Astérisque

BOAS EREZ

A survey of recent work on the square root of the inverse different

Astérisque, tome 198-199-200 (1991), p. 133-152

<http://www.numdam.org/item?id=AST_1991__198-199-200__133_0>

A SURVEY OF RECENT WORK ON THE SQUARE ROOT OF THE INVERSE DIFFERENT

by

Boas EREZ

We will give a survey of recent work done by several authors on the Galois-hermitian module obtained by restricting the trace form of a Galois extension K/F to the ideal in K which -when it exists- is the square root of the inverse different of K/F. This is the only additive Galois module, apart from the ring of integers, whose structure is now fairly well known.

Although the work exposed here has benefitted enormously by the techniques developed by A. FRÖHLICH, M.J. TAYLOR *et alia* to study the structure of the ring of integers, we will not suppose here that the reader is acquainted with them, so that this paper can also serve as an introduction to their work.

We shall begin by fixing the notations which will be in force throughout the paper and then we will define the object of our interest. Next an example is given to try to motivate our subsequent discussion. In Section 2 we analyze the situation for weakly ramified extensions, while in Section 3 we drop the restrictions on ramification but consider only abelian extensions. We also give some details concerning the proofs of several results discussed in Section 3 which are not to be published elsewhere. These are to be found in two appendices due to D. BURNS.

Acknowledgements

I heartily thank C. BACHOC and D. BURNS for their assistance in preparing this paper and J. QUEYRUT for very helpful discussions at an earlier stage of my work, in particular he suggested the use of the Adams operation for Theorem 2.7.

1. The square root of the inverse different

Notations.

The arithmetic side. Let us denote by : K/F a finite Galois extension of either number fields or finite extensions of a p-adic field $\mathbb{Q}_p$, $G = \mathrm{Gal}(K/F)$ its Galois group, $\mathrm{Tr}_{K/F}$ the bilinear trace form of K/F, $\mathbb{Z}_L$ the ring of integers in L, $D(K/F)^{-1}$ the inverse different of K/F.

The algebraic side. We will have to consider : FG (resp. $\mathbb{Z}_F G$) the group algebra of G over F (resp. $\mathbb{Z}_F$), m_G the multiplication form on FG for which the elements in G form an orthonormal basis.

Recall that by a formula due to Hilbert (see e.g.[S1] Chap. IV.1, Prop.4) we can compute the order of the different $D(K/F)$ at any prime P in K by means of the sequence $\{G_i = G_i(P, K/F)\}$ of ramification sub-groups of G :

$$\mathrm{ord}_P(D(K/F)) = \sum_{i>-1} (\mathrm{ord}(G_i) - 1) \ . \tag{1.1}$$

As a consequence we have that for instance in an odd degree Galois extension K/F there exists a unique ideal $A(K/F)$ such that

$$A(K/F)^2 = D(K/F)^{-1} \ . \tag{1.2}$$

We will call the ideal A satisfying (1.2) the *square root of the inverse different* (of K/F).

Since G acts on K as a group of isometries of the trace form $\mathrm{Tr}_{K/F}$ and since the dual with respect to the trace form of an ideal B in K is the ideal $B^{-1}D(K/F)^{-1}$, we see that by restricting the trace form to the square root of the inverse different we get a self-dual integral $\mathbb{Z}_F G$-hermitian form $(A(K/F), \mathrm{Tr}_{K/F})$. One would like to have a description of this form up to equivariant isometry (see [C-P] Question (V.4.3)). It is the aim of this survey to summarize what is known on this problem.

1.1. Example

We show how one can use the results on the hermitian module $(A(K/F), \mathrm{Tr}_{K/F})$ to describe the structure of the module $(\mathbb{Z}_K, \mathrm{Tr}_{K/F})$.
Observe that $\mathbb{Z}_K \leq A(K/F) \leq D(K/F)^{-1}$. Suppose that K/F is tamely ramified, that is all its first ramification groups are trivial. To ensure the existence of $A(K/F)$ suppose K/F is Abelian of odd degree and for simplicity let $F = \mathbb{Q}$.

Since the degree of the extension $K/\mathbb{Q}$ is odd, we know that there is a $\mathbb{Q}G$-equivariant isometry between $(K, \mathrm{Tr}_{K/\mathbb{Q}})$ and $(\mathbb{Q}G, m_G)$ (see [B-L] for a proof under more general hypothesis). So $(\mathbb{Z}_K, \mathrm{Tr}_{K/F})$ is isometric to a $\mathbb{Z}G$-ideal M in $\mathbb{Q}G$ which is locally free because we are supposing that $K/\mathbb{Q}$ is tame. We shall now define one such ideal $M = M(K/\mathbb{Q})$ by defining its localizations $M_p = \mathbb{Z}_p \otimes M$ for all primes p of $\mathbb{Q}$. So fix a prime number p and a prime P in K above p, then choose a uniformizing parameter π in K_P. Let $\theta_p := \theta_{0,p}$ be the *injective* character of the inertia group $I(p) := G_0(P, K/F)$ defined by

$$\theta_p(g) = g(\pi)/\pi \bmod P$$

(see [S1] Chap.IV.2 Prop.7). θ_p generates the (cyclic) group of characters of $I(p)$ and to each integer i between 0 and $e(p) := \mathrm{ord}(I(p))$ we can associate in $\mathbb{Z}_pG$ the idempotent $e_{i,p} = (1/e(p)) \sum_{I(p)} \theta_p^i(g) g^{-1}$.

Now form the sum $E_p = e_{0,p} + e_{1,p} + \cdots + e_{m,p}$ where $m = (e(p) - 1)/2$. Then we define M_p to be $M_p := (p, E_p)\mathbb{Z}_pG$. Of course if p doesn't ramify in K/F (i.e $I(p) = \{1\}$), then $M_p = \mathbb{Z}_pG$ so M is well defined. The interest of M stems from the following result -which is shown in [E-M].

THEOREM 1.3. *Under the restrictions introduced above we have*

(i) $M(K/\mathbb{Q})A(K/\mathbb{Q}) = \mathbb{Z}_K$.

(ii) *The following conditions are equivalent*

(a) $(\mathbb{Z}_K, \mathrm{Tr}_{K/\mathbb{Q}})$ *is* $\mathbb{Z}G$*-isometric to* $(M(K/\mathbb{Q}), m_G)$

(b) $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ *is* $\mathbb{Z}G$*-isometric to* $(\mathbb{Z}G, m_G)$.

Now, under the hypothesis of this example one can show that (ii-b) is true (see Theorem 2.9 and Remark 2.10 below), so that -in this particular case- we have a more precise description of $(\mathbb{Z}_K, \mathrm{Tr}_{K/\mathbb{Q}})$ than in [T1] (see [E-M] for more details).

2. Weakly ramified extensions

Our next result will give necessary and sufficient conditions for the square root of the inverse different $A(K/F)$ to be locally isomorphic to $\mathbb{Z}_FG$, in a way completely analogous to what is known as E. NOETHER's characterization of tame extensions (see e.g. [F1] Theorem 3, p.26).

DEFINITION 2.1. The Galois extension K/F is *weakly ramified* if all its second ramification groups (in lower numbering) are reduced to the identity.

Instances of weakly ramified extensions are

(a) all tamely ramified extensions

(b) absolute Galois extensions of odd prime degree.

(c) the dihedral extension obtained as the compositum of $\mathbb{Q}((-3)^{1/2})$ and the (non-Galois) cubic field $\mathbb{Q}((2)^{1/3})$ (see e.g.[C](16.29) and (17.31)).

Observe that (Galois) sub-extensions of weakly ramified extensions are weakly ramified, but that the compositum of weakly ramified extensions is not necessarily weakly ramified : indeed if p is an odd prime, then the cyclotomic field $\mathbb{Q}(p^2)$ of p^2-th roots of unity is not even weakly ramified over $\mathbb{Q}(p)$ although it is the compositum of $\mathbb{Q}(p)$ and the unique subfield of degree p over $\mathbb{Q}$ which it contains.

THEOREM 2.2. *Suppose* ord(G) *is odd. Then* $A(K/F)$ *is locally free over* $\mathbb{Z}_F G$ *if and only if* K/F *is weakly ramified.*

The necessity of a condition on the second ramification groups for *any* ambiguous ideal to be locally free over $\mathbb{Z}_F G$ has been shown by S.ULLOM in [U1], 2.1. The converse is shown in [E2] by using the results of [U2].

Remark. The computations in [Mi1] et [Mi2] show that the characterization of the first ramification group as "vertex of the ring of integers" has no analog even for the second ramification group -as one would hope in light of Theorem 2.2. (see also [F1] Note 3 to Chapter 1).

H1. HYPOTHESIS. In the rest of this section we will always suppose that the order of G is odd and that K/F is weakly ramified.

To get more precise results in this situation - i.e., to investigate when $A(K/F)$ is globally free over $\mathbb{Z}_F G$ - we are led to describe the class defined by $A(K/F)$ in the group $Cl(\mathbb{Z}G)$ of stable isomorphism classes of locally free $\mathbb{Z}G$-modules (we will eventually have to restrict scalars from $\mathbb{Z}_F$ to $\mathbb{Z}$). Recall that since the order of G is assumed to be odd, the stable isomorphism class defined by $A(K/F)$ completely determines its isomorphism class. We now recall the description of $Cl(\mathbb{Z}_F G)$ in terms of Galois homomorphisms (see (2.3) below). This description will allow us to express the class defined by $A(K/F)$ in a way relating it to the arithmetic of the extension K/F. For ease of notation let $R = \mathbb{Z}_F$, $\Lambda = \mathbb{Z}_F G$, $A = FG$ and $C =$ center(FG). If M is a rank one locally free module over Λ, then for every (finite) prime p in R there exists m_p in M and m_0 such that $\Lambda_p m_p = R_p \otimes_R M$ and $Am_0 = F \otimes_R M$. So for every (finite) prime

p there exists b_p in $(A_p)^x$ such that $m_p = b_p m_0$. Note that since $(\Lambda m_0)_p$ and M_p coincide for almost all p, b_p is a unit in Λ_p for almost all p. It follows that M is isomorphic over Λ to the ideal Λb in A defined at each local completion by $R_p \otimes \Lambda b = \Lambda_p b_p$. These considerations lead to the idelic description of $Cl(\Lambda)$, which generalizes the idelic description of class groups of number fields. Sending b to the class (Λb) gives a surjective homomorphism from the ideles $J(A)$ to $Cl(\Lambda)$ whose kernel can be computed (see [C-R]Vol.II (49.22)). By taking the reduced norm to the center nrd = $\mathrm{nrd}_{A/C}$ (and taking into account the infinite places) one obtains the isomorphism

$$Cl(\Lambda) \cong J(C)/C^x \mathrm{nrd}(U(\Lambda))$$

where $U(\Lambda)$ are the unit ideles of Λ (see[C-R]Vol.II(49.23)). Under this isomorphism the class defined by M corresponds to the class of the reduced norm of b. The final step in the description consists in the following. Choose E to be a "big enough" (finite) extension of F-at least Galois over F and splitting A and write R_G for the group of virtual characters of G. Recall that $C = \Pi F(\chi_i)$, product over a set of representatives of the orbits of absolutely irreducible characters of G. We have an isomorphism $f : C^x \cong \mathrm{Hom}_{\Omega(F)}(R_G, E^x)$ defined by $f(\Pi c_i)(\chi) = \Pi f(c_i)(\chi)$ and $f(c_i)(\chi) = 1$ unless $\chi = \chi_i^\omega$ is in the orbit of χ_i, in which case $f(c_i)(\chi) = c_i^\omega$. This isomorphism then extends to the idele groups and we only have to interpret the image of the reduced norm as so-called determinant homomorphisms to obtain FRÖHLICH's Hom-description :

$$Cl(\Lambda) \cong \mathrm{Hom}_{\Omega(F)}(R_G, J(E))/\mathrm{Hom}_{\Omega(F)}(R_G, E^x)\mathrm{Det}\ (U(\Lambda)) \qquad (2.3)$$

(see[C-R] Vol.II (52.11), [F1] II.1). Here the class defined by M corresponds to the Ω-invariant homomorphism f which on an irreducible character χ takes the idelic value $(f_p(\chi))_p$, where -in $E_p^x = (F_p \otimes E)^x$)-

$$f_p(\chi) = \det_\chi(b_p) \qquad (2.4)$$

is the determinant of the matrix in $GL(E_p)$ obtained by evaluating any extension of an E-representation $T = T_\chi$ with character χ on the (invertible) group algebra element b_p.

Remark. Of course all this goes through for more general orders Λ than group rings.

We will now proceed to give a representative homomorphism for the class defined by $A(K/F)$ in $Cl(\mathbb{Z}_F G)$. Here E will also have to contain K and the

values of arithmetic functions needed. So fix local normal generators m_p of $A(K/F)_p$ over $\mathbb{Z}_{F,p}G$ and a normal generator m_0 of K over FG. Let b_p be such that $b_p m_0 = m_p$. Define the idelic resolvent $(m|\chi)$ by letting its p-component be $(m|\chi)_p = (m_p|\chi) = \det(\sum_G T(g^{-1})g(m_p))$ with $T = T_\chi$ as after (2.4). Then $\mathrm{Det}_\chi(b) = (m|\chi)/(m_0|\chi)$ (see [F1] I.4.1). Observe this is immediate for abelian characters, for which we get the classical Lagrange resolvents. Already because $\mathbb{Z}_F$ need not be a principal ring we will restrict scalars from $\mathbb{Z}_F$ to $\mathbb{Z}$ and consider $A(K/F)$ as a $\mathbb{Z}G$-module; this forces us to replace the above resolvents with norm-resolvents $\mathcal{N}_{F/\mathbb{Q}}(m|\chi)$ -which we will not define (see [F1] Theorem 2 and (2.16)). We will make a full use of the Hom-description in that we will need the (second) Adams operation $\Psi = \Psi_2$ on R_G : this is the endomorphism of R_G defined by $\Psi(\chi)(g) = \chi(g^2)$ (see e.g. [C-R] Vol. I, 12B, [K]). Let $\tau(K/F, \Phi)$ be the Galois-Gauss sum attached to the field extension K/F and the character Φ of G (= $\mathrm{Gal}(K/F)$) (as in say [F1] I.5 or [Ma]). We now change the representative homomorphism above with the aid of the Gauss sum and Ψ.

PROPOSITION 2.5. ([E2] Theorem 3.6). *Suppose* (H1) *is fulfilled, then the class defined by* $A(K/F)$ *in* $Cl(\mathbb{Z}_F G)$ *is represented by the Galois homomorphism* $v_{K/F}$ *which on the character* χ *of* R_G *takes the idelic value* $v_{K/F}(\chi) = \mathcal{N}_{F/\mathbb{Q}}(m|\chi)\tau(K/F, \Psi(\chi) - \chi)^{-1}$.

The proof of this proposition follows -as in the study of rings of integers- from the fact that $\mathcal{N}_{F/\mathbb{Q}}(m_0|\chi)$ and $\tau(K/F, \Psi(\chi) - \chi)$ behave in the same way under Galois action (see[F1] III.3).

Remark 2.6. One is led to consider the representative homomorphism given in the proposition after having noticed the decomposition in terms of the Jacobi sums $\tau(\chi)^2/\tau(\chi^2)$ as given in [E1] for absolute Galois extensions of odd prime degree.

Now that we have a nice representative homomorphism we can try to show it lies in the denominator of the right hand side of (2.3). We have not yet succeeded in doing this in general although it is true for tame extensions (see Theorem 2.8 below), howewer in general we can prove the following. Let $\mathcal{M}$ be any maximal order in $\mathbb{Q}G$ containing $\mathbb{Z}G$ and let $D(\mathbb{Z}G)$ denote the kernel of the (surjective) homomorphism from $Cl(\mathbb{Z}G)$ to $Cl(\mathcal{M})$ obtained by extending scalars from $\mathbb{Z}G$ to $\mathcal{M}$. We know that $D(\mathbb{Z}G)$ does not depend on $\mathcal{M}$.

THEOREM 2.7. ([E2] Theorem 2.) *Suppose* (H1) *is fulfilled, then* $v_{K/F}$ *lies in* $D(\mathbb{Z}G)$, *that is* $\mathcal{M} \otimes_{\mathbb{Z}G} A(K/F)$ *is free over* $\mathcal{M}$.

As with FRÖHLICH in his proof of the Martinet Conjecture for tame extensions (see [F1] Theorems 5 and 23), we show that the components of the ideles $\mathcal{N}_{F/\mathbb{Q}}(m|\chi)$ and $\tau(K/F, \Psi(\chi) - \chi)$ are the same up to units, so that $v_{K/F}$ actually lies in $\mathrm{Hom}_\Omega(R_G, U(E))$ and hence is zero in $Cl(\mathcal{M})$ (see [F1] I.2.19). By using the functorial properties of the ideal $A(K/F)$ and of the homomorphisms involved this amounts to a computation in local totally ramified extensions analogous to the one in [F1], III.7 for the tame case, but involving non-abelian local characters in the wild case (see [E2]).

THEOREM 2.8. ([E2] Theorem 3.) *Suppose* (H1) *is fulfilled, but assume also that* K/F *is at most tamely ramified, then* $A(K/F)$ *is free over* $\mathbb{Z}G$.

Given Theorem 2.7 above and its proof (!), this is an almost formal consequence of M.J. TAYLOR's work on Galois-Gauss sums and on groups of determinant homomorphisms together with his joint work with Ph. CASSOU-NOGUÈS on Adams operations (see [F1] Theorems 30, 31 and 10, [CN-T] Théorème 1′ and (2.7) or [T2] Theorems 8.1.2 and 9.1.2, [E2]). In the absolute abelian case we have a complete picture for the hermitian structure as well.

THEOREM 2.9. ([E3] or [E-M] Theorem 4.1.) *Suppose that* $F = \mathbb{Q}$ *and that* $G = \mathrm{Gal}(K/\mathbb{Q})$ *is abelian of odd order. Then the following are equivalent :*

(a) K/F *is weakly ramified*

(b) *for every prime* p *in* $\mathbb{Z}$ *the order of the inertia group* $G_0(K/\mathbb{Q}, p)$ *is either equal to* p *or prime to* p

(c) $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ *is isometric to* $(\mathbb{Z}G, m_G)$

(d) $A(K/\mathbb{Q})$ *is free over* $\mathbb{Z}G$.

This is less involved than the previous results, the hardest part being the proof that (b) implies (c). We exhibit explicit self-dual normal bases - taken from [E1]- for special extensions $K(p)$, one for each prime p ramified in $K/\mathbb{Q}$, so that : K is contained in the compositum $L = \Pi_p K(p)$, the $K(p)$ are arithmetically disjoint in pairs -hence $(A(L/\mathbb{Q}), \mathrm{Tr}_{L/\mathbb{Q}})$ is the tensor product of the $(A(K(p)/\mathbb{Q}), \mathrm{Tr}_{K(p)/\mathbb{Q}})$ -, and also $A(K/\mathbb{Q}) = \mathrm{Tr}_{L/K}(A(L/\mathbb{Q}))$. (Of course $K(p)$ can be chosen to be the field corresponding to the group X_p of p-parts of the Dirichlet characters associated to K (see [E-M]).)

Recall that by Section 1.1 this theorem gives the structure of the hermitian pair $(\mathbb{Z}_K, \mathrm{Tr}_{K/\mathbb{Q}})$ in this special situation.

Remark 2.10. The recent paper [E-T] deals with the hermitian structure of both the ring of integers $\mathbb{Z}_K$ and the square root of the inverse different $A(K/F)$ in arbitrary odd degree tamely ramified Galois extensions K/F. It contains a generalization of the results of [E-M]. In particular it generalizes the definition of the "comparison" module $M(K/F)$ of Example 1.1 above and it shows how to use Theorem 2.8 to get a description of the class that $A(K/F)$ defines in the Grothendieck group of (locally free) hermitian modules over $\mathbb{Z}G$.

3. Very wildly ramified extensions

Unless explicitly stated, in this section we will always assume.

H2 - HYPOTHESIS. $F = \mathbb{Q}$, $G = \mathrm{Gal}(K/F)$ is abelian and K/F is such that the square root of the inverse different $A(K/F)$ exists.

According to the results above, if K/F is not weakly ramified then on the one hand $A(K/F)$ cannot even be locally isomorphic to $\mathbb{Z}G$ (Theorem 2.2) and on the other hand the trace form on $A(K/F)$ cannot be the standard one (Theorem 2.9). To encompass these difficulties one compares $A(K/F)$ to its associated order Λ, that is the order $\Lambda(A(K/F))$ in FG of elements stabilizing $A(K/F)$. The local problem was considered by D. BURNS who showed

THEOREM 3.1. *Under* (H2) $A(K/F)$ *is locally free over its associated order* $\Lambda(A(K/F))$.

A proof of this theorem is given in Appendix A below.

Remark 3.2. There exist local cyclic extensions $K/F/\mathbb{Q}_p$ in which no fractional ideal is locally free over its associated order; for example if F is absolutely unramified, then this is so for any totally ramified cyclic extension K/F of degree rp^2 with $r > p^2$ (see [Bu2]).

BURNS predicted that the local isometry class would only depend on the group structure of G together with its inertia subgroups. By using Theorem 3.5 below, he and the author were able to show

THEOREM 3.3. *Let* p *be an odd prime and let* $K/\mathbb{Q}_p$ *and* $K'/\mathbb{Q}_p$ *be abelian extensions in which the inverse different has a square root. Suppose* $K/\mathbb{Q}_p$ *and* $K'/\mathbb{Q}_p$ *are such that there exists an isomorphism between their Galois groups which restricts to one between their inertia groups, then there is an equivariant isometry between* $(A(K/\mathbb{Q}_p), \mathrm{Tr}_{K/\mathbb{Q}_p})$ *and* $(A(K'/\mathbb{Q}_p), \mathrm{Tr}_{K'/\mathbb{Q}_p})$.

Proof. We refer to the notation introduced in Appendix A for the proof of Theorem 3.1. By (A.2) the A decompose as

$$A = \bigoplus_{\chi} e(\chi)A = e(1)A \oplus \bigoplus_{\chi \neq 1} (e(\chi) + e(\overline{\chi}))A \ .$$

These are orthogonal sums with respect to the trace form. The summand corresponding to the identity character is dealt with by Theorem 3.5 below : it corresponds to a cyclic p-extension. We then observe that on the summands of the form $(e(\chi)+e(\overline{\chi}))A$ the trace form is even, hyperbolic and self-dual. By [Bas] (4.4), there is only one such form on a projective module over a commutative ring, so we are done by Theorem 3.1.

∎

Remark 3.4. It is shown in [E-M] that for two $\mathbb{Z}G$-projective ideals in $\mathbb{Q}G$, say L and M, the *forms* (L, m_G) and (M, m_G) are locally isometric everywhere if and only if the "discriminant *modules*" $L^\sharp/L$ and $M^\sharp/M$ are isomorphic (here $L^\sharp$ is the dual of L with respect to m_G). Theorem 3.3 would also be a consequence of a result of this kind with $\mathbb{Z}G$ replaced by the associated order of the square root of the inverse different.

The local structure is thus fairly well known, so let us consider global extensions.

THEOREM 3.5. *Suppose* (H2) *holds, and assume the order of G to be odd. If for every prime p of $\mathbb{Q}$ either $G_0(K/\mathbb{Q}, p)$ is a p-group or has order prime to p, then there exists an equivariant isometry between $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ and $(\Lambda(A(K/\mathbb{Q})), n_G)$ where n_G is a form on $\mathbb{Q}G$ not depending on K.*

The proof of this theorem was obtained in two steps. First in [B-E] the Hermitian pair $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ was studied in detail in the special case of cyclic p-extensions totally ramified at p. For instance if the order of G is p^n with $p \neq 3$ and n even, we have that $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ is $\mathbb{Z}G$-isometric to an orthogonal sum $< 1 > \oplus B_2 \oplus B_4 \oplus \ldots \oplus B_n$ where the $B_i = B_i(p)$ are indecomposable, even bilinear forms independent of K with a nice description ; their root system is $(p^{i-2} + p^{i-1})\mathbb{A}_{p-1}$ (standard notation). Later C. BACHOC observed that the results of [B-E] together with an explicit description of the associated order $\Lambda(A(K/\mathbb{Q}))$ were sufficient -via a construction like that given for Theorem 2.9 above- to prove the theorem in the general case under the stated restrictions. Details can be found in [Ba], where a description of n_G is also given.

Remark. We observe that in all the situations so far considered the form

$(A(K/F), \mathrm{Tr}_{K/F})$ always turned out to have a very "symmetric" system of minimal vectors.

In light of Remark 3.2 one couldn't hope for such a precise description in the relative case ($F \neq \mathbb{Q}$), but even for absolute extensions -and quite unexpectedly- D. BURNS was able to prove the following

THEOREM 3.6. *Given any integer n, there exist infinitely many abelian extensions $K = K_n/\mathbb{Q}$ with a square root of the inverse different satisfying the following : let $G_K = \mathrm{Gal}(K/\mathbb{Q})$ and let $\mathcal{M} = \mathcal{M}_K$ denote the maximal order in $\mathbb{Q}G_K$. Write $\mathcal{M}A(K/\mathbb{Q})$ for the smallest $\mathcal{M}$-module in K containing $A(K/\mathbb{Q})$. Then the order of the class of $\mathcal{M}A(K/\mathbb{Q})$ in the locally free class group of $\mathcal{M}$ is greater than n. Moreover, given any odd prime p, one can even choose the extensions $K/\mathbb{Q}$ to be of p-power conductor (and hence cyclic).*

This theorem shows that the analog of LEOPOLDT's Hauptsatz in [L] is false for the square root of the inverse different. In Appendix B the reader will find a complete proof - by BURNS - of the fact that the unique extension of absolute degree 39 and conductor 13^2 is the smallest example of an extension $K/\mathbb{Q}$ for which $\mathcal{M}A(K/\mathbb{Q})$ is not free over $\mathcal{M}$.

In conclusion we can say that, although many results on the square root of the inverse different we have discussed have perfect analogues concerning the ring of integers, some have not and we hope that the parallels that can be drawn will help to throw a different light on this area of research.

Appendix A. Sketch proof of Theorem 3.1

We follow D. BURNS. For the proof it will be sufficient to consider local extensions and by functoriality properties (see e.g. [Be], 2.1) we can even restrict our attention to totally ramified extensions. So let K/F be a local totally ramified Galois extension over $\mathbb{Q}_p$ with Galois group $G = Gal(K/F)$. Let $A = A(K/F)$ and let Λ be its associated order in FG. The strategy of the proof is the following : we show that Λ is weakly self-dual, that is we show that Λ is isomorphic to its linear dual $\Lambda^* = Hom(\Lambda, \mathbb{Z}_F)$. By [F2] Theorem 10 on page 211, this will imply that A is isomorphic to Λ. To show the self-duality of Λ we shall use Theorem 2 of [Bu1] which relates local isomorphism to two other equivalence relations on lattices : factor equivalence (also discussed in [F3]) and G-o-equivalence. (To use this theorem we need to know that F is absolutely unramified). To check these equivalence relations we will need a precise description of the maximal order $\mathcal{M}$ in FG and of Λ.

To begin with, G decomposes into a direct product $G = P \times C$, where P is the p-Sylow subgroup in G. Let r (resp. p^n) be the order of C (resp. P). It is well known that r divides $p-1$.

Case I : p odd. Here G is cyclic and by Hypothesis (H2) r is odd. For i between 0 and n, let $H(i)$ be the subgroup of order p^i in P and let $e(i)$ be the corresponding "trace" idempotent defined by

$$p^i e(i) = \Sigma_{H(i)} h.$$

(A.1) We record the fact that if $k > l$ then $e(k)e(l) = e(k)$. Let also $P = < g >$ and $f = g - 1$.

(A.2) For any character χ of C let :

$$e(\chi) = (\Sigma_C \chi(c^{-1})c)/r.$$

Observe that $e(\chi)$ is in $\mathbb{Z}_L C$ so any G-module M decomposes into $M = \oplus e(\chi)M$, with the sum taken over all characters χ of C. In particular the maximal order $\mathcal{M}$ decomposes in this way and by work of A.-M. BERGÉ a basis of $e(\chi)\mathcal{M}$ is given by the set

$$\{e(\chi)e(i)f^{j(i)}\} \tag{A.3}$$

where $0 \leq i \leq n$ and $j(i)$ runs over a suitable range (see [Bu2]). Let us now check that $\Lambda \cong \Lambda^*$. Since G is cyclic in this case, Λ is factor equivalent to Λ^* and so by Theorem 2 of [Bu1] it is sufficient to check G-o-equivalence. More precisely, for all "trace" idempotents e corresponding to subgroups of G, we must show that both $(\Lambda^*)^e$ and Λ^e have the same associated orders in FGe (see [Bu1] Section 2). But, for any lattice M, the associated order of M equals the associated order of its linear dual M^* and there is also a natural identification $(M^*)^e = (eM)^*$, and hence we must only check that for each "trace" idempotent e :

$$e\Lambda \text{ equals the associated order of } \Lambda^e \text{ in } FGe. \tag{A.4}$$

Now, if e belongs to Λ, then (A.4) is easily verified ; so (A.4) certainly holds for all idempotents e corresponding to subgroups of C, since these are sums of the idempotents $e(\chi)$ and $e(\chi)A \leq A$ by the above observation. Moreover, a simple computation shows (or see [B-E] Proposition 2.3.4) that :

(A.5) for even i, the idempotents $e(i)$ are in Λ,

(A.6) for all i, $fe(i)$ is in Λ.

So we are left to check (A.4) for $e = e(i)$ with odd i. In view of the description (A.3) and of (A.6) it suffices to consider elements m (in $\mathcal{M}$) of the form $m = \Sigma_{k \geq i+1} m_k e(\chi) e(k)$, but since $m = e(i+1)m$ by (A.1), m belongs to the l.h.s. of (A.4) if and only if it belongs to the r.h.s. of (A.4).

Case II : $p = 2$. There really are two subcases here depending on whether G is cyclic or not, but if G is cyclic, then we can argue as in Case I. So let G be non-cyclic. Then G is a 2-group of type $(2^{n-1}, 2) : G =< a > \times < b >$ where a is of order 2^{n-1} and b of order 2. We can compute the valuation of the different by means of Hilbert's formula and results on the ramification sequence (see e.g. [Le], page 147). We find that :

(A.7) if n is even, then A is $\mathbb{Z}_F G$-isomorphic to $\mathbb{Z}_K$ and so the result follows from (4.2.7) of [Bu2] ;

(A.8) if n is odd, then A is isomorphic to $X = P_K^{(\text{ord } G)/2}$ where P_K denotes the maximal ideal in $\mathbb{Z}_K$.

Again we must consider G-o-equivalence : here, between X and its associated order Λ, this is easy so we will not go into it. In view of [Bu2] it suffices to prove that the so-called factorisable quotient function is trivial on the character group $G^\circ = \text{Hom}\,(G, \mathbb{C}^x)$ of G. By definition this means we have to check the equality

$$[\Lambda : i(X)] = \Pi_D f(\Lambda, X)(D) \tag{A.9}$$

where here i is any injective homomorphism from X into Λ with finite cokernel, D runs over all divisions in the character group G° , and $f(\Lambda, X)(D)$ is the ideal of F defined by Möbius inversion from the ideal $f(\Lambda, X)(C) = [\Lambda^{e_H} : (iX)^{e_H}]$, with C the cyclic subgroup $(G/H)^\circ$ of G° (i.e. if $f = f(\Lambda, X)$ and if $\mu(D/C)$ denotes the Möbius function of the order of $< D > /C$, then by definition $f(D) = \Pi_{C<D} f(C)^{\mu(D/C)}$). Since we already know about G-o-equivalence, Lemma (2.11) of [Bu1] tells us that $[\Lambda : i(X)]$ divides $\Pi_D f(\Lambda, X)(D)$. Also by the (general) Theorem 7 in [F3], page 64, we know that $\mathbb{Z}_K$ is *always* factor equivalent to $\mathbb{Z}_F G$, so $[\mathbb{Z}_F G : \mathbb{Z}_K] = \Pi_D f(\mathbb{Z}_F G, \mathbb{Z}_K)(D)$.

Hence we are left to check that

$$[\Lambda : \mathbb{Z}_F G] = (\Pi_D f(\Lambda, \mathbb{Z}_F G)(D)) P_F^{-1} \tag{A.10}$$

(the P_F^{-1} comes from the factorisable quotient function $f(\mathbb{Z}_K, X)$). But the product over divisions in (A.10) equals $2^{\text{ord } G}$, and one can show that here (n odd) Λ contains the order $\{\mathcal{M}(FG(2)), ((1-a)/2)e_{<a^2,b>}\}\mathbb{Z}_F G$ where $G(2) = < a >$ and $\mathcal{M}(FG(2))$ is the maximal order in $FG(2)$. So (A.10) follows since $[\mathcal{M}(FG(2)) : \mathbb{Z}_F G] = 2^{\text{ord } G(2)-1}$.

Appendix B, by D. Burns : A surprising example

Let K be an abelian extension of $\mathbb{Q}$ such that in K there exists the square root of the inverse different $A(K) = A(K/\mathbb{Q})$. In Section 3, it was noted that whilst $A(K)$ is always locally free over its associated order (Theorem 3.1) its global structure depends critically upon the ramification of the extension $K/\mathbb{Q}$. In particular, setting $G_K = \text{Gal}(K/\mathbb{Q})$ with $\mathcal{M}_K$ the maximal $\mathbb{Z}$-order in the $\mathbb{Q}$-algebra $\mathbb{Q}G_K$ it was claimed - in Theorem 3.6 - that even the lattice $\mathcal{M}_K A(K)$ may have a non-trivial structure in the very wildly ramified case. In this appendix, rather than giving a proof of the full Theorem 3.6 we reduce technicalities to a minimum by discussing an explicit example in which $\mathcal{M}_K A(K)$ can be shown to have a non-trivial $\mathcal{M}_K$-structure. In fact, it is not difficult to verify that amongst extensions in which $\mathcal{M}_K A(K)$ has a non-trivial structure the example given here has the minimum possible absolute degree.

For simplicity we shall only consider extensions $K/\mathbb{Q}$ which possess a unique ramified prime (which is therefore totally ramified in the extension $K/\mathbb{Q}$). For p an odd prime, n a positive integer and r an odd divisor of $p-1$ there exists a unique abelian extension $K = K(p,n,r)$ of $\mathbb{Q}$ of degree $p^n r$ in which p is the only ramifying prime. Furthermore, since the degree of any such extension K is odd, we know that the square root of the inverse different $A(K)$ exists. Now, by the Hom-description of the locally free class group $Cl(\mathcal{M}_K)$ of $\mathcal{M}_K$ (see (2.3)), the global structure of a locally free $\mathcal{M}_K$-module X is determined by a function $g = g_X$ defined on the character group $G_K^\circ = Hom(G_K, \mathbb{C}^x)$ and satisfying at each character θ in G_K°

$$g_X(\theta) \text{ is an element of the ideal class group } Cl(\mathbb{Q}(\theta)) \text{ of } \mathbb{Q}(\theta) \tag{B.1}$$

with for each ω in $\text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$

$$g_X(\theta)^\omega = g_X(\theta^\omega). \tag{B.2}$$

Now, if $K = K(p,n,r)$ is such that $\mathcal{M}_K A(K)$ is not free, then by Theorem 3.5 we shall certainly require that $r \neq 1$. Since we also want $Cl(\mathbb{Q}(\theta)) \neq 0$ checking

a table of class numbers now reveals that the smallest possible degree of such an extension occurs with $p = 13$, $n = 1$, and $r = 3$. Indeed we know that $Cl(\mathbb{Q}(39))$ has order 2 whereas $Cl(\mathbb{Q}(3))$ and $Cl(\mathbb{Q}(13))$ are both trivial. In this appendix we shall prove the

THEOREM B.3 : *For $K = K(13,1,3)$ the class $(\mathcal{M}_K A(K))_{\mathcal{M}_K}$ has order 2.*

Henceforth we shall write $K = K(13,1,3)$ with $O = \mathbb{Z}_K$, $G = G_K$, $\mathcal{M} = \mathcal{M}_K$ and $A = A(K)$. Now, by the above remarks one knows that if X is any locally-free $\mathcal{M}$-module and θ is an element of G°, then $g_X(\theta)$ is trivial if the order of θ is not 39. On the other hand, any two elements of G° of exact order 39 are conjugate under the action of $\mathrm{Gal}(\mathbb{Q}(39)/\mathbb{Q})$ and hence (by condition (B.2)) give the same evaluation of g_X. In this case we shall therefore refer to the class $(X)_{\mathcal{M}}$ as being represented by (the class of) a suitable fractional ideal of $\mathbb{Q}(39)$. Set $E = \mathbb{Q}(3)$. In E the rational prime ideal (13) splits as a product $(13)\mathbb{Z}_E = p_1 p_2$ and we let P_1 (respectively P_2) denote the unique prime of $\mathbb{Q}(39)$ lying above p_1 (respectively p_2). The numbering is to be understood as follows. Let F denote the local completion of K at the unique prime of residue characteristic 13. We can and do identify G with the local Galois group $\mathrm{Gal}(F/\mathbb{Q}_{13})$. Fix a character θ of G° of exact order 39. Let t be an embedding of $\mathbb{Q}(39)$ into an algebraic closure $\mathbb{Q}_{13}^c$ of $\mathbb{Q}_{13}$. Composing θ with t gives a 13-adic character which we denote by $\theta(t)$. Decompose G as $G = S \times C$ where S is the subgroup of G of order 13 and C is the complementary subgroup of order 3. Accordingly the character $\theta(t)$ decomposes as $\theta(t) = \Psi \times \Phi$. Let π be any element in F generating the maximal ideal of $\mathbb{Z}_F$. The map sending g in G to $g(\pi)/\pi$ gives an isomorphism θ_0 (independent of the choice of π) from C to a subgroup of the units of the residue field of $\mathbb{Q}_{13}$. Let $\chi = \chi(F)$ denote the element of the group of 13-adic characters C° that induces by passage to the residue field the isomorphism θ_0. Since χ generates C° we can define an integer $u(\Phi) = 1$ or 2 by $\Phi = \chi^{u(\Phi)}$. Then we choose our numbering in such a way that, if the embedding t_1 (respectively t_2) corresponds to the prime ideal P_1 (respectively P_2) and $\theta(t_i) = \Psi_i \times \Phi_i$, then $\Phi_i = \chi(F)^i$ for $i = 1$ or 2. The following lemma reduces the proof of Theorem B.3 to an exercise in explicit class field theory.

LEMMA B.4 : *The class $(\mathcal{M}A)_{\mathcal{M}}$ is represented by the ideal P_1.*

To prove the result of the lemma we first note that if we denote by $A^{\mathcal{M}}$ the largest $\mathcal{M}$-lattice in K contained in A, then

$$(\mathcal{M}A)_{\mathcal{M}} = (A^{\mathcal{M}})_{\mathcal{M}} \ . \tag{B.5}$$

Indeed by definition A is a self dual lattice from which it follows that $\mathcal{M}A$ is a lattice dual to $A^{\mathcal{M}}$. But now, equation (B.5) follows as a consequence of the general theory of the Hom-description (see for example [F1] Section 1.2, Example 1) together with the fact that $Cl(\mathbb{Q}(39))$ admits no non-trivial automorphism. On the other hand, Theorem 2 and Lemma (2.3) of [Bu3] together imply that

$$O^{\mathcal{M}} \cong \mathcal{M} \tag{B.6}$$

since O is known to be locally free over its associated order in $\mathbb{Q}G$. Now, from (B.5) and (B.6) the explicit Hom-description of $Cl(\mathcal{M})$ implies that the class $(\mathcal{M}A)_{\mathcal{M}}$ is represented by the ideal

$$h(\theta) := h_{(\mathcal{M}A)}(\theta) = ([(\mathbb{Z}[\theta] \otimes_{\mathbb{Z}} A)^{\theta} : (\mathbb{Z}[\theta] \otimes_{\mathbb{Z}} O)^{\theta}]_{\mathbb{Z}[\theta]})^{-1}. \tag{B.7}$$

It is immediate that $h(\theta)$ has support only above the rational prime (13). However, to compute expression (B.7) precisely, we go over to the local extension $F/\mathbb{Q}_{13}$. Let $A' = A(F/\mathbb{Q}_{13})$ and $O' = \mathbb{Z}_F$. Write $\mathbb{Z}'_{13}$ for the valuation ring of the local field obtained by adjoining a primitive 13th root of unity η to $\mathbb{Q}_{13}$. For any embedding t of $\mathbb{Q}(39)$ into $\mathbb{Q}^c_{13}$ one has

$$h^t(\theta(t)) := h(\theta)^t = ([(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} A')^{\theta(t)} : (\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} O')^{\theta(t)}]_{\mathbb{Z}'_{13}})^{-1}.$$

If now $\theta(t)$ decomposes as $\theta(t) = \Psi \times \Phi$ and if $e(\theta(t))$, $e(\Psi)$ and $e(\Phi)$ denote the corresponding idempotents of $\mathbb{Q}_{13}(\eta)[G]$, $\mathbb{Q}_{13}(\eta)[S]$ and $\mathbb{Z}_{13}C$ respectively, then of course $e(\theta(t)) = e(\Psi)e(\Phi)$ in $\mathbb{Q}_{13}(\eta)[G]$. Since Φ is non-trivial, one checks that both $(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} A')^{\theta(t)} = e(\theta(t))(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} A')$ and $(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} O')^{\theta(t)} = e(\theta(t))(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} O')$. But, if ε is the identity character of S, then

$$(1 - e(\varepsilon))e(\Phi) = \sum_{\omega} e(\theta(t))^{\omega} \text{ sum over } \omega \text{ in } \mathrm{Gal}(\mathbb{Q}_{13}(\eta)/\mathbb{Q}_{13})$$

and hence for the norm N from $\mathbb{Q}_{13}(\eta)$ to $\mathbb{Q}_{13}$ we have the expression in terms of $\mathbb{Z}_{13}$-indices

$$N(h(\theta)^t) = \prod_{\omega} h^t(\theta(t)^{\omega}) = [e(\varepsilon)e(\Phi)O' : e(\varepsilon)e(\Phi)A']/[e(\Phi)O' : e(\Phi)A']. \tag{B.8}$$

To evaluate the expression (B.8) we recall that to every 13-character Φ of C we have associated an integer $u(\Phi)$ (= 1 or 2). Let x be a non-zero element in F.

Of course, since $e(\Phi)$ is in $\mathbb{Z}_{13}C$, one has for the valuation $v_F(x)$ of x

$$v_F(e(\Phi)x) \geq v_F(x). \tag{B.9}$$

The importance of the integer $u(\Phi)$ is that one has

$$v_F(e(\Phi)x) = v_F(x) \text{ if and only if } v_F(x) = u(\Phi) \text{ modulo (3).} \tag{B.10}$$

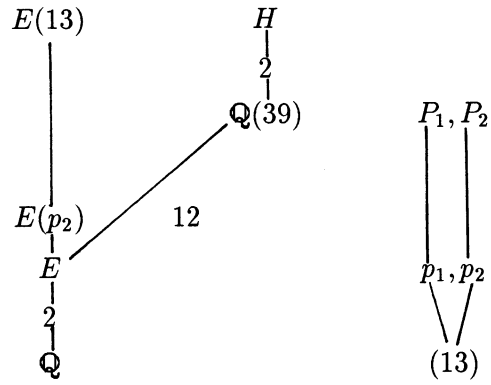
Let now F'' denote the subfield of F of degree 3 over $\mathbb{Q}_{13}$, let O'' denote its valuation ring and P'' the unique maximal ideal of O''. By Hilbert's formula one computes that $A' = (13)^{-1}P'^2$ so that $e(\Phi)A' = e(\Phi)(13)^{-1}P'^2$ and hence $e(\varepsilon)e(\Phi)A' = e(\Phi)(13)^{-1}P'' = e(\Phi)(13)^{-1}P''^{u(\Phi)}$, where for the last equality we have used (B.9) and (B.10). Similarly, one has $e(\varepsilon)e(\Phi)O' = e(\Phi)O'' = e(\Phi)P''^{u(\Phi)}$ and hence $[e(\varepsilon)e(\Phi)O' : e(\varepsilon)e(\Phi)A']_{\mathbb{Z}_{13}} = (13)^{-1}\mathbb{Z}_{13}$. Using the same type of argument one has $e(\Phi)(13)A' = e(\Phi)O' = e(\Phi)P'^2$ if $u(\Phi) = 2$, and $e(\Phi)(13)A' = e(\Phi)P'^4$ and $e(\Phi)O' = e(\Phi)P'$ if $u(\Phi) = 1$. So $[e(\Phi)O' : e(\Phi)A']_{\mathbb{Z}_{13}} = (13^{-13})\mathbb{Z}_{13}$ or $(13^{-12})\mathbb{Z}_{13}$ according as $u(\Phi)$ is 2 or 1. Finally therefore (B.8) becomes

$$\begin{aligned} N(h(\theta)^t) &= (13^{12})\mathbb{Z}_{13} \quad \text{if } u(\Phi) = 2 \text{ and} \\ &= (13^{11})\mathbb{Z}_{13} \quad \text{if } u(\Phi) = 1\,. \end{aligned} \tag{B.11}$$

With the convention of the numbering of primes introduced before the statement of the lemma, (B.11) implies that $h(\theta) = (P_1P_2)^{-12}P_1$. Now P_1P_2 is inflated from $\mathbb{Q}(13)$ and hence is a principal ideal so that in fact the class $(\mathcal{M}A)_{\mathcal{M}}$ is represented by the ideal P_1. But this is precisely the statement of Lemma B.4.

■

Having proved Lemma B.4 we are reduced to a problem of explicit global class field theory - namely to verify that P_1 is not a principal ideal of $\mathbb{Q}(39)$. In general of course, such problems are very difficult but in this case we are saved by reinterpreting the Hilbert class field of $\mathbb{Q}(39)$ as a ray class field of an imaginary quadratic subfield of class number one. To be more precise we write, for each integral ideal J or E, $E(J)$ for the ray class field of E modulo the ideal J. Writing H for the Hilbert class field of $\mathbb{Q}(39)$, one has a diagram of fields and degrees



The key to our computation is the observation that

$$E(13) = H. \tag{B.12}$$

But $\mathbb{Q}(39)$ is the compositum of E and $\mathbb{Q}(13)$ and so is included in $E(13)$ and hence to prove (B.12) we need only to demonstrate that the extension $E(13)/\mathbb{Q}(39)$ is unramified of degree at least two. Of course, one knows *a priori* that $E(13)/\mathbb{Q}(39)$ can be ramified only at either P_1 or P_2. We shall show that there is no ramification above P_1 (with an exactly similar argument proving the same for P_2). Well, p_1 is unramified in the extension $E(p_2)/E$ and totally ramified in the extension $\mathbb{Q}(39)/E$ which is of degree twelve. To conclude, we shall merely compute the degrees $|E(p_2) : E|$ and $|E(13) : E|$. But E has class number one and hence, for any integral $\mathbb{Z}_E$-ideal P, one has an exact sequence

$$\mu_E \longrightarrow (\mathbb{Z}_E/P)^x \longrightarrow \mathrm{Gal}\,(E(P)/E) \longrightarrow 0 \tag{B.13}$$

where here $\mu_E = (\mathbb{Z}_E)^x$ and the second map is derived from the Artin reciprocity law (by choosing a generator of each ideal of $\mathbb{Z}_E$ that is coprime to P). In particular, therefore one has

$$\begin{aligned} |E(P) : E| &= \text{ card (cokernel } (\mu_E \longrightarrow (\mathbb{Z}_E/P)^x) \\ &= \text{ card } ((\mathbb{Z}_E/P)^x) \text{ card } (\mu_E(P))/ \text{ card } (\mu_E) \end{aligned}$$

where we have used the notation $\mu_E(P)$ for the set of elements in μ_E which are congruent to one modulo P. From here one computes that $|E(p_2) : E| = 2$ and $|E(13) : E| = 24$ and it now follows that $E(13)/\mathbb{Q}(39)$ is an extension of degree

two in which P_1 is unramified. A similar argument dealing with P_2 allows us to deduce equality (B.12). We note that this argument also proves that any prime ideal of $E(P_2)$ lying above p_1 is totally ramified in the extension $E(13)/E(P_2)$.

Now by (B.12) together with the prime decomposition law of class field theory we have the equivalence of the following statements :

- P_1 is a principal ideal of $\mathbb{Q}(39)$
- P_1 is split in the extension $E(13)/\mathbb{Q}(39)$
- p_1 is split in the extension $E(p_2)/E$
- if $p_1 = (\pi)\mathbb{Z}_E$, then π is in the kernel of the Artin map (for $P = p_2$)
- π is congruent modulo p_2 to an element in μ_E (B.14)

where for the last equivalence we have used the exact sequence (B.13) with $P = p_2$. Setting now $z = -(1 + (-3)^{1/2})/2$ we can take $\pi = 1 - 3z$ so that $p_2 = (\pi - 5)\mathbb{Z}_E$. But card $(\mu_E) = 6$ and modulo p_2 we have $\pi^6 = 5^6 = (-1)^3 = -1$ so that condition (B.14) cannot be satisfied. Finally therefore one deduces that P_1 is not principal in $\mathbb{Q}(39)$ as was to be proved.

REFERENCES

[Ba] BACHOC C., *Sur les réseaux unimodulaires pour la forme Trace(x^2)*, to appear in the proceedings of the Séminaire de Théorie des Nombres de Paris, (1988-1989).

[B-E] BACHOC C., EREZ B., Forme trace et ramification sauvage, *Proc. London Math. Soc.* (3) **61** (1990), 209-226.

[Bas] BASS H., Unitary algebraic K-theory, 57-265, in *Algebraic K-theory III*, Proceedings of Batelle Institute Conference (1972), Springer Lecture Notes **343**, Berlin, Springer (1973).

[B-L] BAYER E., LENSTRA H.W., Forms in odd degree extensions and self-dual normal bases, *American J. of Math.*, **112** (1990), 359-373.

[Be] BERGÉ A.-M., Extensions galoisiennes a groupe d'inertie cyclique,*Ann. Inst. Fourier*, **28** (1978), 17-44.

[Bu1] BURNS D., Factorisability, group lattices and Galois module structure, *J. of Algebra*, **134** (1990), 257-270.

[Bu2] BURNS D., Factorisability and wildly ramified Galois extensions, to appear in *Ann. Inst. Fourier.*

[Bu3] BURNS D., Canonical factorisability and a variant of Martinet's conjecture, to appear in *J. of the London Math. Soc.*.

[C] COHN H., *A classical invitation to algebraic numbers and class fields*, Universitext. New-York, Springer (1978).

[CN-T] CASSOU-NOGUÈS PH., TAYLOR M.J., Opérations d'Adams et groupes de classes d'algèbres de groupe, *J. of Algebra* (1), **95** (1985), 125-152.

[C-P] CONNER P., PERLIS R., *A survey of trace forms in algebraic number fields*, Singapore, World Scientific (1984).

[C-R] CURTIS C., REINER I., *Methods of representation theory*, 2 volumes, New-York, John Wiley and Sons (1981-1987).

[E1] EREZ B., The Galois structure of the trace form in extensions of odd prime degree, *J. of Algebra*, **118** (1988), 438-446.

[E2] EREZ B., The Galois structure of the square root of the inverse different, to appear in *Math. Z.*.

[E3] EREZ B., *Structure galoisienne et forme trace*, Genève, Thèse (1987).

[E-M] EREZ B., MORALES J., The hermitian structure of rings of integers in odd degree abelian extensions, to appear in *J. of Number Theory.*

[E-T] EREZ B., TAYLOR M.J., *Hermitian modules in Galois extensions of number fields and Adams operations*, Preprint (1990).

[F1] FRÖHLICH A., *Galois module structure of algebraic integers*, Ergebnisse der Mathematik, 3, Folge, Bd. 1, Berlin, Springer (1983).

[F2] FRÖHLICH A., Invariants for modules over commutative separable orders, *Quart. J. Math. Oxford*, **16** (1965), 193-232.

[F3] FRÖHLICH A., L-values at zero and multiplicative Galois module structure (also Galois-Gauss sums and additive Galois module structure), *J. Reine und Angew. Math.*, **397** (1989), 42-99.

[K] KERVAIRE M., Opérations d'Adams en théorie des représentations linéaires des groupes finis, *l'Ens. Math.*, T. XXII, 1-28 (1976).

[L] LEOPOLDT H.W., Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, *J. Reine und Angew, Math.*, **201** (1959), 119-149.

[Ma] MARTINET J., Character theory and Artin L-functions, 1-87, in *Algebraic Number Fields*, Proceedings of the Durham Symposium 1975, London, Academic Press (1977).

[Mi1] MIYATA Y., Vertices of ideals of a p-adic number field, *Illinois J. of Math.* (2), **31** (1987), 185-199.

[Mi2] MIYATA Y., Vertices of ideals of a p-adic number field II, Nagoya Math. J., **107**, 49-62 (1987).

[S1] SERRE J.-P., Corps locaux, 3rd edition, Paris, Hermann (1968).

[T1] TAYLOR M.J., Rings of integers and trace forms, Math. Z, **202**, 313-341 (1989).

[T2] TAYLOR M.J., Classgroups of group rings, London Mathematical Society Lecture Note Series 91, Cambridge, Cambridge University Press (1984).

[U1] ULLOM S., Normal bases in Galois extensions of number fields, Nagoya Math. J., **34**, 153-167.

[U2] ULLOM S., Galois cohomology of ambiguous ideals, J. Number Th., **1**, 11-15 (1969).

Boas EREZ
Section de Mathématiques
Université de Genève
2-4, rue du Lièvre
C.P. 240
CH - 1211 GENEVE 24
SUISSE