JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

D. J. BURNS

Factorisability and the arithmetic of wildly ramified Galois extensions

Journal de Théorie des Nombres de Bordeaux 2^e série, tome 1, n° 1 (1989), p. 59-65

<http://www.numdam.org/item?id=JTNB_1989__1_1_59_0>

Séminaire de Théorie des Nombres,
Bordeaux, **1**, *59–66(1989)*

Factorisability and the arithmetic of wildly ramified Galois extensions.

par D.J. BURNS

Introduction

In this note we briefly describe an interesting arithmetical application of a rather novel approach, developed in [2], to the problem of determining the local structure of modules over certain abelian group rings. Proofs are omitted.

To be more precise we introduce some notation. Let K be a finite extension of the field of p-adic rationals for some odd rational prime p. Let L be a finite abelian Galois extension of K and denote by G the Galois group of the extension L/K. We let $\mathcal{O}$ (respectively $\mathcal{O}_L$) denote the ring of integers of K (respectively of L). The group ring KG acts naturally on L and with respect to this action we let $\mathcal{A}(L/K)$ denote the set of elements of KG that induce endomorphisms of $\mathcal{O}_L$. In fact $\mathcal{A}(L/K)$ is an $\mathcal{O}$-order in KG, the so-called 'associated order' of $\mathcal{O}_L$ in KG. It is of much interest to decide the question of whether $\mathcal{O}_L$ is free as an $\mathcal{A}(L/K)$-module. For the sake of brevity we shall henceforth refer to this as 'the structure question (for the extension L/K)'. If the extension L/K is tamely ramified then, by a classical result of Noether, it is known that $\mathcal{O}_L$ is a free $\mathcal{O}G$-module (so that in particular $\mathcal{A}(L/K) = \mathcal{O}G$). However in the wildly ramified case even today there is only a very incomplete theory for associated orders and in particular there are very few general criteria for answering the structure question. In order to apply the techniques developed in [2] to this problem we assume from now on that K satisfies the following hypothesis:

Hypothesis: K is unramified over $\mathbf{Q}_p$.

In this context, as far as we are aware, the only general case which has so far been decided (by Bergé in [1]) is that in which L/K has a cyclic inertia group. The advantage of our approach is that, for *any* given extension L/K satisfying the above conditions, the structure question is reduced to a question that depends only upon the abstract structure of

Manuscrit reçu le 26 janvier 1989

the order $\mathcal{A}(L/K)$. Furthermore this latter question is trivially answered if L/K has a cyclic inertia group (thus recovering the structure results of Bergé) and more generally could be decided by easy computation in any case in which an explicit description of $\mathcal{A}(L/K)$ is known. In particular our techniques demonstrate that the answer to the structure question for the extension L/K is strongly dependent on the (abstract group) structure of G. Moreover taken together our results suggest a complete answer to the structure question for the class of extensions under consideration.

Finally we note that the techniques by which the results of this note are obtained have a number of other arithmetical applications (concerning for example both the module structure of general fractional ideals of L and of unit groups in real abelian number fields) which, for reasons of brevity, are not discussed here.

Notation

In addition to those already introduced we shall adopt the following notations. Γ denotes a finite abelian group. Γ has character group $\Gamma^\dagger$ and for any subgroup Δ of Γ the subgroup of $\Gamma^\dagger$ consisting of characters that are trivial on Δ is denoted by $G(\Delta)$. If X is an $\mathcal{O}\Gamma$-lattice (i.e. an $\mathcal{O}\Gamma$-module that is $\mathcal{O}$-torsion free) then $\mathcal{A}(K\Gamma, X)$ denotes the set of elements of $K\Gamma$ that induce endomorphisms of X. In particular $\mathcal{A}(L/K) = \mathcal{A}(KG, \mathcal{O}_L)$. For any subgroup Δ of Γ the sublattice of X consisting of elements left invariant under the action of Δ is denoted by X^Δ. We regard X^Δ as an $\mathcal{O}(\Gamma/\Delta)$-lattice by means of the usual identification of algebras $K(\Gamma/\Delta) = (K\Gamma)^\Delta$.

1. Preliminary results

Factorisability was originally introduced, by Nelson in [7], in a representation theoretic setting in the context of arbitrary finite groups. However since we are exclusively concerned with abelian groups we use the more elementary approach adopted by Fröhlich in [5].

Let $\mathcal{S}(\Gamma)$ denote the set of subgroups of $\Gamma^\dagger$. To each injective homomorphism

$$\imath : X \longrightarrow Y \otimes_{\mathcal{O}} K \tag{1.1}$$

of $\mathcal{O}\Gamma$-lattices satisfying $\imath X \otimes_{\mathcal{O}} K = Y \otimes_{\mathcal{O}} K$ one associates a function $f(\imath)$ on $\mathcal{S}(\Gamma)$ defined at element $G(\Delta)$ of $\mathcal{S}(\Gamma)$ by

$$f(\imath)(G(\Delta)) = \left[Y^{\Delta} : (\imath X)^{\Delta}\right]_{\mathcal{O}}$$

where $[:]_{\mathcal{O}}$ denotes the $\mathcal{O}$-module index as defined for $\mathcal{O}$-lattices that span the same K-space. (Here in order to compute the index we regard $\imath X$ and Y as embedded in $Y \otimes_{\mathcal{O}} K$).

A division D of $\Gamma^{\dagger}$ is an equivalence class of $\Gamma^{\dagger}$ with characters θ and θ' belonging to the same division if, and only if, they generate the same (cyclic) subgroup of $\Gamma^{\dagger}$. Thus to each division D there corresponds a unique cyclic subgroup of $\Gamma^{\dagger}$ which we shall denote by $\overline{D}$. One extends the definition of $f(\imath)$ to the set of the divisions of $\Gamma^{\dagger}$ by means of the Möbius μ-function:

$$f(\imath)(D) = \prod_{C \leq \overline{D}} \left(f(\imath)(C)\right)^{\mu(|\overline{D}/C|)} \tag{1.2}$$

where the product is taken over all subgroups of $\overline{D}$. To this extended function one then associates a 'factorisable quotient function' $\tilde{f}(\imath)$ defined at each element H of $\mathcal{S}(\Gamma)$ by

$$\tilde{f}(\imath)(H) = \left(f(\imath)(H)\right)^{-1} \cdot \prod_{D \subset H} f(\imath)(D)$$

where the product is taken over all divisions D contained in H. From (1.2) and the Möbius inversion formula it is clear that if H is cyclic then $\tilde{f}(\imath)(H) = \mathcal{O}$. If, more generally, $\tilde{f}(\imath)(H) = \mathcal{O}$ for <u>all</u> elements H of $\mathcal{S}(\Gamma)$ then one says that the function $f(\imath)$ is 'factorisable'. In fact given any other injective homomorphism as in (1.1), $\jmath$ say, it is easy to see that $f(\imath)$ is factorisable if, and only if, $f(\jmath)$ is factorisable. The above procedure thus leads to a natural equivalence relation on the set of $\mathcal{O}\Gamma$-lattices:

DEFINITION Any two $\mathcal{O}\Gamma$-lattices X and Y are said to be 'Γ-*factor-equivalent*' if there exists an injective $\mathcal{O}\Gamma$-homomorphism $\imath$ as in (1.1) for which the associated function $f(\imath)$ is factorisable.

Example 1: As a consequence of Theorem 4A of [6] one knows that, without any hypothesis on ramification, $\mathcal{O}_L$ is G-factor-equivalent to $\mathcal{O}G$.

An easy argument demonstrates that if X and Y are isomorphic then they are Γ-factor-equivalent. On the other hand if we now specialise to the case $\Gamma = G$, $X = \mathcal{O}_L$, and $Y = \mathcal{A}(L/K)$ then the main result of [2] gives precise conditions under which the G-factor-equivalence of $\mathcal{O}_L$ and $\mathcal{A}(L/K)$ is sufficient to imply that they are in fact isomorphic. This result is stated in terms of another equivalence relation on the set of $\mathcal{O}\Gamma$-lattices.

DEFINITION Any two $\mathcal{O}\Gamma$-lattices X and Y are said to be 'Γ-o-*equivalent*', written $X \circ_\Gamma Y$, if for each cocyclic subgroup Δ of Γ the following equality holds:

$$\mathcal{A}\big(K(\Gamma/\Delta), X^\Delta\big) = \mathcal{A}\big(K(\Gamma/\Delta), Y^\Delta\big).$$

Note: A subgroup Δ of Γ is said to be 'cocyclic (in Γ)' if the quotient group Γ/Δ is cyclic.

Remark: By an easy argument if X is isomorphic to Y then $X \circ_\Gamma Y$.

Let $k = k_{L/K}$ denote the natural inclusion map $k : \mathcal{O}G \longrightarrow \mathcal{A}(L/K)$. Combining now the main result of [2] with the result of example 1 gives

THEOREM 1. *$\mathcal{O}_L$ is a free $\mathcal{A}(L/K)$-module if, and only if, both $\mathcal{O}_L \circ_G \mathcal{A}(L/K)$ and $\tilde{f}(k)(G^\dagger) = \mathcal{O}$.*

This result provided the motivation for the present investigation.

2. The main results

By standard functorial arguments the questions of whether $\mathcal{O}_L$ and $\mathcal{A}(L/K)$ are either isomorphic or G-o-equivalent and whether $\mathcal{A}(L/K)$ and $\mathcal{O}G$ are G-factor-equivalent can all be decided on suitable totally ramified extensions. Thus from now on, unless explicitly stated to the contrary, we shall also assume that L is a totally ramified extension of K.

We first consider the case of G-o-equivalence (of $\mathcal{O}_L$ and $\mathcal{A}(L/K)$). Since K is absolutely unramified (and as a consequence of Propositions (4.2) and (4.3) of [4]) the structure of G as an abstract group uniquely determines its

complete ramification filtration. Knowing this one can reduce the question of G-o-equivalence to calculations in the cyclic subextensions of L/K. But for these subextensions one can use the techniques developed by Bergé in §2.2 of [1] and so obtain a complete classification of the conditions under which $\mathcal{O}_L$ and $\mathcal{A}(L/K)$ are G-o-equivalent.

THEOREM 2. *Let G have order $r.p^N$ with r an integer coprime to p.*

(1): If G is cyclic then $\mathcal{O}_L \circ_G \mathcal{A}(L/K)$ if, and only if, either $N \leq 1$, or $N = 2$ and $r < p^2$, or $N \geq 3$ and $r < p(p-1)$.

(2): If G is not cyclic then $\mathcal{O}_L \circ_G \mathcal{A}(L/K)$ if, and only if, $r < p$.

Now from Theorems 1 and 2 the structure question is reduced to the problem of determining the conditions under which $\tilde{f}(k)(G^\dagger)$ vanishes. But if G is cyclic then trivially $\tilde{f}(k)(G^\dagger) = \mathcal{O}$ and hence we immediately deduce

COROLLARY 2.1. *If G is cyclic then $\mathcal{O}_L$ is a free $\mathcal{A}(L/K)$-module if, and only if, G satisfies the conditions of Theorem 2(1).*

Remark Corollary 2.1 is proved by different methods in §§3 and 4 of [1].

More generally $\tilde{f}(k)(G^\dagger)$ could be evaluated by easy computation in any case in which an explicit description of $\mathcal{A}(L/K)$ is known. In particular therefore the structure question for L/K depends only upon the abstract structure of $\mathcal{A}(L/K)$. In fact this is true even if the extension L/K is not totally ramified.

COROLLARY 2.2. *Let L and L' be (not necessarily totally ramified) Galois extensions of K with corresponding Galois groups G and G' respectively. Suppose that there exists an isomorphism of groups $\theta : G \longrightarrow G'$ which, by K-linearity, extends to an isomorphism $\theta : \mathcal{A}(L/K) \longrightarrow \mathcal{A}(L'/K)$ of $\mathcal{O}$-orders. Then $\mathcal{O}_L$ is a free $\mathcal{A}(L/K)$-module if, and only if, $\mathcal{O}_{L'}$ is a free $\mathcal{A}(L'/K)$-module.*

This corollary suggests a number of interesting global questions similar, for example, to those considered by Wilson in [8].

We now turn our attention to the problem of determining the conditions under which $\mathcal{A}(L/K)$ can be G-factor-equivalent to $\mathcal{O}G$ (recall example 1). Let H denote the Sylow p-subgroup of G. Whilst our results are still partial they demonstrate that, just as G-o-equivalence of $\mathcal{O}_L$ and $\mathcal{A}(L/K)$ imposes strong restrictions on the order of the (cyclic) quotient group G/H,

the (abstract group) structure of H is severely restricted by the condition that $\mathcal{A}(L/K)$ and $\mathcal{O}G$ be G-factor-equivalent.

To be more precise we suppose that H has structure invariants

$$(p^{n(1)}, p^{n(2)}, \ldots\ldots\ldots\ldots, p^{n(\lambda)})$$

for some integer λ and integers $n(1), n(2), \ldots, n(\lambda)$ satisfying

$$n(1) \geq n(2) \geq \ldots\ldots\ldots\ldots \geq n(\lambda).$$

PROPOSITION 2.3. *If $\mathcal{A}(L/K)$ is G-factor-equivalent to $\mathcal{O}G$ then $n(1) = n(\lambda)$, i.e. H is a 'homogeneous' group.*

This result is in fact a straightforward consequence of the following Lemma:

LEMMA 2.4. *If $G = H$ is an elementary abelian group then $\mathcal{O}_L$ is isomorphic to $\mathcal{A}(L/K)$ which is generated as an $\mathcal{O}G$-lattice by 1 $(\in G)$ and $p^{-1}(\sum_{g \in G} g)$.*

Furthermore in the slightly more general case that H is an elementary abelian group and $r < p$ more detailed calculations suggest that unless $r = 1$ then $\mathcal{A}(L/K)$ cannot be G-factor-equivalent to $\mathcal{O}G$. (At the moment however we can prove this only for $p = 3$).

At this point, taking account of all of the preceeding results suggests a complete answer to the structure question for the class of extensions that we are considering:

CONJECTURE 2.5. *Under the above conditions $\mathcal{O}_L$ is a free $\mathcal{A}(L/K)$-module if, and only if, either*

(1): G is cyclic and satisfies the conditions of Theorem 2(1), or

(2): G is an elementary abelian p-group.

Indeed given Theorem 2, Corollary 2.1, Proposition 2.3, and Lemma 2.4 together with the remarks following it, Conjecture 2.5 is very closely related to

CONJECTURE 2.5′. *Under the above conditions if $\mathcal{O}_L$ is a free $\mathcal{A}(L/K)$-module then the same is true for every subextension L'/K.*

Finally we remark that similar (but slightly weaker) results can be obtained by the same techniques in the case that $p = 2$. However, for any residue characteristic, if we allow absolute ramification in the basefield K then the results are of course very different (for example see [3]).

REFERENCES

1. A-M.Bergé, *Arithmétique d'une extension à groupe d'inertie cyclique*, Ann. Inst. Fourier **28** (1978), 17–44..
2. D.Burns, *Factorisabilty, group lattices, and Galois module structure.* to appear in Jnl. of Algebra.
3. M-J.Ferton, *Sur les idéaux d'une extension cyclique de degré premier d'un corps local*, C.R.A.S. (1973). série A.
4. J-M.Fontaine, *Groupes de ramification et représentations d'Artin*, Ann. Scient. Ec. Norm. Sup. **4** (1971), 337–392. 4-eme série.
5. A.Fröhlich, *Module defect and factorisability*, Illinois Jnl. Math. **32.3** (1988), 407–421.
6. A.Fröhlich, *L-values at zero and multiplicative Galois module structure.* to appear in Jnl. reine und angew. Math.
7. A.Nelson, *Monomial representations and Galois module structure*, Ph.D Thesis. King's College, University of London, 1979.
8. S.M.J.Wilson, *Structure Galoisienne et ramification sauvage*, Sém. de Théorie des Nombres de Bordeaux (1986–1987).