

On the equivariant structure of ideals in abelian extensions of local fields (with an appendix by W. Bley)

David Burns

Abstract. Let p be an odd rational prime and K a finite extension of \mathbb{Q}_p . We give a complete classification of those finite abelian extensions L/K in which any ideal of the valuation ring of L is free over its associated order in $\mathbb{Q}_p[Gal(L/K)]$. In an appendix W. Bley describes an algorithm which can be used to determine the structure of Galois stable ideals in abelian extensions of number fields. The algorithm is applied to give several new and interesting examples.

Mathematics Subject Classification (1991). 11R33.

Keywords. Galois module structure, local fields, ideals, associated orders.

1. Introduction

Let L/K be a finite Galois extension of number fields, or of p -adic fields for some rational prime p . For brevity we shall refer to these cases as ‘global’ and ‘local’ respectively. We let G denote the Galois group of L/K , and \mathcal{O}_L the ring of algebraic integers or valuation ring of L in the global and local case respectively. In this paper we are interested in studying, for any subfield E of K , the explicit $\mathcal{O}_E[G]$ -structure of each G -stable \mathcal{O}_L -ideal. This is a long standing and difficult problem.

If L/K is at most tamely ramified, then Ullom has shown that each G -stable ideal of \mathcal{O}_L is locally-free, respectively free, as an $\mathcal{O}_E[G]$ -module in the global, respectively local, case [U1]. In the local case an explicit set of $\mathcal{O}_E[G]$ -generators for each ideal can be described (cf. [K]). In the global case, M. Taylor has characterised the $\mathbb{Z}[G]$ -stable-isomorphism class of \mathcal{O}_L in terms of Artin root numbers attached to the irreducible complex symplectic characters of G ([T2], [Fr3]), and the $\mathcal{O}_K[G]$ -structure of \mathcal{O}_L has been studied by McCulloh [M]. The study of the $\mathbb{Z}[G]$ -structure of other G -stable ideals of \mathcal{O}_L began in a special case in [Er] - where Erez studied the square root $A_{L/K}$ of the inverse different of L/K - and then the general case was investigated in [Bu5]. Taken in conjunction with Taylor’s theorem the techniques of [Bu5] should in fact suffice to explicitly describe

the $\mathbb{Z}[G]$ -stable-isomorphism class of each G -stable ideal of \mathcal{O}_L .

The situation for wildly ramified extensions remains much less clear. In the local case, Ullom has shown that the freeness of any \mathcal{O}_L -ideal I over $\mathcal{O}_E[G]$ is a strong restriction on both the ramification of L/K and the L -valuation of I ([U1], Theorem 2.1). Furthermore, the $\mathcal{O}_E[G]$ -structure of an ideal I depends in general upon more than just the L -valuation of I together with the ramification invariants of L/K and E (cf. for example ([Be2], Chapitre II, IV)), and there are still very few explicit results.

Keeping with the local case, the Krull-Schmidt-Azumaya theorem implies that each ideal of \mathcal{O}_L can be uniquely expressed as a direct sum of indecomposable $\mathcal{O}_E[G]$ -modules. For the case $E = K$ Borevic and Vostokov [Bo,V] and Vostokov [V1], [V2] have characterised $\mathcal{O}_K[G]$ -indecomposability of \mathcal{O}_L -ideals in abelian p -extensions L/K . They prove in particular that if L/K is a non-cyclic abelian p -extension, then all ideals of \mathcal{O}_L are indecomposable as $\mathcal{O}_K[G]$ -modules, and an extension of (a weaker version of) this result to arbitrary non-cyclic abelian groups was recently obtained in [Bl,Bu].

The investigation of \mathcal{O}_L as a sum of explicitly described indecomposable $\mathbb{Z}_p[G]$ -modules was begun in [R-C,V-S,M], and has continued in [E], [E,M1], and [E,M2]. However, even in the case that $\mathbb{Z}_p[G]$ is of finite representation type the full description of \mathcal{O}_L has been only partially achieved, and the general problem still appears to be effectively intractable.

An alternative approach to these problems in both the local and global case is to determine the full endomorphism ring $\mathcal{A}(E[G]; I)$ in $E[G]$ of a G -stable ideal I and then to study the structure of I as an $\mathcal{A}(E[G]; I)$ -module. This approach was originally motivated by work of Leopoldt in [L] and of Fröhlich in [Fr1], and has continued in for example [J], [F], [Be1], [Be2], [T3], [Bu2], [By], [Ch,L] etc..... The extensive theory and results of the global tame theory suggest that, aside from the case $E = K$, the case $E = \mathbb{Q}$, respectively $E = \mathbb{Q}_p$, may be of particular interest in this respect. Furthermore, whilst one knows that \mathcal{O}_L is not in general a free $\mathcal{A}(E[G]; \mathcal{O}_L)$ -module, and that the explicit description of $\mathcal{A}(E[G]; I)$ appears in general to be an intractable problem (cf. [Bl,Bu] for example), certain recent results (cf. [Er], [Er,T], ([Bu2], Proposition 2.2)) suggest that under suitable conditions there may be an interesting structure theory for G -stable ideals other than \mathcal{O}_L .

In this direction we shall give in this paper a complete classification for each odd prime p of those abelian extensions L/K of p -adic fields in which there exists any ideal I of \mathcal{O}_L which is free over $\mathcal{A}(\mathbb{Q}_p[G]; I)$. The main result given here (Theorem 1.3) is, to our knowledge, the first example of a general classification theorem concerning the structure of ideals (over associated orders) in wildly ramified local extensions. The result of Theorem 1.3 is in effect a natural generalisation of the main local results of [U1] and [U2]. Furthermore, the proof we shall give involves extending the main results of [Be1], [Bu2], and [Bl,Bu]. In conjunction with some explicit examples (due to Werner Bley) we are also able to resolve all of the ‘Open

Questions' raised in ([Bu2], §2 and §4.3).

Together with standard localisation procedures, the result of Theorem 1.3 gives a complete classification of those abelian extensions L/K of number fields in which 2 is tamely ramified and some G -stable ideal I of \mathcal{O}_L is locally-free over $\mathcal{A}(\mathbb{Q}[G]; I)$. This result shows how the local aspect of Leopoldt's 'Hauptsatz' [L] fits into a general context. In Leopoldt's examples one has $K = \mathbb{Q}$, and \mathcal{O}_L is always free over $\mathcal{A}(\mathbb{Q}[G]; \mathcal{O}_L)$. In general however, even if $K = \mathbb{Q}$ and G is abelian the local-freeness of an ideal I over $\mathcal{A}(\mathbb{Q}[G]; I)$ does not imply that it is free (cf. [Bu3]) and there is a genuine global problem to consider. The study of extensions in which $\mathcal{A}(\mathbb{Q}[G]; \mathcal{O}_L)$ is equal to the maximal \mathbb{Z} -order in $\mathbb{Q}[G]$ began in [Fr1] and a more or less satisfactory structure theory for \mathcal{O}_L in this case was recently described in [T4]. However, there is at present no similar theory for ideals other than \mathcal{O}_L . The study of $A_{L/K}$ in weakly ramified extensions was begun by Erez in [Er] and then subsequently refined by Erez and Taylor in [Er,T]. Erez and Taylor showed *inter alia* that if L/K is at most tamely ramified, then $A_{L/K}$ is a free $\mathbb{Z}[G]$ -module, but it is still open as to whether $A_{L/K}$ is free in arbitrary weakly ramified extensions. In this direction, we present an appendix prepared by Werner Bley in which is described an algorithm for determining the Galois structure of ideals in abelian extensions of number fields. As particular applications Bley exhibits certain wildly ramified extensions in which there are G -stable ideals I (including in some cases $I = A_{L/K}$) which are free over $\mathcal{A}(E[G]; I)$ for some subfield E of K (cf. Appendix, Example 2). His examples are the first of this type and in particular suggest the possibility that there are finer structure results than those proved in [Er] and [Er,T].

§ 0. Basic notation and preliminaries

Throughout this paper, all fields considered are finite extensions of either \mathbb{Q} or \mathbb{Q}_p for some (odd) rational prime p . We fix algebraic closures \mathbb{Q}^c and \mathbb{Q}_p^c of \mathbb{Q} and \mathbb{Q}_p respectively. If K is a finite extension of \mathbb{Q}_p , then we let e_K denote its absolute ramification degree, $v_K(-)$ its standard valuation, \mathcal{O}_K its valuation ring, and \wp_K and \mathcal{O}_K^* the maximal ideal and unit group of \mathcal{O}_K respectively. If K is a number field, then \mathcal{O}_K is its ring of algebraic integers. In both cases we let \mathcal{I}_K denote the group of fractional \mathcal{O}_K -ideals.

For any finite abelian group Γ , and any commutative ring R , we write $R[\Gamma]$ for the group ring of Γ with coefficients in R . For any finite extension E of \mathbb{Q}_p or \mathbb{Q} and any $\mathcal{O}_E[\Gamma]$ -lattices X and Y which span the same $E[\Gamma]$ -space we write $[X : Y]_{\mathcal{O}_E}$ for the \mathcal{O}_E -module index (an element of \mathcal{I}_E), and we let $\mathcal{A}(E[\Gamma]; X, Y)$ denote the set $\{\lambda \in E[\Gamma] : \lambda X \subseteq Y\}$. For each such lattice X we write $\mathcal{A}(E[\Gamma]; X)$ in place of $\mathcal{A}(E[\Gamma]; X, X)$. This is the 'associated order' of X in $E[\Gamma]$, and is an \mathcal{O}_E -order in $E[\Gamma]$ which contains $\mathcal{O}_E[\Gamma]$. If $X' \subseteq X$ and $Y \subseteq Y'$, then of course

$$\mathcal{A}(E[\Gamma]; X, Y) \subseteq \mathcal{A}(E[\Gamma]; X', Y'). \quad (0.1)$$

We write $\mathcal{M}(E, \Gamma)$ for the unique maximal \mathcal{O}_E -order in $E[\Gamma]$. For each strictly positive integer n we let C_n denote the cyclic group of order n .

The cardinality of a finite set F is written $\#F$. For each subgroup Δ of Γ we set $t_\Delta := \sum_{\delta \in \Delta} \delta$ and let e_Δ denote the idempotent $\#\Delta^{-1}t_\Delta$ of $E[\Gamma]$. For each $\mathcal{O}_E[\Gamma]$ -lattice X we write X^Δ for the $\mathcal{O}_E[\Gamma]$ -sublattice $\{x \in X : \delta x = x, \text{ all } \delta \in \Delta\}$ of Δ -fixed points. There is a natural identification $e_\Delta E[\Gamma] = E[\Gamma/\Delta]$ which restricts to give identifications $e_\Delta \mathcal{M}(E, \Gamma) = \mathcal{M}(E, \Gamma/\Delta)$ and $e_\Delta \mathcal{O}_E[\Gamma] = \mathcal{O}_E[\Gamma/\Delta]$, and with respect to this identification we regard each X^Δ as an $\mathcal{O}_E[\Gamma/\Delta]$ -lattice.

The group of irreducible \mathbb{Q}_p^c -characters of Γ is written Γ^* , and for any character $\theta \in \Gamma^*$ we let e_θ denote the idempotent $\#\Gamma^{-1} \sum_{\gamma \in \Gamma} \theta(\gamma)\gamma^{-1}$ of $\mathbb{Q}_p^c[\Gamma]$.

If L/K is an abelian extension of p -adic fields of group G , then for any subfield E of K and any integers i and j we shall write $\mathcal{A}(E[G]; i, j)$, or exceptionally $(i, j)_E$, in place of $\mathcal{A}(E[G]; \wp_L^i, \wp_L^j)$. If i, j, i' , and j' are any integers such that both $i \leq i'$ and $j \geq j'$, then as a special case of (0.1) one has

$$\mathcal{A}(E[G]; i, j) \subseteq \mathcal{A}(E[G]; i', j'). \quad (0.2)$$

We now quickly recall some of the elementary ramification theory of L/K (details of which can be found in ([S], IV)). If $\lambda \in E[G]$ and Y is any subset of L such that $\lambda Y \neq 0$, then we let $v_L(\lambda Y)$ denote the (finite) minimum of the set $\{v_L(\lambda y) : y \in Y\}$. We let $G^{(i)}$ and $G_{(i)}$ denote the i th upper and lower ramification subgroups of G , and we write $u^{(i)}$ and $u_{(i)}$ for the i th jump numbers of the upper and lower ramification filtrations of L/K . (It is a simple computational matter to convert between these different filtration numberings.) For each $g \in G$, each $x \in L$, and each strictly positive integer i , one has

$$g \in G_{(i)} \setminus G_{(i+1)} \implies v_L((g-1)x) = \begin{cases} v_L(x) + i, & \text{if } p \nmid v_L(x) \\ > v_L(x) + i, & \text{if } p \mid v_L(x). \end{cases} \quad (0.3)$$

For any non-negative integers m and n , any elements $\lambda \in E[G]$ and $\mu \in \mathcal{O}_E[G]$, any elements $\{g_1, g_2\} \subset G_{(i)} \setminus G_{(i+1)}$ for some strictly positive integer i , and any subset $Y \subseteq L$ such that both $(g_1-1)^m \lambda Y \neq 0$ and $(g_2-1)^n \mu \lambda Y \neq 0$, the property (0.3) implies that

$$m < n \implies v_L((g_1-1)^m \lambda Y) < v_L((g_2-1)^n \mu \lambda Y). \quad (0.4)$$

For each integer j , and each subgroup H of G , one has an equality

$$v_{L^H} \left(t_H \wp_L^j \right) = \left[\frac{j + \sum_{i \geq 0} \left(\#(G_{(i)} \cap H) - 1 \right)}{\#(G_{(0)} \cap H)} \right]. \quad (0.5)$$

We now let C denote the maximal subgroup of $G_{(0)}$ of order prime to p . Then C is cyclic, and C^* has a canonical generator $\chi(L/K)$ with the following property: for each $x \in L$, and each $\chi \in C^*$ for which $e_\chi x \neq 0$, one has

$$v_L(e_\chi x) \geq v_L(x) \quad \text{with equality if and only if } \chi = \chi(L/K)^{v_L(x)} \quad (0.6)$$

(cf. ([Be1], §2)).

§ 1. Statement of the main results

Let p be an odd rational prime. Unless stated to the contrary, in this section L/K denotes a totally ramified abelian extension of p -adic fields. The extension L/K has group G and degree $p^n r$ with $n \geq 1$ and $p \nmid r$. We let P and C denote the subgroups of G of order p^n and r respectively, so that in particular one has $P = G^{(1)} = G_{(1)}$.

We recall that L/K is said to be ‘weakly ramified’ if $G_{(2)} = 1$ (cf. [Er]). If this is the case, then since L/K is totally ramified, it follows that G is an elementary abelian p -group.

Lemma 1.1. *Let E be any subfield of K .*

(i) (Ullom, cf. ([U1], Theorem 2.1), ([U2], Theorem 2), and ([U3], Theorem 2)).

For any ideal \mathfrak{o}_L^i the following conditions are equivalent:-

(a) \mathfrak{o}_L^i is free over $\mathcal{O}_E[G]$.

(b) $\hat{H}^0(G, \mathfrak{o}_L^i) = 0$.

(c) L/K is weakly ramified and $i \equiv 1$ modulo $\#G$.

(ii) ([Bu2], Proposition 2.2). If $e_K = 1$ and G is an elementary abelian p -group, then (L/K is weakly ramified and) \mathcal{O}_L is free over $\mathcal{O}_E[G]\{1, p^{-1}t_G\}$. \square

The extension L/K is said to be ‘almost maximally ramified’ if its first (upper) jump number $u^{(1)}$ satisfies $u^{(1)} = (pe_K - \delta)/(p-1)$ for a positive integer δ satisfying $\delta r < p$ (cf. [J], [Fr1]). By an easy exercise in computing valuations one can prove the following result (cf. Lemma 3.2).

Lemma 1.2. *Let E be any absolutely unramified subfield of K . Then $\mathcal{A}(E[G]; \mathcal{O}_L) = \mathcal{M}(E, G)$ if and only if L/K is cyclic and almost maximally ramified.* \square

For any ideal I of \mathcal{O}_L we shall write $\text{Fr}(E[G]; I)$ if I is free over its associated order $\mathcal{A}(E[G]; I)$ in $E[G]$. We shall write $\text{Fr}(E[G]; \mathcal{I}_L)$ to mean that there exists an ideal I of \mathcal{O}_L for which $\text{Fr}(E[G]; I)$. In a similar way, we shall write $\text{NFr}(E[G]; I)$, respectively $\text{NFr}(E[G]; \mathcal{I}_L)$, to indicate that $\text{Fr}(E[G]; I)$ is not true, respectively that $\text{NFr}(E[G]; I)$ for all ideals I of \mathcal{O}_L .

We can now state our main result.

Theorem 1.3.

(i) If $G^{(1)}$ is not cyclic, then $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{I}_L)$ if and only if L/K is weakly ramified.

(ii) Let $G^{(1)}$ be cyclic of order at least p^2 .

(a) If $e_K > 1$, then $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{I}_L)$ if and only if L/K is almost maximally ramified.

(b) If $e_K = 1$ and $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{I}_L)$, then $r < 2p$.

(iii) Let $G^{(1)}$ have order p .

(a) If $e_K > 1$, then $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{I}_L)$ if and only if L/K is either weakly or almost maximally ramified.

(b) If $e_K = 1$, then $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{I}_L)$ if and only if $r < 2p$.

Corollary 1.4. $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$ if and only if either L/K is cyclic and almost maximally ramified or L/K is non-cyclic and both $e_K = 1$ and L/K is weakly ramified.

Proof. If G is non-cyclic and $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$, then Theorem 1.3(i) implies that L/K is weakly ramified. If L/K is weakly ramified and $e_K > 1$, then it will follow from Proposition 1.8 below that $\text{NFr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$. Finally, if L/K is weakly ramified and $e_K = 1$, then $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$ as a consequence of Lemma 1.1(ii).

If L/K is cyclic and almost maximally ramified, then it follows immediately from Lemma 1.2 that $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$. Conversely, Bergé has shown that if $e_K = 1$ and L/K is cyclic, then $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$ implies that L/K is almost maximally ramified (cf. Lemma 3.11). The fact that the same is true if $e_K > 1$ and L/K is cyclic will follow from Theorem 1.3(iii)(a) and Proposition 1.8 below. \square

Remarks 1.5. (i) Theorem 1.3 does not extend to include the case $p = 2$. For example, even with $K = \mathbb{Q}_2$, it is possible that L/K is neither cyclic or weakly ramified and yet $\text{Fr}(\mathbb{Q}_2[G]; \mathcal{I}_L)$ (cf. ([Bl,Bu], Beispiel 3.2)).

(ii) We shall see that if $e_K > 1$, then all (relevant) assertions of Theorem 1.3 remain valid if \mathbb{Q}_p is replaced by any absolutely unramified subfield of K . However, this is not true if $e_K = 1$. Indeed, Example 1.6 below shows that if $e_K = 1$, then $\text{Fr}(K[G]; \mathcal{I}_L)$ is possible even if L/K is neither cyclic or weakly ramified. For any given ideal I of \mathcal{O}_L , and any absolutely unramified subfield E of K , the problems of deciding whether either $\text{Fr}(\mathbb{Q}_p[G]; I)$ or $\text{Fr}(E[G]; I)$ are related by Lemma 1.7 below.

(iii) In the case $e_K = 1$ and G abelian but not cyclic it was first conjectured in [Bu1], respectively [Bu2], that L/K must be weakly ramified if $\text{Fr}(K[G]; \mathcal{O}_L)$, respectively if $\text{Fr}(K[G]; \mathcal{I}_L)$. However, Example 1.6 below shows that this stronger form of Theorem 1.3(i) raised in ([Bu2], Open Question 2.3) is not true. Taken in conjunction with the result of ([Bu2], Theorem 5) it also shows that the answer to ([Bu2], Open Question 2.1) is in general negative. At the moment I know of no counter-example to the conjecture made in [Bu1]. Nevertheless, Theorem 1.3 and Corollary 1.4 are perhaps best regarded as verifications of a generalisation of the ‘corrected version’ of the conjectures made in [Bu2] and [Bu1] respectively.

Example 1.6. (W. Bley, cf. (Appendix, Example 1)). Let $D = \mathbb{Q}(\sqrt{-1})$, and let F be the subfield of the ray class field $D(27)$ of conductor 27 over D which is fixed by the unique subgroup of $\text{Gal}(D(27)/D)$ of order 2 and also by the Frobenius automorphism of 10. Then F/D is an extension with group isomorphic to $C_9 \times C_3$ and is totally ramified at 3. If L and K denote the completions of F and D at the unique prime ideal above 3, then $\text{Fr}(K[\text{Gal}(L/K)]; \wp_L^\delta)$ for each $\delta \in \{8, 9, 10\}$.

The most useful approach to the problem of determining whether modules are locally-free over associated orders is still Fröhlich’s old observation ([Fr2], Theorem 4) that such questions can be determined by means of an index-theoretic criterion. In the next result we use Fröhlich’s criterion to compare the conditions $\text{Fr}(\mathbb{Q}_p[G]; I)$ and $\text{Fr}(E[G]; I)$ for any absolutely unramified subfield E of K .

Lemma 1.7. *Let E be any absolutely unramified subfield of K . Then for any ideal I of \mathcal{O}_L one has $\text{Fr}(\mathbb{Q}_p[G]; I)$ if and only if both $\text{Fr}(E[G]; I)$ and $\mathcal{A}(E[G]; I) = \mathcal{A}(\mathbb{Q}_p[G]; I)\mathcal{O}_E$.*

Proof. We fix an ideal I and write $\mathcal{A}, \mathcal{A}', \mathcal{A}_E, \mathcal{M}$ and \mathcal{M}_E for $\mathcal{A}(\mathbb{Q}_p[G]; I)$, $\mathcal{A}(\mathbb{Q}_p[G]; I)\mathcal{O}_E$, $\mathcal{A}(E[G]; I)$, $\mathcal{M}(\mathbb{Q}_p, G)$ and $\mathcal{M}(E, G)$ respectively. Since $\mathcal{A}' \subseteq \mathcal{A}_E$ and $\mathcal{M}_E = \mathcal{M}\mathcal{O}_E$ the result of ([Fr2], Theorem 4) implies that

$$\text{Fr}(\mathbb{Q}_p[G]; I) \Leftrightarrow [\mathcal{M} : \mathcal{A}]_{\mathbb{Z}_p}^{[K:\mathbb{Q}_p]} = [\mathcal{M}I : I]_{\mathbb{Z}_p}$$

(and after tensoring with \mathcal{O}_E (over \mathbb{Z}_p) this is equivalent to)

$$\begin{aligned} &\Leftrightarrow [\mathcal{M}_E : \mathcal{A}']_{\mathcal{O}_E}^{[K:\mathbb{Q}_p]} = [\mathcal{M}I : I]_{\mathcal{O}_E}^{[E:\mathbb{Q}_p]} \\ &\Leftrightarrow [\mathcal{M}_E : \mathcal{A}']_{\mathcal{O}_E}^{[K:E]} = [\mathcal{M}I : I]_{\mathcal{O}_E} \\ &\Leftrightarrow \text{Fr}(E[G]; I) \text{ and } \mathcal{A}_E = \mathcal{A}' \end{aligned}$$

(where here the last equivalence is again a consequence of ([Fr2], Theorem 4)). \square

As is already clear from Theorem 1.3, the cases of G cyclic and non-cyclic behave quite differently. In §3 we shall see that if G is cyclic, then there are often many ideals I for which $\text{Fr}(\mathbb{Q}_p[G]; I)$. This is in fact especially so if $e_K = 1$ and so in this case we shall give an explicit description of each order $\mathcal{A}(K[G]; I)$ (cf. Lemma 3.7). In conjunction with the techniques of [Bu2] these descriptions are sufficient to determine whether I is free over $\mathcal{A}(E[G]; I)$ (for any subfield E of K), and so in particular resolve the issue left open by Theorem 1.3(ii)(b).

The following results show that, in contrast to the general cyclic case, if L/K is weakly ramified, then there are few ideals I for which $\text{Fr}(\mathbb{Q}_p[G]; I)$.

Proposition 1.8. *Assume $G_{(2)} = 1$, and let E be any absolutely unramified subfield of K .*

- (i) *If $e_K > 1$, then $\text{Fr}(E[G]; \wp_L^i)$ if and only if $i \equiv 1$ modulo $\#G$ (in which case $\mathcal{A}(E[G]; \wp_L^i) = \mathcal{O}_E[G]$).*
- (ii) *If $e_K = 1$, then $\text{Fr}(E[G]; \wp_L^i)$ if either $i \equiv 1$ modulo $\#G$ (in which case $\mathcal{A}(E[G]; \wp_L^i) = \mathcal{O}_E[G]$) or $i \equiv 0$ modulo $\#G$ (in which case $\mathcal{A}(E[G]; \wp_L^i) = \mathcal{O}_E[G]\{1, p^{-1}t_G\}$).*

Remark 1.9. In the case $G_{(2)} = 1$ the explicit $\mathbb{Z}_p[G]$ -structure of \mathcal{O}_L has been determined by Elder and Madan, and is in general rather complicated (cf. [EM1]).

There are however serious technical difficulties involved in trying to extend their methods to deal with arbitrary ideals of \mathcal{O}_L (cf. [EM2], Lemma 2).

In the special case that $\#G = p^2$ and $G_{(2)} = 1$ we shall obtain a result finer than that of Proposition 1.8, and to state this we need a preparatory lemma.

We let Σ denote the set of integers i with $1 \leq i \leq p+1$. If P is any group isomorphic to $C_p \times C_p$ we label its proper subgroups as P_i for $i \in \Sigma$, and for each such subgroup we choose an element $g_i \in P \setminus P_i$ and set $f_i := g_i - 1 \in \mathbb{Z}[P]$ (the precise choice of the elements g_i does not matter in what follows). For each $i \in \Sigma$ we write e_i for the idempotent e_{P_i} , and we let k_E denote the residue field \mathcal{O}_E/\wp_E . We use the following lemma.

Lemma 1.10. *Let E be any absolutely unramified extension of \mathbb{Q}_p . Let P be any group isomorphic to $C_p \times C_p$. For each integer r with $1 \leq r \leq p$ we define an \mathcal{O}_E -lattice*

$$\Lambda_r(E, P) := \begin{cases} \sum_{i=1}^{i=p+1-r} \mathcal{O}_E f_i^{r-1} e_i, & \text{if } 1 \leq r < p, \\ \mathcal{O}_E p e_P, & \text{if } r = p, \end{cases}$$

and then set

$$\mathcal{A}_r(E, P) := \mathcal{O}_E[P] + \sum_{i=r}^{i=p} \Lambda_i(E, P).$$

Then each $\mathcal{A}_r(E, P)$ is an $\mathcal{O}_E[P]$ -sublattice of $\mathcal{M}(E, P)$. Furthermore, if one sets $\mathcal{A}_r(E, P)' := \mathcal{A}_r(E, P)/\mathcal{A}_p(E, P)$, then there is a natural filtration of $k_E[P]$ -spaces

$$\mathcal{A}_1(E, P)' \supset \mathcal{A}_2(E, P)' \supset \dots \supset \mathcal{A}_p(E, P)' = \{0\},$$

and an isomorphism of k_E -spaces

$$\mathcal{A}_1(E, P)' \xrightarrow{\sim} \bigoplus_{r=1}^{r=p-1} \frac{\mathcal{A}_r(E, P)}{\mathcal{A}_{r+1}(E, P)}. \quad (1.1)$$

Proof. We leave this as an exercise for the reader using the following facts:-

$$(1.2) \quad \mathcal{M}(E, P) = \mathcal{O}_E[P] + \mathcal{O}_E e_P + \sum_{i=1}^{i=p+1} \sum_{j=0}^{j=p-2} \mathcal{O}_E f_i^j e_i.$$

$$(1.3) \quad [\mathcal{M}(E, P) : \mathcal{A}_p(E, P)]_{\mathcal{O}_E} = \wp_E^{\frac{1}{2}p(p+1)}.$$

(1.4) For each integer $s \in \Sigma$, each strictly positive integer k , and each choice of elements $\{h_i : 1 \leq i < k\}$ of $P \setminus P_s$ there exists a unit $u \in \mathbb{Z}_p^*$ such that

$$\prod_{i=1}^{i=k-1} (h_i - 1) e_s \text{ is congruent to } u f_s^{k-1} e_s \text{ modulo } f_s^k e_s \mathcal{O}_E[P].$$

(1.5) Taken in conjunction with (1.4) the equality $\sum_{i \in \Sigma} e_i = 1 + p e_P$ can be used to show that for each integer $s \in \Sigma$, and each non-negative integer k with $k \leq p-1$, one has $f_s^k e_s \in \mathcal{A}_{k+1}(E, P)$. \square

The following result is at the heart of our proof of Theorem 1.3(i).

Proposition 1.11. *Let G be isomorphic to either C_p or $C_p \times C_p$, and suppose that $G_{(2)} = 1$. Let E be any absolutely unramified subfield of K .*

(i) *If $e_K > 1$, then for any integer i one has $\mathcal{A}(E[G]; \wp_L^i) = \mathcal{O}_E[G]$. However, one has $\mathcal{A}(K[G]; \wp_L^i) = \mathcal{O}_K[G]$ if and only if $i \equiv 1$ modulo $\#G$.*

(ii) *If $e_K = 1$, then $\mathcal{A}(E[G]; \wp_L^i) = \mathcal{O}_E[G]$ if and only if $i \equiv 1$ modulo $\#G$. Furthermore, if $\#G = p$, then $\text{Fr}(K[G]; \wp_L^i)$ for all integers i , whereas if $\#G = p^2$, then $\text{Fr}(K[G]; \wp_L^i)$ if and only if either $i \equiv 0$ or 1 modulo p^2 , or for some integer κ with $1 \leq \kappa \leq p - 2$ one has both $i \equiv -\kappa$ modulo p^2 and*

$$\mathcal{A}(K[G]; \wp_L^{-\kappa}) \cap (\mathcal{A}_{p-\kappa}(K, G) \setminus \mathcal{A}_{p-\kappa+1}(K, G)) \neq \emptyset.$$

Remarks 1.12. (i) In the case that $e_K > 1$, $G_{(2)} = 1$ and G is isomorphic to either C_p or $C_p \times C_p$, the question of whether $\text{Fr}(E[G]; I)$ is completely answered by Proposition 1.11(i) in conjunction with Lemma 1.1. Note also that since $\mathcal{O}_E[G]$ is Gorenstein these results imply that in this case each ideal of \mathcal{O}_L is decomposable as an $\mathcal{O}_E[G]$ -module (cf. ([Cu,R], (37.13))).

(ii) In the case $e_K = 1$ Lemma 1.7 shows how Proposition 1.11(ii) gives information concerning structure of ideals over all subfields E of K . Taken together with Theorem 1.3(i) the Example 1.6 shows that in this case the condition $\text{Fr}(E[G]; I)$ certainly depends on the field E .

As recalled earlier, Fröhlich has shown that the problem of determining whether modules are locally-free over associated orders can be decided by means of a purely index-theoretic computation. Given the results stated above it is however clear that the main module theoretic problem in local arithmetic is to determine the genus of modules which are not locally-free, and so it would be interesting to know if this more general problem can also be decided by ‘index-theoretic data’ alone. In this direction, it is interesting to note that if G is cyclic, then Jakovlev has shown that the isomorphism class of a finitely generated $\mathbb{Z}_p[G]$ -lattice is uniquely determined by its Tate cohomology groups ([Ja]).

We now turn to consider the global case, and so let L/K denote an abelian extension of number fields. In conjunction with some standard functorial properties of associated orders (cf. [J], [Be2]), Theorem 1.3 gives a complete classification of those extensions L/K in which all primes over 2 are at most tamely ramified and there exists any G -stable ideal I of \mathcal{O}_L which is locally-free over $\mathcal{A}(\mathbb{Q}[G]; I)$. For the special case $I = \mathcal{O}_L$ one knows that if L/K is at most tamely ramified, or if $K = \mathbb{Q}$, then \mathcal{O}_L is free as an $\mathcal{A}(\mathbb{Q}[G]; \mathcal{O}_L)$ -module (cf. [T1], [L]). In general however, and even if both $K = \mathbb{Q}$ and G is cyclic, local-freeness of an ideal I over $\mathcal{A}(\mathbb{Q}[G]; I)$ does not imply its global freeness (cf. [Bu3], Corollary 2), and so there is a genuine global problem to consider. Theorem 1.3 implies that if any ideal

I is locally-free over $\mathcal{A}(\mathbb{Q}[G]; I)$, then (at least in most cases) the inertial subgroup of a wildly ramified prime p is either cyclic and $\mathcal{A}(\mathbb{Q}[G]; I) \otimes \mathbb{Z}_p$ is induced from a maximal order, or the inertial subgroup is an elementary abelian group and $\mathcal{A}(\mathbb{Q}[G]; I) \otimes \mathbb{Z}_p = \mathbb{Z}_p[G]$. There are therefore essentially two ‘extreme’ cases which are of interest in this context: all primes which wildly ramify in L/K are almost maximally ramified and for some ideal I the order $\mathcal{A}(\mathbb{Q}[G]; I)$ is maximal, or L/K is weakly ramified and $\mathcal{A}(\mathbb{Q}[G]; I) = \mathbb{Z}[G]$.

§ 2. The non-cyclic case

Throughout this section p is an odd rational prime, L/K is a totally ramified abelian extension of p -adic fields of degree $p^n r$ with $n \geq 1$ and $p \nmid r$, G is the Galois group of L/K , P and C its subgroups of orders p^n and r respectively, and E is any absolutely unramified subfield of K .

In this section we shall prove Theorem 1.3(i) and Propositions 1.8 and 1.11. A brief outline of the section is as follows. As a first key step we refine the main result of [Bl,Bu]. This refinement is used to describe orders of the form $\mathcal{A}(E[P]; e_\chi I)$ in the case that P is isomorphic to $C_p \times C_p$, and in conjunction with factorisability techniques these descriptions are then used to prove Proposition 1.11. We next consider Proposition 1.8. Whilst Proposition 1.8(ii) follows easily from known results, we prove Proposition 1.8(i) by a fairly straightforward induction on $\#G$, with the inductive base being provided by Proposition 1.11. As a first step towards proving Theorem 1.3(i) we then show that if P is not cyclic and $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{I}_L)$, then $G = P$. Easy functoriality considerations then imply we need only show that $\text{NFr}(\mathbb{Q}_p[G]; \mathcal{I}_L)$ whenever G is isomorphic to $C_{p^2} \times C_p$. If $e_K > 1$ this follows as a consequence of Lemma 1.1, Proposition 1.11(i) and the main result of [Bl,Bu]. In the case $e_K = 1$ however the argument is more involved. A comparison of Tate cohomology groups with respect to the subgroup $G^{(2)}$ is used in conjunction with Proposition 1.11(ii) to reduce the proof to detailed consideration of lattices of the form $\mathcal{A}(E[G/G^{(2)}]; i, j)$ for various integers i and j . The proof is then completed via a careful analysis of such lattices using Lemma 1.1 and computations derived from (0.2-5).

We let Σ^* denote the set of integers $\{0, 1, 2, \dots, p+1\}$ ($= \{0\} \cup \Sigma$). If P is isomorphic to $C_p \times C_p$, then we shall label its subgroups of order p as P_i for $i \in \Sigma$, and for each $i \in \Sigma$ we then set $e_i := e_{P_i}$. In addition, we shall set $e_0 := 2e_P$.

All of our results in this section are based upon the following strengthening of the main result of [Bl,Bu].

Proposition 2.1. *Let P be isomorphic to $C_p \times C_p$. Choose a character $\chi \in C^*$ and let \mathcal{A} be any order of the form $\mathcal{A}(E[P]; e_\chi \mathcal{O}_L^j)$. Let α be any element of $\mathcal{M}(E, P)$ of the form $\alpha = \sum_{i \in \Sigma^*} \lambda_i(\alpha)(e_i - e_P)$ with $\lambda_i(\alpha) \in \mathcal{O}_E$ for each $i \in \Sigma^*$. (i) If $pe_P \in \mathcal{A}$, then $\alpha \in \mathcal{A}$ if and only if there exists an element $\mu \in \mathcal{O}_E$ such that*

$\lambda_i(\alpha) - \mu \in \wp_E$ for all $i \in \Sigma^*$.

(ii) If $pe_P \notin \mathcal{A}$, then $\alpha \in \mathcal{A}$ if and only if there exists an element $\mu \in \mathcal{O}_E$ such that both $\lambda_i(\alpha) - \mu \in \wp_E$ for all $i \in \Sigma^*$ and $\lambda_0(\alpha) - \mu - \sum_{i \in \Sigma} (\lambda_i(\alpha) - \mu) \in \wp_E^2$. In particular therefore, one has $\alpha \in \mathcal{A}$ if and only if $\alpha \in \mathcal{O}_E[P]$.

Proof. From ([Bl,Bu], Satz 3.1) we know that $e_P \notin \mathcal{A}$. However, it may or may not be the case that pe_P belongs to \mathcal{A} and we shall refer to these different possibilities as cases (i) and (ii) respectively.

It is easy to see that if α satisfies the conditions in the conclusion of Proposition 2.1 with respect to some element $\mu \in \mathcal{O}_E$, then it also satisfies the same conditions with respect to any element $\mu' \in \mathcal{O}_E$ such that $\mu - \mu' \in \wp_E$. Setting $m(\alpha) := \#\{i \in \Sigma : \lambda_i(\alpha) \in \wp_E\}$ it follows that if $m(\alpha) > 0$, then we are required to prove that α satisfies the conditions in the conclusion of Proposition 2.1 with respect to the element $\mu = 0$.

We shall prove Proposition 2.1 by inducting on the cardinality $n(\alpha)$ of the set $\{i \in \Sigma : \lambda_i(\alpha) \notin \wp_E^2\}$.

If $n(\alpha) = 0$, then $\alpha \equiv \lambda_0(\alpha)e_P$ modulo $\mathcal{O}_E[P]$ and so $\alpha \in \mathcal{A}$ if and only if $\lambda_0(\alpha)e_P \in \mathcal{A}$. This occurs if and only if $\lambda_0(\alpha)$ belongs to \wp_E , respectively \wp_E^2 , in case (i), respectively case (ii), and this is in turn equivalent to the element α satisfying the conditions in the conclusion of Proposition 2.1 with respect to the element $\mu = 0$.

To prove the inductive step we shall assume that the result of Proposition 2.1 is valid for all elements α for which $n(\alpha) \leq s - 1$ (and also, as noted above, that if $m(\alpha) > 0$, then the element μ can be taken to equal 0). We now suppose that $n(\alpha) = s$, and we relabel so that none of $\lambda_1(\alpha), \lambda_2(\alpha), \dots, \lambda_s(\alpha)$ belong to \wp_E^2 . We set $\alpha_1 := \sum_{i=0}^{i=s} \lambda_i(\alpha)(e_i - e_P)$ so that $\alpha \equiv \alpha_1$ modulo $\mathcal{O}_E[P]$, and hence $\alpha \in \mathcal{A}$ if and only if $\alpha_1 \in \mathcal{A}$.

We deal first with the case that at least one of the elements $\lambda_i(\alpha), 1 \leq i \leq s$, belongs to \wp_E . By relabelling if necessary, we assume that $\lambda_i(\alpha) = p\kappa_1$ with $\kappa_1 \in \mathcal{O}_E$. Setting $\alpha_2 := (\lambda_0(\alpha) - p\kappa_1)e_P + \sum_{i=2}^{i=s} \lambda_i(\alpha)(e_i - e_P)$ one has $\alpha_1 \equiv \alpha_2$ modulo $\mathcal{O}_E[P]$. Since $n(\alpha_2) \leq s - 1$ and $m(\alpha_2) > 0$ we may now apply our inductive hypothesis to α_2 to deduce that

$$\lambda_i(\alpha) \equiv 0 \equiv \lambda_0(\alpha) - p\kappa_1 \text{ modulo } \wp_E \text{ for } 2 \leq i \leq s$$

and

$$\sum_{i=2}^{i=s} \lambda_i(\alpha) \equiv \lambda_0(\alpha) - p\kappa_1 \text{ modulo } \wp_E^2$$

in case (ii), and

$$\lambda_i(\alpha) \equiv 0 \equiv \lambda_0(\alpha) - p\kappa_1 \text{ modulo } \wp_E \text{ for } 2 \leq i \leq s$$

in case (i). These congruences in turn imply that α satisfies the conclusions of Proposition 2.1 with respect to the element $\mu = 0$.

We now consider the case that none of the elements $\lambda_i(\alpha)$, $1 \leq i \leq s$, belong to \wp_E . In this case we may assume without loss of generality that $\lambda_1(\alpha) = 1$. Setting

$$\alpha_3 := \alpha_1^2 - \alpha_1 = (\lambda_0(\alpha)^2 - \lambda_0(\alpha))e_P + \sum_{i=2}^{i=s} (\lambda_i(\alpha)^2 - \lambda_i(\alpha))(e_i - e_P)$$

we have $n(\alpha_3) \leq s - 1$ and $m(\alpha_3) > 0$. Now if $\alpha_1 \in \mathcal{A}$, then $\alpha_3 \in \mathcal{A}$ and so by applying the inductive hypothesis to α_3 we may deduce that

$$\lambda_0(\alpha)^2 - \lambda_0(\alpha) \equiv 0 \equiv \lambda_i(\alpha)^2 - \lambda_i(\alpha) \pmod{\wp_E} \quad \text{for } 2 \leq i \leq s$$

and

$$\sum_{i=2}^{i=s} (\lambda_i(\alpha)^2 - \lambda_i(\alpha)) \equiv \lambda_0(\alpha)^2 - \lambda_0(\alpha) \pmod{\wp_E^2}$$

in case (ii), and

$$\lambda_0(\alpha)^2 - \lambda_0(\alpha) \equiv 0 \equiv \lambda_i(\alpha)^2 - \lambda_i(\alpha) \pmod{\wp_E} \quad \text{for } 2 \leq i \leq s$$

in case (i). From these congruences it follows that for each $i \in \Sigma^*$ there are elements $\kappa_i \in \mathcal{O}_E$, and $\delta_i \in \{0, 1\}$ (with $\kappa_1 = 0$ and $\delta_1 = 1$) such that

$$\lambda_i(\alpha) = \delta_i + p\kappa_i,$$

and also in case (ii) that

$$\kappa_0(2\delta_0 - 1) \equiv \sum_{i=1}^{i=s} \kappa_i(2\delta_i - 1) \pmod{\wp_E}. \quad (2.1)$$

Since $p(\sum_{i=1}^{i=s} \kappa_i e_i) \in \mathcal{O}_E[P]$ we may at this stage replace α by $\alpha_4 := \alpha - p(\sum_{i=1}^{i=s} \kappa_i e_i)$. In the above computation, this change has the effect of replacing κ_i by 0 for each $1 \leq i \leq s$ and replacing κ_0 by $\kappa_0 - \sum_{i=1}^{i=s} \kappa_i$, and after this change the condition (2.1) becomes

$$\kappa_0 - \sum_{i=1}^{i=s} \kappa_i \equiv 0 \pmod{\wp_E}. \quad (2.2)$$

Setting $\alpha_5 := \sum_{i=0}^{i=s} \delta_i(e_i - e_P)$ we have

$$\alpha_4 = \alpha_5 + p(\kappa_0 - \sum_{i=1}^{i=s} \kappa_i)e_P,$$

and in both cases (i) and (ii) (as a consequence of (2.2)) this implies that if $\alpha \in \mathcal{A}$, then $\alpha_5 \in \mathcal{A}$. Since however α_5 is an idempotent the result of ([Bl,Bu], Satz 3.1) implies that $\alpha_5 \in \mathcal{A}$ if and only if $\alpha_5 \in \{0, 1\}$. But we know that $\alpha_5 \neq 0$ (as $\delta_1 = 1$) and hence we must have $\alpha_5 = 1$. This implies both that $s = p + 1$ and $\delta_i = 1$ for all $i \in \Sigma^*$, and this in turn implies that α satisfies the conditions of the conclusion of Proposition 2.1 with respect to the element $\mu = 1$. \square

Corollary 2.2. *Let P be isomorphic to $C_p \times C_p$. Then for each character $\chi \in C^*$ one has $\mathcal{A}(E[P]; e_\chi I) = \mathcal{O}_E[P]$ if and only if $pe_P \notin \mathcal{A}(E[P]; e_\chi I)$.*

Proof. We set $\mathcal{A} := \mathcal{A}(E[P]; e_\chi I)$. We shall assume that $pe_P \notin \mathcal{A}$ and use this to deduce that $\mathcal{A} = \mathcal{O}_E[P]$.

For each index $i \in \Sigma$ we choose elements $g_i \in P \setminus P_i$ and $g'_i \in P_i \setminus \{1\}$, and set $f_i := g_i - 1$ and $f'_i := g'_i - 1$ respectively. The maximal order $\mathcal{M}(E, P)$ is the \mathcal{O}_E -span of the set

$$P \cup \{e_i - e_P : i \in \Sigma^*\} \cup \{f_i^j e_i : 1 \leq j \leq p - 2, 1 \leq i \leq p - j\}$$

(cf. Lemma 1.10). A set of representatives of $\mathcal{M}(E, P)$ modulo $\mathcal{O}_E[P]$ is therefore contained in the set of elements of the type

$$\alpha := \sum_{i \in \Sigma^*} \lambda_i (e_i - e_P) + \beta$$

with each $\lambda_i \in \mathcal{O}_E$ and β equal to a sum of elements of the form $\lambda_{i,j} f_i^j e_i$ with $1 \leq j \leq p - 2, 1 \leq i \leq p - j$ and each $\lambda_{i,j}$ coming from a set of representatives of \mathcal{O}_E modulo \wp_E . Now if $\alpha \in \mathcal{A}$, then $\alpha^p \in \mathcal{A}$. But

$$\alpha^p \equiv \sum_{i \in \Sigma^*} \lambda_i^p (e_i - e_P) \text{ modulo } \mathcal{O}_E[P], \tag{2.3}$$

and hence the element $\sum_{i \in \Sigma^*} \lambda_i^p (e_i - e_P)$ must belong to \mathcal{A} . Proposition 2.1 now implies that there is an element $\mu \in \mathcal{O}_E$ such that $\lambda_i^p \equiv \mu$ modulo \wp_E for all $i \in \Sigma^*$. This in turn implies that there exists an element $\mu' \in \mathcal{O}_E$ such that $\lambda_i \equiv \mu'$ modulo \wp_E for all $i \in \Sigma^*$. By subtracting $\mu' = \sum_{i \in \Sigma^*} \mu' (e_i - e_P)$ from α we may thus henceforth assume that $\lambda_i \in \wp_E$ for each $i \in \Sigma^*$.

Recall now that we are assuming $pe_P \notin \mathcal{A}$. If $\beta = 0$, then (since $\alpha \in \mathcal{A}$) Proposition 2.1(ii) implies that $\alpha \in \mathcal{O}_E[P]$. We therefore assume that $\beta \neq 0$, and we let j_0 denote the least value of j such that there is a term $\lambda_{i_0, j_0} f_{i_0}^{j_0} e_{i_0}$ in the expression for β for which $\lambda_{i_0, j_0} \notin \wp_E$. Now since $\lambda_i \in \wp_E$ for each $i \in \Sigma^*$ there is a unit $u \in \mathbb{Z}_p^*$ such that

$$\left(\prod_{\substack{1 \leq i \leq p - j_0 \\ i \neq i_0}} f'_i \right) \alpha \equiv u \lambda_{i_0, j_0} f_{i_0}^{p-1} e_{i_0} \text{ modulo } \mathcal{O}_E[P]$$

(cf. (1.4)), and since $f_{i_0}^{p-1}e_{i_0} \equiv -p(e_{i_0} - e_P)$ modulo $pf_{i_0}e_{i_0}\mathcal{O}_E[P]$ this last expression is congruent to $u\lambda_{i_0, j_0}pe_P$ modulo $\mathcal{O}_E[P]$. Since however $u\lambda_{i_0, j_0} \in \mathcal{O}_E^*$ this implies that $pe_P \in \mathcal{A}$ and this in turn contradicts our original assumption. This now completes the proof of Corollary 2.2. \square

We now turn to give the proof of Proposition 1.11. The first parts of both Proposition 1.11(i) and (ii) are consequences of Corollary 2.2 and an easy computation of valuations to show that $pe_G \notin \mathcal{A}(E[G]; \wp_L^i)$ if and only if either $e_K > 1$ or $e_K = 1$ and $i \equiv 1$ modulo p^2 . The final part of Proposition 1.11(i) follows from Lemma 1.1(i) and the fact that the order $\mathcal{O}_K[G]$ is Gorenstein, whilst the case $\#G = p$ of Proposition 1.11(ii) follows from the fact that each order $\mathcal{A}(K[G]; I)$ is equal to either $\mathcal{O}_K[G]$ or $\mathcal{M}(K, G)$ and both of these orders are Gorenstein. The sufficiency of the conditions $i \equiv 0$ or 1 modulo p^2 in Proposition 1.11(ii) follows immediately from Lemma 1.1. To prove the last part of Proposition 1.11(ii) we first make two general observations.

Lemma 2.3. *Let P be isomorphic to $C_p \times C_p$. If Q is any subgroup of order p , then for any ideal I of \mathcal{O}_L one has $t_Q\mathcal{A}(E[G]; I) = t_Q\mathcal{O}_E[G]$.*

Proof. We may assume that E is the maximal absolutely unramified subfield of K . Since in this case the algebra $E[C]$ is split one has $\mathcal{A}(E[G]; I) = \bigoplus_{\chi \in C^*} e_\chi \mathcal{A}_\chi$ where for each $\chi \in C^*$ we have set $\mathcal{A}_\chi := \mathcal{A}(E[P]; e_\chi I)$. We therefore need only prove that for each character χ one has $t_Q\mathcal{A}_\chi \subseteq t_Q\mathcal{O}_E[P]$, and to do this we shall use the same argument (and notation) as in the proof of Corollary 2.2. Thus if

$$\alpha := \sum_{i \in \Sigma^*} \lambda_i(e_i - e_P) + \beta \in \mathcal{A}_\chi,$$

then

$$\sum_{i \in \Sigma^*} \lambda_i^p(e_i - e_P) \in \mathcal{A}_\chi$$

(cf. (2.3)) and so Proposition 2.1 implies that there is an element $\mu \in \mathcal{O}_E$ such that $\lambda_i \equiv \mu$ modulo \wp_E for all $i \in \Sigma^*$. Relabelling so that $Q = P_1$, and noting that $t_1\beta \in \mathcal{O}_E[P]$, it follows that

$$t_1\alpha = p\lambda_0e_P + p\lambda_1(e_1 - e_P) + t_1\beta \equiv p(\lambda_0 - \lambda_1)e_P \equiv p(\mu - \mu)e_P \equiv 0 \pmod{\mathcal{O}_E[P]},$$

and hence $t_1\mathcal{A}_\chi \subseteq t_1\mathcal{O}_E[P]$. \square

Lemma 2.4. *Let H be any subgroup of G . If $\text{Fr}(E[G]; I)$, then $\text{Fr}(E[G/H]; t_HI)$ and $\mathcal{A}(E[G/H]; t_HI) = e_H\mathcal{A}(E[G]; I)$.*

Proof. If $\text{Fr}(E[G]; I)$, then $t_H I$ is isomorphic to a direct sum of copies of $e_H \mathcal{A}(E[G]; I)$. This implies the result since $e_H \mathcal{A}(E[G]; I)$ identifies with an order in $E[G/H]$. \square

We now turn to complete the proof of Proposition 1.11(ii). If G is isomorphic to $C_p \times C_p$ and Q is any subgroup of order p , then Lemmas 2.3 and 2.4 imply that $t_Q I$ is free over $\mathcal{O}_E[G/Q]$ and hence, from Lemma 1.1, that $v_{LQ}(t_Q(I)) \equiv 1$ modulo p . Using (0.5) it follows from this that $v_L(I) \equiv -\kappa$ modulo p^2 for some integer κ with $-1 \leq \kappa \leq p-2$. Excluding the cases $\kappa = -1$ and $\kappa = 0$ (which are dealt with in Lemma 1.1) we may thus assume that κ satisfies $1 \leq \kappa \leq p-2$. Our proof is therefore now completed by the following computation.

Lemma 2.5. *Let G be isomorphic to $C_p \times C_p$, and assume that $e_K = 1$. Let κ be any integer with $1 \leq \kappa \leq p-2$. If $\text{Fr}(E[G]; \wp_L^{p^2-\kappa})$, then*

$$[\mathcal{A}(E[G]; \wp_L^{p^2-\kappa}) : \mathcal{O}_E[G]]_{\mathcal{O}_E} = \wp_E^{\kappa+1}.$$

If $E = K$, then in all cases

$$[\mathcal{A}(K[G]; \wp_L^{p^2-\kappa}) : \mathcal{O}_K[G]]_{\mathcal{O}_K} \mid \wp_K^{\kappa+1},$$

and the following conditions are equivalent:-

- (i) $[\mathcal{A}(K[G]; \wp_L^{p^2-\kappa}) : \mathcal{O}_K[G]]_{\mathcal{O}_K} = \wp_K^{\kappa+1}$.
- (ii) $\text{Fr}(K[G]; \wp_L^{p^2-\kappa})$.
- (iii) $\mathcal{A}(K[G]; \wp_L^{p^2-\kappa}) \cap (\mathcal{A}_{p-\kappa}(K, G) \setminus \mathcal{A}_{p-\kappa+1}(K, G)) \neq \emptyset$.

Proof. At the heart of this proof are Fröhlich’s observation that \mathcal{O}_L is factor equivalent to $\mathcal{O}_E[G]^{[K:E]}$ (cf. [Fr4], Theorem 7 (Additive)), and the factorisability techniques developed in [Bu2] and [Bu4]. To be more precise, we shall use the notion of factorisable quotient functions as described in ([Bu2], §1).

Let κ be any integer with $1 \leq \kappa \leq p-2$. Then for any subgroup H of G one has

$$(\wp_L^{p^2-\kappa})^H = \begin{cases} \wp_{LH}^p, & \text{if } \#H = p, \\ \wp_K, & \text{if } H = G. \end{cases}$$

Upon evaluating the $\mathcal{O}_E[G]$ -factorisable quotient function $\tilde{f}_{\wp_L^{p^2-\kappa}, \mathcal{O}_L}$ of $\wp_L^{p^2-\kappa}$ and \mathcal{O}_L at G^* (for the precise definition of such functions see for example ([Bu2], (1.4))) one therefore has

$$\begin{aligned} & \tilde{f}_{\wp_L^{p^2-\kappa}, \mathcal{O}_L}(G^*) \\ &= [\wp_K : \mathcal{O}_K]_{\mathcal{O}_E} \cdot \left(\prod_{\substack{H < G \\ \#H=p}} [\wp_{LH}^p : \mathcal{O}_{LH}]_{\mathcal{O}_E} \cdot [\wp_K : \mathcal{O}_K]_{\mathcal{O}_E}^{-1} \right) \cdot [\wp_L^{p^2-\kappa} : \mathcal{O}_L]_{\mathcal{O}_E}^{-1} \end{aligned}$$

$$= (\wp_E^{-\kappa})^{[K:E]}.$$

Now if $\#H = p$, then $v_{LH} \left((\wp_L^{p^2-\kappa})^H \right) = p$ and (0.5) implies that $v_{LH} \left(e_H \wp_L^{p^2-\kappa} \right) = 1$. Setting $\mathcal{A}_E := \mathcal{A}(E[G]; \wp_L^{p^2-\kappa})$, it follows from these valuations (and (0.3)) that

$$\mathcal{A}_E^H = \begin{cases} \mathcal{O}_E[G]\{t_H, p^{-1}t_G\}, & \text{if } \#H = p, \\ \mathcal{O}_{E^p}^{-1}t_G, & \text{if } H = G. \end{cases} \quad (2.4)$$

The value of the factorisable quotient function $\tilde{f}_{\mathcal{A}_E, \mathcal{O}_E[G]}$ at G^* is therefore equal to

$$\begin{aligned} & [\mathcal{A}_E^G : \mathcal{O}_E[G]^G]_{\mathcal{O}_E} \cdot \left(\prod_{\substack{H < G \\ \#H = p}} [\mathcal{A}_E^H : \mathcal{O}_E[G]^H]_{\mathcal{O}_E} \cdot [\mathcal{A}_E^G : \mathcal{O}_E[G]^G]_{\mathcal{O}_E}^{-1} \right) \cdot [\mathcal{A}_E : \mathcal{O}_E[G]]_{\mathcal{O}_E}^{-1} \\ &= \wp_E \cdot [\mathcal{A}_E : \mathcal{O}_E[G]]_{\mathcal{O}_E}^{-1}. \end{aligned}$$

The first assertion of Lemma 2.5 now follows easily from the fact that \mathcal{O}_L is factor equivalent to $\mathcal{O}_E[G]^{[K:E]}$. Indeed, this fact implies that if $\text{Fr}(E[G]; \wp_L^{p^2-\kappa})$, then $\tilde{f}_{\wp_L^{p^2-\kappa}, \mathcal{O}_L}$ is equal to the $[K : E]$ th-power of $\tilde{f}_{\mathcal{A}_E, \mathcal{O}_E[G]}$, and hence therefore that

$$\tilde{f}_{\wp_L^{p^2-\kappa}, \mathcal{O}_L}(G^*) = \left(\tilde{f}_{\mathcal{A}_E, \mathcal{O}_E[G]}(G^*) \right)^{[K:E]}.$$

We henceforth consider the case $E = K$. We note first that if $\#H = p$, then $(\wp_L^{p^2-\kappa})^H = \wp_{L^H}^p$ so that

$$\mathcal{A}(K[G/H]; (\wp_L^{p^2-\kappa})^H) = \mathcal{A}(K[G/H]; \mathcal{O}_{L^H}) = \mathcal{M}(K, G/H)$$

and hence, in the language of [Bu2], the lattices $\wp_L^{p^2-\kappa}$ and \mathcal{A}_K are G -o-equivalent (cf. [Bu2], 1.11). It follows from ([Bu2], Corollary 1.10) (see also ([Bu4], Theorem 1 and Remarks 1.7)) that

$$\tilde{f}_{\mathcal{A}_K, \mathcal{O}_K[G]}(G^*) \mid \tilde{f}_{\wp_L^{p^2-\kappa}, \mathcal{O}_L}(G^*) \quad (2.5)$$

and furthermore that there is equality here if and only if $\text{Fr}(K[G]; \wp_L^{p^2-\kappa})$. The second assertion, and also the equivalence of conditions (i) and (ii), of Lemma 2.5 now follows by substituting the above explicit expressions for $\tilde{f}_{\mathcal{A}_K, \mathcal{O}_K[G]}(G^*)$ and $\tilde{f}_{\wp_L^{p^2-\kappa}, \mathcal{O}_L}(G^*)$ into (2.5). At this stage, to complete the proof of Lemma 2.5 it only remains for us to show that the conditions (i) and (iii) are equivalent.

Sublemma 2.6. *Let κ be any integer with $1 \leq \kappa \leq p - 2$. We set $\mathcal{A}(\kappa) := \mathcal{A}(K[G]; \wp_L^{p^2-\kappa})$, and for each integer r with $1 \leq r \leq p$ we let \mathcal{A}_r denote the lattice $\mathcal{A}_r(K, G)$. If $r < p$ and $\alpha \in \mathcal{A}(\kappa) \cap (\mathcal{A}_r \setminus \mathcal{A}_{r+1})$, then*

$$\alpha = \sum_{i=1}^{i=p+1-r} c_i f_i^{r-1} e_i + \alpha'$$

with each $c_i \in \mathcal{O}_K^$, and $\alpha' \in \mathcal{A}_{r+1}$. Furthermore, if $\mathcal{A}(\kappa) \cap (\mathcal{A}_r \setminus \mathcal{A}_{r+1}) \neq \emptyset$, then for each integer s with $r \leq s \leq p - 1$ one has $\mathcal{A}(\kappa) \cap (\mathcal{A}_s \setminus \mathcal{A}_{s+1}) \neq \emptyset$.*

Proof. Any element α which belongs to both $\mathcal{A}(\kappa)$ and $\mathcal{A}_r \setminus \mathcal{A}_{r+1}$ is of the form

$$\alpha = \sum_{i=1}^{i=p+1-r} c_i f_i^{r-1} e_i + \alpha'$$

with each $c_i \in \mathcal{O}_K$ and $\alpha' \in \mathcal{A}_{r+1}$, and we need only show that each coefficient c_i belongs to \mathcal{O}_K^* . We set $d := \#\{c_i : c_i \in \mathcal{O}_K^*\}$ so that $0 \leq d \leq p + 1 - r$ and our aim is to show that $d = p + 1 - r$. We argue by contradiction, and so shall assume that $r + d \leq p$. Since $\alpha \notin \mathcal{A}_{r+1}$ we have $d > 0$, and (perhaps after relabelling) we can assume that each of the elements c_1, c_2, \dots, c_d belongs to \mathcal{O}_K^* . For each integer j with $2 \leq j \leq p + 1$ we choose a non-trivial element $g'_j \in P_j$ and then let γ denote the product $\prod_{j=2}^{j=d} (g'_j - 1)$. Since $(g'_j - 1)e_j = 0$ for each j with $2 \leq j \leq d$ one has

$$\begin{aligned} \gamma\alpha &\equiv \gamma c_1 f_1^{r-1} e_1 + \gamma\alpha' \text{ modulo } \mathcal{O}_K[G] \\ &\equiv u c_1 f_1^{r-1+d-1} e_1 \text{ modulo } \mathcal{A}_{r+d} \end{aligned}$$

for some unit $u \in \mathbb{Z}_p^*$ (cf. (1.4)). Now $r - 1 + d - 1 = (r + d) - 2 \leq p - 2$ and so (2.4) implies that $u c_1 f_1^{r-1+d-1} e_1 \notin \mathcal{A}(\kappa)$. By using this and (0.4) one can show that

$$v_L \left(u c_1 f_1^{r-1+d-1} e_1 \wp_L^{p^2-\kappa} \right) < v_L \left(\beta \wp_L^{p^2-\kappa} \right)$$

for any $\beta \in \mathcal{A}_{r+d}$. The above congruence therefore implies that $\gamma\alpha \notin \mathcal{A}(\kappa)$ and this is a contradiction. Hence we must have $d = p + 1 - r$.

To show that $\mathcal{A}(\kappa) \cap (\mathcal{A}_s \setminus \mathcal{A}_{s+1}) \neq \emptyset$ for any integer s with $r < s \leq p - 1$ we simply note that if α is as above, then writing γ for the product $\prod_{i=p+2-s}^{i=p+1-r} (g'_i - 1)$ one has

$$\gamma\alpha \equiv \gamma \left(\sum_{i=1}^{i=p+1-s} c_i f_i^{r-1} e_i \right) \text{ modulo } \mathcal{A}_{s+1}.$$

Using this congruence it is easy to check that $\gamma\alpha$ belongs to $\mathcal{A}_s \setminus \mathcal{A}_{s+1}$. □

We now turn to prove the implication (iii) \Rightarrow (i) of Lemma 2.5. If $\mathcal{A}(\kappa) \cap (\mathcal{A}_{p-\kappa} \setminus \mathcal{A}_{p-\kappa+1}) \neq \emptyset$, then Sublemma 2.6 implies that for each non-negative

integer s with $s < \kappa$ we have $\mathcal{A}(\kappa) \cap (\mathcal{A}_{p-\kappa+s} \setminus \mathcal{A}_{p-\kappa+s+1}) \neq \emptyset$. Using Lemma 1.10 it now follows that $[\mathcal{A}(\kappa) : \mathcal{O}_K[G]]_{\mathcal{O}_K}$ is divisible by $\wp_K^{\kappa+1}$. Since this implies that (2.5) must be an equality it follows that (iii) does indeed imply (i).

Finally, we prove the implication (i) \Rightarrow (iii) of Lemma 2.5. If $\mathcal{A}(\kappa) \cap (\mathcal{A}_{p-\kappa} \setminus \mathcal{A}_{p-\kappa+1})$ is empty, then by using Sublemma 2.6 one can show that $\mathcal{A}(\kappa) \subseteq \mathcal{A}_{p-\kappa+1}$. We let s denote the least integer t such that both $p - \kappa + 1 \leq t \leq p - 1$ and $\mathcal{A}(\kappa) \cap (\mathcal{A}_t \setminus \mathcal{A}_{t+1}) \neq \emptyset$. If α_s is any element of this intersection, then

$$\alpha_s = \alpha_s^* + \alpha_s^{**}$$

with $\alpha_s^* \in \Lambda_s(K, G)$ and $\alpha_s^{**} \in \mathcal{A}_{s+1}$. For any such element Sublemma 2.6 implies that no coefficient of α_s^* belongs to \wp_K . From this last fact it follows that if β_s is any other element of $\mathcal{A}(\kappa) \cap (\mathcal{A}_s \setminus \mathcal{A}_{s+1})$, with a decomposition $\beta_s = \beta_s^* + \beta_s^{**}$ as above, then there exists an element $\mu \in \mathcal{O}_E$ such that $\beta_s^* \equiv \mu \alpha_s^*$ modulo \mathcal{A}_{s+1} . There is therefore an inclusion

$$\mathcal{A}(\kappa) \subseteq \mathcal{O}_K \alpha_s + \mathcal{A}_{s+1}.$$

By repeating this argument one can find for each integer i with $s \leq i \leq p - 1$ an element $\alpha_i \in \mathcal{A}(\kappa) \cap (\mathcal{A}_i \setminus \mathcal{A}_{i+1})$ which is such that

$$\mathcal{A}(\kappa) = \mathcal{A}_p + \sum_{i=s}^{i=p-1} \mathcal{O}_K \alpha_i.$$

Since $p\alpha_i \in \mathcal{A}_p$ it follows from this equality that the index $[\mathcal{A}(\kappa) : \mathcal{O}_K[G]]_{\mathcal{O}_K}$ divides \wp_K^{p-s+1} , and hence is not equal to $\wp_K^{\kappa+1}$. We have now proved that (i) implies (iii). \square

This completes the proof of Proposition 1.11, and so we shall now turn to consider Proposition 1.8. Since the assertion of Proposition 1.8(ii) follows immediately from Lemma 1.1 we need only consider the case that $e_K > 1$.

We suppose for the moment that $G_{(2)} = 1$ and $e_K > 1$. We shall prove Proposition 1.8(i) by an induction on $\#G$. (Recall that G is a p -group since $G_{(2)} = 1$.) From Proposition 1.11(i) we know that if $\#G = p$, then $\mathcal{A}(E[G]; \wp_L^i) = \mathcal{O}_E[G]$ and so the inductive base is a consequence of Lemma 1.1(i).

For the inductive step we take $\#G = p^k$ for an integer $k > 1$ and assume that the result is true if $\#G = p^{k-1}$. We let H denote a subgroup of G of order p and let Γ denote the quotient G/H and F the fixed field L^H . We consider an ideal \wp_L^i with i an integer satisfying $0 \leq i < p^k$. If $\text{Fr}(E[G]; \wp_L^i)$, then $\text{Fr}(E[\Gamma]; t_H \wp_L^i)$ (cf. Lemma 2.4) and so by our inductive hypothesis it follows that $v_F(t_H \wp_L^i) \equiv 1$ modulo p^{k-1} . A simple valuation computation using (0.5) shows that this implies that either $i = 0$, $i = 1$, or $i = p^k - j$ for an integer j satisfying $0 < j \leq p - 2$.

Since the case $i = 1$ is dealt with by Lemma 1.1(i) we only need to show that the other two possibilities cannot occur. Now $\text{Fr}(E[G]; \wp_L^i)$ implies that

$$(\wp_L^i)^H \cong (\mathcal{A}(E[G]; \wp_L^i)^H)^{[K:E]} \tag{2.6}$$

(a direct sum of $[K : E]$ copies of $\mathcal{A}(E[G]; \wp_L^i)^H$). We next note that

$$(\wp_L^i)^H = \begin{cases} \mathcal{O}_F, & \text{if } i = 0, \\ \wp_F^{p^{k-1}}, & \text{if } i = p^k - j, \ 0 < j \leq p - 2 \end{cases}$$

and so, since $\mathcal{A}(E[G]; \wp_L^i)^H = \mathcal{A}(E[\Gamma]; e_H \wp_L^i, (\wp_L^i)^H)$, one has

$$\mathcal{A}(E[G]; \wp_L^i)^H = \begin{cases} \mathcal{A}(E[\Gamma]; 1 - p^{k-1}, 0), & \text{if } i = 0, \\ \mathcal{A}(E[\Gamma]; 1, p^{k-1}), & \text{if } i = p^k - j, \ 0 < j \leq p - 2. \end{cases}$$

In both cases one therefore has

$$(\wp_L^i)^H \cong \mathcal{O}_F \text{ and } \mathcal{A}(E[G]; \wp_L^i)^H \cong \mathcal{A}(E[\Gamma]; 1, 0). \tag{2.7}$$

We next show that

$$\mathcal{A}(E[\Gamma]; 1, 0) = \mathcal{A}(E[\Gamma]; 0, 0). \tag{2.8}$$

To prove this we note that if $\alpha \in \mathcal{A}(E[\Gamma]; 1, 0)$, then $t_\Gamma \alpha_{\wp_F} \subseteq t_\Gamma \mathcal{O}_F$. But if $\epsilon(\alpha)$ denotes the augmentation of α (so that $\epsilon(\alpha) \in E$), then $t_\Gamma \alpha_{\wp_F} = \epsilon(\alpha) t_\Gamma \wp_F = \epsilon(\alpha)_{\wp_K}$ whereas $t_\Gamma \mathcal{O}_F = \wp_K$ and so we must have $\epsilon(\alpha) \in \mathcal{O}_E$. Now since F/K is totally ramified one has $\mathcal{O}_F = \mathcal{O}_K + \wp_F$. Thus if $\alpha \in \mathcal{A}(E[\Gamma]; 1, 0)$, then

$$\alpha \mathcal{O}_F = \alpha \mathcal{O}_K + \alpha_{\wp_F} = \epsilon(\alpha) \mathcal{O}_K + \alpha_{\wp_F} \subseteq \mathcal{O}_F,$$

and so $\alpha \in \mathcal{A}(E[\Gamma]; 0, 0)$. Since the inclusion $\mathcal{A}(E[\Gamma]; 0, 0) \subseteq \mathcal{A}(E[\Gamma]; 1, 0)$ is clear we have now proved the equality (2.8). Now from (2.6-8) it follows that $\text{Fr}(E[\Gamma]; \mathcal{O}_F)$ and this is a contradiction to our inductive hypothesis. \square

In the rest of this section we shall give the proof of Theorem 1.3(i). To this end, we first observe that if G is not cyclic and $\text{Fr}(E[G]; \mathcal{I}_L)$, then G is a p -group. Indeed, this follows immediately from Lemma 2.4 in conjunction with the following result for the special case that P is isomorphic to $C_p \times C_p$.

Lemma 2.7. *Let P be isomorphic to $C_p \times C_p$. If $\text{Fr}(E[G]; \mathcal{I}_L)$, then $G_{(2)} = 1$ and $G = P$.*

Proof. Take a subgroup Q of P with $\#Q = p$. From Lemmas 2.3 and 2.4 we know that $t_Q I$ is free over $t_Q \mathcal{A}(E[G]; I) = t_Q \mathcal{O}_E[G] \cong \mathcal{O}_E[G/Q]$, and so from Lemma 1.1(i) we deduce that $(G/Q)_{(2)} = 1$. It follows from this that G/Q , and hence

also G , is a p -group. Now since $(G/Q)^{(2)} = 1$ for each subgroup Q of order p it follows from Herbrand's theorem that $G^{(2)} = 1$, and hence (since G is a p -group) that $G_{(2)} = 1$. \square

We shall henceforth restrict to the case that G is a p -group. In this case Lemma 2.4 implies that Theorem 1.3(i) will follow if one has $\text{NFr}(E[G]; \mathcal{I}_L)$ whenever G is isomorphic to $C_{p^2} \times C_p$. To prove this we will use the following general result.

Lemma 2.8. *Let G be isomorphic to $C_{p^2} \times C_p$, and let H denote the subgroup of p th powers in G . Then for any element $\alpha \in \mathcal{A}(E[G]; I)^H$ one has $\epsilon(\alpha) \in \wp_E$.*

Proof. For any positive integer m one has $\epsilon(\alpha^m) = \epsilon(\alpha)^m$, and so it suffices for us to prove that $\epsilon(\alpha^{p^n}) \in \wp_E$ for any sufficiently large integer n . Since the group G/H is of type (p, p) there are $p + 1$ subgroups of G which have order p^2 and contain H . We label these subgroups as G_i , $i \in \Sigma$, and we set $e_i := e_{G_i}$ for each $i \in \Sigma$ and $e_0 := 2e_G$. If for each $i \in \Sigma$ we choose an element $g_i \in G \setminus G_i$ and set $f_i := g_i - 1$, then a typical element α of $e_H \mathcal{M}(E, G)$ is of the form

$$\alpha = \sum_{i \in \Sigma^*} \lambda_i (e_i - e_P) + \sum_{\substack{i \in \Sigma \\ j \geq 1}} \lambda_{i,j} f_i^j e_i \quad (2.9)$$

with each coefficient $\lambda_i, \lambda_{i,j}$ belonging to \mathcal{O}_E . For any such element α it is not difficult to show that

$$\alpha^{p^3} \equiv \sum_{i \in \Sigma^*} \lambda_i^{p^3} (e_i - e_P) \text{ modulo } \mathcal{O}_E[P]. \quad (2.10)$$

Now from (2.9) it follows that $\epsilon(\alpha) = \lambda_0$ and so, given the congruence (2.10), it suffices for us to show that for any element β of the form

$$\beta = \sum_{i \in \Sigma^*} \mu_i (e_i - e_P) \in \mathcal{A}$$

one has $\mu_0 \in \wp_E$. If now $J(\beta)$ denotes the set $\{i \in \Sigma^* : \mu_i \notin \wp_E\}$, then with N denoting the exponent of $(\mathcal{O}_E/\wp_E^3)^*$ one has

$$\beta^N \equiv \sum_{i \in J(\beta)} (e_i - e_P) \text{ modulo } \mathcal{O}_E[P],$$

and so we may deduce that $\gamma := \sum_{i \in J(\beta)} (e_i - e_P)$ belongs to \mathcal{A} . Since however γ is an idempotent it follows from ([Bl, Bu], Satz 3.1) that it is equal to either 0 or 1. It is however clear that $\gamma \neq 1$ (since, for example, $\gamma h = \gamma$ for each $h \in H$) and so we must have $\gamma = 0$. This in turn implies that $J(\beta)$ is empty, and in particular therefore that $\mu_0 \in \wp_E$. \square

Proposition 2.9. *Let G be isomorphic to $C_{p^2} \times C_p$. If $e_K > 1$, then $\text{NFr}(E[G]; \mathcal{I}_L)$.*

Proof. Let \mathcal{A} be $\mathcal{A}(E[G]; I)$. We first note that if $\text{Fr}(E[G]; I)$, then $p^2 e_G \in \mathcal{A}$. Indeed, if $\text{Fr}(E[G]; I)$ and $p^2 e_G \notin \mathcal{A}$, then $\hat{H}^0(G, I) = \hat{H}^0(G, \mathcal{A})^{[K:E]} = 0$, and since $G_{(2)} \neq 1$ this contradicts Lemma 1.1.

If $\text{Fr}(E[G]; I)$, then as a consequence of Lemma 2.4 and Lemma 2.7 we must have $G^{(2)}$ equal to the subgroup H of p th-powers in G . Now Lemma 2.8 implies that if $\alpha \in \mathcal{A}^H$, then $p e_G \alpha = p \epsilon(\alpha) e_G \in \mathcal{A}^H$. This implies that $p e_{G/H} \in \mathcal{A}(E[G/H]; \mathcal{A}^H) = \mathcal{A}(E[G/H]; I^H)$, and since $(G/H)_{(2)} = 1$ this in turn contradicts Proposition 1.11(i). \square

Proposition 2.10. *Let G be isomorphic to $C_{p^2} \times C_p$, and suppose that $e_K = 1$. If $\text{Fr}(E[G]; I)$, then $\mathcal{A}(E[G]; I) \neq \mathcal{A}(\mathbb{Q}_p[G]; I) \mathcal{O}_E$.*

Remark 2.11. It follows immediately from Proposition 2.10 that $\text{NFr}(\mathbb{Q}_p[G]; \mathcal{I}_L)$. However, as Example 1.6 above showed, the possibility that for some field E and ideal I one has $\text{Fr}(E[G]; I)$ cannot be ruled out.

In the remainder of this section we shall prove Proposition 2.10. We set $\mathcal{A}_E := \mathcal{A}(E[G]; I)$ and then $\mathcal{A} := \mathcal{A}_{\mathbb{Q}_p}$. Since $e_K = 1$ the ramification filtration of G is given by $G = G^{(1)} > G^{(2)} > G^{(3)} = \{1\}$ with $G^{(2)}$ equal to the subgroup of p th powers in G (cf. [Bu2], Lemma 1.13). We set $H = G^{(2)}$, and write Γ for the quotient G/H , F for the subfield L^H , and $v(-)$ for the valuation $v_F(-)$.

We shall henceforth assume that $\text{Fr}(E[G]; I)$, and our aim is therefore to deduce that $\mathcal{A}_E \neq \mathcal{A} \mathcal{O}_E$. Now, under this assumption, I is a free \mathcal{A}_E -module of rank $[K : E]$ and so, comparing Tate cohomology (with respect to H) in dimension 0, one must have

$$[I^H : t_H I]_{\mathcal{O}_E} = \left([\mathcal{A}_E^H : t_H \mathcal{A}_E]_{\mathcal{O}_E} \right)^{[K:E]}.$$

Now $\mathcal{A}_E^H = \mathcal{A}(E[\Gamma]; e_H I, I^H)$ and, since $\text{Fr}(E[G]; I)$, also $t_H \mathcal{A}_E = p \mathcal{A}(E[\Gamma]; t_H I)$, and hence this equality is equivalent to

$$\wp_E^{v(t_H I) - v(I^H)} = [\mathcal{A}(E[\Gamma]; e_H I, I^H) : p \mathcal{A}(E[\Gamma]; t_H I)]_{\mathcal{O}_E}. \tag{2.11}$$

Henceforth, for each pair of integers i and j we shall write $(i, j)_E$ as shorthand for the lattice $\mathcal{A}(E[\Gamma]; \wp_F^i, \wp_F^j)$.

It suffices for us to check the validity of (2.11) for each ideal $I = \wp_L^\delta$ with δ satisfying $0 \leq \delta < p^3$. To restrict further the possibilities for δ we note that by Lemma 2.4 one has $\text{Fr}(E[\Gamma]; t_H I)$, and hence by Proposition 1.11(ii) that $v(t_H I) \equiv 0, 1, \text{ or } -\kappa \pmod{p^2}$ for some integer κ satisfying $1 \leq \kappa \leq p - 2$. Applying (0.5) one sees that there are correspondingly three different cases to consider.

To describe these cases we let ϵ be any integer satisfying $0 \leq \epsilon < p$, and we let $\hat{\epsilon}$ denote 1, respectively 2, if $\epsilon \neq p - 1$, respectively $\epsilon = p - 1$.

Case (i) $\delta = p^2 - 2p + 2 + \epsilon$. In this case one has $v(t_H \wp_L^\delta) = p^2$, and $v((\wp_L^\delta)^H) = p - 2 + \hat{\epsilon}$.

Case (ii) $\delta = p^2 - p + 2 + \epsilon$. In this case one has $v(t_H \wp_L^\delta) = p^2 + 1$, and $v((\wp_L^\delta)^H) = p - 1 + \hat{\epsilon}$.

Case (iii) $\delta = p(p - 2 - \kappa) + 2 + \epsilon$ for some integer κ satisfying $1 \leq \kappa \leq p - 2$. In this case one has $v(t_H \wp_L^\delta) = p^2 - \kappa$ and $v((\wp_L^\delta)^H) = p - 2 - \kappa + \hat{\epsilon}$.

Taking into account the explicit valuations recorded in each of these cases (i-iii) the equality (2.11) gives

$$\wp_E^{p^2 - p + 2 - \hat{\epsilon}} = [(0, p - 2 + \hat{\epsilon})_E : p(0, 0)_E]_{\mathcal{O}_E} \quad (2.12)$$

in case (i),

$$\wp_E^{p^2 + 1 - p + 1 - \hat{\epsilon}} = [(1, p - 1 + \hat{\epsilon})_E : p(1, 1)_E]_{\mathcal{O}_E} \quad (2.13)$$

in case (ii), and

$$\wp_E^{p^2 - \kappa - p + 2 + \kappa - \hat{\epsilon}} = [(-\kappa, p - 2 - \kappa + \hat{\epsilon})_E : p(-\kappa, -\kappa)_E]_{\mathcal{O}_E} \quad (2.14)$$

in case (iii). Furthermore, in case (iii) one has $\text{Fr}(E[\Gamma]; \wp_F^{p^2 - \kappa})$ and hence Lemma 2.5 implies that

$$[(-\kappa, -\kappa)_E : \mathcal{O}_E[\Gamma]]_{\mathcal{O}_E} = \wp_E^{\kappa + 1}.$$

By incorporating this into the equality (2.14) one obtains in case (iii) the condition

$$\wp_E^{p^2 - p + 2 - \hat{\epsilon} + \kappa + 1} = [(-\kappa, -\kappa + p - 2 + \hat{\epsilon})_E : p\mathcal{O}_E[\Gamma]]_{\mathcal{O}_E},$$

or equivalently

$$\wp_E^{-p + 3 - \hat{\epsilon} + \kappa} = [(-\kappa, -\kappa + p - 2 + \hat{\epsilon})_E : \mathcal{O}_E[\Gamma]]_{\mathcal{O}_E}. \quad (2.15)$$

Writing $J_p(E, \Gamma)$ for the kernel of the natural surjection $\mathcal{O}_E[\Gamma] \rightarrow k_E$ which is induced by taking augmentation, one has

$$[\mathcal{O}_E[\Gamma] : J_p(E, \Gamma)]_{\mathcal{O}_E} = \wp_E. \quad (2.16)$$

Now $(-\kappa, -\kappa + p - 2 + \hat{\epsilon})_E \subseteq (1, 1)_E$ (cf. (0.2)). But we know from Lemma 1.1 that $(1, 1)_E = \mathcal{O}_E[\Gamma]$ and since it is clear that 1 does not belong to $(-\kappa, -\kappa + p - 2 + \hat{\epsilon})_E$ we may deduce that $(-\kappa, -\kappa + p - 2 + \hat{\epsilon})_E \subseteq J_p(E, \Gamma)$. Taking into account the index (2.16) we may thus rewrite the condition (2.15) as

$$[J_p(E, \Gamma) : (-\kappa, -\kappa + p - 2 + \hat{\epsilon})_E]_{\mathcal{O}_E} = \wp_E^{p - 4 - \kappa + \hat{\epsilon}}. \quad (2.17)$$

This equality implies in particular that in case (iii) we can assume $p - 4 - \kappa + \hat{\epsilon} \geq 0$.

In what follows we fix a non-trivial element γ of Γ (the precise choice doesn't matter) and we set $f := \gamma - 1 \in \mathcal{O}_E[\Gamma]$.

Lemma 2.12. *If $p - 4 - \kappa + \hat{\epsilon} \geq 0$, then $f^{p-4-\kappa+\hat{\epsilon}} \notin (-\kappa, -\kappa + p - 2 + \hat{\epsilon})_E$.*

Proof. To prove this lemma we shall use the following

Sublemma 2.13. *For each integer i with $0 \leq i \leq p - 1$ one has*

$$v(f^i \varphi_F^{-\kappa}) = \begin{cases} -\kappa + i, & \text{if } i \leq \kappa \\ i + 1, & \text{if } \kappa < i \leq p - 1. \end{cases} \tag{2.18}$$

Proof. Note that $\gamma \in \Gamma_{(1)} \setminus \Gamma_{(2)}$. If $i \leq \kappa$ we may thus apply (0.3) i times to obtain $v(f^i \varphi_L^{-\kappa}) = -\kappa + i$.

If Δ is the subgroup of Γ which is generated by γ , then $f^{p-1} \equiv t_\Delta$ modulo $p\mathcal{O}_E[\Delta]$. Using this congruence (and a simple application of (0.5)) one computes that

$$v(f^{p-1} \varphi_F^{-\kappa}) = v(t_\Delta \varphi_F^{-\kappa}) = p. \tag{2.19}$$

This proves 2.18 in the case $i = p - 1$. If on the other hand $i > \kappa$, with $i = p - 1 - s$ say, and $s \neq 0$, then applying (0.3) i times shows that $v(f^i \varphi_F^{-\kappa})$ is strictly positive whilst (2.19) implies that it is not divisible by p . Taken together (0.3) and (2.19) now imply that

$$p = v(f^{p-1} \varphi_F^{-\kappa}) = v(f^s (f^i \varphi_F^{-\kappa})) = v(f^i \varphi_F^{-\kappa}) + s$$

so that $v(f^i \varphi_F^{-\kappa}) = p - s = i + 1$. □

We now return to the proof of Lemma 2.12. Following upon Sublemma 2.13 we see that there are naturally two cases to consider.

Subcase (i) $p - 4 - \kappa + \hat{\epsilon} \leq \kappa$. In this case (2.18) gives

$$\begin{aligned} v(f^{p-4-\kappa+\hat{\epsilon}} \varphi_F^{-\kappa}) &= -\kappa + (p - 4 - \kappa + \hat{\epsilon}) \\ &< -\kappa + p - 2 + \hat{\epsilon}, \end{aligned}$$

and this implies the stated claim.

Subcase (ii) $p - 4 - \kappa + \hat{\epsilon} > \kappa$. In this case (2.18) implies that

$$\begin{aligned} v(f^{p-4-\kappa+\hat{\epsilon}} \varphi_F^{-\kappa}) &= (p - 4 - \kappa + \hat{\epsilon}) + 1 \\ &= (-\kappa + p - 2 + \hat{\epsilon}) - 1 \\ &< -\kappa + p - 2 + \hat{\epsilon}, \end{aligned}$$

and once again this implies the stated result. \square

Lemma 2.14. *Let s and t be any pair of integers such that both $s < t$ and $p\mathcal{O}_E[G] \subseteq (s, t)_E \subseteq J_p(E, \Gamma)$. Let n be any strictly positive integer such that $f^n \notin (s, t)_E$.*

(i) *The elements $\{f^i : 1 \leq i \leq n\}$ are linearly independent in the k_E -space $J_p(E, \Gamma)/(s, t)_E$.*

(ii) *If $p \nmid s$, then the \mathbb{F}_p -span of $\{f^i : 1 \leq i \leq n\}$ is strictly smaller than $J_p(\mathbb{Q}_p, \Gamma)/(s, t)_{\mathbb{Q}_p}$.*

Remark 2.15. Example 1.6 shows that assertion (ii) of Lemma 2.14 is in general false if \mathbb{Q}_p is replaced by a bigger (absolutely unramified) field E .

Proof. We deal first with assertion (i). To do this we set $\alpha = \sum_{i=1}^{i=n} c_i f^i$ with $c_i \in \mathcal{O}_E$ for each i , and we assume that $\alpha \in (s, t)_E$. We must show that $\{c_i : 1 \leq i \leq n\} \subset \wp_E$. However, if this is not true, and i_0 denotes the least integer such that $c_{i_0} \notin \wp_E$, then there exist elements $x \in \mathcal{O}_E[\Gamma]$ and $y \in (s, t)_E$ such that $c_{i_0} f^{i_0} = f^{i_0+1} x + y$. Upon applying these elements to \wp_F^s and taking valuations this equality implies that

$$\begin{aligned} v(f^{i_0} \wp_F^s) &= v(c_{i_0} f^{i_0} \wp_F^s) \\ &\geq \min \left\{ v(f^{i_0+1} \wp_F^s), v(y \wp_F^s) \right\} \\ &> v(f^{i_0} \wp_F^s), \end{aligned}$$

and this is obviously a contradiction.

To prove (ii) we shall again argue by contradiction, and so assume that $J_p(\mathbb{Q}_p, \Gamma) = \sum_{i=1}^{i=n} \mathbb{Z}_p f^i + (s, t)$, where we now write (s, t) in place of $(s, t)_{\mathbb{Q}_p}$. It follows from this that for each element $h \in \Gamma$ there are elements $c(h) \in \mathbb{Z}_p$, $d(h) \in \mathbb{Z}_p[\Gamma]f^2$ and $e(h) \in (s, t)$ such that $h - 1 = c(h)f + d(h) + e(h)$. Now $\#\Gamma = p^2$ and so there are elements h_1, h_2 of Γ with $h_1 \neq h_2$ and $c(h_1) \equiv c(h_2)$ modulo p . For these elements one has

$$h_1 h_2^{-1} - 1 = h_2^{-1}(h_1 - h_2) = h_2^{-1}((h_1 - 1) - (h_2 - 1)) \in \mathbb{Z}_p[\Gamma]f^2 + (s, t).$$

Since $f \notin (s, t)$ one therefore has

$$\begin{aligned} v\left((h_1 h_2^{-1} - 1) \wp_F^s\right) &\geq \min \left\{ v(f^2 \wp_F^s), t \right\} \\ &> v(f \wp_F^s) \\ &= s + 1 \end{aligned}$$

(where the last equality here is a consequence of (0.3) and the fact that $p \nmid s$). However, since $h_1 h_2^{-1} \in \Gamma_{(1)} \setminus \Gamma_{(2)}$ and $p \nmid s$ this inequality contradicts (0.3). \square

Since $-\kappa < 1 \leq -\kappa + p - 2 + \hat{\epsilon}$ and $(1, 1)_E = \mathcal{O}_E[\Gamma]$ one has an inclusion (cf. (0.2))

$$(-\kappa, -\kappa + p - 2 + \hat{\epsilon})_E + \sum_{i=1}^{i=p-4-\kappa+\hat{\epsilon}} \mathcal{O}_E f^i \subseteq J_p(E, \Gamma). \tag{2.20}$$

Now Lemma 2.12 implies that we may apply Lemma 2.14 with $s = -\kappa, t = -\kappa + p - 2 + \hat{\epsilon}$ and $n = p - 4 - \kappa + \hat{\epsilon}$. From the conclusion of Lemma 2.14(i) we may thus deduce that if condition (2.17) is satisfied, then the inclusion (2.20) must be an equality. However, if $E = \mathbb{Q}_p$, then (since $p \nmid \kappa$) Lemma 2.14(ii) implies that the inclusion (2.20) is strict and so (2.17) cannot be valid in this case.

At this stage we have shown that (2.11) cannot be valid in case (iii) if we have $E = \mathbb{Q}_p$. It therefore remains for us to deal with the cases (i) and (ii), and since the argument in these cases is somewhat similar to the above we shall be a little briefer with our explanations.

We first deal with the case (i). From Lemma 1.1(ii) we know that $(0, 0)_E = \mathcal{O}_E[\Gamma]\{1, pe_\Gamma\}$ and so

$$[(0, 0)_E : \mathcal{O}_E[\Gamma]]_{\mathcal{O}_E} = \wp_E. \tag{2.21}$$

Also $(1, 1)_E = \mathcal{O}_E[\Gamma]$ and $(0, p - 2 + \hat{\epsilon})_E \subseteq (1, 1)_E$ (cf. (0.2)) so that in fact $(0, p - 2 + \hat{\epsilon})_E \subseteq J_p(E, \Gamma)$. The condition (2.12) can therefore be rewritten as

$$[(0, p - 2 + \hat{\epsilon})_E : \mathcal{O}_E[\Gamma]]_{\mathcal{O}_E} = \wp_E^{-p+2-\hat{\epsilon}+1},$$

or equivalently

$$\begin{aligned} [J_p(E, \Gamma) : (0, p - 2 + \hat{\epsilon})_E]_{\mathcal{O}_E} &= \wp_E^{(p-3+\hat{\epsilon})-1} \\ &= \wp_E^{p-4+\hat{\epsilon}}. \end{aligned} \tag{2.22}$$

Lemma 2.16. *One has $f^{p-4+\hat{\epsilon}} \notin (0, p - 2 + \hat{\epsilon})_E = (1, p - 2 + \hat{\epsilon})_E$.*

Proof. The stated equality follows from the inclusion $(1, p - 2 + \hat{\epsilon})_E \subseteq J_p(E, \Gamma)$ together with the fact that $\mathcal{O}_F = \mathcal{O}_K + \wp_F$. By repeatedly using (0.3) one checks that $v\left(f^{p-4+\hat{\epsilon}}\wp_F\right) = 1 + (p - 4 + \hat{\epsilon}) = p - 3 + \hat{\epsilon} < p - 2 + \hat{\epsilon}$, and so $f^{p-4+\hat{\epsilon}} \notin (1, p - 2 + \hat{\epsilon})_E$. □

Lemma 2.16 implies that we can apply Lemma 2.14 with $s = 1, t = p - 2 + \hat{\epsilon}$ and $n = p - 4 + \hat{\epsilon}$. If firstly $p - 4 + \hat{\epsilon} \geq 1$, then Lemma 2.14(i) implies that (2.22) is equivalent to an equality

$$J_p(E, \Gamma) = \sum_{i=1}^{i=p-4+\hat{\epsilon}} \mathcal{O}_E f^i + (1, p - 2 + \hat{\epsilon})_E,$$

and Lemma 2.14(ii) implies that this cannot occur if $E = \mathbb{Q}_p$. If on the other hand $p - 4 + \hat{\epsilon} = 0$ then $p = 3$ and $\hat{\epsilon} = 1$, and then one has $\delta \in \{5, 6\}$ and (2.22) is equivalent to the equality $J_3(E, \Gamma) = (0, 2)_E$. It is not difficult to check that this equality is in fact correct.

We must finally deal with the case (ii). We first recall from Lemma 1.1(i) that $(1, 1)_E = \mathcal{O}_E[\Gamma]$. From this it follows that $(1, p - 1 + \hat{\epsilon})_E \subseteq J_p(E, \Gamma)$ and so the condition (2.13) is therefore equivalent to

$$\begin{aligned} [J_p(E, \Gamma) : (1, p - 1 + \hat{\epsilon})_E]_{\mathcal{O}_E} &= \wp_E^{(p-2+\hat{\epsilon})-1} \\ &= \wp_E^{p-3+\hat{\epsilon}}. \end{aligned} \quad (2.23)$$

Lemma 2.17. *One has $f^{p-3+\hat{\epsilon}} \notin (1, p - 1 + \hat{\epsilon})_E$.*

Proof.: Applying (0.3) gives $v\left(f^{p-3+\hat{\epsilon}}_{\wp_F}\right) = 1 + (p - 3 + \hat{\epsilon}) = p - 2 + \hat{\epsilon} < p - 1 + \hat{\epsilon}$.
□

This result implies that we may apply Lemma 2.14 with $s = 1$, $t = p - 1 + \hat{\epsilon}$ and $n = p - 3 + \hat{\epsilon}$. In conjunction with the conclusion of Lemma 2.14(i) the condition (2.23) is therefore equivalent to an equality

$$J_p(E, \Gamma) = \sum_{i=1}^{i=p-3+\hat{\epsilon}} \mathcal{O}_E f^i + (1, p - 1 + \hat{\epsilon})_E,$$

and Lemma 2.14(ii) implies that this equality cannot occur if $E = \mathbb{Q}_p$.

At this stage we have proved that if $E = \mathbb{Q}_p$, then the equality (2.11) can only occur if $p = 3$ and $\delta \in \{5, 6\}$. Taking into account the result of Lemma 1.7 our proof of Proposition 2.10 will therefore be completed by the following result.

Lemma 2.18. *Let L/K be any extension as in Proposition 2.10 with $p = 3$. Then both $\text{NFr}(\mathbb{Q}_3[G]; \wp_L^5)$ and $\text{NFr}(\mathbb{Q}_3[G]; \wp_L^6)$.*

Proof. Let Q be any subgroup of G of order 3 with $Q \neq G^{(2)}$ and set $\Gamma = G/Q$ and $F = L^Q$. With $\delta \in \{5, 6\}$ the formula (0.5) implies that $v_F(t_Q \wp_L^\delta) = 3$ and so, given the result of Lemma 2.4, we need only prove that $\text{NFr}(\mathbb{Q}_3[\Gamma]; \wp_F^3)$.

Sublemma 2.19. $\text{NFr}(\mathbb{Q}_3[\Gamma]; \wp_F^3)$.

Proof. We let Δ denote the unique subgroup of Γ which has order 3. If $M = F^\Delta$, then $v_M((\wp_F^3)^\Delta) = 1$, whilst (0.5) implies that $v_M(e_\Delta \wp_F^3) = -1$. From this it follows that

$$\mathcal{A}(\mathbb{Q}_3[\Gamma/\Delta]; (\wp_F^3)^\Delta) = \mathcal{A}(\mathbb{Q}_3[\Gamma/\Delta]; \wp_M) = \mathbb{Z}_3[\Gamma/\Delta] \quad (2.25)$$

(where the last equality is a consequence of Lemma 1.1), and also that

$$\mathcal{A}(\mathbb{Q}_3[\Gamma]; \wp_F^3)^\Delta = \mathcal{A}(\mathbb{Q}_3[\Gamma/\Delta]; -1, 1).$$

But one can check that $\mathcal{A}(\mathbb{Q}_3[\Gamma/\Delta]; -1, 1) \subseteq J_3(\mathbb{Q}_3, \Gamma/\Delta)$ whilst

$$e_{\Gamma/\Delta} J_3(\mathbb{Q}_3, \Gamma/\Delta) \subseteq \mathbb{Z}_3 \cdot t_{\Gamma/\Delta} \subset \mathcal{A}(\mathbb{Q}_3[\Gamma/\Delta]; -1, 1)$$

so that $e_{\Gamma/\Delta} \in \mathcal{A}(\mathbb{Q}_3[\Gamma/\Delta]; \mathcal{A}(\mathbb{Q}_3[\Gamma]; \wp_F^3)^\Delta)$. In conjunction with (2.25) this implies that $\text{NFr}(\mathbb{Q}_3[\Gamma]; \wp_F^3)$. \square

This completes the proof of Proposition 2.10, and hence that of Theorem 1.3(i). \square

§ 3. The cyclic case

In this section p is an odd prime, L/K is a totally ramified cyclic extension of p -adic fields of degree $p^n r$ with $n \geq 1$ and $p \nmid r$, and E is any absolutely unramified subfield of K . We write G for the Galois group of L/K , and let P and C denote its subgroups of order p^n and r respectively. For each integer i with $1 \leq i \leq n$ we let P_i denote the subgroup of P of order p^i , and we write t_i and e_i for t_{P_i} and e_{P_i} respectively. We set $e_0 := 1 \in G$. We write e_K for the absolute ramification degree of K and set $\hat{e}_K := e_K/(p-1)$.

In this section we shall *inter alia* prove Theorem 1.3(ii-iii). A brief outline of the section is as follows. We first characterise the condition $\text{Fr}(E[G]; \mathcal{I}_L)$ in the case that $G = P$ by combining results of Fontaine concerning ramification filtrations with Lemma 1.1, Proposition 1.11, Lemma 2.4 and some explicit computations based on (0.3-5). Using similar techniques we then characterise $\text{Fr}(E[G]; \mathcal{I}_L)$ in the case that $n = 1$ and $e_K > 1$ and combine this with Lemma 2.4 so as to prove Theorem 1.3(ii)(a) and (iii)(a). To prove Theorem 1.3(ii)(b) and (iii)(b) we use the approach of [Bu2]. Via this approach the proof is reduced to giving an explicit description of each order $\mathcal{A}(K[G]; I)$, and to obtain such descriptions we refine the techniques of [Be1].

We first recall the close connection between \hat{e}_K and the upper jump numbers $u^{(j)}$ of L/K .

Lemma 3.1. (Fontaine [Fo]):

- (i) One has either $u^{(1)} = p\hat{e}_K$ or $0 < u^{(1)} < p\hat{e}_K$ and $p \nmid u^{(1)}$.
- (ii) For each $j \in \{1, 2, \dots, n-1\}$ one has
 - (a) if $u^{(j)} \geq \hat{e}_K$, then $u^{(j+1)} = u^{(j)} + e_K$.
 - (b) if $u^{(j)} < \hat{e}_K$, then either $u^{(j+1)} = pu^{(j)}$, or $u^{(j+1)} = p\hat{e}_K$, or $pu^{(j)} < u^{(j+1)} < p\hat{e}_K$ and $p \nmid u^{(j+1)}$. \square

Lemma 3.1(i) allows us to define a non-negative integer δ by setting

$$\delta := pe_K - (p-1)u^{(1)}.$$

We recall that L/K is said to be ‘almost maximally ramified’ if $\delta r < p$. If $e_K = 1$ and $r = 1$, then this is in fact no restriction on L/K . Indeed, in this case Lemma 3.1(i) implies that $u^{(1)} = 1$ so that $\delta = 1$.

Lemma 3.2. *The following conditions are equivalent :-*

- (i) $\mathcal{A}(E[G]; \mathcal{O}_L) = \mathcal{M}(E, G)$.
- (ii) $\mathcal{A}(E[G/Q]; \mathcal{O}_{L^Q}) = \mathcal{M}(E, G/Q)$ for any given subgroup $Q < P$.
- (iii) L/K is almost maximally ramified.

Proof. The implication from (i) to (ii) is clear.

We next assume that (ii) is true with respect to some given subgroup Q of P . If now $H \leq G$ with $\#H = p^{n-1}r$, then $Q \leq H$ and so $\mathcal{A}(E[G/H]; \mathcal{O}_{L^H}) = \mathcal{M}(E, G/H)$. Since the unique jump number of L^H/K is equal to $u^{(1)}$ the formula (0.5) implies that $e_{G/H}\mathcal{O}_{L^H} \subseteq \mathcal{O}_{L^H}$ if and only if $\delta < p$. Now if $\delta < p$, then $u^{(1)} \geq \hat{e}_K$ and hence Lemma 3.1(ii)(a) implies that $u^{(i)} = u^{(1)} + (i-1)e_K$ for each integer $i \in \{2, \dots, n\}$. Upon converting to the lower ramification numbering and using (0.5) one now computes that for each integer j with $1 \leq j \leq n$

$$v_L(e_j \mathcal{O}_L) = p^j \left[\frac{p^j - 1 - \delta r \left(\frac{p^j - 1}{p-1} \right)}{p^j} \right].$$

It is clear from this expression that any idempotent e_j belongs to $\mathcal{A}(E[G]; \mathcal{O}_L)$ if and only if $\delta r < p$. This proves the implications from (ii) to (iii) and from (iii) to (i). \square

In proving Theorem 1.3(ii-iii) we shall first deal with extensions of p -power degree.

Lemma 3.3. *Let L/K be a cyclic extension of degree p . Then $\text{Fr}(E[G]; \mathcal{I}_L)$ if and only if L/K is either weakly or almost maximally ramified.*

Proof. We must prove that if $\text{Fr}(E[G]; \mathcal{I}_L)$, then either $u^{(1)} = 1$ or $\delta < p$.

In this case $u^{(1)} = u_{(1)}$ and so the formula (0.5) gives

$$v_K(e_1 \wp_L^i) = \left[\frac{i + (1 + u_{(1)})(p-1)}{p} \right] - e_K = \left[\frac{i + p - 1 - \delta}{p} \right]. \quad (3.1)$$

If $\delta \geq p$, then this is strictly less than $\lceil i/p \rceil$ and so $\mathcal{A}(E[G]; \wp_L^i) = \mathcal{O}_E[G]$ for all integers i . In this case therefore it follows from Lemma 1.1(i) that $\text{Fr}(E[G]; \mathcal{I}_L)$ if and only if L/K is weakly ramified.

If on the other hand $\delta < p$, then (3.1) implies that $v_K(e_1\mathcal{O}_L) = 0$ so that $\mathcal{A}(E[G]; \mathcal{O}_L) = \mathcal{M}(E, G)$ and hence certainly $\text{Fr}(E[G]; \mathcal{O}_L)$. \square

Lemma 3.4. *Let L/K be a cyclic extension of degree p^n with $n > 1$. Then $\text{Fr}(E[G]; \mathcal{I}_L)$ if and only if L/K is almost maximally ramified.*

Proof. Since $u^{(1)}$ is equal to the first (upper) jump number in any non-trivial subextension F/K of L/K we deduce from Lemma 2.4 and Lemma 3.3 that if $\text{Fr}(E[G]; \mathcal{I}_L)$, then either $u^{(1)} = 1$ or $u^{(1)} = (pe_K - \delta)/(p - 1)$ with $\delta < p$. If $\delta < p$, then L/K is almost maximally ramified and $\text{Fr}(E[G]; \mathcal{O}_L)$ (Lemma 3.2), and so we shall henceforth assume that $u^{(1)} = 1$. In addition, if $e_K = 1$, then L/K is necessarily almost maximally ramified, and so we shall also henceforth assume that $e_K > 1$. It suffices for us to prove that, under these assumptions, if $n = 2$, then $\text{NFr}(E[G]; \mathcal{I}_L)$. To do this we now restrict to the case $n = 2$, and we set $\Gamma := G/P_1$. We shall use the following result.

Sublemma 3.5. *Let G be cyclic of order p^2 . We choose an element $g \in G \setminus P_1$ and set $f := g - 1$. If \mathcal{A} is any order of the form $\mathcal{A}(E[G]; I)$ which contains neither fe_1 or e_2 , then either $\mathcal{A} = \mathcal{O}_E[G]$ or $\mathcal{A}(E[\Gamma]; \mathcal{A}^{P_1}) = \mathcal{M}(E, \Gamma)$. In particular, if $e_K > 1$ and $u^{(1)} = 1$, then $\text{NFr}(E[G]; I)$.*

Proof. If

$$\alpha = c_0e_1 + \sum_{i=1}^{i=p-2} c_i f^i e_1 + ce_2 \in \mathcal{A} \tag{3.2}$$

(with c, c_0 and each c_i belonging to \mathcal{O}_E), then

$$f\alpha = c_0 f e_1 + \sum_{i=1}^{i=p-2} c_i f^{i+1} e_1 \in \mathcal{A}$$

and hence (0.4) implies that $c_0 f e_1 \in \mathcal{A}$. Since $f e_1 \notin \mathcal{A}$ it follows that $c_0 \in \wp_E$ and hence that the element

$$\beta := \alpha - c_0 e_1 = \sum_{i=1}^{i=p-2} c_i f^i e_1 + ce_2$$

belongs to \mathcal{A} . It follows that $\beta^{p^2} \in \mathcal{A}$ and since

$$\beta^{p^2} \equiv c^{p^2} e_G \text{ modulo } \mathcal{O}_E[G]$$

we deduce that $c^{p^2} e_2$ belongs to \mathcal{A} , and hence (since $e_2 \notin \mathcal{A}$) that there exists an integer $c' \in \mathcal{O}_E$ such that $c = pc'$. Since $ce_2 \equiv c' f^{p-1} e_1$ modulo $\mathcal{O}_E[G]$, we may now deduce from (0.4) and the above explicit expression for β that

$$\{c_i f^i e_1 : 1 \leq i \leq p - 2\} \cup \{ce_2\} \subset \mathcal{A}. \tag{3.3}$$

There are now two cases for us to consider.

Case (i) $pe_2 \notin \mathcal{A}$. To within addition of an element of $\mathcal{O}_E[G]$ each element of $\mathcal{M}(E, G)$ is of the form (3.2). It follows that if $pe_2 \notin \mathcal{A}$, then (3.3) implies that $c_i \in \wp_E$ for each $i \in \{1, 2, \dots, p-2\}$ and also $c \in \wp_E^2$, and hence that $\alpha \in \mathcal{O}_E[G]$. In other words, in this case we have $\mathcal{A} = \mathcal{O}_E[G]$ and so since L/K is not weakly ramified it follows that $\text{NFr}(E[G]; I)$.

Case (ii) $pe_2 \in \mathcal{A}$. Any element of \mathcal{A}^{P_1} is of the form (3.2). However, since both c_0 and c belong to \wp_E one has $e_2\alpha = (c_0 + c)e_2 \in \mathcal{A}$ so that $e_\Gamma \in \mathcal{A}(E[\Gamma]; \mathcal{A}^{P_1})$ and hence $\mathcal{A}(E[\Gamma]; \mathcal{A}^{P_1}) = \mathcal{M}(E, \Gamma)$. If $e_K > 1$ and $u^{(1)} = 1$, then this implies $\text{NFr}(E[G]; I)$. Indeed, if $\text{Fr}(E[G]; I)$, then $\mathcal{A}(E[\Gamma]; I^{P_1}) = \mathcal{A}(E[\Gamma]; \mathcal{A}^{P_1}) = \mathcal{M}(E, \Gamma)$ and this contradicts Proposition 1.11(i). \square

Returning to the proof of Lemma 3.4 we now fix an integer i and shall show that $\text{NFr}(E[G]; \wp_L^i)$ if $u^{(1)} = 1$ and $e_K > 1$. To do this we set $F = L^{P_1}$, and first note that since F/K is weakly ramified Proposition 1.11(i) implies that $\mathcal{A}(E[\Gamma]; I) = \mathcal{O}_E[\Gamma]$ for each ideal $I \in \mathcal{I}_F$. Lemma 2.4 and Lemma 1.1 therefore imply that

$$\text{Fr}(E[G]; \wp_L^i) \Rightarrow \text{Fr}(E[\Gamma]; t_1 \wp_L^i) \Rightarrow v_F(t_1 \wp_L^i) \equiv 1 \pmod{p}. \quad (3.4)$$

We set $\mathcal{A} := \mathcal{A}(E[G]; \wp_L^i)$. In completing the proof of Lemma 3.4 there are two cases for us to consider.

Case (i) $1 = u^{(1)} < \hat{e}_K$. In this case Lemma 3.1(ii)(b) implies that $u^{(2)} = (pe_K - \eta)/(p-1)$ for some non-negative integer η . Converting to lower numbering gives $u_{(1)} = 1$ and $u_{(2)} = 1 + p((pe_K - \eta)/(p-1) - 1)$. The formula (0.5) now shows that $e_2 \notin \mathcal{A}$. In addition, as a consequence of (3.4), (0.3) and (0.5) one has

$$\begin{aligned} v_F(fe_1 \wp_L^i) &= v_F(e_1 \wp_L^i) + 1 \\ &= \left[\frac{i + (1 + u_{(2)})(p-1)}{p} \right] - e_K p + 1 \\ &= \left[\frac{i + (2(p-1) + p(pe_K - \eta - (p-1)))}{p} \right] - e_K p + 1 \\ &= \left[\frac{i + p - 2}{p} \right] - \eta - (p-3). \end{aligned}$$

Unless $p = 3$ and $\eta = 0$ (and $i \not\equiv 1 \pmod{3}$) this last expression is strictly less than $[i/p]$ so that $fe_1 \notin \mathcal{A}$, and hence $\text{NFr}(E[G]; \wp_L^i)$ as a consequence of Sublemma 3.5. In the special case $p = 3$ and $\eta = 0$ one can show that

$$\wp_E e_2 \subset \mathcal{A} \subseteq \mathcal{O}_E[G] \{1, fe_1, e_1 - e_2\}$$

so that $\mathcal{A}(E[\Gamma]; \mathcal{A}^{P_1}) = \mathcal{M}(E, \Gamma)$. However since $e_K > 1$ and F/K is weakly ramified Proposition 1.11(i) implies that $\mathcal{A}(E[\Gamma]; (\wp_L^i)^{P_1}) = \mathcal{O}_E[\Gamma]$ and hence $\text{NFr}(E[G]; \wp_L^i)$.

Case (ii) $1 = u^{(1)} \geq \hat{e}_K$. In this case Lemma 3.1(ii)(a) implies that $u^{(2)} = 1 + e_K$. After converting to lower numbering this implies (via (0.5)) that $e_2 \notin \mathcal{A}$ and (taking into account (3.4), (0.3) and (0.5)) also that

$$\begin{aligned} v_F(fe_1\wp_L^i) &= v_F(e_1\wp_L^i) + 1 \\ &= \left\lfloor \frac{i + (2 + pe_K)(p - 1)}{p} \right\rfloor - e_Kp + 1 \\ &= \left\lfloor \frac{i + p - 2}{p} \right\rfloor + 2 - e_K. \end{aligned}$$

If $e_K > 2$ it follows that $fe_1 \notin \mathcal{A}$ and the required result follows by applying Sublemma 3.5. If however $e_K = 2$, then it is possible that $fe_1 \in \mathcal{A}$. But in this case it is easy to check that pe_2 also belongs to \mathcal{A} so that

$$\wp_E e_2 \subset \mathcal{A} \subseteq \mathcal{O}_E[G]\{1, fe_1, e_1 - e_2\}$$

and hence that $e_\Gamma \in \mathcal{A}(E[\Gamma]; \mathcal{A}^{P_1})$. This again implies that $\text{NFr}(E[G]; \wp_L^i)$. \square

At this stage, we can turn to consider extensions of mixed degree.

Lemma 3.6. *Let G be a cyclic group of order pr . If $e_K \geq 2$, then $\text{Fr}(E[G]; \mathcal{I}_L)$ if and only if L/K is either weakly ramified or almost maximally ramified.*

Proof. We need only show that if L/K is neither weakly or almost maximally ramified, then $\text{NFr}(E[G]; \mathcal{I}_L)$. As a consequence of Lemma 1.7 it is in fact enough for us to show that in this case $\text{NFr}(K_0[G]; \mathcal{I}_L)$ where here K_0 denotes the maximal absolutely unramified subfield of K . Now since L/K is totally ramified it follows that K_0 contains a primitive r th root of unity, so that the algebra $K_0[C]$ is totally split. From the decomposition $I = \bigoplus_{\chi \in C^*} e_\chi I$ it is therefore enough for us to prove that for each ideal I there is at least one character $\chi \in C^*$ which is such that $e_\chi I$ is not free as an $\mathcal{A}(K_0[G]e_\chi; I)$ -module.

As a consequence of Lemma 2.4 and Lemma 3.3 we may henceforth assume that either $u^{(1)} = 1$ or $u^{(1)} = (pe_K - \delta)/(p - 1)$ with $0 \leq \delta < p$. We let π denote a uniformising parameter of K , and write F for the field L^P . From (0.5) we obtain in this case

$$\begin{aligned} v_F(\pi^{-j}t_1\wp_L^i) &= \left\lfloor \frac{i + (1 + ru^{(1)})(p - 1)}{p} \right\rfloor - jr \\ &= \begin{cases} \left\lfloor \frac{i + p - 1 + r(p - 1 - pj)}{p} \right\rfloor, & \text{if } u^{(1)} = 1, \\ \left\lfloor \frac{i + p - 1 + r(pe_K - j - \delta)}{p} \right\rfloor, & \text{if } u^{(1)} = (pe_K - \delta)/(p - 1), 0 \leq \delta < p. \end{cases} \end{aligned} \tag{3.5}$$

We set $I := \wp_L^i$. If $u^{(1)} = 1$, then by substituting $j = e_K$ into (3.5) one can show that $\mathcal{A}(K_0[G]; I) = \mathcal{O}_{K_0}[G]$, and hence Lemma 1.1 implies that $\text{NFr}(K_0[G]; \mathcal{I}_L)$ unless L/K is weakly ramified.

Henceforth we assume that $\delta \leq p-1$, and that $\delta r = p + \xi$ for some positive integer ξ , and we shall prove that $\text{NFr}(K_0[G]e_\chi; I)$ for some character χ . By substituting $j = e_K$ into (3.5) we obtain

$$v_F(e_1 I) = \left\lceil \frac{i+p-1-\xi}{p} \right\rceil - 1 \leq \left\lceil \frac{i}{p} \right\rceil - 1,$$

and so there is at least one character $\chi \in C^*$ such that $e_1 e_\chi \notin \mathcal{A}(K_0[G]e_\chi; I)$. For any such character χ one has $\mathcal{A}(K_0[G]e_\chi; I) = \mathcal{O}_{K_0}[G]e_\chi$ and hence if $\text{Fr}(K_0[G]; I)$, then $e_\chi I$ is a free $\mathcal{O}_{K_0}[G]e_\chi$ -module. If this is true, then $\hat{H}^0(P, e_\chi I) = \hat{H}^0(P, \mathcal{O}_{K_0}[G]e_\chi) = 0$ and so

$$(e_\chi I)^P = t_1 e_\chi I. \quad (3.6)$$

However, substituting $j = 1$ into the expression (3.5) one has

$$v_F(\pi^{-1} t_1 I) = \left\lceil \frac{i+p-1+r(p(e_K-1)-\delta)}{p} \right\rceil$$

and since $e_K \geq 2$ and $\delta \leq p-1$ this is at least $\lceil i/p \rceil$. In other words, one has $\pi^{-1} t_1 I \subseteq I$ so that $\pi^{-1} t_1 e_\chi I \subseteq (e_\chi I)^P$ and this contradicts the equality (3.6). \square

By combining the results of Lemmas 3.4 and 3.6 with Lemma 2.4 one obtains proofs of Theorem 1.3(ii)(a) and (iii)(a), and so it only remains for us to consider more fully the case that $e_K = 1$.

The important point in this case is that (in conjunction with Lemma 1.7) the techniques of [Bu2] reduce the question of whether $\text{Fr}(E[G]; I)$ to the problem of obtaining an explicit description of each order $\mathcal{A}(K[G]; I)$.

Since $K[C]$ is totally split, the direct sum decomposition $I = \bigoplus_{\chi \in C^*} e_\chi I$ induces a decomposition

$$\mathcal{A}(K[G]; I) = \bigoplus_{\chi \in C^*} \mathcal{A}(K[G]e_\chi; I),$$

and so it suffices to describe each order $\mathcal{A}(K[G]e_\chi; I)$. To do this we choose any generator g of P , and set $f := g-1$. We recall first that for each character $\chi \in C^*$ one has

$$\mathcal{M}(K, G)e_\chi = \sum_{i=0}^{i=n} \sum_{j \geq 0} \mathcal{O}_K f^j e_i e_\chi \quad (3.7)$$

(cf. for example ([Be1], §2.2, Lemme 2)). The case $I = \mathcal{O}_L$ of the following result is equivalent to ([Be1], Théorème 1).

Lemma 3.7. *Let $e_K = 1$. Then for each ideal I of \mathcal{O}_L and for each character $\chi \in C^*$ the order $\mathcal{A}(K[G]e_\chi; I)$ is generated over $\mathcal{O}_K[G]e_\chi$ by a set of the form*

$$\{1\} \cup \{f e_i : 1 \leq i \leq n-1\} \cup \{c_i e_i : 1 \leq i \leq n\}$$

where $c_i \in \{1, p\}$ for each index i .

Remark 3.8. Using (0.5) and (0.6) it is easy to determine whether any given element $e_i e_\chi$ belongs to $\mathcal{A}(K[G]e_\chi; I)$.

Proof. Lemma 3.1 implies that $u^{(j)} = j$ for each integer j with $1 \leq j \leq n$. Using (3.7), (0.3) and (0.5) one can now check that

$$f\mathcal{M}(K, G)e_\chi + p\mathcal{M}(K, G)e_\chi \subseteq \mathcal{A}(K[G]e_\chi; I)$$

(cf. [Bu2], proof of Lemma 5.6), and so, given the description (3.7), we need only consider elements of the form $\sum_{i=1}^{i=n} c_i e_i e_\chi$ with $c_i \in \mathcal{O}_K^*$ for each integer i .

We now fix I and χ and let \mathcal{A} denote the order $\mathcal{A}(K[G]e_\chi; I)$. We suppose we are given s integers

$$i(1) < i(2) < \dots < i(s)$$

which are such that $e_{i(k)} e_\chi \notin \mathcal{A}$ for each $k \in \{1, 2, \dots, s\}$. We must show that for any subset $\{c_{i(k)} : 1 \leq k \leq s\}$ of \mathcal{O}_K^* the element $\alpha := \sum_{k=1}^{k=s} c_{i(k)} e_{i(k)} e_\chi$ does not belong to \mathcal{A} . We shall argue by contradiction, and so shall assume that $\alpha \in \mathcal{A}$.

We set $J := \{i(k) : 1 \leq k \leq s\}$ and let M denote the minimum element of the set $\{v_L(e_j e_\chi I) : j \in J\}$, so that $M < v_L(I)$. We also set $J' := \{j \in J \mid v_L(e_j e_\chi I) = M\}$ and $s' := \#J'$. Note that since $M < v_L(I)$ and $\alpha \in \mathcal{A}$ one has $s' \geq 2$.

We now relabel the elements of J' as $i'(1) < i'(2) < \dots < i'(s')$, so that in particular M is divisible by $p^{i'(s')}$. In addition, for each integer k with $1 \leq k \leq s'$ we shall in the remainder of this proof write M_k for $p^{-i'(k)} M$, G_k for $P_{i'(k)}$, Q_k for G/G_k , L_k for L^{G_k} , $v_k(-)$ for $v_{L_k}(-)$, e_k for $e_{i'(k)}$, and c_k for $c_{i'(k)}$.

We let β denote the element $\sum_{k=1}^{k=s'} c_k e_k e_\chi$, and write β_1 for the image of β in $K[Q_1]$. Since $\alpha \in \mathcal{A}$ we must have $v_L(\beta I) > M$ and so $v_1(\beta_1 e_1 I) > M_1$, or equivalently (taking into account (0.6))

$$\beta_1 \in \mathcal{A}(K[Q_1]e_\chi; M_1, M_1 + r). \tag{3.8}$$

We now choose any element x of $L_{s'-1}$ such that $v_{s'-1}(x) \geq M_{s'-1} + r$. Then one has

$$\beta_1 x = \sum_{k=1}^{k=s'-1} c_k e_\chi(x) + c_{s'} e_{s'} e_\chi(x). \tag{3.9}$$

It is clear that

$$v_1 \left(\sum_{k=1}^{k=s'-1} c_k e_\chi(x) \right) \geq v_1(x) = p^{i'(s'-1)-i'(1)} v_{s'-1}(x) > M_1. \tag{3.10}$$

On the other hand, writing $\wp_{s'-1}$ for the maximal ideal of $\mathcal{O}_{L_{s'-1}}$, the formula (0.5) (together with our knowledge of the ramification filtration of $L_{s'-1}/L_{s'}$) implies that

$$\begin{aligned} & v_{s'} \left(e_{s'} \wp_{s'-1}^{M_{s'-1}+r} \right) \\ &= \left[\frac{1}{p^{i'(s')-i'(s'-1)}} \left((M_{s'-1} + r) - r \left(\frac{p^{i'(s')-i'(s'-1)} - 1}{p-1} \right) + p^{i'(s')-i'(s'-1)} - 1 \right) \right] \\ &= M_{s'} + \left[\frac{1}{p^{i'(s')-i'(s'-1)}} \left(r - r \left(\frac{p^{i'(s')-i'(s'-1)} - 1}{p-1} \right) + p^{i'(s')-i'(s'-1)} - 1 \right) \right] \end{aligned}$$

so that

$$M_{s'} - r < v_{s'} \left(e_{s'} \wp_{s'-1}^{M_{s'-1}+r} \right) \leq M_{s'}.$$

In conjunction with these inequalities the property (0.6) implies that $v_{s'} \left(e_{s'} e_{\chi} \wp_{s'-1}^{M_{s'-1}+r} \right) = M_{s'}$, and so we may assume that our chosen element x satisfies $v_1(e_{s'} e_{\chi} x) = M_1$. But for any such element we may deduce from (3.9-10) and $c_{s'} \in \mathcal{O}_K^*$ that $v_1(\beta_1 x) = M_1 < M_1 + r$, and this in turn contradicts the inclusion (3.8). \square

Lemma 3.7 has reduced the problems of explicitly describing the order $\mathcal{A}(K[G]; I)$ and then of checking whether $\text{Fr}(K[G]; I)$ to straightforward computational matters. (It incidentally can also be used to give a much quicker proof of ([Bu2], Theorem 6) than the one originally given in ([Bu2], §5)).

Theorem 1.3(ii)(b) is a consequence of Theorem 1.3(iii)(b) and Lemma 2.4, and so to complete the proof of Theorem 1.3 we need only prove Theorem 1.3(iii)(b). We thus now suppose that L/K has degree pr and that $e_K = 1$. In this case it is easy to check that all \mathcal{O}_K -orders in $K[G]$ which contain $\mathcal{O}_K[G]$ are Gorenstein (or ‘self-dual’ in the language of ([Fr2], Theorem 10)) and so one has $\text{Fr}(K[G]; I)$ for all ideals I of \mathcal{O}_L . From Lemma 1.7 it follows that

$$\text{Fr}(\mathbb{Q}_p[G]; I) \Leftrightarrow \mathcal{A}(K[G]; I) = \mathcal{A}(\mathbb{Q}_p[G]; I)\mathcal{O}_K.$$

Our proof of Theorem 1.3(iii)(b) is thus completed by the following result.

Lemma 3.9. *Suppose that $\#G = pr$ and that $e_K = 1$. Then there exists an ideal I of \mathcal{O}_L for which $\mathcal{A}(K[G]; I) = \mathcal{A}(\mathbb{Q}_p[G]; I)\mathcal{O}_K$ if and only if $r < 2p$.*

Proof. Let $I = \wp_L^i$. Since $u^{(1)} = 1$ the formula (0.5) gives

$$v_1(e_1 I) = \left[\frac{i + (1+r)(p-1)}{p} \right] - r$$

$$= \left\lceil \frac{i + p - 1 - r}{p} \right\rceil, \tag{3.11}$$

and hence

$$\lceil i/p \rceil - \lceil r/p \rceil - 1 \leq v_1(e_1 I) \leq \lceil i/p \rceil - \lceil r/p \rceil. \tag{3.12}$$

The generator $\chi(L/K)$ of C^* (cf. (0.6)) induces a bijection between C^* and any complete set J of residues modulo r : each $\chi \in C^*$ corresponds to the integer $j(\chi) \in J$ such that $\chi = \chi(L/K)^{j(\chi)}$. If F is the absolute Frobenius of p , then

$$j(\chi^F) \equiv pj(\chi) \pmod{r}. \tag{3.13}$$

Moreover, if $J'(i)$ denotes the subset of J consisting of those integers $j(\chi)$ for which $e_\chi e_1 \notin \mathcal{A}(K[G]; I)$, then (0.6) implies that we may choose J in such a way that both J and $J'(i)$ is a set of consecutive integers. We shall henceforth suppose that J is chosen in this way. We note that the inequalities (3.12) imply $\lceil r/p \rceil + 1 \geq \#J'(i) \geq \lceil r/p \rceil$.

Now if $\mathcal{A}(K[G]; I) = \mathcal{A}(\mathbb{Q}_p[G]; I)\mathcal{O}_K$, then (3.13) implies that $J'(i)$ must be stable (at least modulo r) under multiplication by p . The fact that $\mathcal{A}(K[G]; I) \neq \mathcal{A}(\mathbb{Q}_p[G]; I)\mathcal{O}_K$ if $r > 2p$ is thus a consequence of the following sublemma.

Sublemma 3.10. *If $r > 2p$, then for any integer i there exists an integer $j \in J'(i)$ such that pj is not congruent modulo r to any element of $J'(i)$.*

Proof. We write J' for $J'(i)$. We shall argue by contradiction and so assume that multiplication by p induces a bijection of J' (with its elements considered as residue classes modulo r). We let j_1 and j_2 denote the least and greatest elements of J' respectively. There are two cases for us to consider.

Case (i) $j_2 - j_1 \geq p - 1$. In this case we know that for some $s \in \{1, 2\}$ there is an integer $\lambda \in J'$ such that $p\lambda \equiv j_2 - (p - s)$ modulo r and $\lambda + 1 \in J'$. One therefore has

$$p(\lambda + 1) \equiv j_2 - (p - s) + p \equiv j_2 + s \pmod{r},$$

and since by assumption this is congruent modulo r to an element of J' we must have $j_2 + s \geq j_1 + r$. However, this inequality implies that

$$r/p + 1 \geq \lceil r/p \rceil + 1 \geq \#J' = j_2 - j_1 + 1 \geq r - s + 1 \geq r - 1,$$

and this certainly cannot happen if $r > 2p$.

Case (ii) $j_2 - j_1 < p - 1$. Since $\#J' \geq \lceil r/p \rceil$ and $r > 2p$ one has $\#J' \geq 2$. For some $s \in \{0, 1\}$ there is therefore an integer $\lambda \in J'$ such that $p\lambda \equiv j_1 + s$ modulo r and $\lambda + 1 \in J'$. Then we have $p(\lambda + 1) \equiv j_1 + s + p$ modulo r . Since however

$$j_2 < j_1 + p - 1 < j_1 + p + s < j_1 + r$$

this implies that $p(\lambda + 1)$ is not congruent modulo r to any element of J' , and this is a contradiction. \square

At this stage it suffices for us to show that if $r < 2p$, then there exists an ideal I of \mathcal{O}_L such that $\mathcal{A}(K[G]; I) = \mathcal{A}(\mathbb{Q}_p[G]; I)\mathcal{O}_K$. Now if $r < p$, then

$$\mathcal{A}(K[G]; \mathcal{O}_L) = \mathcal{M}(K, G) = \mathcal{M}(\mathbb{Q}_p, G)\mathcal{O}_K,$$

and so we shall assume that $r = p + \xi$ with $1 \leq \xi \leq p - 1$. From (3.11) one has

$$v_1(e_1 \rho_L^i) = \left\lfloor \frac{i + p - 1 - \xi}{p} \right\rfloor - 1. \quad (3.14)$$

We write $i + p - 1 = sp + t$ with s and t integers such that $0 \leq t < p - 1$. If $t \geq \xi$, then the expression (3.14) is equal to $\lceil i/p \rceil - 1 = s - 1$, and so the subset $J'(i)$ is the singleton consisting of the unique integer $j' \in J$ such that $j' \equiv s - 1$ modulo r . Regarding j' as a residue class modulo r it is invariant under multiplication by p if and only if the integer s satisfies $p(s - 1) \equiv s - 1$ modulo r . Choosing s and t to satisfy the above stated conditions it follows that

$$\mathcal{A}(K[G]e_\chi; I) = \begin{cases} \mathcal{M}(K, G)e_\chi, & \text{if } j(\chi) \neq j', \\ \mathcal{O}_K[G]e_\chi, & \text{if } j(\chi) = j'. \end{cases} \quad (3.15)$$

We reiterate that, since $j(\chi) = j'$ implies that χ is \mathbb{Q}_p -valued, the order $\mathcal{A}(K[G]; I)$ which is described by (3.15) is indeed induced from a \mathbb{Z}_p -order. \square

We have now completed the proof of all parts of Theorem 1.3. It therefore only remains for us to complete the proof of Corollary 1.4 by showing that if $e_K = 1$, then $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$ implies that L/K is almost maximally ramified.

Lemma 3.11. (Bergé): *Suppose that $e_K = 1$, and that L/K is cyclic. Then $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$ implies that L/K is almost maximally ramified.*

Proof. If $\text{Fr}(\mathbb{Q}_p[G]; \mathcal{O}_L)$, then Lemma 1.7 implies that $\mathcal{A}(K[G]; \mathcal{O}_L) = \mathcal{A}(\mathbb{Q}_p[G]; \mathcal{O}_L)\mathcal{O}_K$, and this condition can be investigated by using the same techniques as in the proof of Lemma 3.9. Just such an analysis is made in ([Be1], §2.3, Corollaire 4 and Lemme 5) and shows that $\mathcal{A}(K[G]; \mathcal{O}_L) = \mathcal{A}(\mathbb{Q}_p[G]; \mathcal{O}_L)\mathcal{O}_K$ if and only if L/K is almost maximally ramified. \square

Appendix: An algorithmic approach to determining local and global module structures (W. Bley)

In this appendix we let L/K denote an abelian extension of number fields with Galois group G . We let E be a subfield of K with class number one, and we

shall consider G -stable ideals I of \mathcal{O}_L which are locally free over $\mathcal{A}(E[G]; I)$. Our aim is to algorithmically determine their class in the locally free class group of $\mathcal{A}(E[G]; I)$.

We recall that if $\mathcal{A}(E[G]; I)$ is explicitly known, then the question of local freeness of I over $\mathcal{A}(E[G]; I)$ is reduced to an index-theoretical computation using ([Fr2], Theorem 4) (see also Lemma 2.7 in [Bl]). Algorithms for computing associated orders of unit lattices and for deciding if these lattices are locally or globally free over their associated orders are already given in [Bl]. These algorithms can be easily adapted to the rank one case of the present problem (that is, the case $E = K$), and so we shall focus on the problems which arise when $E \neq K$.

In the following we write $n = [L : K]$ and $m = [K : E]$. By the normal basis theorem we know that there exist elements $\theta_1, \dots, \theta_m$ of I such that $L = \bigoplus_{i=1}^m E[G]\theta_i$. We first describe an algorithm for explicitly computing such a set $\{\theta_1, \dots, \theta_m\}$. This is a generalization of a procedure introduced by K. Girstmair in [G].

The simple Wedderburn components of $E[G]$ are parametrized by the set $D(G)$ of irreducible E -characters of G . For each $\rho \in D(G)$ we write e_ρ for the corresponding idempotent $\frac{1}{n} \sum_{g \in G} \rho(g)g^{-1}$ of $E[G]$.

ALGORITHM

Given a basis $\omega_1, \dots, \omega_{nm}$ of L over E and matrices $A(g) \in Gl_{nm}(E)$ for each $g \in G$ such that

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_{nm} \end{pmatrix}^g = A(g) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_{nm} \end{pmatrix},$$

this algorithm computes normal basis generators $\theta_1, \dots, \theta_m$ of L over $E[G]$.

STEP 1: Set $j = 1$, $W = \{\omega_1, \dots, \omega_{nm}\}$, $V = \{\}$ and let A be the identity matrix of size nm .

STEP 2: For each $\rho \in D(G)$ choose $\omega_\rho^{(j)} \in W$ such that $e_\rho(\omega_\rho^{(j)}) \notin \text{span}_E(V)$ and put $\theta_j = \sum_{\rho \in D(G)} e_\rho(\omega_\rho^{(j)})$.

STEP 3: Compute the E -basis $T = \{\theta_j^g : g \in G\}$ of $E[G]\theta_j$ and a subset W' of W such that $L = \text{span}_E(V) \oplus \text{span}_E(T) \oplus \text{span}_E(W')$. Also compute a matrix B that transforms our new basis $V \cup T \cup W'$ to the old basis $V \cup W$. Set $j \leftarrow j + 1$, $W \leftarrow W'$, $V \leftarrow V \cup T$ and $A \leftarrow AB$.

STEP 4: If $j \leq m$ go to step 2. Otherwise output $\theta_1, \dots, \theta_m$.

In order to prove the correctness of this algorithm we proceed by induction on j . We suppose then that for some $j \leq m$ we have both

(i) $\dim_E(\text{span}_E(V)) = (j - 1)n$,

and

(ii) $\text{span}_E(V) \oplus \text{span}_E(W) = L$.

We note first that $\text{span}_E(V) = \bigoplus_{k=1}^{j-1} E[G]\theta_k$. Because of (ii) we find for each $\rho \in D(G)$ an element $\omega_\rho^{(j)} \in W$ such that $e_\rho(\omega_\rho^{(j)}) \notin \text{span}_E(V)$. In particular $e_\rho(\theta_j) = e_\rho(\omega_\rho^{(j)}) \neq 0$ and this implies $e_\chi(\theta_j) \neq 0$ for all irreducible \mathbb{Q}^c -characters χ contained in ρ . Therefore $\dim_E(E[G]\theta_j) = n$.

We now prove that $\text{span}_E(V) \cap E[G]\theta_j = \{0\}$. If λ is an element in this intersection, then $e_\rho\lambda \in e_\rho(\text{span}_E(V)) \cap e_\rho E[G]\theta_j$. Since $e_\rho E[G]\theta_j$ is a simple $E[G]$ -module and $e_\rho(\theta_j) = e_\rho(\omega_\rho^{(j)}) \notin \text{span}_E(V)$ we deduce that $e_\rho(\lambda) = 0$ for all $\rho \in D(G)$; hence $\lambda = 0$.

Since $\text{span}_E(V) \cap E[G]\theta_j = \{0\}$ the computations in step 3 can easily be performed using linear algebra, and this obviously proves that both $\dim_E(\text{span}_E(V \cup T)) = jn$ and $\text{span}_E(V \cup T) \oplus \text{span}_E(W') = L$. \square

Remarks. (i) In order to implement steps 2 and 3 of the algorithm we must be able to compute the action of elements λ of $E[G]$ on the basis elements $\omega \in W$ and to express each $\lambda(\omega)$ in terms of the basis $V \cup W$. Using the matrices $A(g), g \in G$, it is easy to compute $\lambda(\omega)$ as a linear combination $a_1\omega_1 + \dots + a_{nm}\omega_{nm}$ of the original basis. Then $(a_1, \dots, a_{nm})A$ gives the coefficients of a representation of $\lambda(\omega)$ in the basis $V \cup W$.

(ii) If $\omega_1, \dots, \omega_{nm}$ is an \mathcal{O}_E -basis of a G -stable ideal I of \mathcal{O}_L , then we obtain normal basis generators $\theta_1, \dots, \theta_m$ which are contained in I by setting $\theta_j = n \sum_{\rho \in D(G)} e_\rho(\omega_\rho^{(j)})$ in step 2.

We assume henceforth that we explicitly know an \mathcal{O}_E -basis $\omega_1, \dots, \omega_{nm}$ of I and also the representation matrices $A(g) \in \text{Gl}_{nm}(\mathcal{O}_E)$ induced by this basis. By applying the above algorithm we compute normal basis generators $\theta_1, \dots, \theta_m$ of L over $E[G]$ that are contained in I . To shorten the notation we write $\theta = (\theta_1, \dots, \theta_m)$.

Next we compute the $\mathcal{O}_E[G]$ -lattice

$$\mathcal{A}_\theta(I) := \{\lambda \in E[G]^m : \lambda \cdot \theta \in I\},$$

where for any $\lambda = (\lambda_1, \dots, \lambda_m) \in E[G]^m$ and $\alpha = (\alpha_1, \dots, \alpha_m) \in L^m$ we write $\lambda \cdot \alpha$ for the sum $\sum_{i=1}^m \lambda_i(\alpha_i)$. To determine $\mathcal{A}_\theta(I)$ we compute elements λ_j of $E[G]^m$ such that $\lambda_j \cdot \theta = \omega_j$ for $j = 1, \dots, nm$. Then the set $\{\lambda_1, \dots, \lambda_{nm}\}$ is an \mathcal{O}_E -basis of $\mathcal{A}_\theta(I)$.

The order $\mathcal{A}(E[G]; I)$ acts diagonally from the left on $\mathcal{A}_\theta(I)$ and in fact $\mathcal{A}(E[G]; I) = \{\lambda \in E[G] : \lambda \mathcal{A}_\theta(I) \subseteq \mathcal{A}_\theta(I)\}$. We denote by

$$t : E[G] \times E[G] \longrightarrow E$$

the symmetric, non-degenerate E -bilinear pairing which satisfies

$$t(g, h) = \begin{cases} 1, & \text{if } gh = 1, \\ 0, & \text{otherwise,} \end{cases}$$

for all elements g, h of G , and we let

$$s : E[G]^m \times E[G]^m \longrightarrow E$$

be the m -fold orthogonal sum of t . For any $\mathcal{O}_E[G]$ -module Y in $E[G]^m$, respectively $E[G]$, we identify the linear dual $Y^* := \text{Hom}_{\mathcal{O}_E}(Y, \mathcal{O}_E)$ with $\{\lambda \in E[G]^m : s(\lambda, Y) \subseteq \mathcal{O}_E\}$, respectively $\{\lambda \in E[G] : t(\lambda, Y) \subseteq \mathcal{O}_E\}$.

We now define an $\mathcal{O}_E[G]$ -module homomorphism

$$(\cdot, \cdot) : \mathcal{A}_\theta(I) \times \mathcal{A}_\theta(I)^* \longrightarrow \mathcal{O}_E[G]$$

by setting $(\mu, \nu) = \sum_{g \in G} s(g\mu, \nu)g^{-1}$ for $\mu \in \mathcal{A}_\theta(I)$ and $\nu \in \mathcal{A}_\theta(I)^*$. This homomorphism satisfies

$$t((\mu, \nu), \delta) = s(\nu, \delta\mu) = s(\nu\delta, \mu) \tag{2}$$

for $\mu \in \mathcal{A}_\theta(I), \nu \in \mathcal{A}_\theta(I)^*$ and $\delta \in E[G]$. Using (2) the following lemma is proved in the same way as Lemma 4.2 in [Bl,Bu].

Lemma 1. $(\mathcal{A}_\theta(I), \mathcal{A}_\theta(I)^*) = \mathcal{A}(E[G]; I)^*$. □

This lemma leads to an algorithm for computing $\mathcal{A}(E[G]; I)$. (The reader should consult [Bl,Bu] for a discussion of this algorithm in the case $m = 1$.)

We assume henceforth that we can compute explicit \mathcal{O}_E -bases for $\mathcal{A}_\theta(I)$, $\mathcal{A}(E[G]; I)$ and $\mathcal{M}(E, G)$. We shall for brevity now write \mathcal{A}_E and \mathcal{M}_E in place of $\mathcal{A}(E[G]; I)$ and $\mathcal{M}(E, G)$ respectively.

By its very definition $\mathcal{A}_\theta(I)$ is $\mathcal{O}_E[G]$ -isomorphic to I , and so we need only determine the \mathcal{A}_E -structure of $\mathcal{A}_\theta(I)$. Theorem 4 in [Fr2] implies that $\mathcal{A}_\theta(I)$ is locally free over \mathcal{A}_E if and only if $[\mathcal{A}_\theta(I)\mathcal{M}_E : \mathcal{A}_\theta(I)]_{\mathcal{O}_E} = [\mathcal{M}_E : \mathcal{A}_E]_{\mathcal{O}_E}^m$. Since $\mathcal{A}_\theta(I), \mathcal{A}_E$ and \mathcal{M}_E are assumed to be explicitly known the question of local freeness can therefore be decided by algorithm.

Example 1. Let K be $\mathbb{Q}(\sqrt{-1})$ and let L be the subfield of the ray class field $K(27)$ of conductor 27 over K which is fixed by the unique subgroup of $\text{Gal}(K(27)/K)$ of order 2 and also by the Frobenius automorphism of 10. Then L/K is an extension of group $C_9 \times C_3$ and is totally ramified above 3. We let \mathfrak{p}_L denote the unique prime ideal of \mathcal{O}_L lying above 3. With the same methods as described in ([Bl,Bu], §5) one can compute $\mathcal{A}(K[G]; \mathfrak{p}_L^i)$ and $\mathcal{A}_\theta(\mathfrak{p}_L^i)$ (for some normal basis element θ of L over $K[G]$) for each i with $0 \leq i \leq 26$. Theoretical considerations (similar to those used in §2) show that if \mathfrak{p}_L^i is locally-free over $\mathcal{A}(K[G]; \mathfrak{p}_L^i)$, then $i \in \{8, 9, 10\}$, and computation of the relevant indices shows that each of these 3 ideals is indeed locally-free over its associated order in $K[G]$.

If now F/K is the unique subextension of L/K which has group isomorphic to $C_3 \times C_3$, $\Gamma = \text{Gal}(F/K)$, and $\mathfrak{p}_F = \mathcal{O}_F \cap \mathfrak{p}_L$, then each of the orders $\mathcal{A}(K[\Gamma]; \mathfrak{p}_F^i)$ was computed in ([Bl,Bu], §5 and §6). From Lemma 1.1 one knows that \mathfrak{p}_F^i is

locally-free over $\mathcal{A}(K[\Gamma]; \mathfrak{p}_F^i)$ if either $i = 0$ or $i = 1$. Applying the algorithm to check local-freeness of \mathfrak{p}_F^i over $\mathcal{A}(K[\Gamma]; \mathfrak{p}_F^i)$ for each of the remaining indices i with $0 \leq i \leq 8$ one finds local-freeness only for $i = 8$. Using Lemma 1.7 one can also check that \mathfrak{p}_F^8 is not locally-free over $\mathcal{A}(\mathbb{Q}[\Gamma]; \mathfrak{p}_F^8)$.

There are entirely similar results concerning powers of the unique prime ideal above 3 in the unique extension of $\mathbb{Q}(\sqrt{-7})$ which has group isomorphic to $C_3 \times C_3$ and lies in the ray class field $\mathbb{Q}(\sqrt{-7})(9)$.

We now turn to consider the problem of global freeness. To that end we shall suppose that $\mathcal{A}_\theta(I)$ is a locally free \mathcal{A}_E -sublattice of $E[G]^m$. Our aim is to reduce the global freeness problem to the rank one case and then simply adapt the algorithm presented in ([Bl], §2.2).

In the following we shall for brevity write \mathcal{M} , \mathcal{A} and \mathcal{A}_θ for \mathcal{M}_E , \mathcal{A}_E and $\mathcal{A}_\theta(I)$ respectively. We let $Pic(\mathcal{A})$ denote the Picard group of \mathcal{A} . Since \mathcal{A} has Krull dimension one, taking determinants (that is, top exterior powers) over \mathcal{A} induces an isomorphism between the locally-free class group of \mathcal{A} and $Pic(\mathcal{A})$ (cf. [Ba], Ch. IX, §3). It follows that to determine the structure of any locally-free \mathcal{A} -lattice X we need only analyse the invertible \mathcal{A} -lattice $\det_{\mathcal{A}}(X)$.

The lattice \mathcal{A}_θ is by assumption a locally free \mathcal{A} -module, and so $\det_{\mathcal{A}}(\mathcal{A}_\theta)$ canonically embeds into $\det_{E[G]}(\mathcal{A}_\theta \otimes_{\mathcal{O}_E} E)$. Using this it is easy to show that $\det_{\mathcal{A}}(\mathcal{A}_\theta)$ is generated by the determinants

$$\det \begin{pmatrix} \lambda_{i_1,1} & \lambda_{i_1,2} & \cdots & \lambda_{i_1,m} \\ \lambda_{i_2,1} & \lambda_{i_2,2} & \cdots & \lambda_{i_2,m} \\ \vdots & & \ddots & \vdots \\ \lambda_{i_m,1} & \lambda_{i_m,2} & \cdots & \lambda_{i_m,m} \end{pmatrix}, \quad 1 \leq i_1 < \cdots < i_m \leq nm,$$

where $\mathcal{A}_\theta = \langle \lambda_1, \dots, \lambda_{nm} \rangle_{\mathcal{O}_E}$ with elements $\lambda_i = (\lambda_{i,1}, \dots, \lambda_{i,m}) \in E[G]^m$ for each of $i = 1, \dots, nm$.

This gives a lattice with $\binom{nm}{m}$ generators, and before proceeding one has to compute an \mathcal{O}_E -basis. Whilst theoretically this is a trivial task, its actual implementation is usually quite delicate since one rapidly runs into numerical difficulties (cf. comment following Lemma 4.2 of [Bl,Bu]).

Having now reduced the global freeness problem to consideration of lattices which have rank one over $\mathcal{O}_E[G]$ one can proceed just as in ([Bl], §2.2). There is only a slight difference in the definition of the ideals I_ρ in this new context: for each irreducible E -character ρ of G we let \mathcal{O}_ρ denote the ring of algebraic integers in the field E_ρ which is generated over E by the values of any irreducible \mathbb{Q}^c -character contained in ρ , and we now set $I_\rho := [\mathcal{A}_\theta \mathcal{M}e_\rho : \mathcal{M}e_\rho]_{\mathcal{O}_\rho}$. In addition, in the present case the set $D(G)$ is the set of all irreducible E -characters of G .

In the last part of this section we briefly describe how our algorithm can be used to compute $Pic(\mathcal{A})$, in the sense that we exhibit an explicit \mathcal{A} -sublattice

M of $E[G]$ lying in each class of $Pic(\mathcal{A})$. Once such a description of the Picard group is available, we can use the algorithm to determine the class of \mathcal{A}_θ (which is now assumed to be of rank one). Indeed, to do this we need only compute the tensor product $\mathcal{A}_\theta \otimes_{\mathcal{A}} M$ for each representative M of $Pic(\mathcal{A})$ and then apply the algorithm to check whether $\mathcal{A}_\theta \otimes_{\mathcal{A}} M$ is a free \mathcal{A} -lattice. Note that if $\mathcal{A}_\theta = \langle \lambda_1, \dots, \lambda_n \rangle_{\mathcal{O}_E}$ and $M = \langle \mu_1, \dots, \mu_n \rangle_{\mathcal{O}_E}$, then $\mathcal{A}_\theta \otimes_{\mathcal{A}} M \simeq \mathcal{A}_\theta M$ is generated over \mathcal{O}_E by the n^2 elements $\{\lambda_i \mu_j : 1 \leq i, j \leq n\}$.

We let $J(E[G])$ denote the group of finite idèles of $E[G]$, and we regard $E[G]^*$ as diagonally embedded in $J(E[G])$. For any \mathcal{O}_E -order Λ in $E[G]$ we write $U(\Lambda)$ for the group of unit idèles of Λ .

For each $\rho \in D(G)$ we fix an irreducible \mathbb{Q}^c -character χ_ρ contained in ρ . The Wedderburn decomposition of $E[G]$ is explicitly given by the E -algebra homomorphism

$$\Phi : E[G] \longrightarrow \bigoplus_{\rho \in D(G)} E_\rho,$$

which is induced by sending a group element $g \in G$ to $(\chi_\rho(g))_{\rho \in D(G)}$.

We let \mathfrak{f} be any integral \mathcal{O}_E -ideal such that $\mathfrak{f}\mathcal{M} \subseteq \mathcal{A}$ and put $\mathcal{B} = \mathcal{O}_E + \mathfrak{f}\mathcal{M}$. We denote by $cl_{\mathfrak{f}}(E_\rho)$ the ray class group of E_ρ of conductor \mathfrak{f} . Then Φ (or rather its inverse), together with class field theory, induces a well-defined epimorphism

$$\kappa_{\mathfrak{f}} : \bigoplus_{\rho \in D(G)} cl_{\mathfrak{f}}(E_\rho) \longrightarrow \frac{J(E[G])}{E[G]^*U(\mathcal{B})} \longrightarrow Pic(\mathcal{A}).$$

For any fractional ideal \mathfrak{a}_ρ of E_ρ , respectively any locally free \mathcal{A} -lattice M in $E[G]$, we denote its class in $cl_{\mathfrak{f}}(E_\rho)$, respectively in $Pic(\mathcal{A})$, by $[\mathfrak{a}_\rho]$, respectively $[M]$.

Lemma 2. For each $\rho \in D(G)$ let \mathfrak{a}_ρ denote an ideal of \mathcal{O}_ρ such that $(\mathfrak{a}_\rho, \mathfrak{f}) = 1$. Then:

$$\left[\Phi^{-1}([\mathfrak{a}_\rho]_{\rho \in D(G)}) \cap \mathcal{A} \right] = \kappa_{\mathfrak{f}}([\mathfrak{a}_\rho]_{\rho \in D(G)}).$$

Proof. For each $\rho \in D(G)$ we define an idèle $\alpha_\rho \in J(E_\rho)$ by setting $\alpha_{\rho, \mathfrak{P}} = 1$ for $\mathfrak{P} \nmid \mathfrak{a}_\rho$ and choosing $\alpha_{\rho, \mathfrak{P}} \in E_{\rho, \mathfrak{P}}$ such that $v_{\mathfrak{P}}(\alpha_{\rho, \mathfrak{P}}) = v_{\mathfrak{P}}(\mathfrak{a}_\rho)$ for $\mathfrak{P} | \mathfrak{a}_\rho$, where $v_{\mathfrak{P}}(-)$ denotes the \mathfrak{P} -adic valuation. Identifying $E_\rho \otimes_E E_{\mathfrak{p}}$ with $\bigoplus_{\mathfrak{P} | \mathfrak{p}} E_{\rho, \mathfrak{P}}$ we write $\alpha_\rho = \sum_i x_\rho^{(i)} \otimes \beta_\rho^{(i)}$, where $x_\rho^{(i)} \in E_\rho$, $\beta_\rho^{(i)} \in J(E)$ and the sum is over some finite index set. Then $\kappa_{\mathfrak{f}}([\mathfrak{a}_\rho]_{\rho \in D(G)})$ is represented by the unique lattice whose completions are given by $\theta_{\mathfrak{p}}\mathcal{A}_{\mathfrak{p}}$ with $\theta_{\mathfrak{p}} := \sum_{\rho \in D(G)} \sum_i \Phi^{-1}(x_\rho^{(i)})\beta_{\rho, \mathfrak{p}}^{(i)}$. On the other hand it is easily seen that the completion of $\Phi^{-1}([\mathfrak{a}_\rho]_{\rho \in D(G)})$ at \mathfrak{p} is given by $\theta_{\mathfrak{p}}\mathcal{M}_{\mathfrak{p}}$. The special choice of the idèles $\alpha_\rho \in J(E_\rho)$, $\rho \in D(G)$, implies that $\theta_{\mathfrak{p}} = 1$ for primes \mathfrak{p} which divide \mathfrak{f} whereas $\mathcal{A}_{\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}}$ for primes \mathfrak{p} which do not divide \mathfrak{f} . We therefore conclude that $\theta_{\mathfrak{p}}\mathcal{M}_{\mathfrak{p}} \cap \mathcal{A}_{\mathfrak{p}} = \theta_{\mathfrak{p}}\mathcal{A}_{\mathfrak{p}}$. \square

Remarks. (i) If for each $\rho \in D(G)$ we know an \mathcal{O}_E -basis of \mathfrak{a}_ρ , then by using an explicit description of Φ we can compute an \mathcal{O}_E -basis of $M = \Phi^{-1}([\mathfrak{a}_\rho]_{\rho \in D(G)})$.

The most efficient way to compute the intersection with \mathcal{A} is probably to use the equality $M \cap \mathcal{A} = (M^* + \mathcal{A}^*)^*$.

(ii) If one explicitly knows the ray class groups $cl_f(E_\rho)$ for all $\rho \in D(G)$, then the algorithm can be used to determine the group structure of $Pic(\mathcal{A})$. For each element $x \in \prod_{\rho \in D(G)} cl_f(E_\rho)$, we compute a representative of $\kappa_f(x)$ and by applying the algorithm we can decide if x is in the kernel of κ_f . This gives the exact order of $Pic(\mathcal{A})$.

Suppose in addition that $\prod_{\rho \in D(G)} cl_f(E_\rho)$ is given by a set of generators $\{x_1, \dots, x_s\}$ and a set of relations R . Let L' be the free \mathbb{Z} -module on $\{x_1, \dots, x_s\}$ and let $L \subseteq L'$ be the \mathbb{Z} -submodule generated by R . Then

$$Pic(\mathcal{A}) \simeq L' / \langle L, \ker(\kappa_f) \rangle_{\mathbb{Z}},$$

and by applying algorithms for Hermite Normal Form and Smith Normal Form (see [C], Ch. II, 2.4) this gives the complete group structure of the Picard group and also a set of explicit generators.

Example 2. Continuing with the notation of Example 1, we let $K = \mathbb{Q}(\sqrt{-1})$ or $K = \mathbb{Q}(\sqrt{-7})$, and let F be the unique extension of K which has group isomorphic to $C_3 \times C_3$ and is contained in the ray class field $K(9)$. Then one knows that \mathcal{O}_F , \mathfrak{p}_F , and \mathfrak{p}_F^8 are all locally-free over their respective associated orders in $K[\Gamma]$. The algorithm described above can be used to show that each of these ideals is in fact free over its associated order in $K[\Gamma]$. (Note that F/K is weakly ramified so that $\mathcal{A}(K[\Gamma]; \mathfrak{p}_F) = \mathcal{O}_K[\Gamma]$ (cf. Lemma 1.1). Note also that in this case $A_{F/K} = \mathfrak{p}_F^{1-p^2} = 3^{-1} \mathfrak{p}_F \cong \mathfrak{p}_F$.)

The above algorithm was implemented using the number theory package KANT [GvS]. The numerical results and also a more detailed description of the implementation are available upon request from the author at the following address: Institut für Mathematik der Universität Augsburg, Universitätsstr. 8, D-86159 Augsburg, Germany (e-mail: bley@uni-augsburg.de), (<http://www.math.uni-augsburg.de/~bley>).

Acknowledgments

I am grateful to both Ali Fröhlich and Werner Bley for numerous conversations on this topic. I am in addition grateful to Werner Bley for providing the illuminating computational results described in the appendix, and for very carefully checking through an earlier version of this manuscript. Lastly, I am grateful to the referee for several helpful remarks.

References

- [B] H. Bass, *Algebraic K-theory*, W.A.Benjamin Inc., New York 1968.
- [Be1] A-M. Bergé, Arithmétique d'une extension à groupe d'inertie cyclique, *Ann. Inst. Fourier* **28** (1978), 17-44.
- [Be2] A-M. Bergé, Anneaux d'entiers et ordres associés, Thèse, Université de Bordeaux, 1979.
- [Bl] W. Bley, Computing associated orders and Galois generating elements of unit lattices, *J. Number Theory* **62** (1997), 242-256.
- [Bl,Bu] W. Bley and D. Burns, Über arithmetische assoziierte Ordnungen, *J. Number Theory* **58** (1996), 361-387.
- [Bo,V] Z. I. Borevic and S. V. Vostokov, Rings of integers in an extension of prime degree of a local field as a Galois module, *Journal of Soviet Math.* **6** (1976), 227-238.
- [Bu1] D. Burns, Factorisability and the arithmetic of wildly ramified Galois extensions, *Sém. Théorie des Nombres de Bordeaux* **1** (1989), 59-66.
- [Bu2] D. Burns, Factorisability and wildly ramified Galois extensions, *Ann. Inst. Fourier* **41** (1991), 393-430.
- [Bu3] D. Burns, On the Galois structure of the square root of the codifferent, *Sém. Théorie des Nombres de Bordeaux* **3** (1991), 73-92.
- [Bu4] D. Burns, On the Galois structure of units in number fields, *Proc. London Math. Soc.* **66** (1993), 71-91.
- [Bu5] D. Burns, On arithmetically realizable classes, *Math. Proc. Cambridge Phil. Soc.* **118** (1995), 383-392.
- [By] N. P. Byott, Some self-dual rings of integers which are not free over their associated orders, *Math. Proc. Cambridge Phil. Soc.* **110** (1991), 5-10.
- [C] H. Cohen, *A course in computational algebraic number theory*, Springer, Heidelberg 1993.
- [Ch,L] S-P. Chan and C. H. Lim, The associated order of rings of integers in Lubin-Tate division fields over the p -adic number field, *Illinois J. Math.* **39** (1995), 205-220.
- [Cu,R] C. W. Curtis and I. Reiner, *Methods of representation theory*, Vol. I, Wiley Classics Library, John Wiley and Sons, New York 1990.
- [E,M1] G. G. Elder and M. L. Madan, Galois module structure of integers in weakly ramified extensions, *Arch. Math.* **64** (1995), 117-120.
- [E,M2] G. G. Elder and M. L. Madan, Galois module structure of integers in wildly ramified $C_p \times C_p$ extensions, to appear in *Canadian J. Math.*
- [Er] B. Erez, The Galois structure of the square root of the inverse different, *Math. Zeit.* **208** (1991), 239-255.
- [Er,T] B. Erez and M. J. Taylor, Hermitian modules in Galois extensions of number fields and Adams operations, *Annals of Math.* **135** (1992), 271-296.
- [F] M-J. Ferton, Sur les idéaux d'une extension cyclique de degré premier d'un corps local, *C. R. Acad. Sc. Paris* **276** (1973), 1483-1486.
- [Fo] J-M. Fontaine, Groupes de ramification et représentations d'Artin, *Ann. Scient. Éc. Norm. Sup.* **4** (1971), 337-392.
- [Fr1] A. Fröhlich, The module structure of Kummer extensions over Dedekind domains, *J. Reine Angew. Math.* **209** (1962), 39-53.
- [Fr2] A. Fröhlich, Invariants for modules over commutative separable orders, *Quart. J. Math. Oxford* **16** (1965), 193-232.
- [Fr3] A. Fröhlich, *Galois module structure of algebraic integers*, Springer, Heidelberg 1983.
- [Fr4] A. Fröhlich, L -values at zero and multiplicative Galois module structure (also Galois Gauss sums and additive Galois module structure), *J. Reine Angew. Math.* **397** (1989), 42-99.
- [G] K. Girstmair, A Remark on Normal Bases, *J. Number Theory* **58** (1996), 64-65.

- [GvS] J. Graf V. Schmettow, KANT – a tool for computations in algebraic number fields. In: A. Pethö, M. E. Pohst, H. C. Williams, H. G. Zimmer (eds.), *Computational Number Theory*, Walter de Gruyter, 1991, pp. 321-330.
- [J] H. Jacobinski, Über die Hauptordnung eines Körpers als Gruppenmodul, *J. Reine Angew. Math.* **213** (1963), 151-164.
- [Ja] A. V. Jakovlev, Homological determinacy of p -adic representations of rings with power basis, *Math. USSR-Izvestija* **4** (1970), 1001-1016.
- [K] F. Kawamoto, On normal integral bases of local fields, *J. Algebra* **98** (1986), 197-199.
- [L] H. W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, *J. Reine Angew. Math.* **201** (1959), 119-149.
- [M] L. McCulloh, Galois module structure of abelian extensions, *J. Reine Angew. Math.* **375-376** (1987) 259-306.
- [R-C,V-S,M] M. Rzedowski Calderón, G.D. Villa Salvador and M. L. Madan, Galois module structure of rings of integers, *Math. Zeit.* **204** (1990), 401-424.
- [S] J-P. Serre, *Corps Locaux*, Hermann, Paris 1962.
- [T1] M. J. Taylor, Galois module structure of integers of relative abelian extensions, *J. Reine Angew. Math.* **303/304** (1978), 97-101.
- [T2] M. J. Taylor, On Fröhlich's conjecture for rings of integers of tame extensions, *Invent. Math.* **63** (1981), 41-79.
- [T3] M. J. Taylor, Formal groups and Galois module structure of local rings of integers, *J. Reine Angew. Math.* **358** (1985), 97-103.
- [T4] M. J. Taylor, On the Galois module structure of rings of integers of wild abelian extensions, *J. London Math. Soc.* **52** (1995), 73-87.
- [U1] S. V. Ullom, Normal bases in Galois extensions of number fields, *Nagoya Math. J.* **34** (1969), 153-167.
- [U2] S. V. Ullom, Galois cohomology of ambiguous ideals, *J. Number Theory* **1** (1969), 11-15.
- [U3] S. V. Ullom, Integral normal bases in Galois extensions of local fields, *Nagoya Math. J.* **39** (1970), 141-148.
- [V1] S. V. Vostokov, Ideals of an abelian p -extension of an irregular local field as Galois modules, *Journal of Soviet Math.* **9** (1978), 299-317.
- [V2] S. V. Vostokov, Ideals of an abelian p -extension of a local field as Galois modules, *Journal of Soviet Math.* **11** (1979), 567-584.

David Burns
 Department of Mathematics
 King's College London
 Strand
 London WC2R 2LS
 e-mail: david.burns@kcl.ac.uk

(Received: May 5, 1996)