manuscripta math. 75, 333 - 347 (1992)

manuscripta
mathematica

ON THE GALOIS MODULE STRUCTURE OVER CM-FIELDS

Jan Brinkhuis

In this paper we make a contribution to the problem of the existence of a normal integral basis. Our main result is that unramified realizations of a given finite abelian group Δ as a Galois group $\mathrm{Gal}(N/K)$ of an extension N of a given CM-field K are invariant under the involution on the set of all realizations of Δ over K which is induced by complex conjugation on K and by inversion on Δ. We give various implications of this result. For example, we show that the tame realizations of a finite abelian group Δ of odd order over a totally real number field K are completely characterized by ramification and Galois module structure.

Introduction

By a classical theorem of Hermite each algebraic number field K has only finitely many field extensions of given degree and discriminant over K. In an attempt towards a refinement of this result one could ask the following question. To what extent are the realizations of a given finite abelian group Δ as a Galois group $\mathrm{Gal}(N/K)$ of a tame field extension N of a given number field K characterized by their 'ramification' and their 'Galois module structure', where the latter is defined to be the isomorphism class of $\mathfrak{o}_N$, the ring of integers in N, as a module over the group ring $\mathfrak{o}_K\Delta$ of Δ over $\mathfrak{o}_K$? It has been shown in [3] that this question is equivalent to the following one, which seems more restricted at first sight: are realizations of Δ over K which are unramified –at all finite primes– and which have moreover a normal integral basis over K, rare? In the present paper we offer the following result on this question if K is a CM–field (our definition of CM–fields includes totally real fields).

All unramified realizations of Δ over K with a normal integral basis are invariant under the 'obvious' involution on the set of all realizations of Δ over K which is induced by complex conjugation on K and by inversion on Δ.

In the remainder of this introduction we point out some consequences of this result. In the case that K is totally real, the result can be restated as follows: *unramified abelian extensions of a totally real number field K have never a normal integral basis over K, with the possible exception of composita of quadratic extensions of K.* Such exceptions can indeed exist, as we will see. This result implies the following ones. The Galois module structure of an unramified realization of Δ over K, viewed as an element of the locally free class group $C\ell(\mathfrak{o}_K\Delta)$ has order either $\exp\Delta$ or $\frac{\exp\Delta}{2}$ where $\exp\Delta$ is the exponent of the group Δ. Thus, in particular, this order is precisely $\exp\Delta$ if $|\Delta|$ is odd. Moreover, returning to the question posed at the beginning of this introduction, *the tame Galois algebra realizations of a finite abelian group Δ of odd order over a totally real number field K are completely characterized by ramification and Galois module structure.* In particular, for such K and Δ, the unramified realizations of Δ over K have mutually non–isomorphic Galois module structures.

In the other case, namely that K is a totally imaginary quadratic extension of a totally real number field, our result has for example the following consequence: *if H_K, the Hilbert class field of K, has a normal integral basis over K, then $h_{K^+}=1$* or 2, *where h_{K^+} is the class number of K^+, the maximal real subfield of K.*

Taking a different point of view, our result exhibits via Galois modules non-trivial elements in $C\ell(\mathfrak{o}_K\Delta)$, the existence of which cannot -at least so far- be demonstrated otherwise.

Finally we remark that the old problem of the existence of normal integral bases has led in the last twenty years to an extensive literature on Galois module structure of rings of integers, with powerful methods and deep theorems; however it seems that this is the first time that it is possible to obtain precise information on the Galois module structure and in particular on the classical normal integral basis problem of extensions inside the Hilbert class field of a CM-field.

1. The main result

Let $\mathbb{Q}^c$ be an algebraic closure of $\mathbb{Q}$, the field of rational numbers; all number fields will be considered to be subfields of $\mathbb{Q}^c$. Let K be a CM-field, that is, it is a number field which has an automorphism which coincides for each embedding of K into $\mathbb{C}$, the field of complex numbers, with complex conjugation. This is equivalent to the requirement that K is either a totally real number field or a totally imaginary quadratic extension of a totally real number field. In the last case we speak of a *proper* CM-field. Let Δ be a finite abelian group.

(1.1) **Definition.** A realization of Δ over K is a pair $r=(N,\psi)$ consisting of a Galois extension N of K together with an isomorphism ψ from $\mathrm{Gal}(N/K)$ to Δ.

Now we choose an embedding of $\mathbb{Q}^c$ into $\mathbb{C}$ and we restrict complex conjugation on $\mathbb{C}$ to an automorphism of $\mathbb{Q}^c$ which we denote by c. For each group G and each G–module A we will denote the action of G on A by the left exponential notation $(g,a) \to {}^g a$ (for all $g \in G$, $a \in A$). We will use the left exponential notation more generally to denote the action of the group ring $\mathbb{Z}G$ on A.

(1.2) **Definition.** For each realization $r=(N,\psi)$ of Δ over K, its *complex conjugate realization* $\bar{r}=(\bar{N},\bar{\psi})$ is defined as follows

$$\bar{N}=\left\{{}^c n \mid n \in N\right\}$$

$$\bar{\psi}(\omega)=\psi(c^{-1}\omega c)^{-1} \text{ for all } \omega \in \mathrm{Gal}(\bar{N}/K)$$

(1.3) *Warning.* Notice the second inverse sign. Inversion on the group Δ 'plays the role of complex conjugation'.

(1.4) *Remark.* This definition does not depend on the chosen embedding of $\mathbb{Q}^c$ into $\mathbb{C}$.

A realization $r=(N,\psi)$ is called unramified if N/K is unramified at all finite primes. A realization $r=(N,\psi)$ is said to have a normal integral basis if $\mathfrak{o}_N$, the ring of integers in N, is a free module on one generator on $\mathfrak{o}_K\Delta$, the group ring of Δ over $\mathfrak{o}_K$.

Now we come to the main result of this paper.

(1.5) **Theorem.** *Each unramified realization of a finite abelian group over a CM-field with a normal integral basis is equal to its complex conjugate realization.*

This result can also be stated as follows. Let K^+ be the maximal real subfield of K.

(1.6) *Each unramified abelian extension N of a CM-field K with a normal integral basis over K is Galois over K^+ and moreover the action of complex conjugation on* $\mathrm{Gal}(N/K)$ *by conjugation in the group* $\mathrm{Gal}(N/K^+)$ *is equal to inversion.*

In a previous paper [4] a related result is given –theorem 2.9– and in [2] we proved a much weaker version of this theorem; certain corollaries of theorem (1.5), to be given below, have been obtained already in [2] and [4].

Our proof of theorem (1.5) will be based on the following criterion. Before stating it, we have to make some preparations. We recall that Galois theory establishes a bijection between the group $H^1(\Omega_K,\Delta)=\mathrm{Hom}(\Omega_K,\Delta)$, the set of all continuous homomorphisms ϕ from $\Omega_K=\mathrm{Gal}(\mathrm{Q}^c/K)$ to Δ, and the set of *Galois algebras* A over K with Galois group Δ. For each $\phi\in\mathrm{Hom}(\Omega_K,\Delta)$ let A_ϕ be the corresponding Galois algebra and let K_ϕ be $(\mathrm{Q}^c)^{\mathrm{Ker}\phi}$, the fixed field of $\mathrm{Ker}\phi$, the kernel of ϕ. One says that A_ϕ is unramified if the field extension K_ϕ/K is unramified at all finite primes. Let $\mathfrak{a}_\phi$ be the maximal order in A_ϕ. One says that A_ϕ has a normal integral basis if $\mathfrak{a}_\phi \simeq \mathfrak{o}_K\Delta$ as $\mathfrak{o}_K\Delta$-modules. We consider the action of the group Ω_K on the ring $\mathbb{Z}^c\Delta$ –the group ring of Δ over $\mathbb{Z}^c$, the ring of algebraic integers in $\mathbb{Q}^c$ – which acts trivially on Δ $(\subseteq\mathbb{Z}^c\Delta)$ and which acts on $\mathbb{Z}^c$ $(\subseteq\mathbb{Z}^c\Delta)$ by the Galois action. The inclusion map i from Δ (with trivial Ω_K–action) into $\mathbb{Z}^c\Delta^*$, the group of invertible elements in $\mathbb{Z}^c\Delta$, preserves Ω_K–action and so it induces a map of Galois cohomology groups

$$i^{\times}\colon \operatorname{Hom}(\Omega_K,\Delta)=H^1(\Omega_K,\Delta) \to H^1(\Omega_K,\mathbb{Z}^c\Delta^*)$$

Now we can state the promised criterion (for the proof we refer to [4]).

(1.7) **Proposition.** *Let* $\phi\in\operatorname{Hom}(\Omega_K,\Delta)$. *The following conditions on* ϕ *are equivalent*

(i) *The Galois algebra* A_ϕ *corresponding to* ϕ *is unramified and has a normal integral basis.*

(ii) $i^{\times}(\phi)=1.$

Moreover the following result will play a crucial role in our proof. Let G be the product group $\Omega_{K^+}\times C_2$ and let σ be the non–trivial element of C_2. We will consider Ω_{K^+} and C_2 as subgroups of G. We let the group G act on the group ring $\mathbb{Z}^c\Delta$ as follows: let Ω_K act on $\mathbb{Z}^c$ by the Galois actions, on Δ trivially, let σ act on Δ by inversion and $\mathbb{Z}^c$ trivially. The action of the element $\alpha=(c,\sigma)\in G$ on $\mathbb{Z}^c\Delta$ plays the role of complex conjugation. Let μ be the group of all roots of unity in $\mathbb{Q}^c$.

(1.8) **Proposition.** *Let* $u \in \mathbb{Z}^c\Delta^*$ *and assume that* $u^m \in \mathrm{o}_K\Delta^*$ *for some* $m > 1$. *Then*

$$^{1-\alpha}u \in \mu{\cdot}\Delta$$

Proof. To begin with, α acts on the field components of the semisimple algebra $K\Delta$, which are all *CM*–fields, as complex conjugation. Therefore, if we project the element $^{1-\alpha}(u^m)$ of $K\Delta$ on one of the field components of $K\Delta$, then we get an algebraic unit of absolute value 1; it is a standard result that such units must be roots of unity. It follows that $^{1-\alpha}(u^m)$ and so $^{1-\alpha}u$ is a torsion element in $\mathbb{Z}^c\Delta^*$. Finally, it is well–known that the torsion subgroup of $\mathbb{Z}^c\Delta^*$ is $\mu{\cdot}\Delta$. □

We write $\omega^* = c^{-1}\omega c$ for all $\omega \in \Omega_K$. We define for each $\phi \in \mathrm{Hom}(\Omega_K, \Delta)$ its 'complex conjugate' $\bar{\phi} \in \mathrm{Hom}(\Omega_K, \Delta)$ as follows

$$\bar{\phi}(\omega) = \phi(\omega^*)^{-1} \text{ for all } \omega \in \Omega_K.$$

Now we are ready to state and prove the following implication which is the key step in the proof.

(1.9) **Proposition.** *Let* $\phi \in \mathrm{Hom}(\Omega_K, \Delta)$. *If* $i^\times(\phi) = 1$, *then* $\phi = \bar{\phi}$.

Proof. Assume $i^\times(\phi) = 1$. This means that there is an element $u \in \mathbb{Z}^c\Delta^*$ such that

$$\phi(\omega) = {}^{\omega-1}u \qquad \forall \omega \in \Omega_K \tag{1.10}$$

Let m be the order of ϕ. Then, by (1.10), u^m is fixed by Ω_K, and so, as $(\mathbb{Z}^c\Delta^*)^{\Omega_K} = \mathrm{o}_K\Delta^*$, (1.11) $u^m \in \mathrm{o}_K \Delta^*$.

Therefore, by proposition (1.8), ${}^{1-\alpha}u \in \mu \cdot \Delta$ and so we can write

(1.12) ${}^{1-\alpha}u = \zeta\rho$

with $\zeta \in \mu$ and $\rho \in \Delta$.

Now we are going to compute for all $\omega \in \Omega_K$ the element

$$\theta = {}^{(\omega-1)(1-\alpha)}u$$

in two different ways. On the one hand, by (1.12), θ is equal to ${}^{\omega-1}(\zeta\rho)$, which equals ${}^{\omega-1}\zeta \in \mu$. On the other hand, θ is equal to ${}^{\omega-1}u^{-(\omega-1)\alpha}u$, so, as $(\omega-1)\alpha = \alpha(\omega^*-1)$, this is, by (1.10), equal to $\phi(\omega)^{-\alpha}\phi(\omega^*)$; as α acts on Δ by inversion, this last expression is equal to $\phi(\omega)\phi(\omega^*) \in \Delta$. Comparing these two outcomes and projecting from $\mu.\Delta = \mu \times \Delta$ onto Δ we get

$$\phi(\omega)\phi(\omega^*) = 1.$$

This holds for all $\omega \in \Omega_K$, that is, $\phi = \bar{\phi}$. □

By proposition (1.7) and proposition (1.9) we have now proved the following result.

(1.5)′ **Theorem.** *Let $\phi \in \mathrm{Hom}(\Omega_K, \Delta)$. If the Galois algebra A_ϕ corresponding to ϕ is unramified and has a normal integral basis, then $\phi = \bar{\phi}$.*

We have also proved theorem (1.5) as this is readily seen to be just theorem (1.5)′ with the additional assumption that ϕ is surjective.

2. Consequences

We start with the implications of our result for the normal integral basis problem. These are rather strong if K is totally real.

(2.1) **Corollary.** *There is no unramified abelian extension of any totally real number field with a normal integral basis with the possible exception of composita of quadratic extensions.*

Proof. This is just a reformulation of theorem (1.5) for the case that K is totally real. To show this, it is convenient to use the terminology of theorem (1.5)′ let $\phi \in \mathrm{Hom}(\Omega_K, \Delta)$ be such that the Galois algebra A_ϕ is unramified and has a normal integral basis. To establish the corollary we have to show $\phi^2 = 1$. As K is totally real, the automorphism c lies in Ω_K and so, as $\phi \in \mathrm{Hom}(\Omega_K, \Delta)$, $\phi(\omega^*) = \phi(c^{-1}\omega c) = \phi(\omega)$ for all $\omega \in \Omega_K$, that is $\bar{\phi} = \phi^{-1}$. Therefore the conclusion of theorem (1.5)′, $\phi = \bar{\phi}$, comes down to $\phi^2 = 1$. This finishes the proof of the corollary. □

The possible exceptions mentioned in (2.1) can actually occur for certain K. For example let K be a real quadratic number field of odd discriminant. It is well-known that there are precisely $2^{k-1} - 1$ unramified quadratic extensions of K where k is the number of prime numbers dividing the discriminant of K. In [1] we proved the following result (see proposition (IV 3.5a) in [6]). Let $S(K)$ be the set of number fields which are composita of unramified quadratic extensions of K.

(2.2) **Theorem.** *Let K be a real quadratic number field of odd discriminant. If the norm of the fundamental unit equals $+1$, then there is a unique field $N \in S(K)$ with a normal integral basis over K; this is a quadratic extension of K. If this norm is -1, then no $N \in S(K)$ has a normal integral basis over K.*

Now assume that K is a *proper* CM-field. By class field theory the Galois group over K of H_K, the maximal unramified abelian extension of K, is canonically isomorphic to $C\ell_K$, the class group of K. Therefore, by Galois theory, unramified abelian extensions of K correspond to subgroups of $C\ell_K$. We recall that the norm map from $C\ell_K$ to $C\ell_{K^+}$ is surjective and that the kernel of the canonical map from $C\ell_{K^+}$ to $C\ell_K$ has either 1 or 2 elements.

(2.3) **Corollary.** *If an unramified abelian extension of a proper CM-field K has a normal integral basis then the corresponding subgroup of $C\ell_K$ contains the image of $C\ell_{K^+}$.*

Proof. Let $\phi \in \mathrm{Hom}(\Omega_K, \Delta)$ correspond to an unramified Galois algebra A_ϕ with a normal integral basis. Now ϕ factorizes in a canonical way over a homomorphism ϕ_0 from $C\ell_K$ to Δ. Translating the conclusion of theorem (1.5)$'$, $\phi = \bar{\phi}$ in terms of ϕ_0 we get $\phi_0(x) = \phi_0(\bar{x})^{-1}$ for all $x \in C\ell_K$, where $\bar{\ }$ denotes the action of complex conjugation on $C\ell_K$. Therefore $\phi_0(x\bar{x}) = 1$. By the remarks preceding the corollary it follows that Ker ϕ_0 contains the image of $C\ell_{K^+}$. □

In particular, letting h_{K^+} be the class number of K^+, we get the following result.

(2.4) **Corollary.** *If H_K, the Hilbert class field of a proper CM-field K, has a normal integral basis over K, then* $h_{K^+} = 1$ or 2.

Proof. Immediate from corollary (2.3) and the remarks preceding it. □

For unramified abelian extensions N/K, the $\mathfrak{o}_K\Delta$-module $\mathfrak{o}_N$ –where $\Delta = \mathrm{Gal}(N/K)$– is locally free (or, what is the same here, projective) of rank one. Therefore its isomorphism class can be viewed as an element of the following finite abelian group, $C\ell(\mathfrak{o}_K\Delta)$, the class group of the ring $\mathfrak{o}_K\Delta$. It is trivial precisely if the extension has a normal integral basis. The results above show that in many cases this element is non-trivial, so one is naturally led to ask what its order in the group $C\ell(\mathfrak{o}_K\Delta)$ is. We will denote this order by $\mathrm{ord}(\mathfrak{o}_N)$. We can give the following divisibility result for it.

(2.5) **Corollary.** *Let K be a CM-field and Δ a finite abelian group. Let an unramified realization* $\mathrm{Gal}(N/K) \simeq \Delta$ *of Δ over K be given and let ϕ be the corresponding element in* $\mathrm{Hom}(\Omega_K,\Delta)$. *Then*

$$\mathrm{ord}(\phi\bar{\phi}^{-1})\,|\,\mathrm{ord}(\mathfrak{o}_N)\,|\,\mathrm{ord}\phi.$$

Proof. Let H_K^+ be the maximal unramified abelian extension of K. We will view $\mathrm{Hom}(\mathrm{Gal}(H_K^+/K),\Delta)$ as a subgroup of $\mathrm{Hom}(\Omega_K,\Delta)$ via inflation. Let g be the map from $\mathrm{Hom}(\mathrm{Gal}(H_K^+/K),\Delta)$ to

$C\ell(\mathfrak{o}_K\Delta)$ which sends each ϕ to the $\mathfrak{o}_K\Delta$-isomorphism class of $\mathfrak{a}_\phi$, the maximal order of the Galois algebra A_ϕ. We have to prove that, for all subjective $\phi\in\mathrm{Hom}(\mathrm{Gal}(H_K^+/K),\Delta)$, one has

$$\text{(2.6)}\qquad \mathrm{ord}(\phi\overline{\phi}^{-1})\,|\,\mathrm{ord}g(\phi)\,|\,\mathrm{ord}\phi.$$

This holds in fact more generally without the surjectivity condition: it is known that g is a homomorphism, moreover we have proved that the condition $g(\phi)=1$ implies $\phi=\overline{\phi}$; clearly (2.6) is an elementary group theoretic consequence of these facts. □

If K is totally real, this result amounts to the following one.

(2.7) **Corollary.** *If N is an unramified abelian extension of a totally real number field K, then* $\mathrm{ord}(\mathfrak{o}_N)$ *is k or ½k where k is the exponent of the Galois group of N/K. In particular, if $[N{:}K]$ is odd, then* $\mathrm{ord}(\mathfrak{o}_N)=k$.

Finally we turn to the question mentioned at the beginning of the introduction to this paper. In [3] we made the following definitions. Let K be a CM-field and let Δ be a finite abelian group. An extension F/E of number field is called tame if for each finite prime of E which ramifies in F, the ramification index is not divisible by the residual characteristic. A tame realization of Δ over K is defined to be a pair (M,ϕ) consisting of a tame Galois extension M of K together with an isomorphism from $\mathrm{Gal}(M/K)$ to Δ. Two tame realizations (M,ϕ) and (N,ψ) of Δ over K are defined to have the same ramification if they become isomorphic under a suitable unramified base field extension L of K of finite degree, in the following sense: the tensor products $L\otimes_K M$ and

$L\otimes_K N$ are isomorphic as $L-\Delta-$algebras, that is, there is an isomorphism of L–algebras from $L\otimes_K M$ to $L\otimes_K N$ which preserves $\Delta-$actions. Two tame realizations (M,ϕ) and (N,ψ) of Δ over K are said to have the same Galois module structure if the maximal orders $\mathfrak{o}_M$ and $\mathfrak{o}_N$ are isomorphic as modules over the group ring $\mathfrak{o}_K\Delta$. We proved the following result in [3].

(2.8) *Two tame realizations (M,ϕ) and (N,ψ) of Δ over K have the same ramification and the same Galois module structure if and only if $i^\times(\phi)=i^\times(\psi)$.*

Here $i^\times$ is as in proposition (1.7) and we have identified ϕ and ψ with the elements of $\mathrm{Hom}(\Omega_K,\Delta)$ which one gets from them by inflation.

The question, to what extent tame realizations of Δ over K are characterized by their ramification and Galois module structure is therefore essentially equivalent to the question how far the homomorphism $i^\times$ is removed from being injective. The result of the present paper that $i^\times(\phi)=1$ implies $\phi=\overline{\phi}$ gives information in a positive direction. For example, we thus get the following result.

(2.9) **Corollary.** *Let K be a totally real number field and let Δ be a finite abelian group of odd order. Then the tame realizations of Δ over K are characterized by their ramification and their Galois module structure.*

Proof. Let (M,ϕ_0) and (N,ψ_0) be tame realizations of Δ over K with the same ramification and the same Galois module structure. Let ϕ resp. ψ be the element of $\mathrm{Hom}(\Omega_K,\Delta)$ which we get from ϕ_0 resp. ψ_0 by inflation. Then by (2.8) we get

$i^{\times}(\phi)=i^{\times}(\psi)$ and so $i^{\times}(\phi\psi^{-1})=1$. Therefore, by proposition (1.9), $\phi\psi^{-1}=\overline{\phi\psi^{-1}}$. As K is totally real, this is equivalent to the condition $(\phi\psi^{-1})^2=1$, and so, as Δ has odd order, $\phi\psi^{-1}=1$, that is $\phi=\psi$. This proves $(M,\phi_0)=(M,\psi_0)$. □

In particular we get the following result.

(2.10) **Corollary.** *Let K be a totally real number field and Δ a finite abelian group of odd order. Then the unramified realizations of Δ over K have mutually non-isomorphic Galois module structures.*

REFERENCES

[1] J. Brinkhuis, *Embedding problems and Galois modules*, doctoral dissertation, Leiden (1981)

[2] J. Brinkhuis, *Normal integral bases and complex conjugation*, J. reine angew. Math. 375/376, 157–166 (1987)

[3] J. Brinkhuis, *Galois module structure as the obstruction to a local-global principle*, to appear in the Journal of Algebra

[4] J. Brinkhuis, *Unramified abelian extensions of CM-fields and their Galois module structure*, preprint (1989)

[5] L. Childs, *The group of unramified Kummer extensions of prime degree*, Proc. L.M.S. 35/3, 407–422 (1977)

[6] A. Fröhlich, *Galois module structure of algebraic integers*, Ergebnisse der Math. 3, 1 (1983)

[7] V. Fleckinger et T. Nguyen Quang Do, *Bases normales, unités et conjecture faible de Leopoldt*, preprint (1990)

[8] I. Kersten and J. Michaliček: *$\mathbb{Z}_p$-extensions of CM-fields*, J. Number Theory, 32, no. 2, 131–150 (1989)

[9] I. Kersten and J. Michaliček: *On Vandiver's conjecture and $\mathbb{Z}_p$-extensions of $\mathbb{Q}(\zeta_p n)$*, J. Number Theory, 32, no. 3, 371–386 (1989)

[10] L. McCulloh, *Galois module structure of abelian extensions*, J. reine angew. Math. 375/376, 259–306 (1987)

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

[12] M.J. Taylor, *The Galois module structure of certain arithmetic principal homogeneous spaces*, preprint, (1990)

Jan Brinkhuis
Econometric Institute
Erasmus University
P.O. Box 1738
3000 DR Rotterdam
The Netherlands

(Received February 7, 1991;
in revised form January 23, 1992)