ON THE EXISTENCE OF MINKOWSKI UNITS

DAVID BURNS, DONGHYEOK LIM AND CHRISTIAN MAIRE

ABSTRACT. We investigate the Galois structure of algebraic units in cyclic extensions of number fields and thereby obtain strong new results on the existence of independent Minkowski S-units.

1. INTRODUCTION

At the outset we fix an odd prime number p and write $\mathbb{F}$ for the field of cardinality p. We then fix a finite Galois extension of number fields L/K of degree divisible by p and set $G := \mathrm{Gal}(L/K)$. For a finite set of places S of K, we write $\mathcal{O}_{L,S}$ for the subring of L comprising elements that are integral at all non-archimedean places of L that do not lie above a place in S and, with μ_L denoting the group of roots of unity in L, we obtain a $\mathbb{Z}_p[G]$-lattice by setting $U_{L,S} := \mathbb{Z}_p \otimes_{\mathbb{Z}} (\mathcal{O}_{L,S}^{\times}/\mu_L)$.

If the G-module $U_{L,S}/U_{L,S}^p$ has a direct summand isomorphic to $\mathbb{F}[G]^m$ for a natural number m, then one says L/K has a family of 'm independent Minkowski S-units (at p)'. In particular, by the Krull-Schmidt Theorem, the maximum size $m_{L/K,S} = m_{L/K,S,p}$ of a family of independent Minkowski S-units (at p) for L/K is well-defined. In addition, recent work in [9] has shown that $m_{L/K,S}$ plays an important role in the study of both tamely ramified pro-p extensions and the deficiency of p-class tower groups and also, following work of Ozaki [17], of the inverse Galois problem for the p-class field tower (cf. [10]). Unfortunately, however, the determination of $m_{L/K,S}$ appears, in general, to be a very difficult problem.

In this note we identify conditions under which one can 'bound' the complexity of the $\mathbb{Z}_p[G]$-lattice $U_{L,S}$ and thereby deduce new results on $m_{L/K,S}$. Here we recall that understanding the explicit structure of arithmetic lattices is a notoriously difficult problem, not least because, by well-known results of Heller and Reiner [12, 13], the relevant theory of integral representations is usually extremely complicated.

To recall the most general (as far as we are aware) result in this direction, we fix an abstract finite group Γ, a finite set of places Σ of K containing all p-adic places and a p-adic Galois representation T over K unramified outside Σ. Then [3, Th. 1.1] proves the existence of an upper bound on the number of isomorphism classes of indecomposable modules that occur in the Krull-Schmidt decompositions of the $\mathbb{Z}_p[\Gamma]$-lattices arising from the p-adic étale cohomology groups $H^i(\mathrm{Spec}(\mathcal{O}_{L',\Sigma})_{\text{ét}}, T) \cong H^i(\mathrm{Spec}(\mathcal{O}_{K',\Sigma})_{\text{ét}}, \mathbb{Z}_p[\Gamma] \otimes_{\mathbb{Z}_p} T)$ as L'/K' ranges over extensions of K for which L'/K' is unramified outside Σ, Galois and such that $\mathrm{Gal}(L'/K')$ identifies with Γ. In particular, in the case ($i = 1$ and $T = \mathbb{Z}_p(1)$) relevant to us, this result relates to the module $U_{L,S}$

2000 *Mathematics Subject Classification.* 11R33, 11R34, 11R37.

Key words and phrases. Minkowski units, Galois structure of algebraic units, Krull-Schmidt decomposition, Yakovlev diagram.

only if S contains all places that are p-adic or ramify in L and gives bounds depending on Γ and the number of places of L that are p-adic or divide the different of L/K.

In contrast, we shall now obtain the finer information about $U_{L,S}$ contained in the following result. In this result, for each natural number n we write $\mathcal{C}_n$ for the (countably infinite) collection of pairs $(L/K, S)$ comprising a Galois extension of number fields L/K for which G identifies with the cyclic group $\mathbb{Z}/p^n$ of order p^n and $\mathrm{Norm}_{L/K}(\mu_L) = \mu_K$, and a finite set S of places of K for which the S-ideal p-class group of every intermediate field of L/K is cyclic.

Theorem 1.1. *Fix a natural number n. Then, as $(L/K, S)$ ranges over $\mathcal{C}_n$, only finitely many isomorphism classes of indecomposable $\mathbb{Z}_p[\mathbb{Z}/p^n]$-lattices arise as direct summands of any $U_{L,S}$.*

The starting point for our proof of this is an algebraic result of Yakovlev (see Proposition 4.1) which implies that, if L/K is any cyclic extension of degree p^n, then for every finite set S the $\mathbb{Z}_p[\mathbb{Z}/p^n]$-module structure of $U_{L,S}$ is determined up to direct summands that are permutation modules by restriction and corestriction maps between the Galois cohomology groups $H^1(J, U_{L,S})$ as J runs over subgroups of $\mathbb{Z}/p^n$. Then, for $(L/K, S)$ in $\mathcal{C}_n$, class-field theoretic arguments allow us to parametrise $H^1(J, U_{L,S})$ in terms of (an auxiliary prime ideal and) J-stable fractional ideals of L supported on the set $R_{L/K}$ of places of K ramifying in L (see Proposition 3.2). In general, the difficulty of determining relations between the classes of such ideals is a serious obstacle to obtaining a fully explicit description of the cohomology groups. However, if $|R_{L/K}|$ is 'large' compared to p^n, then there must exist pairs of subgroups (J_1, J_2) of $\mathbb{Z}/p^n$ for which there are multiple places in $R_{L/K}$ that have inertia subgroup J_1 and decomposition subgroup J_2, and we can use such subgroup pairs to construct explicit direct summands of each group $H^1(J, U_{L,S})$. Whilst these direct summands do not fully determine the cohomology groups, they do at least mean that the undetermined part can be 'bounded' as $(L/K, S)$ ranges over $\mathcal{C}_n$ and this leads to the finiteness assertion in Theorem 1.1.

Here we note that this finiteness result is, a priori, far from clear as the $\mathbb{Z}_p$-rank of $U_{L,S}$ is unbounded as $(L/K, S)$ ranges over $\mathcal{C}_n$, whilst, if $n > 2$, then there exist infinitely many non-isomorphic indecomposable $\mathbb{Z}_p[\mathbb{Z}/p^n]$-lattices (cf. [13]). In addition, Theorem 1.1 is stronger than the corresponding case of [3, Th. 1.1] since, firstly, its conclusion does not require S to contain all places that are either p-adic or ramify in L and, secondly, its proof gives more information on the occurring indecomposable modules and thereby leads both to sharper bounds on the number of such isomorphism classes and also, upon appropriate specialisation, to some very concrete consequences. For example, if the p-Hilbert S-class field of L is cyclic over K, then it implies the $\mathbb{Z}_p[G]$-structure of $U_{L,S}$ depends only on the ramification and residue degrees of places of K that are ramified in L or belong to S and can even be described completely explicitly if L/K is unramified (see Theorem 4.4).

These improvements also mean that Theorem 1.1 can be used to deduce the existence of families of extensions in which $m_{L/K,S}$ is unbounded even though the set of places ramifying in L/K remains small and contains no place that is tamely ramified, thereby complementing the constructions of [11]. (For details see Corollary 5.1 and Examples 5.2).

We remark that several aspects of the techniques developed here can be extended to more general classes of extensions L/K (thereby further refining the general approach of [3]). Such results are discussed in the articles [2] and [14] of Bouazzaoui and the second author and of Kumon and the second author respectively.

Finally, for the reader's convenience, we record some general notation. For a Galois extension of fields F/E, we abbreviate $\mathrm{Gal}(F/E)$ to $G(F/E)$. For a finitely generated $\mathbb{Z}_p$-module M we write $\mathrm{rk}(M)$ for its rank $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} M)$. For an abelian group X we set $X_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} X$. For a natural number n, we set $[n] := \{i \in \mathbb{Z} : 1 \leq i \leq n\}$ and $[n]^* := \{0\} \cup [n]$.

Acknowledgement We are grateful to Manabu Ozaki and Ravi Ramakrishna for their interest in our work and helpful comments. We are also very grateful to the anonymous referee for several suggestions that improved our article.

2. Hypotheses and examples

At the outset we fix an odd prime number p. For an extension of number fields L/K and finite set S of places of K, we write $A_{L,S}$ for the Sylow p-subgroup of the S-ideal class group of L (that is, the quotient of the ideal class group of L by the subgroup generated by the classes of prime ideals lying above S), $H_{L,S}$ for the p-Hilbert S-class field of L (that is, the maximal unramified abelian p-extension of L in which all places of L above S split completely) so that $A_{L,S}$ is canonically isomorphic to $G(H_{L,S}/L)$, and $R_{L/K}$ for the set of places of K that ramify in L. If $S = \emptyset$, then we abbreviate $H_{L,S}$, $A_{L,S}$ and $U_{L,S}$ to H_L, A_L and U_L respectively. We also write K_S for the maximal pro-p extension of K unramified outside S and set $G_{K,S} := \mathrm{G}(K_S/K)$.

We now fix the following data:

$$\begin{cases} \text{a finite cyclic } p\text{-extension of number fields } L/K \text{ with Galois group } G; \\ \text{a finite set } S \text{ of places of } K \text{ with } S \cap R_{L/K} = \emptyset. \end{cases} \tag{1}$$

We assume that this data satisfies the following hypothesis.

Hypothesis 2.1.

(C1) For every intermediate subfield E of L/K, the group $A_{E,S}$ is cyclic.

(C2) $\mathrm{Norm}_{L/K}(\mu_L) = \mu_K$.

Remark 2.2. Condition (C2) has a conceptual interpretation: since G is a cyclic p-group and μ_L is finite, a Herbrand quotient argument can be combined with general results (cf. [1, Th. 5 and Th. 9]) to show (C2) is satisfied if and only if μ_L is a cohomologically-trivial G-module. In addition, since p is odd, a straightforward analysis also shows that the latter condition is satisfied if and only if either the Sylow p-subgroup $\mu_{K,p}$ of μ_K is trivial or one has $L = K(\mu_{L,p})$ (see, for example, [18, Lem. 5.4.4(1)]).

It is clear that, for any given L/K, the Chebotarev Density Theorem implies that one can simply increase the set S in order to satisfy (C1). On the other hand, for several natural families of extensions L/K, such as in the following examples, (C1) is satisfied with $S = \emptyset$.

Examples 2.3. In each of the following cases, the extension L/K is tamely ramified.
(i) Assume A_K is cyclic and non-trivial. By the Burnside Basis Theorem, $G_{K,\emptyset}$ is pro-cyclic and hence abelian. Therefore the p-class field tower of K terminates at H_K and so $H_E = H_K$ for any unramified p-extension E of K. Hence, if $L \subseteq H_K$, then $(L/K, \emptyset)$ satisfies (C1).

(ii) Assume A_K is trivial and set $r_K := \dim_{\mathbb{F}}(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p)$. Then, for any $s \in [r_K+1]$, the Gras-Munnier Theorem (cf. [7, Prop. 3.1], [8]) implies the existence of infinitely many sets Σ of non-archimedean, non p-adic, places of K for which $|\Sigma| = s$, $G_{K,\Sigma}$ is a non-trivial cyclic group and $G_{K,\Sigma'}$ is trivial for all $\Sigma' \subsetneq \Sigma$. In this case every place in Σ is totally ramified in K_Σ and so, for any intermediate field L of K_Σ/K, one has $A_L = (0)$ so that $(L/K, \emptyset)$ satisfies (C1).

More generally, the following observation leads to many examples in which (C1) is satisfied and S does not contain all places that are either p-adic or ramify in L.

Lemma 2.4. *Let L/K and S be as in (1). If there exists a place $\mathfrak{q}$ of K that does not split in $H_{L,S}$, then the following claims are valid.*

(i) $A_{E,S}$ is cyclic (so that $(L/K, S)$ has property (C1)).

(ii) $A_{E,S}$ is generated by the unique prime $\mathfrak{q}_E$ of E above $\mathfrak{q}$.

(iii) $G(E/K)$ acts trivially on $A_{E,S}$.

Proof. If $A_{E,S} = G(H_{E,S}/E)$ is not cyclic, then no place of E can have full decomposition group in $G(H_{E,S}/E)$. In particular, as $H_{E,S} \subseteq H_{L,S}$, this contradicts the existence of $\mathfrak{q}$ and so proves claim (i). Since $\mathfrak{q}_E$ is unramified in $H_{E,S}$, claim (ii) follows directly from class field theory. Claim (iii) then follows from claim (ii) and the fact $\mathfrak{q}_E$ is invariant under the action of $G(E/K)$. □

Remark 2.5. If A_K is cyclic, then there are infinitely many sets Σ of non-archimedean, non-p-adic, places of K for which the (finite) extension K_Σ/K satisfies the non-splitting hypothesis of Lemma 2.4. To show this, we recall the 'governing field' $\mathrm{Gov}(K)$ of K is defined in [7, Def. 3.1] to be $K(\zeta_p, \sqrt[p]{V_\emptyset(K)})$, where $V_\emptyset(K)$ denotes the subgroup of $K^\times$ comprising elements whose principal fractional ideal is a p-th power of a fractional ideal of K. In particular, by applying the Chebotarev Density Theorem to the finite extension $\mathrm{Gov}(K)H_K/K(\zeta_p)$, one can choose a non-archimedean, non p-adic, place $\mathfrak{p}$ of K that is inert in H_K, splits completely in $K(\zeta_p)$ and is such that, for any, and therefore every, fixed place $\mathfrak{q}$ of $K(\zeta_p)$ above $\mathfrak{p}$, the Frobenius automorphism $\mathrm{Fr}_\mathfrak{q}$ of $\mathfrak{q}$ in $V := G(\mathrm{Gov}(K)/K(\zeta_p))$ is non-trivial (it is possible that $H_K \subseteq \mathrm{Gov}(K)$, but this fact has no impact on our construction of $\mathfrak{p}$). Now fix $s \in [r_K+1]$. Then, as the $\mathbb{F}$-space V has dimension r_K+1 (cf. [8, (1.1)]), one can fix a subset $\{v_i\}_{i\in[s+1]}$ of V, with $v_{s+1} = \mathrm{Fr}_\mathfrak{q}$, that spans a subspace of dimension s and is such that any proper subset is linearly independent. Let $\Sigma = \{\mathfrak{p}_i\}_{i\in[s+1]}$ be a set formed by choosing $\mathfrak{p}_{s+1} = \mathfrak{p}$ and a non-p-adic place $\mathfrak{p}_i$ of K for each $i \in [s]$ such that $\mathfrak{p}_i$ splits in $K(\zeta_p)$ and v_i is equal to the Frobenius automorphism at a place of $K(\zeta_p)$ above $\mathfrak{p}_i$. Then $G_{K,\Sigma}$ has generator rank 2 as a consequence of the Gras-Munnier Theorem, the cyclicity of A_K, and the cyclicity of the inertia subgroup of the Galois group at a non-p-adic place for pro-p extensions of number fields. In addition, by construction, $\mathfrak{p}$ is inert in H_K and ramified in the degree p extension of K (in the Gras-Munnier Theorem) that is ramified precisely at Σ. Hence, $\mathfrak{p}$ does not split in K_Σ by the Burnside Basis Theorem.

Remark 2.6. Fix a number field F and a finite set Σ of places of F containing all places that are either p-adic or archimedean. Then, following Wingberg [19], the group $G_{F,\Sigma}$ is said to be 'of local type' if some place $\mathfrak{p}$ in Σ has full decomposition group in $G_{F,\Sigma}$. In this case, since $\mathfrak{p}$ does not split in F_Σ, Lemma 2.4 implies that (C1) is satisfied by any cyclic p-extension L/K with $F \subseteq K \subseteq L \subset F_\Sigma$. In addition, if F is totally real, then [19, Prop. 1.1] implies $G_{F,\Sigma}$ is of local type if and only if F is p-rational and Σ is primitive (in the sense of [6, §IV.3], [15]) and so a recent conjecture of Gras [5] implies there should be many such $G_{F,\Sigma}$. More generally, [19] gives a criterion in terms of the arithmetic of F for the group $G_{F,\Sigma}$ to be of local type and explicit examples of such F for which $G_{F,\Sigma}$ is 'large' (such as a Demushkin group of rank 4).

3. Galois cohomology

In this section, we fix data as in (1) and establish (in Proposition 3.2) the key consequence that Hypothesis 2.1 has for our theory. To do so, we fix a subgroup J of G, set $E := L^J$ and use the following notations.

- I_E is the pro-p completion of the group of fractional $\mathcal{O}_E$-ideals.
- P_E is the pro-p completion of the group of principal $\mathcal{O}_E$-ideals.
- For a finite set S of primes of K, $\langle S\rangle_E$ is the $\mathbb{Z}_p$-submodule of I_E generated by the prime ideals of E above S.
- We write $I_{E,S}$ and $P_{E,S}$ to denote $I_E/\langle S\rangle_E$ and $P_E/(P_E\cap\langle S\rangle_E)$ respectively.
- By abuse of notations, we use $I_{E,S}$ and $P_{E,S}$ to denote also their images in $I_{L,S}$ under the map $I_{E,S}\to I_{L,S}$ induced by the lifting map.
- For a fractional ideal ρ of $\mathcal{O}_E$, we will also use ρ to denote its image in I_E.

We regard all of the groups listed above as $\mathbb{Z}_p[G(E/K)]$-modules in the natural way.

The following result gives an easy consequence of (C2) regarding these modules that will form the basis of our approach. (We note that all results in this section are vacuously true for the trivial subgroup J and so we will only consider the case that J is non-trivial in the proofs.)

Lemma 3.1. *If L/K satisfies (C2), then there exists a canonical identification of $\mathbb{Z}_p[G/J]$-modules*

$$H^1(J,U_{L,S})\cong (P_{L,S})^J/P_{E,S}\cong \ker\bigl((I_L)^J/\langle S\rangle_E P_E\xrightarrow{\iota} A_{L,S}\cong I_L/\langle S\rangle_L P_L\bigr),$$

where ι is induced by the natural map $I_L\to A_{L,S}\cong I_L/\langle S\rangle_L P_L$.

Proof. There is a canonical exact sequence

$$0\to \mathcal{O}_{L,S}^\times\to L^\times\to P(L)/P_S(L)\to 0,$$

where for each intermediate field E of L/K, $P(E)$ denotes the group of principal fractional $\mathcal{O}_E$-ideals and $P_S(E)$ is the subgroup of principal fractional ideals generated by S-units. By Galois cohomology and Hilbert's Theorem 90, we have an exact sequence

$$0\longrightarrow \mathcal{O}_{E,S}^\times\longrightarrow E^\times\longrightarrow \bigl(P(L)/P_S(L)\bigr)^J\longrightarrow H^1(J,\mathcal{O}_{L,S}^\times)\longrightarrow 0,$$

and hence an induced isomorphism

$$H^1(J,\mathcal{O}_{L,S}^\times)\cong \operatorname{coker}\bigl(P(E)/P_S(E)\to (P(L)/P_S(L))^J\bigr).$$

Upon passing to pro-p completions, this identifies $H^1(J,(\mathcal{O}_{L,S}^\times)_p)$ with $\operatorname{coker}(P_{E,S}\to (P_{L,S})^J)$.

We next recall (from Remark 2.2) that (C2) implies μ_L is a cohomologically-trivial G-module, and hence that the group $H^i(J,\mu_{L,p})$ vanishes for every i. From the tautological short exact sequence $0\to\mu_{L,p}\to(\mathcal{O}_{L,S}^\times)_p\to U_{L,S}\to 0$, we can thus deduce that, if (C2) is satisfied, then the natural map $H^1(J,(\mathcal{O}_{L,S}^\times)_p)\to H^1(J,U_{L,S})$ is bijective. The above argument therefore shows that $H^1(J,U_{L,S})$ is isomorphic to $(P_{L,S})^J/P_{E,S}$, as claimed.

Finally, we note that $(I_{L,S})^J\cap P_{L,S}=(P_{L,S})^J$ and hence that $(P_{L,S})^J/P_{E,S}$ is the kernel of the natural map $(I_{L,S})^J/P_{E,S}\to I_{L,S}/P_{L,S}$. We have $(I_{L,S})^J/P_{E,S}\cong(I_L)^J/\langle S\rangle_E P_E$ because $(I_{L,S})^J$ identifies with $(I_L)^J/\langle S\rangle_E$ since $H^1(J,\langle S\rangle_L)$ vanishes and $S\cap R_{L/K}=\emptyset$. Therefore, the second claimed isomorphism follows. □

Via this result, the group $H^1(J,U_{L,S})$ is parametrised, under Hypotheses 2.1, in terms of the classes in $I_L/\langle S\rangle_E P_E$ of certain J-invariant ideals in I_L, and in the next result we describe this parametrisation explicitly.

We assume henceforth that Hypothesis 2.1 is satisfied and use the following notation.

- For $\mathfrak{a}\in I_E$ and $\mathfrak{b}\in(I_L)^J$, we write $[\mathfrak{a}]_E$ and $[\mathfrak{b}]'_E$ for their respective images in $A_{E,S}$ and $(I_L)^J/\langle S\rangle_E P_E$.
- We fix a prime $\mathfrak{q}_E$ of E not above $R_{L/K}$ whose class generates $A_{E,S}$.
- The decomposition and inertia subgroups in G of a place $\mathfrak{r}$ of K are $G(\mathfrak{r})$ and $I(\mathfrak{r})$.
- For $\mathfrak{p}\in R_{L/K}$ we fix a $\mathfrak{p}$-adic place $\mathfrak{p}_L$ of L. We then define J-invariant ideals by setting

$$\mathfrak{p}_{L/E}:=\prod\nolimits_{\sigma\in J/(J\cap G(\mathfrak{p}))}\sigma(\mathfrak{p}_L).$$

In the sequel we also write the action of $\mathbb{Z}_p[G/J]$ on $H^1(J,U_{L,S})$ additively and, for $\mathfrak{p}\in R_{L/K}$, we denote the projection map $\mathbb{Z}_p[G/J]\to\mathbb{Z}_p[G/JG(\mathfrak{p})]$ by $\pi_J^{\mathfrak{p}}$.

Proposition 3.2. *If Hypothesis 2.1 is satisfied, then the following claims are valid.*

(i) The $\mathbb{Z}_p[G/J]$-module $H^1(J,U_{L,S})$ is contained (via isomorphism of Lemma 3.1) in the $\mathbb{Z}_p[G/J]$-module $(I_L)^J/\langle S\rangle_E P_E$ which is generated by $\{[\mathfrak{q}_E]'_E\}\cup\{[\mathfrak{p}_{L/E}]'_E\}_{\mathfrak{p}\in R_{L/K}}$.

(ii) Fix $m\in\mathbb{Z}$ and $\{x(\mathfrak{p})\}_{\mathfrak{p}\in R_{L/K}}\subset\mathbb{Z}_p[G/J]$. Then $[\mathfrak{q}_E^m\prod_{\mathfrak{p}\in R_{L/K}}(\mathfrak{p}_{L/E})^{x(\mathfrak{p})}]'_E=0$ only if for all $\mathfrak{p}\in R_{L/K}$ the element $\pi_J^{\mathfrak{p}}(x(\mathfrak{p}))$ is divisible by $|J\cap I(\mathfrak{p})|$.

(iii) Fix subgroups H and H' of G and let Ω be a subset of $R_{L/K}$ with the property that, for all $\mathfrak{p}$ in Ω, one has $I(\mathfrak{p})=H$ and $G(\mathfrak{p})=H'$. Then, if $|\Omega|\geq 3$, there exists a $\mathbb{Z}_p[G/J]$-module direct summand of $H^1(J,U_{L,S})$ that is isomorphic to the direct sum of $|\Omega|-2$ copies of $(\mathbb{Z}/|J\cap H|)[G/JH']$.

Proof. By definition, $(P_{L,S})^J/P_{E,S}$ is a subset of $(I_{L,S})^J/P_{E,S}$. We can analyze $(I_{L,S})^J/P_{E,S}$ by the exact sequence

$$0\to A_{E,S}\to(I_{L,S})^J/P_{E,S}\xrightarrow{\psi}(I_{L,S})^J/I_{E,S}\to 0 \tag{2}$$

and the isomorphism of $\mathbb{Z}_p[G]$-modules

$$(I_{L,S})^J/I_{E,S}\cong(I_L)^J/I_E\cong\bigoplus\nolimits_{\mathfrak{p}\in R_{L/K}}(\mathbb{Z}/|J\cap I(\mathfrak{p})|)[G/JG(\mathfrak{p})] \tag{3}$$

in which each summand is generated by the class of $\mathfrak{p}_{L/E}$. The first isomorphism follows from the condition $S\cap R_{L/K}=\emptyset$. Claim (i) follows because $A_{E,S}$ is generated by $[\mathfrak{q}_E]_E$.

To prove claim (ii) we note that for any $\mathfrak{p}\in R_{L/K}$, any prime $\mathfrak{P}$ of L above $\mathfrak{p}$ and any natural number n, one has

$$\big(\textstyle\prod_{\sigma\in J/(J\cap G(\mathfrak{p}))}\sigma(\mathfrak{P})\big)^n\in I_E \iff n \text{ is divisible by } |J\cap I(\mathfrak{p})|.$$

In particular, since the action of G/J on $\mathfrak{p}_{L/E}$ factors through $\pi_J^{\mathfrak{p}}$, we have $\mathfrak{p}_{L/E}^{x(\mathfrak{p})}\in I_E$ if and only if $\pi_J^{\mathfrak{p}}(x(\mathfrak{p}))$ is divisible by $|J\cap I(\mathfrak{p})|$.

If $[\mathfrak{q}_E^m\prod_{\mathfrak{p}\in R_{L/K}}(\mathfrak{p}_{L/E})^{x(\mathfrak{p})}]'_E=0$, then the ideal $\mathfrak{q}_E^m\prod_{\mathfrak{p}\in R_{L/K}}(\mathfrak{p}_{L/E})^{x(\mathfrak{p})}$ represents an element of $\ker(\psi)$. Claim (ii) is thus a consequence of (3).

To prove claim (iii), we set $t:=|\Omega|$ and label the places in Ω as $\{\mathfrak{p}_i\}_{i\in[t]}$. We assume, after relabelling if necessary, that $[\mathfrak{p}_1]_L$ has maximum order (in $A_{L,S}$) amongst the elements $\{[\mathfrak{p}_i]_L\}_{i\in[t]}$. Then, for $j\in[t]\setminus\{1\}$, we fix $m(j)=m(L/K,j)\in\mathbb{Z}$ with $[\mathfrak{p}_j\cdot\mathfrak{p}_1^{-m(j)}]_L=0\in A_{L,S}$ so that

$$\mathfrak{p}_{1,j,E}:=\mathfrak{p}_{j,L/E}\cdot\mathfrak{p}_{1,L/E}^{-m(j)}\in\langle S\rangle_L P_L\cap(I_L)^J$$

defines an element of $H^1(J,U_{L,S})$. Such a linear relation exists because $A_{L,S}$ is cyclic. Next we note that, for $j\in[t]\setminus\{1\}$, there exists a unique ideal $\mathfrak{p}^*_{1,j,E}$ of E with $\mathfrak{p}_{1,j,E}^{|J\cap H|}=\mathfrak{p}^*_{1,j,E}\mathcal{O}_L$. After relabelling if necessary, we assume the order of $[\mathfrak{p}^*_{1,2,E}]_E$ (in $A_{E,S}$) is maximal amongst the orders of $\{[\mathfrak{p}^*_{1,j,E}]_E\}_{j\in[t]\setminus\{1\}}$ and then, for $k\in[t]\setminus\{1,2\}$, we fix

$$n(k)=n(L/K,E,k)\in\mathbb{Z} \tag{4}$$

with $[\mathfrak{p}^*_{1,k,E}(\mathfrak{p}^*_{1,2,E})^{-n(k)}]_E=0\in A_{E,S}$ by using the cyclicity of $A_{E,S}$. Setting for each $3\le k\le t$

$$\begin{aligned}\mathfrak{b}_{k,E}=\mathfrak{b}_{k,L/K,E}&:=\mathfrak{p}_{1,k,E}\cdot(\mathfrak{p}_{1,2,E})^{-n(k)}\\&=(\mathfrak{p}_{1,L/E})^{m(2)n(k)-m(k)}\cdot(\mathfrak{p}_{2,L/E})^{-n(k)}\cdot\mathfrak{p}_{k,L/E}\\&\in(I_L)^{JH'}\cap\langle S\rangle_LP_L\subseteq(I_L)^J\cap\langle S\rangle_LP_L\end{aligned}$$

one therefore has

$$|J\cap H|[\mathfrak{b}_{k,E}]'_E=[\mathfrak{p}^*_{1,k,E}(\mathfrak{p}^*_{1,2,E})^{-n(k)}\mathcal{O}_L]'_E=0. \tag{5}$$

In particular, since the $\mathfrak{p}_{k,L/E}$-component of the decomposition (3) is generated over $\mathbb{Z}_p[G/JH']$ by the image of $\mathfrak{b}_{k,E}$ under the map ψ in (2), the $\mathbb{Z}_p[G/J]$-submodule of $H^1(J,U_{L,S})$ generated by $[\mathfrak{b}_{k,E}]'_E$ is isomorphic to $(\mathbb{Z}/|J\cap H|)[G/JH']$.

Next we note that, setting $\Omega':=R_{L/K}\setminus\{\mathfrak{p}_i\}_{i\in[t]\setminus\{1,2\}}$, claim (i) implies every element of $H^1(J,U_{L,S})$ is represented by an ideal in $\langle S\rangle_LP_L\cap(I_L)^J$ of the form

$$\begin{aligned}&\big(\mathfrak{q}_E^m\textstyle\prod_{\mathfrak{p}\in\Omega'}(\mathfrak{p}_{L/E})^{x(\mathfrak{p})}\big)\times\big(\textstyle\prod_{k\in[t]\setminus\{1,2\}}(\mathfrak{b}_{k,E})^{x(k)}\big)\\&\qquad\qquad=\mathfrak{q}_E^m\textstyle\prod_{\mathfrak{p}\in\Omega'}(\mathfrak{p}_{L/E})^{x(\mathfrak{p})'}\textstyle\prod_{k\in[t]\setminus\{1,2\}}(\mathfrak{p}_{k,L/E})^{x(k)},\end{aligned} \tag{6}$$

for elements $x(k)$ of $\mathbb{Z}_p[G/J]$ and suitable integers m and elements $x(\mathfrak{p})$ of $\mathbb{Z}_p[G/J]$. Here, to ensure the equality, we have set

$$x(\mathfrak{p})' := \begin{cases} x(\mathfrak{p}) + \sum_{k\in[t]\setminus\{1,2\}}(m(2)n(k) - m(k))x(k), & \text{if } \mathfrak{p} = \mathfrak{p}_1; \\ x(\mathfrak{p}) - \sum_{k\in[t]\setminus\{1,2\}}n(k)x(k), & \text{if } \mathfrak{p} = \mathfrak{p}_2; \\ x(\mathfrak{p}), & \text{if } \mathfrak{p} \in \Omega' \setminus \{\mathfrak{p}_1, \mathfrak{p}_2\}. \end{cases}$$

Now, since the ideal (6) represents the trivial class in $A_{L,S}$, the first factor in the product on the left hand side must belong to the group

$$I^* := \langle S\rangle_L P_L \cap \{\mathfrak{q}_E^m \textstyle\prod_{\mathfrak{p}\in\Omega'}(\mathfrak{p}_{L/E})^{x(\mathfrak{p})} : m \in \mathbb{Z},\ \ x(\mathfrak{p}) \in \mathbb{Z}_p[G/J]\} \subseteq (I_L)^J.$$

We now write X and Y for the $\mathbb{Z}_p[G/J]$-submodules of $H^1(J, U_{L,S})$ that are respectively generated by the classes of ideals in I^* and $\{\mathfrak{b}_{k,E}\}_{k\in[t]\setminus\{1,2\}}$. Then, to prove the claim, it is enough to show that $H^1(J, U_{L,S})$ decomposes as a direct sum of $\mathbb{Z}_p[G/J]$-modules $X \oplus Y$ and that Y is isomorphic to a direct sum of $t-2$ copies of $(\mathbb{Z}/|J\cap H|)[G/JH']$.

To show this, it is in turn enough to assume the ideal (6) has trivial class in $H^1(J, U_{L,S})$, and thereby deduce every element $\pi_J^{\mathfrak{p}}(x(k))$ is divisible by $|J \cap H|$ and the ideal $\big(\mathfrak{q}_E^m \prod_{\mathfrak{p}\in\Omega'} \mathfrak{p}_{L/E}^{x(\mathfrak{p})}\big)$ has trivial class in $H^1(J, U_{L,S})$. The first condition follows directly upon applying claim (ii) to the right hand side of (6). Since this combines with (5) to imply $[\prod_{k\in[t]\setminus\{1,2\}}(\mathfrak{b}_{k,E})^{x(k)}]'_E = 0$, the vanishing of $[\mathfrak{q}_E^m \prod_{\mathfrak{p}\in\Omega'}(\mathfrak{p}_{L/E})^{x(\mathfrak{p})}]'_E$ then follows from the left hand expression in (6). □

4. Module structures

In this section, we fix a natural number n and a cyclic group Γ of order p^n, with generator σ. For $i \in [n]^*$, we write Γ_i for the subgroup of Γ generated by $\sigma^{p^{n-i}}$ (so that $|\Gamma_i| = p^i$).

We write Lat_n for the category of $\mathbb{Z}_p[\Gamma]$-lattices and fix a set of representatives $\mathcal{I}_n$ of the isomorphism classes of indecomposable $\mathbb{Z}_p[\Gamma]$-lattices that contains $\mathbb{Z}_p[\Gamma/\Gamma_i]$ for every $i \in [n]^*$.

4.1. **Yakovlev diagrams.**

We write $\mathfrak{M}_n$ for the category of diagrams

$$(A_\bullet, \alpha_\bullet, \beta_\bullet):\ A_1 \underset{\beta_1}{\overset{\alpha_1}{\leftrightarrows}} A_2 \underset{\beta_2}{\overset{\alpha_2}{\leftrightarrows}} \cdots \underset{\beta_{n-1}}{\overset{\alpha_{n-1}}{\leftrightarrows}} A_n$$

in which each A_i is a finite $(\mathbb{Z}/p^i)[\Gamma/\Gamma_i]$-module, and each α_i and β_i is a morphism of $\mathbb{Z}_p[\Gamma]$-modules such that $\beta_i \circ \alpha_i$ and $\alpha_i \circ \beta_i$ are respectively induced by multiplication by p and by the action of $\sum_{\gamma\in\Gamma_{i+1}/\Gamma_i}\gamma$. A morphism $(A_\bullet, \alpha_\bullet, \beta_\bullet) \to (A'_\bullet, \alpha'_\bullet, \beta'_\bullet)$ in $\mathfrak{M}_n$ is a collection of maps $\{\gamma_i : A_i \to A'_i\}_{i\in[n]}$ of $\mathbb{Z}_p[\Gamma]$-modules that commute with the respective maps $\alpha_\bullet, \beta_\bullet, \alpha'_\bullet, \beta'_\bullet$ (in particular, such a morphism is an isomorphism if and only if each map γ_i is bijective).

As a concrete example, each M in Lat_n gives an object

$$\Delta(M) = (A_\bullet, \alpha_\bullet, \beta_\bullet)$$

of $\mathfrak{M}_n$ in which each A_i is $H^1(\Gamma_i, M)$ and each α_i and β_i the natural restriction and corestriction maps. The importance of such examples is explained by the following result.

Proposition 4.1 (Yakovlev [20]). *The assignment $M \mapsto \Delta(M)$ induces a covariant essentially surjective functor $\Delta : \mathrm{Lat}_n \to \mathfrak{M}_n$. In addition, if $\Delta(M)$ and $\Delta(N)$ are isomorphic, then there are non-negative integers $\{m_i\}_{i\in[n]^*}$ and $\{m_i'\}_{i\in[n]^*}$ and an isomorphism in Lat_n of the form*

$$M \oplus \bigoplus\nolimits_{i\in[n]^*} \mathbb{Z}_p[\Gamma/\Gamma_i]^{m_i} \cong N \oplus \bigoplus\nolimits_{i\in[n]^*} \mathbb{Z}_p[\Gamma/\Gamma_i]^{m_i'}.$$

Remark 4.2. When combined with the Krull-Schmidt Theorem (for the category Lat_n), the final assertion of this result implies that if $\Delta(M)$ and $\Delta(N)$ are isomorphic, then any lattice in $\mathcal{I}_n$ that occurs (with a given multiplicity) as a direct summand of M is either $\mathbb{Z}_p[\Gamma/\Gamma_i]$ for some i or occurs (with the same multiplicity) as a direct summand of N. In particular, the isomorphism class of $\Delta(U_{L,S})$ in $\mathfrak{M}_n$ determines, uniquely up to isomorphism, a module $U^\dagger_{L,S}$ in Lat_n that has no direct summand isomorphic to $\mathbb{Z}_p[\Gamma/\Gamma_i]$ for any $i \in [n]^*$ and is such that for some (uniquely determined) set $\{t_i\}_{i\in[n]^*}$ of non-negative integers, there exists an isomorphism in Lat_n of the form

$$U_{L,S} \cong U^\dagger_{L,S} \oplus \bigoplus\nolimits_{i\in[n]^*} \mathbb{Z}_p[\Gamma/\Gamma_i]^{t_i}. \tag{7}$$

The next result presents an explicit example that will be useful in the next section.

Lemma 4.3. *Fix $a \in [n]$ and a non-negative integer b with $a + b \le n$ and set $c := n - (a + b)$.*

(i) If $b = 0$, then $M_{a,0} := \mathbb{Z}_p[\Gamma](\sigma^{p^c} - 1)$ is an indecomposable $\mathbb{Z}_p[\Gamma]$-lattice.

(ii) If $b \neq 0$, then $M_{a,b} := \mathbb{Z}_p[\Gamma](p^a, \sigma^{p^c} - 1)$ is an indecomposable $\mathbb{Z}_p[\Gamma]$-lattice.

(iii) For all a and b, the morphisms

$$H^1(\Gamma_i, M_{a,b}) \xrightarrow{\mathrm{res}} H^1(\Gamma_{i-1}, M_{a,b}) \xrightarrow{\mathrm{cor}} H^1(\Gamma_i, M_{a,b})$$

are equivalent to

$$\begin{cases} (\mathbb{Z}/p^i)[\Gamma/\Gamma_{a+b}] \to (\mathbb{Z}/p^{i-1})[\Gamma/\Gamma_{a+b}] \xrightarrow{\times p} (\mathbb{Z}/p^i)[\Gamma/\Gamma_{a+b}], & \textit{if } 1 < i \le a,\\ (\mathbb{Z}/p^a)[\Gamma/\Gamma_{a+b}] \xrightarrow{\mathrm{id}} (\mathbb{Z}/p^a)[\Gamma/\Gamma_{a+b}] \xrightarrow{\times p} (\mathbb{Z}/p^a)[\Gamma/\Gamma_{a+b}], & \textit{if } a < i \le a+b,\\ (\mathbb{Z}/p^a)[\Gamma/\Gamma_i] \xrightarrow{T_i} (\mathbb{Z}/p^a)[\Gamma/\Gamma_{i-1}] \to (\mathbb{Z}/p^a)[\Gamma/\Gamma_i], & \textit{if } a+b < i \le n. \end{cases}$$

Here the two unlabelled arrows are the natural projection maps and T_i sends each element γ of Γ/Γ_i to the sum in $(\mathbb{Z}/p^a)[\Gamma/\Gamma_{i-1}]$ of all elements of Γ/Γ_{i-1} that project to γ.

Proof. We set $I_{a,b} := \mathbb{Z}_p[\Gamma](p^a, \sigma^{p^c} - 1)$ (so that $I_{a,b} = M_{a,b}$ if $b \neq 0$). Then, in all cases, there is an exact sequence of $\mathbb{Z}_p[\Gamma]$-modules $0 \longrightarrow I_{a,b} \longrightarrow \mathbb{Z}_p[\Gamma] \longrightarrow (\mathbb{Z}/p^a)[\Gamma/\Gamma_{a+b}] \longrightarrow 0$. Upon taking Γ_i-cohomology of this sequence, one obtains an exact sequence of $\mathbb{Z}_p[\Gamma/\Gamma_i]$-modules

$$(\mathbb{Z}_p[\Gamma])^{\Gamma_i} \longrightarrow \big((\mathbb{Z}/p^a)[\Gamma/\Gamma_{a+b}]\big)^{\Gamma_i} \longrightarrow H^1(\Gamma_i, I_{a,b}) \longrightarrow 0.$$

A direct calculation using these sequences shows that the morphisms

$$H^1(\Gamma_i, I_{a,b}) \xrightarrow{\mathrm{res}} H^1(\Gamma_{i-1}, I_{a,b}) \xrightarrow{\mathrm{cor}} H^1(\Gamma_i, I_{a,b})$$

are equivalent to the morphisms in claim (iii). Since all of the $\mathbb{Z}_p[\Gamma]$-modules that occur in this description have cyclic Γ-coinvariants, Nakayama's lemma (for the local ring $\mathbb{Z}_p[\Gamma]$) implies that they are each indecomposable. Hence, as all occurring maps are non-zero, the diagram $\Delta(I_{a,b})$ must itself be indecomposable. In particular, if $I_{a,b}$ is decomposable, then it must have the form

$I_{a,b} = N_1 \oplus N_2$ for an indecomposable module N_1 with $\Delta(N_1) \cong \Delta(I_{a,b})$, and $H^1(\Gamma_i, N_2) = 0$ for all $i \in [n]^*$. Remark 4.2 then implies that N_2 is isomorphic to a direct sum $\bigoplus_{t\in[n]^*} \mathbb{Z}_p[\Gamma/\Gamma_t]^{m_t}$ for suitable integers m_t. Now, if $N_2 \neq (0)$, then, as $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} I_{a,b} = \mathbb{Q}_p[\Gamma]$, there exists a unique $s \in [n]^*$ for which $m_s = 1$ and $m_t = 0$ for all $t \in [n]^* \setminus \{s\}$ and so $I_{a,b} \cong N_1 \oplus \mathbb{Z}_p[\Gamma/\Gamma_s]$. This decomposition implies $\Sigma_s := \sum_{\gamma\in\Gamma_s}\gamma \in \mathbb{Z}_p[\Gamma]$ acts as the zero map on N_1 and hence that $I_{a,b}$ is preserved by the action of $p^{-s}\Sigma_s$. By explicit check, one finds this can only happen if $a = s$ and $b = 0$ so that $I_{a,b} = M_{a,0} \oplus \mathbb{Z}_p[\Gamma](\sum_{\gamma\in\Gamma_a}\gamma)$. In addition, $M_{a,0}$ is a cyclic module over the local ring $\mathbb{Z}_p[\Gamma]$ and so indecomposable. This verifies all of the stated claims. □

4.2. **The proof of Theorem 1.1.** We write $\mathcal{C}_n$ for the class of pairs $(L/K, S)$ comprising a cyclic extension L/K of number fields of degree p^n and a finite set S of places of K satisfying Hypothesis 2.1 and, for every $(L/K, S)$ in $\mathcal{C}_n$, we fix an identification of $G := G(L/K)$ with Γ. Before starting the proof of Theorem 1.1, we recall that Heller and Reiner [13] have shown $\mathcal{I}_n$, the set of indecomposable $\mathbb{Z}_p[\Gamma]$-lattices fixed before, to be infinite if $n > 2$ and note that, as $(L/K, S)$ ranges over $\mathcal{C}_n$, the rank $\mathrm{rk}(U_{L,S})$ is unbounded. Given these facts, the result of Theorem 1.1 is therefore, a priori, far from clear.

Turning now to its proof, we introduce some useful notation. Firstly, J and J' will henceforth always denote non-trivial subgroups of Γ (as the group $H^1(\{1\}, U_{L,S})$ vanishes and so plays no role in Yakovlev's theory); then, for subgroups $H \subseteq H'$ of Γ, and each $(L/K, S)$ in $\mathcal{C}_n$, we set

$$\Omega^{H,H'}_{L/K} := \{\mathfrak{p} \in R_{L/K} : I(\mathfrak{p}) = H, G(\mathfrak{p}) = H'\} \quad \text{and} \quad t^{H,H'}_{L/K} := |\Omega^{H,H'}_{L/K}|.$$

Then, assuming $t^{H,H'}_{L/K} > 2$, the argument of Proposition 3.2(iii) gives, for each subgroup J of Γ, and $k \in t^{H,H'}_{L/K} \setminus \{1, 2\}$, an ideal

$$\mathfrak{b}^{H,H'}_k(L/K, S, J) \in (I_L)^{JH'} \cap \langle S\rangle_L P_L \subseteq (I_L)^J \cap \langle S\rangle_L P_L$$

as follows: with $\mathfrak{b}^{H,H'}_k(L/K, S, H')$ denoting the ideal $\mathfrak{b}_{k,L^{H'}}$ constructed in the proof of Proposition 3.2(iii) for the case $\Omega = \Omega^{H,H'}_{L/K}$, we set

$$\mathfrak{b}^{H,H'}_k(L/K, S, J) = \begin{cases} \mathfrak{b}^{H,H'}_k(L/K, S, H') & \text{if } J \subseteq H', \\ \mathrm{Norm}_{L^{H'}/E}(\mathfrak{b}^{H,H'}_k(L/K, S, H')) & \text{if } H' \subsetneq J. \end{cases} \tag{8}$$

With these choices, for subgroups $J' < J$ with $|J/J'| = p$, one has

$$\prod\nolimits_{\sigma\in J/J'} \sigma(\mathfrak{b}^{H,H'}_k(L/K, S, J')) = \begin{cases} \mathfrak{b}^{H,H'}_k(L/K, S, J)^p & \text{if } J \subseteq H', \\ \mathfrak{b}^{H,H'}_k(L/K, S, J) & \text{if } H' \subsetneq J. \end{cases} \tag{9}$$

For each $J \leq \Gamma$, $H \subseteq H'$ with $|t^{H,H'}_{L/K}| > 2$ and $k \in [t^{H,H'}_{L/K}] \setminus \{1, 2\}$, we set

$$B^{H,H'}_k(L/K, S, J) := \mathbb{Z}_p[\Gamma/J][\mathfrak{b}^{H,H'}_k(L/K, S, J)]'_E \subseteq H^1(J, U_{L,S}).$$

Then, by the argument of Proposition 3.2(iii), the module $B_k^{H,H'}(L/K,S,J)$ is isomorphic to $(\mathbb{Z}/|J\cap H|)[\Gamma/JH']$ and there exists an isomorphism of $\mathbb{Z}_p[\Gamma/J]$-modules

$$H^1(J,U_{L,S})\cong C_J\oplus\bigoplus\nolimits_{(H,H')\in\Upsilon_{L/K}}\bigoplus\nolimits_{k\in[t_{L/K}^{H,H'}]\setminus\{1,2\}}B_k^{H,H'}(L/K,S,J). \tag{10}$$

Here $\Upsilon_{L/K}$ denotes the collection of pairs (H,H') of subgroups of Γ with $H\le H'$ and $t_{L/K}^{H,H'}>2$ and C_J is generated by the classes arising from (suitable) products of the conjugates of ideals in the set

$$\Omega^*_{L/K,S,J}:=\{\mathfrak{q}_E\}\cup\{\mathfrak{p}_{L/E}:\mathfrak{p}\in R_{L/K},(I(\mathfrak{p}),G(\mathfrak{p}))\notin\Upsilon_{L/K}\}\cup\{\mathfrak{p}_{L/E}:\mathfrak{p}\in\bigcup\nolimits_{(H,H')}\Omega_{H,H'}\}$$

where (H,H') runs over $\Upsilon_{L/K}$ and $\Omega_{H,H'}$ is a subset of $\Omega_{L/K}^{H,H'}$ of cardinality 2 (corresponding to the first two places in the ordering of $\Omega_{L/K}^{H,H'}$ fixed in the proof of Proposition 3.2(iii)).

Next we note that, with respect to the identification in Lemma 3.1, for subgroups $J'\le J$, the corestriction $H^1(J',U_{L,S})\to H^1(J,U_{L,S})$ and restriction $H^1(J,U_{L,S})\to H^1(J',U_{L,S})$ maps are respectively induced by the map $(I_L)^{J'}\to(I_L)^J$ sending each $\mathfrak{a}$ to $\prod_{\sigma\in J/J'}\sigma(\mathfrak{a})$ and by the inclusion $(I_L)^J\subseteq(I_L)^{J'}$. From (9), we can therefore deduce that, as J varies, the decompositions (10) respect the relevant restriction and corestriction maps and so induce a decomposition of Yakovlev diagrams

$$\Delta(U_{L,S})=\Delta_1(U_{L,S})\oplus\bigoplus\nolimits_{(H,H')\in\Upsilon_{L/K}}\bigoplus\nolimits_{k\in[t_{L/K}^{H,H'}]\setminus\{1,2\}}\Delta_k^{H,H'}(U_{L,S}),$$

where $\Delta_1(U_{L,S})$ is constructed from $\{C_J\}_{J\le\Gamma}$ and $\Delta_k^{H,H'}(U_{L,S})$ from $\{B_k^{H,H'}(L/K,S,J)\}_{J\le\Gamma}$. In addition, by comparing (9) to the result of Lemma 4.3(iii), one deduces that each diagram $\Delta_k^{H,H'}(U_{L,S})$ is isomorphic to $\Delta(M_{H,H'})$, with $M_{H,H'}:=M_{a,b}$ for integers a and b specified by $|H|=p^a$ and $|H'/H|=p^b$. The above decomposition is thus equivalent to an isomorphism

$$\Delta(U_{L,S})\cong\Delta_1(U_{L,S})\oplus\Delta\big(\bigoplus\nolimits_{(H,H')\in\Upsilon_{L/K}}(M_{H,H'})^{(t_{L/K}^{H,H'}-2)}\big) \tag{11}$$

in $\mathfrak{M}_n$. Finally we note that $|\Omega^*_{L/K,S,J}|\le 1+2B_n$ with B_n the number of subgroup pairs (H,H') of Γ and hence that the order of each (finite) group C_J is bounded by a number that depends only on p and n. Thus, as $(L/K,S)$ ranges over $\mathcal{C}_n$, the number of isomorphism classes of possible diagrams $\Delta_1(U_{L,S})$ is also bounded by a number depending only on p and n. Hence, by combining the isomorphism (11) with the observation in Remark 4.2, we can finally deduce that, as $(L/K,S)$ ranges over $\mathcal{C}_n$, the number of modules in $\mathcal{I}_n$ that can arise in the Krull-Schmidt decomposition of at least one of the lattices $U_{L,S}$ is finite. This completes the proof of Theorem 1.1.

4.3. **Some special cases.** There are at least two situations in which a closer analysis of the above argument can give more information. Firstly, if n is 'small', then the $\mathbb{Z}[\Gamma]$-module structures of terms in $\Delta(U_{L,S})$ are relatively simple and the categories Lat_n and $\mathfrak{M}_n$ are even completely understood for $n\in\{1,2\}$ (cf. [12] and [20, Th. 5] respectively). Hence, the argument of Proposition 3.2(iii) can sometimes give an effective means of obtaining the full Krull-Schmidt decomposition of $U_{L,S}$ (see [14] for results in this direction for cyclic extensions of degree dividing p^3). Secondly, if $H_{L,S}$ is a cyclic extension of K, then the argument in §4.2 can be simplified and leads to the following result.

Theorem 4.4. *Let L/K be a finite cyclic p-extension of number fields with $\mathrm{Norm}_{L/K}(\mu_L) = \mu_K$ and S a finite set of places of K such that $H_{L,S}/K$ is cyclic. Then the $\mathbb{Z}_p[G(L/K)]$-module structure of $U_{L,S}$ depends only on the ramification and inertia degrees of the places in $S \cup R_{L/K}$. In particular, if L/K is unramified and all places in S split completely in L, then there exists an isomorphism of $\mathbb{Z}_p[G(L/K)]$-modules*

$$U_{L,S} \cong \big(\mathbb{Z}_p[G(L/K)]/(\textstyle\sum_{g\in G(L/K)} g)\big) \oplus \mathbb{Z}_p[G(L/K)]^{(\mathrm{rk}(U_K)+|S|)}.$$

Proof. We assume $[L : K] = p^n$ and fix an identification $G(L/K) = \Gamma$. We also write $G(S)$ for the subgroup $\prod_{\tau\in S} G(\tau)$ of Γ that is generated by $\bigcup_{\tau\in S} G(\tau)$.

At the outset we note that, if $A_{L,S} \neq (0)$, then, as $H_{L,S}/K$ is a cyclic p-extension, L/K is unramified (so $R_{L/K} = \emptyset$), all places in S split completely in L and, for every intermediate field E of L/K, one has $H_{E,S} = H_{L,S}$. On the other hand, if $A_{L,S} = (0)$, then $H_{E,S}$ is the maximum unramified extension of E in L in which all places in S split completely.

Next we note that, since $(L/K, S)$ satisfies the hypothesis of Lemma 2.4, the results of Lemma 2.4(ii) and (iii) imply that $G(E/K)$ acts trivially on $A_{E,S}$ and that the (equivalence class of) transfer and norm maps between the respective groups $\{A_{E,S}\}_E$ are uniquely determined by the orders of each group $A_{E,S}$. In particular, in this way one finds that each transfer map $A_{E,S} \to A_{L,S}$ is surjective and that

$$|\ker(A_{E,S} \to A_{L,S})| = |(JG(S)\textstyle\prod_{\mathfrak{p}\in R_{L/K}} I(\mathfrak{p}))/(G(S)\prod_{\mathfrak{p}\in R_{L/K}} I(\mathfrak{p}))|.$$

In the remainder of the argument, we consider separately the cases $R_{L/K} \neq \emptyset$ and $R_{L/K} = \emptyset$. Thus, until further notice, we assume $R_{L/K} \neq \emptyset$. We write L' for the maximal unramified extension of K in L and set $\Gamma' := G(L/L')$ and $Z := U_{L,S}$. In this case one has $A_{L,S} = (0)$ and so the module $H^1(J, Z) = (P_{L,S})^J/P_{E,S} = (I_{L,S})^J/P_{E,S}$ lies in a canonical short exact sequence

$$0 \to A_{E,S} \to H^1(J, Z) \to (I_{L,S})^J/I_{E,S} \to 0 \qquad (12)$$

and $(I_{L,S})^J/I_{E,S} \cong (I_L)^J/I_E$ is explicitly known via the isomorphism (3).

For $\mathfrak{p} \in R_{L/K}$ we set $J_0(\mathfrak{p}) := J \cap I(\mathfrak{p})$ and $J_1(\mathfrak{p}) := J \cap G(\mathfrak{p})$. Then one has $\mathfrak{p}_{L/E}^{|J_0(\mathfrak{p})|} = \mathfrak{p}_E\mathcal{O}_L$, with $\mathfrak{p}_E = \mathfrak{p}_L \cap \mathcal{O}_E$ and so the element $|J_0(\mathfrak{p})|[\mathfrak{p}_{L/E}]'_E$ of $H^1(J, Z)$ is represented (via (12)) by the class $[\mathfrak{p}_E]_E \in A_{E,S} \subseteq H^1(J, Z)$. In addition, all of these classes $\{[\mathfrak{p}_E]_E\}$ are related to the single class $[\mathfrak{p}_{L(\mathfrak{p})}]_{L(\mathfrak{p})}$ with $L(\mathfrak{p}) = L^{G(\mathfrak{p})}$ by norm and transfer maps. If $J \subseteq I(\mathfrak{p})$, then $A_{E,S} = (0)$, if $I(\mathfrak{p}) \subseteq J \subseteq G(\mathfrak{p})$, then $\mathfrak{p}_E = \mathfrak{p}_{L(\mathfrak{p})}\mathcal{O}_E$ and if $G(\mathfrak{p}) \subseteq J$, then $\mathfrak{p}_E = \mathrm{Norm}_{L(\mathfrak{p})/E}(\mathfrak{p}_{L(\mathfrak{p})})$. For every E, the index in $A_{E,S}$ of the subgroup generated by $[\mathfrak{p}_E]_E$ is equal to

$$e(J, \mathfrak{p}) := (J\Gamma'G(S) : J_1(\mathfrak{p})\Gamma'G(S)).$$

Let us fix a place $\mathfrak{q} \notin R_{L/K} \cup S$ of K that is inert in $H_{L,S}$ and write $\mathfrak{q}_E$ for the place of E above $\mathfrak{q}$. Then, for each $\mathfrak{p} \in R_{L/K}$, Lemma 2.4(ii) implies there exists an integer $u(\mathfrak{p})$ that is prime to p and such that

$$[(\mathfrak{p}_{L/L(\mathfrak{p})})^{|I(\mathfrak{p})|u(\mathfrak{p})}]'_{L(\mathfrak{p})} = [\mathfrak{q}_{L(\mathfrak{p})}^{e(G(\mathfrak{p}),\mathfrak{p})}]'_{L(\mathfrak{p})} = [\mathfrak{q}_{L(\mathfrak{p})}]'_{L(\mathfrak{p})}.$$

In particular, by the preceding remark, for every E one has

$$[(\mathfrak{p}_{L/E})^{|J_0(\mathfrak{p})|u(\mathfrak{p})}]'_E = [\mathfrak{q}_E^{e(J,\mathfrak{p})}]'_E.$$

Now the argument of the proof of Proposition 3.2 (i) and (ii) implies $H^1(J,Z)$ is isomorphic to the $\mathbb{Z}[\Gamma/J]$-module W_J with generators $\{Y_J\} \cup \{X_{\mathfrak{p},J}\}_{\mathfrak{p}\in R_{L/K}}$ and relations

$$|A_{E,S}|Y_J,\ \sigma Y_J = Y_J,\ |J_0(\mathfrak{p})|X_{\mathfrak{p},J} = e(J,\mathfrak{p})Y_J,\ \sigma^{|\Gamma/(G(\mathfrak{p})J)|}X_{\mathfrak{p},J} = X_{\mathfrak{p},J}.$$

Furthermore, by the construction of $\{u(\mathfrak{p})\}_{\mathfrak{p}\in R_{L/K}}$ and $\{\mathfrak{q}_E\}_{J<\Gamma}$, these presentations of $H^1(J,Z)$ are compatible with varying J in the following sense. If J' is the subgroup of J of index p, then the restriction $H^1(J,Z)\to H^1(J',Z)$ and corestriction $H^1(J',Z)\to H^1(J,Z)$ maps correspond to the homomorphisms $\alpha_J : W_J \to W_{J'}$ and $\beta_J : W_{J'} \to W_J$ specified by

$$\alpha_J(Y_J) = Y_{J'} \quad \text{and} \quad \alpha_J(X_{\mathfrak{p},J}) = \begin{cases} X_{\mathfrak{p},J'} & \text{if } J \subseteq G(\mathfrak{p}) \\ T_{J/J'}(X_{\mathfrak{p},J'}) & \text{if } G(\mathfrak{p}) \subsetneq J, \end{cases}$$

$$\beta_J(Y_{J'}) = pY_J \quad \text{and} \quad \beta_J(X_{\mathfrak{p},J'}) = \begin{cases} pX_{\mathfrak{p},J} & \text{if } J \subseteq G(\mathfrak{p}) \\ X_{\mathfrak{p},J} & \text{if } G(\mathfrak{p}) \subsetneq J. \end{cases}$$

This analysis shows that the isomorphism class in $\mathfrak{M}_n$ of the diagram $\Delta(U_{L,S})$ depends only on the groups $I(\mathfrak{p})$ and $G(\mathfrak{p})$ for $\mathfrak{p}$ in $R_{L/K}$, and $G(S)$. Hence, recalling the decomposition (7), to determine the isomorphism class of Z itself, it is sufficient to determine the integers t_i. For $j\in[n]^*$, let s_j be the number of primes $\mathfrak{p}$ of S such that Γ_j is the decomposition subgroup in Γ of the place of L above $\mathfrak{p}$. Then one can determine the integers t_i by using the fact, for each $j\in[n]^*$, that

$$\begin{aligned} \mathrm{rk}\big(Z^{\Gamma_j}\big) - \mathrm{rk}\big(Z^{\Gamma_{j+1}}\big) &= \mathrm{rk}((Z^\dagger)^{\Gamma_j}) - \mathrm{rk}((Z^\dagger)^{\Gamma_{j+1}}) + (p^{n-j}-p^{n-j-1})\textstyle\sum_{i\in[j]^*} t_i \qquad (13)\\ &= (p^{n-j}-p^{n-j-1})(\mathrm{rk}(U_K) + 1 + \textstyle\sum_{i\in[j]^*} s_i) \end{aligned}$$

where the last equality follows by applying the Dirichlet-Herbrand Theorem to the $\mathbb{Q}_p[\Gamma]$-module $\mathbb{Q}_p\otimes_{\mathbb{Z}_p} U_{L,S}$ (cf. [6, Th. I.3.7]). Since the isomorphism class of $Z^\dagger$ is determined by $\Delta(U_{L,S})$, we can determine $\{t_i\}_{i\in[n]^*}$ recursively.

This establishes the claimed result in the case $R_{L/K}\neq\emptyset$ and so in the rest of the argument we assume $R_{L/K}=\emptyset$ (so that L/K is unramified). In this case, for a subgroup J of Γ one has $(I_{L,S})^J/I_{E,S} = (0)$ and so $H^1(J,Z)$ identifies with the kernel of the transfer map $A_{E,S}\to A_{L,S}$. By the observation made at the beginning of this proof, for each $i\in[n]^*$ the morphisms

$$H^1(\Gamma_i,Z) \xrightarrow{\mathrm{res}} H^1(\Gamma_{i-1},Z) \xrightarrow{\mathrm{cor}} H^1(\Gamma_i,Z)$$

are uniquely determined by $G(S)$. In particular, if all places of S split completely in L, then one has $H_{E,S} = H_{L,S}$ for all intermediate fields E of L/K and the above morphisms identify with $\mathbb{Z}/p^i \to \mathbb{Z}/p^{i-1} \to \mathbb{Z}/p^i$, where the first arrow is the natural projection map and the second sends 1 to p. Given this description, an easy exercise shows that $\Delta(Z)$ is isomorphic in $\mathfrak{M}_n$ to $\Delta(N)$ for the indecomposable $\mathbb{Z}_p[\Gamma]$-lattice $N := \mathbb{Z}_p[\Gamma]/(\sum_{\gamma\in\Gamma}\gamma)$. Just as above, it then follows that, for suitable (uniquely determined) integers $\{t_i\}_{i\in[n]^*}$, there is an isomorphism in Lat_n

$$Z \cong N \oplus \bigoplus\nolimits_{i\in[n]^*} \mathbb{Z}_p[\Gamma/\Gamma_i]^{t_i}.$$

In addition, the Dirichlet-Herbrand Theorem for S-units implies the existence of an isomorphism

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} Z \cong (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} N) \oplus \mathbb{Q}_p[\Gamma]^{(\mathrm{rk}(U_K)+|S|)}$$

of $\mathbb{Q}_p[\Gamma]$-modules. Upon comparing these isomorphisms, and noting $\mathbb{Q}_p[\Gamma]$ is semisimple, it follows that $t_i = 0$ for $i \neq 0$ and $t_0 = \mathrm{rk}(U_K) + |S|$. This implies the claimed isomorphism. □

5. Minkowski units

In this final section, we derive a consequence of Theorem 1.1 regarding the existence of independent Minkowski units (at p), as discussed in the Introduction.

To state the result, we use the family of field extensions $\mathcal{C}_n$ defined at the beginning of §4.2. For $(L/K, S)$ in $\mathcal{C}_n$ we recall, from the argument in §4.2, that $\Upsilon_{L/K}$ denotes the set of subgroup pairs of Γ that arise as $(I(\mathfrak{p}), G(\mathfrak{p}))$ for at least *three* distinct places in $R_{L/K}$ and we set

$$R^{(3)}_{L/K} := \{\mathfrak{p} \in R_{L/K} : (I(\mathfrak{p}), G(\mathfrak{p})) \in \Upsilon_{L/K}\}.$$

We also write $r_1(K)$ and $r_2(K)$ for the respective numbers of real and complex places of K, and $n_{S,L}$ for the number of places in S that split completely in L.

Corollary 5.1. *There exists a natural number $N_{p,n}$ that depends only on p and n and has the following property: for each $(L/K, S)$ in $\mathcal{C}_n$, one has*

$$m_{L/K,S} = r_1(K) + r_2(K) + n_{S,L} + (2|\Upsilon_{L/K}| - |R^{(3)}_{L/K}|) + d_{L/K,S}$$

with $|d_{L/K,S}| \leq N_{p,n}$.

Proof. The isomorphism (11) in $\mathfrak{M}_n$ implies the existence of a module $M_{L/K} = M_{L/K,S}$ in Lat_n for which there is an isomorphism (in Lat_n) of the form

$$U^{\dagger}_{L,S} \cong M_{L/K} \oplus \bigoplus\nolimits_{(H,H')\in\Upsilon_{L/K}} (M_{H,H'})^{(t^{H,H'}_{L/K}-2)}, \tag{14}$$

and one has $\mathrm{rk}(M_{L/K}) \leq N'_{p,n}$ for an integer $N'_{p,n}$ that depends only on p and n.

We first claim that, for each of the $\mathbb{Z}_p[\Gamma]$-lattices $M_{a,b}$ in Lemma 4.3, the corresponding $\mathbb{F}[\Gamma]$-module $M_{a,b}/pM_{a,b}$ does not contain $\mathbb{F}[\Gamma]$ as a direct summand. To see this, note $\mathrm{rk}(M_{a,b}) \leq p^n$ and so $M_{a,b}/pM_{a,b}$ can have a direct summand isomorphic to $\mathbb{F}[\Gamma]$ only if $M_{a,b} \cong \mathbb{Z}_p[\Gamma]$ and, since $M_{a,b}$ is not cohomologically-trivial, this is not true.

Hence, with t_0 the integer that occurs in (7), the isomorphism (14) implies that the non-negative integer $m_{L/K,S} - t_0$ is bounded above by the multiplicity of $\mathbb{F}[\Gamma]$ in $M_{L/K}/pM_{L/K}$. In particular, since $\mathrm{rk}(M_{L/K})$ is bounded solely in terms of p and n, there exists a natural number $N''_{p,n}$ that depends only on p and n and is such that $0 \leq m_{L/K,S} - t_0 \leq N''_{p,n}$.

Next we set $r_1 = r_1(K)$ and $r_2 = r_2(K)$ and note that the formula (13) (in which the term s_0 is equal to $n_{S,L}$) implies that

$$(p^n - p^{n-1})(r_1 + r_2 + n_{S,L}) = \mathrm{rk}(U^{\dagger}_{L,S}) - \mathrm{rk}\big((U^{\dagger}_{L,S})^{\Gamma_1}\big) + (p^n - p^{n-1})t_0. \tag{15}$$

In addition, for $(H, H') \in \Upsilon_{L/K}$, a straightforward computation (using the fact $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} I_{a,b} = \mathbb{Q}_p[\Gamma]$ for each of the lattices $I_{a,b}$ that occur in the proof of Lemma 4.3) shows that

$$\mathrm{rk}(M_{H,H'}) - \mathrm{rk}((M_{H,H'})^{\Gamma_1}) = p^n - p^{n-1}.$$

From the isomorphism (14), one therefore deduces that

$$\mathrm{rk}(U^{\dagger}_{L,S}) - \mathrm{rk}\big((U^{\dagger}_{L,S})^{\Gamma_1}\big) = d'_{L/K,S} + \sum\nolimits_{(H,H')\in\Upsilon_{L/K}} (p^n - p^{n-1})(t^{H,H'}_{L/K} - 2),$$

with $d'_{L/K,S} := \mathrm{rk}(M_{L/K}) - \mathrm{rk}(M^{\Gamma_1}_{L/K})$ (so that $0 \le d'_{L/K,S} \le N'_{p,n}$). Upon substituting this into (15), and dividing the resulting equality by $p^n - p^{n-1}$, one deduces that

$$\begin{aligned} t_0 &= r_1 + r_2 + n_{S,L} - \sum\nolimits_{(H,H')\in\Upsilon_{L/K}} (t^{H,H'}_{L/K} - 2) - d'_{L/K,S}/(p^n - p^{n-1}) \\ &= r_1 + r_2 + n_{S,L} + (2|\Upsilon_{L/K}| - |R^{(3)}_{L/K}|) - d'_{L/K,S}/(p^n - p^{n-1}), \end{aligned}$$

where the second equality is true since $\sum_{(H,H')\in\Upsilon_{L/K}} t^{H,H'}_{L/K} = |R^{(3)}_{L/K}|$, as follows from a direct comparison of the definitions of the terms $R^{(3)}_{L/K}$, $\Upsilon_{L/K}$ and $t^{H,H'}_{L/K}$.

The claimed result is therefore obtained by setting

$$d_{L/K,S} := -d'_{L/K,S}/(p^n - p^{n-1}) + (m_{L/K,S} - t_0)$$

and taking $N_{p,n}$ to be the integer part of $N'_{p,n}/(p^n - p^{n-1}) + N''_{p,n}$. □

In [11, §5], the authors construct families of Galois extensions in which Minkowski units (at p) can be shown to exist. We now finish this section by using Corollary 5.1 to describe new families of extensions in which there are many such Minkowski units. In particular, the following examples show that, for each n, the quantity $m_{L/K,S}$ is unbounded as $(L/K, S)$ ranges over $\mathcal{C}_n$. We remark that these examples are qualitatively different from those in [11] since the existence of Minkowski units is not being forced either by tame ramification or by large numbers of ramified places.

Examples 5.2. In order to show that $m_{L/K,S}$ is unbounded as $(L/K, S)$ ranges over $\mathcal{C}_n$ it is sufficient, by Corollary 5.1, to identify families of $(L/K, S)$ for which $|R_{L/K}|$ is bounded but $r_1(K) + r_2(K) + n_{S,L}$ is unbounded. In particular, for a fixed extension L/K, the quantity $n_{S,L}$, and hence also $m_{L/K,S}$, is clearly unbounded as one increases the set S. Of more interest, however, is the fact (evidenced by the following examples) that the required conditions are also satisfied in cases with $S = \emptyset$.

(i) Assume F has a unique p-adic place $\mathfrak{p}$ and $A_F = (0)$. Then, for the set $\Sigma = \{\mathfrak{p}\}$, $G_{F,\Sigma}$ is the inertia subgroup of the unique p-adic place of F_Σ (cf. Example 2.6). Hence, $\mathfrak{p}$ is totally ramified in F_Σ and $A_L = (0)$ for every finite extension L of F in F_Σ. The quantity $m_{L/K,\emptyset}$ is therefore unbounded as L/K ranges over intermediate fields of the tower F_Σ/F since each such extension is ramified precisely at the unique p-adic place. In addition, for each such L/K and a subgroup J of $G(L/K)$, $(P_L)^J/P_E \cong (I_L)^J/I_E$ is generated by the class of the prime of L above $\mathfrak{p}$. By the argument in §4.2, $\Delta(U_L) \cong \Delta(M_{n,0})$ for the lattice $M_{n,0}$ in Lemma 4.3. Hence, there is an isomorphism of $\mathbb{Z}_p[G(L/K)]$-modules

$$U_L \cong \big(\mathbb{Z}_p[G(L/K)]/(\textstyle\sum_{g\in G(L/K)} g)\big) \oplus \mathbb{Z}_p[G(L/K)]^{\mathrm{rk}(U_K)}.$$

(ii) Let p and q be distinct primes, with p odd and $q \equiv 1 \pmod{p}$. Then, if both $q \not\equiv 1 \bmod p^2$ and p is not a p-th power modulo q, the Burnside Basis Theorem implies that neither p nor q can split in the pro-p extension $\mathbb{Q}_{\{p,q\}}/\mathbb{Q}$. In this case, therefore, Corollary 5.1 implies that the quantity $m_{L/K,\emptyset}$ is unbounded in the family of cyclic extensions L/K with $L \subset \mathbb{Q}_{\{p,q\}}$ since each such extension is ramified at at most two places.

Remark 5.3. The mutual congruence conditions on p and q in Examples 5.2(iii) also arise in the theory of central extensions of number fields (cf. [4, Th. 5.2]). The following observation, which we have not been able to find in the literature, is thus also perhaps of interest beyond ensuring the existence of independent Minkowski units.

Proposition 5.4. *For each odd prime p, there are infinitely many primes $q \equiv 1 \pmod{p}$ such that both $q \not\equiv 1 \pmod{p^2}$ and p is not a p-th power modulo q.*

Proof. Set $E := \mathbb{Q}(\zeta_p, \sqrt[p]{p})$ and $F := \mathbb{Q}(\zeta_{p^2}, \sqrt[p]{p})$. Then, since E is a non-abelian Galois extension of $\mathbb{Q}$, the fields E and $\mathbb{Q}(\zeta_{p^2})$ are linearly disjoint over $\mathbb{Q}(\zeta_p)$ and so the group $G(F/\mathbb{Q}(\zeta_p))$ is isomorphic to $(\mathbb{Z}/p)^2$.

Let now q be a rational prime such that the Frobenius automorphism Fr_q in $G(F/\mathbb{Q})$ at a place of F above q is contained in $G(F/\mathbb{Q}(\zeta_p))$ but not in either $G(F/\mathbb{Q}(\zeta_{p^2}))$ or $G(F/E)$. Then one has $q \equiv 1 \pmod{p}$ as $\mathrm{Fr}_q \in G(F/\mathbb{Q}(\zeta_p))$ and also $q \not\equiv 1 \pmod{p^2}$ since $\mathrm{Fr}_q \notin G(F/\mathbb{Q}(\zeta_{p^2}))$. In particular, if p was a p-th power modulo q, then q would split completely in E and this is not possible since $\mathrm{Fr}_q \notin G(F/E)$, (To ensure consistency with [2, Rem. 6.23], we note the fact that p is not a p-th power modulo q can also be deduced from the Gras-Munnier Theorem [6, Th. V. 2.4.2]). □

REFERENCES

[1] M. F. Atiyah, C. T. C. Wall, ‘Cohomology of groups’, In Algebraic Number Theory, edited by J. W. S. Cassels and A. Fröhlich, 94-115, Academic Press, London, 1967.

[2] Z. Bouazzaoui, D. Lim, On the Galois structure of units in totally real p-rational number fields, New York J. Math. **31** (2025) 1439-1481.

[3] D. Burns, On the Galois structure of arithmetic cohomology I: Compactly supported p-adic cohomology, Nagoya Math. J. **239** (2020) 294-321.

[4] A. Fröhlich, Central extensions, Galois groups and ideal class groups of number fields, Contemp. Math. **24**, Amer. Math. Soc. Providence (1983).

[5] G. Gras, Les θ-régulateurs locaux d’un nombre algébrique: Conjectures p-adiques, Can. J. Math. **68** (2016) 571-624.

[6] G. Gras, Class field theory: from theory to practice, 2nd ed., Springer Monographs in Mathematics, Springer, Berlin, (2005).

[7] G. Gras, A. Munnier, Extensions cycliques T-totalement ramifiées, Publ. Math. Besançon. (1998) 1-17.

[8] F. Hajir, C. Maire, R. Ramakrishna, On tame $\mathbb{Z}/p\mathbb{Z}$-extensions with prescribed ramification, Can. Math. Bull. (2023) 1-9.

[9] F. Hajir, C. Maire, R. Ramakrishna, Deficiency of p-class tower groups and Minkowski units. Ann. Inst. Fourier. **75** (2025) 1415-1462.

[10] F. Hajir, C. Maire, R. Ramakrishna, On Ozaki's theorem realizing prescribed p-groups as p-class tower groups, Algebra & Number Theory **18** (2024) 771-786.

[11] F. Hajir, C. Maire, R. Ramakrishna, Cutting towers of number fields, Ann. Math. Québec **45** (2021) 321-345.

[12] A. Heller, I. Reiner, Representations of cyclic groups in rings of integers I, Ann. Math. **76** (1962) 73-92.

[13] A. Heller, I. Reiner, Representations of cyclic groups in rings of integers II, Ann. Math. (1963) 318-328.

[14] A. Kumon, D. Lim, On Krull-Schmidt decompositions of unit groups of number fields, Acta Arith. **218** (2025) 77-96.

[15] A. Movahhedi, Sur les p-extensions des corps p-rationnels, Math. Nach. **149** (1990) 163-176.

[16] A. Movahhedi, T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p-rationnels, Sem. Th. Nombres Paris 1987-88 (1990) 155-200.

[17] M. Ozaki, Construction of maximal unramified p-extensions with prescribed Galois groups, Invent. Math, **183** (2011) no.3, 649-680.

[18] C. Popescu, Base change for Stark-type Conjectures "over $\mathbb{Z}$", J. Reine Angew. Math. **542** (2002) 85-111.

[19] K. Wingberg, Galois groups of local and global type, J. Reine Angew. Math **517** (1999) 223-239.

[20] A. V. Yakovlev, Homological determinacy of p-adic representations of rings with power basis, Izv. Mat. **34** (1970) 1000-1014.

KING'S COLLEGE LONDON, DEPARTMENT OF MATHEMATICS, LONDON WC2R 2LS, U.K.
Email address: david.burns@kcl.ac.uk

DEPARTMENT OF MATHEMATICS EDUCATION, KOREA NATIONAL UNIVERSITY OF EDUCATION, CHEONGJU 28173, SOUTH KOREA
Email address: donghyeokklim@gmail.com

FEMTO-ST INSTITUTE, UNIVERSITÉ FRANCHE-COMTÉ, CNRS, 15B AVENUE DES MONTBOUCONS, 25000 BESANÇON, FRANCE
Email address: christian.maire@univ-fcomte.fr