ACTA ARITHMETICA
LXIX.1 (1995)

Normal integral bases and the Spiegelungssatz of Scholz

by

Jan Brinkhuis (Rotterdam)

Introduction. In Hilbert's Zahlbericht one can find the first global result on the Galois module structure of rings of integers ([H], Satz 132). Slightly extended it states that if $N/\mathbb{Q}$ is a tame extension with abelian Galois group $\varDelta$, then $\mathfrak{o}_N$, the ring of integers in N, is free as a module over the group ring $\mathbb{Z}\varDelta$; moreover, an explicit canonical algebraic integer a such that $\mathfrak{o}_N = \mathbb{Z}\varDelta a$ can be given. The numbers a^δ ($\delta \in \varDelta$), the algebraic conjugates of a, are said to form a normal integral basis of the field extension $N/\mathbb{Q}$.

This result has been the starting point for a modern development, which has led to the deep result that the structure of $\mathfrak{o}_N$ as a module over $\mathbb{Z}\varDelta$, for arbitrary tame Galois extensions of number fields N/K with Galois group $\varDelta$, is determined in terms of the symplectic root numbers of N/K (see [F] and [T1]). Fröhlich's book [F] also contains a detailed introduction and a rather complete list of references. For a more recent survey on Galois module theory we refer to [Ca–Ch–F–T].

In the special case that $\varDelta$ is of odd order the result mentioned above gives that $\mathfrak{o}_N$ is a free $\mathbb{Z}\varDelta$-module, but the proof does not provide an explicit basis. If one considers the richer $\mathfrak{o}_K\varDelta$-module structure of $\mathfrak{o}_N$ rather than the $\mathbb{Z}\varDelta$-module structure alone, then $\mathfrak{o}_N$ is expected to be "usually" not even free if $K \neq \mathbb{Q}$. Results of Taylor show that by modifying both $\mathfrak{o}_N$ and $\mathfrak{o}_K\varDelta$ one can sometimes—if K and N are certain ray class fields over imaginary quadratic number fields—achieve the "ideal" of free modules with explicit generators (see [C–T]). However, if one decides not to modify the original classical problem of the determination of the $\mathfrak{o}_K\varDelta$-module structure of $\mathfrak{o}_N$, then a natural question is to what extent, for given K and $\varDelta$, the realization of $\varDelta$ as a Galois group of a tame extension N/K is determined by the ramification of N/K together with the structure of $\mathfrak{o}_N$ as an $\mathfrak{o}_K\varDelta$-module. This point of view is worked out in [B2]. In a sense the core of the question is how rare unramified extensions which possess a normal integral basis are. We mention in passing that this question is equivalent to a special case of a problem considered by Taylor in recent work, that of determining the kernel of the homomorphism ψ (see [T4]). In [B3] it is shown that such extensions cannot exist if K is totally real and $\varDelta$ is abelian of odd degree. It seemed worthwhile, also in view of the current interest in the theme of the Galois module structure of abelian extensions of imaginary quadratic number fields (see for example [T2]), to consider the following further example: K is an imaginary quadratic number field and $\varDelta$ is cyclic of order 3. Our result is that one gets at most one such an extension for each K. We recall here that it is generally believed that the number of all unramified cubic cyclic extensions of an imaginary quadratic field can be arbitrarily large. Our result is essentially a reformulation of the classical Spiegelungssatz of Scholz which is concerned with a relation between the ideal class groups of $\mathbb{Q}\sqrt{-d}$ and $\mathbb{Q}\sqrt{3d}$ ([S]). In fact, there exists a quite general connection between reflection theorems and Galois module structure, but the present special case could be dealt with so directly that it seemed appropriate to give a separate account of it, before dealing with the general situation. Before stating our result precisely, we finally remark that only very few explicit examples of normal integral bases are known.

THEOREM. (i) *A given imaginary quadratic number field has at most one unramified cubic cyclic extension with a normal integral basis.*

(ii) *Let m be a rational integer which cannot be written in the form n^3-n^2 for any rational integer n. Then the splitting field N of the polynomial $f(X) = X^3-X^2-m$ is an unramified cubic cyclic extension of the imaginary quadratic number field $K = \mathbb{Q}\sqrt{-27m^2-4m}$ and the roots of $f(X)$ form a normal integral basis of the extension N/K; this basis is moreover selfdual with respect to the trace form.*

(iii) *There are no examples of unramified cubic cyclic extensions of imaginary quadratic number fields with a normal integral basis other than those given in* (ii).

(iv) *A given imaginary quadratic number field $K = \mathbb{Q}\sqrt{-d}$ has an unramified cubic cyclic extension with a normal integral basis if and only if in the real quadratic number field $\mathbb{Q}\sqrt{3d}$ there is an algebraic unit which is $\equiv 1 \bmod 3\sqrt{3}$ and which is not a third power.*

This work was begun in May 1988 while the author enjoyed the hospitality of the University of Bordeaux I.

1. Notation and auxiliary results. Let N/K be a Galois extension of algebraic number fields with Galois group $\varDelta$. A basis of $\mathfrak{o}_N$, the ring of algebraic integers in N, as a module over $\mathfrak{o}_K$, the ring of algebraic integers in K, which consists of the algebraic conjugates over K of one algebraic integer a, is called a *normal integral basis*; then a is called a *normal integral generator*. Let the group $\varDelta$ act on the group ring $N\varDelta$ by the Galois action on the coefficient ring N. For each $n \in N$ let the *Lagrange resolvent* of n be the element of $N\varDelta$ defined by

$$R(n) = \sum_{\delta} n^{\delta}\delta^{-1},$$

where δ runs over $\varDelta$. It satisfies the relation $R(n)^{\delta} = R(n) \cdot \delta$ for all $\delta \in \varDelta$. The extension N/K will be called *unramified* if it is unramified at all finite primes of K.

(1.1) Proposition. (i) *If N/K is unramified and if moreover it has a normal integral generator a, then $R(a) \in \mathfrak{o}_N\varDelta^{\times}$, the group of units of $\mathfrak{o}_N\varDelta$.*

(ii) *If there is an element $u \in \mathfrak{o}_N\varDelta^{\times}$ with $u^{\delta} = u \cdot \delta$ for all $\delta \in \varDelta$, then N/K is unramified, $u = R(a)$ for some $a \in \mathfrak{o}_N$ and this number a is a normal integral generator of N/K.*

Proof. See [B1]. ■

The trivial homomorphism $\varDelta \to 1$ induces a morphism of rings $N\varDelta \to N$ which is called *augmentation* and which is denoted by aug. Let $\mathrm{Tr}_{N/K}$ be the trace map from N to K. For each $n \in N$, one has, by the definitions, the following identity:

$$\operatorname{aug} R(n) = \mathrm{Tr}_{N/K}\, n. \tag{1.2}$$

Let $\widehat{\ }$ denote the standard involution on $N\varDelta$ given by inversion on $\varDelta$.

(1.3) Corollary of Proposition (1.1). *The following conditions on an algebraic integer a in N are equivalent and imply that N/K is unramified and that a is a normal generator of N/K.*

(i) *For all* $\gamma, \delta \in \varDelta$,

$$\mathrm{Tr}_{N/K}(a^{\gamma}a^{\delta}) = \begin{cases} 1 & \text{if } \gamma = \delta, \\ 0 & \text{otherwise}. \end{cases}$$

(ii) $R(a)\widehat{R}(a) = 1$.

An algebraic integer in N which satisfies the conditions of Corollary (1.3) is called a *selfdual normal integral generator* (*with respect to the trace form*) and the basis it generates a *selfdual normal integral basis* (*with respect to the trace form*).

In the rest of this section we assume that the extension $N/\mathbb{Q}$ is Galois and $K/\mathbb{Q}$ is abelian. We choose an embedding $i : N \hookrightarrow \mathbb{C}$; then complex conjugation on $\mathbb{C}$ restricts to an automorphism of N which we denote in the usual way by writing $\overline{x}$ for the image of $x \in N$ under the automorphism. This automorphism of N depends in general on the chosen embedding i, but its restriction to K is independent of the choice of i. One defines an involution on $N\varDelta$, which in a sense "plays the role of complex conjugation", by the formula

$$(1.4)\qquad \overline{\sum_\delta a_\delta \delta} = \sum_\delta \overline{a_\delta}\delta^{-1},$$

where δ runs over Δ; that is, one acts on N by $\overline{}$ and simultaneously on Δ by inversion. For each abelian group A let $\mathrm{tor}(A)$ be its torsion subgroup. Let μ be the group of roots of unity in $\mathbb{Q}^{\mathrm{c}}$, an algebraic closure of $\mathbb{Q}$. Let $\mathbb{Z}^{\mathrm{c}}$ be the ring of algebraic integers in $\mathbb{Q}^{\mathrm{c}}$. We will need the following facts.

(1.5) Lemma. (i) *If* $u \in \mathfrak{o}_K\Delta^\times$ *then* $u(\overline{u})^{-1} \in \mathrm{tor}(\mathfrak{o}_K\Delta^\times)$.
(ii) $\mathrm{tor}(\mathbb{Z}^{\mathrm{c}}\Delta^\times) = \mu\cdot\Delta$.

Proof. See [B1] for (i); (ii) is a well-known fact. ∎

2. Proof of the Theorem

(2.1) Remark. To put the last statement of (ii) in a more general perspective, we mention that the argument in Taylor's article [T3] in Proposition 4.2.3 shows that if N/K is abelian, odd, unramified and with a normal integral basis, then it necessarily has a selfdual normal integral basis.

(2.2) Remark. We want to draw attention in particular to the somewhat unusual verification, in the proof of (iii) below, that the number $m \in \mathbb{Q}\sqrt{-d}$ satisfies $m = \overline{m}$.

(2.3) Proof of (ii). Let m be a rational integer which cannot be written in the form $n^3 - n^2$ with $n \in \mathbb{Z}$. Then the polynomial $f(X) = X^3 - X^2 - m$ is irreducible over $\mathbb{Q}$. Let N be the splitting field of $f(X)$ and let α_1, α_2, α_3 be the roots of $f(X)$. The discriminant of $f(X)$ is $-27m^2 - 4m = [(\alpha_1-\alpha_2) \times (\alpha_2-\alpha_3)(\alpha_3-\alpha_1)]^2$ (see [Jac], Vol. III, p. 93, formula (6)). This is a negative number, so it is not a square in $\mathbb{Z}$ and therefore the Galois group of N over $\mathbb{Q}$ is the symmetric group S_3. Moreover, N contains the imaginary quadratic field $K = \mathbb{Q}\sqrt{-27m^2-4m}$ and N/K is a cubic cyclic extension. Expressing the coefficients of $f(X)$ in terms of its roots we obtain the relations $\alpha_1+\alpha_2+\alpha_3 = 1$ and $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = 0$; it follows that $\alpha_1^2+\alpha_2^2+\alpha_3^2 = 1$. The last two relations can be written as follows:

$$\mathrm{Tr}_{N/K}(\alpha_i\alpha_j) = \delta_{i,j} \quad \text{for all } 1 \le i,j \le 3$$

(with Tr = Trace and δ = Kronecker delta), that is, α_1, α_2, α_3 form a selfdual normal integral basis of N/K; moreover, by Corollary (1.3), N/K is unramified. ∎

(2.4) Proof of (iii). Let N be an unramified cubic cyclic extension of an imaginary quadratic field K such that N/K has a normal integral basis. Let β_1, β_2, β_3 be a normal integral basis of N/K and let $\delta \in \Delta = \mathrm{Gal}(N/K)$ be such that $\beta_1^\delta = \beta_2$. We let w be $R(\beta_1)$, the Lagrange resolvent of β_1. Then $w^\delta = w\cdot\delta$ and by Proposition (1.1) one has $w \in \mathfrak{o}_N\Delta^\times$. Therefore $\widehat{w}^\delta =$

$\widehat{w}\cdot\delta^{-1}$ and it follows that the element $u = \widehat{w}w^{-1}$ satisfies $u \in \mathfrak{o}_N\Delta^\times$, $u^\delta = u{\cdot}\delta$ and $u\widehat{u} = 1$. It follows from Proposition (1.1)(ii) and Corollary (1.3) that, if we write $u = \alpha_1 + \alpha_2\delta^{-1} + \alpha_3\delta^{-2}$ with $\alpha_1, \alpha_2, \alpha_3 \in \mathfrak{o}_N$, then α_1, α_2, α_3 form a selfdual normal integral basis of N/K. That is, α_1, α_2, α_3 form a set of algebraic integers in N satisfying the relations $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 1$ and $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = 0$ and hence $(\alpha_1 + \alpha_2 + \alpha_3)^2 = 1$. Therefore we may assume that $\alpha_1 + \alpha_2 + \alpha_3 = 1$, replacing, if necessary, α_1, α_2, α_3 by $-\alpha_1$, $-\alpha_2$, $-\alpha_3$. Moreover, the numbers α_1, α_2, α_3 are roots of the polynomial $f(X) = X^3 - X^2 - m$, where $m = \alpha_1\alpha_2\alpha_3$. We still have to show that $m \in \mathbb{Z}$. The problem is that though we know that the algebraic integers α_1, α_2, α_3 form a complete set of conjugates over K and so that their product m lies in $\mathfrak{o}_K$, we do not yet know whether they form a complete set of conjugates over $\mathbb{Q}$, that is, we do not yet know whether $\overline{m} = m$, where $\overline{}$ is complex conjugation. We recall that the properties of α_1, α_2, α_3 can be expressed in terms of the Lagrange resolvend u as follows:

$$u \in \mathfrak{o}_N\Delta^\times, \quad u\widehat{u} = 1, \quad u^\delta = u\cdot\delta, \quad \operatorname{aug} u = 1,$$

where aug is the augmentation homomorphism from $\mathfrak{o}_N\Delta^\times$ to $\mathfrak{o}_N^\times$. It follows that the action of the group $\Delta = \mathrm{Gal}(N/K)$ leaves u^3 fixed, that is, all the coefficients of u^3 lie in K and therefore $u^3 \in \mathfrak{o}_K\Delta^\times$. As $K/\mathbb{Q}$ is abelian, it follows from Lemma (1.5)(i) that $u^3(\overline{u^3})^{-1} \in \mathrm{tor}(\mathfrak{o}_K\Delta^\times)$.

Now we need the fact that an unramified abelian extension of a quadratic number field is always Galois over $\mathbb{Q}$. By lack of a reference we include a proof. For each ideal of K its absolute norm is a principal ideal; therefore the Galois action of $\mathrm{Gal}(K/\mathbb{Q})$ on the ideal classgroup Cl_K leaves each subgroup of Cl_K stable. Transferring this fact, via the canonical isomorphism from class field theory, from Cl_K to $\mathrm{Gal}(H_K/K)$, where H_K is the maximal unramified abelian extension of K, gives the following result (see also statement (i) of Theorem (11.5) in [C–F]): each subgroup of $\mathrm{Gal}(H_K/K)$ is a normal subgroup of $\mathrm{Gal}(H_K/\mathbb{Q})$. By Galois theory this can be reformulated as follows: each unramified abelian extension of K is Galois over $\mathbb{Q}$.

We choose an embedding $N \hookrightarrow \mathbb{C}$ and define "complex conjugation" on the group ring $N\Delta$ accordingly (see (1.4)). It follows that $u\overline{u}^{-1} \in \mathrm{tor}(\mathfrak{o}_N\Delta^\times)$ and so by Lemma (1.5)(ii) that $u\overline{u}^{-1} \in \mu_N \cdot \Delta$.

On the other hand, as $\operatorname{aug} u = 1$, it follows that $\operatorname{aug}(u\overline{u}^{-1}) = 1$. Therefore $u\overline{u}^{-1} \in \Delta$, that is,

$$\alpha_1 + \alpha_2\delta^{-1} + \alpha_3\delta^{-2} = (\overline{\alpha}_1 + \overline{\alpha}_2\delta + \overline{\alpha}_3\delta^2)\gamma$$

for some $\gamma \in \Delta$. Hence, applying the map from $N\Delta$ to N which sends each element to the product of its coefficients, we get

$$m = \alpha_1\alpha_2\alpha_3 = \overline{\alpha_1\alpha_2\alpha_3} = \overline{m},$$

that is, $m \in \mathbb{Z}$, as required.

Finally, the polynomial

$$f(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3) = X^3 - X^2 - m$$

is clearly not reducible over $\mathbb{Q}$, and so m cannot be written in the form $n^3 - n^2$ for any $n \in \mathbb{Z}$. ∎

In the proof of (iv) we will use the following lemma.

(2.5) Lemma. *Let N be an unramified cubic cyclic extension of an imaginary quadratic number field K with a selfdual normal integral basis α_1, α_2, α_3 with $\alpha_1+\alpha_2+\alpha_3 = 1$. Then $m = \alpha_1\alpha_2\alpha_3$ lies in $\mathbb{Z}$ and for each primitive cube root of unity ζ the following identity holds*:

$$(\alpha_1 + \alpha_2\zeta^{-1} + \alpha_3\zeta^{-2})^3 = 1 + \tfrac{27}{2}m \pm \tfrac{3}{2}\sqrt{81m^2+12m}$$

where the sign ± has to be chosen suitably.

Proof. We have already shown that $m \in \mathbb{Z}$ in the proof of statement (iii) of the Theorem. An easy calculation, using $\alpha_1+\alpha_2+\alpha_3 = 1$, $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = 0$ and $\alpha_1\alpha_2\alpha_3 = m$, gives the identity

$$\begin{aligned}(\alpha_1 + \alpha_2\delta^{-1} + \alpha_3\delta^{-2})^3 \\ = (1+9m) + \big(-\tfrac{9}{2}m - \tfrac{3}{2}D\big)\delta^{-1} + \big(-\tfrac{9}{2}m + \tfrac{3}{2}D\big)\delta^{-2},\end{aligned}$$

where $D = (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)$. We recall that $D^2 = -27m^2 - 4m$. Specializing δ to ζ and writing $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ gives the identity in the statement of the lemma. ∎

(2.6) Remark. The following consequence is perhaps of some independent interest:

Let $m \in \mathbb{Z}$ be such that $81m^2+12m$ is not a square. Then $1 + \frac{27}{2}m + \frac{3}{2}\sqrt{81m^2+12m}$ is an algebraic unit in the real quadratic number field $\mathbb{Q}\sqrt{81m^2+12m}$.

(2.7) Proof of (iv). Firstly we prove the following implication. If an imaginary quadratic number field $K = \mathbb{Q}\sqrt{-d}$ has an unramified cubic cyclic extension with a normal integral basis, then there is an algebraic unit t in $\mathbb{Q}\sqrt{3d}$ which is $\equiv 1 \bmod 3\sqrt{3}$ and which is not a third power in $\mathbb{Q}\sqrt{3d}$. We use statement (iii) of the theorem: let $m \in \mathbb{Z}$ be such that N is the splitting field of $X^3 - X^2 - m$ and let α_1, α_2, α_3 be the roots of this polynomial. Then the choice $t = (\alpha_1 + \alpha_2\zeta^{-1} + \alpha_3\zeta^{-2})^3$ has the required properties by Lemma (2.5).

Secondly we prove the converse. Let t be an algebraic unit in $\mathbb{Q}\sqrt{3d}$ which is $\equiv 1 \bmod 3\sqrt{3}$ and which is not a third power in $\mathbb{Q}\sqrt{3d}$. Let s be a cube root of t. Let v be a valuation above 3 on the number field $\mathbb{Q}(s,\zeta)$. Then the product of the three numbers $s-1$, $s-\zeta$ and $s-\zeta^2$ is $u - 1 \equiv 0 \bmod 3\sqrt{3}$, so at least one of them has v-valuation $\geq v(\sqrt{3})$. Therefore, as these three numbers are clearly congruent modulo $\sqrt{3}$, it follows that each of them has v-valuation $\geq v(\sqrt{3})$. As this holds for each valuation v on $\mathbb{Q}(s,\zeta)$ above 3, we conclude that $s \equiv 1 \bmod \sqrt{3}$. Now we define the numbers α_1, α_2, α_3 by the following system of equations:

$$\begin{aligned}&\alpha_1+\alpha_2+\alpha_3=1,\\&\alpha_1+\zeta^{-1}\alpha_2+\zeta^{-2}\alpha_3=s,\\&\alpha_1+\zeta\alpha_2+\zeta^2\alpha_3=s^{-1}.\end{aligned}$$

Adding the equations gives $3\alpha_1 = 1+s+s^{-1} = 3+s^{-1}(s-1)^2$, which is $\equiv 0 \bmod 3$, as $s \equiv 1 \bmod \sqrt{3}$. Therefore α_1 is an algebraic integer. In the same way one proves that α_2 and α_3 are also algebraic integers. Now we consider the element $u = \alpha_1 + \alpha_2\delta^{-1} + \alpha_3\delta^{-2}$ in the group ring $\mathbb{Z}^{\mathrm{c}}\varDelta$ where $\varDelta$ is a cyclic group of order 3 with generator δ. Let ζ be a primitive cube root of unity. We use the fact that the map from $\mathbb{Q}^{\mathrm{c}}\varDelta$ to $\mathbb{Q}^{\mathrm{c}}\times\mathbb{Q}^{\mathrm{c}}\times\mathbb{Q}^{\mathrm{c}}$ given by $a+b\delta+c\delta^2 \to (a+b+c, a+b\zeta+c\zeta^2, a+b\zeta^2+c\zeta)$ is an isomorphism of $\mathbb{Q}^{\mathrm{c}}$-algebras: it follows that $u\widehat{u}=1$ and that the coefficients of u^3 lie in K. The latter fact can be expressed as follows: $u^3 = (u^3)^\omega$ for all $\omega \in \varOmega_K = \mathrm{Gal}(\mathbb{Q}^{\mathrm{c}}/K)$. Therefore $u(u^\omega)^{-1} \in \mathrm{tor}(\mathbb{Z}^{\mathrm{c}}\varDelta^\times)$, which is equal to $\mu\cdot\varDelta$ by Lemma (1.5). Therefore, as $\mathrm{aug}\, u = 1$, it follows that $u(u^\omega)^{-1} \in \varDelta$ for all $\omega \in \varOmega_K$. That is, the coefficients of u form a complete set of algebraic conjugates over K of one integer. As moreover $u\widehat{u}=1$, it follows from Corollary (1.3) that the coefficients α_1, α_2, α_3 of u form a selfdual normal integral basis of the unramified cubic cyclic extension $K(\alpha_1,\alpha_2,\alpha_3)/K$. ∎

(2.8) Proof of (i). Let $K=\mathbb{Q}\sqrt{-d}$ be an imaginary quadratic number field. Suppose N/K is an unramified cubic cyclic extension with a normal integral basis. Let α_1, α_2, α_3 be a selfdual normal integral basis of N/K with $\alpha_1+\alpha_2+\alpha_3=1$. We write $u=\alpha_1+\alpha_2\delta^{-1}+\alpha_3\delta^{-2}$ in $\mathbb{Z}^{\mathrm{c}}\varDelta$ where $\delta\in\varDelta=\mathrm{Gal}(N/K)$ is defined by $\alpha_1^\delta=\alpha_2$. Then $u\widehat{u}=1$ and $u^3\in\mathfrak{o}_K\varDelta^\times$. Therefore $(\alpha_1+\zeta\alpha_2+\zeta^2\alpha_3)(\alpha_1+\zeta^2\alpha_2+\zeta\alpha_3)=1$ and $(\alpha_1+\zeta\alpha_2+\zeta^2\alpha_3)^3\in\mathfrak{o}_{K(\zeta)}^\times$. We write $s=\alpha_1+\zeta^2\alpha_2+\zeta\alpha_3$ and $t=s^3$. Then

$$\begin{aligned}&\alpha_1+\alpha_2+\alpha_3=1,\\&\alpha_1+\zeta^2\alpha_2+\zeta\alpha_3=s,\\&\alpha_1+\zeta\alpha_2+\zeta^2\alpha_3=s^{-1},\end{aligned}$$

and $t\in\mathfrak{o}_{K(\zeta)}^\times$ with $t\equiv 1$ mod $3\sqrt{3}$.

Clearly $N(\zeta)=K(\zeta)(s)$, so t determines $N(\zeta)$ and so it determines N. Now we consider the following subgroups of $\mathfrak{o}_{K(\zeta)}^\times$:

$$\begin{aligned}U&=\{r\in\mathfrak{o}_{K(\zeta)}^\times \mid r\equiv 1 \bmod 3\sqrt{3}\},\\V&=\{w^3\mid w\in\mathfrak{o}_{K(\zeta)}^\times,\ w\equiv 1\bmod\sqrt{3}\}.\end{aligned}$$

Clearly $t \in U$ and changing t by a factor which belongs to V does not change the field $K(\zeta)(s)$; therefore the image of t in the quotient group U/V determines N. Moreover, as $t = (\alpha_1 + \zeta^{-1}\alpha_2 + \zeta^{-2}\alpha_3)^3$, it does not belong to V, that is, the image of t in U/V is not trivial. Furthermore, replacing t by t^{-1} also does not change the field $K(\zeta)(s)$. So the image of t in the set S of orbits in $(U/V) - \{1\}$ under the action by inversion determines N. Therefore, in order to prove (i), it suffices to show that S cannot have more than one element. Applying Dirichlet's unit theorem to the biquadratic imaginary number field $K(\zeta)$ it follows that $U/V \simeq \mathbb{Z}/3$ or $\simeq 1$, which gives the desired conclusion. ■

3. A Galois module interpretation of the Spiegelungssatz of Scholz. We recall the following classical result. Let, for each $d \in \mathbb{Z}$, $r_3(d)$ be the 3-rank of the ideal classgroup of $\mathbb{Q}\sqrt{d}$.

(3.1) Theorem (Scholz [S]). *Let $d \in \mathbb{N}$. Then $r_3(-d) - r_3(3d) = 0$ or 1.*

This is the simplest non-trivial example of Leopoldt's Spiegelungssatz (see [Jau] for details). We are now going to outline a version of the usual proof of (3.1).

(3.2) Sketch of the proof of (3.1). Combining class field theory and Kummer theory, a "reflection homomorphism" m_d from $(\widehat{Cl}_{\mathbb{Q}\sqrt{-d}})_3$, the 3-torsion subgroup of the dual of the ideal classgroup of $\mathbb{Q}\sqrt{-d}$, to $(Cl_{\mathbb{Q}\sqrt{3d}})_3$, the 3-torsion subgroup of the ideal classgroup of $\mathbb{Q}\sqrt{3d}$, is defined for all $d \in \mathbb{Z}$. Then the following description of its kernel in terms of unit groups is derived:

$$\ker m_d \simeq \frac{\{u \in \mathfrak{o}^*_{\mathbb{Q}\sqrt{3d}} \mid u \equiv 1 \bmod 3\sqrt{3}\}}{\{u \in (\mathfrak{o}^*_{\mathbb{Q}\sqrt{3d}})^3 \mid u \equiv 1 \bmod 3\sqrt{3}\}}. \tag{3.3}$$

Therefore, by Dirichlet's unit theorem, we get

$$\dim_{\mathbb{F}_3} \ker m_d = \begin{cases} 0 \text{ or } 1 & \text{if } d > 0, \\ 0 & \text{if } d < 0. \end{cases} \tag{3.4}$$

It is a routine exercise in finite abelian groups to derive Theorem (3.1) from statement (3.4). ■

From this outline of the proof it is clear that (3.3) is the heart of the matter. Combining (3.3) with statement (iv) of the main result of this paper we get the following Galois module interpretation for the kernel of the reflection homomorphism m_d.

(3.5) Corollary. *If $d > 0$ then the kernel of the reflection homomorphism m_d is non-trivial if and only if there exists an unramified cubic cyclic extension of $\mathbb{Q}\sqrt{-d}$ with a normal integral basis.*

References

[B1] J. Brinkhuis, *Normal integral bases and complex conjugation*, J. Reine Angew. Math. 375/376 (1987), 157–166.

[B2] —, *Galois module structure as the obstruction to a local-global principle*, J. Algebra 145 (1992), 454–462.

[B3] —, *On the Galois module structure over CM-fields*, Manuscripta Math. 75 (1992), 333–347.

[C–F] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967.

[Ca–Ch–F–T] Ph. Cassou-Noguès, T. Chinburg, A. Fröhlich and M. J. Taylor, *L-functions and Galois modules*, Notes by D. Burns and N. P. Byott, in: Proceedings of the Durham Symposium, July 1989, Cambridge University Press, Cambridge, 1991, 75–139.

[C–T] Ph. Cassou-Noguès and M. J. Taylor, *Elliptic Functions and Rings of Integers*, Progr. Math. 66, Birkhäuser, Boston, 1987.

[F] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergeb. Math. Grenzgeb. (3) 1, Springer, 1981.

[H] D. Hilbert, *Die Theorie der algebraischen Zahlkörper* (*"Zahlbericht"*), Jahresber. Deutsch. Math.-Verein. 4 (1897), 175–546, or: *Gesammelte Abhandlungen*, I, Berlin, 1932, 63–363.

[Jac] N. Jacobson, *Lectures in Algebra*, Vol. III, Princeton Univ. Press, 1964.

[Jau] J.-F. Jaulent, *Dualité dans les corps surcirculaires*, in: Séminaire de Théorie des Nombres, Paris 1986–87, Progr. Math. 75, Birkhäuser, 1988, 183–220.

[S] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. 166 (1932), 201–203.

[T1] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. 63 (1981), 41–79.

[T2] —, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math. 121 (1985), 519–535.

[T3] —, *Rings of integers and trace forms for tame extensions of odd degree*, Math. Z. 202 (1989), 313–341.

[T4] —, *The Galois module structure of certain arithmetic principal homogeneous spaces*, J. Algebra 153 (1992), 203–214.

ECONOMETRIC INSTITUTE
ERASMUS UNIVERSITY
P.O. BOX 1738
3000 DR ROTTERDAM, THE NETHERLANDS

Received on 8.2.1991
and in revised form on 20.7.1992 (2120)