next proposition.

PROPOSITION 1. *If* $L/K$ *is normal with Galois group* $G$, *then it has property* (N*) *iff* $(G, \mathscr{C}_L)$ *has property* (N*).

The main idea leading to the translation of factorization problems into $\mathscr{C}_L$ is the following: For $\alpha \in \mathcal{O}_L$ let

$$\alpha \cdot \mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{p}_i$$

be the unique factorization of the principal ideal $\alpha \cdot \mathcal{O}_L$ into prime ideals. Denote the ideal class containing $\mathfrak{p}_i$ by $[\mathfrak{p}_i]$. Then $\alpha$ is an irreducible integer iff the block

$$([\mathfrak{p}_1], [\mathfrak{p}_2], \ldots, [\mathfrak{p}_r])$$

is irreducible.

Proof of Proposition 1. Assume that $(G, \mathscr{C}_L)$ has property (N*). Let $\alpha \in \mathcal{O}_L$ be irreducible and

$$\alpha \cdot \mathcal{O}_L = \prod_{i \in I} \mathfrak{p}_i$$

be the factorization into prime ideals; then $([\mathfrak{p}_i])_{i \in I}$ is an irreducible block in $\mathscr{C}_L$. If $\beta \in \mathcal{O}_L$ with $N\alpha \sim N\beta$, then the prime ideal decomposition of $\beta \cdot \mathcal{O}_L$ is of the form

$$\beta \cdot \mathcal{O}_L = \prod_{i \in I} \mathfrak{p}_i^{\sigma_i} \quad \text{with } \sigma_i \in G.$$

Property (N*) of $(G, \mathscr{C}_L)$ ensures that the block $(\sigma_i [\mathfrak{p}_i])_{i \in I}$ is irreducible, thus $\beta$ is irreducible as well.

Now assume that $L/K$ has property (N*). Let $(a_i)_{i \in I}$ be an irreducible block in $\mathscr{C}_L$ and $\sigma_i \in G$ be such that $(\sigma_i a_i)_{i \in I}$ is a block. For each $i \in I$ choose a prime ideal $\mathfrak{p}_i \in a_i$. The ideal $\prod_{i \in I} \mathfrak{p}_i$ is a principal ideal generated by an irreducible element $\alpha \in \mathcal{O}_L$. The ideal $\prod_{i \in I} \mathfrak{p}_i^{\sigma_i}$ is also a principal ideal generated by some $\beta \in \mathcal{O}_L$ with $N\alpha \sim N\beta$. So $\beta$ is irreducible, and therefore the block $(\sigma_i a_i)_{i \in I}$ is also irreducible, which proves (N*) for $(G, \mathscr{C}_L)$.

One can generalize Proposition 1 by taking $L$ the quotient field of an arbitrary Dedekind ring, but note that for the second part of the proof we need each ideal class of $L$ to contain at least one prime ideal. Proposition 1 shows the way to prove Theorem 1. We will characterize all pairs $(G, A)$ of multiplicative groups $G$ and $G$-modules $A$ having property (N*), and then transfer into algebraic number theory. For technical reasons we need another characterization of property (N*) (see [1]):

PROPOSITION 2. *Let $G$ be a group and $A$ a $G$-module. Then $(G, A)$ has property* (N*) *iff the following holds:*

*For each pair of mappings $c\colon G \to A$ and $d\colon G \to A$ with*

$$\{\sigma \in G \mid c(\sigma) \neq 0 \text{ or } d(\sigma) \neq 0\} \text{ finite}$$

*and*

$$(*) \qquad c \neq 0, \quad d \neq 0, \quad \sum_{\sigma \in G} c(\sigma) = \sum_{\sigma \in G} d(\sigma) = \sum_{\sigma \in G} \sigma\big(c(\sigma) + d(\sigma)\big) = 0,$$

*the block* $(\sigma c(\sigma), \varrho d(\varrho))$ $(\sigma, \varrho \in G, c(\sigma) \neq 0, d(\varrho) \neq 0)$ *is reducible.*

Proof of Proposition 2. Assume that $(G, A)$ has property $(N^*)$ and let $c$, $d$ be mappings satisfying $(*)$. The block $(c(\sigma), d(\varrho))$ $(\sigma, \varrho \in G, c(\sigma) \neq 0, d(\varrho) \neq 0)$ is a reducible block in $A$ with the proper subblock $(c(\sigma))$ $(\sigma \in G, c(\sigma) \neq 0)$. Thus $(*)$ implies that $(\sigma c(\sigma), \varrho d(\varrho))$ $(\sigma, \varrho \in G, c(\sigma) \neq 0, d(\varrho) \neq 0)$ is a block, which is reducible, since $(N^*)$ holds.

Now assume that $(G, A)$ does not have property $(N^*)$. Then there exist an irreducible block $(a_i)_{i \in I}$ and a family $(\sigma_i)_{i \in I}$ so that $(\sigma_i a_i)_{i \in I}$ is a reducible block. Let $I = I_1 \dot{\cup} I_2$ be a nontrivial partition such that $(\sigma_i a_i)_{i \in I_1}$ and $(\sigma_i a_i)_{i \in I_2}$ are blocks. Define the mappings $c, d$: $G \to A$ by

$$c(\sigma) = \sum_{\substack{i \in I_1 \\ \sigma_i = \sigma^{-1}}} \sigma_i a_i \quad \text{and} \quad d(\sigma) = \sum_{\substack{i \in I_2 \\ \sigma_i = \sigma^{-1}}} \sigma_i a_i \quad \text{for all } \sigma \in G,$$

where empty sums are equal to $0 \in A$. Then $c$, $d$ satisfy $(*)$, but $(\sigma c(\sigma), \varrho d(\varrho))$ $(\sigma, \varrho \in G, c(\sigma) \neq 0, d(\varrho) \neq 0)$ is irreducible, which completes the proof of Proposition 2.

For a $G$-module $A$ set

$$G_0 = \{\sigma \in G \mid \sigma a = a \text{ for all } a \in A\}.$$

$G_0$ is a normal subgroup of $G$ and $A$ is a faithful $(G/G_0)$-module. It is easy to check that $(G, A)$ has property $(N^*)$ iff $(G/G_0, A)$ has property $(N^*)$. Therefore, we can confine ourselves to faithful $G$-modules $A$, and hence assume $G$ to be contained in $\mathrm{End}(A)$, the ring of endomorphisms of $A$. Denote by $1 \in G$ the identity, by $-1$ the automorphism mapping each $a \in A$ onto $-a$, and by $0$ the endomorphism mapping each $a \in A$ onto 0.

THEOREM 2. *Let G be a group and A a faithful G-module. Then* $(G, A)$ *has property* $(N^*)$ *exactly in the following cases*:

(a) $A \cong C_2 \oplus C_2$ *and* $G \leqslant \mathrm{Aut}(A) \cong S_3$ ($S_3$ *denotes the symmetric group on* 3 *elements*);

(b) $G = \{1\}$;

(c) $G = \{1, -1\}$, *and A contains no element of order* 2.

By Proposition 1 and the above remarks, Theorem 1 is obtained from Theorem 2 if one factorizes the Galois group $G$ of an extension $L/K$ by its normal subgroup $G_0$ consisting of all automorphisms acting trivially on $\mathscr{C}_L$, which gives $\mathscr{C}_L$ the structure of a faithful $(G/G_0)$-module.

**3. Proof of Theorem 2.** The proof is made up of several lemmas.

LEMMA 1. *Let* $G = \{1, -1\}$ *and* $A$ *be a faithful* $G$*-module. Then* $(G, A)$ *has property* (N*) *iff* $A$ *contains no element of order* 2.

Proof. Let $G = \{1, -1\}$ and $A$ be a faithful $G$-module. We use Proposition 2 to check property (N*) for $(G, A)$. Two mappings $c, d\colon G \to A$ satisfying (*) of Proposition 2 can only have the form

| $\sigma$ | $c(\sigma)$ | $d(\sigma)$ |
|---|---|---|
| $1$ | $x$ | $y$ |
| $-1$ | $-x$ | $-y$ |

with $x, y \in A \setminus \{0\}$ and

$$\sum_{\sigma \in G} \sigma\big(c(\sigma) + d(\sigma)\big) = 2(x+y) = 0.$$

So $(G, A)$ has property (N*) iff, for all $x, y \in A \setminus \{0\}$, $2(x+y) = 0$ implies that $(x, x, y, y)$ is a reducible block in $A$.

Suppose $A$ has no element of order 2. Then $2(x+y) = 0$ implies $y = -x$ and $(x, x, -x, -x)$ is reducible, showing that $(G, A)$ has property (N*).

Suppose there exists $z \in A$ with order 2. Since $A$ is a faithful $\{1, -1\}$-module, the exponent of $A$ is greater than 2. So there exists $x \in A \setminus \{0, z\}$ of order greater than 2. Put $y = z - x$; then $2(x+y) = 2z = 0$, but the block $(x, x, z-x, z-x)$ is irreducible. Thus $(G, A)$ does not have property (N*) and Lemma 1 is proved.

LEMMA 2 (see [1], Proposition 2). *Let* $A$ *be a faithful* $G$*-module and suppose* $(G, A)$ *has property* (N*). *Then for* $\varrho \in G$ *either* $\varrho^2 - 1 = 0$ *or* $\varrho^2 + \varrho + 1 = 0$.

Proof. Assume $\varrho \in G$ with $\varrho^2 \neq 1$. Consider $x \in A$ with $\varrho^2 x \neq x$ and define $c, d\colon G \to A$ by

| $\sigma$ | $c(\sigma)$ | $d(\sigma)$ |
|---|---|---|
| $1$ | $x$ | $-x-\varrho x$ |
| $\varrho$ | $0$ | $x+\varrho x$ |
| $\varrho^2$ | $-x$ | $0$ |

(All elements of $G$ not listed in the table are mapped onto 0.)

$c$ and $d$ satisfy (*) of Proposition 2 and $(G, A)$ has property (N*), so the block

$$(x,\ -\varrho^2 x,\ -x-\varrho x,\ \varrho x+\varrho^2 x)$$

must be reducible. As $x$, $\varrho x$, $\varrho^2 x$, $\varrho x+x$, $\varrho^2 x-x$ are not 0, necessarily $\varrho^2 x+\varrho x+x=0$. This gives

$$A=\ker(1-\varrho^2)\cup\ker(1+\varrho+\varrho^2),$$

but $A$ cannot be the union of two proper subgroups, so

$$A=\ker(1+\varrho+\varrho^2),$$

and Lemma 2 is proved.

LEMMA 3. *Let $G$ be a group and $A\simeq C_2\oplus C_2$ be a faithful $G$-module. Then $(G, A)$ has property* ($N^*$).

Proof. If $G=\{1\}$, the lemma is obvious, so assume that $G\neq\{1\}$. We will use Proposition 2 again. If $c, d\colon G\to A$ satisfy (∗), the block $(\sigma c(\sigma), \varrho d(\varrho))$ ($\sigma, \varrho\in G$, $c(\sigma)\neq 0$, $d(\varrho)\neq 0$) has at least 4 elements. Davenport's constant for $C_2\oplus C_2$ is 3, so this block is always reducible. (For the definition of Davenport's constant and its computation in some special cases see [4] and [5].)

LEMMA 4. *Let $A$ be a faithful $G$-module and $(G, A)$ have property* ($N^*$). *If there exists $\varrho\in G\setminus\{1\}$ with $\varrho^2+\varrho+1=0$, then*

$$A\cong C_2\oplus C_2.$$

Proof. Let $\varrho\in G\setminus\{1\}$ with $\varrho^2+\varrho+1=0$, which implies $\varrho^3=1$. Consider $x\in A\setminus\ker(1-\varrho)$ and define $c, d\colon G\to A$ by

| $\sigma$ | $c(\sigma)$ | $d(\sigma)$ |
|---|---|---|
| $1$ | $x$ | $-x+\varrho x$ |
| $\varrho$ | $\varrho^2 x$ | $0$ |
| $\varrho^2$ | $\varrho x$ | $x-\varrho x$ |

(All elements of $G$ not listed in the table are mapped onto 0.)

$c$ and $d$ satisfy (∗), so by Proposition 2 the block

$$(x, x, x, -x+\varrho x, \varrho^2 x-x)$$

must be reducible, which can only hold if $2x=0$ or $3x=0$. If $y\in\ker(1-\varrho)$, then

$$(\varrho^2+\varrho+1)y=3y=0.$$

Combining these results, we see that the exponent of $A$ is 2 or 3.

Assume that the exponent of $A$ is 3. Choose $x\in A\setminus\ker(1-\varrho)$ and define $c, d\colon G\to A$ by

| $\sigma$ | $c(\sigma)$ | $d(\sigma)$ |
|---|---|---|
| $1$ | $2x$ | $0$ |
| $\varrho$ | $x$ | $x$ |
| $\varrho^2$ | $0$ | $2x$ |

(All elements of $G$ not listed in the table are mapped onto 0.)

$c$ and $d$ satisfy (*), but the block $(2x, \varrho x, \varrho x, 2\varrho^2 x)$ turns out to be irreducible, contradicting property (N*). Therefore, the exponent of $A$ must be 2. We have $\ker(1-\varrho) = \{0\}$, because the order of every element of $\ker(1-\varrho)$ divides 3. If $x \in A \setminus \{0\}$, then $x, \varrho x, \varrho^2 x = x + \varrho x$ are different elements of $A$ and $A_x = \{0, x, \varrho x, \varrho^2 x\}$ is a subgroup of $A$, invariant under the action of $\varrho$. If there exists $y \in A \setminus A_x$, we define $c, d\colon G \to A$ by

| $\sigma$ | $c(\sigma)$ | $d(\sigma)$ |
|---|---|---|
| $1$ | $x$ | $x+\varrho y$ |
| $\varrho$ | $x$ | $x+\varrho^2 y$ |
| $\varrho^2$ | $0$ | $y$ |

(All elements of $G$ not listed in the table are mapped onto 0.)

$c$ and $d$ satisfy (*), but the block

$$(x, \varrho x, x+\varrho y, \varrho x + y, \varrho^2 y)$$

is irreducible, which contradicts property (N*). Therefore,

$$A = A_x \cong C_2 \oplus C_2.$$

Lemma 3 shows that property (N*) holds in this case, which completes the proof of Lemma 4.

LEMMA 5. *Let $G \neq \{1\}$, $G \neq \{1, -1\}$, $A$ be a faithful $G$-module and $(G, A)$ have property* (N*). *If $\varrho^2 - 1 = 0$ holds for all $\varrho \in G$, then $A \cong C_2 \oplus C_2$.*

Proof. Let $\varrho \in G$, $\varrho \neq \pm 1$. If $\ker(1-\varrho) = \{0\}$, then for all $x \in A$ we have

$$(1-\varrho)(1+\varrho)x = 0 \quad \text{and} \quad (1+\varrho)x \in \ker(1-\varrho) = \{0\}.$$

Then $\varrho = -1$, contrary to our choice of $\varrho$. Thus there exists $y \in \ker(1-\varrho) \setminus \{0\}$. For $x \in A \setminus \ker(1-\varrho)$ define two mappings $c, d\colon G \to A$ by

| $\sigma$ | $c(\sigma)$ | $d(\sigma)$ |
|---|---|---|
| $1$ | $x$ | $-x+y$ |
| $\varrho$ | $-x$ | $x-y$ |

(All elements of $G$ not listed in the table are mapped onto 0.)

$c$ and $d$ satisfy $(*)$, so by Proposition 2 the block

$$(x,\ -\varrho x,\ -x+y,\ \varrho x-\varrho y)$$

must be reducible. This can only occur if $\varrho x = -x+y$ holds. It follows easily that $\ker(1-\varrho) = \{0, y\}$, the order of $y$ is 2, and $\varrho x = -x+y$ for all $x \in A\setminus\ker(1-\varrho)$. If there exists an $\bar{x} \in A\setminus\ker(1-\varrho)$ with $\bar{x} \neq x$, then

$$\varrho(x+\bar{x}) = -(x+\bar{x}) \neq -(x+\bar{x})+y,$$

so $x+\bar{x}$ must be contained in $\ker(1-\varrho)$ and $A$ has at most 5 elements. Since $y \in A$ has order 2 and the only automorphisms of $C_4$ are $1$ and $-1$, only $A \cong C_2 \oplus C_2$ remains possible. Lemma 3 assures that (N*) holds in this case, and Lemma 4 is proved.

Proof of Theorem 2. Assume that $A$ is a faithful $G$-module and that $(G, A)$ has property (N*). If $G = \{1\}$, then $(G, A)$ has property (N*) for arbitrary $A$, which gives part (b) of Theorem 2. If $G = \{1, -1\}$, part (c) of Theorem 2 results from Lemma 1. If $G \neq \{1\}$ and $G \neq \{1, -1\}$, then Lemmas 2, 4 and 5 imply part (a) of Theorem 2.

I would like to thank Professor F. Halter-Koch for many discussions and advice during the preparation of the manuscript.

*REFERENCES*

[1] R. T. Bumby, *Irreducible integers in Galois extensions*, Pacific J. Math. 22 (1967), pp. 221–229.

[2] – and E. C. Dade, *Remark on a problem of Niven and Zuckerman*, ibidem 22 (1967), pp. 15–18.

[3] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11 (1960), pp. 391–392.

[4] P. van Emde Boas, *A combinatorial problem on finite Abelian groups. II*, Reports of the Mathematisch Centrum Amsterdam, ZW–1969–007.

[5] W. Narkiewicz, *Finite Abelian groups and factorization problems*, Colloq. Math. 42 (1979), pp. 319–330.

INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
HALBÄRTHGASSE 1
A-8010 GRAZ

*Reçu par la Rédaction le 30. 5. 1983*