JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

D. BURNS

On the Galois structure of the square root of the codifferent

Journal de Théorie des Nombres de Bordeaux, tome 3, n° 1 (1991), p. 73-92

<http://www.numdam.org/item?id=JTNB_1991__3_1_73_0>

Séminaire de Théorie des Nombres,
Bordeaux **3** *(1991), 73-92*

On the Galois structure of the square root of the codifferent.

par D. BURNS

Résumé — Soit L une extension abélienne finie de $\mathbb{Q}$, et $\mathcal{O}_L$ son anneau des entiers. Nous poursuivons l'étude du seul idéal fractionnaire de $\mathcal{O}_L$ qui (s'il existe) est unimodulaire pour la forme trace de $L/\mathbb{Q}$.

Abstract — *Let L be a finite abelian extension of $\mathbb{Q}$, with $\mathcal{O}_L$ the ring of algebraic integers of L. We investigate the Galois structure of the unique fractional $\mathcal{O}_L$ -ideal which (if it exists) is unimodular with respect to the trace form of $L/\mathbb{Q}$.*

Introduction

Let L be a finite Galois extension of the field of rationals $\mathbb{Q}$, and let G_L denote the Galois group $\mathrm{Gal}(L/\mathbb{Q})$. Letting $\mathcal{O}_L$ denote the ring of algebraic integers of L we henceforth *assume* that there exists a fractional $\mathcal{O}_L$-ideal A_L the square of which is the codifferent of the extension $L/\mathbb{Q}$. (This is a mild condition on the ramification of $L/\mathbb{Q}$ which is certainly satisfied if, for example, $L/\mathbb{Q}$ has odd degree.) This ideal A_L is therefore ambiguous, i.e. it admits an action of $\mathbb{Z}[G_L]$, and is in fact the unique fractional $\mathcal{O}_L$-ideal which is unimodular with respect to the G_L-equivariant $\mathbb{Z}$-bilinear form $Tr_L : A_L \times A_L \to \mathbb{Z}$ which is given by

$$Tr_L : (x, y) \mapsto |\mathrm{trace}|_{L/\mathbb{Q}}(xy).$$

There is by now a considerable literature dedicated to the problem of determining the structure of the Hermitian-Galois module (A_L, Tr_L) over $\mathbb{Z}[G_L]$. Most notably, this structure *(inter alia)* has been explicitly described by Erez and Taylor [9] in the case that $L/\mathbb{Q}$ is at most tamely ramified, and by Bachoc and Erez [3] and Bachoc [1] under certain less restrictive ramification hypotheses but with the condition that G_L be abelian. In this note we are not concerned with Hermitian structure and shall only study the

1980 *Mathematics Subject Classification* (1985 *Revision*). 11R33.
Mots clefs: corps de nombres, formes quadratiques entières.
Manuscrit reçu le 30 octobre 1990 .

structure of A_L as Galois module in the case G_L abelian but without any ramification hypotheses on $L/\mathbb{Q}$ (other than that A_L exists). In fact Bachoc has recently shown that the description of Galois structure which we shall give here is for a large class of abelian extensions $L/\mathbb{Q}$ actually sufficient to determine uniquely the full Hermitian-Galois structure of (A_L, Tr_L) over $\mathbb{Z}[G_L]$ (her results are to appear in [2]). *Henceforth therefore G_L is abelian.* In this case A_L is known to be locally-free as a module over an explicitly described $\mathbb{Z}$-order $\mathcal{A}_L \subset \mathbb{Q}[G_L]$([8], Theorem 3.1) and so it defines a class (A_L) in the locally-free class group $\mathrm{Cl}(\mathcal{A}_L)$ of $\mathcal{A}_L$-modules. Letting $\mathcal{M}_L$ denote the maximal $\mathbb{Z}$-order in $\mathbb{Q}[G_L]$ we shall here explicitly describe the image of $(\mathcal{A}_L)$ under the natural surjective map

$$\pi_L : C\ell(\mathcal{A}_L) \to C\ell(\mathcal{M}_L)$$

which is induced by the map defined on each locally-free $\mathcal{A}_L$- module X by

$$X \mapsto X \otimes_{\mathcal{A}_L} \mathcal{M}_L \cong X\mathcal{M}_L.$$

Our description of $\pi_L(A_L)$ will be given in terms of the standard Hom-description of $C\ell(\mathcal{M}_L)$ (to be recalled in §1). As a particular consequence we shall prove that, given any rational integer N, there are infinitely many fields L as above for which the order of the class $\pi_L(A_L)$ (and hence also that of the class (A_L)) exceeds N. This is a striking result given the strong analogies between the Hermitian-Galois structures of (A_L, Tr_L) and $(\mathcal{O}_L, Tr_L)$ which are valid under the hypothesis of tameness (c.f. [8], Theorem 1.3) together with the fact that, without any ramification hypotheses, $\mathcal{O}_L$ is always free over an explicitly described $\mathbb{Z}$-order in $\mathbb{Q}[G_L]$ (this is the famous Hauptsatz of Leopoldt [12] (for a simple proof of which see Lettl [13])). Specifically therefore it follows that the (techniques and) results of [1] and [3] are no longer valid after any weakening of the ramification hypotheses imposed there. Nevertheless our description does give a uniformity-type result more general (but weaker) than that of Théorème 0.3 of [3].

Acknowledgements : The author would like to thank Christine Bachoc and Boas Erez for many stimulating conversations. Also, the final version of this note was written whilst he benefitted from the generosity and warm hospitality of the Institut für Mathematik der Universität Augsburg, Germany.

Notations : We fix an algebraic closure $\mathbb{Q}^c$ of $\mathbb{Q}$, and for each rational prime p, an algebraic closure $\mathbb{Q}_p^c$ of the field of p-adic rationals $\mathbb{Q}_p$. We

let $\Omega_{\mathbb{Q}}$ (respectively $\Omega_{\mathbb{Q}_p}$) denote the absolute Galois group $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ (respectively $\mathrm{Gal}(\mathbb{Q}_p^c/\mathbb{Q}_p)$). For any finite extension L of $\mathbb{Q}$ (respectively $\mathbb{Q}_p$) which is contained in $\mathbb{Q}^c$ (respectively $\mathbb{Q}_p^c$) we let $\mathcal{O}_L$ denote the ring of algebraic integers (respectively valuation ring) of L, $\mathcal{I}_L$ the group of fractional $\mathcal{O}_L$-ideals, $\mathcal{P}r_L$ the subgroup of $\mathcal{I}_L$ consisting of principal fractional $\mathcal{O}_L$-ideals, and $C\ell_L$ the ideal class group $\mathcal{I}_L/\mathcal{P}r_L$ of L. For any such fields $K \subseteq L$ we shall often identify the group $\mathcal{I}_K$ with a subgroup of $\mathcal{I}_L$ in the usual way (i.e. via inflation of ideals).

1 - The 'Hom-description' of $C\ell(\mathcal{M}_L)$.

Our description of the class $\pi_L(A_L)$ uses the characterisation of $C\ell(\mathcal{M}_L)$ in terms of $\Omega_{\mathbb{Q}}$-equivariant homomorphisms defined on the set of irreducible $\mathbb{Q}^c$-valued characters of G_L. For the reader's convenience we shall in this section briefly recall this 'Hom-description' of $C\ell(\mathcal{M}_L)$. (For a thorough discussion of this description as applied to the locally-free class group $C\ell(\mathcal{A})$ of any $\mathbb{Z}$-order $\mathcal{A}$ of $\mathbb{Q}[G_L]$ the reader is referred to Chapters 1 and 2 of [10].)

We now let Γ denote an arbitrary finite abelian group, with $\Gamma^\dagger$ its multiplicative character group $\mathrm{Hom}(\Gamma, \mathbb{Q}^{c\star})$. A *division* of $\Gamma^\dagger$ is then an equivalence class of characters under the relation of $\Omega_{\mathbb{Q}}$-conjugacy. For each character $\theta \in \Gamma^\dagger$ we let $\mathbb{Q}(\theta)$ denote the field extension of $\mathbb{Q}$ generated by the set $\{\theta(\gamma) : \gamma \in \Gamma\}$. This field only depends upon the division D to which θ belongs and accordingly we shall frequently denote it $\mathbb{Q}(D)$, with $\mathbb{Z}[D] = \mathcal{O}_{\mathbb{Q}(D)} (= \mathbb{Z}[\theta])$. For each character $\theta \in \Gamma^\dagger$ we define an idempotent e_θ of the $\mathbb{Q}(\theta)$-algebra $\mathbb{Q}(\theta)[\Gamma]$ by

$$e_\theta = \frac{1}{\#\Gamma} \sum_{\gamma \in \Gamma} \theta(\gamma^{-1})\gamma,$$

and for each division D of $\Gamma^\dagger$ we then define an idempotent e_D of $\mathbb{Q}[\Gamma]$ by

$$e_D = \sum_{\theta \in D} e_\theta.$$

The maximal $\mathbb{Z}$-order of $\mathbb{Q}[\Gamma]$ is then

$$\mathcal{M}_\Gamma = \bigoplus_D \mathbb{Z}[\Gamma] e_D \tag{1}$$

with the sum taken over all divisions D of $\Gamma^\dagger$. Corresponding to the decomposition (1) there is a direct sum decomposition of any $\mathcal{M}_\Gamma$-module X as

$$X = \bigoplus_D X e_D,$$

and hence we need only describe the structure of lattices over each of the rings $\mathcal{M}_D := \mathbb{Z}[\Gamma]e_D$. Now for each division D the ring $\mathcal{M}_D$ naturally identifies with the Dedekind domain $\mathbb{Z}[D]$. The structure of each finitely generated $\mathcal{M}_D$- lattice is thus determined up to isomorphism by its rank and *Steinitz class* (c.f. Theorem (4.13) of [14]). The *Steinitz class* $(X_D)_D$ of an $\mathcal{M}_D$-lattice X_D is the element of the ideal class group $C\ell_D$ of the ring $\mathcal{M}_D$ which is characterised by

(2)(i) $\qquad (Y_D)_D = 1 \quad$ if Y_D is a free $\mathcal{M}_D$ – *lattice*

and, if X_D and Y_D are $\mathcal{M}_D$-lattices which span the same $\mathbb{Q}[\Gamma]e_D$-space, then

(2)(ii) $\qquad (X_D)_D(Y_D)_D^{-1}$ is the element of $C\ell_D$ generated by the ideal $[Y_D : X_D]_{\mathcal{M}_D}$,

where here $[:]_{\mathcal{M}_D}$ denotes the $\mathcal{M}_D$-module index as defined for any two $\mathcal{M}_D$-lattices which span the same $\mathbb{Q}[\Gamma]e_D$-space. Next, we introduce the character functions which will describe the locally-free class group $C\ell(\mathcal{M}_D)$ of the ring $\mathcal{M}_D$. We consider functions g on D with values in the group $\mathcal{I}_D$ of $\mathbb{Z}[D]$-fractional ideals, and such that

$$g(\theta^\omega) = g(\theta)^\omega,$$

for each character $\theta \in \Gamma^\dagger$ and each element $\omega \in \Omega_\mathbb{Q}$. Such functions form a multiplicative group $I_{\mathbb{Q},D}$. We let I_D denote the group of fractional $\mathcal{M}_D$-ideals. There is then an isomorphism

(3) $$I_D \overset{\mathcal{R}}{\cong} I_{\mathbb{Q},D}.$$

To describe this isomorphism note that any character $\theta \in D$ extends by $\mathbb{Q}$-linearity to give an isomorphism $\mathbb{Q}[\Gamma]e_D \cong \mathbb{Q}(D)$ which we shall denote by $\tilde{\theta}$. Then for any ideal $\mathfrak{b} \in I_D$, the function $\mathcal{R}(\mathfrak{b})$ is defined at each character $\theta \in D$ by

$$\mathcal{R}(\mathfrak{b})(\theta) = \tilde{\theta}(\mathfrak{b}).$$

To give an example, for any character $\theta \in \Gamma^\dagger$ and any $\mathbb{Z}[\theta]$-lattice Z, we let Z^θ denote the θ-isotypic component of Z which is defined by

$$Z^\theta = Z \cap Ze_\theta.$$

LEMMA 4. *If X_D and Y_D are any $\mathcal{M}_D$ lattices (which span the same $\mathbb{Q}[\Gamma]e_D$-space) then, at each character $\theta \in D$, one has*

$$\mathcal{R}([X_D : Y_D]_{\mathcal{M}_D})(\theta) = [(X_D \otimes_{\mathbb{Z}} \mathbb{Z}[D])^\theta : (Y_D \otimes_{\mathbb{Z}} \mathbb{Z}[D])^\theta]_{\mathbb{Z}[D]}.$$

Proof : Exercise.

Now, if $Pr_{\mathbb{Q},D}$ denotes the subgroup of $I_{\mathbb{Q},D}$ consisting of those functions g which only take values in $\mathcal{P}r_{\mathbb{Q}(D)}$, then the isomorphism (3) induces an isomorphism

$$C\ell(\mathcal{M}_D) \cong I_{\mathbb{Q},D}/Pr_{\mathbb{Q},D} \tag{5}$$

which we shall denote by $\tilde{\mathcal{R}}$. It is thus natural to say that an element $\mathcal{C} \in C\ell(\mathcal{M}_D)$ is 'represented by' a function $g \in I_{\mathbb{Q},D}$ if the class of g modulo $Pr_{\mathbb{Q},D}$ corresponds to $\mathcal{C}$ under the isomorphism $\tilde{\mathcal{R}}$.

2 - Some reduction steps

In this section we shall reduce the explicit description of the Galois structure of $A_L\mathcal{M}_L$ to a local computation. We here fix L and set $G = G_L, \mathcal{M} = \mathcal{M}_L$, and $C\ell(L) = C\ell(\mathcal{M})$. For any (right) $\mathbb{Z}[G]$-lattice X we shall let $X^\wedge$ denote the $\mathbb{Z}$-linear dual-lattice $Hom_{\mathbb{Z}}(X, \mathbb{Z})$ considered as a (right) $\mathbb{Z}[G]$-lattice in the usual fashion. For any such lattice X we write $X^{\mathcal{M}}$ for the maximal sublattice of X which admits an action of $\mathcal{M}$.

LEMMA 6 ([3], PROPOSITION 2.1 (1)). *The $\mathcal{M}$-lattices $A_L\mathcal{M}$ and $(A_L^{\mathcal{M}})^\wedge$ are naturally identified by means of the trace form of $L/\mathbb{Q}$.*

Thus to describe the structure of $A_L\mathcal{M}$ it suffices to describe that of $A_L^{\mathcal{M}}$. Note further that, since $\mathcal{M}^\wedge$ is $\mathcal{M}$- isomorphic to $\mathcal{M}$, the classes of the lattices $A_L\mathcal{M}$ and $A_L^{\mathcal{M}}$ in $C\ell(L)$ have the same order. In the remainder of this note we are therefore content to give an explicit description of the class of $A_L^{\mathcal{M}}$ in $C\ell(L)$.

LEMMA 7 (c.f. [6], THEOREM 2.1 and LEMMA 2.3) $\mathcal{O}_L^{\mathcal{M}} \cong \mathcal{M}$.

Therefore, by using (2), Lemma 4, and the isomorphism $\tilde{R}$ of (5), to describe the class of $A_L^{\mathcal{M}}$ in $C\ell(L)$ it suffices to explicitly describe the function defined on $G^\dagger$ by

$$g : \theta \mapsto [(\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}[\theta])^\theta : (A_L \otimes_{\mathbb{Z}} \mathbb{Z}[\theta])^\theta]_{\mathbb{Z}[\theta]}.$$

For each rational prime p we define a function $g_{(p)}$ on $G^\dagger$ by

$$g_{(p)} : \theta \mapsto \text{ the } p - \text{primary part of the ideal } g(\theta)$$

so that

$$g = \prod_p g_{(p)},$$

and we shall compute each function $g_{(p)}$ seperately. For this we need to know the localisation properties of the $\mathbb{Z}[G]$-lattices A_L and $\mathcal{O}_L$. Thus we now fix a rational prime p and let I_p (or simply I whenever the prime p is clear from context) denote the inertia subgroup of G corresponding to p. We set $K = L^I$. We fix a prime $\mathcal{O}_L$-ideal $\mathcal{P}$ of residue characteristic p, and we set $\mathfrak{p} = \mathcal{P} \cap K$. We let F (respectively E) denote the local completion of L (respectively K) at the place corresponding to $\mathcal{P}$ (respectively $\mathfrak{p}$), and we set $\mathcal{O} = \mathcal{O}_F, A = A_{F/\mathbb{Q}_p}$, and $\tilde{\mathcal{O}} = \mathcal{O}_E$. We let D denote the decomposition subgroup of p in G and, in the usual fashion, we identify this with $\mathrm{Gal}(F/\mathbb{Q}_p)$.

Now, as is well known, there is a canonical $\mathbb{Q}_p[G]$-module isomorphism

$$\alpha : L \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong F \otimes_{\mathbb{Q}_p[D]} \mathbb{Q}_p[G]$$

which restricts to give both

$$\alpha(\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \mathcal{O} \otimes_{\mathbb{Z}_p[D]} \mathbb{Z}_p[G]$$

and

$$\alpha(A_L \otimes_{\mathbb{Z}} \mathbb{Z}_p) = A \otimes_{\mathbb{Z}_p[D]} \mathbb{Z}_p[G].$$

(Concerning A_L see for example Proposition 7, Chapter 3 of [11].) Furthermore, since D is abelian, in [5] Bergé has described an $E[D]$-module isomorphism

$$\beta : F \otimes_{\mathbb{Q}_p} E \cong F \otimes_{E[I]} E[D]$$

which restricts to give

$$\beta(\mathcal{O} \otimes_{\mathbb{Z}_p} \tilde{\mathcal{O}}) = \mathcal{O} \otimes_{\tilde{\mathcal{O}}[I]} \tilde{\mathcal{O}}[D]$$

and also (although not explicitly mentioned in [5])

$$\beta(A \otimes_{\mathbb{Z}_p} \tilde{\mathcal{O}}) = A \otimes_{\tilde{\mathcal{O}}[I]} \tilde{\mathcal{O}}[D].$$

Thus one has

LEMMA 8. *The E[G]-module isomorphism*

$$\gamma = \beta \circ \alpha : L \otimes_{\mathbb{Q}} E \cong F \otimes_{F[\Gamma]} E[G]$$

restricts to give both

$$\gamma(\mathcal{O}_L \otimes_{\mathbb{Z}} \tilde{\mathcal{O}}) = \mathcal{O} \otimes_{\tilde{\mathcal{O}}[\Gamma]} \tilde{\mathcal{O}}[G]$$

and

$$\gamma(A_L \otimes_{\mathbb{Z}} \tilde{\mathcal{O}}) = A \otimes_{\tilde{\mathcal{O}}[\Gamma]} \tilde{\mathcal{O}}[G].$$

To proceed we now set $I^{\dagger}_{\mathrm{loc}} = Hom(I, \mathbb{Q}_p^{c\star})$. We define a function g_p on $I^{\dagger}_{\mathrm{loc}}$ by

$$g_p(\phi) = [(\mathcal{O} \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\phi])^{\phi} : (A \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\phi])^{\phi}]_{\tilde{\mathcal{O}}[\phi]}$$

for each character $\phi \in I^{\dagger}_{\mathrm{loc}}$.

LEMMA 9. *For each rational prime p, each embedding $\jmath : \mathbb{Q}^c \hookrightarrow \mathbb{Q}_p^c$, and each character $\theta \in G_L^{\dagger}$ one has*

$$\overline{g_{(p)}(\theta)^{\jmath}} = g_p(res^G_{I_p}(\theta)^{\jmath})$$

(where here the bar indicates closure with respect to the p-adic topology).

Proof : One has

$$\overline{g_{(p)}(\theta)^{\jmath}} = [(\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}[\theta])^{\theta} : (A_L \otimes_{\mathbb{Z}} \mathbb{Z}[\theta])^{\theta}]_{\mathbb{Z}[\theta]} \otimes_{\mathbb{Z}[\theta],\jmath} \mathbb{Z}_p[\theta^{\jmath}]$$

(where here $\otimes_{\mathbb{Z}[\theta],\jmath}$ indicates that the tensor product is taken with $\mathbb{Z}_p[\theta^{\jmath}]$ considered as a $\mathbb{Z}[\theta]$-module via the embedding $\jmath : \mathbb{Z}[\theta] \hookrightarrow \mathbb{Z}_p[\theta^{\jmath}]$). Now if X (respectively X') denotes either $\mathcal{O}_L$ or A_L (respectively either $\mathcal{O}$ or A) then

$$(X \otimes_{\mathbb{Z}} \mathbb{Z}[\theta])^{\theta} \otimes_{\mathbb{Z}[\theta],\jmath} \tilde{\mathcal{O}}[\theta^{\jmath}] = ((X \otimes_{\mathbb{Z}} \tilde{\mathcal{O}}) \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\theta^{\jmath}])^{\theta^{\jmath}}$$

and, via the isomorphism γ of Lemma 8, this is $\tilde{\mathcal{O}}[\theta^{\jmath}][G]$- isomorphic to

$$((X' \otimes_{\tilde{\mathcal{O}}[\Gamma]} \tilde{\mathcal{O}}[G]) \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\theta^{\jmath}])^{\theta^{\jmath}}.$$

Thus, setting $\phi = \mathrm{res}^G_I(\theta)^{\jmath}$ $(= \mathrm{res}^G_I(\theta^{\jmath})$ one has

$$\begin{aligned}
\overline{g_{(p)}(\theta)^{\jmath}} &= [(\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}[\theta])^{\theta} : (A_L \otimes_{\mathbb{Z}} \mathbb{Z}[\theta])^{\theta}]_{\mathbb{Z}[\theta]} \otimes_{\mathbb{Z}[\theta],\jmath} \mathbb{Z}_p[\theta^{\jmath}] \\
&= [(((\mathcal{O} \otimes_{\tilde{\mathcal{O}}[\Gamma]} \tilde{\mathcal{O}}[G]) \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\theta^{\jmath}])^{\theta^{\jmath}} : ((A \otimes_{\tilde{\mathcal{O}}[\Gamma]} \tilde{\mathcal{O}}[G]) \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\theta^{\jmath}])^{\theta^{\jmath}}]_{\tilde{\mathcal{O}}[\theta^{\jmath}]} \\
&= [(\mathcal{O} \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\phi])^{\phi} : (A \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\phi])^{\phi}]_{\tilde{\mathcal{O}}[\phi]} \\
&= g_p(\phi).
\end{aligned}$$

LEMMA 10. *If* $\mathrm{res}^G_{I_p}(\theta)$ *has* p*-power order then* $g_{(p)}(\theta) \in \mathcal{P}r_{\mathbb{Q}(\theta)}$.

Proof : If $\phi = \mathrm{res}^G_{I_p}(\theta)$ has p-power order then, for any embeddings $\jmath_1, \jmath_2 : \mathbb{Q}^c \hookrightarrow \mathbb{Q}_p^c$ there exists an automorphism $\eta \in \Omega_{\mathbb{Q}_p}$ such that $\phi^{\jmath_1} = \phi^{\jmath_2 \circ \eta}$. Hence, by using Lemma 9,

$$\begin{aligned}\overline{g_{(p)}(\theta)^{\jmath_1}} &= g_p(\phi^{\jmath_1}) \\ &= g_p(\phi^{\jmath_2 \circ \eta}) \\ &= g_p(\phi^{\jmath_2})^{\eta} \\ &= g_p(\phi^{\jmath_2}) \\ &= \overline{g_{(p)}(\theta)^{\jmath_2}}.\end{aligned}$$

Hence $g_p(\theta)$ is inflated from a p-primary ideal in a cyclotomic field of p-power conductor and is therefore an element of $\mathcal{P}r_{\mathbb{Q}(\theta)}$.

Note that I_2 is a 2-group and so in particular Lemma 10 implies that

$$g_{(2)}(\theta) \in \mathcal{P}r_{\mathbb{Q}(\theta)} \text{ for each character } \theta \in G^{\dagger}_{L}. \tag{11}$$

Thus we need only describe $g_{(p)}$ for an odd prime p. In this case I is a cyclic group of order $p^n r$ say, with $n \geq 0$ and r an odd divisor of $p-1$ (r must be odd in order that A exists). We let P denote the Sylow p-subgroup of I with C the unique subgroup of I of order r. The direct product decomposition $I = P \times C$ leads to a corresponding decomposition of the local character groups $I^{\dagger}_{\mathrm{loc}} = P^{\dagger}_{\mathrm{loc}} \times C^{\dagger}_{\mathrm{loc}}$. For each character $\phi \in \mathcal{I}^{\dagger}_{\mathrm{loc}}$ we set $\phi_P = \phi|_P \in P^{\dagger}_{\mathrm{loc}}$ and $\phi_C = \phi|_C \in C^{\dagger}_{\mathrm{loc}}$ so that $\phi = \phi_P \times \phi_C$. For each $\psi \in P^{\dagger}_{\mathrm{loc}}$ and $\lambda \in C^{\dagger}_{\mathrm{loc}}$ we define idempotents

$$e_{\psi} = \frac{1}{p^n} \sum_{\rho \in P} \psi(\rho^{-1})\rho \in \mathbb{Q}_p(\psi)[P]$$

and

$$e_{\lambda} = \frac{1}{r} \sum_{\kappa \in C} \lambda(\kappa^{-1})\kappa \in \mathbb{Z}_p[C].$$

For each non-negative integer $i \leq n$ we let P_i denote the subgroup of P of order p^i, so that in particular $P_n = P$. For each such integer i we let e_i denote the idempotent

$$e_i = \frac{1}{p^i} \sum_{\gamma \in P_i} \gamma = \sum_{\substack{\psi \in P^{\dagger}_{\mathrm{loc}} \\ \psi(P_i)=1}} e_{\psi} \in \mathbb{Q}_p[P]$$

and for convenience we also set $e_{n+1} = 0$. For any (right) $\mathbb{Z}[I]$-lattice X and subgroup $H \leq I$ we let X^H denote the sublattice of X consisting of those elements which are invariant under the action of each element of H. We let $\mathcal{N}$ denote the maximal $\tilde{\mathcal{O}}$-order of the E-algebra $E[I]$. Finally, for any integer n we let $\Phi(n)$ denote the order of the multiplicative group $R_n = (\mathbb{Z}/n\mathbb{Z})^\star$.

LEMMA 12. *If $\phi \in I^\dagger_{\mathrm{loc}}$ has order $p^i r'$ with $i \leq n$ and $r' | r$ then, setting $\lambda = \phi_C$ and $j = n - i$, one has*

$$g_p(\phi)^{\Phi(p^i)} = \frac{[(\mathcal{O}^{\mathcal{N}})^{P_j} e_\lambda : (A^{\mathcal{N}})^{P_j} e_\lambda]_{\tilde{\mathcal{O}}}}{[(\mathcal{O}^{\mathcal{N}})^{P_{j+1}} e_\lambda : (A^{\mathcal{N}})^{P_{j+1}} e_\lambda]_{\tilde{\mathcal{O}}}}$$

where here we set

$$[(\mathcal{O}^{\mathcal{N}})^{P_{n+1}} e_\lambda : (A^{\mathcal{N}})^{P_{n+1}} e_\lambda]_{\tilde{\mathcal{O}}} = \tilde{\mathcal{O}}.$$

Proof: Since $E/\mathbb{Q}_p$ is unramified one has $E \cap \mathbb{Q}_p(\phi) = \mathbb{Q}_p$ and so letting D_ϕ denote the division of $P^\dagger_{\mathrm{loc}}$ to which ϕ_P belongs then

$$\begin{aligned} g_p(\phi)^{\Phi(p^i)} &= \mathrm{Norm}_{E(\phi)/E}(g_p(\phi)) \\ &= \prod_{\eta \in \mathrm{Gal}(E(\phi)/E)} g_p(\phi)^\eta \\ &= \prod_{\eta \in \mathrm{Gal}(E(\phi)/E)} g_p(\phi^\eta) \\ &= \prod_{\psi \in D_\phi} g_p(\psi \times \lambda) \\ &= \prod_{\psi \in D_\phi} [(\mathcal{O} \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\psi])^\psi e_\lambda : (A \otimes_{\tilde{\mathcal{O}}} \tilde{\mathcal{O}}[\psi])^\psi e_\lambda]_{\tilde{\mathcal{O}}[\psi]} \\ &= [\mathcal{O}^{\mathcal{N}(e_j - e_{j+1})} e_\lambda : A^{\mathcal{N}(e_j - e_{j+1})} e_\lambda]_{\tilde{\mathcal{O}}}. \end{aligned} \tag{13}$$

But for any (right) $\tilde{\mathcal{O}}[I]$-lattice X and any character $\lambda \in C^\dagger_{\mathrm{loc}}$ one has a short exact sequence of $\tilde{\mathcal{O}}$-lattices

$$0 \to X^{\mathcal{N}(e_j - e_{j+1})} e_\lambda \to X^{\mathcal{N}} e_j e_\lambda \xrightarrow{\cdot e_{j+1}} X^{\mathcal{N}} e_{j+1} e_\lambda \to 0$$

with the third arrow indicating multiplication by e_{j+1}. Thus the expression (13) is equal to

$$\frac{[(\mathcal{O}^{\mathcal{N}}) e_j e_\lambda : (A^{\mathcal{N}}) e_j e_\lambda]_{\tilde{\mathcal{O}}}}{[(\mathcal{O}^{\mathcal{N}}) e_{j+1} e_\lambda : (A^{\mathcal{N}}) e_{j+1} e_\lambda]_{\tilde{\mathcal{O}}}} = \frac{[(\mathcal{O}^{\mathcal{N}})^{P_j} e_\lambda : (A^{\mathcal{N}})^{P_j} e_\lambda]_{\tilde{\mathcal{O}}}}{[(\mathcal{O}^{\mathcal{N}})^{P_{j+1}} e_\lambda : (A^{\mathcal{N}})^{P_{j+1}} e_\lambda]_{\tilde{\mathcal{O}}}}.$$

3 - The local calculation

In order to describe the class of $A_L\mathcal{M}_L$ in $C\ell(L)$ it suffices, by using the work of §2, to determine the behaviour of each of the lattices $A^{\mathcal{N}}e_\lambda$ and $\mathcal{O}^{\mathcal{N}}e_\lambda$ under fixing by the subgroups P_i for all non-negative integers $i \leq n$, and for all characters $\lambda \in C^\dagger_{\mathrm{loc}}$. Since $E/\mathbb{Q}_p$ is unramified we can here use the techniques of Bergé developed in [4]. For each non-negative integer $i \leq n$ we set $F_i = F^{P_i}, \mathcal{O}_i = \mathcal{O}_{F_i}$, and we let v_i denote the valuation of the field F_i. To be more precise concerning the character group $C^\dagger_{\mathrm{loc}}$ we fix a uniformising parameter π for F. The map defined on I by $\gamma \mapsto \pi\gamma/\pi$ induces an isomorphism θ_0 (which is independent of the choice of π) between C and a subgroup of the roots of unity of the residue class field of E. We let $\chi_{F/E}$ denote the (unique) element of $C^\dagger_{\mathrm{loc}}$ which induces by passage to the residue class field the isomorphism θ_0. Then $\chi_{F/E}$ is a generator of $C^\dagger_{\mathrm{loc}}$, and hence to each character $\chi \in C^\dagger_{\mathrm{loc}}$ one can associate an integer $u_\chi \in \{1, 2, ..., r\}$ defined by

$$\chi = (\chi_{F/E})^{-u_\chi}. \tag{14}$$

Given the above definition of $\chi_{F/E}$ the following lemma is not difficult to prove.

LEMMA 15 (c.f. [4], PROPOSITION 1). *Let χ be an element of $C^\dagger_{\mathrm{loc}}$. For any (non-zero) element $x \in F$ one has*

$$v_0(xe_\chi) \geq v_0(x),$$

with equality here if and only if $v_0(x) \equiv -u_\chi$ modulo (r). In particular, for each integer $i \in \{0, 1, 2, ..., n\}$ if $xe_\chi e_i$ is non-zero then

$$v_i(xe_\chi e_i) \equiv -u_\chi \ modulo(r).$$

LEMMA 16. *For each integer $i \in \{0, 1, ..., n\}$ one has $(\mathcal{O}^{\mathcal{N}})^{P_i} = \mathcal{O}^{P_i} = \mathcal{O}_i$.*

Proof : This is obvious since $\mathcal{O}^{\mathcal{N}} = \mathcal{O}$ ([4], Théorème 1).

Since $E/\mathbb{Q}_p$ is unramified the complete ramification filtration of I is known and so, by means of Hilbert's formula ([15], Chapitre IV.1, Proposition 4), one can explicitly compute the valuation $v_0(A)$. The techniques of Bergé ([4],§2.2) then easily prove

LEMMA 17. *(i) If $\lambda \in C^{\dagger}_{\mathrm{loc}}$ is not trivial then $A^{\mathcal{N}} e_\lambda = A e_\lambda$.*

(ii) : If $i \in \{0, 1, .., n\}$ is even then $A e_i = A^{P_i}$.

Remark : Lemma 17(ii) is also a consequence of Proposition 2.3(4) of [3].

For each integer $i \in \{0, 1, ..n\}$ the lattice A^{P_i} identifies with a fractional $\mathcal{O}_i$-ideal which can also be explicitly computed. However, for our purposes it is sufficient to note the following.

LEMMA 18. *For each $i \in \{0, 1, .., n-1\}$ one has*

$$v_i(A^{P_i}) \equiv \begin{cases} \frac{1}{2}(1+r) \text{ modulo } (pr), & \text{if } i \text{ is even ;} \\ 1 \text{ modulo } (r), & \text{if } i \text{ is odd.} \end{cases}$$

One also has

$$v_n(A^{P_n}) \equiv \begin{cases} \frac{1}{2}(1+r) \text{ modulo } (r), & \text{if } n \text{ is even ;} \\ 1 \text{ modulo } (r), & \text{if } n \text{ is odd.} \end{cases}$$

Proof : If $i = 2j+1 \leq n$ then the claimed result for i follows easily from that for $2j$. On the other hand if $i = 2j \leq n$ then $A e_i = A^{P_i}$ (Lemma 17 (ii)), and using the characterisation of $A_{F_i/\mathbb{Q}_p}$ as the unique fractional $\mathcal{O}_i$- ideal which is unimodular with respect to the trace form of $F_i/\mathbb{Q}_p$ this implies that $A^{P_i} = p^{-j} A_{F_i/\mathbb{Q}_p}$. (By an induction on n) it therefore suffices to prove the claimed results only for the case $i = 0$, and in this special case the result is easily verified using the explicit formula of Hilbert mentioned above.

LEMMA 19. *Let $\lambda \in C^{\dagger}_{\mathrm{loc}}$ be non-trivial. If $i \in \{0, 1, ..n\}$ is odd then*

$$[\mathcal{O}^{P_i} e_\lambda : A^{P_i} e_\lambda]_{\tilde{\mathcal{O}}} = \mathfrak{p}^{a_i}$$

for an explicitly computable integer a_i which is independent of λ. If $i \in \{0, 1, ..n\}$ is even then

$$[\mathcal{O}^{P_i} e_\lambda : A^{P_i} e_\lambda]_{\tilde{\mathcal{O}}} = \mathfrak{p}^{a_i + \delta(\lambda)}$$

where a_i is an explicitly computable integer which is independent of λ, and

$$\delta(\lambda) = \begin{cases} 1, & \text{if } 2u_\lambda > r; \\ 0, & \text{otherwise.} \end{cases}$$

Proof : For each non-negative integer $i \leq n$ we let $\mathcal{P}_i$ denote the maximal ideal of the valuation ring $\mathcal{O}_i$, and we let κ_i be any uniformising parameter of the subfield $K_i = F_i^G$. By Lemma 18 there exists an (explicitly computable) integer a_i such that

$$A^{P_i} = \kappa_i^{a_i} \mathcal{P}_i^{r_i}$$

with

$$r_i = \begin{cases} \frac{1}{2}(1+r), & \text{if } i \text{ is even ;} \\ 1, & \text{otherwise.} \end{cases}$$

Thus, if $\lambda \in C^{\dagger}_{\mathrm{loc}}$ is non-trivial then from Lemma 15 one has

$$A^{P_i} e_\lambda = \kappa_i^{a_i} \mathcal{P}_i^{r_i} e_\lambda = \kappa_i^{a_i} \times \begin{cases} \kappa_i \mathcal{O}_i e_\lambda, & \text{if } i \text{ is even and } 2u_\lambda > r; \\ \mathcal{O}_i e_\lambda, & \text{otherwise.} \end{cases}$$

Thus, if i is odd or if $2u_\lambda < r$ then one has

$$\begin{aligned} [\mathcal{O}^{P_i} e_\lambda : A^{P_i} e_\lambda]_{\bar{\mathcal{O}}} &= \mathrm{Norm}_{K_i/F}([\mathcal{O}_i e_\lambda : \kappa_i^{a_i} \mathcal{O}_i e_\lambda]_{\mathcal{O}_{K_i}}) \\ &= \mathrm{Norm}_{K_i/F}(\kappa_i^{a_i} \mathcal{O}_{K_i}) \\ &= \mathfrak{p}^{a_i}. \end{aligned}$$

But on the other hand if i is even and $2u_\lambda > r$ then

$$\begin{aligned} [\mathcal{O}^{P_i} e_\lambda : A^{P_i} e_\lambda]_{\bar{\mathcal{O}}} &= \mathrm{Norm}_{K_i/F}([\mathcal{O}_i e_\lambda : \kappa_i^{a_i+1} \mathcal{O}_i e_\lambda]_{\mathcal{O}_{K_i}}) \\ &= \mathrm{Norm}_{K_i/F}(\kappa_i^{a_i+1} \mathcal{O}_{K_i}) \\ &= \mathfrak{p}^{a_i+1}. \end{aligned}$$

4 - The explicit description

By Lemmata 9,12,16,17(i) and 19 we have now computed each fractional ideal $g_{(p)}(\theta)$. To state this result explicitly we must label the p-primary prime ideals of $\mathbb{Z}[\theta]$. For each positive integer n we now let $\mathbb{Q}(n)$ denote the splitting field (in $\mathbb{Q}^c$) of the polynomial $X^n - 1 \in \mathbb{Q}[X]$. For each character $\theta \in G^{\dagger}_{I_p}$ we set $\theta_p = \mathrm{res}^G_{I_p}(\theta) \in I_p^{\dagger}$, and we denote the order of θ_p by $p^{n_\theta} r_\theta$ for integers $n_\theta \leq n$ and $r_\theta | r$. Lemma 9 implies that $g_{(p)}(\theta)$ is inflated from an ideal of $\mathbb{Z}[\theta_p]$. Since p splits completely in $\mathbb{Q}(r_\theta)/\mathbb{Q}$ and totally ramifies in $\mathbb{Q}(\theta_p)/\mathbb{Q}(r_\theta)$ the p-primary prime ideals of $\mathbb{Z}[\theta_p]$ are in bijective correspondence with the elements of the group R_{r_θ}. We use the labelling $\{\mathcal{P}(\theta_p)_u : u \in R_{r_\theta}\}$ for the p-primary prime ideals of $\mathbb{Z}[\theta_p]$ where

here for each class $u \in R_{r_\theta}$ the prime ideal $\mathcal{P}(\theta_p)_u$ corresponds to a field embedding $\jmath : \mathbb{Q}^c \hookrightarrow \mathbb{Q}_p^c$ for which

$$\theta_p^\jmath = (\chi_{F/E})^{-rr_\theta^{-1}u}.$$

We also define a function $h_{(p)}$ on the character group $I_p^\dagger$ by

$$h_{(p)}(\phi) = \prod_{\substack{u \in R_{r_\phi} \\ 2\overline{u} > r_\phi}} \mathcal{P}(\phi)_u \in \mathcal{I}_{\mathbb{Q}(\phi)} \tag{20}$$

where here, for each element $u \in R_{r_\phi}$, we write $\overline{u}$ for the least strictly positive integer with residue u. In terms of this labelling Lemmata 9,12,16,17(i) and 19 together give the following explicit description of each function $g_{(p)}$. (For convenience we shall now also set $a_{n+1} = 0$.)

THEOREM 1. *For each character $\theta \in G_{L,}^\dagger$, and for each rational prime p which ramifies in $L/\mathbb{Q}$, if $\theta_p = res_{I_p}^G(\theta)$ has order $p^{n_\theta} r_\theta$ with $p \nmid r_\theta$ then*

$$g_{(p)}(\theta) = \left(\prod_{u \in R_{r_\theta}} \mathcal{P}(\theta_p)_u \right)^{a_{n_\theta} - a_{n_\theta + 1}} h_{(p)}(\theta_p)^{(-1)^{n-n_\theta}} \in \mathcal{I}_{\mathbb{Q}(\theta)}.$$

Note that

$$\prod_{u \in R_{r_\theta}} \mathcal{P}(\theta_p)_u \in \mathcal{P}r_{\mathbb{Q}(\theta_p)}$$

for each character $\theta \in G_{L,}^\dagger$, and so the class of $A_{L,}^{\mathcal{M}_{L,}}$ in $C\ell(L)$ is in fact represented by the function on $G_{L,}^\dagger$, which has p-primary parts $\theta \mapsto h_{(p)}(\theta_p)^{(-1)^{n-n_\theta}}$.

COROLLARY 1. *For any character $\theta \in G_{L,}^\dagger$, if $res_{I_p}^G(\theta)$ has order coprime to p then $g_{(p)}(\theta) \in \mathcal{P}r_{\mathbb{Q}(\theta)}$.*

Proof : In this case $h_{(p)}(\mathrm{res}_{I_p}^G(\theta)) \in \mathcal{P}r_{\mathbb{Q}(\theta)}$ as an easy consequence of the factorisation properties of Jacobi sums (c.f. [11], Chapter IV, Theorem 11) as first used in this context by Erez in [7].

Following Erez [7] a rational prime p is said to be *weakly ramified (peu ramifiée)* in $L/\mathbb{Q}$ if either $\#I_p = p$ or $p \nmid \#I_p$, and is otherwise said to be *very wildly ramified* in $L/\mathbb{Q}$. From Lemma 10, (11), and Corollary 1 we now need only consider functions $g_{(p)}$ for odd rational primes p which are

very wildly ramified in $L/\mathbb{Q}$. To consider this case more carefully we shall assume for simplicity that p is totally ramified in $L/\mathbb{Q}$ and that all other rational primes are weakly ramified in $L/\mathbb{Q}$.

If now $L/\mathbb{Q}$ has degree $p^n r$ with $n \geq 1$ then, defining a natural number $c(p,n,r)$ by

$$c(p,n,r) = \ell cm\{\text{order of the class of } h_{(p)}(\phi) \text{ in } C\ell_{\mathbb{Q}(p^n r_\phi)} : \phi \in G_{L.}^{\dagger}, p \nmid \text{order}(\phi^p)\}$$

(this is indeed dependent only upon p, n and r and not on the particular field L within the stated conditions), one has

COROLLARY 2. *If p is totally ramified in the extension $L/\mathbb{Q}$ and all other rational primes are weakly ramified in $L/\mathbb{Q}$ then the order of the class of $A_{L.}\mathcal{M}_{L.}$ in $C\ell(L)$ is $p^{n-1}c(p,n,r)$.*

Remarks (0) : Recall that the classes of $A_{L.}\mathcal{M}_{L.}$ and $A_{L.}^{\mathcal{M}_{L.}}$ have the same order in $C\ell(L)$ (c.f. Lemma 6 and the remarks which follow it).

(i) : If $n = 1$ then $A_{L.}\mathcal{M}_{L.}$ may or may not be free over $\mathcal{M}_{L.}$. Indeed it is certainly possible that $C\ell_{\mathbb{Q}(pr)}$ is trivial so that necessarilly $A_{L.}\mathcal{M}_{L.}$ is free, but on the other hand for example the unique subfield L of $\mathbb{Q}(169)$ which has absolute degree 39 satisfies the conditions of Corollary 2 with $p = 13, n = 1$, and $r = 3$ and yet $c(13,1,3) = 2$ ([8], Theorem B.3).

(ii) : From Corollary 2 it follows immediately that given any rational integer N there are infinitely many absolutely cyclic fields L for which the order of the class of $A_{L.}\mathcal{M}_{L.}$ in $C\ell(L)$ exceeds N. (This result was first stated as Theorem 3.6 in [8].)

Proof : We shall first prove a preliminary lemma concerning the behaviour of certain ideal classes. For each integer $n \geq -1$ and for each integer $d \geq 3$ we set $k_d(n) = \mathbb{Q}(p^{n+1}d)$ (but we shall henceforth not explicitly indicate the dependence on d). For each such integer we let $C(n)$ denote the ideal class group of $k(n)$ with $A(n)$ its p-primary subgroup. We let J denote the automorphism of $k(n)$ (and hence of $C(n)$ etc...) which is induced by the action of complex conjugation. We also define an integer $s = \Phi(d)/2$.

LEMMA 21. *For each integer $n \geq -1$ the prime ideals of $\mathcal{O}_{k(n)}$ lying above p are of the form $\mathfrak{p}_1(n), \mathfrak{p}_1(n)^J, ..., \mathfrak{p}_s(n), \mathfrak{p}_s(n)^J$ for distinct prime ideals $\mathfrak{p}_1(n), ..., \mathfrak{p}_s(n)$. Furthermore the subgroup of $A(n)$ generated by the*

classes of the ideals $\mathfrak{p}_1(n)^{1-J}, ..., \mathfrak{p}_s(n)^{1-J}$ *contains a subgroup isomorphic to* $(\mathbb{Z}/p^n\mathbb{Z})^s$.

Proof : Only the remark concerning the subgroup of $A(n)$ which is generated by the classes of the ideals $\mathfrak{p}_1(n)^{1-J}, ..., \mathfrak{p}_s(n)^{1-J}$ is not obvious. Thus suppose that for some integers a_i one has

$$\prod_{i=1}^{s} (\mathfrak{p}_i(n)^{1-J})^{a_i} = (\alpha)$$

for some element α of $k(n)$ - we must show that $p^n | a_i$ for each i with $1 \leq i \leq s$. Let $\beta = \alpha^{1-J}$ so that $(\beta) = (\alpha)^2$. Let $\eta = \beta^{\sigma-1}$ for σ a generator of $\mathrm{Gal}(k(n)/k(0))$. Then η is a unit of $k(n)$ all of whose conjugates have absolute value equal to 1, and hence is a root of unity. Also $\mathrm{Norm}_{k(n)/k(0)}(\eta) = 1$ and hence by Hilbert's Theorem 90 there exists an element ζ of $k(n)$ such that $\eta = \zeta^{\sigma-1}$. It is easy to check that in fact ζ must also be a root of unity. But $\beta\zeta^{-1} \in k(0)$ and therefore $(\alpha)^2 = (\beta) = (\beta\zeta^{-1})$ is in fact an element of $\mathcal{I}_{k(0)}$. Hence $p^n | a_i$ for $1 \leq i \leq s$, as required.

Now to prove Corollary 2 by using Theorem 1 we need only consider the ideals $h_{(p)}(\theta)$ for those characters $\theta \in G_L^\dagger$ for which both $n_\theta \geq 1$ and $r_\theta \neq 1$ (c.f. Lemma 10 and Corollary 1). If $\theta \in G_L^\dagger$ is any such character we let a_θ denote the order of the class of $h_{(p)}(\theta)$ in $C\ell_{\mathbb{Q}(\theta)}$ so that in particular

$$(h_{(p)}(\theta)^{1-J})^{a_\theta} \in \mathcal{P}r_{\mathbb{Q}(\theta)}. \tag{22}$$

But on the other hand, if $\mathcal{P}$ is any p-primary prime ideal of $\mathbb{Z}[\theta]$ then $\mathcal{P} | h_{(p)}(\theta)$ if and only if $\mathcal{P}^J \nmid h_{(p)}(\theta)$ (c.f. (20) for the definition of $h_{(p)}$) and so, using the notation of Lemma 21 (with $d = r_\theta$), one has

$$h_{(p)}(\theta)^{1-J} = \prod_{i=1}^{s} (\mathfrak{p}_i(n_\theta - 1)^{1-J})^{d_i} \tag{23}$$

with $d_i \in \{+1, -1\}$ for each $i \in \{1, ...s\}$. Thus by Lemma 21 the conditions (22) and (23) together imply that $a_\theta = p^{n_\theta - 1} a'_\theta$ for some natural number a'_θ. But setting $\theta'' = \theta^{p^{n_\theta - 1}}$ then

$$h_{(p)}(\theta)^{a_\theta} = h_{(p)}(\theta'')^{a'_\theta}$$

and so the order of the class of $A_L \mathcal{M}_L$ in $C\ell(L)$ is equal to

$$\ell cm\{p^{n_\theta - 1} . (\text{order of class of } h_{(p)}(\theta'') \text{ in } C\ell_{\mathbb{Q}(\theta)}) : \theta \in G_L^\dagger, n_\theta \geq 1\}.$$

By a straightforward exercise this last expression is indeed equal to $p^{n-1}c(p,n,r)$.

5 - A uniformity result

We are grateful to Christine Bachoc for helpful remarks concerning the material of this section.

Let L and L' be finite abelian Galois extensions of $\mathbb{Q}$ of groups G and G' respectively. For each rational prime p we let I_p (respectively I'_p) denote the inertia subgroup of G (respectively G') at the prime p. We shall say that G and G' are *inertia isomorphic* if there exists a group isomorphism $\theta : G \to G'$ which is *inertia-preserving*, i.e. such that $\theta(I_p) = I'_p$ for all rational primes p. In this final section we shall briefly remark on implications of Theorem 1 concerning the question

24. *If $L/\mathbb{Q}$ and $L'/\mathbb{Q}$ are odd degree abelian Galois extensions with inertia-isomorphic Galois groups is there necessarilly an inertia-preserving isomorphism between G and G' with respect to which there exists a Galois equivariant isomorphism between the lattices $A_{L/}\mathcal{M}_L$ and $A_{L'/}\mathcal{M}_{L'}$?*

Under certain restrictive ramification hypotheses the answer to (24) is already known to be affirmative. Indeed, even more strongly, from Bachoc-Erez [3] and Bachoc [1] one has

THEOREM 2 (BACHOC-EREZ, BACHOC). *Assume that $L/\mathbb{Q}$ is abelian of odd degree and that, for each rational prime p, the inertia subgroup I_p has order which is either a power of p or is coprime to p. Then there exists a G_L-equivariant isometry between (A_L, Tr_L) and $(\mathcal{A}_L, n_{G_L})$ for an explicitly described G_L-equivariant $\mathbb{Q}$-bilinear form n_{G_L} on $\mathbb{Q}[G_L]$. Moreover if $L'/\mathbb{Q}$ is any other Galois extension for which G_L and $G_{L'}$ are inertia isomorphic then any inertia-preserving isomorphism between G_L and $G_{L'}$ induces a Galois equivariant isometry between $(\mathcal{A}_L, n_{G_L})$ and $(\mathcal{A}_{L'}, n_{G_{L'}})$.*

Theorem 2 also implies that if $L/\mathbb{Q}$ and $L'/\mathbb{Q}$ are any odd degree abelian extensions with inertia-isomorphic Galois groups then, at each rational prime p, there is a Galois-equivariant isometry between the localised Galois-Hermitian modules $(A_L, \mathrm{Tr}_L) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $(A_{L'}, \mathrm{Tr}_{L'}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ ([8], Theorem 3.3). Thus, since there are no local obstructions, question 24 is the first problem one encounters when attempting to generalise the result of Theorem 2 to the case in which there are wildly ramified rational primes p for which $\#I_p$ is not a p-power.

To be more precise we shall now fix an abstract finite abelian group Γ

of odd order, and for each rational prime p, we fix a subgroup $\Delta_p \leq \Gamma$ such that $\#\Delta_p = 1$ for almost all p. We let $\mathcal{E}$ denote the set of Galois extensions L of $\mathbb{Q}$ for which there exists an isomorphism

(25)(i) $$\lambda : G_L \to \Gamma$$

such that, for all rational primes p,

(25)(ii) $\lambda^{-1}(\Delta_p)$ is the inertia subgroup of p in G_L.

For each $L \in \mathcal{E}$ we let Λ_L denote the set of isomorphisms λ as in (25). We now let $\mathcal{M}$ denote the maximal $\mathbb{Z}$-order in the $\mathbb{Q}$-algebra $\mathbb{Q}[\Gamma]$. For each $L \in \mathcal{E}$ and $\lambda \in \Lambda_L$ we let $[L, \lambda]$ denote the element of the locally-free class group $C\ell(\mathcal{M})$ which corresponds to $A_L\mathcal{M}_L$ under the isomorphism λ. For each $L \in \mathcal{E}$ we then set

$$c_L = \{[L, \lambda] : L \in \mathcal{E}, \lambda \in \Lambda_L\} \subseteq C\ell(\mathcal{M}).$$

The question (24) is then

(26)(i)
For any two fields $L, L' \in \mathcal{E}$ is it necessarilly true that $c_L \cap c_{L'} \neq \emptyset$?

or equivalently

(26)(ii) For any two fields $L, L' \in \mathcal{E}$ is it necessarilly true that $c_L = c_{L'}$?

We shall now show how the description of Theorem 1 easily implies a uniformity result similar to (but still considerably weaker than) an affirmative answer to (26). For this result we pass from L to its *absolute genus field* $\tilde{L}$. To be more precise here, if $L \in \mathcal{E}$ then for each rational prime p which is ramified in the extension $L/\mathbb{Q}$ we let L_p denote the unique abelian extension of $\mathbb{Q}$ which is ramified only at p and is of order $\#\Delta_p$, and we then let $\tilde{L}$ denote the compositum of all such fields L_p (so that in particular $L \subseteq \tilde{L}$). We also set $\tilde{G}_L = G_{\tilde{L}}$.

COROLLARY 3. *If L and L' are any elements of $\mathcal{E}$ then there exists an inertia- preserving isomorphism $\phi : \tilde{G}_L \to \tilde{G}_{L'}$, which induces a natural bijection*

$$\{c_E : E \in \mathcal{E}, E \leq \tilde{L}\} \leftrightarrow \{c_{E'} : E' \in \mathcal{E}, E' \leq \tilde{L}'\}.$$

Proof : We let $\{p_i : 1 \leq i \leq t\}$ (respectively $\{p_i : 1 \leq i \leq s\}$) be the set of rational primes which are ramified (respectively very wildly ramified) in the extensions $L/\mathbb{Q}$ and $L'/\mathbb{Q}$. For each $i \in \{1, ...t\}$ we set $I_i = I_{p_i}$ and $I' = I'_{p_i}$ so that

$$\tilde{G}_{\tilde{L}} \cong \bigoplus_{i=1}^{t} I_i \tag{27(i)}$$

and

$$\tilde{G}_{\tilde{L}'} \cong \bigoplus_{i=1}^{t} I'_i. \tag{27(ii)}$$

For each $i \in \{1, ...s\}$ we fix a prime ideal $\tilde{p}_i$ of $\mathcal{O}_{\tilde{L}}$ lying over p_i and then let F_i (respectively E_i) denote the local complection of $\tilde{L}$ (respectively $\tilde{L}^{I_i}$) at the place corresponding to $\tilde{p}_i$. We similarly define local fields F'_i and E'_i coming from $\tilde{L}'$. Since each subgroup I_i is cyclic the existence of an inertia-preserving isomorphism between $G_{\tilde{L}}$ and $G_{\tilde{L}'}$ implies the existence of isomorphisms

$$\phi_i : I_i \to I'_i, \text{ for } i = 1, ...t \tag{28(i)}$$

such that

$$\chi_{F'_i/F'_i} \circ \phi_i = \chi_{F_i/F_i}, \text{ for } i = 1, ...s. \tag{28(ii)}$$

(c.f. the remarks preceeding (14) for the definition of the characters χ_{F_i/F_i}.) Let now $\tilde{\Gamma}$ denote an abstract abelian group which is isomorphic to $\tilde{G}_{\tilde{L}}$ and let $\tilde{\mathcal{M}}$ then denote the maximal $\mathbb{Z}$-order in $\mathbb{Q}[\tilde{\Gamma}]$. By (27), (28), the description of Theorem 1, and the result of Lemma 6 the inertia-preserving isomorphism

$$\phi = \bigoplus_{i=1}^{t} \phi_i \ : \ \bigoplus_{i=1}^{t} I_i \to \bigoplus_{i=1}^{t} I'_i$$

induces an equality of sets

$$c_{\tilde{L}} = c_{\tilde{L}'} \subseteq C\ell(\tilde{\mathcal{M}}). \tag{29}$$

But now if $E \subseteq \tilde{L}$ and $E \in \mathcal{E}$ (so that $\tilde{E} = \tilde{L}$) then $\tilde{L}/E$ is unramified and so, setting $H = \text{Gal}(\tilde{L}/E) \leq \tilde{G}_{\tilde{L}}$ and $t_H = \sum_{\delta \in H} \delta$ (i.e. t_H is the field-theoretic map $\text{trace}_{\tilde{L}/E} : \tilde{L} \to E$), one has $A_{\tilde{L}} = A_E \mathcal{O}_{\tilde{L}}$ and $\mathcal{O}_{\tilde{L}} t_H = \mathcal{O}_E$ and therefore

$$(A_{\tilde{L}} \mathcal{M}_{\tilde{L}}) t_H = A_E \mathcal{M}_E. \tag{30(i)}$$

But if $E' = \tilde{L}'^{\phi(H)}$ then $E' \in \mathcal{E}$ and $\tilde{L}'/E'$ is unramified so that again one has

$$(30)(\text{ii}) \qquad (A_{\tilde{L}'}\mathcal{M}_{\tilde{L}'})t_{\phi(H)} = A_{E'}\mathcal{M}_{E'}.$$

But given (29) and (30) the map $E \mapsto E'$ now gives the bijection of Corollary 3.

Of course if $\tilde{L} = \tilde{L}'$ then the assertion of Corollary 3 is trivially satisfied. It is however possible that a stronger uniformity result is true -for example, Théorème 0.3 of [3] does not seem to be a special case of Corollary 3. Nevertheless, given the description of Theorem 1 (and in particular the dependence of the function $h_{(p)}$ on the field L (c.f. (20)), it seems to us very unlikely indeed that the answer to (26) is always affirmative. However to decide this would at some stage involve an analysis of the behaviour of certain ideal classes and we do not consider this any further here.

RÉFÉRENCES

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

[2] C. BACHOC, *Sur la structure hermitienne de la racine carrée de la codifférente*, to appear.

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

[4] A-M. BERGÉ, *Arithmétique d'une extension galoisienne à groupe d'inertie cyclique*, Ann. Inst. Fourier **28** (1978), 17–44.

[5] A-M. BERGÉ, *A propos du genre des entiers d'une extension*, Publications Math. Sc. Besançon (1979-1980), 1–9.

[6] D. BURNS, *Canonical factorisability and a variant of Martinet's conjecture*, to appear in J. London Math. Soc. (1991).

[7] B. EREZ, *Structure galoisienne et forme trace*, Thèse, Genève 1987 ; see also J. Algebra **118** (1988), 438–446.

[8] B. EREZ, *A survey of recent work on the square root of the inverse different*, to appear in the proceedings of the Journées arithmétiques, Luminy (1989).

[9] B. EREZ and M.J. TAYLOR, *Hermitian modules in Galois extensions of number fields and Adams operations*, to appear.

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

[11] S. LANG, *Algebraic Number Theory*, Graduate Texts in Mathematics **110** Springer-Verlag, Heidelberg (1986).

[12] H.W. LEOPOLDT, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine und angew. Math **201** (1959), 119–149.

[13] G. LETTL, *The ring of integers of an abelian number field*, J. reine und angew. Math. **400** (1990), 162–170.

[14] I. REINER, *Maximal Orders*, Academic Press, London (1975).

[15] J-P. SERRE, *Corps Locaux*, Hermann, Paris, (1962).

Fitzwilliam College
Cambridge CB3 0DG
England U.K.

Present address :

Institut für Mathematik
Universität Augsburg
Universitätsstrasse 8
8900 Augsburg
Deutschland.