New York Journal of Mathematics

New York J. Math. **31** (2025) 1439–1481.

# On the Galois structure of units in totally real $p$-rational number fields

**Zakariae Bouazzaoui and Donghyeok Lim**

ABSTRACT. The theory of factor-equivalence of integral lattices establishes a far-reaching relationship between the Galois module structure of the unit group of the ring of integers of a number field and its arithmetic. For a number field $K$ that is Galois over $\mathbb{Q}$ or an imaginary quadratic field, we prove a necessary and sufficient condition on the quotients of class numbers of subfields of $K$, for the quotient $E_K$ of the unit group of the ring of integers of $K$ modulo the subgroup of roots of unity to be factor equivalent to the standard cyclic Galois module. Using strong arithmetic properties of totally real $p$-rational number fields, we prove that the non-abelian $p$-rational $p$-extensions of $\mathbb{Q}$ do not admit Minkowski units, thereby extending a result of Burns to non-abelian number fields. We also study the relative Galois module structure of $E_L$ for varying Galois extensions $L/F$ of totally real $p$-rational number fields whose Galois groups are isomorphic to a fixed finite group $G$. In that case, we prove that there exists a finite set $\Omega$ of $\mathbb{Z}_p[G]$-lattices such that for every $L$, $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_L$ is factor equivalent to $\mathbb{Z}_p[G]^n \oplus X$ as $\mathbb{Z}_p[G]$-lattices for some $X \in \Omega$ and an integer $n \geq 0$.

CONTENTS



Received April 4, 2023.

2010 *Mathematics Subject Classification.* 11R33, 11R80.

*Key words and phrases.* $p$-rationality, Galois module structure of algebraic units, factor equivalence, regulator constant.

ISSN 1076-9803/2025

## 1. Introduction

Let $k$ be a number field that is either $\mathbb{Q}$ or an imaginary quadratic number field. For brevity, let us call such a number field *admissible* (cf. [12]). Let $K$ be a Galois extension of $k$ with Galois group $G_{K/k}$ such that the infinite places of $k$ are unramified in $K$. Let $\mathcal{O}_K$ be its ring of integers. In the late nineteenth century, Minkowski proved that there exists a unit in $\mathcal{O}_K$ whose conjugates over $k$ generate a full-rank subgroup of $\mathcal{O}_K^\times$. As a consequence of Minkowski's theorem, if we regard $\mathcal{O}_K^\times$ as a $\mathbb{Z}[G_{K/k}]$-module, then there is an isomorphism of $\mathbb{Q}[G_{K/k}]$-modules

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K^\times \simeq A_{G_{K/k}} := \mathbb{Q}[G_{K/k}]/(s_{G_{K/k}}).$$

For a finite group $G$, we write $s_G$ for the element $\sum_{g\in G} g$ in $\mathbb{Z}[G] \subset \mathbb{Q}[G]$, and write $(s_G)$ for the submodule generated by $s_G$.

Despite the long history of interest in $\mathcal{O}_K^\times$, the $\mathbb{Z}[G_{K/k}]$-module structure of $\mathcal{O}_K^\times$ is barely understood until now. One of the principal problems in this area is to determine if $K$ has a (strong) *Minkowski unit*, in other words, a unit $u \in \mathcal{O}_K^\times$ whose conjugates over $k$ generate $\mathcal{O}_K^\times$ modulo the subgroup $\mu(K)$ of roots of unity of $K$. The problem is equivalent to asking whether the *unit lattice* $E_K := \mathcal{O}_K^\times/\mu(K)$ is isomorphic to the *standard cyclic Galois module* $\mathcal{A}_{G_{K/k}} := \mathbb{Z}[G_{K/k}]/(s_{G_{K/k}})$ as $\mathbb{Z}[G_{K/k}]$-modules.

Studying the Galois module structure of the unit lattice is complicated for the following reasons. First of all, it is very difficult to compute a system of fundamental units. Therefore, number theorists tried to use arithmetic information on $K$ to study the cyclicity of $E_K$ as a $\mathbb{Z}[G_{K/k}]$-module. However, the involved arithmetic information is still difficult to obtain. Lastly, to be sure that certain arithmetic information suffices to guarantee that $E_K$ is cyclic, we need enough results on the classification of $\mathbb{Z}[G_{K/k}]$-lattices of the same rank as $E_K$. However, even for a finite group $G$ with a simple structure, classifying integral representations of $G$ is very difficult. Hence, studying the Galois module structure of the unit lattice requires knowledge of both the theory of integral representations of finite groups and the arithmetic of number fields. We examine both aspects of the problem in this paper, which is organized into 8 sections.

I. Representation-Theoretic Part (§2 – §5)

Several approaches have been introduced to study the integral Galois module structure of $E_K$. One approach is to study whether $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_K$ is isomorphic to $\mathbb{Z}_p[G_{K/k}]/(s_{G_{K/k}}) \simeq \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{A}_{G_{K/k}}$ as $\mathbb{Z}_p[G_{K/k}]$-modules for every prime $p$ (the problem of existence of *local* Minkowski units), by using the Krull-Schmidt theorem. This approach has limitations because there are many non-isomorphic indecomposable $\mathbb{Z}_p[G]$-lattices even for finite groups $G$ with simple structures. In this context, recall that two $\mathbb{Z}[G]$-lattices $M$ and $N$ are said to be genus equivalent if we have $\mathbb{Z}_p[G] \otimes_{\mathbb{Z}} M \simeq \mathbb{Z}_p[G] \otimes_{\mathbb{Z}} N$ for every prime $p$.

In the 1980s, A. Fröhlich and his students began to develop the theory of *factor equivalence* between integral lattices. This approach is computationally more effective because instead of studying each lattice, it focuses on comparing two lattices from the start. Although factor equivalence is weaker than genus equivalence, it nevertheless has profound applications in number theory, explaining how arithmetic influences the Galois module structure of the unit lattice for general Galois groups. Moreover, it was fruitful in yielding a necessary and sufficient condition for the existence of local Minkowski units, valid for all abelian extensions [12].

In the 2010s, A. Bartel revisited the connection between the integral Galois module structure of unit lattices and the arithmetic of number fields. In [1], Bartel used the *regulator constant* of integral lattices (cf. [24]) to obtain the most general Brauer-Kuroda type formula for dihedral extensions of number fields of degree $2p$ for an odd prime $p$. The regulator constant establishes a relationship between the Galois module structure of the unit lattice of a number field and a quotient of Dirichlet regulators of its subfields. In fact, the factor equivalence and the regulator constants are closely related. This connection is made precise by a theorem of Bartel [2, Cor. 2.12], which states that for a finite group $G$, two $\mathbb{Z}[G]$ lattices $\mathcal{M}$ and $\mathcal{N}$ with isomorphic self-dual rational representations are factor equivalent if and only if their regulator constants coincide for all $G$-relations (for the precise definition of $G$-relations, see Definition 3.13 and Example 3.14).

In the first part of this paper, we establish a formula for the regulator constants of $\mathcal{A}_G = \mathbb{Z}[G]/(s_G)$ (Proposition 4.1), which yields the following theorem.

**Theorem A.** Let $K$ be a number field that is Galois over an admissible field $k$ with Galois group $G_{K/k}$. Assume that $K/k$ is unramified at the infinite places of $k$. For each subgroup $H$ of $G_{K/k}$, let $h_{K^H}$ (resp. $w_{K^H}$) denote the class number (resp. the number of roots of unity) of the fixed field $K^H$. Define $\lambda(H)$ to be the order of the kernel of the map

$$H^1(H, \mu(K)) \to H^1(H, \mathcal{O}_K^\times)$$

induced by the embedding $\mu(K) \hookrightarrow \mathcal{O}_K^\times$. Then, $E_K$ is factor equivalent to $\mathcal{A}_{G_{K/k}}$ if and only if the equality

$$\prod_{H \leq G_{K/k}} \left( \frac{|H| \cdot h_{K^H} \cdot \lambda(H)}{w_{K^H}} \right)^{n_H} = 1$$

holds for every $G$-relation $\sum_{H \leq G_{K/k}} n_H H$ of $G_{K/k}$.

Theorem A generalizes the previously known necessary conditions on quotients of class numbers of subfields for the existence of Minkowski units, extending them to all non-cyclic finite groups.

## II. Arithmetic Part (§6 – §8)

Even for number fields of small degree, it is very difficult to obtain detailed information on unit lattices, since the relevant arithmetic invariants are challenging to analyze. In [12], Burns exploited strong arithmetic properties of $p$-power genus field extensions to study the existence of local Minkowski units in abelian $p$-extensions of admissible fields. In the second part of this work, we investigate the Galois module structure of the unit lattices for a new family of number fields, namely totally real *$p$-rational* number fields.

Let $p$ be an odd prime. A number field $F$ is called $p$-rational if the Galois group of the maximal pro-$p$ extension $F_{S_p}$ of $F$ that is unramified outside the set $S_p$ of $p$-adic primes is a free pro-$p$ group (cf. [58, 39]). Totally real $p$-rational number fields form an interesting class to work with. Their $p$-class numbers can be computed rather explicitly, a feature that is not often available in general and which makes it possible to carry out our theory in practice. Moreover, they give rise to infinitely many infinite non-abelian pro-$p$ towers, which not only allow us to study non-abelian cases but also provide a wealth of examples to which our results apply. In §7, we establish the following theorem on the non-existence of Minkowski units.

**Theorem B.** Let $p$ be an odd prime. If $F$ is a non-abelian $p$-rational $p$-extension of $\mathbb{Q}$, then $F$ does not have a local Minkowski unit.

Theorem B provides an infinite family of non-abelian number fields without Minkowski units. This result may be viewed as a non-abelian extension of Burns's theorem on the existence of local Minkowski units in $p$-power genus field extensions of admissible number fields (cf. [12, Thm. 5]).

We also study in §8 the relative Galois module structure of unit lattices for *varying* Galois extensions of totally real $p$-rational number fields with Galois group isomorphic to a *fixed* finite group $G$. Note that in this setting the base field is not required to be admissible. Since the $\mathbb{Z}$-rank of the unit lattice is unbounded as the extension varies, infinitely many non-isomorphic indecomposable $\mathbb{Z}_p[G]$-lattices can occur in the Krull-Schmidt decomposition of its $p$-adic completion.

In [14], Burns established that for every finite group $G$ and a finite set $S$ of primes of $\mathbb{Z}$ containing $p$, there exists a natural infinite family of relative Galois extensions $\mathscr{L}/\mathscr{K}$ with $\mathrm{Gal}(\mathscr{L}/\mathscr{K}) \simeq G$ in which the sum of the $\mathbb{Z}_p$-ranks of the non-projective indecomposable components in a Krull-Schmidt decomposition of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_{\mathscr{L},S}$ (as a $\mathbb{Z}_p[G]$-lattice) is uniformly bounded. Here, $E_{\mathscr{L},S}$ denotes the quotient of $S$-unit group $\mathcal{O}^{\times}_{\mathscr{L},S}$ of $\mathscr{L}$ by $\mu(\mathscr{L})$. It then follows from the Jordan-Zassenhaus theorem that only finitely many non-isomorphic indecomposable $\mathbb{Z}_p[G]$-lattices appear in the Krull-Schmidt decomposition of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_{\mathscr{L},S}$ for such extensions $\mathscr{L}/\mathscr{K}$ belonging to this family.

In §8, we observe a similar phenomenon in the relative Galois module structure of the group of *ordinary* units when the number fields are totally real and $p$-rational.

**Theorem C.** Let $G$ be a finite group. Then, there exists a finite set $\Omega$ of $\mathbb{Z}_p[G]$-lattices such that for every relative Galois extension $\mathscr{L}/\mathscr{K}$ of totally real $p$-rational number fields with $\mathrm{Gal}(\mathscr{L}/\mathscr{K}) \simeq G$, there exists $X \in \Omega$ and a non-negative integer $m$ such that $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_{\mathscr{L}}$ is factor equivalent to $X \oplus \mathbb{Z}_p[G]^m$ as $\mathbb{Z}_p[G]$-lattices.

The arithmetic of a totally real $p$-rational number field becomes particularly simple when there is a unique $p$-adic prime (cf. §6.2). In this case, Theorem C can be sharpened. We now make this setting more precise.

Let $p$ be an odd prime, and let $F$ be a totally real $p$-rational number field. Fix a finite non-$p$-adic prime $\mathfrak{q}$ of $F$ that does not split in the cyclotomic $\mathbb{Z}_p$-extension $F_\infty/F$. Denote by $F_{S_p\cup\{\mathfrak{q}\}}$ (resp. $F_{\{\mathfrak{q}\}}$) the maximal pro-$p$ extension of $F$ unramified outside $S_p \cup \{\mathfrak{q}\}$ (resp. unramified outside $\mathfrak{q}$). We remark that $\mathrm{Gal}(F_{S_p\cup\{\mathfrak{q}\}}/F)$ is a Demuškin group of rank 2, while $F_{\{\mathfrak{q}\}}/F$ is finite. For a finite group $G$, we denote by $I_G$ the augmentation ideal of the group ring $\mathbb{Z}[G]$.

**Theorem D.** Suppose that $p$ does not split in $F_{S_p\cup\{\mathfrak{q}\}}$. Then, for every Galois extension $\mathscr{L}/\mathscr{K}$ of number fields satisfying

$$F_{\{\mathfrak{q}\}} \subseteq \mathscr{K} \subseteq \mathscr{L} \subset F_{S_p\cup\{\mathfrak{q}\}}$$

with Galois group $G$, the lattice $E_{\mathscr{L}}$ is factor equivalent to

$$\mathcal{A}_G \oplus I_G \oplus \mathbb{Z} \oplus \mathbb{Z}[G]^{[\mathscr{K}:\mathbb{Q}]-2}$$

as $\mathbb{Z}[G]$-lattices.

## Notations

For a finite group $G$, let $s_G := \sum_{g\in G} g$ denote the trace element, $I_G$ the augmentation ideal, and $\mathcal{A}_G := \mathbb{Z}[G]/(s_G)$ the standard cyclic $\mathbb{Z}[G]$-module. We write $G^{\mathrm{ab}}$ for the abelianization of $G$, and $(G : H)$ for the index of $H$ in $G$ for every subgroup $H$ of $G$. For an abelian group $A$, $\mathrm{rk}_p(A)$ denotes its $p$-rank. If $X$ is a $G$-set, $X^G$ is the subset fixed by $G$. For a natural number $n$, $|n|_p$ denotes its $p$-part, and for $x \in \mathbb{Q}^\times$, $v_p(x)$ denotes the $p$-adic valuation. Finally, all modules over a ring $R$ are understood to be left $R$-modules.

For an extension $L/K$ of number fields, we write $\mathrm{Ram}(L/K)$ for the set of places of $K$ that ramify in $L$. If $L/K$ is Galois, we denote $G_{L/K} := \mathrm{Gal}(L/K)$. For a number field $F$, we let $h_F$ denote its class number, $w_F$ the number of roots of unity in $F$, and $R_F$ its Dirichlet regulator. If $v$ is a place of $F$, then $F_v$ denotes the completion of $F$ at $v$.

In the sections devoted to $p$-rationality, we adopt the following notation. We fix an odd prime $p$ and denote by $\mathfrak{h}_F$ the $p$-class number of a number field $F$. We write $F_\infty$ for its cyclotomic $\mathbb{Z}_p$-extension, $F_n$ for the $n$-th layer of $F_\infty/F$, and $H_F$ for the Hilbert $p$-class field of $F$. We also let $S_p$ denote the set of $p$-adic places

of a number field. Since the base field will always be clear from the context, this notation will cause no ambiguity.

In addition, we introduce the following notation, which will be used frequently in §6.2 and §7. For a finite set $S$ of places of $F$, we write $F_S$ for the maximal pro-$p$ extension of $F$ unramified outside $S$. If $\mathfrak{q}$ is a non-$p$-adic prime of $F$, we set:

- $\mathfrak{q}_L$ : the unique prime above $\mathfrak{q}$ in an extension $F \subset L \subset F_{S_p\cup\{\mathfrak{q}\}}$ (when $F$ is $p$-rational and $S_p \cup \{\mathfrak{q}\}$ is primitive for $(F, p)$, see Lemma 6.15);
- $L^{\mathrm{el}}_{p,\mathfrak{q}}$ : the maximal elementary abelian $p$-extension of $L$ contained in $F_{S_p\cup\{\mathfrak{q}\}}$ (in the same setting as above);
- $p_L$ : the unique prime of $L$ above $p$ for $F \subset L \subset F_{S_p\cup\{\mathfrak{q}\}}$ (when $p$ does not split in $F_{S_p\cup\{\mathfrak{q}\}}$);
- $\mathcal{J}_{L,\upsilon}$ : the inertia subgroup of $G_{L^{\mathrm{el}}_{p,\mathfrak{q}}/L}$ at $\upsilon$ (see the discussion preceding Lemma 7.6).

**Acknowledgements**

We would like to thank David Burns for his helpful discussion and encouragement, Abbas Movahhedi for pointing out an error on $p$-rationality in the first version of the paper, and Christian Maire for Remark 6.23. We also would like to thank Jilali Assim, Zouhair Boughadi, Asuka Kumon, El Boukhari Saad, Bouchaïb Sodaïgui, and Youness Mazigh for their interest in this work and helpful comments. The revision of this paper was carried out while D. Lim was a visiting researcher at FEMTO-ST in Besançon in 2023 and during his visit to the Institute for Advanced Studies in Mathematics (IASM) in Harbin Institute of Technology in 2025. D. Lim would like to thank both institutions for their friendly environment. Finally, we would like to thank the anonymous referee for his or her patience over a long period and for the sharp and constructive comments, which greatly enhanced the overall quality of the paper. In particular, we are grateful for the valuable mathematical suggestions regarding Section 4.

**Funding**

D. Lim was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. NRF-2022R1I1A1A01071431). He was also supported by the Core Research Institute Basic Science Research Program through the National Research Foundation of Korea(NRF), funded by the Ministry of Education (Grant No. 2019R1A6A1A11051177).

## 2. Genus equivalence

Throughout this section, let $k$ be an admissible field and $K/k$ a Galois extension of number fields in which the infinite places of $k$ are unramified. Since the

$\mathbb{Z}[G_{K/k}]$-module structure of $E_K$ is difficult to study (cf. [10, 53]), it is natural to first examine the $\mathbb{Z}_p[G_{K/k}]$-module structure of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_K$ for all primes $p$. For a Dedekind domain $R$ and a finite group $G$, a finitely generated $R[G]$-module that is torsion-free as an $R$-module is called an $R[G]$-*lattice*.

**Definition 2.1.** Two $R[G]$-lattices $M$ and $N$ are said to be *genus equivalent* if for every non-zero prime $\mathfrak{p}$ of $R$, we have

$$R_{\mathfrak{p}} \otimes_R M \simeq R_{\mathfrak{p}} \otimes_R N$$

as $R_{\mathfrak{p}}[G]$-modules, where $R_{\mathfrak{p}}$ denotes the completion of $R$ at $\mathfrak{p}$.

If $p$ does not divide $|G_{K/k}|$, then we have

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} E_K \simeq \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{A}_{G_{K/k}}$$

by representation theory (cf. [63, §15.5]). Therefore, the study of the genus equivalence class of $E_K$ concerns only those primes $p$ dividing $|G_{K/k}|$.
A $\mathbb{Z}_p[G]$-lattice is said to be *indecomposable* if it is not a direct sum of two proper $\mathbb{Z}[G]$-sublattices. The Krull-Schmidt theorem is available for $\mathbb{Z}_p[G]$-lattices.

**Theorem 2.2.** *(cf.* [19, p. 83]*) Let $M$ be a $\mathbb{Z}_p[G]$-lattice, and suppose that*

$$M \simeq U_1 \oplus \cdots \oplus U_m \simeq V_1 \oplus \cdots \oplus V_n$$

*are two decompositions of $M$ into indecomposable $\mathbb{Z}_p[G]$-sublattices. Then, we have $m = n$, and after a suitable reindexing we have $U_i \simeq V_i$ as $\mathbb{Z}_p[G]$-lattices for every $1 \leq i \leq m$.*

Therefore, if we classify the indecomposable $\mathbb{Z}_p[G_{K/k}]$-lattices of $\mathbb{Z}_p$-rank at most $|G_{K/k}|$, then *in principle*, we can study the $\mathbb{Z}_p[G_{K/k}]$-module structure of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_K$ by computing the multiplicity of each indecomposable $\mathbb{Z}_p[G_{K/k}]$-lattice in the Krull-Schmidt decomposition of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_K$.

**Example 2.3.**

(i) If $G$ is cyclic of order $p$, then by a theorem of Diederichsen, there are precisely three isomorphism classes of indecomposable $\mathbb{Z}_p[G]$-lattices [22]. From this, we can easily check the genus equivalence of $E_K$ and $\mathcal{A}_{G_{K/k}}$ for every cyclic extension $K/k$ of prime degree.

(ii) When $G$ is the elementary abelian $p$-group $(\mathbb{Z}/p\mathbb{Z})^2$ of rank 2, Payan, Bouvier, and Duval classified indecomposable $\mathbb{Z}_p[G]$-lattices that can be realized as $\mathbb{Z}_p[G]$-sublattices of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_K$ for some Galois extensions $K/k$ with Galois group $G_{K/k} \simeq G$ (cf. [8, 26, 27]). In [27], Duval used these results to study the genus equivalence of $E_K$ and $\mathcal{A}_{G_{K/k}}$ in the case $G_{K/k} \simeq (\mathbb{Z}/p\mathbb{Z})^2$.

(iii) Assume that $G_{K/k}$ is a metacyclic group of the form $\mathbb{Z}/p\mathbb{Z} \rtimes T$, where $T$ is a cyclic group whose order divides $p-1$. Marszalek obtained necessary and sufficient conditions for the genus equivalence of $E_K$ and $\mathcal{A}_{G_{K/k}}$ for the case when the action of $T$ on $\mathbb{Z}/p\mathbb{Z}$ is faithful by using the classification of integral representations [54, 55]. The interested readers can also refer to [43, 44].

The study of the genus equivalence class of $E_K$ has not been extended to more general Galois groups, because the classification of the indecomposable integral representations is highly complicated, even for groups with simple structures.

**Remark 2.4.** (i) In [41, 42], Heller and Reiner studied the indecomposable $\mathbb{Z}_p[\mathbb{Z}/p^e\mathbb{Z}]$-lattices for $e \geq 2$. In [41], they proved that there are precisely $4p+1$ non-isomorphic indecomposable representations of $\mathbb{Z}/p^2\mathbb{Z}$ over $\mathbb{Z}_p$. However, there are infinitely many non-isomorphic indecomposable representations over $\mathbb{Z}_p$ if $e$ is larger than 2 [42]. There has been no attempt to classify indecomposable $\mathbb{Z}_p[\mathbb{Z}/p^3\mathbb{Z}]$-lattices even for small $\mathbb{Z}_p$-ranks.

(ii) Duval obtained a necessary and sufficient condition for the genus equivalence between $E_K$ and $\mathcal{A}_{G_{K/k}}$ only in the cases $p = 2$ or 3 for $G_{K/k} \simeq (\mathbb{Z}/p\mathbb{Z})^2$, as the classification was too difficult and incomplete for larger $p$. For an illustration of the difficulty of classifying integral representations of $(\mathbb{Z}/p\mathbb{Z})^2$ over $\mathbb{Z}_p$, see the table on page 241 of [27], which is far from exhaustive for general $p$.

## 3. Factor equivalence, theorems of Burns and regulator constant

In this section, we explain basic concepts in the theory of factor equivalence and its application to the Galois module structure of unit lattices. We then present some basic results on the regulator constants. Lastly, we explain the connection between factor equivalence and regulator constants.

**3.1. Factor equivalence of integral lattices.** Throughout this section, let $K$ be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$. We write $\mathcal{O}_K$ for its ring of integers and $\mathrm{Id}_K$ for its group of fractional ideals. For a finite group $G$, denote by $\mathcal{S}(G)$ the set of subgroups of $G$.

As in the theory of genus equivalence, the theory of factor equivalence [59] compares two $\mathcal{O}_K[G]$-lattices $\mathcal{M}$ and $\mathcal{N}$ such that we have $K \otimes_{\mathcal{O}_K} \mathcal{M} \simeq K \otimes_{\mathcal{O}_K} \mathcal{N}$ as $K[G]$-modules. From such a $K[G]$-isomorphism, one obtains an injective $\mathcal{O}_K[G]$-module homomorphism $\iota : \mathcal{M} \to \mathcal{N}$. The relation of factor equivalence of $\mathcal{M}$ and $\mathcal{N}$ is defined in terms of the *factorisability* of a natural function associated with $\iota$. We therefore begin by introducing the notion of factorisability of general functions from $\mathcal{S}(G)$ to an abelian group $X$.

**Definition 3.1.** (cf. [2, 16, 21]) Let $G$ be a finite group and $X$ be an abelian group written multiplicatively. A function $f : \mathcal{S}(G) \to X$ is said to be factorisable if there exists an injection of abelian groups $\psi : X \hookrightarrow Y$ for some $Y$ and a function $g : \mathrm{Irr}(G) \to Y$ defined on a full set $\mathrm{Irr}(G)$ of isomorphism classes of irreducible complex characters of $G$ such that

$$\psi(f(H)) = \prod_{\chi \in \mathrm{Irr}(G)} g(\chi)^{\langle \chi, \mathbb{C}[G/H] \rangle}$$

holds for all $H \in \mathcal{S}(G)$, where $\langle \chi, \mathbb{C}[G/H] \rangle$ denotes the multiplicity of $\chi$ in the representation $\mathbb{C}[G/H]$.

In [11, 12, 30], Fröhlich and Burns focused on the case when $G$ is abelian. In this situation, the factorisability of a function $f : \mathcal{S}(G) \longrightarrow X$ can be studied via its *factorisable quotient* $\tilde{f}$. For a finite abelian group $G$, define a binary relation on $G$ by declaring $x, y \in G$ to be related if and only if they generate the same cyclic subgroup of $G$. This defines an equivalence relation, and we call each equivalence class $D$ a *division* of $G$. Given a function $f : \mathcal{S}(G) \longrightarrow X$, we associate a function $f'$ on the set of divisions of $G$ with values in $X$ by

$$f'(D) := \prod_{C<\overline{D}} f(C)^{\mu((\overline{D}:C))},$$

where $\overline{D}$ denotes the subgroup of $G$ generated by any element $x \in D$, and $\mu$ is the Möbius function. We define the factorisable quotient $\tilde{f} : \mathcal{S}(G) \longrightarrow X$ of $f$ by

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

for every $H \in \mathcal{S}(G)$. It is known that for general $f$, one always has $\tilde{f}(H) = 1$ for all cyclic subgroups $H$ of $G$. We have the following proposition.

**Proposition 3.2.** *([29, 30]) Let $G$ be a finite abelian group and $f : \mathcal{S}(G) \to X$ a function from $\mathcal{S}(G)$ to an abelian group $X$. Then $f$ is factorisable if and only if we have $\tilde{f}(H) = 1$ for all subgroups $H$ of $G$.*

With the notion of factorisability of a function, we can define the factor equivalence between two $\mathcal{O}_K[G]$-lattices.

**Definition 3.3.** Let $\mathcal{M}, \mathcal{N}$ and $\iota : \mathcal{M} \to \mathcal{N}$ be as in the beginning of this subsection. Two lattices $\mathcal{M}$ and $\mathcal{N}$ are said to be factor equivalent if the function from $\mathcal{S}(G)$ to the group $\mathrm{Id}_K$ defined by

$$H \longrightarrow [\, \mathcal{N}^H : \iota(\mathcal{M}^H)\,]_{\mathcal{O}_K}$$

is factorisable, where $[\, \mathcal{N}^H : \iota(\mathcal{M}^H)\,]_{\mathcal{O}_K} \in \mathrm{Id}_K$ denotes the order ideal (cf. [19, §80]) of the $\mathcal{O}_K$-torsion module $\mathcal{N}^H/\iota(\mathcal{M}^H)$.

**Remark 3.4.** (cf. [21, Prop. 2.5]) We record the following basic facts:

(i) The definition of factor equivalence does not depend on the choice of $\iota$.
(ii) The factor equivalence is an equivalence relation.

The following fact is well-known, but we provide a proof for the readers' convenience.

**Lemma 3.5.** *Let $\mathcal{M}$ and $\mathcal{N}$ be two $\mathcal{O}_K[G]$-lattices. If they are genus equivalent, then they are factor equivalent.*

**Proof.** There is a canonical isomorphism $\mathrm{Id}_K \simeq \bigoplus_{\mathfrak{p}} \mathrm{Id}_{K_\mathfrak{p}}$ where $\mathfrak{p}$ runs over the maximal ideals of $\mathcal{O}_K$. Under this isomorphism, the ideal $[\, \mathcal{N}^H : \iota(\mathcal{M}^H)\,]_{\mathcal{O}_K}$ corresponds to the element

$$\left( [\, (\mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{N})^H : (1\otimes\iota)((\mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{M})^H)\,]_{\mathcal{O}_{K_\mathfrak{p}}} \right)_{\mathfrak{p}} \in \bigoplus_{\mathfrak{p}} \mathrm{Id}_{K_\mathfrak{p}}.$$

Hence, $\mathcal{N}$ and $\mathcal{M}$ are factor equivalent if and only if $\mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{N}$ and $\mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{M}$ are factor equivalent for all maximal ideals $\mathfrak{p}$. The latter can be checked by applying Remark 3.4 (i) to the isomorphic $\mathcal{O}_{K_\mathfrak{p}}[G]$-lattices $\mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{M}$ and $\mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{N}$. □

Applying the theory of factor equivalence to arithmetic Galois modules has proved fruitful, with one lattice taken to be an arithmetic object and the other a standard (module-theoretic) lattice, as illustrated by the following examples (cf. [21, 30]).

**Example 3.6.** (i) For a Galois extension $L/K$ of number fields, the normal basis theorem gives an isomorphism

$$K \otimes_{\mathcal{O}_K} \mathcal{O}_L \simeq K[G_{L/K}] \simeq K \otimes_{\mathcal{O}_K} \mathcal{O}_K[G_{L/K}]$$

of $K[G_{L/K}]$-modules. Hence it is natural to study the factor equivalence between $\mathcal{O}_L$ and $\mathcal{O}_K[G_{L/K}]$.

(ii) Let $L/K$ be a Galois extension of number fields, and let $S$ be a finite set of places of $L$ containing the set $S_{L,\infty}$ of all the archimedean places of $L$. Assume that $S$ is invariant under the action of $G_{L/K}$. Let $X_S$ denote the free abelian group generated by $S$, and let $Y_S$ be the kernel of the augmentation map $X_S \to \mathbb{Z}$, which maps each element of $S$ to 1. By the generalized Dirichlet-Herbrand theorem on $S$-units (cf. [35, Thm. I.3.7]), the multiplicative group $\mathcal{O}_{L,S}^\times$ of $S$-units of $L$ satisfies an isomorphism

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_{L,S}^\times \simeq \mathbb{Q} \otimes_{\mathbb{Z}} Y_S$$

of $\mathbb{Q}[G_{L/K}]$-modules. Therefore, we can study the factor equivalence between $E_{L,S} := \mathcal{O}_{L,S}^\times/\mu(L)$ and $Y_S$. We remark that if $L$ is a Galois extension over an admissible field $k$ where no infinite places of $k$ are ramified, then $Y_{S_{L,\infty}}$ is isomorphic to the augmentation ideal $I_{G_{L/k}}$ as $\mathbb{Z}[G_{L/k}]$-lattices.

**3.2. Theorems of Burns.** As in §3.1, let $K$ be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$. When $G$ is a finite abelian group, Burns [11] investigated when the factor equivalence of two $\mathcal{O}_K[G]$-lattices implies the genus equivalence. Building on this, in [12], he obtained a necessary and sufficient condition for the genus equivalence of $E_L$ and $\mathcal{A}_{G_{L/k}}$, valid for all abelian extensions $L/k$ of admissible number fields $k$ unramified at the infinite places. In this subsection, we briefly explain these results, assuming throughout that $G$ is abelian and that $L/k$ is an abelian extension of an admissible field unramified at the infinite places.

**3.2.1. Arithmetic criteria for the existence of local Minkowski units in Abelian extensions.** Let $\mathcal{A}$ be a $K$-algebra that is a quotient of $K[G]$, and let $X$ be an $\mathcal{O}_K[G]$-lattice such that $\mathcal{A}$ acts on $K \otimes_{\mathcal{O}_K} X$. We then set

$$\mathfrak{A}(\mathcal{A}, X) := \{\, \lambda \in \mathcal{A} \mid \lambda \cdot X \subseteq X \,\}.$$

Suppose now that $K \otimes_{\mathcal{O}_K} X$ is a subrepresentation of the regular representation $K[G]$. Then it is necessarily cyclic as a $K[G]$-module by the semisimplicity of $K[G]$. Since $G$ is abelian, the action of $K[G]$ factors through the unique quotient $K$-algebra $K(X)$ of $K[G]$. The induced action of $K(X)$ on $K \otimes_{\mathcal{O}_K} X$ is faithful. Consequently, $\mathfrak{A}(K(X), X)$ is an $\mathcal{O}_K$-order in $K(X)$, called the *associated order* of $X$ in $K(X)$.

A normal subgroup $H$ of $G$ is called cocyclic (written $H <_c G$) if the quotient $G/H$ is cyclic. Burns introduced another equivalence relation on $\mathcal{O}_K[G]$-lattices called the *order-equivalence*.

**Definition 3.7.** (cf. [11, §2], [12, §1]) Two $\mathcal{O}_K[G]$-lattices $X$ and $Y$ are said to be order-equivalent (written $X \circ Y$) if for every cocyclic subgroup $H$ of $G$ one has

$$\mathfrak{A}(K[G/H], X^H) = \mathfrak{A}(K[G/H], Y^H).$$

Let $\mathfrak{M}_{K,G}$ denote the maximal $\mathcal{O}_K$-order in $K[G]$, and for every $\mathcal{O}_K[G]$-lattice $M$, let $M^{\mathfrak{M}_{K,G}}$ denote the maximal $\mathfrak{M}_{K,G}$-module contained in $M$. We also write $\hat{G}$ for the group of characters of $G$. For each subgroup $H$ of $G$, we let $H^\perp$ denote the subgroup of $\hat{G}$ consisting of characters that are trivial on $H$.

Given $\mathcal{O}_K[G]$-lattices $X$ and $Y$ with $K \otimes_{\mathcal{O}_K} X \simeq K \otimes_{\mathcal{O}_K} Y$ as $K[G]$-modules, we define the *defect function* (cf. [11, p. 260], [29, (1.16)])

$$J(X, Y) : \mathcal{S}(\hat{G}) \to \mathrm{Id}_K.$$

For every subgroup $H^\perp$ of $\hat{G}$, it is given by

$$J(X, Y)(H^\perp) = \frac{[X^H : (X^{\mathfrak{M}_{K,G}})^H]_{\mathcal{O}_K}}{[Y^H : (Y^{\mathfrak{M}_{K,G}})^H]_{\mathcal{O}_K}}.$$

The defect function is important in the works of Fröhlich and Burns, since $X$ and $Y$ are factor equivalent if and only if $J(X, Y)$ is factorisable (cf. [29, (1.17) in p. 411]). Using the order-equivalence, Burns proved the following theorem.

**Theorem 3.8.** *(cf.* [11, Thm. 2]*) Let $K$ be a field of one of the following types:*

(*i*) *a number field in which no prime divisor of $|G|$ ramifies in $K/\mathbb{Q}$, or*
(*ii*) *an absolutely unramified local field, i.e. a finite unramified extension of $\mathbb{Q}_p$.*

*Let $X$ be an $\mathcal{O}_K[G]$-lattice such that $K \otimes_{\mathcal{O}_K} X$ is isomorphic to a quotient $Q$ of $K[G]$, and let $\mathfrak{A} = \mathfrak{A}(Q, X)$ be the associated order of $X$ in $Q$. Then, $X$ and $\mathfrak{A}$ are genus equivalent if and only if both $X \circ \mathfrak{A}$ and $\widetilde{J(X, \mathfrak{A})}(\hat{G}) = \mathcal{O}_K$ hold, where $\widetilde{J(X, \mathfrak{A})}$ denotes the factorisable quotient of the defect function $J(X, \mathfrak{A})$.*

**Remark 3.9.** The original formulation of Theorem 3.8 in [11, Thm. 2] is stated with $G$-$\circ$-equivalence in place of order equivalence. Since order equivalence implies $G$-$\circ$-equivalence while genus equivalence implies order equivalence, the present formulation, as used also in [12], follows directly from Theorem 2 of [11].

We now return to the setting of local Minkowski units. Recall that $L/k$ is an abelian extension of an admissible field unramified at the infinite places. One easily checks that $\mathbb{Q} \otimes_{\mathbb{Z}} E_L$ is a subrepresentation of $\mathbb{Q}[G_{L/k}]$, and that $\mathbb{Q}(E_L) = A_{G_{L/k}}$ (the specialization of $K(X)$ with $K = \mathbb{Q}, X = E_L$).

At first sight, Theorem 3.8 appears to relate $E_L$ to $\mathfrak{A}(A_{G_{L/k}}, E_L)$, which contains $\mathcal{A}_{G_{L/k}}$. However, its significance lies in showing that certain arithmetic necessary conditions for the genus equivalence of $E_L$ and $\mathcal{A}_{G_{L/k}}$ are actually sufficient.

The arithmetic necessary conditions are expressed in terms of the factorisable quotients of two functions

$$h_{L/k}, w_{L/k} : \mathcal{S}(\widehat{G_{L/k}}) \longrightarrow \mathbb{N},$$

where $\widehat{G_{L/k}}$ denotes the character group of $G_{L/k}$. They are defined by

$$h_{L/k}(H^\perp) := \mathrm{lcm}(\, h_{L^H}, |G_{L/k}|\,), \qquad w_{L/k}(H^\perp) := \mathrm{lcm}(\, w_{L^H}, |G_{L/k}|\,)$$

for every $H^\perp \in \mathcal{S}(\widehat{G_{L/k}})$. Here, $\mathrm{lcm}(a, b)$ denotes the least common multiple of $a, b \in \mathbb{N}$. Recall that $h_{L^H}$ (resp. $w_{L^H}$) stands for the class number (resp. the number of roots of unity) of $L^H$. For each abelian group $G$, define

$$\tilde{\mathfrak{F}}_G := \Big(\prod_p p^{J_p}\Big) \cdot |G|^{-1},$$

where, for every prime $p$, we write $J_p$ for the number of non-trivial divisions of the $p$-Sylow subgroup of $G$.

**Theorem 3.10.** *(*[12, Thm. 3]*) Let $k$ be an admissible field. Let $L/k$ be an abelian extension unramified at the infinite places. Then, $E_L$ is genus equivalent to $\mathcal{A}_{G_{L/k}}$ if and only if we have both*

$$\tilde{h}_{L/k}(\widehat{G_{L/k}}) = \tilde{w}_{L/k}(\widehat{G_{L/k}}) \cdot \tilde{\mathfrak{F}}_{G_{L/k}},$$

*and $\hat{H}^0(H, E_L) = 1$ for every cocyclic subgroup $H$ of $G_{L/k}$.*

A noteworthy feature of this theorem is that it applies to all abelian Galois groups, since its proof does not rely on the classification of integral representations of $G_{L/k}$ over $\mathbb{Z}_p$. The functions $h_{L/k}$ and $w_{L/k}$ are related to the factor equivalence of $E_L$ and the lattice $Y_{S_{L,\infty}}$ introduced in Example 3.6 (ii) (cf. [21, Thm. 5.2], [30, Thm. 7 (Multiplicative)]). The invariant $\tilde{\mathfrak{F}}_G$ appears when considering the factor equivalence of $\mathcal{A}_G$ and $I_G$ (cf. [12, page 75], [29]). Since $Y_{S_{L,\infty}}$ is isomorphic to $I_{G_{L/k}}$, this accounts for the appearance of these quantities in Theorem 3.10.

**3.2.2. Applications of the arithmetic criteria to genus field extensions.** The existence of local Minkowski units in a general Galois extension cannot

be settled by representation-theoretic considerations alone. Since the arithmetic of general extensions is highly intricate, it is necessary to apply the arithmetic criteria in special cases where the number fields enjoy suitable arithmetic properties. Using Theorem 3.10 together with the theory of central class fields (cf. [28]), Burns proved the existence of local Minkowski units for certain abelian $p$-extensions of admissible fields. This subsection briefly reviews these results and explains how they motivate our approach.

Throughout this subsection, let $k$ be an admissible field and $p$ a prime that does not divide $h_k w_k$. Following [12], an abelian $p$-extension $L$ of $k$ is called a *$p$-power genus field extension* if we have

$$G_{L/k} = \bigoplus_{v \in \mathrm{Ram}(L/k)} I_{L/k,v},$$

where $I_{L/k,v}$ denotes the inertia subgroup of $G_{L/k}$ at $v$. By a formula of Furuta [31], $L$ is a $p$-power genus field extension of $k$ if and only if $p$ does not divide the genus number of $L$ over $k$.

To state Burns's theorem, we recall some notation from [66]. For each finite place $v$ of $k$, let $\mathfrak{p}_v$ denote the maximal ideal of the valuation ring $\mathcal{O}_{k_v}$ for the local field $k_v$, and write $\mathbf{N}\mathfrak{p}_v \in \mathbb{N}$ for its ideal norm. Let $h_v$ be the smallest positive integer such that the $h_v$-th power of the prime ideal of $k$ corresponding to $v$ is principal, and fix a generator $\pi_v$ of this principal ideal.

If $v$ does not divide $p$, fix an element $x_v \in \mathcal{O}_{k_v}^{\times}$ whose class in the residue field $\kappa_v := \mathcal{O}_{k_v}/\mathfrak{p}_v$ generates the multiplicative group $\kappa_v^{\times}$. If $v$ divides $p$ and $I_{L/k,v}$ is cyclic, then fix $x_v \in \mathcal{O}_{k_v}^{\times}$ whose class in

$$\mathcal{O}_{k_v}^{\times}/N_{L_w/k_v}\mathcal{O}_{L_w}^{\times} \simeq I_{L/k,v}$$

generates the group, where $w$ is a fixed prime of $L$ above $v$. For $x \in \mathcal{O}_{k_v}^{\times}$, define

$$[\,v, x\,] = \begin{cases} m \bmod (\mathbf{N}\mathfrak{p}_v - 1) & \text{if } v \nmid p \text{ and } x \equiv x_v^m \pmod{\mathfrak{p}_v} \\ s \bmod |I_{L/k,v}| & \text{if } v \mid p,\ I_{L/k,v} \text{ is cyclic, and } x \equiv x_v^s \pmod{N_{L_w/k_v}\mathcal{O}_{L_w}^{\times}} \end{cases}$$

For finite places $v, v' \in \mathrm{Ram}(L/k)$, we consider $\pi_{v'} \in k^{\times}$ as an element of $\mathcal{O}_{k_v}$ and evaluate $[v, \pi_{v'}]$. Although $x_v$ and $\pi_v$ are chosen arbitrarily, this choice does not affect the $p$-divisibility of $[v, \pi_{v'}]$.

In [28, 66], for an admissible field $k$ and a prime $p \nmid h_k w_k$, the $p$-power genus field extensions $L$ of $k$ with $p \nmid h_L$ were completely characterized in terms of the set $\mathrm{Ram}(L/k)$ and the $p$-divisibility of $[v_i, \pi_{v_j}]$ for $v_i, v_j \in \mathrm{Ram}(L/k)$ (cf. [12, Thm. 4]). Building on this, Burns [12] gave a complete characterization of the existence of local Minkowski units in such $L$.

As a preliminary remark, note that if $L$ is a $p$-power degree genus field extension of $k$ with $p \nmid h_L$ and $\mathrm{rk}_p(G_{L/k}) \leq 2$, then we have $|\mathrm{Ram}(L/k)| = \mathrm{rk}_p(G_{L/k})$ (cf. [12, Thm. 4.(b)]). In particular, the group $I_{L/k,v}$ is cyclic for every $v \in \mathrm{Ram}(L/k)$.

**Theorem 3.11.** *([12, Thm. 5]) Let $k$ be an admissible field. Let $p$ be a prime not dividing $h_k w_k$. Let $L$ be a $p$-power degree genus field extension of $k$ with $p \nmid h_L$. Then $E_L$ and $\mathcal{A}_{G_{L/k}}$ are genus equivalent if and only if one of the following holds:*

*(i)* $\mathrm{Ram}(L/k) = \{v_1\}$*, and the group $G_{L/k}$ is cyclic;*
*(ii)* $\mathrm{Ram}(L/k) = \{v_1, v_2\}$*, the $p$-rank of $G_{L/k}$ is 2, and both $[v_1, \pi_{v_2}]$ and $[v_2, \pi_{v_1}]$ are not divisible by $p$.*

**Remark 3.12.** Consider the case $k = \mathbb{Q}$ with $p$ an odd prime. By class field theory, $I_{L/\mathbb{Q},v}$ is cyclic for every prime $v$ and every abelian $p$-extension $L/\mathbb{Q}$. Since $\mathbb{Q}$ has class number 1, we may take $\pi_q = q$ for each rational prime $q$. It is known (cf. [12, page 86]) that:

(i) $[\, p, q\,]$ is divisible by $p$ if and only if $q \equiv 1 \pmod{p^2}$, and
(ii) $[\, q, p\,]$ is divisible by $p$ if and only if $p$ is a $p$-th power residue modulo $q$.

Let $L$ be a $p$-power genus field extension of $\mathbb{Q}$ ramified precisely at $p$ and $q$. If $[\, p, q\,]$ is not divisible by $p$, then $h_L$ is prime to $p$ by a theorem of Fröhlich (cf. [12, Thm. 4.(b)]). In this case, $L$ is moreover $p$-rational (cf. Corollary 6.10).

In §6 we shall extend Theorem 3.11 to *non-abelian* $p$-extensions of $\mathbb{Q}$ unramified outside $p$ and $q$ such that $[\, p, q\,]$ is not divisible by $p$.

**3.3. Factor equivalence and regulator constants.** In this subsection, we present basic properties of the regulator constant that will be useful in later sections. We also recall the theorem of Bartel on the relationship between the theory of factor equivalence and the theory of regulator constants.

**3.3.1. Basic facts on regulator constants.** Let $G$ be a finite group and $\mathcal{R}$ a principal ideal domain with field of fractions $\mathcal{K}$. Throughout this subsection, we assume that $\mathcal{K}$ has characteristic prime to $|G|$. The regulator constant $\mathcal{C}_\Theta(\mathcal{M})$ is an element of $\mathcal{K}^\times/\mathcal{R}^{\times 2}$, defined for every pair $(\mathcal{M}, \Theta)$ of a $G$-relation $\Theta$ and an $\mathcal{R}[G]$-lattice $\mathcal{M}$ such that $\mathcal{K} \otimes_{\mathcal{R}} \mathcal{M}$ is a self-dual representation of $G$ over $\mathcal{K}$. The theory of regulator constant was introduced by Tim and Vladimir Dokchitser in [25] and has played a central role in several subsequent works.

**Definition 3.13.** A formal sum $\Theta = \sum_{H \leq G} n_H H$ of subgroups $H$ of $G$ with coefficients $n_H \in \mathbb{Z}$ is called a $G$-relation if there is an isomorphism

$$\bigoplus_{\substack{H \leq G \\ n_H < 0}} \mathbb{Q}[G/H]^{-n_H} \simeq \bigoplus_{\substack{H \leq G \\ n_H > 0}} \mathbb{Q}[G/H]^{n_H}$$

of $\mathbb{Q}[G]$-modules.

The set of $G$-relations forms a subgroup of the free abelian group $\mathbb{Z}[\mathcal{S}(G)]$ over the set $\mathcal{S}(G)$ of subgroups of $G$. Its $\mathbb{Z}$-rank is known to equal the number of conjugacy classes of non-cyclic subgroups of $G$ (cf. [63, §13.1, Thm. 30]).

**Example 3.14.** (i) If $G$ is cyclic, then there are no non-trivial $G$-relations.

(ii) If $G$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ for a prime $p$, then the group of $G$-relations is generated over $\mathbb{Z}$ by the $G$-relation

$$1 + p \cdot G - \sum_H H,$$

where $H$ runs over the subgroups of $G$ of order $p$, and 1 denotes the trivial subgroup.

**Definition 3.15.** ([24, Rem. 2.27]) Let $\mathcal{R}, \mathcal{K}, G$, and $\mathcal{M}$ be as above. Let $\langle \cdot, \cdot \rangle : \mathcal{M} \times \mathcal{M} \longrightarrow \mathcal{L}$ be a $\mathcal{R}$-bilinear, $G$-invariant pairing that is non-degenerate, with values in some extension $\mathcal{L}$ of $\mathcal{K}$. Let $\Theta = \sum_{H \leq G} n_H H$ be a $G$-relation. The regulator constant $\mathcal{C}_\Theta(\mathcal{M})$ of $\mathcal{M}$ with respect to $\Theta$ is defined by

$$\mathcal{C}_\Theta(\mathcal{M}) = \prod_{H \leq G} \det\left( \frac{1}{|H|} \langle \cdot, \cdot \rangle \big|_{\mathcal{M}^H} \right)^{n_H} \in \mathcal{L}^\times / \mathcal{R}^{\times 2},$$

where each determinant is taken with respect to any $\mathcal{R}$-basis of $\mathcal{M}^H$.

**Remark 3.16.**
(i) It is known that $\mathcal{C}_\Theta(\mathcal{M})$ is independent of the particular choice of pairing (cf. [24, Thm. 2.17]). Since $\mathcal{K} \otimes_\mathcal{R} \mathcal{M}$ is self-dual, there exists a non-degenerate $G$-invariant $\mathcal{K}$-bilinear pairing on $\mathcal{K} \otimes_\mathcal{R} \mathcal{M}$ with values in $\mathcal{K}$. Therefore, $\mathcal{C}_\Theta(\mathcal{M})$ is in fact defined in $\mathcal{K}^\times / \mathcal{R}^{\times 2}$.
(ii) When $\mathcal{R}$ is equal to $\mathbb{Z}$, the regulator constants $\mathcal{C}_\Theta(\mathcal{M})$ take values in $\mathbb{Q}^\times$ because $\mathcal{R}^{\times 2}$ is trivial.
(iii) The rational representations of the form

$$\bigoplus_{H \leq G} \mathbb{Q}[G/H]^{a_H}, \qquad (a_H \in \mathbb{N})$$

are called *permutation representations*. It is known that permutation representations are self-dual (cf. [1, §3]). Therefore, the regulator constant can be used to study $\mathbb{Z}[G]$-lattices whose rational representations are isomorphic to $A_G \oplus \mathbb{Q}[G]^m$ for $m \geq 0$, where $A_G$ denotes the representation $\mathbb{Q}[G]/(s_G)$.
(iv) The readers can also refer to [1, §3] and [13, Lem. 4.3] for other conceptual formulations of the regulator constant.

The following lemma is immediate from the definition.

**Lemma 3.17.** *Let $\Theta$ and $\Theta'$ be $G$-relations, and let $\mathcal{M}$ and $\mathcal{M}'$ be $\mathcal{R}[G]$-lattices whose rational representations are self-dual. Then we have*

$$\mathcal{C}_\Theta(\mathcal{M} \oplus \mathcal{M}') = \mathcal{C}_\Theta(\mathcal{M}) \cdot \mathcal{C}_\Theta(\mathcal{M}'), \qquad \mathcal{C}_{\Theta+\Theta'}(\mathcal{M}) = \mathcal{C}_\Theta(\mathcal{M}) \cdot \mathcal{C}_{\Theta'}(\mathcal{M}).$$

The following properties of $G$-relations and the regulator constants will be useful.

**Lemma 3.18.** *([24, Exam. 2.30]) If $\sum_{H \leq G} n_H H$ is a $G$-relation, then we have $\sum_{H \leq G} n_H = 0$.*

**Lemma 3.19.** *(*[24, Lem. 2.46], [65, Rem. 3.2]*) If $H$ is a cyclic subgroup of $G$, then we have*

$$\mathcal{C}_\Theta(\mathcal{R}[G/H]) = 1$$

*for every $G$-relation $\Theta$.*

For a finite group $G$, there are two natural ways to construct $G$-relations from those of its subgroups and quotient groups.

(i) Let $H$ be a subgroup of $G$ and let $\Theta = \sum_{H' \leq H} n_{H'} H'$ be an $H$-relation. Then, $\Theta$ is also a $G$-relation, which we denote by $\mathrm{Ind}_H^G \Theta$.

(ii) Let $B$ be a normal subgroup of $G$ and set $G' = G/B$. Suppose $\Theta' = \sum_{B \leq H \leq G} a_{H/B}(H/B)$ is a $G'$-relation. Then,

$$\sum_{B \leq H \leq G} a_{H/B} H$$

is a $G$-relation, called the *inflation* of $\Theta$, and is denoted by $\mathrm{Inf}_{G'}^G \Theta'$.

If $\mathcal{M}$ is an $\mathcal{R}[G']$-lattice, then $\mathcal{M}$ can be viewed as an $\mathcal{R}[G]$-lattice via the natural projection $G \to G'$. We denote this $\mathcal{R}[G]$-lattice by $\mathrm{Inf}_{G'}^G \mathcal{M}$. Similarly, if $\mathcal{N}$ is an $\mathcal{R}[G]$-lattice and $H \leq G$, we denote by $\mathrm{Res}_H^G \mathcal{N}$ the corresponding $\mathcal{R}[H]$-lattice obtained by restriction. Then, we have the following proposition.

**Proposition 3.20.** *(*[24, Prop. 2.45]*) The following statements hold:*

*(i) Let $G$ be a finite group and $G'$ a quotient of $G$. For every $G'$-relation $\Theta'$ and every $\mathcal{R}[G']$-lattice $\mathcal{M}$ with self-dual rational representation, we have*

$$\mathcal{C}_{\mathrm{Inf}_{G'}^G \Theta'}(\mathrm{Inf}_{G'}^G \mathcal{M}) = \mathcal{C}_{\Theta'}(\mathcal{M}).$$

*(ii) Let $H$ be a subgroup of $G$. For every $H$-relation $\Theta$ and every $\mathcal{R}[G]$-lattice $\mathcal{N}$ with self-dual rational representation, we have*

$$\mathcal{C}_{\mathrm{Ind}_H^G \Theta}(\mathcal{N}) = \mathcal{C}_\Theta(\mathrm{Res}_H^G \mathcal{N}).$$

**Proof.** Let $\langle\,,\,\rangle$ be a $G'$-invariant $\mathcal{R}$-bilinear non-degenerate pairing on $\mathcal{M}$. Then $\langle\,,\,\rangle$ is also a $G$-invariant non-degenerate pairing on $\mathrm{Inf}_{G'}^G \mathcal{M}$. The first equality follows from computing both regulator constants with $\langle\,,\,\rangle$. The second equality can be checked similarly by using a $G$-invariant $\mathcal{R}$-bilinear pairing on $\mathcal{N}$ as an $H$-bilinear pairing on $\mathrm{Res}_H^G \mathcal{N}$. □

Lastly, we mention a result on $v_p(\mathcal{C}_\Theta(\mathcal{M}))$ for rational primes $p$ when $\mathcal{R}$ is equal to $\mathbb{Z}$.

**Proposition 3.21.** *(*[1, Prop. 3.9]*) Suppose that $\mathcal{R}$ is equal to $\mathbb{Z}$. Let $G$ be a finite group and $B$ be a normal subgroup of $G$ such that the quotient group $C = G/B$ is cyclic. Let $p$ be a prime not dividing $|B|$. Then, we have $v_p(\mathcal{C}_\Theta(\mathcal{M})) = 0$ for every $G$-relation $\Theta$ and every $\mathbb{Z}[G]$-lattice $\mathcal{M}$ whose rational representation is self-dual.*

**3.3.2. Theorems of Bartel.** The regulator constant yields a new criterion to verify the factor equivalence of two $\mathbb{Z}[G]$-lattices.

**Theorem 3.22.** *([2, Cor. 2.12]) Let $G$ be a finite group. Let $\mathcal{M}$ and $\mathcal{N}$ be two $\mathbb{Z}[G]$-lattices with the same self-dual rational representation. Then, $\mathcal{M}$ and $\mathcal{N}$ are factor equivalent if and only if we have*

$$\mathcal{C}_\Theta(\mathcal{M}) = \mathcal{C}_\Theta(\mathcal{N})$$

*for all $G$-relations $\Theta$.*

The factor equivalence of two lattices can be studied locally, as shown in the following proposition.

**Proposition 3.23.** *Let $G$ be a finite group and $p$ a prime. Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathbb{Z}[G]$-lattices as in Theorem 3.22. Then, $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{M}$ and $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{N}$ are factor equivalent as $\mathbb{Z}_p[G]$-lattices if and only if we have*

$$v_p(\mathcal{C}_\Theta(\mathcal{M})) = v_p(\mathcal{C}_\Theta(\mathcal{N}))$$

*for all $G$-relations $\Theta$.*

**Proof.** For an injective $\mathbb{Z}[G]$-morphism $\iota\colon \mathcal{M} \to \mathcal{N}$ and a $G$-relation $\Theta = \sum_{H\le G} n_H H$, we have

$$\mathcal{C}_\Theta(\mathcal{M})/\mathcal{C}_\Theta(\mathcal{N}) = \prod_{H\le G} [\,\mathcal{N}^H : \iota(\mathcal{M}^H)\,]^{2n_H} \tag{1}$$

(cf. [2, Lem. 2.11]). The claim follows from the equality

$$[\,(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{N})^H : (1\otimes\iota)((\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{M})^H)\,]_{\mathbb{Z}_p} = |[\,\mathcal{N}^H : \iota(\mathcal{M}^H)\,]|_p$$

and [2, Prop. 2.4.(4)]. □

**Corollary 3.24.** *Let $G$ be a finite $p$-group, and let $\mathcal{M}$ and $\mathcal{N}$ be $\mathbb{Z}[G]$-lattices affording the same self-dual rational representation. Then $\mathcal{M}$ and $\mathcal{N}$ are factor equivalent if and only if we have*

$$v_p(\mathcal{C}_\Theta(\mathcal{M})) = v_p(\mathcal{C}_\Theta(\mathcal{N}))$$

*for all $G$-relations $\Theta$.*

**Proof.** By the proof of Lemma 3.5, $\mathcal{M}$ and $\mathcal{N}$ are factor equivalent if and only if $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{M}$ and $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{N}$ are factor equivalent as $\mathbb{Z}_\ell[G]$-lattices for every prime $\ell$. Since $G$ is a $p$-group, these lattices are isomorphic for all $\ell \neq p$. Hence, the claim follows from Proposition 3.23. □

In [30], Fröhlich obtained a theorem [30, Thm. 7 (Multiplicative)] on the factor equivalence of $S$-units and $Y_S$ (cf. Example 3.6). This theorem of Fröhlich was generalized by de Smit, who also gave a simplified proof [21, Thm. 5.2]. In [1], Bartel independently proved a theorem (Theorem 3.25) on the regulator constant of the $S$-units. He later verified that his theorem is equivalent to the theorem of de Smit (cf. [2, page 8]) by using Theorem 3.22. The following theorem of Bartel provides an arithmetic description of the regulator constant of the

unit lattice, which is the principal integral lattice in this paper. Although his theorem is formulated for general $S$-units, we restrict here to the special case of the group of ordinary units.

**Theorem 3.25.** *([1, Prop. 2.15]) Let $L/K$ be a finite Galois extension of number fields with Galois group $G$. For each subgroup $H$ of $G$, write $\lambda(H)$ for the order of the kernel of the map*

$$H^1(H, \mu(L)) \longrightarrow H^1(H, \mathcal{O}_L^\times)$$

*induced by the inclusion $\mu(L) \hookrightarrow \mathcal{O}_L^\times$. If $\Theta = \sum_{H \leq G} n_H H$ is a $G$-relation, then we have*

$$\mathcal{C}_\Theta(E_L) = \mathcal{C}_\Theta(\mathbb{Z}) \cdot \prod_{H \leq G} \left( \frac{R_{L^H}}{\lambda(H)} \right)^{2n_H},$$

*where $\mathbb{Z}$ in $\mathcal{C}_\Theta(\mathbb{Z})$ denotes the $\mathbb{Z}[G]$-lattice $\mathbb{Z}$ with trivial $G$-action.*

**Remark 3.26.** Let $\Theta = \sum_{H \leq G} n_H H$ be a $G$-relation. One checks

$$\mathcal{C}_\Theta(\mathbb{Z}) = \prod_{H \leq G} |H|^{-n_H}$$

using the bilinear map $\langle n, m \rangle := nm$ on $\mathbb{Z}$.

**Remark 3.27.** ([1, Lem. 2.14]) Let $L/K$ be a Galois extension of number fields with Galois group $G$. Let $H$ be a subgroup of $G$. The embedding $\mathcal{O}_{L^H}^\times \hookrightarrow \mathcal{O}_L^\times$ induces an embedding $E_{L^H} \hookrightarrow E_L^H$. We can easily check

$$\lambda(H) = [E_L^H : E_{L^H}]$$

by using cohomology.

## 4. Regulator constants of some standard lattices

In this section, we derive formulae for $\mathcal{C}_\Theta(\mathcal{A}_G)$ and $\mathcal{C}_\Theta(I_G)$ that hold for general finite groups $G$ and $G$-relations $\Theta$. In [29], Fröhlich proved that $\mathcal{A}_G$ and $I_G$ are not factor equivalent when $G$ is a non-cyclic abelian group. We provide a proof of this theorem by explicitly showing that if $G$ is not cyclic, then we have $\mathcal{C}_\Theta(\mathcal{A}_G) \neq \mathcal{C}_\Theta(I_G)$ for some $G$-relation $\Theta$. Our formulae will be useful in the study of the Galois module structure of unit lattices in later sections. When $G$ is cyclic, the lattices $\mathcal{A}_G$ and $I_G$ are factor equivalent, because $G$ has no non-trivial $G$-relations. Therefore, in this section, we assume that $G$ is non-cyclic.

**Proposition 4.1.** *Let $G$ be a non-cyclic finite group, and let $\Theta = \sum_{H \leq G} n_H H$ be a $G$-relation. Then we have*

$$\mathcal{C}_\Theta(\mathcal{A}_G) = \prod_{H \leq G} |H|^{n_H}. \tag{2}$$

**Proof.** By Remark 3.16 (i), we may compute $\mathcal{C}_\Theta(\mathcal{A}_G)$ with any non-degenerate bilinear $G$-invariant pairing on $\mathcal{A}_G$. Let $(\ ,\ )$ denote the pairing on $\mathbb{Z}[G]$ defined

by $(g,g') := \delta_{g,g'}$ for all $g,g' \in G$, where $\delta_{g,g'}$ denotes the Kronecker delta symbol. Define a second pairing $\langle\ ,\ \rangle$ on $\mathbb{Z}[G]$ by

$$\langle x,y\rangle := (\,x - \frac{1}{|G|}\sum_{g\in G} gx\,,\ y - \frac{1}{|G|}\sum_{g\in G} gy\,)$$

for all $x,y \in \mathbb{Z}[G]$. A straightforward computation shows that $\langle g,g'\rangle = \delta_{g,g'} - 1/|G|$ for all $g,g' \in G$. From this, one checks that both the left and right kernels of $\langle\ ,\ \rangle$ coincide with the subspace $(s_G)$ of $\mathbb{Z}[G]$ generated by $s_G$. Hence, $\langle\ ,\ \rangle$ induces a non-degenerate bilinear pairing on $\mathcal{A}_G$. The $G$-invariance of $\langle\ ,\ \rangle$ on $\mathcal{A}_G$ follows directly from its $G$-invariance on $\mathbb{Z}[G]$.

We can compute $\mathcal{C}_\Theta(\mathcal{A}_G)$ by evaluating the determinant $\det\big(\langle\ ,\ \rangle|_{(\mathcal{A}_G)^H}\big)$ for each subgroup $H$ of $G$. For each subgroup $H$ of $G$, the set $\{\overline{s_H\cdot\sigma}\}_{\sigma\notin H}$ of the classes of $s_H\cdot\sigma \in \mathbb{Z}[G]$ with $\sigma \notin H$, taken in $\mathcal{A}_G$, forms a $\mathbb{Z}$-basis of $\big(\mathcal{A}_G\big)^H$. By definition of $\langle\ ,\ \rangle$, we have

$$\big\langle \overline{s_H\cdot g_1},\, \overline{s_H\cdot g_2}\big\rangle = \begin{cases} \dfrac{|H|\cdot(|G|-|H|)}{|G|} & \text{if } Hg_1 = Hg_2,\\[2ex] -\dfrac{|H|^2}{|G|} & \text{if } Hg_1 \neq Hg_2. \end{cases}$$

Consequently, the matrix of $\big(\frac{1}{|H|}\langle\ ,\ \rangle|_{(\mathcal{A}_G)^H}\big)$ with respect to the basis $\{\overline{s_H\cdot\sigma}\}_{\sigma\notin H}$ is the following circulant matrix of rank $(G:H)-1$:

$$\begin{pmatrix} \frac{|G|-|H|}{|G|} & -\frac{|H|}{|G|} & \cdots & -\frac{|H|}{|G|} & -\frac{|H|}{|G|} \\ -\frac{|H|}{|G|} & \frac{|G|-|H|}{|G|} & \cdots & -\frac{|H|}{|G|} & -\frac{|H|}{|G|} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -\frac{|H|}{|G|} & -\frac{|H|}{|G|} & \cdots & \frac{|G|-|H|}{|G|} & -\frac{|H|}{|G|} \\ -\frac{|H|}{|G|} & -\frac{|H|}{|G|} & \cdots & -\frac{|H|}{|G|} & \frac{|G|-|H|}{|G|} \end{pmatrix} \tag{3}$$

By the formula for the determinant of circulant matrices (cf. [18, Thm. 1]), the determinant of (3) equals

$$\frac{1}{|G|^{(G:H)-1}}\cdot\prod_{j=0}^{(G:H)-2}\Big((|G|-|H|) - |H|\big(\omega^j+\omega^{2j}+\cdots+\omega^{((G:H)-2)j}\big)\Big),$$

where $\omega$ denotes a primitive $((G:H)-1)$th root of unity. The factor in the product equals $|H|$ when $j=0$, and $|G|$ otherwise. Therefore, the determinant $\det\big(\frac{1}{|H|}\langle\ ,\ \rangle|_{(\mathcal{A}_G)^H}\big)$ is equal to $|H||G|^{-1}$. Hence, we have

$$\mathcal{C}_\Theta(\mathcal{A}_G) = \prod_{H\leq G}\big(|H||G|^{-1}\big)^{n_H}. \tag{4}$$

By Lemma 3.18, the exponent of $|G|$ in (4) is 0. □

**Proposition 4.2.** *Let $G$ be a non-cyclic finite group. Let $\Theta = \sum_{H\leq G} n_H H$ be a $G$-relation. Then we have*

$$\mathcal{C}_\Theta(I_G) = \prod_{H\leq G} |H|^{-n_H}.$$

**Proof.** We use the restriction to $I_G$ of the pairing $(\ ,\ )$ defined on $\mathbb{Z}[G]$ by $(g, g') = \delta_{g,g'}$ for $g, g' \in G$. This pairing is $G$-invariant and symmetric. Moreover, the left kernel of $(\ ,\ )$ is trivial, because if $\sum_{\tau\in G} a_\tau \tau \in I_G$ lies in the left kernel, then we have

$$\Big(\sum_{\tau\in G} a_\tau \tau\,,\, \sigma - 1\Big) = a_\sigma - a_1 = 0$$

for all $\sigma \in G$. From $\sum_{\tau\in G} a_\tau = 0$, we deduce $a_1 = 0$. By the symmetry of the pairing, the right kernel is also trivial.

For every subgroup $H$ of $G$, the submodule $(I_G)^H$ coincides with the kernel of the restriction of the augmentation map to $s_H \cdot \mathbb{Z}[G] = (\mathbb{Z}[G])^H$. Hence, $(I_G)^H$ is equal to $s_H \cdot I_G$ with $\mathbb{Z}$-basis $\{s_H \cdot (\sigma - 1)\}_{H\sigma\neq H}$. For this basis, we have

$$\frac{1}{|H|} \cdot \big(s_H \cdot (\sigma - 1),\, s_H \cdot (\tau - 1)\big) = \begin{cases} 2 & \text{if } H\sigma = H\tau, \\ 1 & \text{otherwise.} \end{cases}$$

Thus, the matrix $\Big(\frac{1}{|H|}(\ s_H \cdot (\sigma - 1),\ s_H \cdot (\tau - 1)\ )\Big)_{H\tau, H\sigma\neq H}$ is the circulant matrix of rank $(G : H) - 1$, whose diagonal entries are equal to 2 and whose off-diagonal entries are equal to 1. Its determinant is equal to

$$\prod_{j=0}^{(G:H)-2} \Big(2 + (\omega^j + \omega^{2j} + \cdots + \omega^{((G:H)-2)j})\Big), \tag{5}$$

where $\omega$ denotes a primitive $((G : H) - 1)$th root of unity. The product (5) equals $(G : H)$. In conclusion, we have

$$\mathcal{C}_\Theta(I_G) = \prod_{H\leq G} (G : H)^{n_H} = \prod_{H\leq G} |H|^{-n_H}.$$

The last equality follows from Lemma 3.18. □

The formulae for the regulator constants of $\mathcal{A}_G$ and $I_G$ yield the following corollary.

**Corollary 4.3.** *For every non-cyclic group $G$ and every $G$-relation $\Theta$, we have $\mathcal{C}_\Theta(\mathcal{A}_G) = \mathcal{C}_\Theta(I_G)^{-1}$. In particular, $\mathcal{A}_G$ and $I_G$ are not factor equivalent if $G$ is not cyclic.*

**Proof.** The first part of the statement follows immediately from Proposition 4.1 and Proposition 4.2. By Theorem 3.22, the $\mathbb{Z}[G]$-lattices $\mathcal{A}_G$ and $I_G$ are factor equivalent if and only if we have $\mathcal{C}_\Theta(\mathcal{A}_G) = \mathcal{C}_\Theta(I_G)$ for every $G$-relation $\Theta$. By Remark 3.26, this is equivalent to $\mathcal{C}_\Theta(I_G) = \mathcal{C}_\Theta(\mathbb{Z}) = 1$ for all $\Theta$. By [4, Cor. 9.2], for a prime $l$, there exists a $G$-relation $\Theta$ with $v_l(\mathcal{C}_\Theta(\mathbb{Z})) \neq 1$ if and only if $G$ has a subquotient isomorphic to $(\mathbb{Z}/l\mathbb{Z})^2$ or to $\mathbb{Z}/l\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ for a prime $p$ such

that $\mathbb{Z}/p\mathbb{Z}$ acts faithfully on $\mathbb{Z}/l\mathbb{Z}$. It remains to show that such a subquotient exists if $G$ is not cyclic.

Suppose that $G$ is a non-cyclic group. If $G$ has no subquotient of the form $(\mathbb{Z}/l\mathbb{Z})^2$ for any prime $l$, then all the Sylow subgroups of $G$ are cyclic. By [62, Thm. 10.1.10], the group $G$ admits a presentation

$$\langle\, a, b \mid a^m = 1 = b^n,\ b^{-1}ab = a^r \,\rangle$$

for some integers $m, n, r > 0$ with $(r-1)n$ relatively prime to $m$. For every quotient $Q$ of $G$, write $a_Q$ and $b_Q$ for the classes of $a$ and $b$ in $Q$ respectively. For any element $x$ of a group, let $\langle x\rangle$ be the cyclic subgroup generated by $x$. Since $r-1$ is coprime to $m$, the commutator subgroup $[G,G]$ is equal to $\langle a\rangle$. Hence, for every prime $l$ dividing $m$, the quotient $G(l) := G/\langle a^l\rangle$ is non-abelian. Let $G(l)'$ be the quotient of $G(l)$ by the subgroup of elements of $\langle b_{G(l)}\rangle$ that commute with $a_{G(l)}$. Then, the quotient $G(l)'$ is isomorphic to a semi-direct product $\mathbb{Z}/l\mathbb{Z} \rtimes \mathbb{Z}/n'\mathbb{Z}$ for some $n'|n$ such that $\mathbb{Z}/n'\mathbb{Z}$ acts faithfully on $\mathbb{Z}/l\mathbb{Z}$. For each prime divisor $p$ of $n'$, the subgroup of $G(l)'$ generated by $a_{G(l)'}$ and $b_{G(l)'}^{n'/p}$ is a non-abelian group of order $pl$. □

## 5. Proof of Theorem A

In this section, we prove Theorem A. Let $L$ be a number field. From the analytic class number formula and the functional equation of the Dedekind zeta function $\zeta_L$, we obtain the following formula

$$\zeta_L^*(0) = -\frac{h_L}{w_L} R_L \tag{6}$$

for the special value of $\zeta_L(s)$ at 0. The Artin formalism for Artin $L$-functions, together with (6), yields the following theorem proved independently by Brauer [9] and by Kuroda [49].

**Theorem 5.1** (Brauer–Kuroda)**.** *Let $L/K$ be a Galois extension of number fields with Galois group $G$. If there is a $G$-relation $\Theta = \sum_{H\le G} n_H H$, then we have the equality*

$$\prod_{H\le G}\left(\frac{h_{L^H} R_{L^H}}{w_{L^H}}\right)^{n_H} = 1. \tag{7}$$

We shall use the following equivalent form of (7), which is more convenient for our purpose :

$$\prod_{H\le G} h_{L^H}^{n_H} = \Big(\prod_{H\le G} R_{L^H}^{n_H}\Big)^{-1} \times \Big(\prod_{H\le G} w_{L^H}^{n_H}\Big). \tag{8}$$

**Theorem 5.2** (Theorem A)**.** *Let $L$ be a Galois extension of an admissible field $k$ with Galois group $G$. Suppose that no infinite places of $k$ are ramified in $L$. Then $E_L$ is factor equivalent to $\mathcal{A}_G$ as $\mathbb{Z}[G]$-lattices if and only if we have the equality*

$$\prod_{H\le G} |H|^{n_H} = \prod_{H\le G} h_{L^H}^{-n_H} \cdot \prod_{H\le G}\left(\frac{\lambda(H)}{w_{L^H}}\right)^{-n_H}$$

*for all $G$-relations $\Theta = \sum_{H \leq G} n_H H$.*

**Proof.** By Theorem 3.22, $E_L$ is factor-equivalent to $\mathcal{A}_G$ as $\mathbb{Z}[G]$-lattices if and only if we have $\mathcal{C}_\Theta(E_L) = \mathcal{C}_\Theta(\mathcal{A}_G)$ for all $G$-relations $\Theta$. By Theorem 3.25 and Proposition 4.1, this holds if and only if we have

$$\prod_{H \leq G} |H|^{n_H} = \mathcal{C}_\Theta(\mathbb{Z}) \cdot \prod_{H \leq G} \left( \frac{R_{L^H}}{\lambda(H)} \right)^{2n_H} \tag{9}$$

for all $G$-relations $\Theta = \sum_{H \leq G} n_H H$. By the equality (8) and Remark 3.26, the condition (9) is equivalent to the condition

$$\prod_{H \leq G} |H|^{2n_H} = \prod_{H \leq G} h_{L^H}^{-2n_H} \cdot \prod_{H \leq G} \lambda(H)^{-2n_H} \cdot \prod_{H \leq G} w_{L^H}^{2n_H}. \tag{10}$$

Taking the positive square root of (10) yields the claim. □

**Remark 5.3.** ([9, §2]) Brauer proved that for every Galois extension $L/K$ of number fields and every $G_{L/K}$-relation $\Theta = \sum_{H \leq G_{L/K}} n_H H$, the quotient $\prod_{H \leq G_{L/K}} w_{L^H}^{n_H}$ is a power of 2.

Let $L$ and $G$ be as in Theorem 5.2. If $L$ is totally real, then we have $w_{L^H} = 2$ for all subgroups $H$ of $G$. Then, the quotients of $w_{L^H}$'s are equal to 1 by Lemma 3.18. Furthermore, if $G$ has an odd order, then we have $\lambda(H) = 1$ for every subgroup $H$ of $G$. Therefore, we have the following corollary.

**Corollary 5.4.** *Let $L$ be a real Galois number field of odd degree. Let $G$ be the Galois group of $L$ over $\mathbb{Q}$. Then, the $\mathbb{Z}[G]$-lattices $E_L$ and $\mathcal{A}_G$ are factor equivalent if and only if we have the equality*

$$\prod_{H \leq G} |H|^{n_H} = \prod_{H \leq G} h_{L^H}^{-n_H}$$

*for all $G$-relations $\Theta = \sum_{H \leq G} n_H H$.*

**Remark 5.5.** Theorem A is a generalization of the necessary conditions on the quotient of class numbers of subfields for the existence of local Minkowski units that were obtained by Burns [12, Thm. 3], Duval [27, Rem. 5.3 (a)], and Marszalek [55, Thm. 2.8. (b)].

**Example 5.6.** Let $G = (\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ be the Heisenberg group of order $p^3$ with $p \geq 3$. It has the $G$-relation

$$\Theta = I - IZ - J + JZ,$$

where $Z$ denotes the center of $G$, and $I$ and $J$ are two non-conjugate, non-central subgroups of order $p$. Let $L$ be a Galois extension of $\mathbb{Q}$ with Galois group $G$. Then, the factor equivalence of $E_L$ and $\mathcal{A}_G$ is subject to the following necessary condition

$$\frac{h_{L^I} h_{L^{JZ}}}{h_{L^J} h_{L^{IZ}}} = 1.$$

**Remark 5.7.** For a finite group $G$, a $G$-relation $\Theta = \sum_{H \leq G} n_H H$ is called *useful* (cf. [6]) if we have $n_1 \neq 0$ for the trivial subgroup 1 of $G$. For a certain useful $G$-relation $\Theta$ (cf. [3, Assumption 1.3]), the index

$$[\mathcal{M} : \sum_{n_H \cdot n_1 < 0} \mathcal{M}^H] \in \mathbb{N}$$

is finite for every $\mathbb{Z}[G]$-lattice $\mathcal{M}$. In [3], the authors studied the relationship between this index, the rational representation $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{M}$, and the factor equivalence class of $\mathcal{M}$ for $G$-relations satisfying [3, Assumption 1.3]. As a consequence, if $\mathcal{M}$ is the unit lattice of a Galois extension $L$ of an admissible field $k$ where no infinite places of $k$ are ramified in $L$, then the index (for the $G$-relations satisfying [3, Assumption 1.3]) is uniquely determined by the factor equivalence class of $\mathcal{M}$.

**Remark 5.8.** In [3], the authors showed that the regulator constant can be used to obtain analogous results on the integral Galois module structure of higher K-groups of number fields and the Mordell-Weil groups of elliptic curves.

## 6. The arithmetic properties of totally real $p$-rational number fields

The theory of factor equivalence provides a method to study the Galois module structure of unit lattices in terms of class numbers. However, applying the theory *in practice* is usually difficult because class numbers are notoriously hard to compute. Burns exploited the strong arithmetic properties of $p$-power genus field extensions of admissible fields to study the existence of local Minkowski units (cf. §3.2).

In the remainder of this paper, we examine the Galois module structure of unit lattices for another special family of totally real number fields, called $p$-rational fields. The $p$-rational fields were investigated in [45, 58, 57] to construct infinitely many non-abelian extensions of $\mathbb{Q}$ satisfying Leopoldt's conjecture at the prime $p$. It has long been observed that many arithmetic problems become simpler when the field is $p$-rational. In the totally real case, this principle appears to be more amenable to direct treatment, since the Galois group of the maximal pro-$p$ extension unramified outside $p$ has a simpler structure (cf. [37, Figure 1]), which permits more straightforward methods of relating the defect of $p$-rationality to the complexity of the problems (cf. [38, 37]). Motivated by this perspective, we apply the strong arithmetic properties of $p$-rational fields to prove the non-existence of Minkowski units in non-abelian $p$-rational $p$-extensions of $\mathbb{Q}$ (§7), and to study the relative Galois module structure of unit lattices in Galois extensions of totally real $p$-rational fields (§8).

The abundance of $p$-rational fields in our context is illustrated by the following two facts:

(i) By a theorem of Movahhedi (Theorem 6.8), if a number field $F$ is $p$-rational, then there exists an infinite family of infinite pro-$p$ towers of $p$-rational $p$-extensions of $F$.
(ii) It is widely believed that a number field $F$ is $p$-rational for many primes $p$. In [36], Gras even conjectured that $F$ is $p$-rational for all but finitely many primes $p$.

Thus, our results on the Galois module structure of unit lattices apply to a large family of number fields.

We will focus on the Galois module structure of unit lattices in non-cyclic Galois extensions of number fields, as the theory of factor equivalence becomes trivial when the Galois group is cyclic (cf. Proposition 3.2 and the remark preceding it).

**6.1. Totally real $p$-rational number fields.** Let $F$ be a number field and $p$ an odd prime. We write $F_\infty$ for the cyclotomic $\mathbb{Z}_p$-extension of $F$. For each integer $n \geq 0$, let $F_n$ denote the $n$th layer of the extension $F_\infty/F$. We write $H_F$ for the $p$-Hilbert class field of $F$, and $\mathfrak{h}_F$ for the $p$-class number of $F$. For a set $S$ of primes of $F$, let $F_S$ denote the maximal pro-$p$ extension of $F$ unramified outside $S$, and write $G_S(F)$ for the Galois group of $F_S$ over $F$. We denote by $S_p$ the set of $p$-adic primes of $F$. By local class field theory, a non-$p$-adic prime $\mathfrak{q}$ of $F$ can ramify in a pro-$p$ extension of $F$ only if its ideal norm $\mathbf{N}\mathfrak{q}$ is congruent to 1 modulo $p$ (see [46, §8.5] for an elementary explanation). Thus, without this congruence, the situation is vacuous, and we may assume that every non-$p$-adic prime in $S$ satisfies this congruence.

In this subsection, we briefly recall some arithmetic properties of totally real $p$-rational number fields that will be useful later. Except for Proposition 6.5, Conjecture 6.6, and Theorem 6.8, we assume throughout that $F$ is totally real. For more general information on $p$-rational number fields, the reader is referred to [35, 45, 56, 58, 57, 5].

Several equivalent characterizations of $p$-rationality can be found in the literature, for example, in [56, page 22].

**Definition 6.1.** A number field $F$ is said to be $p$-rational if one of the following equivalent conditions holds:

(1) The Galois group $G_{S_p}(F)$ is a free pro-$p$ group, where $S_p$ is the set of $p$-adic primes of $F$;
(2) We have an isomorphism $G_{S_p}(F)^{\mathrm{ab}} \simeq \mathbb{Z}_p^{c_F+1}$, where $c_F$ denotes the number of complex places of $F$.

In particular, a totally real number field $F$ is $p$-rational precisely when we have

$$G_{S_p}(F) \simeq G_{S_p}(F)^{\mathrm{ab}} \simeq \mathbb{Z}_p.$$

**Example 6.2.** By the Kronecker–Weber theorem, the rational number field $\mathbb{Q}$ is $p$-rational for every prime $p$.

We now return to the setting of a general totally real $p$-rational field. Since $F_\infty$ is a subfield of $F_{S_p}$, we have $F_{S_p} = F_\infty$ in this case. Therefore, $H_F$ is a subfield of $F_\infty$, and we obtain the following proposition.

**Proposition 6.3.** *Let $F$ be a totally real $p$-rational number field. Let $m$ be the largest integer such that $F_m/F$ is unramified. Then, we have $\mathfrak{h}_F = p^m$.*

As an immediate consequence of Proposition 6.3, we can observe the following lemma. We also note in passing that, in fact, in a Galois $p$-extension of totally real $p$-rational number fields, at most one non-$p$-adic prime can be ramified, while there is no such restriction on the $p$-adic places (cf. Corollary 6.10).

**Lemma 6.4.** *Let $L/F$ be an extension of totally real $p$-rational number fields. Then, the following claims are valid.*

*(i) We have the inequalities $\mathfrak{h}_F \cdot |[L : F]|_p^{-1} \leq \mathfrak{h}_L \leq \mathfrak{h}_F \cdot [L : F]$.*
*(ii) If $L/F$ is a cyclic extension of degree $p$ that is unramified outside $p$, then we have $\mathfrak{h}_L = \max\{\mathfrak{h}_F/p, 1\}$.*
*(iii) If $L/F$ is a cyclic extension of degree $p$ that is ramified precisely at a non-$p$-adic prime, then we have $\mathfrak{h}_L = \mathfrak{h}_F$.*

**Proof.** (i) The left inequality follows from the inclusion $LH_F \subseteq H_L$ and the equalities

$$[LH_F : L] = [H_F : H_F \cap L] = \mathfrak{h}_F \cdot [H_F \cap L : F]^{-1}.$$

Since $H_L$ is contained in $L_\infty = LF_\infty$, there is some $m \in \mathbb{N}$ such that $H_L$ is equal to the compositum of $L$ and $F_m$. Every $p$-adic prime of $F$ has ramification index at most $[L : F]$ in the extension $H_L/F$. Hence, the degree $[F_m : F]$, which is bounded above by the product of $\mathfrak{h}_F$ and the maximal ramification index of the $p$-adic primes of $F$ in the extension $F_m/F$, is in turn bounded above by $\mathfrak{h}_F \cdot [L : F]$. Therefore, we have $\mathfrak{h}_L = [H_L : L] \leq [F_m : F] \leq \mathfrak{h}_F \cdot [L : F]$.

(ii) If $L/F$ is unramified outside $p$, then $L$ is equal to $F_1$. If $F$ has $p$-class number 1, then at least one prime of $F$ is totally ramified in $F_\infty$. Hence, we have $\mathfrak{h}_F = \mathfrak{h}_L = 1$. If we have $H_F \neq F$, then we have $H_F = H_L$ because $H_F/L$ is unramified and $F_\infty/H_F$ is totally ramified at some $p$-adic prime. Thus, we have $\mathfrak{h}_L = [H_F : L] = p^{-1}\mathfrak{h}_F$.

(iii) Let $r$ be an integer such that $H_F$ is equal to $F_{r-1}$. Then $F_r/F$ is ramified at some $p$-adic prime of $F$ say $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified in $L/F$, $F_rL/L$ is ramified at the primes of $L$ above $\mathfrak{p}$. Thus, we have $H_L \subsetneq F_rL$ and consequently $H_L = H_FL$. The claim follows because $L$ and $H_F$ are linearly disjoint over $F$.

□

The $p$-rationality of number fields satisfies the following descending property.

**Proposition 6.5.** *(cf.* [32, Thm. I.1], [56, Prop. 5 on page 30]*) Let $L/F$ be an extension of number fields. If $L$ is $p$-rational, then $F$ is also $p$-rational.*

By Propositions 6.3 and 6.5, we can study the $p$-part of the quotients of class numbers of subfields appearing in Theorem A, and investigate the factor equivalence class of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_F$ when $F$ is a totally real $p$-rational Galois extension of $\mathbb{Q}$. Therefore, understanding the existence of Galois extensions of totally real $p$-rational fields with various Galois groups is also of interest in the study of the Galois module structure of unit lattices.

For finite $p$-groups, one can apply the results of Movahhedi [57] on the ascent of $p$-rationality in Galois $p$-extensions of number fields. However, the problem for general groups remains poorly understood. Some recent progress has been made for groups of the form $(\mathbb{Z}/2\mathbb{Z})^t$ for $t \geq 1$ (cf. [17, 39, 47, 52]).

We also record the following conjecture due to Gras, which indicates that studying $p$-rational fields can yield results of a rather general nature for number fields.

**Conjecture 6.6.** *(*[36]*) A number field is $p$-rational for all but finitely many primes.*

To state the theorem of Movahhedi (Theorem 6.8), we first recall the notion of a primitive set of places (cf. [34, 56]). Let $F$ be a number field. Let $F_{S_p}(1)$ denote the maximal elementary abelian extension of $F$ in $F_{S_p}$. Hence, if $F$ is $p$-rational, then the Galois group $\mathrm{Gal}(F_{S_p}(1)/F)$ of $F_{S_p}(1)$ over $F$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{c_F+1}$ as a vector space over the finite field $\mathbb{Z}/p\mathbb{Z}$.

**Definition 6.7.** Let $F$ be a number field. Let $S$ be a finite set of finite places of $F$ containing $S_p$. The set $S$ is called *primitive* for $(F, p)$ if the set of Frobenius automorphisms in $\mathrm{Gal}(F_{S_p}(1)/F)$ at the finite non-$p$-adic primes of $S$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$.

With this notion, we can now state the following theorem.

**Theorem 6.8.** *(*[57, Thm.2]*) Let $F$ be a $p$-rational number field. Let $L$ be a Galois $p$-extension of $F$. Then, $L$ is $p$-rational if and only if the set* $\mathrm{Ram}(L/F) \cup S_p$ *is primitive for $(F, p)$, where* $\mathrm{Ram}(L/F)$ *denotes the set of primes ramified in $L/F$.*

**Remark 6.9.** The readers can also refer to [32, 33] for a class field theoretic approach on the ascent of $p$-rationality under the Leopoldt conjecture at $p$.

**Corollary 6.10.** *Let $F$ be a totally real $p$-rational number field. For a non-$p$-adic prime $\mathfrak{q}$ of $F$, the set $S_p \cup \{\mathfrak{q}\}$ is primitive for $(F, p)$ if and only if $\mathfrak{q}$ does not split in $F_1$. It follows that if $L$ is a Galois $p$-extension of $F$, then $L$ is $p$-rational if and only if there exists such a prime $\mathfrak{q}$ with* $\mathrm{Ram}(L/F) \subseteq S_p \cup \{\mathfrak{q}\}$.

**Remark 6.11.** If $F$ is $p$-rational, then it is easily seen that $p$-rationality ascends in the pro-$p$ tower $F_{S_p}/F$, since every closed subgroup of a free pro-$p$ group is free (cf. [64, Cor. 3 on page 31]). In comparison, Theorem 6.8 addresses the ascent in larger pro-$p$ towers.

By Chebotarev's density theorem, Theorem 6.8 ensures the existence of infinitely many towers of $p$-rational $p$-extensions of a number field $F$, provided that $F$ itself is $p$-rational.

Moreover, when $F$ is $p$-rational and the set $S$ is primitive for the pair $(F, p)$, the structure of the Galois group $G_S(F)$ is well understood, thanks to a theorem of Movahhedi. We state Movahhedi's theorem below in the case where $F$ is totally real.

**Proposition 6.12.** *(*[58, Thm. 3.3]*) Let $F$ be a totally real $p$-rational number field. Let $\mathfrak{q}$ be a non-$p$-adic prime of $F$ such that $S = S_p \cup \{\mathfrak{q}\}$ is primitive for $(F, p)$. Then, $G_S(F)$ is the Demuškin group of rank 2 with minimal presentation*

$$\langle\ \sigma, \tau\ \mid\ \tau^{\mathbf{N}\mathfrak{q}-1}[\tau, \sigma] = 1\ \rangle,$$

*where $\mathbf{N}\mathfrak{q}$ is the ideal norm of the prime ideal $\mathfrak{q}$.*

By Proposition 6.12, the group $G_S(F)$ is a Demuškin group of rank 2. This yields information on the $G$-relations needed to apply Proposition 3.23 to the $\mathbb{Z}_p[G_{L/F}]$-lattice $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_L$, where $L/F$ is a Galois $p$-extension contained in $F_S$ (cf. §7). Moreover, the group structure can be exploited to obtain more precise information on the $p$-class group (cf. §6.2).

**Proposition 6.13.** *(*[58, Lem. 2.5]*) Let $F$ be a totally real $p$-rational number field. Let $S$ be a finite set of primes of $F$ containing $S_p$. Then we have*

$$G_S(F)^{\mathrm{ab}} \simeq \mathbb{Z}_p \times \prod_{v} \mathbb{Z}/\mu_p(F_v)\mathbb{Z},$$

*where $v$ runs over the finite non-$p$-adic primes of $S$, and $\mu_p(F_v)$ denotes the number of $p$-power roots of unity in the completion $F_v$ of $F$ at $v$.*

In particular, Proposition 6.13 implies the following corollary, which may also be understood from the fact that every open subgroup of a Demuškin group of rank 2 has generator rank 2.

**Corollary 6.14.** *Let $\mathfrak{q}$ be a finite non-$p$-adic prime of $F$ that does not split in $F_\infty$. Then, the maximal elementary abelian extension of $F$ in $F_{S_p\cup\{\mathfrak{q}\}}$ is the compositum of $F_1$ and a cyclic $p$-extension of $F$ in which $\mathfrak{q}$ is ramified (note that $p$ may also ramify in that cyclic extension).*

By the Burnside Basis theorem, Corollary 6.14 implies the following.

**Lemma 6.15.** *(*[57, Thm. 2]*) Let $F$ be a totally real $p$-rational number field and $\mathfrak{q}$ a non-$p$-adic prime such that $S_p \cup \{\mathfrak{q}\}$ is primitive for $(F, p)$. Then, $\mathfrak{q}$ does not split in $F_{S_p\cup\{\mathfrak{q}\}}$. In this situation, for any finite extension $L$ of $F$ contained in $F_{S_p\cup\{\mathfrak{q}\}}$, we denote by $\mathfrak{q}_L$ the unique prime of $L$ above $\mathfrak{q}$.*

For a totally real $p$-rational field $F$ and a finite non-$p$-adic prime $\mathfrak{q}$ of $F$ such that $S_p \cup \{\mathfrak{q}\}$ is primitive for $(F, p)$, we will frequently consider finite extensions $L/F$ contained in the tower $F_{S_p\cup\{\mathfrak{q}\}}$. By Corollary 6.14, for each such extension

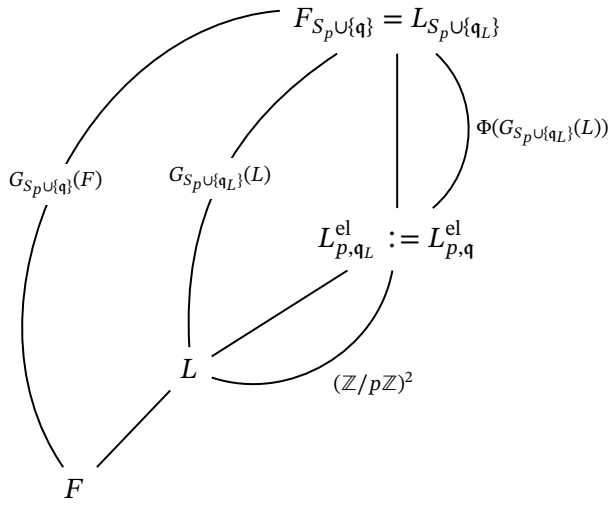
$L$, there exists a unique elementary abelian extension of $L$ in $F_{S_p\cup\{\mathfrak{q}\}}$. Since these extensions play a central role, we fix the following notation.

For the base field $F$, we denote by $F^{\mathrm{el}}_{p,\mathfrak{q}}$ the maximal elementary abelian extension of $F$ contained in $F_{S_p\cup\{\mathfrak{q}\}}$. By definition and Lemma 6.15, we have

$$F_{S_p\cup\{\mathfrak{q}\}} = L_{S_p\cup\{\mathfrak{q}_L\}} \quad \text{and} \quad \mathrm{Gal}(F_{S_p\cup\{\mathfrak{q}\}}/L) = G_{S_p\cup\{\mathfrak{q}_L\}}(L).$$

Hence, we define $L^{\mathrm{el}}_{p,\mathfrak{q}_L}$ analogously, and, for simplicity, write $L^{\mathrm{el}}_{p,\mathfrak{q}}$ instead. By Corollary 6.14, this is the unique extension of $L$ in $F_{S_p\cup\{\mathfrak{q}\}}$ with $G_{L^{\mathrm{el}}_{p,\mathfrak{q}}/L} \simeq (\mathbb{Z}/p\mathbb{Z})^2$.

Since the base field $F$ and the prime $\mathfrak{q}$ are clear from the context, the shorthand $L^{\mathrm{el}}_{p,\mathfrak{q}}$ will cause no ambiguity. In particular, we obtain the following field diagram.




where $\Phi(G_{S_p\cup\{\mathfrak{q}_L\}}(L))$ denotes the Frattini subgroup of $G_{S_p\cup\{\mathfrak{q}_L\}}(L)$.

**6.2. On the $p$-class numbers in a pro-$p$ tower of totally real $p$-rational number fields when $p$ does not split.** We have seen in Proposition 6.3 and Lemma 6.4 that the $p$-class numbers of totally real $p$-rational fields are relatively easy to analyze. When there is a unique $p$-adic prime, these results can be refined further. This refinement will play an important role in the proof of Theorem B in the next section. In order to make this refinement precise, we now consider a totally real $p$-rational field $F$ together with a finite non-$p$-adic prime $\mathfrak{q}$, and introduce the following hypothesis on the triple $(F, p, \mathfrak{q})$.

$$S_p \cup \{\mathfrak{q}\} \text{ is primitive for } (F, p), \text{and } p \text{ does not split in } F_{S_p\cup\{\mathfrak{q}\}}. \tag{U}$$

By the Burnside basis theorem, the triple $(F, p, \mathfrak{q})$ satisfies condition (U) precisely when $F$ has a unique $p$-adic prime and the local degree of this prime in the extension $F^{\mathrm{el}}_{p,\mathfrak{q}}$ is $p^2$. In this subsection, we obtain a structural result on the $p$-class numbers of number fields in the tower $F_{S_p\cup\{\mathfrak{q}\}}/F$ for those $(F, p, \mathfrak{q})$ satisfying (U), by exploiting the inertia subgroup of $G_{S_p\cup\{\mathfrak{q}\}}(F)$ at the unique $p$-adic

place of $F_{S_p\cup\{\mathfrak{q}\}}$. For each number field $F \subseteq L \subset F_{S_p\cup\{\mathfrak{q}\}}$, we denote by $p_L$ the unique prime of $L$ lying above $p$.

The inertia subgroup of $G_{S_p\cup\{\mathfrak{q}\}}(F)$ at the unique $p$-adic place of $F_{S_p\cup\{\mathfrak{q}\}}$ corresponds to the maximal tamely ramified extension $F_{\{\mathfrak{q}\}}$ of $F$ contained in $F_{S_p\cup\{\mathfrak{q}\}}$.

**Lemma 6.16.** *(cf.* [50, Thm. 1.1]*) Let $F$ be a totally real $p$-rational number field. Let $\mathfrak{q}$ be a non-$p$-adic prime of $F$ such that $S_p \cup \{\mathfrak{q}\}$ is primitive for $(F, p)$. Then, the extension $F_{\{\mathfrak{q}\}}/F$ is finite.*

**Proof.** Since $G_{\{\mathfrak{q}\}}(F)$ is a quotient of the Demuškin group $G_{S_p\cup\{\mathfrak{q}\}}(F)$, it is powerful (cf. [23, Chap. 3]) with generator rank at most 2. By [23, Thm. 8.32], $G_{\{\mathfrak{q}\}}(F)$ admits an open uniformly powerful subgroup $\mathcal{U}$. By [23, Thm. 3.8], the generator rank of $\mathcal{U}$ is at most 2. If $G_{\{\mathfrak{q}\}}(F)$ is infinite, then so is $\mathcal{U}$, and in this case $\mathcal{U}$ admits a quotient isomorphic to $\mathbb{Z}_p$ (cf. [23, Exercise 3.11]). It follows that if $F_{\{\mathfrak{q}\}}/F$ were infinite, then $F_{\{\mathfrak{q}\}}$ would contain a $\mathbb{Z}_p$-extension of a finite extension of $F$, which is impossible since in any $\mathbb{Z}_p$-extension of a number field at least one $p$-adic prime must ramify. Therefore $F_{\{\mathfrak{q}\}}/F$ is finite. □

**Proposition 6.17.** *Suppose that $(F, p, \mathfrak{q})$ satisfies* (U)*. Then, we have $\mathfrak{h}_L = 1$ for every number field $L$ with $F_{\{\mathfrak{q}\}} \subseteq L \subset F_{S_p\cup\{\mathfrak{q}\}}$.*

**Proof.** Let $L$ be a number field as above. Then $p_L$ is totally ramified in $F_{S_p\cup\{\mathfrak{q}\}}$ because $\mathrm{Gal}(F_{S_p\cup\{\mathfrak{q}\}}/L)$ is a subgroup of the inertia subgroup of $G_{S_p\cup\{\mathfrak{q}\}}(F)$ at the $p$-adic place of $F_{S_p\cup\{\mathfrak{q}\}}$. Since $p_L$ is ramified in $L_1$, the conclusion follows from Proposition 6.3. □

**Example 6.18.** Note that $(\mathbb{Q}, p, q)$ satisfies (U) if and only if both $[\, p, q\,]$ and $[\, q, p\,]$ are not divisible by $p$ (cf. Remark 3.12). For example, the triple $(\mathbb{Q}, 7, 71)$ satisfies (U). In that case, the $p$-class number is 1 along the tower $\mathbb{Q}_{S_p\cup\{q\}}/\mathbb{Q}_{\{q\}}$ by Proposition 6.17.

**Remark 6.19.** It may be difficult to generalize Proposition 6.17 to a pro-$p$ tower $F_{S_p\cup\{\mathfrak{q}\}}/F$ in which $p$ splits, since one need to take into account all the inertia subgroups of $G_{S_p\cup\{\mathfrak{q}\}}(F)$ at the $p$-adic places. For example, one may recall that the $p$-class field tower of $F$ is the subfield of $F_{S_p}$ fixed by the inertia subgroups of $G_{S_p}(F)$ at the $p$-adic places.

**Corollary 6.20.** *Suppose that $(F, p, \mathfrak{q})$ satisfies* (U)*. Let $L$ be a finite extension of $F$ in $F_{S_p\cup\{\mathfrak{q}\}}$. The extension $F_{S_p\cup\{\mathfrak{q}\}}/L$ is totally ramified at $p_L$ if and only if $F_{\{\mathfrak{q}\}}$ is a subfield of $L$.*

**Proof.** Suppose that $p_L$ is totally ramified in $F_{S_p\cup\{\mathfrak{q}\}}/L$. Then we have $F_{\{\mathfrak{q}\}}L = L$ because $F_{\{\mathfrak{q}\}}L/L$ is unramified at $p_L$. The sufficiency is trivial. □

Now, we study the $p$-class numbers in a cyclic extension $L/K$ of number fields with $[L : K] = p$ contained in $F_{S_p\cup\{\mathfrak{q}\}}/F$ for a triple $(F, p, \mathfrak{q})$ satisfying (U). By (ii) and (iii) of Lemma 6.4, it remains to treat the case where $L/K$ is ramified both at $p_K$ and $\mathfrak{q}_K$.

**Proposition 6.21.** *Suppose that* $(F, p, \mathfrak{q})$ *satisfies* (U)*. Let* $L/K$ *be a cyclic extension of number fields of degree* $p$ *contained in* $F_{S_p\cup\{\mathfrak{q}\}}/F$*, ramified at both* $p_K$ *and* $\mathfrak{q}_K$*. Then, we have*

$$\mathfrak{h}_L = \begin{cases} \mathfrak{h}_K & \text{if } F_{\{\mathfrak{q}\}} \subseteq H_K, \\ p \cdot \mathfrak{h}_K & \text{otherwise.} \end{cases}$$

**Proof.** For all integers $m \geq 0$, we have $L_m = LK_m$ because $L/K$ is ramified at $\mathfrak{q}_K$. By the $p$-rationality of $K$, there is some integer $n \geq 0$ such that we have $H_K = K_n$. Then, $\mathfrak{h}_L$ is equal to one of $p^n$ and $p^{n+1}$ by Lemma 6.4 (i).

By Proposition 6.3, we have $\mathfrak{h}_L = p^{n+1}$ if and only if $L_{n+1}/L_n$ is unramified. Since $K_n/K$ is unramified, both $p_{K_n}$ and $\mathfrak{q}_{K_n}$ are ramified in $L_n/K_n$. Since the ramification index of $\mathfrak{q}_{K_n}$ in $L_{n+1}/K_n$ is $p$, we can check that $G_{L_{n+1}/K_n}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$. In particular, $L_{n+1}$ is equal to $(K_n)^{\mathrm{el}}_{p,\mathfrak{q}}$.

If $L_{n+1}/L_n$ is ramified at $p_{L_n}$, then $G_{L_{n+1}/K_n}$ coincides with the inertia subgroup at $p_{L_{n+1}}$. By the Burnside basis theorem, this occurs if and only if $p_{K_n}$ is totally ramified in $F_{S_p\cup\{\mathfrak{q}\}}$ (cf. [60, Chap. II, Thm. 10.7]). Hence, the claim follows from Corollary 6.20. □

Even though condition (U) may appear restrictive, we can find many triples $(F, p, \mathfrak{q})$ satisfying (U) under the Gras Conjecture (Conjecture 6.6). Let $F$ be a totally real cyclic extension of $\mathbb{Q}$. According to the conjecture, there are expected to be infinitely many rational primes $p$ such that

- $F$ is $p$-rational,
- $p \nmid [F : \mathbb{Q}]$,
- $p$ does not split in $F$.

In the following proposition, we assume that $p$ is such a prime, so that $F$ is $p$-rational. Examples of this type can be found in [51].

**Proposition 6.22.** *Let* $F$ *and* $p$ *be as above. Let* $q$ *be a rational prime such that* $(\mathbb{Q}, p, q)$ *satisfies* (U) *(cf. Example* 6.18*). Then, for every prime* $\mathfrak{q}$ *of* $F$ *above* $q$*, the hypothesis* (U) *is satisfied by* $(F, p, \mathfrak{q})$*.*

**Proof.** Let $S_q$ be the set of primes of $F$ above $q$. Since $p$ is prime to $[F : \mathbb{Q}]$, every element $\mathfrak{q}$ of $S_q$ does not split in $F_\infty = F\mathbb{Q}_\infty$ by the primitivity of the set $S_p \cup \{q\}$. Hence, the set $S_p \cup \{\mathfrak{q}\}$ is primitive for $(F, p)$ for every $\mathfrak{q} \in S_q$ by Corollary 6.10.

It remains to show that the unique $p$-adic prime $\mathfrak{p}$ of $F$ does not split in $F_{S_p\cup\{\mathfrak{q}\}}$ for every $\mathfrak{q} \in S_q$. By the Burnside basis theorem, this happens if and only if $\mathfrak{p}$ does not split in $F^{\mathrm{el}}_{p,\mathfrak{q}}$ (cf. [60, Chap. II, Prop. 9.6]). Since $[F : \mathbb{Q}]$ is prime to $p$, $\mathfrak{p}$ is totally ramified in $F_\infty/F$. In particular, we have $\mathfrak{h}_F = 1$. Therefore, the ramification index of $\mathfrak{p}$ in $F^{\mathrm{el}}_{p,\mathfrak{q}}/F$ is at least $p$, and $\mathfrak{p}$ splits in $F^{\mathrm{el}}_{p,\mathfrak{q}}$ only if there exists a cyclic extension $F(\mathfrak{q})$ of $F$ of degree $p$ in which $\mathfrak{p}$ splits and $\mathfrak{q}$ is ramified. Such an extension $F(\mathfrak{q})$ is unique if it exists.

Since $G_{F/\mathbb{Q}}$ acts transitively on $S_q$, the pro-$p$ extensions $\{F_{S_p\cup\{\mathfrak{q}\}}\}_{\mathfrak{q}\in S_q}$ are conjugate to each other over $\mathbb{Q}$. Hence, if $F(\mathfrak{q})$ exists for some $\mathfrak{q} \in S_q$, then $F(\mathfrak{q})$

exists for every $\mathfrak{q} \in S_q$. Let $\mathcal{F}$ be the compositum of the fields $F(\mathfrak{q})$ for all $\mathfrak{q} \in S_q$. Then, $\mathfrak{p}$ splits completely in $\mathcal{F}$.

On the other hand, by class field theory and the triviality of the $p$-class group of $F$, $\mathcal{F}$ contains the compositum of $F$ and the subfield $\mathcal{K}$ of $\mathbb{Q}(\zeta_q)$ with $[\mathcal{K} : \mathbb{Q}] = p$. Since $p$ does not split in $\mathbb{Q}_{S_p \cup \{q\}}$, the residue class degree of $p$ in $\mathcal{K}$ is $p$. Hence, the residue class degree of $\mathfrak{p}$ in $\mathcal{F}$ is divisible by $p$, a contradiction. □

**Remark 6.23.** In fact, for every odd prime $p$, there exist infinitely many primes $q$ such that $(\mathbb{Q}, p, q)$ satisfy (U). For a proof, we refer the readers to the application of the Gras-Munnier theorem in [15].

## 7. Non-existence of Minkowski units in non-abelian $p$-rational $p$-extensions of $\mathbb{Q}$

In this section, we will prove Theorem B. Let $F$ be a non-abelian $p$-rational Galois $p$-extension of $\mathbb{Q}$. Since $G_{F/\mathbb{Q}}$ is a $p$-group, we may apply the theorem of Tornehave and Bouc on the generators of $G$-relations of finite $p$-groups $G$. We shall show that the factor equivalence class of $E_F$ can be analyzed via Galois extensions $L/K$ of subfields of $F$ with $G_{L/K} \simeq (\mathbb{Z}/p\mathbb{Z})^2$. To begin, let us recall the theorem of Tornehave and Bouc.

**Theorem 7.1.** *(cf.* [4, Thm. 5.3], [7, Cor. 6.16]*) Let $G$ be a finite $p$-group. Then, all $G$-relations are $\mathbb{Z}$-linear combinations of ones of the form* $\mathrm{Ind}_H^G \mathrm{Inf}_{H/B}^H \Theta$ *for pairs $(H/B, \Theta)$ of subquotients $H/B$ of $G$ and $H/B$-relations $\Theta$ of the following types:*

*(i)* $H/B \simeq (\mathbb{Z}/p\mathbb{Z})^2$ *with the $H/B$-relation* $\Theta$

$$1 - \sum_C C + p \cdot H/B,$$

*where $C$ runs over all the subgroups of $H/B$ of order $p$.*

*(ii)* $H/B$ *is the Heisenberg group of order $p^3$ and $\Theta$ is the $H/B$-relation*

$$I - IZ - J + JZ,$$

*where $Z$ is the center of $H/B$ and $I, J$ are two non-conjugate non-central subgroups of $H/B$ of order $p$.*

*(iii)* $H/B$ *is isomorphic to the dihedral group $D_{2^n}$ for some $n \geq 4$ and $\Theta$ is the $H/B$-relation*

$$I - IZ - J + JZ,$$

*where $Z$ is the center of $H/B$ and $I, J$ are two non-conjugate non-central subgroups of $H/B$ of order 2.*

Let $L/K$ be a Galois $p$-extension of number fields. Let $H/B$ be a subquotient of $G_{L/K}$, and let

$$\Theta = \sum_{B \leq H' \leq H} n_{H'}(H'/B)$$

be an $H/B$-relation. A straightforward computation shows that we have

$$\mathrm{Ind}_H^{G_{L/K}} \mathrm{Inf}_{H/B}^H \Theta = \sum_{B \le H' \le H} n_{H'} H'.$$

By Theorem 3.25, we then obtain the equality

$$\mathcal{C}_{\mathrm{Ind}_H^{G_{L/K}} \mathrm{Inf}_{H/B}^H \Theta}(E_L) = \mathcal{C}_{\mathrm{Ind}_H^{G_{L/K}} \mathrm{Inf}_{H/B}^H \Theta}(\mathbb{Z}) \cdot \prod_{B \le H' \le H} \left( \frac{R_{L^{H'}}}{\lambda(H')} \right)^{2n_{H'}}. \tag{11}$$

Applying Theorem 5.1, (11) becomes

$$\mathcal{C}_{\mathrm{Ind}_H^{G_{L/K}} \mathrm{Inf}_{H/B}^H \Theta}(E_L) = \mathcal{C}_{\mathrm{Ind}_H^{G_{L/K}} \mathrm{Inf}_{H/B}^H \Theta}(\mathbb{Z}) \cdot \prod_{B \le H' \le H} \left( \frac{w_{L^{H'}}}{\lambda(H') \cdot h_{L^{H'}}} \right)^{2n_{H'}}. \tag{12}$$

Since $G_{L/K}$ is a $p$-group, Proposition 3.21 implies that we have

$$v_l\big( \mathcal{C}_{\mathrm{Ind}_H^{G_{L/K}} \mathrm{Inf}_{H/B}^H \Theta}(E_L) \big) = 0 \quad \text{for all primes } l \neq p.$$

Since the same holds for the regulator constants of the lattice $\mathbb{Z}$, the product in (12) involving $w_{L^{H'}}$, $\lambda(H')$, and $h_{L^{H'}}$ can be replaced by its $p$-part. In particular, if $L$ is totally real, then we obtain the following observation.

**Proposition 7.2.** *Let $L/K$ be a Galois $p$-extension of totally real number fields. Then, the factor equivalence class of $E_L$ as a $\mathbb{Z}[G_{L/K}]$-lattice is uniquely determined by the quotients of $p$-class numbers of subfields of $L$ associated with the pairs $(H/B, \Theta)$ in Theorem* 7.1.

**Proof.** The quotients involving $w_{L^{H'}}$ in (12) are equal to 1 by Lemma 3.18. The claim follows because we have $\lambda(H') = 1$. □

The following corollary is helpful in studying the existence of Minkowski units in Galois $p$-extensions of $\mathbb{Q}$.

**Corollary 7.3.** *Let $p$ be an odd prime, and let $L/\mathbb{Q}$ be a Galois $p$-extension. Then $E_L$ is factor equivalent to $\mathcal{A}_{G_{L/\mathbb{Q}}}$ as $\mathbb{Z}[G_{L/\mathbb{Q}}]$-lattices if and only if we have*

$$\prod_{B \le H' \le H} \text{ы}_{L^{H'}}^{n_{H'}} = \prod_{B \le H' \le H} h_{L^{H'}}^{n_{H'}} = \prod_{B \le H' \le H} |H'|^{-n_{H'}} = \prod_{B \le H' \le H} |H'/B|^{-n_{H'}} \tag{13}$$

*for all the pairs $(H/B, \Theta)$ consisting of a subquotient $H/B$ of $G_{L/\mathbb{Q}}$ and an $H/B$-relation*

$$\Theta = \sum_{B \le H' \le H} n_{H'} (H'/B)$$

*as in Theorem* 7.1.

For Galois $p$-extensions of totally real $p$-rational number fields, Proposition 7.2 can be refined as follows.

**Proposition 7.4.** *Let $L/K$ be a Galois $p$-extension of totally real $p$-rational number fields. Then the factor equivalence class of $E_L$ as a $\mathbb{Z}[G_{L/K}]$-lattice is determined by the quotients of $p$-class numbers of subfields of $L$ associated to the pairs $(H/B, \Theta)$ in Theorem* 7.1 *such that $H/B \simeq (\mathbb{Z}/p\mathbb{Z})^2$.*

**Proof.** By Theorem 7.1 and Proposition 7.2, it suffices to prove that $G_{L/K}$ has no subquotient $H/B$ isomorphic to the Heisenberg group of order $p^3$. By Corollary 6.10 and Proposition 6.12, $G_{L/K}$ is isomorphic to a subquotient of a Demuškin group of rank 2. It is known that open subgroups of a Demuškin group of rank 2 are themselves Demuškin of rank 2 (cf. [64, §4.5]). Hence, every subquotient of a Demuškin group of rank 2 is powerful. The claim follows since the Heisenberg group of order $p^3$ is not powerful. □

Now, we give a proof of Theorem B. Let $F$ be a non-abelian $p$-rational $p$-extension of $\mathbb{Q}$, and let $F^{\mathrm{ab}}$ be the maximal subfield of $F$ that is abelian over $\mathbb{Q}$. By group theory, $F^{\mathrm{ab}}/\mathbb{Q}$ is not cyclic. Since $\mathbb{Q}$ is $p$-rational, there exists a non-$p$ prime $q$ such that $\mathrm{Ram}(F/\mathbb{Q}) = \{p, q\}$. Hence, $F$ is contained in $\mathbb{Q}_{S_p \cup \{q\}}$, and the arithmetic of $F$ can be analyzed via the tower $\mathbb{Q}_{S_p \cup \{q\}}/\mathbb{Q}$.

The case where $p$ splits in $F$ is easy and can be settled immediately.

**Lemma 7.5.** *If $p$ splits in $F$, then $F$ does not admit a local Minkowski unit.*

**Proof.** It is well known that if $F$ admits a local Minkowski unit, then so does every subfield of $F$ that is Galois over $\mathbb{Q}$. By the Burnside basis theorem, $p$ splits in $F$ if and only if it splits in $\mathbb{Q}_{\{q\}}$. In this case, Theorem 3.11 (ii) together with Remark 3.12 implies that $F$ does not admit a local Minkowski unit. □

Hence, it remains to prove Theorem B in the case where $p$ does not split in $F$. In what follows, we work under this assumption. Following §6.2, we denote by $p_K$ the unique $p$-adic prime of each subfield $K$ of $F$ (both $K$ and $F$ being contained in $\mathbb{Q}_{S_p \cup \{q\}}$). By Corollary 7.3 and Proposition 7.4, $E_F$ is factor equivalent to $\mathcal{A}_{G_{F/\mathbb{Q}}}$ if and only if the equality (13) holds for every extension $K^{\mathrm{el}}_{p,q}/K$ contained in $F$. For ease of notation, we set

$$\begin{aligned} \mathcal{I}_{K,p} &:= \text{the inertia subgroup of } G_{K^{\mathrm{el}}_{p,q}/K} \text{ at } p_{K^{\mathrm{el}}_{p,q}}, \\ \mathcal{I}_{K,q} &:= \text{the inertia subgroup of } G_{K^{\mathrm{el}}_{p,q}/K} \text{ at } q_{K^{\mathrm{el}}_{p,q}}. \end{aligned}$$

**Lemma 7.6.** *Let $F$ be a $p$-rational non-cyclic $p$-extension of $\mathbb{Q}$ with a unique $p$-adic prime. Let $q$ be the rational non-$p$ prime with* $\mathrm{Ram}(F/\mathbb{Q}) = \{p, q\}$. *Let $K$ be a subfield of $F$ with $K^{\mathrm{el}}_{p,q} \subseteq F$. The following claims are valid:*

*(i) We have $\mathcal{I}_{K,p} \neq 1$ and $\mathcal{I}_{K,q} \simeq \mathbb{Z}/p\mathbb{Z}$.*

*(ii) If we have $\mathcal{I}_{K,p} = G_{K^{\mathrm{el}}_{p,q}/K}$, then the necessary condition* (13) *associated to $K^{\mathrm{el}}_{p,q}/K$ is not satisfied.*

*(iii) If we have $\mathcal{I}_{K,p} \neq G_{K^{\mathrm{el}}_{p,q}/K}$ and $\mathcal{I}_{K,p} \neq \mathcal{I}_{K,q}$, then the necessary condition* (13) *associated to $K^{\mathrm{el}}_{p,q}/K$ is satisfied.*

(iv) *If we have* $\mathcal{I}_{K,p} = \mathcal{I}_{K,q}$*, then the necessary condition* (13) *associated to* $K_{p,q}^{\mathrm{el}}/K$ *is satisfied if and only if* $\mathfrak{h}_{K_{p,q}^{\mathrm{el}}} = \mathfrak{h}_K$.

**Proof.** (i) The subgroup $\mathcal{I}_{K,p}$ must be non-trivial because otherwise $p_K$ splits in $K_{p,q}^{\mathrm{el}}$. Since $K$ is $p$-rational and $G_{K_{p,q}^{\mathrm{el}}/K}$ is not cyclic, we have $\mathcal{I}_{K,q} \neq 1$. The cyclicity of $\mathcal{I}_{K,q}$ follows from the class field theory.

(ii) The Galois group $G_{K_{p,q}^{\mathrm{el}}/K}$ is the maximal elementary abelian quotient of $G_{S_p\cup\{q_K\}}(K)$. If $\mathcal{I}_{K,p} = G_{K_{p,q}^{\mathrm{el}}/K}$, then $G_{S_p\cup\{q_K\}}(K)$ coincides with the inertia subgroup at the unique $p$-adic prime by the Burnside basis theorem. Hence, every subfield of $F$ containing $K$ has $p$-class number 1 by Proposition 6.17 and Corollary 6.20. Therefore, the quotient of $p$-class groups in (13) associated with $K_{p,q}^{\mathrm{el}}/K$ is 1, and so the equality in (13) fails.

(iii) The group $\mathcal{I}_{K,p}$ is non-trivial by (i). By the $p$-rationality of $K$, the subgroup $\mathcal{I}_{K,q}$ corresponds to the first layer $K_1$ of $K_\infty/K$. Let $K'$ be the subfield of $K_{p,q}^{\mathrm{el}}$ fixed by the subgroup $\mathcal{I}_{K,p}$. By the assumption, the extensions $K_{p,q}^{\mathrm{el}}/K'$ and $K_1/K$ are ramified precisely at the $p$-adic primes. Hence, we have

$$\mathfrak{h}_K = \mathfrak{h}_{K_1} = \mathfrak{h}_{K'} = \mathfrak{h}_{K_{p,q}^{\mathrm{el}}} = 1$$

by Lemma 6.4 (ii). For any other degree $p$-extension $N$ of $K$ in $K_{p,q}^{\mathrm{el}}$ distinct from $K'$ and $K_1$, the extension $K_{p,q}^{\mathrm{el}}/N$ is unramified, since $K_{p,\mathfrak{q}}^{\mathrm{el}}$ is equal to both $NK_1$ and $NK'$. By Lemma 6.4 (i), we then have $\mathfrak{h}_N = p$ for all such $N$. Thus, condition (13) is satisfied for the extension $K_{p,q}^{\mathrm{el}}/K$.

(iv) In this case, the first layer $K_1$ of $K_\infty/K$ is the subfield of $K_{p,q}^{\mathrm{el}}$ corresponding to the subgroup $\mathcal{I}_{K,p} = \mathcal{I}_{K,q}$. For any degree-$p$ extension $N$ of $K$ contained in $K_{p,q}^{\mathrm{el}}$ other than $K_1$, we have $K_{p,q}^{\mathrm{el}} = N_1$. Therefore, we have

$$\mathfrak{h}_K = p \cdot \mathfrak{h}_{K_1}, \qquad \mathfrak{h}_N = p \cdot \mathfrak{h}_{K_{p,q}^{\mathrm{el}}}$$

for all such $N$ by Proposition 6.3. From these identities, the claim follows.

□

Before proving Theorem B, we recall a well-known fact about the subgroup lattice of the non-abelian semi-direct product $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

**Lemma 7.7.** *Let $p$ be an odd prime, and let $G \simeq \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ be the non-abelian semidirect product. Then, $G$ has a unique subgroup $H$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$. Moreover, every subgroup of $G$ of order $p$ is contained in $H$.*

**Proof.** By elementary arguments, one checks that the center $Z(G)$ of $G$ coincides with the commutator subgroup $[G,G]$. Every subgroup of $G$ of order $p^2$ must contain the center, because otherwise $G$ would be abelian. Since the quotient $G/Z(G) = G/[G,G]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, there are precisely $p+1$

subgroups of $G$ of order $p^2$. It is known that $G$ admits the following presentation (cf. [62, Exercise 5.3.6])

$$\langle x, y \mid x^{p^2} = 1 = y^p,\ y^{-1}xy = x^{1+p} \rangle.$$

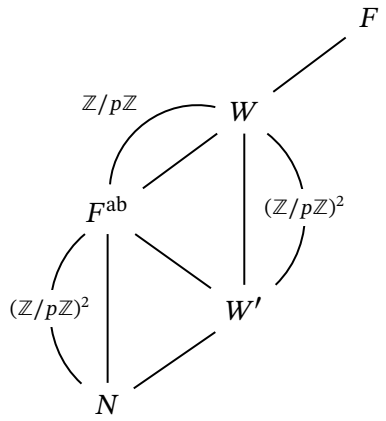
Using the congruence

$$(xy)^n \equiv x^n y^n (y^{-1}x^{-1}yx)^{n(n-1)/2} \equiv [[G,G],G]$$

(cf. [23, §0.1]), we can check that the elements $xy^i$ for $1 \leq i \leq p$ generate $p$ distinct normal cyclic subgroups of order $p^2$. Therefore, the non-cyclic subgroup $H$ of order $p^2$ generated by $x^p$ and $y$ is the unique subgroup of $G$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$. The last claim follows because every subgroup of order $p$ is either equal to $Z(G)$ or generates a rank-2 elementary abelian subgroup with $Z(G)$. □

**Proof of Theorem B.** First, the extension $F/F^{\mathrm{ab}}$ is cyclic and $q_{F^{\mathrm{ab}}}$ is totally ramified in $F$. If $F/F^{\mathrm{ab}}$ were not cyclic, then we would have $(F^{\mathrm{ab}})^{\mathrm{el}}_{p,q} \subsetneq F$. Then, we have a contradiction to the maximality of $F^{\mathrm{ab}}$ because $(F^{\mathrm{ab}})_1$, which is a subfield of $(F^{\mathrm{ab}})^{\mathrm{el}}_{p,q}$, is abelian over $\mathbb{Q}$. Similarly, $q_{F^{\mathrm{ab}}}$ must be totally ramified in $F$ because otherwise $(F^{\mathrm{ab}})_1$ would be a subfield of $F$.

Since $G_{F/F^{\mathrm{ab}}}$ is cyclic, there exists a unique extension $W$ of $F^{\mathrm{ab}}$ in $F$ with $[W : F^{\mathrm{ab}}] = p$. As both $F$ and $F^{\mathrm{ab}}$ are Galois over $\mathbb{Q}$, the same holds true for $W$. Let $N$ be the subfield of $F^{\mathrm{ab}}$ such that $G_{F^{\mathrm{ab}}/N}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$. Then, $G_{W/N}$ is either isomorphic to $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ or to the non-abelian semi-direct product $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. By considering their subgroup lattices, one finds a subfield $N \subsetneq W' \subsetneq F^{\mathrm{ab}}$ with $G_{W/W'} \simeq (\mathbb{Z}/p\mathbb{Z})^2$ (cf. Lemma 7.7). We will show that the necessary condition (13) associated with $W/W'$ for the factor equivalence of $E_F$ and $\mathcal{A}_{G_{F/\mathbb{Q}}}$ is not satisfied.




Since $F^{\mathrm{ab}}$ contains $\mathbb{Q}^{\mathrm{el}}_{p,q}$, the prime $q$ is ramified in $F$. Moreover, by the primitivity of $S_p \cup \{q\}$, we have $q \not\equiv 1 \pmod{p^2}$. Hence, by local class field theory, the ramification index of $q$ in $F^{\mathrm{ab}}/\mathbb{Q}$ is exactly $p$.

The prime $q$ must also be ramified in $W'/\mathbb{Q}$, for otherwise $F^{\mathrm{ab}}/W'$ would be ramified at $q_{W'}$, forcing $\mathcal{I}_{W',q} = G_{W/W'}$ and thereby contradicting Lemma 7.6 (i).

Since the compositum $\mathbb{Q}_{\{q\}}W'$ is abelian over $\mathbb{Q}$, the previous argument shows that $q_{W'}$ is unramified in $W'\mathbb{Q}_{\{q\}}/W'$. Thus we deduce that $\mathbb{Q}_{\{q\}} \subset H_{W'}$.

We now complete the proof by applying Lemma 7.6 to the extension $W/W'$. There are three possible cases for the relation among $\mathcal{I}_{W',p}$, $\mathcal{I}_{W',q}$, and $G_{W/W'}$.

(i) If we have $\mathcal{I}_{W',p} = G_{W/W'}$, then $E_F$ is not factor equivalent to $\mathcal{A}_{G_{F/\mathbb{Q}}}$ by Lemma 7.6 (ii).

(ii) The case $\mathcal{I}_{W',p} \neq G_{W/W'}$ and $\mathcal{I}_{W',p} \neq \mathcal{I}_{W',q}$ (i.e., Lemma 7.6 (iii)) cannot occur. Otherwise, we have $\mathfrak{h}_{W'} = 1$ by the proof of Lemma 7.6 (iii). Since $H_{W'} = W'$ contains $\mathbb{Q}_{\{q\}}$, we then obtain $G_{W/W'} = \mathcal{I}_{W',p}$ by Corollary 6.20, a contradiction.

(iii) If we have $\mathcal{I}_{W',p} \neq G_{W/W'}$ and $\mathcal{I}_{W',p} = \mathcal{I}_{W',q}$, then the necessary condition (13) associated to $W/W'$ is satisfied if and only if we have $\mathfrak{h}_W = \mathfrak{h}_{W'}$ by Lemma 7.6 (iv). Furthermore, the proof of Lemma 7.6 (iv) shows that this equality holds if and only if we have $\mathfrak{h}_N = p\mathfrak{h}_{W'}$ for every degree-$p$ extension $N$ of $W'$ in $W$ in which both $p_{W'}$ and $q_{W'}$ are ramified. Since we have $\mathbb{Q}_{\{q\}} \subseteq H_{W'}$, we have $\mathfrak{h}_{W'} = \mathfrak{h}_N$ for all such $N$ by Proposition 6.21. Thus, the necessary condition is not satisfied.

□

## 8. Relative Galois module structure of the unit lattices of totally real *p*-rational number fields

In this final section, we study the relative Galois module structure of the unit lattices for Galois extensions of totally real $p$-rational number fields. We begin by introducing the following notation, which is convenient for the discussion. For each Galois extension $L/K$ of number fields and each finite set $S$ of places of $K$, we write $S_L$ for the set of places of $L$ above $S$, and $S_{L,f}$ for the set of finite places of $L$ above $S$. We denote by $\mathcal{O}_{L,S}^{\times}$ the group $\mathcal{O}_{L,S_L}^{\times}$ of $S_L$-units of $L$, and by $\mathrm{Cl}_S(L)$ the $S_L$-ideal class group of $L$. As in the case of $S_p$, we let $S_\infty$ denote the set of infinite places of a base field. Finally, we set $E_{L,S} := \mathcal{O}_{L,S}^{\times}/\mu(L)$.

In [14], for a *fixed* general finite group $G$ and *varying* Galois extensions $L/K$ of number fields with $G_{L/K} \simeq G$, Burns studied the $\mathbb{Z}_p[G]$-module structures of the pro-$p$ completions of several arithmetic objects attached to $L$. In particular, his results apply to $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_{L,S}$ for any finite set $S$ of primes of $K$ containing $S_p \cup S_\infty \cup \mathrm{Ram}(L/K)$. In this section, for every Galois extension $L/K$ with $G_{L/K} \simeq G$, we fix a group isomorphism and consider $E_L$ as a $\mathbb{Z}[G]$-lattice.

This investigation of the $\mathbb{Z}_p[G]$-structure of $E_{L,S}$ for varying $L/K$ is of intrinsic interest because, as $L/K$ varies, the $\mathbb{Z}_p$-ranks of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_{L,S}$ are unbounded. Consequently, if the $p$-Sylow subgroup of $G$ is not cyclic of order 1, $p$, or $p^2$,

then infinitely many non-isomorphic indecomposable $\mathbb{Z}_p[G]$-lattices can appear in the Krull-Schmidt decomposition of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_{L,S}$ (cf. [19, §81.A]). Beyond this intrinsic interest, the knowledge of relative Galois module structures of the unit lattices also has various applications in the study of tamely ramified pro-$p$ extensions of number fields (cf. [40, 50]).

Let $S$ be a finite set of places of $\mathbb{Q}$ containing $S_p \cup S_\infty$, and let $L/K$ be a Galois extension of number fields with Galois group $G$ that is unramified outside $S$. In [14], Burns proved that the sum of the $\mathbb{Z}_p$-ranks of the non-projective components in a Krull-Schmidt decomposition of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_{L,S}$ (as $\mathbb{Z}_p[G]$-lattices) is bounded above by a function that depends only on $|G|$, the $p$-rank of $\mathrm{Cl}_S(L(\zeta_p))$, and $|S_{L,f}|$. By the Jordan-Zassenhaus theorem (cf. [20, Thm. 24.2]), we obtain the following result.

**Theorem 8.1.** *(*[14, Cor. 4.1]*) Let $S$ be a finite set of places of $\mathbb{Q}$ containing $S_p \cup S_\infty$. Let $G$ be a finite group and $b$ a natural number. Define* $\mathrm{Ext}(G, S, b)$ *to be the family of Galois extensions of number fields $L/K$ satisfying the following conditions :*

*(i)* $G_{L/K} \simeq G$,
*(ii)* $\zeta_p \in K$,
*(iii)* $L/K$ *is unramified outside* $S$,
*(iv)* $\mathrm{rk}_p(Cl_S(L)) + |S_{L,f}| \leq b$.

*Then, there exists a finite set $\Omega$ of $\mathbb{Z}_p[G]$-lattices such that for every $L/K \in \mathrm{Ext}(G, S, b)$, there exists $X \in \Omega$ and a projective $\mathbb{Z}_p[G]$-lattice $P$ with*

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} E_{L,S} \simeq X \oplus P$$

*as $\mathbb{Z}_p[G]$-lattices.*

**Remark 8.2.** Theorem 8.1 was obtained by analyzing the Krull-Schmidt decomposition of étale cohomology groups and the compactly supported $p$-adic étale cohomology groups of general $p$-adic Galois representations over number fields. Theorem 8.1 is formulated in terms of $S$-units for $S \supset S_p \cup S_\infty$ because $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_{L,S}^\times$ is isomorphic to the étale cohomology group $H^1(\mathrm{Spec}(\mathcal{O}_{L,S})_{\acute{e}t}, \mathbb{Z}_p(1))$. The paper [14] also treats the ray class groups (cf. Artin-Verdier duality) and higher algebraic K-groups (cf. Voevodsky's Theorem). For further details we refer the readers to [14, §4].

We conclude this paper by establishing that for Galois extensions of totally real $p$-rational number fields, an analogous phenomenon occurs in the relative Galois module structure of the group of *ordinary* units.

**Theorem 8.3** (Theorem C)**.** *Let $G$ be a finite group and $p$ an odd prime. Then, there exists a finite set $\Omega$ of $\mathbb{Z}_p[G]$-lattices such that for every Galois extension $L/K$ of totally real $p$-rational number fields with $G_{L/K} \simeq G$, there exists $X \in \Omega$ and an integer $m \geq 0$ such that $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_L$ is factor equivalent to $X \oplus \mathbb{Z}_p[G]^m$ as $\mathbb{Z}_p[G]$-lattices.*

**Proof.** By Lemma 6.4 (i), for every extension $M/N$ of totally real $p$-rational number fields, we have the inequalities

$$v_p(\mathfrak{h}_N) - v_p([M : N]) \leq v_p(\mathfrak{h}_M) \leq v_p(\mathfrak{h}_N) + \log_p[M : N].$$

Therefore, for any fixed $G$-relation $\Theta$ and varying Galois extensions $M/N$ of totally real $p$-rational number fields with $G_{M/N} \simeq G$, only finitely many values for $v_p(\mathcal{C}_\Theta(E_M))$ can occur by Lemma 3.18.

Fix a $\mathbb{Z}$-basis Y of the group of $G$-relations, and let $\Xi$ be the set of functions $f : \mathrm{Y} \to \mathbb{Z}$ such that there exists a Galois extension $M/N$ of totally real $p$-rational number fields with $G_{M/N} \simeq G$, such that

$$f(\Theta) = v_p(\mathcal{C}_\Theta(E_M))$$

for every $\Theta \in \mathrm{Y}$. By the above argument, $\Xi$ is a finite set.

For each $x \in \Xi$, choose a Galois extension $L_x/K_x$ of totally real $p$-rational fields with minimal $[K_x : \mathbb{Q}]$ such that we have $G_{L_x/K_x} \simeq G$ and $x(\Theta) = v_p(\mathcal{C}_\Theta(E_{L_x}))$ for every $\Theta \in \mathrm{Y}$. We now show that the set

$$\Omega = \left\{ \mathbb{Z}_p \otimes_{\mathbb{Z}} E_{L_x} \right\}_{x \in \Xi}$$

satisfies the claim of the theorem.

Let $L/K$ be a Galois extension of totally real $p$-rational fields with $G_{L/K} \simeq G$. Proposition 3.23 implies that the factor equivalence class of $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_L$ as a $\mathbb{Z}_p[G]$-lattice is uniquely determined by $v_p(\mathcal{C}_\Theta(E_L))$ for all the $G$-relations $\Theta \in \mathrm{Y}$. From the construction of $\Xi$, there exists a unique $y \in \Xi$ such that we have $v_p(\mathcal{C}_\Theta(E_L)) = y(\Theta)$ for every $\Theta \in \mathrm{Y}$. We claim that $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_L$ is factor equivalent to $\mathbb{Z}_p \otimes_{\mathbb{Z}} V$ as $\mathbb{Z}_p[G]$-lattices, where we have

$$V := E_{L_y} \oplus \mathbb{Z}[G]^m, \quad \text{with} \quad m = \frac{[L : \mathbb{Q}] - [L_y : \mathbb{Q}]}{|G|}.$$

By the Dirichlet-Herbrand theorem (cf. [35, Lem. I.3.6]), the two $\mathbb{Z}[G]$-lattices $E_L$ and $V$ have the same rational representation. Moreover, for every $\Theta \in \mathrm{Y}$, we have

$$v_p(\mathcal{C}_\Theta(V)) = v_p(\mathcal{C}_\Theta(E_{L_y})) = v_p(\mathcal{C}_\Theta(E_L)).$$

The first equality follows from Lemma 3.17 and Lemma 3.19. The second equality follows from the construction of $E_{L_y}$. Therefore, by Proposition 3.23, we conclude that $\mathbb{Z}_p \otimes_{\mathbb{Z}} E_L$ is factor equivalent to $\mathbb{Z}_p \otimes_{\mathbb{Z}} V$ as $\mathbb{Z}_p[G]$-lattices. □

As discussed in §6.2, the arithmetic is particularly simple in a pro-$p$ tower of totally real $p$-rational fields $F_{S_p \cup \{\mathfrak{q}\}}/F$ for $(F, p, \mathfrak{q})$ satisfying (U).

**Theorem 8.4** (Theorem D)**.** *Let $F$ be a totally real $p$-rational number field, and let $\mathfrak{q}$ be a non-$p$-adic prime of $F$ such that $(F, p, \mathfrak{q})$ satisfies* (U)*. For every Galois extension $L/K$ satisfying*

$$F_{\{\mathfrak{q}\}} \subseteq K \subseteq L \subset F_{S_p \cup \{\mathfrak{q}\}},$$

*the $\mathbb{Z}[G_{L/K}]$-lattices $E_L$ and $\mathcal{A}_{G_{L/K}} \oplus I_{G_{L/K}} \oplus \mathbb{Z} \oplus \mathbb{Z}[G_{L/K}]^{[K:\mathbb{Q}]-2}$ are factor equivalent.*

**Proof.** Let $L/K$ be a Galois extension of totally real $p$-rational fields as in the statement of the theorem. From the isomorphisms $\mathbb{Q}[G_{L/K}] \simeq \mathbb{Q} \otimes_{\mathbb{Z}} (I_{G_{L/K}} \oplus \mathbb{Z})$ of $\mathbb{Q}[G_{L/K}]$-modules, we have an isomorphism

$$\mathbb{Q} \otimes_{\mathbb{Z}} E_L \simeq \mathbb{Q} \otimes_{\mathbb{Z}} (\mathcal{A}_{G_{L/K}} \oplus I_{G_{L/K}} \oplus \mathbb{Z} \oplus \mathbb{Z}[G_{L/K}]^{[K:\mathbb{Q}]-2})$$

of $\mathbb{Q}[G_{L/K}]$-modules. By Theorem 3.22, it remains to show that $E_L$ and $\mathcal{A}_{G_{L/K}} \oplus I_{G_{L/K}} \oplus \mathbb{Z} \oplus \mathbb{Z}[G_{L/K}]^{[K:\mathbb{Q}]-2}$ have the same regulator constants for all $G$-relations of $G_{L/K}$. By the Brauer-Kuroda theorem and Theorem 3.25, for a $G$-relation $\Theta = \sum_{H \leq G_{L/K}} n_H H$, we have

$$\mathcal{C}_\Theta(E_L) = \mathcal{C}_\Theta(\mathbb{Z}) \cdot \prod_{H \leq G_{L/K}} \left( \frac{w_{L^H}}{h_{L^H} \lambda(H)} \right)^{2n_H}.$$

As a consequence, we have $\mathcal{C}_\Theta(E_L) = \mathcal{C}_\Theta(\mathbb{Z})$ by the argument used in the proof of Proposition 7.2 and Proposition 6.17. On the other hand, we have

$$\mathcal{C}_\Theta(\mathcal{A}_{G_{L/K}} \oplus I_{G_{L/K}} \oplus \mathbb{Z} \oplus \mathbb{Z}[G_{L/K}]^{[K:\mathbb{Q}]-2}) = \mathcal{C}_\Theta(\mathbb{Z})$$

by Lemma 3.17, Lemma 3.19, and Corollary 4.3. □

**Remark 8.5.** We remark that our results can be extended to other families of Galois extensions provided that the Galois group and its relationship with inertia subgroups at the ramified primes are sufficiently simple.

One easy example is when $F$ is an imaginary number field with a unique $p$-adic prime and $p$-class number 1. Then $G_{S_p}(F)$ coincides with the inertia subgroup at the $p$-adic place. Hence, the $p$-adic prime of $F$ is totally ramified in $F_{S_p}$. As a consequence, every extension of $F$ in $F_{S_p}$ has $p$-class number 1.

Thus Theorem B holds for every extension $L$ of $F$ in $F_{S_p}$ that is Galois over an imaginary quadratic field and has non-cyclic $G_{L/F}$. Moreover, Theorem D also applies to every Galois extension of number fields in the tower $F_{S_p}/F$, provided $F$ does not contain the $p$th roots of unity.

As an explicit illustration, for $p = 3$ one can take $F = \mathbb{Q}(\sqrt{6}, \sqrt{-1})$ [67, p. 239]. We note that this field is not 3-rational.

**Remark 8.6.** After this work was completed, the results of Burns in the direction of Theorem 8.1 on the $S$-unit group were extended to ordinary unit lattices in [48, Thm. A]. Since the classification of integral representations is unavailable in general, information on the $\mathbb{Z}_p$-ranks of the non-projective components alone does not effectively bound the number of possible $\mathbb{Z}_p[G]$-module structures (cf. [48, Thm. B]).

Theorem C shows that the number of possible factor equivalence classes of unit lattices of totally real $p$-rational fields—depending only on the set of $G$-relations—is highly restricted, in sharp contrast with genus equivalence. This

rigidity also indicates, however, that factor equivalence itself provides only limited information about the underlying Galois module structure.

For readers interested in the Krull–Schmidt decomposition of unit lattices in cyclic $p$-extensions of totally real $p$-rational fields, we refer to [15]. In a different direction, Ozaki obtained a result [61] on the Galois structure of unit lattices in cyclic $p$-extensions, indicating that the range of genus equivalence classes of the unit lattice is essentially as large as that of integral $\mathbb{Z}_p[G]$-modules.

## References


[1] BARTEL, A. On Brauer–Kuroda type relations of $S$-class numbers in dihedral extensions. *J. Reine Angew. Math.* **668** (2012), 211–244. MR2948877, doi: 10.1515/CRELLE.2011.152, Zbl 1270.11115. 1441, 1453, 1454, 1455, 1456

[2] BARTEL, A. Factor equivalence of Galois modules and regulator constants. *Int. J. Number Theory* **10** (2014), no. 1, 1–12. MR3189963, doi: 10.1142/S1793042113500772, Zbl 1286.11185. 1441, 1446, 1455

[3] BARTEL, A.; DE SMIT, B. Index formulae for integral Galois modules. *J. Lond. Math. Soc. (2)* **88** (2013), no. 3, 845–859. MR3145134, doi: 10.1112/jlms/jdt033, Zbl 1290.11152. 1461

[4] BARTEL, A.; DOKCHITSER, T. Brauer relations in finite groups. *J. Eur. Math. Soc. (JEMS)* **17** (2015), no. 10, 2473–2512. MR3420514, doi: 10.4171/JEMS/563, Zbl 1331.19002. 1458, 1469

[5] BENMERIEME, Y.; MOVAHHEDI, A. Multi-quadratic $p$-rational number fields. *J. Pure Appl. Algebra* **225** (2021), no. 9, Article no. 106657, 17 pp. MR4192837, doi: 10.1016/j.jpaa.2020.106657, Zbl 1470.11290. 1462

[6] BIASSE, J. F.; FIEKER, C.; HOFMANN, T.; PAGE, A. Norm relations and computational problems in number fields. *J. Lond. Math. Soc. (2)* **105** (2022), no. 4, 2373–2414. MR4440537, doi: 10.1112/jlms.12563, Zbl 1530.11098. 1461

[7] BOUC, S. The Dade group of a $p$-group. *Invent. Math.* **164** (2006), 189–231. MR2207787, doi: 10.1007/s00222-005-0476-6, Zbl 1099.20004. 1469

[8] BOUVIER, L.; PAYAN, J. J. Sur la structure galoisienne du groupe des unités d'un corps abélien de type $(p, p)$. *Ann. Inst. Fourier (Grenoble)* **29** (1979), 171–187. MR0526783, doi: 10.5802/aif.733, Zbl 0387.12007. 1445

[9] BRAUER, R. Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers. *Math. Nachr.* **4** (1951), 158–174. MR0039760, doi: 10.1002/mana.3210040116, Zbl 0042.03801. 1459, 1460

[10] BRUMER, A. On the group of units of an absolutely cyclic number field of prime degree. *J. Math. Soc. Japan* **21** (1969), no. 3, 357–358. MR0244193, doi: 10.2969/jmsj/02130357, Zbl 0188.35301. 1445

[11] BURNS, D. J. Factorisability, group lattices and Galois module structure. *J. Algebra* **134** (1990), 257–270. MR1074329, doi: 10.1016/0021-8693(90)90053-Q, Zbl 0734.11064. 1447, 1448, 1449

[12] BURNS, D. J. On the Galois structure of units in number fields. *Proc. London Math. Soc.* **66** (1993), no. 3, 71–91. MR1189093, doi: 10.1112/plms/s3-66.1.71, Zbl 0806.11049. 1440, 1441, 1442, 1447, 1448, 1449, 1450, 1451, 1452, 1460

[13] BURNS, D. J. On Artin formalism for the conjecture of Bloch and Kato. *Math. Res. Lett.* **19** (2013), no. 5, 1155–1169. MR3039838, doi: 10.4310/MRL.2012.v19.n5.a16, Zbl 1368.11051. 1453

[14] BURNS, D. J. On the Galois structure of arithmetic cohomology I: Compactly supported $p$-adic cohomology. *Nagoya Math. J.* **239** (2020), 294–321. MR4138903, doi: 10.1017/nmj.2018.41, Zbl 1459.11217. 1442, 1474, 1475

[15] BURNS, D. J.; LIM, D.; MAIRE, C. On the existence of Minkowski units. *arXiv preprint arXiv:2401.00181* (2023). 1469, 1478

[16] CASSOU-NOGUÈS, PH.; CHINBURG, T.; FRÖHLICH, A.; TAYLOR, M. J. $L$-functions and Galois modules, $L$-functions and arithmetic. In: *London Math. Soc. Lecture Note Ser.*, vol. 153 (1991), 75–139. MR1110391, doi: 10.1017/CBO9780511526053.005, Zbl 0733.11044. 1446

[17] CHATTOPADHYAY, J.; LAXMI, H.; SAIKIA, A. On the $p$-rationality of consecutive quadratic fields. *J. Number Theory* **248** (2023), 14–26. MR4556155, doi: 10.1016/j.jnt.2023.01.001, Zbl 1526.11061. 1464

[18] CONRAD, K. On the origin of representation theory. *Enseign. Math.* **44** (1998), no. 2, 361–392. 1457

[19] CURTIS, C. W.; REINER, I. Representation theory of finite groups and associative algebras. *AMS Chelsea Publishing, Providence, RI*, (2006). Reprint of the 1962 original. MR0144979, Zbl 1093.20003. 1445, 1447, 1475

[20] CURTIS, C. W.; REINER, I. Methods of representation theory. Vol. I. *John Wiley & Sons, Inc.*, New York (1981). MR1038525, Zbl 0469.20001. 1475

[21] DE SMIT, B. Factor equivalence results for integers and units. *Enseign. Math. (2)* **42** (1996), no. 2, 383–394. MR1426445, Zbl 0884.11044. 1446, 1447, 1448, 1450, 1455

[22] DIEDERICHSEN, F. E. Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz. *Abh. Math. Sem. Hansischen Univ.* **13** (1940), 357–412. MR0002133, doi: 10.1007/BF02940768, Zbl 0023.01302. 1445

[23] DIXON, J. D.; DU SAUTOY, M. P. F.; MANN, A.; SEGAL, D. Analytic pro-$p$ groups, 2nd Edition. Cambridge Studies in Advanced Mathematics 61. *Cambridge University Press.* (1999) xviii+368 pp. ISBN: 0-521-65011-9. MR1720368, doi: 10.1017/CBO9780511470882, Zbl 0934.20001. 1467, 1473

[24] DOKCHITSER, T.; DOKCHITSER, V. Regulator constants and the parity conjecture. *Invent. Math.* **178** (2009), no. 1, 23–71. MR2534092, doi: 10.1007/s00222-009-0193-7, Zbl 1219.11083. 1441, 1453, 1454

[25] DOKCHITSER, T.; DOKCHITSER, V. On the Birch–Swinnerton–Dyer quotients modulo squares. *Ann. of Math. (2)* **172** (2010), no. 1, 567–596. MR2680426, doi: 10.4007/annals.2010.172.567, Zbl 1223.11079. 1452

[26] DUVAL, D. Sur la structure galoisienne du groupe des unités d'un corps abélien réel de type $(p, p)$. *Séminaire de théorie des nombres de Grenoble* **7** (1978–1979), 1–41. 1445

[27] DUVAL, D. Sur la structure galoisienne du groupe des unités d'un corps abélien réel de type $(p, p)$. *J. Number Theory* **13** (1981), no. 2, 228–245. MR0612684, doi: 10.1016/0022-314X(81)90006-8, Zbl 0459.12002. 1445, 1446, 1460

[28] FRÖHLICH, A. Central extensions, Galois groups, and ideal class groups of number fields. *Contemp. Math.* **24** (1983). MR0720859, doi: 10.1090/conm/024, Zbl 0519.12001. 1451

[29] FRÖHLICH, A. Module defect and factorisability. *Illinois J. Math.* **32** (1988), no. 3, 407–421. MR0947035, doi: 10.1215/ijm/1255988994, Zbl 0664.12007. 1447, 1449, 1450, 1456

[30] FRÖHLICH, A. $L$-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. MR0993218, doi: 10.1515/crll.1989.397.42, Zbl 0693.12012. 1447, 1448, 1450, 1455

[31] FURUTA, Y. The genus field and genus number in algebraic number fields. *Nagoya Math. J.* **29** (1967), 281–285. MR0209260, doi: 10.1017/S0027763000024387, Zbl 0166.05901. 1451

[32] GRAS, G. Groupe de Galois de la $p$-extension abélienne $p$-ramifiée maximale d'un corps de nombres. *J. Reine Angew. Math.* **333** (1982), 86–132. MR0660786, doi: 10.1515/crll.1982.333.86, Zbl 0477.12009. 1464

[33] GRAS, G. Logarithme $p$-adique et groupes de Galois. *J. Reine Angew. Math.* **343** (1983), 64–80. MR0705877, doi: 10.1515/crll.1983.343.64, Zbl 0501.12015. 1464

[34] GRAS, G. Remarks on $K_2$ of number fields. *J. Number Theory* **23** (1986), no. 3, 322–335. MR0846962, doi: 10.1016/0022-314X(86)90077-6, Zbl 0589.12010. 1464

[35] GRAS, G. Class field theory: from theory to practice, corr. 2nd ed. Springer (2005). MR1941965, doi: 10.1007/978-3-662-11323-3, Zbl 1019.11032. 1448, 1462, 1476

[36] GRAS, G. Les $\theta$-régulateurs locaux d'un nombre algébrique: conjectures $p$-adiques. *Canad. J. Math.* **68** (2016), 571–624. MR3492629, doi: 10.4153/CJM-2015-026-3, Zbl 1351.11033. 1462, 1464

[37] GRAS, G. Algorithmic complexity of Greenberg's conjecture. *Arch. Math. (Basel)* **117** (2021), no. 3, 277–289. MR4293861, doi: 10.1007/s00013-021-01618-9, Zbl 1469.11420. 1461

[38] GRAS, G. Tate–Shafarevich groups in the cyclotomic $\widehat{\mathbb{Z}}$-extension and Weber's class number problem. *J. Number Theory* **228** (2021), 219–252. MR4271818, doi: 10.1016/j.jnt.2021.04.019, Zbl 1472.11279. 1461

[39] GREENBERG, R. Galois representations with open image. *Ann. Math. Qué.* **40** (2016), no. 1, 83–119. MR3512524, doi: 10.1007/s40316-015-0050-6, Zbl 1414.11151. 1442, 1464

[40] HAJIR, F.; MAIRE, C.; RAMAKRISHNA, R. Deficiency of $p$-class tower groups and Minkowski units. *Ann. Inst. Fourier (Grenoble)* **75** (2025), no. 4, 1415–1462. MR4940709, doi: 10.5802/aif.3677, Zbl 08076176. 1475

[41] HELLER, A.; REINER, I. Representations of cyclic groups in rings of integers I. *Ann. of Math. (2)* **76** (1962), no. 2, 73–92. MR0140575, doi: 10.2307/1970266, Zbl 0108.03101. 1446

[42] HELLER, A.; REINER, I. Representations of cyclic groups in rings of integers II. *Ann. of Math. (2)* **77** (1963), no. 2, 318–328. MR0144980, doi: 10.2307/1970218, Zbl 0119.03004. 1446

[43] JAULENT, J. F. Unités et classes dans les extensions métabéliennes de degré $n\ell^s$ sur un corps de nombres algébriques. *Ann. Inst. Fourier (Grenoble)* **31** (1981), no. 1, 39–62. MR0613028 doi: 10.5802/aif.816, Zbl 0436.12007. 1445

[44] JAULENT, J. F. Sur la $\mathbb{Z}_\ell[G]$-structure des unités principales d'un corps local et des unités globales d'un corps de nombres à groupe de Galois métacyclique. *Abh. Math. Sem. Univ. Hamburg* **52** (1982), 235–253. MR0710548, doi: 10.1007/BF02941881, Zbl 0493.12020. 1445

[45] JAULENT, J. F.; NGUYEN QUANG DO, T. Corps $p$-rationnels, corps $p$-réguliers, et ramification restreinte. *J. Théor. Nombres Bordeaux* **5** (1993), no. 2, 343–363. MR1265910, Zbl 0957.11046. 1461, 1462

[46] KOCH, H. Galois theory of $p$-extensions. Springer Monographs in Mathematics. *Springer Verlag*, Berlin, (2002). xiv+190 pp. ISBN: 3-540-43629-4. MR1930372, doi: 10.1007/978-3-662-04967-9, Zbl 1023.11002. 1462

[47] KOPERECZ, J. Triquadratic $p$-rational fields. *J. Number Theory* **242** (2023), 402–408. MR4490454, doi: 10.1016/j.jnt.2022.04.011, Zbl 1509.11106. 1464

[48] KUMON, A.; LIM, D. On Krull–Schmidt decompositions of unit groups of number fields. *Acta Arith.* **218** (2025), no. 1, 77–96. MR4870081, doi: 10.4064/aa240314-24-8, Zbl 08012199. 1477

[49] KURODA, S. Über die Klassenzahlen algebraischer Zahlkörper. *Nagoya Math. J.* **1** (1950), 1–10. MR0039759, doi: 10.1017/S0027763000022777, Zbl 0037.16101. 1459

[50] LEE, Y.; LIM, D. The finitude of tamely ramified pro-$p$ extensions of number fields with cyclic $p$-class groups. *J. Number Theory* **259** (2024), 338–356. MR4711123, doi: 10.1016/j.jnt.2024.01.005, Zbl 1557.11150. 1467, 1475

[51] LIM, D. On $p$-rationality of $\mathbb{Q}(\zeta_{2\ell+1})^+$ for Sophie Germain primes $\ell$. *J. Number Theory* **231** (2022), 378–400. MR4330938, doi: 10.1016/j.jnt.2021.05.009, Zbl 1484.11207. 1468

[52] MAIRE, C. On Galois representations with large image. *Trans. Amer. Math. Soc.* **376** (2023), 7287–7305. MR4636685, doi: 10.1090/tran/8952, Zbl 1540.11058. 1464

[53] MARKO, F. On the existence of Minkowski units in totally real cyclic fields. *J. Théor. Nombres Bordeaux* **17** (2005), no. 1, 195–206. MR2152220, doi: 10.5802/jtnb.486, Zbl 1089.11062. 1445

[54] MARSZALEK, R. Minkowski units in certain metacyclic fields. *Acta Arith.* **51** (1988), 381–391. MR0971088, doi: 10.4064/aa-51-4-381-391, Zbl 0665.12006. 1445

[55] MARSZALEK, R. Minkowski units in a class of metabelian fields. *J. Number Theory* **37** (1991), 67–91. MR1089790, doi: 10.1016/S0022-314X(05)80025-3, Zbl 0728.11060. 1445, 1460

[56] MOVAHHEDI, A. Sur les $p$-extensions des corps $p$-rationnels. Ph.D. thesis, Paris 7 (1988). 1462, 1464

[57] MOVAHHEDI, A. Sur les $p$-extensions des corps $p$-rationnels. *Math. Nachr.* **149** (1990), 163–176. MR1124802, doi: 10.1002/mana.19901490113, Zbl 0723.11054. 1461, 1462, 1464, 1465

[58] MOVAHHEDI, A.; NGUYEN QUANG DO, T. Sur l'arithmétique des corps de nombres $p$-rationnels. In: *Séminaire de Théorie des Nombres de Paris, 1987–88*, C. Goldstein (ed.), Birkhäuser (1990), 155–200. MR1042770, doi: 10.1007/978-1-4612-3460-9_9, Zbl 0703.11059. 1442, 1461, 1462, 1465

[59] NELSON, A. Monomial representations and Galois module structure. Ph.D. thesis, King's College, University of London (1979). 1446

[60] NEUKIRCH, J. Algebraic number theory. *Springer Verlag*, Berlin, (1999). xviii+571 pp. ISBN: 3-540-65399-6. MR1697859, doi: 10.1007/978-3-662-03983-0, Zbl 0956.11021. 1468

[61] OZAKI, M. Construction of a cyclic $p$-extension of number fields whose unit group has prescribed Galois module structure. *arXiv preprint arXiv:2507.12949* (2025). 1478

[62] ROBINSON, D. J. S. A Course in the Theory of Groups. *Springer*, New York, (2012), vol. 80. MR1357169, doi: 10.1007/978-1-4419-8594-1, Zbl 0836.20001. 1459, 1473

[63] SERRE, J. P. Linear representations of finite groups. Graduate Texts in Mathematics, vol. 42. *Springer-Verlag*, New York-Heidelberg, (1977). MR0450380, doi: 10.1007/978-1-4684-9458-7, Zbl 0355.20006. 1445, 1452

[64] SERRE, J. P. Galois cohomology. *Springer* (1994). MR1324577, doi: 10.1007/978-3-642-59141-9, Zbl 0902.12004. 1464, 1471

[65] TORZEWSKI, A. Regulator constants of integral representations of finite groups. *Math. Proc. Cambridge Philos. Soc.* **168** (2020), no. 1, 75–117. MR4043822, doi: 10.1017/S0305004118000579, Zbl 1506.20003. 1454

[66] ULLOM, S. V.; WATT, S. B. Class number restrictions for certain $\ell$-extensions of imaginary quadratic fields. *Illinois J. Math.* **32** (1988), 422–427. MR0947036, doi: 10.1215/ijm/1255988995, Zbl 0654.12005. 1451

[67] WINGBERG, K. Galois groups of local and global type. *J. Reine Angew. Math.* **517** (1999), 223–239. MR1728539, doi: 10.1515/crll.1999.096, Zbl 0935.11042. 1477

(Zakariae Bouazzaoui) ÉCOLE SUPÉRIEURE DE L'EDUCATION ET DE LA FORMATION OUJDA 60000, MOROCCO
z.bouazzaou@ump.ac.ma

(Donghyeok Lim) INSTITUTE OF MATHEMATICAL SCIENCES, EWHA WOMANS UNIVERSITY, SEOUL 03760, REPUBLIC OF KOREA
donghyeokklim@gmail.com

This paper is available via http://nyjm.albany.edu/j/2025/31-56.html.