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 We also give some details concerning the proofs of several results discussed in Section 3 which are not to be published elsewhere.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 $C = \text{center}(FG)$. 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