ANNALES DE L'INSTITUT FOURIER

DAVID J. BURNS

Factorisability and wildly ramified Galois extensions

Annales de l'institut Fourier, tome 41, nº 2 (1991), p. 393-430

<http://www.numdam.org/item?id=AIF_1991__41_2_393_0>

Ann. Inst. Fourier, Grenoble
41, 2 (1991), 393-430

FACTORISABILITY AND WILDLY RAMIFIED GALOIS EXTENSIONS

by David J. BURNS

INTRODUCTION

Let p denote a rational prime which, unless explicitly stated to the contrary, is odd. Let K be a finite field extension of $\mathbb{Q}_p$, with L a finite abelian field extension of K. Let $G = \mathrm{Gal}(L/K)$ denote the group of L/K. Let $\mathcal{O}_L$ denote the ring of integers of L, and set $\mathcal{O} = \mathcal{O}_K$. Let $\mathcal{I}_L$ denote the multiplicative group of fractional $\mathcal{O}_L$-ideals.

There is a natural action of $K[G]$ on L and, with respect to this action, each ideal $I \in \mathcal{I}_L$ is an $\mathcal{O}[G]$-module. We are interested in studying the structure of these $\mathcal{O}[G]$-modules. Ullom has shown that if L/K is at most tamely ramified then all ideals I are $\mathcal{O}[G]$-isomorphic to $\mathcal{O}[G]$ ([21] Proposition 1.3). Furthermore, for each ideal one can give an explicit normal basis (see for example [14]). Thus in the tamely ramified case there is nothing more to say. If L/K is wildly ramified however the situation is very different.

For each ideal $I \in \mathcal{I}_L$ we let $\mathcal{A}_{K[G]}(I)$ denote the full set of elements of $K[G]$ which induce endomorphisms of I. This set $\mathcal{A}_{K[G]}(I)$ is an $\mathcal{O}$-order in $K[G]$, the « associated order » of I in $K[G]$, and contains $\mathcal{O}[G]$ (of course, if L/K is at most tamely ramified then $\mathcal{A}_{K[G]}(I) = \mathcal{O}[G]$). It is most natural to consider the structure of each ideal I as an $\mathcal{A}_{K[G]}(I)$-module, and not just as an $\mathcal{O}[G]$-module. In the wildly ramified case therefore there are three distinct problems which one should consider. Firstly, for any given ideal I one should give an explicit description of the associated order $\mathcal{A}_{K[G]}(I)$. Next, if such a description

Key-words : Galois module structure - Ambiguous ideals.
A.M.S. Classification : 11R33.

is available, one should describe the structure of I as an $\mathcal{A}_{K[G]}(I)$-module, and in particular determine whether I is free over, i.e. is isomorphic to, $\mathcal{A}_{K[G]}(I)$. Lastly, in those cases in which I is isomorphic to $\mathcal{A}_{K[G]}(I)$, one should give an explicit generator of I over $\mathcal{A}_{K[G]}(I)$. Except in very special cases little appears to be known concerning these problems, and there are no general patterns of behaviour yet apparent. Ferton has dealt in complete generality with the case of extensions of degree p (c.f. [9]), Taylor has dealt with the ideal $I = \mathcal{O}_L$ for a certain class of Lubin-Tate extensions (cf. [7], Chapter X, § 3), and very recently Byott has dealt with certain non-cyclic Kummer extensions of degree p^2. Other than this however, the only case which has so far been considered, by Bergé in [1], is that in which $K/\mathbb{Q}_p$ is unramified, G has a cyclic inertia subgroup, and $I = \mathcal{O}_L$. In this case $\mathcal{O}_L$ is not always isomorphic to $\mathcal{A}_{K[G]}(\mathcal{O}_L)$. This last fact is already somewhat surprising since the conditions imposed on K and on G by Bergé are merely the abstraction of conditions satisfied by all absolutely abelian extensions (i.e. $K = \mathbb{Q}_p$), and for these a classical result of Leopoldt [15] implies that $\mathcal{O}_L$ is isomorphic to $\mathcal{A}_{\mathbb{Q}_p[G]}(\mathcal{O}_L)$, and that an explicit generator for $\mathcal{O}_L$ over $\mathcal{A}_{\mathbb{Q}_p[G]}(\mathcal{O}_L)$ can be given (in terms of Gauss sums). In her more general setting Bergé does not consider the problem of giving explicit generators for those cases in which $\mathcal{O}_L$ is isomorphic to $\mathcal{A}_{K[G]}(\mathcal{O}_L)$.

Henceforth we shall assume, unless explicitly stated to the contrary, that $K/\mathbb{Q}_p$ is unramified. Under this restriction we introduced in [3] a new approach to the problem of determining, at least in certain cases, the structure of $\mathcal{O}[\Gamma]$-lattices for any finite abelian group Γ. In this paper we shall combine the approach of [3] with an arithmetical factorisability result of Fröhlich [13] and so consider afresh the problem of determining whether any given ideal I is isomorphic to its associated order $\mathcal{A}_{K[G]}(I)$. This is the first systematic analysis of the consequences of factorisability considerations in an arithmetical setting.

Our approach provides no new method for explicitly describing associated orders, or for giving explicit generators for those ideals which are free. Its advantage is that, for any given abelian G, and for any given ideal I, if $\mathcal{A}_{K[G]}(I)$ is explicitly known then the question of whether I is isomorphic to $\mathcal{A}_{K[G]}(I)$ is reduced to a matter of explicit (and occasionally straightforward) computation. By these means we shall prove that, for any given abstract structure of G (and of the inertial subgroup of G), the question of whether an ideal I is isomorphic to

$\mathscr{A}_{K[G]}(I)$ is dependent only upon the L-valuation of I together with the abstract structure of the $\mathcal{O}$-order $\mathscr{A}_{K[G]}(I)$. This last type of result (stated precisely in § 2) suggests interesting « comparison results » in the number field case, similar, for example, to those previously obtained by Wilson [23]. Our techniques, being essentially computational, are also well suited to deriving explicit results. For example, if G has a cyclic inertia subgroup and $I = \mathcal{O}_L$ then, given Bergé's explicit description of $\mathscr{A}_{K[G]}(\mathcal{O}_L)$, the necessary computations are effected without great difficulty, and so we give a new proof of the freeness results of [1] § 4. Moreover, even in cases in which we cannot explicitly describe $\mathscr{A}_{K[G]}(I)$, we can use the techniques of [1] § 2.2 to obtain new and explicit results in the case of non-cyclic inertia subgroups.

Since our approach is more general than that of Bergé we are therefore now able to set her results in a wider context. In addition, even though we cannot at present completely solve the problems in this more general setting, our explicit results suggest interesting patterns of behaviour which hitherto have not been apparent. For example they suggest that, at least for the class of extensions under consideration, the fractional ideal $\mathcal{O}_L$ plays an especially significant role in these matters (this is made more precise in § 2).

This paper is arranged as follows. In § 1 we briefly recall the notions and results which we shall subsequently make heavy use of, and in terms of which some of our results will be stated. In § 2 our main results are stated. In § 3 we deal with the cyclic case, and in § 4 with the non-cyclic case. In § 5 we shall prove the « comparison » result mentioned above.

Acknowledgement. The author is very grateful to the referee for the painstaking way in which he/she criticised the first version of this paper.

Basic Notations. In addition to those already introduced we shall make use of the following notations.

The cardinality of Γ is written $\operatorname{ord}(\Gamma)$. For any subgroup $\Delta \leqslant \Gamma$ we shall write e_Δ for the idempotent $(\operatorname{ord}(\Delta))^{-1} \sum_{\delta \in \Delta} \delta$ of $\mathbb{Q}_p[\Delta]$. If X is an $\mathcal{O}[\Gamma]$-lattice then X^Δ denotes the sublattice of elements which are invariant under the action of each element of Δ, i.e. $X^\Delta = \{x \in X : x = xe_\Delta\}$. The lattice X has associated order $\mathscr{A}_{K[\Gamma]}(X)$ in $K[\Gamma]$. The (unique) maximal $\mathcal{O}$-order in $K[\Gamma]$ is $\mathscr{M}(\mathcal{O},\Gamma)$. We let $X^{\mathscr{M}(\mathcal{O},\Gamma)}$ denote the maximal sublattice of X which admits an action of $\mathcal{M}(\mathcal{O},\Gamma)$. Thus $X = X^{\mathcal{M}(\mathcal{O},\Gamma)}$ if and only if $\mathcal{A}_{K[\Gamma]}(X) = \mathcal{M}(\mathcal{O},\Gamma)$. There is a natural identification $K[\Gamma]e_\Delta = K[\Gamma/\Delta]$ which restricts to give identifications $\mathcal{M}(\mathcal{O},\Gamma)e_\Delta = \mathcal{M}(\mathcal{O},\Gamma/\Delta)$ and $\mathcal{O}[\Gamma]e_\Delta = \mathcal{O}[\Gamma/\Delta]$, and with respect to this identification we shall regard each X^Δ as an $\mathcal{O}[\Gamma/\Delta]$-lattice. For any commutative ring R the group of multiplicative units is denoted R^*.

1. SOME PRELIMINARIES

Before stating our main results it will be useful to briefly recall some of the notions and techniques that we shall make heavy use of, and in terms of which some of our results are stated. This then is the aim of the present section.

Let Γ denote a finite abelian group. We shall first recall the notion of factorisability and the associated relation of Γ-factor-equivalence defined on the set of $\mathcal{O}[\Gamma]$-lattices. The notion of factorisability was first studied by Nelson [16] in a representation theoretic setting in the context of arbitrary finite groups. However since our groups are abelian we may adopt a much more elementary approach. There are by now a number of different treatments, and indeed notions, of factor-equivalence in the literature (see for example [12], [13], [3], [4], [5] or [19]) but we shall here only deal with that which is most convenient for our present purposes. Thus, for example, the notion of factor-equivalence we define here coincides with the relation $\wedge$ defined in [12] (1.13) and [3], and with the relation $\wedge_\Gamma$ defined in [4] § 1.

We fix an algebraic closure $\mathbb{Q}_p^c$ of the field $\mathbb{Q}_p$. We let $\Gamma^\dagger$ denote the group of multiplicative characters $\mathrm{Hom}(\Gamma,(\mathbb{Q}_p^c)^*)$, with $S(\Gamma^\dagger)$ the set of subgroups of $\Gamma^\dagger$. For each subgroup $\Delta \leqslant \Gamma$ we let $\mathcal{G}(\Delta)$ denote the group $\{\theta \in \Gamma^\dagger : \theta(\Delta)=1\}$. Thus $S(\Gamma^\dagger) = \{\mathcal{G}(\Delta) : \Delta \leqslant \Gamma\}$. To each injective homomorphism

$$\eta : X \hookrightarrow Y \otimes_{\mathcal{O}} K \tag{1.1}$$

of $\mathcal{O}[\Gamma]$-lattices X and Y which satisfies

$$\eta X \otimes_{\mathcal{O}} K = Y \otimes_{\mathcal{O}} K$$

one associates a function $f_\eta = f_{Y,X,\eta}$ on $S(\Gamma^\dagger)$ which is defined by

$$f_\eta(\mathcal{G}(\Delta)) = [Y^\Delta : (\eta X)^\Delta]_{\mathcal{O}}, \qquad \text{all } \Delta \leqslant \Gamma$$

where here $[\,:\,]_{\mathcal{O}}$ is the $\mathcal{O}$-module index as defined for $\mathcal{O}$-lattices which span the same K-space (cf. Fröhlich's article in [6]). Note that if X and Y span the *same* $K[\Gamma]$-space, then we shall always take the embedding η in (1.1) as that induced by the identity map id on the ambient $K[\Gamma]$-space and, for brevity, we shall then write $f_{Y,X}$ in place of $f_{Y,X,\mathrm{id}}$.

A *division* of $\Gamma^\dagger$ is an equivalence class of characters with characters θ and θ' belonging to the same division if and only if they generate the same cyclic subgroup. To each division D of $\Gamma^\dagger$ there is thus associated a unique cyclic subgroup of $\Gamma^\dagger$ which we shall denote by $\bar{D}$ (i.e. $\bar{D}$ is the subgroup of $\Gamma^\dagger$ which is generated by any element of D). One now defines the value of f_η at each division D of $\Gamma^\dagger$ by means of the Möbius μ-function :

$$(1.2) \qquad f_\eta(D) = \prod_{C \leqslant \bar{D}} f_\eta(C)^{\mu(\mathrm{ord}\,(\bar{D}/C))}$$

where here the product is taken over all (cyclic) subgroups $C \leqslant \bar{D}$. By Möbius inversion (1.2) is equivalent to

$$(1.3)\,(a) \quad f_\eta(H) = \prod_{D \subset H} f_\eta(D), \qquad \text{for all cyclic } H \leqslant \Gamma^\dagger$$

where here the product is taken over all divisions D contained in H. It is useful to introduce an associated function, the *factorisable quotient function* $\tilde{f}_\eta$, which measures the extent to which (1.3) (a) is valid for general subgroups $H \leqslant \Gamma^\dagger$. Thus $\tilde{f}_\eta$ is defined at each subgroup $H \leqslant \Gamma^\dagger$ by

$$(1.4) \qquad \tilde{f}_\eta(H) = (f_\eta(H))^{-1} \prod_{D \subset H} f_\eta(D).$$

Equation (1.3) (a) is thus equivalent to

$$(1.3)\,(b) \quad \tilde{f}_\eta(H) = \mathcal{O}, \qquad \text{for all cyclic subgroups } H \leqslant \Gamma^\dagger.$$

If $\tilde{f}_\eta(H) = \mathcal{O}$ for *all* subgroups $H \leqslant \Gamma^\dagger$, i.e. if the function $\tilde{f}_\eta$ is identically trivial, then one says that the function f_η is *factorisable.*

Set $\mathcal{M} = \mathcal{M}(\mathcal{O}, \Gamma)$. Any embedding η as in (1.1) gives rise to a corresponding embedding

$$\eta_{\max} : X^{\mathcal{M}} \hookrightarrow Y^{\mathcal{M}} \otimes_{\mathcal{O}} K$$

which satisfies

$$\eta_{\max} X^{\mathcal{M}} \otimes_{\mathcal{O}} K = Y^{\mathcal{M}} \otimes_{\mathcal{O}} K$$

and it is not difficult to verify that the function $f_{\eta\max}$ is always factorisable. Furthermore, for each subgroup $\Delta \leqslant \Gamma$ one has

$$f_{\eta}(\mathscr{G}(\Delta))f_{\eta\max}(\mathscr{G}(\Delta))^{-1} = \frac{[Y^{\Delta} : (Y^{\mathscr{M}})^{\Delta}]_{\mathcal{O}}}{[X^{\Delta} : (X^{\mathscr{M}})^{\Delta}]_{\mathcal{O}}}$$

so that the function $f_{\eta}f_{\eta\max}^{-1}$ is in fact independent of the particular choice of the embedding η as in (1.1). Following Fröhlich we set $\mathscr{I}_{Y,X} = f_{\eta}f_{\eta\max}^{-1}$ and refer to this function as the *defect function* of Y and X. Note that, if η and η' are any two embeddings as in (1.1) then one has

$$f_{\eta} \text{ is factorisable} \Leftrightarrow \mathscr{I}_{Y,X} \text{ is factorisable} \Leftrightarrow f_{\eta'} \text{ is factorisable.}$$

DEFINITION 1.5. — *Two $\mathcal{O}[\Gamma]$-lattices X and Y will be said to be Γ-factor-equivalent, written $X \wedge_{\Gamma} Y$, if there exists an injective homomorphism η as in* (1.1) *such that the function $f_{Y,X,\eta}$ is factorisable.*

Remark. — For an interpretation of the condition $X \wedge_{\Gamma} Y$ in terms of relations between certain natural $\mathcal{O}[\Gamma]$-sublattices of X and Y see [3] § 1.

It is not difficult to check that $\wedge_{\Gamma}$ is an equivalence relation on the set of $\mathcal{O}[\Gamma]$-lattices. This relation is weaker than the relation of $\mathcal{O}[\Gamma]$-isomorphism, which we shall henceforth write as $\cong_{\mathcal{O}[\Gamma]}$. Indeed if $X \cong_{\mathcal{O}[\Gamma]} Y$ then the function $\mathscr{I}_{Y,X}$ is identically trivial and so $X \wedge_{\Gamma} Y$. Also $\wedge_{\Gamma}$ behaves very well functorially, for example under extension or restriction of scalars, or induction of modules from subgroups. A further functorial property which we shall later use is that

$$(1.6) \quad X \wedge_{\Gamma} Y \Rightarrow X^{\Delta} \wedge_{\Gamma/\Delta} Y^{\Delta} \qquad \text{for all subgroups } \Delta \leqslant \Gamma,$$

a property which follows straight from the definitions.

By explicit example the relation $\wedge_{\Gamma}$ is seen to be far from trivial:

LEMMA 1.7 (Nelson, [16]). — *$\mathscr{M}(\mathcal{O},\Gamma) \wedge_{\Gamma} \mathcal{O}[\Gamma]$ if and only if Γ is cyclic.*

Fortunately however it seems that factorisable functions are relatively abundant in arithmetic. In particular, in the context of this paper one has the following beautiful result:

THEOREM 1 (Fröhlich, [13]). — *If F/E is any abelian extension of local fields then*

$$\mathcal{O}_F \wedge_{\mathrm{Gal}(F/E)} \mathcal{O}_E[\mathrm{Gal}(F/E)].$$

Remarks. — (i) This result, although not explicitly stated in [13], follows by the same argument used to prove Theorem 7 (additive) of [13].

(ii) Theorem 1 is especially interesting if F/E is wildly ramified since then $\mathcal{O}_F$ is not isomorphic to $\mathcal{O}_E[\mathrm{Gal}\,(F/E)]$.

(iii) For other interesting arithmetical examples of factorisable functions, in particular concerning the Galois module structures of unit groups, see [13] and [19].

COROLLARY 1.8. — *Let F/E be an abelian extension of local fields. If $\mathcal{O}_F$ admits an action of $\mathcal{M}(\mathcal{O}_E, \mathrm{Gal}\,(F/E))$ then* $\mathrm{Gal}\,(F/E)$ *is cyclic.*

Proof. — Set $H = \mathrm{Gal}\,(F/E)$, and $\mathcal{M} = \mathcal{M}(\mathcal{O}_E, H)$. If $\mathcal{O}_F$ admits an action of $\mathcal{M}$, i.e. if $\mathcal{M}\mathcal{O}_F \subseteq \mathcal{O}_F$, then $\mathcal{O}_F \cong_{\mathcal{O}_E[H]} \mathcal{M}$ (this is a standard property of maximal orders — for example see [17] (17.3), or [11] Theorem 10). Hence $\mathcal{O}_F \wedge_H \mathcal{M}$ and so, by Theorem 1, $\mathcal{M} \wedge_H \mathcal{O}_E[H]$. The result now follows as a consequence of Lemma (1.7). □

This corollary gives some indication of how the notion of factor-equivalence may be of considerable arithmetical usefulness. Indeed whilst questions concerning $\cong_{\mathcal{O}[G]}$ are often quite subtle, (given the result of Theorem 1) questions concerning $\wedge_G$ are of an essentially computational nature and as such are often much more approachable. In particular therefore one can often much more easily prove that two lattices are not isomorphic by demonstrating that they are not factor-equivalent rather than by any more direct method. Of course it would be of much more interest to be able to deduce the relation $\cong_{\mathcal{O}[G]}$ by using factorisability considerations. This was the main aim in [3], in which we introduced another equivalence relation on the set of $\mathcal{O}[\Gamma]$-lattices which when combined with factorisability considerations allowed us (under certain conditions) to characterise triviality of the defect function. A deep theorem of Fröhlich ([11], Theorem 4) on the defect function then led to a result of the required form. To state this result we must introduce some notation. We shall call a subgroup $\Delta \leqslant \Gamma$ *cocyclic* if the quotient groupe Γ/Δ is cyclic.

DEFINITION 1.9. — *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 $\Delta \leqslant \Gamma$ one has $\mathcal{A}_{K[\Gamma/\Delta]}(X^\Delta) = \mathcal{A}_{K[\Gamma/\Delta]}(Y^\Delta)$.*

Now if Δ is a subgroup of Γ of order coprime to p then for any $\mathcal{O}[\Gamma]$-lattice X one has $X^\Delta = e_\Delta X$ and so

$$\mathcal{A}_{K[\Gamma]}(X)^\Delta = e_\Delta \mathcal{A}_{K[\Gamma]}(X) = \mathcal{A}_{K[\Gamma/\Delta]}(e_\Delta X) = \mathcal{A}_{K[\Gamma/\Delta]}(X^\Delta).$$

Thus for example if Γ is cyclic then $X \circ_\Gamma Y$ if and only if $\mathcal{A}_{K[\Gamma/\Delta]}(X^\Delta) = \mathcal{A}_{K[\Gamma/\Delta]}(Y^\Delta)$ for all p-primary subgroups $\Delta \leqslant \Gamma$.

This relation of Γ-$\circ$-equivalence is in fact strictly stronger than that introduced in § 2 of [3]. However it is obviously weaker than $\cong_{\mathcal{O}[\Gamma]}$ and so the argument of [3] § 2 still proves the following result.

THEOREM 2. — *Let X be an $\mathcal{O}[\Gamma]$-lattice such that*

$$X \otimes_{\mathcal{O}} K \cong_{K[\Gamma]} K[\Gamma],$$

and set $\mathcal{A} = \mathcal{A}_{K[\Gamma]}(X)$. Then $X \cong_{\mathcal{O}[\Gamma]} \mathcal{A}$ if and only if both $X \circ_\Gamma \mathcal{A}$ and $\tilde{\mathcal{I}}_{X,\mathcal{A}}(\Gamma^\dagger) = \mathcal{O}$.

COROLLARY 1.10. — *If $I \in \mathcal{I}_L$ then $I \cong_{\mathcal{O}[G]} \mathcal{A}_{K[G]}(I)$ if and only if both $I \circ_G \mathcal{A}_{K[G]}(I)$ and $\tilde{f}_{\mathcal{A}_{K[G]}(I),\mathcal{O}[G]}(G^\dagger) = \tilde{f}_{I,\mathcal{O}_L}(G^\dagger)$.*

Proof. — By Theorem 2 one has

$$I \cong_{\mathcal{O}[G]} \mathcal{A}_{K[G]}(I) \Leftrightarrow I \circ_G \mathcal{A}_{K[G]}(I) \qquad \text{and} \qquad \tilde{\mathcal{I}}_{I,\mathcal{A}_{K[G]}(I)}(G^\dagger) = \mathcal{O},$$

and, by Theorem 1,

$$\begin{aligned}\tilde{\mathcal{I}}_{I,\mathcal{A}_{K[G]}(I)}(G^\dagger) &= \tilde{\mathcal{I}}_{I,\mathcal{O}_L}(G^\dagger) \cdot \tilde{\mathcal{I}}_{\mathcal{O}_L,\mathcal{O}[G]}(G^\dagger) \cdot \tilde{\mathcal{I}}_{\mathcal{O}[G],\mathcal{A}_{K[G]}(I)}(G^\dagger)\\ &= \tilde{\mathcal{I}}_{I,\mathcal{O}_L}(G^\dagger) \cdot \tilde{\mathcal{I}}_{\mathcal{O}[G],\mathcal{A}_{K[G]}(I)}(G^\dagger)\\ &= \tilde{f}_{I,\mathcal{O}_L}(G^\dagger) \cdot \tilde{f}_{\mathcal{A}_{K[G]}(I),\mathcal{O}[G]}(G^\dagger)^{-1}.\end{aligned}$$ □

The result of Corollary (1.10) motivated our present investigation. Indeed, by using techniques of Bergé dealing with cyclic extensions (to be recalled in § 3.1) one can in principle completely analyse the question of G-$\circ$-equivalence, and also obtain much explicit information on the validity or otherwise of the equality $\tilde{f}_{\mathcal{A}_{K[G]}(I),\mathcal{O}[G]}(G^\dagger) = \tilde{f}_{I,\mathcal{O}_L}(G^\dagger)$.

Note that in the context of Theorem 2 the relation of Γ-$\circ$-equivalence is of most interest when comparing an $\mathcal{O}[\Gamma]$-lattice X to its associated order $\mathcal{A}_{K[\Gamma]}(X)$. In this case an easy exercise shows that

$$(1.11) \quad \mathcal{O}[\Gamma/\Delta] \subseteq \mathcal{A}_{K[\Gamma/\Delta]}(X^\Delta) \subseteq \mathcal{A}_{K[\Gamma/\Delta]}(\mathcal{A}_{K[\Gamma]}(X)^\Delta) \subseteq \mathcal{M}(\mathcal{O},\Gamma/\Delta)$$

for each subgroup $\Delta \leqslant \Gamma$. For a more thorough analysis in the arithmetical setting of Corollary (1.10) we now introduce, for any given Galois extension F/E of local fields, and any given integers i and j, an $\mathcal{O}[\mathrm{Gal}(F/E)]$-lattice $\mathscr{A}(F/E,i,j)$ which is defined by

$$\mathscr{A}(F/E,i,j) = \{\lambda \in E[\mathrm{Gal}\,(F/E)] : \lambda(\wp_F^i) \subseteqq \{\wp_F^j\},$$

where here (and in the sequel) we write $\wp_F$ for the (unique) maximal ideal of $\mathcal{O}_F$. The connection with matters of o-equivalence is made clear by the next lemma.

For any local field F we shall write v_F for the valuation of F which is normalised such that $v_F(\pi) = 1$ for any generator π of $\wp_F$. For any subset $Y \subset F^*$ we let $v_F(Y)$ denote the infimum of the set $\{v_F(y) : y \in Y\}$. Thus if $I \in \mathscr{I}_F$ then $I = \wp_F^{v_F(I)}$. For any abelian group Γ we write Tr_Γ for the trace element $\mathrm{ord}\,(\Gamma)e_\Gamma = \sum_{\gamma\in\Gamma} \gamma \in \mathbb{Z}_p[\Gamma]$. In particular if $H \leqslant G$ then Tr_H is the field theoretic trace map $\mathrm{Tr}_{L/L^H} : L \to L^H$. Thus if $I \in \mathscr{I}_L$ then both $e_H I$ and I^H are elements of $\mathscr{I}_{L^H}$.

LEMMA 1.12. – *Let H be a subgroup of G of order $p^t r$ with $p \nmid r$. For any ideal $I \in \mathscr{I}_L$ one has*

$$\begin{aligned}\mathscr{A}_{K[G]}(I)^H &= \mathscr{A}(L^H/K, v_{L^H}(e_H(I)), v_{L^H}(I^H))\\ &= p^t\,\mathscr{A}(L^H/K, v_{L^H}(\mathrm{Tr}_H(I)), v_{L^H}(I^H)).\end{aligned}$$

Remark. – Recall that, for any given subgroup $H \leqslant G$, the natural identification $K[G]e_H = K[G/H]$ restricts to give an identification $\mathscr{M}(\mathcal{O},G)e_H = \mathscr{M}(\mathcal{O},G/H)$, and the first equality of the lemma is to be interpreted in this fashion.

Proof. – Since $\mathrm{Tr}_H = p^t r.e_H$ the second equality of Lemma (1.12) is clear. As for the first equality, if $\lambda \in K[G]$ then

$$\begin{aligned}\lambda e_H \in \mathscr{A}_{K[G]}(I)^H &\Leftrightarrow \lambda e_H \in \mathscr{A}_{K[G]}(I)\\ &\Leftrightarrow \lambda e_H(I) \subseteqq I\\ &\Leftrightarrow \bar{\lambda}(e_H(I)) \subseteqq I^H\end{aligned}$$

(where here $\bar{\lambda}$ denotes λe_H regarded as an element of $K[G/H]$)

$$\Leftrightarrow \bar{\lambda} \in \mathscr{A}(L^H/K, v_{L^H}(e_H(I)), v_{L^H}(I^H)). \qquad \square$$

In our case one can even give explicit formulae for $v_{L^H}(\mathrm{Tr}_H(I))$ and $v_{L^H}(I^H)$ which are dependent only upon $v_L(I)$, H and the inertia subgroup G_{ram} of G. To be more specific we first note that, since $K/\mathbb{Q}_p$ is unramified (and p is odd), the complete ramification filtration of G is determined by the abstract structure of G_{ram}. To state this result we let $\{G^{(i)}\}_{i \geqslant 0}$ (respectively $\{G_{(i)}\}_{i \geqslant 0}$) denote the ramification filtration of G using the upper (respectively lower) numbering. In particular therefore $G^{(0)} = G_{(0)} = G_{\mathrm{ram}}$. For any abelian p-group P and any integer $i \geqslant 0$, we shall also write $P(i)$ for the subgroup of P formed by the elements which are p^i-th powers in P.

LEMMA 1.13. – *The group $G^{(1)}$ is equal to the Sylow p-subgroup of G_{ram}. Moreover, for each integer $i \geqslant 1$, $G^{(i)} = G^{(1)}(i-1)$.*

Proof. – The first assertion is standard. Moreover, if $G^{(1)}$ is either cyclic or elementary abelian then (since the field K is absolutely unramified, and p is odd) the second assertion is a consequence of Propositions (4.2) and (4.3) of [10]. From these special cases the general result follows by using Herbrand's Theorem and the fact that, for each integer $i \geqslant 1$, the quotient $G^{(i)}/G^{(i+1)}$ is an elementary abelian p-group (cf. [18] Chapitre IV). □

Let p^{n_1} denote exponent of $G^{(1)}$. Lemma (1.13) implies that $G^{(n_1)} > G^{(n_1+1)} = 1$. For each integer $i = 1, \ldots, n_1$ we let t_i denote the i-th jump number of the lower ramification filtration and we set $t_0 = 0$. Converting between the upper and lower ramification numbering (cf. [18] Chapitre IV, § 3), one has

$$(1.14) \qquad t_i - t_{i-1} = \mathrm{ord}\,(G/G^{(i)})$$

for each integer $i = 1, \ldots, n_1$. Also for any subgroup $H \leqslant G$ one has (cf. [18] Chapitre III, Proposition 7, and Chapitre IV, Propositions 2 and 4)

$$\begin{aligned}(1.15)\,(a)\quad & v_{L^H}(\mathrm{Tr}_H(I)) \\ &= \left[\frac{1}{\mathrm{ord}\,(G_{(0)} \cap H)}\left(v_L(I) + \sum_{i \geqslant 0}(\mathrm{ord}\,(G_{(i)} \cap H) - 1)\right)\right] \\ &= \left[\frac{1}{\mathrm{ord}\,(G^{(0)} \cap H)}\left(v_L(I) + \mathrm{ord}\,(G^{(0)} \cap H) - 1\right.\right. \\ &\quad \left.\left. + \sum_{i=1}^{i=n_1}(t_i - t_{i-1})(\mathrm{ord}\,(G^{(i)} \cap H) - 1)\right)\right],\end{aligned}$$

and

$$(1.15)\,(b) \qquad v_{L^H}(I^H) = \left\lceil \frac{v_L(I)}{\mathrm{ord}\,(G^{(0)} \cap H)} \right\rceil$$

where here, for any real number x, we write $[x]$ for the greatest integer not exceeding x, and $\lceil x \rceil$ for the least integer not less than x (i.e. $\lceil x \rceil = -[-x]$).

As a final remark we note that the totally ramified case is naturally of most interest to us. To be more specific here we let L_0 denote the inertial subfield $L^{G_{\mathrm{ram}}}$ of L (i.e. L_0 is the maximal unramified extension of K which is contained in L).

LEMMA 1.16. – *For any ideal $I \in \mathscr{I}_L$ one has an isomorphism*

$$(1.17) \qquad \mathcal{O}_{L_0} \otimes_{\mathcal{O}} I \cong_{\mathcal{O}_{L_0}[G]} \mathcal{O}_{L_0}[G] \otimes_{\mathcal{O}_{L_0}[G_{\mathrm{ram}}]} I$$

(*where on the left of* (1.17) *the ideal I is regarded as an $\mathcal{O}[G]$-lattice, and on the right as an $\mathcal{O}_{L_0}[G_{\mathrm{ram}}]$-lattice*). *Thus*

$$(1.18) \quad \mathcal{O}_{L_0} \otimes_{\mathcal{O}} \mathscr{A}_{K[G]}(I) = \mathcal{O}_{L_0}[G] \otimes_{\mathcal{O}_{L_0}[G_{\mathrm{ram}}]} \mathscr{A}_{L_0[G_{\mathrm{ram}}]}(I),$$

and

$$(1.19) \quad I \cong_{\mathcal{O}[G]} \mathscr{A}_{K[G]}(I) \Leftrightarrow I \cong_{\mathcal{O}_{L_0}[G_{\mathrm{ram}}]} \mathscr{A}_{L_0[G_{\mathrm{ram}}]}(I).$$

Proof. – This can be proved by the arguments of [2] § 2. (It is important here that G be abelian.) □

2. STATEMENT OF THE MAIN RESULTS

Unless explicitly stated to the contrary, in this section the extension L/K is assumed to be totally ramified. The degree of L/K is $p^N R$ with $p \nmid R$. We need only deal with wildly ramified extensions and so shall assume that $N \geqslant 1$.

It is convenient to introduce some additional notation. If $I \in \mathscr{I}_L$ then we shall write $\mathbf{Fr}_K(I)$ (respectively $\neg\,\mathbf{Fr}_K(I)$) if I is (respectively is not) free over (i.e. isomorphic to) $\mathscr{A}_{K[G]}(I)$. More generally we shall write $\mathbf{Fr}_K(\mathscr{I}_L)$ (respectively $\neg\,\mathbf{Fr}_K(\mathscr{I}_L)$) if $\mathbf{Fr}_K(I)$ for some $I \in \mathscr{I}_L$ (respectively if $\neg\,\mathbf{Fr}_K(I)$ for all $I \in \mathscr{I}_L$).

By use of the approach described in § 1 we shall in this paper obtain explicit conditions on the abstract structure of G which are implied by, and in certain cases imply, $\mathbf{Fr}_K(\mathscr{I}_L)$. In particular, we shall see that $\mathbf{Fr}_K(\mathscr{I}_L)$ is a severe restriction on the possible structures for G. In the cyclic case we shall obtain a complete characterisation of $\mathbf{Fr}_K(\mathscr{I}_L)$. In the non-cyclic case our results are still partial. As an underlying general philosophy however, our results can all be interpreted as providing strong evidence for an affirmative answer to the following.

Open Question 2.1. – Is $\mathbf{Fr}_K(\mathcal{O}_L)$ implied by $\mathbf{Fr}_K(\mathscr{I}_L)$?

In a special case (2.1) is easily shown to have an affirmative answer as a consequence of well known results:

PROPOSITION 2.2. – *If there exists an ideal $I \in \mathscr{I}_L$ such that $I \cong_{\mathcal{O}[G]} \mathcal{O}[G]$ then $\mathbf{Fr}_K(\mathcal{O}_L)$. Furthermore, such an ideal exists if and only if G is an elementary abelian p-group. In this case $\mathscr{A}_{K[G]}(\mathcal{O}_L)$ is generated as an $\mathcal{O}$-lattice by the set $\{G\} \cup \{p^{-1}\mathrm{Tr}_G\}$, and $\mathcal{O}_L$ is generated over $\mathscr{A}_{K[G]}(\mathcal{O}_L)$ by any uniformising parameter.*

Proof. – For any ideal $I \in \mathscr{I}_L$ one has

$I \cong_{\mathcal{O}[G]} \mathcal{O}[G]$

$\Leftrightarrow$ I is a projective $\mathcal{O}[G]$-module ([20] Corollary 6.4)

$\Leftrightarrow$ I is a cohomologically trivial G-module (c.f. [18] Chapitre IX)

$\Leftrightarrow$ $\hat{\mathrm{H}}^0(G_{(1)}, I) = 1$ ([22] Theorem 2)

$\Leftrightarrow$ $\mathrm{Tr}_{G_{(1)}}(I) = I^{G_{(1)}}$.

Using the formulae (1.15) this last condition is seen to be equivalent to $G_{(0)} = G_{(1)} \geqslant G_{(2)} = 1$ and $v_L(I) \equiv 1$ modulo p^N (cf. [21] Theorem 2.1). But since $K/\mathbb{Q}_p$ is unramified (1.13) and (1.14) together imply that $G_{(2)} = 1$ if and only if G is elementary abelian. Thus, if such an ideal I exists then $\mathrm{ord}\,(G) = p^N$ so that $I \cong_{\mathcal{O}[G]} \wp_L$. In this case, if $\pi \in L$ then it is not difficult to check that $\wp_L = (\mathcal{O}[G])\pi$ if and only if $v_L(\pi) = 1$. But then $\mathrm{Tr}_G(\wp_L) = (\wp_L)^G = \wp_K$ and thus, since L/K is totally ramified, one has

$$\mathcal{O}_L = \mathcal{O} + \wp_L = (\wp_K^{-1}\mathrm{Tr}_G + \mathcal{O}[G])\pi$$

as was required. □

In case G is cyclic we can prove a result directly analogous to Proposition (2.2). In this case note that, since all questions of G-factor-equivalence are trivially satisfed (cf. (1.3) (*b*)), Corollary (1.10) implies that we need only check conditions for G-o-equivalence. In § 3, by an analysis of this question using techniques from [1] § 2.2 we shall prove

THEOREM 3. — *If G is cyclic then the following conditions are equivalent :*

(i) $\mathbf{Fr}_K(\mathscr{I}_L)$;

(ii) $\mathbf{Fr}_K(\mathcal{O}_L)$;

(iii) $N = 1$, or $N = 2$ *and* $R < p^2$, *or* $N > 2$ *and* $R < p(p-1)$.

Remarks. — (i) The equivalence (ii) $\Leftrightarrow$ (iii) is due originally to Bergé ([1], Corollary to Theorem 3), although the proof given here is very different from hers.

(ii) It is not true that $\mathbf{Fr}_K(\mathcal{O}_L)$ implies $\mathbf{Fr}_K(I)$ for all $I \in \mathscr{I}_L$.

If G is not cyclic our results do not give a complete characterisation of $\mathbf{Fr}_K(\mathscr{I}_L)$. However the explicit results we can prove may all be interpreted as providing evidence for an affirmative answer to the following

Open Question 2.3. — If G is not cyclic are the following conditions equivalent :

(i) $\mathbf{Fr}_K(\mathscr{I}_L)$;

(ii) $\mathbf{Fr}_K(\mathcal{O}_L)$;

(iii) G is an elementary abelian p-group ?

(Recall that the implication (iii) $\Rightarrow$ (ii) has already been proved in Proposition (2.2)).

For example, in § 4.1 we shall derive an upper bound on R from the assumption $\mathbf{Fr}_K(\mathscr{I}_L)$. To state this we assume that the Sylow p-subgroup $\mathrm{Syl}_p(G)$ of G has structure invariants

$$p^{n_1},\ p^{n_2},\ \ldots,\ p^{n_s}$$

for an integer s ($\geqslant 2$) and integers $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_s$. For brevity we shall often refer to such a group as being of type $(p^{n_1}, p^{n_2}, \ldots, p^{n_s})$.

THEOREM 4. — *If G is not cyclic and $\mathbf{Fr}_K(\mathscr{I}_L)$ then $R < p^s(p^{s-1}-1)^{-1}$. In particular, if $s \geqslant 3$ and $\mathbf{Fr}_K(\mathscr{I}_L)$ then $R < p$* so that $\mathcal{O}_L \circ_G \mathscr{A}_{K[G]}(\mathcal{O}_L)$.

Remark. – In fact one can prove that $\mathcal{O}_L \circ_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$ if and only if $R < p$. However no such simple criterion exists for the general ideal $I \in \mathcal{I}_L$.

An affirmative answer to (2.3) certainly requires a proof of the implication $\mathbf{Fr}_K(\mathcal{I}_L) \Rightarrow R = 1$ in case $\mathrm{Syl}_p(G)$ non-cyclic. However to improve the upper bounds of Theorem 4 by our approach would seem to require a technique for explicity describing associated orders in the case that $\mathrm{Syl}_p(G)$ is not cyclic. At the moment, even in case that $\mathrm{Syl}_p(G)$ is of type (p,p), we have not been able to develop such a technique. We do however have some results in this direction. Moreover these results seem to fit a common pattern which itself suggests further evidence for the implication $\mathbf{Fr}_K(\mathcal{I}_L) \Rightarrow R = 1$. We shall discuss this in a little more detail in § 4.3.

Theorem 4 indicates that $\mathbf{Fr}_K(\mathcal{I}_L)$ imposes strong restrictions on R. In a similar fashion the assumption $\mathbf{Fr}_K(\mathcal{O}_L)$ imposes strong restrictions on the abstract structure of $\mathrm{Syl}_p(G)$. Specifically in § 4.2 we shall prove.

THEOREM 5. – *If* $\mathcal{O}_L \wedge_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$ *then* $n_1 = n_s$, *i.e.* $\mathrm{Syl}_p(G)$ *is « homogenous ».*

This result gives some evidence for the implication (ii) $\Rightarrow$ (iii) of (2.3). In this context it also naturally raises the question of whether $\mathbf{Fr}_K(\mathcal{O}_L)$ is inherited by sub-extensions, i.e. of whether $\mathbf{Fr}_K(\mathcal{O}_L) \Rightarrow \mathbf{Fr}_K(\mathcal{O}_{L'})$ for all fields L' such that $K \subseteqq L' \subseteqq L$. Indeed if this is the case then (since $s > 1$ and $n_1 > 1$ implies that $\mathrm{Syl}_p(G)$ has a non-homogeneous quotient) the conditions $s > 1$ and $\mathbf{Fr}_K(\mathcal{O}_L)$ together imply (via Theorem 5) that $n_1 = 1$, as is required for an affirmative answer to (2.3). Note that the equivalence (ii) $\Leftrightarrow$ (iii) of Theorem 3 implies that $\mathbf{Fr}_K(\mathcal{O}_L)$ is inherited by subextensions in the cyclic case (a fact first noted in [1] § 4). More generally, one at least knows that the condition $\mathcal{O}_L \circ_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$ is inherited by subextensions (cf. the remark following the statement of Theorem 4).

Apart from the results of Theorems 3, 4 and 5 we have one further piece of evidence which suggests that the ideal $\mathcal{O}_L$ plays a distinguished role with respect to questions of freeness over associated orders. There is naturally a certain amount of interest in ideals $I \in \mathcal{I}_L$ which are « self-dual », i.e. which are $\mathcal{O}[G]$-isomorphic to the dual lattice defined with respect to the trace form of the extension L/K. It is of some interest therefore to question whether the self-duality of an ideal I has any implications concerning the validity of $\mathbf{Fr}_K(I)$. In general there is no strong implication – for example, if ord(G) is odd then the different of L/K has a square root whose inverse $A_{L/K}$ is necessarily self-dual and yet Theorems 3, 4 and 5 indicate that in general $\neg\,\mathbf{Fr}_K(\mathrm{A}_{L/K})$. However by the methods of this paper one can completely characterise those extensions L/K for which $\mathcal{O}_L$ is self-dual, and as a result verify that the self-duality of $\mathcal{O}_L$ does indeed imply $\mathbf{Fr}_K(\mathcal{O}_L)$ (this is true even for the case $p = 2$). This last result gives a partial answer to a question of Ph. Cassou-Noguès and M. J. Taylor [7] (page 148) (their question is raised without any ramification hypothesis on $K/\mathbb{Q}_p$) but, since it is not central to our exposition, we shall not prove it here.

Even though we cannot in general describe $\mathcal{A}_{K[G]}(I)$ in case G not cyclic, the techniques of Bergé allow us to explicitly describe the lattices $\mathcal{A}_{K[G]}(I)^H$ for each cocyclic subgroup $H \leqslant G$. Using these descriptions we can prove that, for any given abstract structure of G (and of the inertia group G_{ram}), the validity or otherwise of $\mathbf{Fr}_K(I)$ is dependent only upon the value $v_L(I)$ together with the abstract structure of the $\mathcal{O}$-order $\mathcal{A}_{K[G]}(I)$. This type of result suggests interesting « comparison » results in the number field case similar, for example, to those obtained by Wilson (c.f. [23]). To state our result precisely it seems worth while relaxing the condition that L/K is totally ramified.

THEOREM 6. – *Let K and K' be finite unramified extensions of $\mathbb{Q}_p$, and let Σ denote the compositum field KK'. Let L/K and L'/K' be (not necessarily totally ramified) abelian extensions of groups G and G' respectively. Assume that there exists an isomorphism $\Psi : G \cong G'$ which restricts to give an isomorphism of inertia groups $\Psi : G_{\mathrm{ram}} \cong G'_{\mathrm{ram}}$. Extending Ψ by Σ-linearity one obtains an isomorphism of Σ-algebras $\Psi : \Sigma[G] \cong \Sigma[G']$. If i is any integer such that Ψ restricts to give an isomorphism of $\mathcal{O}_\Sigma$-orders*

$$\Psi : \mathcal{O}_\Sigma \otimes_{\mathcal{O}_K} \mathcal{A}_{K[G]}(\wp_L^i) \cong \mathcal{O}_\Sigma \otimes_{\mathcal{O}_{K'}} \mathcal{A}_{K'}[\mathrm{G}](\wp_{L'}^i)$$

then $\mathbf{Fr}_K(\wp_L^{i\prime})$ if and only if $\mathbf{Fr}_{K'}(\wp_{L'}^i)$.

Remark. – If one restricts to the case $i=0$ (i.e. $\wp_L^i = \mathcal{O}_L$ and $\wp_{L'}^i = \mathcal{O}_{L'}$) then one can in fact prove the conclusion of Theorem 6 without assuming *a priori* that Ψ restricts to give an isomorphism $G_{\mathrm{ram}} \cong G'_{\mathrm{ram}}$. For this however one must use Noether's criterion together with the fact that $\mathcal{O}_L \circ_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$ if and only if $R < p$.

We end this section by remarking on those extensions not considered here. Firstly, our techniques apply equally well in the case that K is an unramified extension of $\mathbb{Q}_2$. However, we do not here consider this case since calculations tend to be more complicated (this is essentially because there are more ramification filtrations to consider, i.e. if $p = 2$ then knowledge of the abstract structure of G_{ram} does not specify the complete filtration). In this case one can obtain explicit results similar to those given above, but there are some differences apparent. For example, there are non-homogeneous extensions with $\mathbf{Fr}_K(\mathcal{O}_L)$, and also the condition $\mathcal{O}_L \circ_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$ is not in general inherited by subextensions. For an example of a calculation in this case (in fact involving the ideal $A_{L/K}$) see the appendix to [8]. Whatever the residue characteristic however, if we allow ramification in the extension $K/\mathbb{Q}_p$ then the results are very different. In particular, in this more general context the answer to (2.1) is negative – for example there are local Galois extensions F/E of degree p such that $\mathbf{Fr}_E(\mathcal{I}_F)$ and yet $\neg\, \mathbf{Fr}_E(\mathcal{O}_F)$ (c.f. [9]).

3. THE CYCLIC CASE

In the section we shall prove Theorem 3, and for this we must first recall the available techniques for describing the lattices $\mathcal{A}(L/K,i,j)$ in the case that G is cyclic. Throughout this section then L/K is a totally ramified cyclic extension.

3.1. Description of the associated orders.

In this subsection we shall analyse the lattices $\mathcal{A}(L/K,i,j)$. The results quoted here are either standard facts of ramification theory (for which see for example [18] Chapitre IV) or else taken from [1] § 2.2, and so no proofs will be given.

In deciding questions of G-o-equivalence we are only interested in the associated orders of the lattices $\mathcal{A}(L/K,i,j)$ and hence, without any loss of generality, we may assume that $i \leqslant j$. (Indeed, even if $i > j$ one has $i - tp^N R < j$ for any sufficiently large integer t, and $\mathcal{A}(L/K,i-tp^N R,j) = p^t \mathcal{A}(L/K,i,j)$ has the same associated order as $\mathcal{A}(L/K,i,j)$.) With this assumption $\mathcal{A}(L/K,i,j) \subseteqq \mathcal{A}(L/K,j,j)$ which is an $\mathcal{O}$-order in $K[G]$ and so in contained is $\mathcal{M}(\mathcal{O},G)$. We shall therefore first give an explicit description of $\mathcal{M}(\mathcal{O},G)$.

We must introduce some notation. Let C denote the subgroup of G of order R. Let Π denote any uniformising parameter for L. The map defined on G by $g \mapsto \Pi^g/\Pi$ induces an isomorphism θ_0 (independent of the choice of Π) between C and a subgroup of the roots of unity of the residue field of K. In particular therefore K contains a primitive R-th root of unity. Hence, if χ is any element of $C^\dagger$, then the corresponding idempotent $e_\chi = 1/R \sum_{c \in C} \chi(c^{-1})c$ belongs to $\mathcal{O}[C]$. Therefore any $\mathcal{O}[G]$-lattice X decomposes as a direct sum

$$X = \bigoplus_{\chi \in C^\dagger} e_\chi X .$$

To give an $\mathcal{O}$-basis of X one need therefore only give an $\mathcal{O}$-basis for each isotypic component $e_\chi X$. This is easy in the case $X = \mathcal{M}(\mathcal{O}, G)$. For this we need some more notation. For each integer i with $0 \leqslant i \leqslant N$, we let G_i denote the (unique) subgroup of G of order p^i. We also let e_i denote the corresponding idempotent $e_{G_i} \in \mathbb{Q}_p[G_i]$. We let g_* denote a generator of $G_N(=\mathrm{Syl}_p(G))$. When passing to subextensions we shall identify C with its image in each quotient group G/G_i. For each integer i with $0 \leqslant i \leqslant N$ we set $L_i = L^{G_i}$. Furthermore, for each integer $i \geqslant 0$ we define an integer

$$m_i = \begin{cases} p^{i-1}(p-1), & \text{if} \quad i \geqslant 1\,; \\ 1, & \text{if} \quad i = 0\,. \end{cases}$$

LEMMA 3.1. – *For each character $\chi \in C^\dagger$ the lattice $e_\chi \mathcal{M}(\mathcal{O}, G)$ has an $\mathcal{O}$-basis given by the set*

$$\{e_\chi e_i (g_* - 1)^{j_i} : 0 \leqslant i \leqslant N, 0 \leqslant j_i < m_{N-i}\} .$$

To give a similar description of the lattices $e_\chi \mathcal{A}(L/K, i, j)$ we must be more precise about the character group $C^\dagger$. Thus we let $\chi_{L/K}$ denote the (unique) element of $C^\dagger$ which induces by passage to the residue field the isomorphism θ_0. Then $\chi_{L/K}$ is a generator of $C^\dagger$, and hence to each character $\chi \in C^\dagger$ one can associate integers

$$u_{L/K, i, \chi} \in \{1, 2, \ldots, R\}$$

(written $u_{i,\chi}$ if the extension L/K is clear from context) which are defined for each integer $i = 0, 1, \ldots, N$ by

$$\chi = \chi_{L/K}^{-p^i u_{i,\chi}} . \tag{3.2}$$

It is not difficult to prove

LEMMA 3.3. — *Let χ be an element of $C^{\dagger}$. For any (non-zero) element $x \in L$ one has*

$$v_L(e_\chi x) \geqslant v_L(x),$$

with equality here if, and only if, $\chi = \chi_{L/K}^{v_L(x)}$. In particular, for each integer $i = 1, 2, \ldots, N$ and for each (non-zero) element $x \in L$, one has

$$v_{L_i}(e_\chi e_i x) \equiv - u_{L/K,i,\chi} \text{ modulo } (R). \tag{3.4}$$

By Lemma (1.13) the complete ramification filtration of G is known. By substituting this into the expression (1.15) (a) one obtains

$$v_{L_s}(e_s(\wp_L^k)) = \left[\frac{1}{p^s}\left(k - \frac{R(p^s-1)}{p-1} + p^s - 1\right)\right] \tag{3.5}$$

for each integer k and each integer s such that $0 \leqslant s \leqslant N$. In the special case of the lattices $\mathscr{A}(L/K, i, 0)$ the result of Lemma (3.3) together with the formula (3.5) proves that

$$e_\chi e_s \in \mathscr{A}(L/K, i, 0) \Leftrightarrow i > \frac{R(p^s-1)}{p-1} - p^s u_{s,\chi}. \tag{3.6$_{(i,s)}$}$$

Next we examine the effect of action by elements of $(g_* - 1)\mathscr{M}(\mathcal{O}, G)$ on the valuations of elements of L. Well, $g_* \in G^{(1)} \backslash G^{(2)}$ (Lemma (1.13)), i.e. $g_* \in G_{(R)} \backslash G_{(R+1)}$ ((1.14)), and thus, by a standard property of the lower filtration, for any (non-zero) element $x \in L$ one has

$$v_L((g_* - 1)x) \geqslant v_L(x) + R \tag{3.7}$$

with equality here if and only if $v_L(x) \not\equiv 0$ modulo (p).

Finally we specialise to the case $\mathscr{A}(L/K, 0, 0) = \mathscr{A}_{K[G]}(\mathcal{O}_L)$. Using (3.5) and (3.7) one sees that $(g_* - 1)\mathscr{M}(\mathcal{O}, G) \subseteqq \mathscr{A}_{K[G]}(\mathcal{O}_L)$. Lemma (3.1) therefore implies that to give an explicit description of each $e_\chi \mathscr{A}_{K[G]}(\mathcal{O}_L)$ it suffices to determine which elements of the set

$$\bigoplus_{i=0}^{i=N} \mathcal{O} e_\chi e_i$$

belong to $\mathscr{A}_{K[G]}(\mathcal{O}_L)$. Using the equivalence $(3.6)_{(0,s)}$ this is not difficult. To record the final result we define for each non-negative integer j an integer

$$U_j = \left[\frac{R(p^j-1)}{p^j(p-1)}\right]. \tag{3.8}$$

PROPOSITION 3.9 (Bergé). — *Let χ be an element of $C^\dagger$. The lattice $e_\chi \mathscr{A}_{K[G]}(\mathcal{O}_L)$ has an $\mathcal{O}$-basis given by the set*

$$\{e_\chi e_i : 0 \leqslant i \leqslant N, u_{i,\chi} > U_i\} \cup \{pe_\chi e_i : 0 \leqslant i \leqslant N, u_{i,\chi} \leqslant U_i\}$$
$$\cup \{e_\chi e_i(g_* - 1)^{j_i} : 0 \leqslant i < N, 1 \leqslant j_i < m_{N-i}\}.$$

3.2. The proof of Theorem 3.

In this subsection we assume the notations of Theorem 3 and of § 3.1. Since G is cyclic, in order to prove Theorem 3 by means of Corollary (1.10) we need only check questions of G-o-equivalence.

We shall first deal quickly with the case $N = 1$.

LEMMA 3.10. — *If $N = 1$ then $\mathrm{Fr}_K(I)$ for all $I \in \mathscr{I}_L$.*

Proof. — Fix $I \in \mathscr{I}_L$ and set $\mathscr{A} = \mathscr{A}_{K[G]}(I)$. Corollary (1.10) implies that $I \cong_{\mathcal{O}[G]} \mathscr{A}$ if and only if

$$\mathscr{A}_{K[G/G_1]}(I^{G_1}) = \mathscr{A}_{K[G/G_1]}(\mathscr{A}^{G_1}) \tag{3.11}$$

(recall also the remarks following Definition (1.9)). But $G/G_1 = C$ has order coprime to p so that $\mathcal{O}[C] = \mathscr{M}(\mathcal{O}, C)$ and the equality (3.11) is clear. □

Henceforth we restrict to the case $N \geqslant 2$. We shall first prove the implication (i) $\Rightarrow$ (iii) of Theorem 3.

Set $H = G_{N-1}$, $F = L_{N-1}$ and $\Gamma = G/H$ (a group of order pR). We shall now show that if either $R > p^2$, or if $N \geqslant 3$ and $R > p(p-1)$, then for any ideal $I \in \mathscr{I}_L$ one has

$$\mathscr{A}_{K[\Gamma]}(I^H) \subsetneqq \mathscr{A}_{K[\Gamma]}(\mathscr{A}_{K[G]}(I)^H) \tag{3.12}$$

so that I is not G-o-equivalent to $\mathscr{A}_{K[G]}(I)$. To prove this we shall first re-interpret these rather curious restrictions on N and R.

LEMMA 3.13. – *Let $N \geqslant 2$. Then*

$$(3.14)_\iota \qquad v_F((\wp_L^\iota)^H) - R < v_F(e_H(\wp_L^\iota)) \leqslant v_F((\wp_L^\iota)^H) - p$$

for all integers ι if and only if either $R > p^2$, or $N \geqslant 3$ and $R > p(p-1)$.

Proof. – Explicitly one has $v_F((\wp_L^\iota)^H) = \lceil \iota/p^{N-1} \rceil$, and (by (3.5))

$$(3.15) \quad v_F(e_H(\wp_L^\iota)) = \left\lceil \frac{1}{p^{N-1}} \left(\iota - \frac{R(p^{N-1}-1)}{p-1} + p^{N-1} - 1 \right) \right\rceil .$$

Now if $R > p^2$, or if $N \geqslant 3$ and $R > p(p-1)$, then it is not difficult to deduce $(3.14)_\iota$ by using these explicit expressions. On the other hand, if $R < p(p-1)$, or if $N = 2$ and $R < p^2$, then $\iota = 0$ does not satisfy the second inequality of $(3.14)_0$. □

We fix an integer ι, and set $I = \wp_L^\iota$. For brevity we set $\iota_* = v_F(e_H(I))$ and $\iota^* = v_F(I^H)$. We want to compare $\mathscr{A}_{K[\Gamma]}(I^H)$ with $\mathscr{A}_{K[\Gamma]}(\mathscr{A}_{K[G]}(I)^H)$, i.e. (by (1.12)) to compare $\mathscr{A}(F/K, \iota^*, \iota^*)$ with $\mathscr{A}_{K[\Gamma]}(\mathscr{A}(F/K, \iota_*, \iota^*))$. We assume now that either $R > p^2$, or that $N \geqslant 3$ and $R > p(p-1)$, so that the inequalities (3.14) are all satisfied. We let e denote the idempotent $e_{\Gamma_1} \in K[\Gamma]$. Note that for each integer j the formula (3.5) implies

$$(3.16)_j \quad j - R \leqslant v_F(e(\wp_F^j)) \leqslant j - R + p - 1 < j - p .$$

Because of the right hand inequalities of (3.14) and (3.16) there exists an integer x such that

$$(3.17) \qquad \text{maximum of } \{v_F(e(\wp_F^{\iota^*})), \iota_*\} \leqslant px < \iota^* .$$

We choose such an integer x and set $\theta = \chi_{F/K}^{-px} \in C^\dagger$ (the character $\chi_{F/K}$ was defined in § 3.1). Our aim is to prove that for any such character θ one has a strict inclusion

$$(3.18) \qquad e_\theta \mathscr{A}(F/K, \iota^*, \iota^*) \subsetneqq e_\theta \mathscr{A}_{K[\Gamma]}(\mathscr{A}(F/K, \iota_*, \iota^*)) .$$

Well, by combining Lemma (3.3) together with (3.17) one sees that $e_\theta e \notin \mathscr{A}(F/K, \iota^*, \iota^*)$, i.e. that $e_\theta \mathscr{A}(F/K, \iota^*, \iota^*) = e_\theta \mathscr{O}[\Gamma]$, and also that

$$(3.19) \qquad e_\theta \notin e_\theta \mathscr{A}(F/K, \iota_*, \iota^*) .$$

But on the other hand, from the left hand inequalities of (3.16) and (3.14) one has

$$v_F(pe(\wp_F^{\iota_*})) = pR + v_F(e(\wp_L^{\iota_*})) \geqslant pR + \iota_* - R > \iota^* + (p-2)R > i^*$$

so that $pe_\theta\mathcal{M}(\mathcal{O},\Gamma) \subseteqq e_\theta\mathscr{A}(F/K,\imath_*,\imath^*)$. Now since $\imath_* < \imath^*$ the lattice $e_\theta\mathscr{A}(F/K,\imath_*,\imath^*)$ is a mutliplicatively closed sublattice of $e_\theta\mathscr{A}(F/K,\imath^*,\imath^*) = e_\theta\mathcal{O}[\Gamma]$. A typical element of $e_\theta\mathscr{A}(F/K,\imath_*,\imath^*)$ can therefore be written in the form

$$\alpha = \sum_{i=0}^{i=p-2} a_i e_\theta(\gamma_* - 1)^i + pae_\theta e \qquad ,$$

$$\{a_i : i=0,\ldots,p-2\} \cup \{a\} \subset \mathcal{O},$$

where here γ_* is some generator of $\mathrm{Syl}_p(\Gamma)$.

Now $\alpha^p \in \mathscr{A}(F/K,\imath^*,\imath_*)$, and $\alpha^p \equiv a_0^p e_\theta$ modulo $pe_\theta\mathcal{M}(\mathcal{O},\Gamma)$, so that $a_0^p e_\theta \in \mathscr{A}(F/K,\imath_*,\imath^*)$. Because of (3.19) we must therefore have $p\,|\,a_0$. Hence one has

$$e_\theta e \cdot \alpha = (a_O + pa)e_\theta e \in pe_\theta\mathcal{M}(\mathcal{O},\Gamma) \subset e_\theta\mathscr{A}(F/K,\imath_*,i^*).$$

Since α is an arbitrary element of $e_\theta\mathscr{A}(F/K,\imath_*,i^*)$ we have proved that

$$e_\theta e \in e_\theta\mathscr{A}_{K[\Gamma]}(\mathscr{A}(F/K,\imath_*,i^*)).$$

But $e_\theta e \notin e_\theta\mathscr{A}(F/K,\imath^*,\imath^*)$ and hence we have proved (3.18). This then completes the proof of the implication (i) $\Rightarrow$ (iii) of Theorem 3.

Since the implication (ii) $\Rightarrow$ (i) of Theorem 3 is trivial it only remains for us to prove the implication (iii) $\Rightarrow$ (ii). We shall first deal with the special case $N = 2$. In this case one knows that $\mathcal{O}_L \circ_G \mathscr{A}_{K[G]}(\mathcal{O}_L)$ if and only if

$$\mathscr{A}_{K[\Gamma]}(\mathcal{O}_F) = \mathscr{A}_{K[\Gamma]}(\mathscr{A}_{K[G]}(\mathcal{O}_L)^{G_1}) \tag{3.20}$$

where here we again set $\Gamma = G/G_1$ and $F = L_1$. Proposition (3.9) gives an explicit description of $\mathscr{A}_{K[\Gamma]}(\mathcal{O}_F)$ and we shall use this to check the validity of (3.20).

LEMMA 3.21. – *If $N = 2$ then $\mathcal{O}_L \circ_G \mathscr{A}_{K[G]}(\mathcal{O}_F)$ if and only if $R < p^2$.*

Proof. – The necessity of the condition $R < p^2$ has already been proved above. We shall show here that if $R < p^2$ the (3.20) is valid. Well, taking into account the inclusions (1.11) one sees that (3.20) is satisfied if there is no character $\theta \in C^\dagger$ such that

$$e_\theta e \in \mathscr{A}_{K[\Gamma]}(\mathscr{A}(F/K,-U_1,0)) \backslash \mathscr{A}_{K[\Gamma]}(\mathcal{O}_F) \tag{3.22}$$

where here we write $e = e_{\Gamma_1} \in K[\Gamma]$ (recall that $U_1 = [R/p]$ so that, by (3.5), $v_F(e_{G_1}(\mathcal{O}_L)) = -U_1)$. We assume therefore that there exists a character $\theta \in C^\dagger$ such that $e_\theta e \notin \mathcal{A}_{K[\Gamma]}(\mathcal{O}_F)$, i.e. such that $u_{F/K,1,\theta} \leqslant U_1$ (c.f. Proposition (3.9), and (3.2) for the definition of the $u_{F/K,i,\theta})$. We must show that $e_\theta e \notin \mathcal{A}_{K[\Gamma]}(\mathcal{A}(F/K, -U_1,0))$. Now $e_\theta e \notin \mathcal{A}(F/K, -U_1,0)$ while $pe_\theta \mathcal{M}(\mathcal{O},\Gamma) \subset \mathcal{A}(F/K, -U_1,0)$ and from this, by using the same type of analysis as used to prove (3.18), it is not difficult to verify that

$$(3.23)\quad e_\theta e \notin \mathcal{A}_{K[\Gamma]}(\mathcal{A}(F/K, -U_1,0)) \Leftrightarrow e_\theta \in \mathcal{A}(F/K, -U_1,0) \Leftrightarrow -U_1 > -u_{F/K,0,\theta}$$

where the last equivalence here is a consequence of $(3.6)_{(-U_1,0)}$. Now (3.2) implies that $pu_{F/K,1,\theta} \equiv u_{F/K,0,\theta}$ modulo (R). But $pu_{F/K,1,\theta} \leqslant pU_1 < R$ and hence $pu_{F/K,1,\theta} = u_{F/K,0,\theta}$. Thus the inequality (3.23) is certainly satisfied if $U_1 < p$, i.e. if $R < p^2$. □

At this stage, to complete the proof of Theorem 3 we need only prove that if $R < p(p-1)$ (and $N \geqslant 3$) then $\mathcal{O}_L \circ_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$. Thus we shall henceforth assume that $R < p(p-1)$.

The analysis in this case uses the same basic idea as used in Lemma (3.21). In this new case however we have need of a preliminary lemma. For any character $\theta \in C^\dagger$ we define an integer $t(L/K,\theta) =$ maximum of $\{i : 0 \leqslant i \leqslant N, \{e_\theta e_j : 0 \leqslant j \leqslant i\} \subseteq \mathcal{A}_{K[G]}(\mathcal{O}_L)\}$.

Lemma 3.24. — *Let $R < p(p-1)$. Fix a character $\theta \in C^\dagger$, and set $t = t(L/K,\theta)$. If $t < N$ then $e_\theta e_t \in e_\theta \mathcal{A}(L/K, -U_m,0)$ for each integer $m \geqslant 1$.*

Proof. — Assume that $t < N$. By Proposition (3.9) one knows that t satisfies both $u_{t,\theta} > U_t$ and $u_{t+1,\theta} \leqslant U_{t+1}$. It follows that

$$pu_{t+1,\theta} \leqslant pU_{t+1} \leqslant U_t + R < u_{t,\theta} + R,$$

and hence (since $pu_{t+1,\theta} \equiv u_{t,\theta}$ modulo (R)) that $pu_{t+1,\theta} = u_{t,\theta}$. Thus

$$(3.25)\qquad u_{t,\theta} \geqslant p.$$

On the other hand, $(3.6)_{(-U_m,t)}$ implies that $e_\theta e_t \in \mathcal{A}(L/K, -U_m,0)$ if, and only if,

$$(3.26)\qquad p^t u_{t,\theta} > R(p^t-1)/(p-1) + U_m.$$

But the inequality (3.26) is a consequence of (3.25) together with the fact that $U_m \leqslant [R/(p-1)]$, and the assumption that $R < p(p-1)$. □

Now to prove $\mathcal{O}_L \circ_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$ it suffices to prove that

$$(3.27)_i \qquad \mathcal{A}_{K[G/G_i]}(\mathcal{O}_{L_i}) = \mathcal{A}_{K[G/G_i]}(\mathcal{A}(L_i/K, -U_i, 0))$$

for all integers $i = 1,2, \ldots, N$. We fix an integer i with $0 \leqslant i \leqslant N$, and set $F = L_i$ with $\Gamma = G/G_i$, so that Γ has order $p^{N-i}R$. We now let γ_* denote a generator of the group $\mathrm{Syl}_p(\Gamma)$. For any character $\theta \in C^\dagger$ one has

$$(\gamma_* - 1)e_\theta \mathcal{M}(\mathcal{O}, \Gamma) \subset e_\theta \mathcal{A}_{K[\Gamma]}(\mathcal{O}_F)$$

$$\subseteqq \mathcal{A}_{K[\Gamma]e_\theta}(e_\theta \mathcal{A}(F/K, -U_i, 0)) \subseteqq e_\theta \mathcal{M}(\mathcal{O}, \Gamma)$$

(cf. Proposition (3.9) for the first inclusion and (1.11) for the second). Given the explicit description of $e_\theta \mathcal{M}(\mathcal{O}, \Gamma)$ in Lemma (3.1) we need therefore only prove that

$$(3.28) \quad \mathcal{A}_{K[\Gamma]e_\theta}(e_\theta \mathcal{A}(F/K, -U_i, 0)) \cap \left(\bigoplus_{j=0}^{j=N-1} \mathcal{O} e_\theta e_{\Gamma_j} \right) \subset e_\theta \mathcal{A}_{K[\Gamma]}(\mathcal{O}_F).$$

Let $\beta = \sum_{j=0}^{j=N-i} b_j e_\theta e_{\Gamma_j}$ be an element of the left hand side of (3.28). Set $t = t(F/K, \theta)$. If $t = N - i$ then $e_\theta \mathcal{A}_{K[\Gamma]}(\mathcal{O}_F) = e_\theta \mathcal{M}(\mathcal{O}, \Gamma)$ and the inclusion (3.28) is obvious. On the other hand, if $t < N - i$ then, setting

$$\delta = \sum_{j=0}^{j=t} b_j e_\theta e_{\Gamma_j}$$

one has $\delta \in e_\theta \mathcal{A}_{K[\Gamma]}(\mathcal{O}_F)$ and so $\beta - \delta \in \mathcal{A}_{K[\Gamma]e_\theta}(e_\theta \mathcal{A}(F/K, -U_i, 0))$. But by Lemma (3.24) one knows that $e_\theta e_{\Gamma_t} \in e_\theta \mathcal{A}(F/K, -U_i, 0)$ and therefore

$$\beta - \delta = (\beta - \delta) e_\theta e_{\Gamma_t} \in e_\theta \mathcal{A}(F/K, -U_i, 0) \subseteqq e_\theta \mathcal{A}_{K[\Gamma]}(\mathcal{O}_F).$$

Thus $\beta = (\beta - \delta) + \delta \in e_\theta \mathcal{A}_{K[\Gamma]}(\mathcal{O}_F)$ as was required to prove (3.28).

This then completes the proof of Theorem 3. □

4. THE NON-CYCLIC CASE

In this section we shall prove Theorems 4 and 5 (in §§ 4.1 and 4.2 respectively). In this non-cyclic case our results are only partial since we do not have good descriptions of the associated orders $\mathcal{A}_{K[G]}(I)$. Indeed the two results we prove here both essentially result merely from a first analysis of the situation in the 'smallest possible' non-cyclic case, i.e. that in which $\mathrm{Syl}_p(G)$ is of type (p,p). In § 4.3 we shall briefly discuss a possible way to improve our results.

4.1. A proof of Theorem 4.

We first note that $\mathbf{Fr}_K(\mathcal{I}_L) \Rightarrow \mathbf{Fr}_K(\mathcal{I}_{L'})$ for any subextension L'. Indeed, if $K \subseteqq L' \subseteqq L$ with $H = \mathrm{Gal}(L/L')$, and if $\mathbf{Fr}_K(I)$ for some $I \in \mathcal{I}_L$, then $e_H \mathcal{A}_{K[G]}(I)$ is an $\mathcal{O}$-order and $e_H I \cong_{\mathcal{O}[G]} e_H \mathcal{A}_{K[G]}(I)$. Without loss of generality therefore, in proving Theorem 4 we may pass to any subextension L' such that $|L : L'|$ is a power of p. Taking this into account we shall assume in this subsection that $\mathrm{Syl}_p(G)$ is an elementary abelian group of order p^s.

The result of Theorem 4 is an immediate consequence of the following result.

PROPOSITION 4.1. — *There exists an ideal $I \in \mathcal{I}_L$ such that $I \circ_G \mathcal{A}_{K[G]}(I)$ if and only if $R < p^s(p^{s-1}-1)^{-1}$.*

Remark. — If $s > 2$ the condition here is that $R < p$. If $s = 2$ the condition is that $R \leqslant p + 1$.

We first note that if $R < p$ then $\mathcal{O}_L \circ_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$. Indeed if $R < p$ then Proposition (3.9) and Lemma (3.1) together imply that $\mathcal{A}_{K[G/H]}((\mathcal{O}_L)^H) = \mathcal{M}(\mathcal{O}, G/H)$ for any cocyclic subgroup $H \leqslant G$, and so G-$\circ$-equivalence follows trivially from the inclusions (1.11). (In fact one can also prove that $\mathcal{O}_L \circ_G \mathcal{A}_{K[G[}(\mathcal{O}_L)$ implies $R < p$). On the other hand, if $s = 2$ and $R = p + 1$ then it is not difficult to prove that $\wp_L^R \circ_G \mathcal{A}_{K[G]}(\wp_L^R)$.

We need therefore only prove that $I \circ_G \mathscr{A}_{K[G]}(I) \Rightarrow R < p^s(p^{s-1}-1)^{-1}$. The analysis of G-$\circ$-equivalence we shall give here follows the same pattern as that used in order to prove Theorem 3.

Let H denote any subgroup of $\mathrm{Syl}_p(G)$ of index p. Set $F = L^{\mathrm{H}}$ with $\Gamma = \mathrm{G}/H = \mathrm{Gal}(F/K)$, a cyclic group of order pR. Set $e = e_{\Gamma_1} \in K[\Gamma]$. Let $I = \wp_L^{\iota}$ and then define integers ι^* and ι_* by $I^H = \wp_F^{\iota^*}$ and $\mathrm{Tr}_H(I) = \wp_F^{\iota_*}$. By Lemma (1.13) the ramification filtration of G is $G = G^{(0)} = \mathrm{G}^{(1)} > G^{(2)} = 1$, and so the formulae (1.15) specialise to give

$$(4.2) \quad \iota^* = \left\lceil \frac{\iota}{p^{s-1}} \right\rceil \qquad \text{and} \qquad \iota_* = 1 + R + \left[\frac{1}{p^{s-1}}(\iota - 1 - R) \right].$$

We set $\mathscr{A}' = \mathscr{A}(F/K, \iota_* - pR, \iota^*)$, i.e. $\mathscr{A}' = p^{2-s}\mathscr{A}_{K[G]}(I)^H$. We shall prove that

$$\mathscr{A}_{K[\Gamma]}(I^H) = \mathscr{A}_{K[\Gamma]}(\mathscr{A}') \Rightarrow R < p^s(p^{s-1}-1)^{-1}.$$

For this we shall first show that if both

$$(4.3)\,(a) \quad \iota^* - R \leqslant v_F(e(I^H)) \leqslant \iota^* - R + p - 1 < \iota^*$$

and

$$(4.3)\,(b) \qquad v_F(e(\mathrm{Tr}_H(I))) > v_F(e(I^H))$$

then

$$(4.4) \qquad \mathscr{A}_{K[\Gamma]}(I^H) \subsetneqq \mathscr{A}_{K[\Gamma]}(\mathscr{A}').$$

We shall then show that the condition $R > p^s(p^{s-1}-1)^{-1}$ is sufficient to ensure that the inequalities of (4.3) are satisfied.

We assume for the moment then that (4.3) is satisfied, and deduce (4.4). We set $F_1 = F^{\Gamma_1}$. Using the notation of § 3.1 we let θ denote the character of C which is defined by the condition $u_{F/K,1,\theta} \equiv -v_{F_1}(e(I^H))$ modulo (R). For this character Lemma (3.3) and (4.3) (a) together imply that

$$v_F(e_\theta e(I^H)) = v_F(e(I^H)) < \iota^*$$

so that $e_\theta e \notin \mathscr{A}_{K[\Gamma]}(I^H)$. We will now show that $e_\theta e \in \mathscr{A}_{K[\Gamma]}(\mathscr{A}')$ which thus establishes (4.4).

We first note that $pe_\theta\mathcal{M}(\mathcal{O},\Gamma) = pe_\theta\mathcal{O}[\Gamma] + p\mathcal{O}e_\theta e \subset \mathcal{A}'$. Indeed, $\imath_* > \imath^*$ so that $p\mathcal{O}[\Gamma] \subset \mathcal{A}'$. Also, by assumption one has

$$v_{F_1}(e(\mathrm{Tr}_H(I))) > v_{F_1}(e(I^H)),$$

and so Lemma (3.3) together with the first inequality of (4.3) (*a*) implies

$$\begin{aligned} v_F(pe_\theta e(\wp_F^{\imath_* - pR})) = v_F(e_\theta e(\mathrm{Tr}_H(I))) &= pv_{F_1}(e_\theta e(\mathrm{Tr}_H(I))) \\ &\geqslant p(v_{F_1}(e(I^H)) + R) \geqslant \imath^* + (p-1)R > \imath^* \end{aligned}$$

so that $pe_\theta e \in \mathcal{A}'$. Now

$$\imath_* - pR \leqslant \imath^* - R$$

(an easy consequence of (4.2)), from which we deduce that $e_\theta \notin \mathcal{A}'$, and also that $\mathcal{A}'$ is a multiplicatively closed sublattice of $e_\theta\mathcal{A}(L/K,\imath^*,\imath^*) = e_\theta\mathcal{A}_{K[\Gamma]}(I^H) \subseteqq e_\theta\mathcal{M}(\mathcal{O},\Gamma)$. Thus if γ_* is a generator of $\mathrm{Syl}_p(\Gamma)$ and

$$\alpha = \sum_{i=0}^{i=p-2} a_i e_\theta(\gamma_* - 1)^i + ae_\theta e \in \mathcal{A}'$$

$$\{a_i : i=0,1,\cdots,p-2\} \cup \{a\} \subset \mathcal{O},$$

then $\alpha^p \in \mathcal{A}'$. But $\alpha^p \equiv a_0^p e_\theta + a^p e_\theta e$ modulo $pe_\theta\mathcal{M}(\mathcal{O},\Gamma)$ and hence $a_0^p e_\theta + a^p e_\theta e \in \mathcal{A}'$. Hence $a^p e_\theta e \in \mathcal{A}_{K[\Gamma]}(I^H)$ so that $p|a^p$, i.e. $p|a$. Hence $a_0^p e_\theta \in \mathcal{A}'$ and therefore $p|a_0$. Now α is an arbitrary element of $\mathcal{A}'$, and our argument has shown that

$$e_\theta e.\alpha = (a_0 + a)e_\theta e \in pe_\theta\mathcal{M}(\mathcal{O},\Gamma) \subset \mathcal{A}'.$$

Thus $e_\theta e \in \mathcal{A}_{K[\Gamma]}(\mathcal{A}')$ as was required.

It therefore suffices to prove that the conditions (4.3) are satisfied whenever R is 'sufficiently large'. Using (3.5) it is easy to see that (4.3) (*a*) is satisfied for any $R > p$. As for (4.3) (*b*) the explicit formulae of (3.5) and (4.2) give

$$v_{F_1}(e(\mathrm{Tr}_H(I))) = \left[\frac{1}{p}\left(1 + R + \left[\frac{1}{p^{s-1}}(\imath - 1 - R)\right] - R + p - 1\right)\right]$$

and

$$v_{F_1}(e(I^H)) = \left[\frac{1}{p}\left(\left[\frac{\imath}{p^{s-1}}\right] - R + p - 1\right)\right].$$

Hence condition (4.3) (b) is satisfied if and only if

$$\left[\frac{1}{p}\left(1+R+\left[\frac{1}{p^{s-1}}(\imath-1-R)\right]-R+p-1\right)\right]>\left[\frac{1}{p}\left(\left[\frac{\imath}{p^{s-1}}\right]-R+p-1\right)\right].$$

which is satisfied if

$$1+R+\left[\frac{1}{p^{s-1}}(\imath-1-R)\right]\geqslant\left[\frac{\imath}{p^{s-1}}\right]+p,$$

which is satisfied if

$$1+R+\left[\frac{\imath}{p^{s-1}}\right]-1-\left[\frac{R}{p^{s-1}}\right]\geqslant\left[\frac{\imath}{p^{s-1}}\right]+p,$$

which is satisfied if

$$R-R/p^{s-1}>p,$$

which is satisfied if and only if

$$R>p^{s}(p^{s-1}-1)^{-1}.$$

□

4.2. A proof of Theorem 5.

In this subsection we prove Theorem 5. For this we shall first make a reduction to the case of p-groups.

If $\mathcal{O}_L \wedge_G \mathcal{A}_{K[G]}(\mathcal{O}_L)$ then, by (1.6), for any subgroup $H \leqslant G$ one has

$$(4.5)_H \qquad (\mathcal{O}_L)^H \wedge_{G/H} \mathcal{A}_{K[G]}(\mathcal{O}_L)^H .$$

But $(\mathcal{O}_L)^H = \mathcal{O}_{L^H}$ and, if $p \nmid \operatorname{ord}(H)$, then

$$\begin{aligned}\mathcal{A}_{K[G]}(\mathcal{O}_L)^H &= e_H\mathcal{A}_{K[G]}(\mathcal{O}_L) = \mathcal{A}_{K[G/H]}(e_H(\mathcal{O}_L))\\ &= \mathcal{A}_{K[G/H]}((\mathcal{O}_L)^H) = \mathcal{A}_{K[G/H]}(\mathcal{O}_{L^H}).\end{aligned}$$

In order to prove Theorem 5 we need therefore only consider the case of G a p-group (i.e. for the reduction use $(4.5)_C$ with C the subgroup of G of order R). In this section we shall therefore assume that $R = 1$.

In general of course for a subgroup $H \leqslant G$ one has $\mathcal{A}_{K[G]}(\mathcal{O}_L)^H = \mathcal{A}(L^H/K, i(H), j(H))$ for suitable integers $i(H)$ and $j(H)$ (cf. Lemma (1.12)). In proving Theorem 5 we shall choose a particular subgroup $H_0 < G$, compute explicitly the integers $i(H_0)$ and $j(H_0)$, and then show that $(4.5)_{H_0}$ implies $n_1 = n_s$. Of the subextensions available to us Proposition (2.2) gives us explicit information on the maximal elementary abelian extension of K which is contained in L. Thus we choose $H_0 = G^{(2)}$, and set $F = L^{H_0}$. This field F is an elementary abelian extension of K of degree p^s. We set $\Gamma = G/H_0 = \mathrm{Gal}(F/K)$.

We assume now that $(4.5)_{H_0}$ is satisfied, i.e. that $\mathcal{O}_F \wedge_\Gamma \mathcal{A}_{K[G]}(\mathcal{O}_L)^{H_0}$, or equivalently (Theorem 1) that

$$\mathcal{O}[G]^{H_0} \wedge_\Gamma \mathcal{A}_{K[G]}(\mathcal{O}_L)^{H_0}. \tag{4.6}$$

To compute with expression (4.6) we must first describe the lattices $\mathcal{A}_{K[G]}(\mathcal{O}_L)^H$ for each subgroup H such that $H_0 \leqslant H \leqslant G$.

LEMMA 4.7. – *If H is any subgroup of G such that $H_0 \leqslant H \leqslant G$ then*

$$p^{n_1-N}\mathcal{A}_{K[G]}(\mathcal{O}_L)^H = \begin{cases} e_H\mathcal{M}(\mathcal{O},G), & \text{if } \operatorname{ord}(G/H) = p \\ \mathcal{O}e_G, & \text{if } H = G \\ p^{1-s}\mathcal{A}(F/K,-\kappa,0), & \text{if } H = H_0, \end{cases}$$

where in case $H = H_0$ we have used the identification $e_H\mathcal{M}(\mathcal{O},G) = \mathcal{M}(\mathcal{O},G/H)$, and κ is an explicitly computable non-negative integer which satisfies $\kappa = 0 \Leftrightarrow n_1 = n_s$.

Assuming for the moment the result of Lemma (4.7) one has

$$[\mathcal{A}_{K[G]}(\mathcal{O}_L)^H : \mathcal{O}[G]^h]_{\mathcal{O}} = \begin{cases} \wp_K^{(n_1-1)p+1}, & \text{if } \operatorname{ord}(G/H) = p \\ \wp_K^{n_1}, & \text{if } H = G \\ \wp_K^{(n_1-1)p^s}\Lambda(H_0,\kappa), & \text{if } H = H_0, \end{cases} \tag{4.8}$$

with

$$\Lambda(H_0,\kappa) = [\mathcal{A}(F/K,-\kappa,0) : \mathcal{O}[\Gamma]]_{\mathcal{O}}.$$

Now there are $(p^s-1)/(p-1)$ subgroups H such that $H_0 < H < G$ and $\operatorname{ord}(G/H) = p$, and so the relation (4.6) is equivalent to the equality

$$[\mathcal{A}_{K[G]}(\mathcal{O}_L)^{H_0} : \mathcal{O}[G]^{H_0}]_{\mathcal{O}}$$
$$= ([\mathcal{A}_{K[G]}(\mathcal{O}_L)^G : \mathcal{O}[G]^G]_{\mathcal{O}})^{1-\left(\frac{p^s-1}{p-1}\right)} \cdot \prod_{\substack{H_0<H<G \\ \operatorname{ord}(G/H)=p}} [\mathcal{A}_{K[G]}(\mathcal{O}_L)^H : \mathcal{O}[G]^H]_{\mathcal{O}},$$

which upon substituting (4.8) becomes

$$(4.9) \qquad [\mathscr{A}(F/K, -\kappa, 0) : \mathcal{O}[\Gamma]]_{\mathcal{O}} = \wp_K .$$

But on the other hand, from Proposition (2.2) one knows that

$$(4.10) \qquad [\mathscr{A}_{K[\Gamma]}(\mathcal{O}_F) : \mathcal{O}[\Gamma]]_{\mathcal{O}} = \wp_K .$$

Now $\kappa \geqslant 0$ so that $\mathscr{A}(F/K, -\kappa, 0) \subseteqq \mathscr{A}(F/K, 0, 0) = \mathscr{A}_{K[\Gamma]}(\mathcal{O}_F)$, and hence (4.9) and (4.10) together imply $\mathscr{A}(F/K, -\kappa, 0) = \mathscr{A}_{K[\Gamma]}(\mathcal{O}_F)$. But this is clearly absurd if $\kappa > 0$.

It therefore suffices for us to prove Lemma 4.7.

Proof of Lemma 4.7. – We may assume that G is not cyclic so that $s > 1$. From Lemma 1.13 one knows that, for each integer $i \geqslant 1$, the upper ramification subgroup $G^{(i)}$ is equal to $G^{(1)}(i-1)$ and so has structure invariants

$$p^{\delta_{1i}(n_1+1-i)}, p^{\delta_{2i}(n_2+1-i)}, \ldots, p^{\delta_{si}(n_s+1-i)}$$

where, for each integer $i \geqslant 1$ and $j = 1, 2, \ldots s$,

$$\delta_{ji} = \begin{cases} 1, & \text{if } n_j + 1 - i \geqslant 0; \\ 0, & \text{otherwise.} \end{cases}$$

In particular then $G^{(n_1)} > G^{(n_1+1)} = 1$. We define an integer d by

$$p^d = \operatorname{ord}(G^{(n_1)}),$$

so that $1 \leqslant d \leqslant s$ and

$$(4.11) \qquad s = d \Leftrightarrow n_1 = n_s .$$

If $G^{(2)} \leqslant H$ then combining (1.14) and (1.15) (*a*) gives

$$(4.12) \quad v_{LH}(\mathrm{Tr}_H(\mathcal{O}_L)) = \left[\frac{1}{\operatorname{ord}(H)}(2.\operatorname{ord}(H) + (n_1 - 1)\operatorname{ord}(G) - t_{n_1} - 1)\right]$$
$$= 2 + (n_1 - 1).\operatorname{ord}(G/H) + \left[\frac{-t_{n_1} - 1}{\operatorname{ord}(H)}\right].$$

From (1.14) one obtains

$$(4.13) \quad \begin{cases} p^{N-d} < t_{n_1} + 1 = \displaystyle\sum_{i=0}^{i=n_1} \operatorname{ord}(G/G^{(i)}) \\ \qquad = p^{N-d} + \displaystyle\sum_{i=0}^{i=n_1-1} \operatorname{ord}(G/G^{(i)}) < 2p^{N-d} . \end{cases}$$

In particular therefore, if $\operatorname{ord}(G/H) = p$ equation (4.12) gives

$$(4.14) \qquad v_{L^H}(\mathrm{Tr}_H(\mathcal{O}_L)) = 2 + (n_1 - 1)p + \begin{cases} -1, & \text{if} \quad d > 1\,; \\ -2, & \text{if} \quad d = 1\,. \end{cases}$$

Furthermore, in this case one checks that

$$\mathscr{A}(L^H/K,1,0) = \mathscr{A}(L^H/K,0,0) = \mathscr{M}(\mathcal{O},G/H),$$

and this together with (4.14) proves the first assertion of Lemma 4.7. The statement for the case $H = G$ follows by a similar calculation. As for the case $H = G^{(2)}$, the expression (4.12) gives

$$(4.15) \qquad v_F(\mathrm{Tr}_{G^{(2)}}(\mathcal{O}_L)) - (n_1 - 1)p^s = 2 + \left[\frac{-t_{n_1} - 1}{p^{N-s}}\right]$$

$$(4.16) \qquad = \begin{cases} 0, & \text{if} \quad s = d \\ < 0, & \text{if} \quad s > d\,, \end{cases}$$

where here the last equality is a consequence of (4.13). But this proves the final assertion of Lemma 4.7, with the integer $-\kappa$ equal to the right hand side of equality (4.15). (The condition $\kappa = 0 \Leftrightarrow n_1 = n_s$ then follows from combining (4.11) and (4.16)).

4.3. On possible further progress.

It will be clear that our results in the non-cyclic case are restricted precisely because we have no general technique for explicitly describing the orders $\mathscr{A}_{K[G]}(I)$ if G is not cyclic. In fact, even for the case $\mathrm{Syl}_p(G)$ is of type (p,p) we have not been able to overcome this difficulty except in special cases. In this subsection we assume (without further comment) that $\mathrm{Syl}_p(G)$ is of type (p,p) and briefly describe the implications of possible results in this case for the general problem of Open Question (2.3).

If H is any non-trivial subgroup of $\mathrm{Syl}_p(G)$ then G/H is cyclic and we can use the techniques of § 3.1 to explicitly describe the lattice $\mathscr{A}_{K[G]}(I)^H$ for any given $I \in \mathscr{I}_L$. Furthermore, in all examples for which we have managed to completely describe $\mathscr{A}_{K[G]}(I)$ one has

$$(4.17) \qquad \mathscr{A}_{K[G]}(I) = \mathcal{O}[G] + \sum_{1 < H \leqslant G} \mathscr{A}_{K[G]}(I)^H\,.$$

Explicitly we know this in the following cases:

- $r = 1$ and $I = \wp_L^j$ with $j = 0$ and 1 (cf. Proposition (2.2));
- $p = 3$, $r = 1$ and $I = \wp_L^j$ with $j = 0, 1, 2, 5$, and 6;
- $p = 3$, $r = 2$ and $I = \wp_L^j$ with $j = 0$ and $j = 1$.

We believe that (4.17) may well be valid for all $I \in \mathscr{I}_L$ but we cannot prove this. The validity of (4.17) has interesting implications concerning Open Question (2.3). In fact by the same kind of analysis as used in §§ 4.1 and 4.2 one can prove that if an ideal $I \in \mathscr{I}_L$ satisfies (4.17) then $\mathbf{Fr}_K(I)$ if and only if $R = 1$ and either $I = \mathcal{O}_L$ or $I = \wp_L$. In particular therefore if (4.17) is valid for all $I \in \mathscr{I}_L$ then (since any non-cyclic abelian p-group has a quotient of type (p,p)) the conclusion of Theorem 4 is immediately strengthened to give $R = 1$. It also seems likely that any technique which would settle the question of the general validity of (4.17) would provide methods giving a sharpening of the conclusion of Theorem 5. We hope to return to this general question in a subsequent paper.

5. A COMPARISON RESULT

In this section we shall give a proof of Theorem 6, the notation of which we shall continue to use. Throughout we identify G and G', and hence also the inertia subgroups $G_{(0)}$ and $G'_{(0)}$, by means of the given isomorphism Ψ.

Equivalence (1.19) implies that both

$$\mathbf{Fr}_K(\wp_L^i) \Leftrightarrow \mathbf{Fr}_{L_0}(\wp_L^i) \qquad \text{and} \qquad \mathbf{Fr}_{K'}(\wp_{L'}^i) \Leftrightarrow \mathbf{Fr}_{L'_0}(\wp_{L'}^i).$$

Also, under the assumptions of Theorem 6, equation (1.18) gives an equality

$$\text{(5.1)} \qquad \mathcal{O}_\Lambda \otimes_{\mathcal{O}_{L_0}} \mathscr{A}_{L_0[G_{(0)}]}(\wp_L^i) = \mathcal{O}_\Lambda \otimes_{\mathcal{O}_{L'_0}} \mathscr{A}_{L'_0[G_{(0)}]}(\wp_{L'}^i),$$

where here we write Λ for the compositum field $L_0 L'_0$. Therefore we need only deal with the totally ramified extensions L/L_0 and L'/L'_0. For notational convenience we shall henceforth assume that the extensions L/K and L'/K' are totally ramified, i.e. that $G = G_{(0)} = G'_{(0)}$ so that $K = L_0$ and $K' = L'_0$.

Now Corollary (1.10) implies that

(5.2)
$$\mathbf{Fr}_K(\wp_L^i) \Leftrightarrow \wp_L^i \circ_G \mathscr{A}_{K[G]}(\wp_L^i) \quad \text{and} \quad \tilde{f}_{\mathscr{A}_{K[G]}(\wp_L^i), \mathcal{O}_K[G]}(G^\dagger) = \tilde{f}_{\wp_L^i, \mathcal{O}_L}(G^\dagger)$$

and similarly upon replacing L/K by L'/K'. But by direct computation

$$\mathcal{O}_\Lambda \otimes_{\mathcal{O}_K} \tilde{f}_{\wp_L^i, \mathcal{O}_L}(G^\dagger) = \mathcal{O}_\Lambda \otimes_{\mathcal{O}_{K'}} \tilde{f}_{\wp_{L'}^i, \mathcal{O}_{L'}}(G^\dagger),$$

and also from (5.1) one has

$$\mathcal{O}_\Lambda \otimes_{\mathcal{O}_K} \tilde{f}_{\mathscr{A}_{K[G]}(\wp_L^i), \mathcal{O}_K[G]}(G^\dagger) = \mathcal{O}_\Lambda \otimes_{\mathcal{O}_{K'}} \tilde{f}_{\mathscr{A}_{K'[G]}(\wp_{L'}^i), \mathcal{O}_{K'}[G]}(G^\dagger)$$

so that

$$\tilde{f}_{\mathscr{A}_{K[G]}(\wp_L^i), \mathcal{O}_K[G]}(G^\dagger) = \tilde{f}_{\wp_L^i, \mathcal{O}_L}(G^\dagger) \Leftrightarrow \tilde{f}_{\mathscr{A}_{K'[G]}(\wp_{L'}^i), \mathcal{O}_{K'}[G]}(G^\dagger) = \tilde{f}_{\wp_{L'}^i, \mathcal{O}_{L'}}(G^\dagger).$$

In order to prove Theorem 6 we need therefore only demonstrate that

$$\wp_L^i \circ_G \mathscr{A}_{K[G]}(\wp_L^i) \Leftrightarrow \wp_{L'}^i \circ_G \mathscr{A}_{K'[G]}(\wp_{L'}^i).$$

By symmetry we need only prove one direction of this double implication. Henceforth we shall assume that $\wp_L^i \circ_G \mathscr{A}_{K[G]}(\wp_L^i)$ and so aim to prove that $\wp_{L'}^i \circ_G \mathscr{A}_{K'[G]}(\wp_{L'}^i)$. To be specific, if $H < G$ is cocyclic and $\Gamma = G/H$ we now assume the equality

$$\mathscr{A}_{K[\Gamma]}((\wp_L^i)^H) = \mathscr{A}_{K[\Gamma]}(\mathscr{A}_{K[G]}(\wp_L^i)^H) \tag{5.3}$$

and deduce from it the equality

$$\mathscr{A}_{K'[\Gamma]}((\wp_{L'}^i)^H) = \mathscr{A}_{K'[\Gamma]}(\mathscr{A}_{K'[G]}(\wp_{L'}^i)^H). \tag{5.4}$$

Now as a consequence of (5.1) one has

$$\mathcal{O}_\Lambda \otimes_{\mathcal{O}_K} \mathscr{A}_{K[\Gamma]}(\mathscr{A}_{K[G]}(\wp_L^i)^H) = \mathcal{O}_\Lambda \otimes_{\mathcal{O}_{K'}} \mathscr{A}_{K'[\Gamma]}(\mathscr{A}_{K'[G]}(\wp_{L'}^i)^H). \tag{5.5}$$

In order to similarly compare the left hand sides of (5.3) and (5.4) we shall need a lemma concerning cyclic extensions.

Let F/E (respectively F'/E') be a totally ramified cyclic extension of degree $p^m r (p \nmid r)$ with E (respectively E') a finite unramified extension of $\mathbb{Q}_p$. Set $\Delta = \mathrm{Gal}(F/E)$, $\Pi = \mathrm{Syl}_p(\Delta)$ and let Ω denote the subgroup of Δ which has order r. By fixing an isomorphism $\Delta \to \mathrm{Gal}(F'/E')$ we shall henceforth identify these groups. As in § 3.1 therefore, to each character $\theta \in \Omega^{\dagger}$ one can associate integers $u_{F/E,0,\theta}$ and $u_{F'/E',0,\theta}$, each belonging to the set $\{j : 1 \leqslant j \leqslant r\}$. *A priori* it need not be the case that $u_{F/E,0,\theta} = u_{F'/E',0,\theta}$ for all characters $\theta \in \Omega^{\dagger}$. Thus we use a prime $'$ to denote the induced permutation of $\Omega^{\dagger}$ which is given by

$$u_{F'/E',0,\theta'} = u_{F/E,0,\theta} \qquad \text{for all } \theta \in \Omega^{\dagger}.$$

For any $\mathcal{O}_E[\Delta]$-lattice (respectively $\mathcal{O}_{E'}[\Delta]$-lattice) X one has a decomposition

$$X = \bigoplus_{\theta \in \Omega^{\dagger}} e_\theta X = \bigoplus_{\theta \in \Omega^{\dagger}} e_\theta X_\theta ,$$

where here each X_θ is an $\mathcal{O}_E[\Pi]$-(respectively $\mathcal{O}_{E'}[\Pi]$-)lattice spanning $E[\Pi]$ (respectively $E'[\Pi]$).

The key to our proof is the observation that, for any character $\theta \in \Omega^{\dagger}$ and any ideal $I \in \mathscr{I}_F$, the abstract structure of the lattice $\mathscr{A}_{E[\Delta]}(I)_\theta$ depends only upon the valuation $v_F(I)$ and the integer $u_{F/E,0,\theta}$. To be more precise we let $\tilde{E}$ denote the compositum field EE'. Also if X (respectively X') is an $\mathcal{O}_E[\Delta]$-lattice (respectively $\mathcal{O}_{E'}[\Delta]$-lattice) then we shall write $X \asymp X'$ to denote the equality $\mathcal{O}_{\tilde{E}} \otimes_{\mathcal{O}_E} X = \mathcal{O}_{\tilde{E}} \otimes_{\mathcal{O}_{E'}} X'$. In the sequel we shall use without mention the fact that scalar extension is a faithfully flat functor, i.e. that if X spans the $E[\Delta]$-vector space V then (in $\tilde{E} \otimes_E V$) one has $V \cap (\mathcal{O}_{\tilde{E}} \otimes_{\mathcal{O}_E} X) = X$.

LEMMA 5.6. – *For any integer κ and any character $\theta \in \Omega^{\dagger}$ there is an equality*

$$\mathscr{A}_{E[\Delta]}(\wp_F^{\kappa})_\theta \asymp \mathscr{A}_{E'[\Delta]}(\wp_{F'}^{\kappa})_{\theta'} .$$

Before proving Lemma 5.6 we demonstrate that it is sufficient to prove (5.4).

Set $F = L^H$ and $F' = L'^H$, with $E = K$ and $E' = K'$. We identify $\mathrm{Gal}(F/E)$ and $\mathrm{Gal}(F'/E')$ by means of the isomorphism induced by the given isomorphism $\Psi : G \to G'$. Lemma (5.6) implies an equality of sets

$$(5.7) \quad \{\mathcal{O}_\Lambda \otimes_{\mathcal{O}_K} \mathscr{A}_{K[\Gamma]}((\wp_L^i)^H)_\theta : \theta \in C^{\dagger}\} = \{\mathcal{O}_\Lambda \otimes_{\mathcal{O}_{K'}} \mathscr{A}_{K'[\Gamma]}((\wp_{L'}^i)^H)_\theta : \theta \in C^{\dagger}\}.$$

On the other hand, by taking (5.3) together with the equality (5.5) and the middle inclusion of (1.11), one deduces that, for any character $\theta \in C^\dagger$,

$$(5.8)_\theta \qquad \mathcal{O}_\Lambda \otimes_{\mathcal{O}_{K'}} \mathcal{A}_{K'[\Gamma]}((\wp_{L'}^{i})^H)_\theta \subseteqq \mathcal{O}_\Lambda \otimes_K \mathcal{A}_{K[\Gamma]}((\wp_L^i)^H)_\theta .$$

By combining Lemma 5.6 together with the inclusions $(5.8)_{\theta'}$ one deduces that

$$(5.9)_\theta \qquad \mathcal{A}_{K[\Gamma]}((\wp_L^i)^H)_\theta \subseteqq \mathcal{A}_{K[\Gamma]}((\wp_L^i)^H)_{\theta'}$$

for each character $\theta \in C^\dagger$.

Let now T denote the set in (5.7) (say on the left hand side). We partially order T by set theoretic inclusion. As a consequence of the inclusions $(5.9)_\theta$ the permutation $\theta \mapsto \theta'$ induces an increasing permutation of T. But there can be no strictly increasing permutation of a finite partially ordered set and so one must have equality in each $(5.9)_\theta$, and hence in each $(5.8)_\theta$. Thus, one has

$$\mathcal{O}_\Lambda \otimes_{\mathcal{O}_K} \mathcal{A}_{K[\Gamma]}((\wp_L^i)^H) = \mathcal{O}_\Lambda \otimes_{\mathcal{O}_{K'}} \mathcal{A}_{K'[\Gamma]}((\wp_{L'}^i)^H)$$

and by combining this with (5.5) and (5.3) one obtains the required equality (5.4).

It thus suffices to prove Lemma 5.6.

Proof of Lemma 5.6. – Set $I = \wp_F^\kappa$ and $I' = \wp_{F'}^\kappa$. Fix a character $\theta \in \Omega^\dagger$. Let δ_* denote any generator of Π. Using (3.5) and (3.7) it is not difficult to prove that

$$(\delta_* - 1)e_\theta \mathcal{M}(\mathcal{O}_E, \Delta) \cup pe_\theta \mathcal{M}(\mathcal{O}_E, \Delta) \subset e_\theta \mathcal{A}_{E[\Delta]}(I),$$

and similarly that

$$(\delta_* - 1)e_{\theta'} \mathcal{M}(\mathcal{O}_{E'}, \Delta) \cup pe_{\theta'} \mathcal{M}(\mathcal{O}_{E'}, \Delta) \subset e_{\theta'} \mathcal{A}_{E'[\Delta]}(I').$$

Given the explicit descriptions of $e_\theta \mathcal{M}(\mathcal{O}_E, \Delta)$ and $e_{\theta'} \mathcal{M}(\mathcal{O}_{E'}, \Delta)$ afforded by Lemma 3.1 it therefore suffices to prove that

$$\left(\bigoplus_{i=0}^{i=m} \mathcal{O}_E e_\theta e_{\Delta_i} \right) \cap \mathcal{A}_{E[\Delta]}(I) \asymp \left(\bigoplus_{i=0}^{i=m} \mathcal{O}_{E'} e_{\theta'} e_{\Delta_i} \right) \cap \mathcal{A}_{E'[\Delta]}(I').$$

For each non-negative integer i such that $i \leqslant m$ we set $F_i = F^{\Delta_i}$, so that $|F : F_i| = p^i$. We shall also write e_i for the idempotent $e_{\Delta_i} \in K[\Delta_i]$ and v_i for the valuation of the field F_i. As usual we shall identify Ω with its image in each of the quotient groups Δ/Δ_i. For each pair of integers (κ_1, κ_2) we set $\mathscr{A}_i(\kappa_1, \kappa_2) = \mathscr{A}(F_{m-i}/E, \kappa_1, \kappa_2)$. We similarly define lattices $\mathscr{A}'_i(\kappa_1, \kappa_2)$ with respect to the extension F'/E'.

LEMMA 5.10. – *For each integer* κ *and for each character* $\theta \in \Omega^\dagger$, *one has*

$$(5.11) \qquad \left(\bigoplus_{i=0}^{i=m} \mathcal{O}_E e_\theta e_i \right) \cap \mathscr{A}_m(\kappa, \kappa) \asymp \left(\bigoplus_{i=0}^{i=m} \mathcal{O}_{E'} e_{\theta'} e_i \right) \cap \mathscr{A}'_m(\kappa, \kappa)$$

and

$$(5.12) \qquad \left(\bigoplus_{i=0}^{i=m} \mathcal{O}_E e_\theta e_i \right) \cap \mathscr{A}_m(\kappa, \kappa + r) \asymp \left(\bigoplus_{i=0}^{i=m} \mathcal{O}_{E'} e_{\theta'} e_i \right) \cap \mathscr{A}'_m(\kappa, \kappa + r).$$

Remark. – Note that the assertion (5.11) is sufficient to prove Lemma 5.6. However in order to prove this we shall argue by an induction on m, and for this we shall need the assertion (5.12) in order to help with our inductive step.

Proof. – We shall first prove the claim (5.12). To prove this we argue by induction on m. For $m = 0$ the result is obvious. We assume that the result of Lemma 5.10 is valid for the integer $m - 1$. We now fix a character $\theta \in \Omega^\dagger$. For each integer κ we let $\kappa_{F/E,0}$ denote the least integer such that $\kappa_{F/E,0} \geqslant \kappa$ and $\kappa_{F/E,0} \equiv -u_{F/E,0,\theta}$ modulo (r). For brevity we shall often write κ_0 in place of $\kappa_{F/E,0}$ when the extension F/E is clear from context. For each integer $j \geqslant 1$ we then set $\kappa_j = \lceil \kappa_0 p^{-j} \rceil$ and $\kappa_{j,+} = \lceil (\kappa_0 + r) p^{-j} \rceil$. Choosing an element

$$\alpha = \sum_{i=0}^{i=m} a_i e_\theta e_i \in \bigoplus_{i=0}^{i=m} \mathcal{O}_E e_\theta e_i,$$

we first claim that

$$(5.13) \qquad \alpha \in \mathscr{A}_m(\kappa, \kappa + r) \Rightarrow p \mid a_0.$$

To prove this we note that $p\mathscr{M}(\mathcal{O}_E, \Delta) \subset \mathscr{A}_m(\kappa, \kappa + r)$ (c.f. (3.1), (3.5) and (3.7)), and also, as a consequence of Lemma 3.3, that

$$\alpha \in \mathscr{A}_m(\kappa, \kappa + r) \Leftrightarrow \alpha \in \mathscr{A}_m(\kappa_0, \kappa_0 + r).$$

Suppose now that $\alpha \in \mathscr{A}_m(\kappa_0, \kappa_0+r)$ and yet that $p \nmid a_0$. Well $e_0 \notin \mathscr{A}_m(\kappa_0, \kappa_0+r)$ and hence $p^t | \kappa_0$ where t is the least integer such that $1 \leqslant t \leqslant m$ and $p \nmid a_t$. Since $p^t | \kappa_0$ one has $\wp_F^{\kappa_0} = \wp_F^{\kappa_t} + \wp_F^{\kappa_0+1}$ and hence if $\beta \in e_\theta E[\Delta]$ then

$$\beta \in \mathscr{A}_m(\kappa_0, \kappa_0+r) \Leftrightarrow \beta((\wp_{F_t})^{\kappa_t}) \subseteqq (\wp_{F_t})^{\kappa_{t,+}} \quad \text{and} \quad \beta \in \mathscr{A}_m(\kappa_0+r, \kappa_0+r).$$

We set $\Sigma = \Delta/\Delta_t$. Now

$$(5.14) \quad \alpha((\wp_{F_t})^{\kappa_t}) \subseteqq (\wp_{F_t})^{\kappa_{t,+}} \Rightarrow (a_0+a_t)e_\theta + \sum_{j=1}^{j=m-t} a_{t+j}e_\theta e_{\Sigma_j} \in \mathscr{A}_{m-t}(\kappa_t, \kappa_{t,+}).$$

On the other hand

$$(5.15) \quad \alpha \in \mathscr{A}_m(\kappa_0+r, \kappa_0+r) \Rightarrow \alpha - a_0e_\theta \in \mathscr{A}_m(\kappa_0+r, \kappa_0+r) \Rightarrow \alpha_te_\theta + \sum_{j=1}^{j=m-t} a_{t+j}e_\theta e_{\Sigma_j} \in \mathscr{A}_{m-t}(v_t(e_t(\wp_F^{\kappa_0+r})), \kappa_{t,+}).$$

But from (3.5) one has

$$v_t(e_t(\wp_F^{\kappa_0+r})) = \left[\frac{1}{p^t}\left(\kappa_0+r-r\left(\frac{p^t-1}{p-1}\right) + p^t-1\right)\right] = \kappa_t + \left[\frac{1}{p^t}\left(r-r\left(\frac{p^t-1}{p-1}\right) + p^t-1\right)\right] \leqslant \kappa_t$$

so that (5.15) implies

$$(5.16) \qquad a_te_\theta + \sum_{j=1}^{j=m-t} a_{t+j}e_\theta e_{\Sigma_j} \in \mathscr{A}_{m-t}(\kappa_t, \kappa_{t,+}).$$

Combining (5.14) and (5.16) we therefore obtain $a_0e_\theta \in \mathscr{A}_{m-t}(\kappa_t, \kappa_{t,+})$. But

$$\kappa_{t,+} > \kappa_t \equiv -u_{F_t/E,0,\theta} \quad \text{modulo } (r)$$

and so (by Lemma 3.3) this contradicts our initial assumption that $p \nmid a_0$. This proves (5.13).

Set $\tilde{\alpha} = \alpha - a_0e_\theta$ regarded as an element of $E[\Delta/\Delta_1]$. From (5.13) one has

$$\alpha \in \mathscr{A}_m(\kappa, \kappa+r) \Leftrightarrow \alpha - a_0e_\theta \in \mathscr{A}_m(\kappa_0, \kappa_0+r) \Leftrightarrow \tilde{\alpha} \in \mathscr{A}_{m-1}(v_1(e_1(\wp_F^{\kappa_0})), \kappa_{1,+}).$$

Set $\kappa^\dagger = v_1(e_1(\wp_F^{\kappa_0}))_{F_1/E,0}$. Now, using (3.5), one easily checks that

$$v_1(e_1(\wp_F^{\kappa_0})) \leqslant \kappa_{1,+} \leqslant v_1(e_1(\wp_F^{\kappa_0})) + r,$$

and hence (by Lemma 3.3) that

$$(5.17)\quad \alpha \in \mathscr{A}_m(\kappa,\kappa+r) \Leftrightarrow \tilde{\alpha} \in \begin{cases} \mathscr{A}_{m-1}(\kappa^\dagger,\kappa^\dagger), & \text{if } \kappa^\dagger \geqslant \kappa_{1,+}\,; \\ \mathscr{A}_{m-1}(\kappa^\dagger,\kappa^\dagger+r), & \text{otherwise.} \end{cases}$$

But for any character $\theta \in \Omega^\dagger$ the integer $u_{F_1/E,0,\theta}$ is uniquely specified by

$$u_{F_1/E,0,\theta} \equiv p^{-1} u_{F/E,0,\theta} \quad \text{modulo } (r)$$

and hence (given Δ) the choice in (5.17) is determined completely by the values of κ and $u_{F/E,0,\theta}$. By using a similar analysis of $\mathscr{A}'_m(\kappa,\kappa+r)$ the claim (5.12) therefore follows by our inductive hypothesis at $m-1$.

We can now prove the assertion (5.11). Indeed,

$$\alpha \in \mathscr{A}_m(\kappa,\kappa) \Leftrightarrow \alpha - a_0 e_\theta \in \mathscr{A}_m(\kappa_0,\kappa_0) \Leftrightarrow \tilde{\alpha} \in \mathscr{A}_{m-1}(v_1(e_1(\wp_F^{\kappa_0})),\kappa_1).$$

But

$$v_1(e_1(\wp_F^{\kappa_0})) \leqslant \kappa_1 \leqslant v_1(e_1(\wp_F^{\kappa_0})) + r$$

and so the required claim follows by an induction on m just as in the argument used to prove the claim (5.12) (i.e. via choices of the form (5.17)).

This completes the proof of Lemma 5.10 and hence also the proof of Theorem 6. □

BIBLIOGRAPHY

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

[2] A.-M. Bergé, A propos du genre de l'anneau des entiers d'une extension, Publications Math. Sc. Besançon, (1979-1980), 1-9.

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

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

[5] S. U. Chase and F. Destrempes, Factorizability, Grothendieck groups and Galois module structure, preprint, 1989.

[6] J. W. S. CASSELS and A. FRÖHLICH (eds), Algebraic Number Theory, Proc. Brighton Symp., 1965, Academic Press, London, 1967.

[7] Ph. CASSOU-NOGUÈS and M. J. TAYLOR, Elliptic functions and rings of integers, Progress in Mathematics, Volume 66, Birkhäuser Boston-Basel-Stuttgart, 1987.

[8] B. EREZ, A survey of recent work on the square root of the inverse different, Proceedings of the Journées Arithmétique 1989 at Luminy.

[9] M.-J. FERTON, Sur les idéaux d'une extension cyclique de degré premier d'un corps local, C.R. Acad. Sc. Paris, 276 Série A (1973), 1483-1486.

[10] J.-M. FONTAINE, Groupes de ramification et représentations d'Artin, Ann. Scient. Éc. Norm. Sup., 4e série, 4 (1971), 337-392.

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

[12] A. FRÖHLICH, Module defect and factorisability, Illinois J. Math., 32, 3 (1988), 407-421.

[13] A. FRÖHLICH, 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.

[14] F. KAWAMOTO, On normal integral bases of local fields, J. of Algebra, 98 (1986), 197-199.

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

[16] A. NELSON, Monomial representations and Galois module structure, Ph. D. Thesis, King's College, University of London, 1979.

[17] I. REINER, Maximal Orders, Academic Press, London, 1975.

[18] J.-P. SERRE, Corps Locaux, Hermann, Paris, 1962.

[19] D. SOLOMON, Iwasawa theory, factorisability and the Galois module structure of units, to appear.

[20] R. G. SWAN, Induced representations and projective modules, Ann. of Math., 71 (1960), 552-578.

[21] S. ULLOM, Normal bases in Galois extensions of number fields, Nagoya J., 34 (1969), 153-167.

[22] S. ULLOM, Galois cohomology of Ambiguous Ideals, J. Number Theory, 1 (1969), 11-15.

[23] S. M. J. WILSON, Extensions with identical wild ramification, Sém. de Théorie des Nombres, Université de Bordeaux I, (1980-1981).

Manuscrit reçu le 10 avril 1989,
révisé le 4 mai 1990.

David J. BURNS,
Fitzwilliam College
Cambridge, CB3 0DG (England).