Glasgow Mathematical Journal (2024), 1–30
doi:10.1017/S0017089523000460

Glasgow
Mathematical
Journal

RESEARCH ARTICLE

Leopoldt-type theorems for non-abelian extensions of $\mathbb{Q}$

Fabio Ferri

Department of Mathematics, University of Exeter, Exeter, EX4 4QF, UK
Email: fabioferri94@gmail.com

Received: 7 June 2022; **Revised:** 14 September 2023; **Accepted:** 27 November 2023

Keywords: algebraic number theory; Galois module structure; wild ramification; associated orders; normal integral bases

2020 Mathematics Subject Classification: *Primary* - 11R33, 11Y40, 16H20; *Secondary* - 11R04, 11R21, 11R32, 11S20, 13G05, 16G30, 16H10, 16Z05, 20C05

Abstract

We prove new results concerning the additive Galois module structure of wildly ramified non-abelian extensions $K/\mathbb{Q}$ with Galois group isomorphic to A_4, S_4, A_5, and dihedral groups of order $2p^n$ for certain prime powers p^n. In particular, when $K/\mathbb{Q}$ is a Galois extension with Galois group G isomorphic to A_4, S_4 or A_5, we give necessary and sufficient conditions for the ring of integers $\mathcal{O}_K$ to be free over its associated order in the rational group algebra $\mathbb{Q}[G]$.

1. Introduction

Let K/F be a finite Galois extension of number fields or p-adic fields and let $G = \mathrm{Gal}(K/F)$. The classical normal basis theorem says that K is free of rank 1 as a module over the group algebra $F[G]$. A much more difficult problem is that of determining whether the ring of integers $\mathcal{O}_K$ is free of rank 1 over an appropriate $\mathcal{O}_F$-order in $F[G]$. The natural choice of such an order is the so-called associated order

$$\mathfrak{A}_{K/F} := \{\lambda \in F[G] : \lambda\mathcal{O}_K \subseteq \mathcal{O}_K\},$$

since this is the only $\mathcal{O}_F$-order in $F[G]$ over which $\mathcal{O}_K$ can possibly be free.

It is clear that the group ring $\mathcal{O}_F[G]$ is contained in $\mathfrak{A}_{K/F}$. In fact, $\mathfrak{A}_{K/F} = \mathcal{O}_F[G]$ if and only if K/F is at most tamely ramified. It is in this setting that by far the most progress has been made and we say that K/F has a normal integral basis if $\mathcal{O}_K$ is free over $\mathcal{O}_F[G]$. The celebrated Hilbert-Speiser theorem says that if $K/\mathbb{Q}$ is a tamely ramified finite abelian extension, then it has a normal integral basis. Leopoldt removed the assumption on ramification to obtain the following generalisation of this result.

Theorem 1.1. [27] *Let $K/\mathbb{Q}$ be a finite abelian extension. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Leopoldt also specified a generator and the associated order; Lettl [28] gave a simplified and more explicit proof of the same result. We also have the following result of Bergé.

Theorem 1.2. [2] *Let p be a prime and let $K/\mathbb{Q}$ be a dihedral extension of degree $2p$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Now let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong Q_8$, the quaternion group of order 8. Suppose that $K/\mathbb{Q}$ is tamely ramified. Martinet [31] gave three examples of such extensions, one with and two without normal integral bases. Moreover, Fröhlich [14] showed that both possibilities occur infinitely often. By contrast, in the case that $K/\mathbb{Q}$ is wildly ramified, we have the following result of Martinet.

Theorem 1.3. [32] *Let $K/\mathbb{Q}$ be a wildly ramified Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong Q_8$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

In the present article, we prove other Leopoldt-type theorems for non-abelian extensions of $\mathbb{Q}$. An important notion is that of local freeness, which we now review.

For the rest of the introduction, let $K/\mathbb{Q}$ be a finite Galois extension and let $G = \mathrm{Gal}(K/\mathbb{Q})$. We recall that $\mathcal{O}_K$ is said to be locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at a rational prime p if $\mathcal{O}_{K,p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K$ is free as an $\mathfrak{A}_{K/\mathbb{Q},p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathfrak{A}_{K/\mathbb{Q}}$-module. We say that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ if this holds for all rational primes p. Of course, this condition is necessary for $\mathcal{O}_K$ to be free over $\mathfrak{A}_{K/\mathbb{Q}}$.

If $K/\mathbb{Q}$ is tamely ramified, then $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}} = \mathbb{Z}[G]$ (see Theorem 3.14). By contrast, if $K/\mathbb{Q}$ is wildly ramified then $\mathbb{Z}[G]$ is strictly contained in $\mathfrak{A}_{K/\mathbb{Q}}$ and $\mathcal{O}_K$ is not necessarily locally free over $\mathfrak{A}_{K/\mathbb{Q}}$. For instance, Bergé [4] gave examples of wildly ramified dihedral extensions of $\mathbb{Q}$ without the local freeness property (see Theorem 3.18 for a complete classification).

Now let N/M be a finite Galois extension of p-adic fields. One can consider the analogous problem of whether $\mathcal{O}_N$ is free over $\mathfrak{A}_{N/M}$. Indeed, this is the case when N/M is unramified, tamely ramified or weakly ramified, or $M = \mathbb{Q}_p$ and $N/\mathbb{Q}_p$ is abelian or dihedral of order 2ℓ for some prime ℓ (see Section 3.1 for a detailed overview of such results). However, freeness in this situation does not relate to the aforementioned notion of local freeness in the way one might expect.

Definition 1.4. *A rational prime p is said to be a decomposition obstruction for K if $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$ for one (indeed, every) prime $\mathfrak{P}$ of K above p, but $\mathcal{O}_{K,p}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},p}$ (here $K_{\mathfrak{P}}$ denotes the completion of K at $\mathfrak{P}$).*

Note that decomposition obstructions do exist. This is an important obstacle that can arise when the decomposition group is a proper non-trivial subgroup of the Galois group, and it needs to be overcome in the proofs of the main results of the present article. In Sections 6 and 7, we will present a detailed algebraic interpretation of such a property: we will start from the results of Bergé [4] on the induction of associated orders and then prove new results that will be crucial for our purpose.

We now return to the problem of whether $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$. If $K/\mathbb{Q}$ is (at most) tamely ramified, then the problem of determining whether it has a normal integral basis is well understood, thanks to Taylor's proof of Fröhlich's conjecture [39]: he determined the class of $\mathcal{O}_K$ in the so-called locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ (see Definition 2.4) in terms of Artin root numbers of the irreducible symplectic characters of G (see [15, I] for an overview). In particular, if G has no irreducible symplectic characters (this is the case, for instance, if G is abelian, dihedral or of odd order), then $K/\mathbb{Q}$ has a normal integral basis.

In the present article, we consider the question of whether $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ in certain cases where the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial. In this situation, it is also the case that $\mathrm{Cl}(\mathfrak{A}_{K/\mathbb{Q}})$ is trivial and the question reduces to whether $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$. A result of Endô and Hironaka [12] shows that if G is non-abelian and non-dihedral then $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial if and only if G is isomorphic to A_4, S_4 or A_5.

In the case that G is dihedral of order $2p^n$ for a prime number p and a positive integer n, Keating [26] gave sufficient conditions for $\mathrm{Cl}(\mathbb{Z}[G])$ to be trivial and Bergé [4] gave necessary and sufficient conditions for $\mathcal{O}_K$ to be locally free over $\mathfrak{A}_{K/\mathbb{Q}}$. Despite being a straightforward application of these existing results, the following result does not appear to have been known until now.

Theorem 1.5. *Let n be a positive integer and let $p \geq 5$ be a regular prime number such that the class number of $\mathbb{Q}(\zeta_{p^n})^+$ is 1. Let $K/\mathbb{Q}$ be a dihedral extension of degree $2p^n$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if the ramification index of p in $K/\mathbb{Q}$ either is coprime to p or is a power of p.*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Here $\mathbb{Q}(\zeta_{p^n})^+$ denotes the maximal totally real subfield $\mathbb{Q}(\zeta_{p^n})$. Using the class number computations of Miller [33], we obtain the following corollary.

Corollary 1.6. *Let $K/\mathbb{Q}$ be a dihedral extension of degree $2p^n$ where (p, n) is $(5, 2)$, $(5, 3)$, $(7, 2)$ or $(11, 2)$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if the ramification index of p in $K/\mathbb{Q}$ either is coprime to p or is a power of p.*

Similar but more complicated results hold when $p = 2$ or 3 (see Theorem 5.2 for the full statement and proof).

The main results of the present article will be necessary and sufficient conditions for $\mathcal{O}_K$ to be free over $\mathfrak{A}_{K/\mathbb{Q}}$ when G is isomorphic to A_4, S_4 or A_5. The discussion above shows that the main work is in determining when $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$. A key ingredient is the notion of hybrid p-adic group rings, introduced by Johnston and Nickel [21]; using this tool, it is straightforward to show that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at $p = 3$ when G is isomorphic to A_4 or S_4.

The statements of the following theorems will depend on certain primes of K having given decomposition or inertia subgroups up to conjugation. We remark that such properties will not depend on which prime of K we choose above a given rational prime. For example, saying that a prime p is tamely ramified will mean that some, and hence every, prime of K above p is (at most) tamely ramified in $K/\mathbb{Q}$. We shall henceforth abbreviate ‘at most tamely ramified’ to ‘tamely ramified’. We will say that a rational prime p has full decomposition group if there is only one prime in K above p, with decomposition group equal to $\mathrm{Gal}(K/\mathbb{Q})$.

The following result is Theorem 8.1.

Theorem 1.7. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if 2 is tamely ramified or has full decomposition group.*

The proof of the ‘if’ direction of this result involves the aforementioned tools. To prove the converse, we show that if 2 is wildly ramified and has decomposition group of order 2 or 4 then $\mathcal{O}_K$ is not locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at $p = 2$. This reduces to showing that the lattice $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} := \mathbb{Z}_2[G] \otimes_{\mathbb{Z}_2[D]} \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$, where $\mathfrak{P}$ is a fixed prime above 2 and D is its decomposition group. The main theorem used here is Hattori’s result [17] that commutative orders are ‘clean’ (see Section 6.2).

The following two results are Theorem 8.3 and Theorem 8.6, respectively.

Theorem 1.8. *Let $K/\mathbb{Q}$ be a Galois extension with $G := \mathrm{Gal}(K/\mathbb{Q}) \cong S_4$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if one of the following conditions on $K/\mathbb{Q}$ holds:*

(i) *2 is tamely ramified;*
(ii) *2 has decomposition group equal to the unique subgroup of G of order 12;*
(iii) *2 is wildly and weakly ramified and has full decomposition group; or*
(iv) *2 is wildly and weakly ramified, has decomposition group of order 8 in G, and has inertia subgroup equal to the unique normal subgroup of order 4 in G.*

Theorem 1.9. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if all three of the following conditions on $K/\mathbb{Q}$ hold:*

(i) *2 is tamely ramified;*
(ii) *3 is tamely ramified or is weakly ramified with ramification index 6; and*
(iii) *5 is tamely ramified or is weakly ramified with ramification index 10.*

In contrast to the proof of Theorem 1.7, the proofs of Theorems 1.8 and 1.9 use the (updated) implementations in Magma [1] of the algorithms developed by Bley and Johnston [5] and by Hofmann and Johnston [18].

Notation and conventions. *All rings are assumed to have an identity element, and all modules are assumed to be left modules unless otherwise stated. We denote certain finite groups as follows:*

- *D_{2n} is the dihedral group of order $2n$;*
- *Q_8 is the quaternion group of order 8;*
- *A_n is the alternating group on n letters;*
- *S_n is the symmetric group on n letters.*

Let K be a number field. By a prime of K, we mean a non-zero prime ideal of $\mathcal{O}_K$. If $\mathfrak{P}$ be a prime of K, we let $K_{\mathfrak{P}}$ denote the completion of K at $\mathfrak{P}$. We say that a prime is tamely ramified if it is at most tamely ramified.

Let H be a subgroup of a finite group G. We denote by $\mathrm{ncl}_G(H)$ the normal closure of H in G, defined as the smallest normal subgroup of G containing H or, equivalently, the subgroup generated by all the conjugates of H in G.

For a positive integer n, we let ζ_n denote a primitive nth root of unity.

2. Associated orders and local freeness

2.1. Lattices and orders

For further background, we refer the reader to [35] or [9]. Let R be a Dedekind domain with field of fractions F. An R-lattice M is a finitely generated torsion-free R-module, or equivalently, a finitely generated projective R-module. Note that any R-submodule of an R-lattice is again an R-lattice. For any finite-dimensional F-vector space V, an R-lattice in V is a finitely generated R-submodule M in V. We define a F-vector subspace of V by

$$FM := \{\alpha_1 m_1 + \alpha_2 m_2 + \cdots + \alpha_r m_r \mid r \in \mathbb{Z}_{\geq 0}, \alpha_i \in F, m_i \in M\}$$

and say that M is a full R-lattice in V if $FM = V$. We may identify FM with $F \otimes_R M$.

Let A be a finite-dimensional F-algebra. An R-order in A is a subring Λ of A (so in particular has the same unity element as A) such that Λ is a full R-lattice in A. A Λ-lattice is a Λ-module which is also an R-lattice. For Λ-lattices M and N, a homomorphism of Λ-modules $f : M \to N$ is called a homomorphism of Λ-lattices.

The following well-known lemma follows from [9, Exercise 23.2].

Lemma 2.1. *Let $\Lambda \subseteq \Gamma$ be two R-orders in A. Let M and N be Γ-lattices and let $f : M \to N$ be a homomorphism of Λ-lattices. Then, f is a homomorphism of Γ-lattices.*

2.2. Associated orders

Let Λ be an R-order in a finite-dimensional F-algebra A. Let M be a full R-lattice in a free A-module of rank 1 (thus $FM \cong A$ as A-modules). The *associated order* of M is defined to be

$$\mathfrak{A}(A, M) = \{\lambda \in A : \lambda M \subseteq M\}.$$

Note that $\mathfrak{A}(A, M)$ is an R-order (see [35, §8]). In particular, it is the largest order Λ over which M has a structure of Λ-module. The following well-known result says that $\mathfrak{A}(A, M)$ is the only R-order in A over which M can possibly be free.

Proposition 2.2. *Let Λ be an R-order in A and let M be a free Λ-lattice of rank 1. Then, FM is a free A-module of rank 1 and $\Lambda = \mathfrak{A}(A, M)$.*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Proof. By hypothesis there exists $\alpha \in M$ such that $M = \Lambda\alpha$ is a free Λ-module. Thus, $FM = A\alpha$ is free over A. Let $x \in \mathfrak{A}(A, M)$. Then, $x\alpha \in M = \Lambda\alpha$, so $x\alpha = y\alpha$ for some $y \in \Lambda$. Since FM is freely generated by α, we must have $x = y$. Hence, $\mathfrak{A}(A, M) \subseteq \Lambda$. The reverse inclusion is trivial and therefore $\Lambda = \mathfrak{A}(A, M)$. □

Remark 2.3. *Suppose Λ is an R-order in A. Then, clearly $\Lambda \subseteq \mathfrak{A}(A, \Lambda)$. Moreover, $\mathfrak{A}(A, \Lambda)1_A \subseteq \Lambda$ and so $\mathfrak{A}(A, \Lambda) \subseteq \Lambda$. Therefore, $\mathfrak{A}(A, \Lambda) = \Lambda$.*

2.3. Completion and local freeness

Let $\mathfrak{p}$ be any maximal ideal of R. Let $F_\mathfrak{p}$ denote the completion of F with respect to a valuation defined by $\mathfrak{p}$ and let $R_\mathfrak{p}$ be the corresponding valuation ring. For any R-module M we write $M_\mathfrak{p}$ for $R_\mathfrak{p} \otimes_R M$ and $V_\mathfrak{p} = F_\mathfrak{p} \otimes_F V$ for any F-vector space V. These two notations are consistent as the map $\lambda \otimes_{\mathcal{O}_F} v \mapsto \lambda \otimes_F v$ ($v \in V$, $\lambda \in \mathcal{O}_{F_\mathfrak{p}}$) is an isomorphism (see [16, p. 93]).

Let Λ be an R-order and let M be a Λ-lattice in some A-module V. Then, $\Lambda_\mathfrak{p}$ is an $R_\mathfrak{p}$-order in $A_\mathfrak{p}$ and $M_\mathfrak{p}$ is a $\Lambda_\mathfrak{p}$-lattice in $V_\mathfrak{p}$. We say that M is locally free over Λ if $M_\mathfrak{p}$ is free over $\Lambda_\mathfrak{p}$ for every $\mathfrak{p}$.

Let G be a finite group and let M be a full $R[G]$-lattice in a free A-module of rank 1. Then, $R[G] \subseteq \mathfrak{A}(F[G], M)$ and $R_\mathfrak{p}[G] \subseteq \mathfrak{A}(F_\mathfrak{p}[G], M_\mathfrak{p}) \cong \mathfrak{A}(F[G], M)_\mathfrak{p}$. Moreover, M is locally free over $\mathfrak{A}(F[G], M)$ if $M_\mathfrak{p}$ is free over $\mathfrak{A}(F_\mathfrak{p}[G], M_\mathfrak{p})$ for every $\mathfrak{p}$.

2.4. Associated orders of rings of integers and decomposition obstructions

Let K/F be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/F)$. We consider the behaviour of the associated order $\mathfrak{A}_{K/F} := \mathfrak{A}(F[G], \mathcal{O}_K)$ with respect to localisation and induction.

Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_F$. Then, we have decompositions

$$K_\mathfrak{p} := F_\mathfrak{p} \otimes_F K \cong \prod_{\mathfrak{P}' \mid \mathfrak{p}} K_{\mathfrak{P}'} \quad \text{and} \quad \mathcal{O}_{K,\mathfrak{p}} := \mathcal{O}_{F_\mathfrak{p}} \otimes_{\mathcal{O}_F} \mathcal{O}_K \cong \prod_{\mathfrak{P}' \mid \mathfrak{p}} \mathcal{O}_{K_{\mathfrak{P}'}},$$

where $\{\mathfrak{P}' \mid \mathfrak{p}\}$ consists of the primes of $\mathcal{O}_K$ above $\mathfrak{p}$ (see [16, p. 109]). Fix a prime $\mathfrak{P}$ above $\mathfrak{p}$ and let D be its decomposition group in G. Then, as G acts transitively on $\{\mathfrak{P}' \mid \mathfrak{p}\}$ we have

$$K_\mathfrak{p} \cong \prod_{s \in G/D} sK_\mathfrak{P} \quad \text{and} \quad \mathcal{O}_{K,\mathfrak{p}} \cong \prod_{s \in G/D} s\mathcal{O}_{K_\mathfrak{P}},$$

where the products run over a system of representatives of the left cosets G/D. Hence,

$$\mathcal{O}_{K,\mathfrak{p}} \cong \mathrm{Ind}_D^G \mathcal{O}_{K_\mathfrak{P}} := \mathcal{O}_{F_\mathfrak{p}}[G] \otimes_{\mathcal{O}_{F_\mathfrak{p}}[D]} \mathcal{O}_{K_\mathfrak{P}},$$

and

$$\mathfrak{A}_{K/F,\mathfrak{p}} = \mathfrak{A}(F[G], \mathcal{O}_K)_\mathfrak{p} \cong \mathfrak{A}(F_\mathfrak{p}[G], \mathrm{Ind}_D^G \mathcal{O}_{K_\mathfrak{P}}),$$

where the last isomorphism follows from [9, Exercise 24.2], for instance. Thus, $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/F}$ at $\mathfrak{p}$ if and only if $\mathrm{Ind}_D^G \mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}(F_\mathfrak{p}[G], \mathrm{Ind}_D^G \mathcal{O}_{K_\mathfrak{P}})$.

We recall from the introduction that it may be the case that we encounter a prime $\mathfrak{p}$ that is a decomposition obstruction for K, i.e. such that $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/F_\mathfrak{p}}$ but $\mathcal{O}_K$ is not locally free over $\mathfrak{A}_{K/F}$ at $\mathfrak{p}$ (indeed, Definition 1.4 can be easily generalised to base fields other than $\mathbb{Q}$). In Section 6, we will consider the relationship between $\mathfrak{A}(F_\mathfrak{p}[G], \mathrm{Ind}_D^G \mathcal{O}_{K_\mathfrak{P}})$ and $\mathrm{Ind}_D^G \mathfrak{A}_{K_\mathfrak{P}/F_\mathfrak{p}}$, as well as conditions under which the implication ‘if $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/F_\mathfrak{p}}$ then $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/F}$ at $\mathfrak{p}$’ holds.

Notation. *We henceforth consider the isomorphism $\mathfrak{A}_{K/F,\mathfrak{p}} \cong \mathfrak{A}(F_\mathfrak{p}[G], \mathcal{O}_{K,\mathfrak{p}})$ as an identification. In particular, we consider $\mathfrak{A}_{K/F,\mathfrak{p}}$ as an $\mathcal{O}_{F,\mathfrak{p}}$-order in $F_\mathfrak{p}[G]$.*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

2.5. Reduction to the study of local freeness

We define locally free class groups. Background material on locally free class groups, including a discussion of equivalent definitions, can be found in [10, §49].

Definition 2.4. *Let F be a number field with ring of integers $\mathcal{O}_F$ and let Λ be an $\mathcal{O}_F$-order in a finite-dimensional semisimple F-algebra A. Let $P(\Lambda)$ be the free abelian group generated by symbols $[X]$, one for each isomorphism class of locally free Λ-lattices X, modulo relations $[X] = [X_1] + [X_2]$ whenever $X \cong X_1 \oplus X_2$. We define the locally free class group $\mathrm{Cl}(\Lambda)$ of Λ to be the subgroup of $P(\Lambda)$ consisting of all expressions $[X] - [Y]$, with X, Y locally free and $FX \cong FY$. If X is a Λ-lattice such that $FX \cong A$, we will refer to $[X] - [\Lambda]$ as the class of X in $\mathrm{Cl}(\Lambda)$.*

Remark 2.5. *By [9, Corollary (31.7)], each element of $\mathrm{Cl}(\Lambda)$ can be written in the form $[M] - [\Lambda]$ for some locally free Λ-lattice M of rank 1. As a consequence, the Jordan-Zassenhaus Theorem [9, Theorem (24.1)] implies that the locally free class group $\mathrm{Cl}(\Lambda)$ is always finite.*

The following proposition underpins the proofs of all the new theorems stated in the introduction.

Proposition 2.6. *Let G be a finite group such that $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial and let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Proof. One implication is trivial. By [10, Theorem (49.25)], the inclusion $\mathbb{Z}[G] \subseteq \mathfrak{A}_{K/\mathbb{Q}}$ induces a surjection $\mathrm{Cl}(\mathbb{Z}[G]) \twoheadrightarrow \mathrm{Cl}(\mathfrak{A}_{K/\mathbb{Q}})$, and so $\mathrm{Cl}(\mathfrak{A}_{K/\mathbb{Q}})$ is also trivial. Moreover, by [12] the triviality of $\mathrm{Cl}(\mathbb{Z}[G])$ implies that G must be abelian, dihedral, or isomorphic to A_4, S_4 or A_5 (see also [10, Theorem (50.29)]). In each of these cases, $\mathbb{Q}[G]$ is isomorphic to a finite direct product of matrix rings over number fields. Hence by [10, Proposition (51.2)] $\mathbb{Q}[G]$ satisfies the Eichler condition (see [10, Definitions (45.4) or §51A]). Thus the Jacobinski cancellation theorem [19] (see also [10, Theorem (51.24)]) implies that $\mathfrak{A}_{K/\mathbb{Q}}$ has the locally free cancellation property. The non-trivial implication now follows easily. □

Corollary 2.7. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$, S_4 or A_5. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Proof. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. In each case $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial, as shown in [37]. □

3. Review of results relating to local freeness in field extensions

3.1. Freeness results for Galois extensions of p-adic fields

Many of the results and definitions of this subsection also hold for local fields of positive characteristic, but for simplicity we restrict to the case of p-adic fields. We fix a prime number p.

Theorem 3.1. *Let K/F be a tamely ramified finite Galois extension of p-adic fields and let $G = \mathrm{Gal}(K/F)$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/F} = \mathcal{O}_F[G]$.*

Remark 3.2. *Theorem 3.1 is usually attributed to Emmy Noether [34]. In fact, as noted in [8], she only stated and proved the result in the case that $p \nmid |G|$. Complete proofs can be found in [15], [25] and [8].*

Theorem 3.3. [29] *Let K/F be an extension of p-adic fields such that $K/\mathbb{Q}_p$ is a finite abelian extension. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/F}$.*

Theorem 3.4. [2] *Let $K/\mathbb{Q}_p$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong D_{2\ell}$, where ℓ is a prime number. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}_p}$.*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Theorem 3.5. [32] *Let $K/\mathbb{Q}_p$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong Q_8$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}_p}$.*

Remark 3.6. *Theorem 3.5 is not explicitly stated in [32]. However, the proof of Theorem 1.3 given in loc. cit. also works essentially unchanged in the setting of Theorem 3.5.*

Theorem 3.7. [20] *Let p, n and r be positive integers such that p is an odd prime, n divides $p-1$ and r is a primitive nth root modulo p. Let G be the metacyclic group with the following structure:*

$$G = \langle x, y : x^p = 1, y^n = 1, yxy^{-1} = x^r \rangle \cong C_p \rtimes C_n. \tag{3.1}$$

Let $K/\mathbb{Q}_p$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong G$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}_p}$.

Remark 3.8. *In the special case $n = 2$, the group G of (3.1) is dihedral of order $2p$.*

Let K/F be a Galois extension of p-adic fields and let $G = \mathrm{Gal}(K/F)$. We recall that for an integer $t \geq -1$ the tth ramification group is defined to be

$$G_t := \{\sigma \in G : v_K(\sigma(x) - x) \geq t + 1 \ \forall x \in \mathcal{O}_K\},$$

where v_K is the normalised valuation on K (i.e. with image $\mathbb{Z}$). When it is not obvious which extension we are referring to we will use the notation '$G_t(K/F)$' or similar. Thus, K/F is unramified if and only if G_0 is trivial and is tamely ramified if and only if G_1 is trivial. We say that the extension is weakly ramified if G_2 is trivial.

Theorem 3.9. [23] *Let K/F be a weakly ramified finite Galois extension of p-adic fields and let $G = \mathrm{Gal}(K/F)$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/F}$. Moreover, if K/F is both wildly and weakly ramified then $\mathfrak{A}_{K/F} = \mathcal{O}_F[G][\pi_F^{-1}\mathrm{Tr}_{G_0}]$ (i.e. the $\mathcal{O}_F[G]$-algebra generated by $\pi_F^{-1}\mathrm{Tr}_{G_0}$, which is an $\mathcal{O}_F$-order), where π_F is a uniformiser of $\mathcal{O}_F$ and $\mathrm{Tr}_{G_0} = \sum_{\gamma \in G_0} \gamma$ is the sum of the elements of the inertia group G_0.*

For a subgroup H of G define $\mathrm{Tr}_H = \sum_{h \in H} h \in F[G]$ and $e_H = \frac{1}{|H|}\mathrm{Tr}_H \in F[G]$. Note that e_H is an idempotent. We say that K/F is almost-maximally ramified if $e_H \in \mathfrak{A}_{K/F}$ for every subgroup H of G such that $G_{t+1} \subseteq H \subseteq G_t$ for some $t \geq 1$.

Theorem 3.10 ([4, Proposition 7]). *Let K/F be a finite dihedral extension of p-adic fields such that $F/\mathbb{Q}_p$ is unramified. Let $G = \mathrm{Gal}(K/F)$. Then, $\mathcal{O}_K$ is projective over $\mathfrak{A}_{K/F}$ if and only if $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/F}$ if and only if either*

(i) K/F is almost-maximally ramified, in which case $\mathfrak{A}_{K/F} = \mathcal{O}_F[G][\{e_{G_t}\}_{t \geq 1}]$, or

(ii) K/F is not almost-maximally ramified, and the inertia subgroup G_0 is dihedral of order $2p$, in which case $\mathfrak{A}_{K/F} = \mathcal{O}_F[G][2e_{G_0}]$.

Remark 3.11. *Throughout the article, and in particular in Theorem 3.10, the group $C_2 \times C_2$ is considered to be dihedral of order $2 \cdot 2$.*

Remark 3.12. *Let H be a subgroup of G and let r be a positive integer. We now show how to determine whether $\frac{1}{r}\mathrm{Tr}_H \in \mathfrak{A}_{K/F}$. For example, when $r = |H|$ this can be used to check for almost-maximal ramification. Let M be the subfield of K fixed by H. We denote by $\mathfrak{D}_{K/M}$ the different of the extension K/M (see [38, III§3]) and by $v_p(x)$ the p-adic valuation of an integer x (thus, v_p is the restriction of $v_{\mathbb{Q}_p}$ to $\mathbb{Z}$).*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

$$\begin{aligned}
\frac{1}{r}\mathrm{Tr}_H \in \mathfrak{A}_{K/F} &\iff \frac{1}{r}\mathrm{Tr}_{K/M}(\mathcal{O}_K) \subseteq \mathcal{O}_M \\
&\iff \mathrm{Tr}_{K/M}(\mathcal{O}_K) \subseteq r\mathcal{O}_M \\
&\iff \mathcal{O}_K \subseteq r\mathcal{O}_M\mathfrak{D}_{K/M}^{-1} \text{ by [Ser79, III Proposition 7]} \\
&\iff \mathfrak{D}_{K/M} \subseteq r\mathcal{O}_K \\
&\iff v_K(\mathfrak{D}_{K/M}) \geq e(K/\mathbb{Q}_p)v_p(r) \\
&\iff \sum_{i=0}^{\infty}(|G_i(K/M)| - 1) \geq e(K/\mathbb{Q}_p)v_p(r) \text{ by [Ser79, IV Proposition 4].}
\end{aligned}$$

Remark 3.13. *From Theorem 3.4, Theorem 3.10, and Remark 3.12 (also see [3, Corollaire to Proposition 3]), we deduce that a dihedral extension $K/\mathbb{Q}_p$ of degree $2p$ either is almost-maximally ramified or is weakly and totally ramified.*

3.2. Local freeness results for Galois extensions of number fields

Let K/F be a finite Galois extension of number fields. If $\mathcal{O}_K$ is free over $\mathfrak{A}_{F/K}$, then it is clear that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{F/K}$. In particular, the analogues of Theorems 1.1, 1.2 and 1.3 all hold, with 'locally free' in place of 'free'. Theorems 3.15 and 3.17 below are generalisations of the first two of these analogues.

Theorem 3.14. *Let K/F be a finite Galois extension of number fields. Let $G = \mathrm{Gal}(K/F)$ and let $\mathfrak{p}$ be a prime of F that is tamely ramified in K/F. Then, $\mathcal{O}_{K,\mathfrak{p}}$ is free over $\mathfrak{A}_{K/F,\mathfrak{p}} = \mathcal{O}_{F_\mathfrak{p}}[G]$.*

Theorem 3.15. [29] *Let K/F be an extension of number fields such that $K/\mathbb{Q}$ is a finite abelian extension. Then, $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/F}$.*

Remark 3.16. *Theorems 3.14 and 3.15 are well-known consequences of Theorems 3.1 and 3.3, respectively. For a proof see Remark 6.3 and Corollary 6.6, for instance.*

Theorem 3.17. [20] *Let $K/\mathbb{Q}$ be a Galois extension such that $\mathrm{Gal}(K/\mathbb{Q})$ is metacyclic of type (3.1). Then, $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Theorem 3.18 ([4, Théorème]). *Let $K/\mathbb{Q}$ be a finite dihedral extension and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let p be an odd prime number that is wildly ramified in $K/\mathbb{Q}$ and let N be the unique cyclic subgroup of G of index 2. Then, $\mathcal{O}_{K,p}$ is projective over $\mathfrak{A}_{K/\mathbb{Q},p}$ if and only if $\mathcal{O}_{K,p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$ if and only if one of the following conditions holds:*

(i) p is almost-maximally ramified in $K/\mathbb{Q}$, in which case

$$\mathfrak{A}_{K/\mathbb{Q},p} = \mathbb{Z}_p[G][\{e_{G_t}\}_{t\geq 1}], \text{ or}$$

(ii) p is not almost-maximally ramified, $|G_0| = 2p$ and $[G : G_0] \mid 2$, in which case

$$\mathfrak{A}_{K/\mathbb{Q},p} = \mathbb{Z}_p[G][e_{G_0}].$$

Remark 3.19. *In fact, Theorem 3.18 is [4, Théorème] specialised to the case that p is odd and the base field is $\mathbb{Q}$; the more general statement is somewhat more complicated.*

4. Hybrid group rings and applications to local freeness

4.1. Hybrid group rings

Let R be a discrete valuation ring with fraction field F and let G be a finite group. Let M be a full $R[G]$-lattice in $F[G]$. Note that $R[G] \subseteq \mathfrak{A}(F[G], M)$.

For a normal subgroup N of G define $e_N = \frac{1}{|N|} \sum_{n \in N} n \in F[G]$ to be the central idempotent associated with N.

Proposition 4.1. *If N is a normal subgroup of G such that $|N| \in R^\times$, then*

(i) $R[G] = e_N R[G] \times (1 - e_N)R[G] \cong R[G/N] \times (1 - e_N)R[G]$,
(ii) $e_N M$ *has the structure of a* $e_N R[G] \cong R[G/N]$*-lattice, and*
(iii) $e_N \mathfrak{A}(F[G], M) = \mathfrak{A}(F[G], M) \cap e_N F[G] = \mathfrak{A}(e_N F[G], e_N M) \cong \mathfrak{A}(F[G/N], e_N M)$.

Proof. Since $|N| \in R^\times$ we have $e_N \in R[G]$. Moreover, it is straightforward to show that $e_N R[G] \cong R[G/N]$. Thus, we have established (i) and (ii), and it remains to prove (iii).

The last isomorphism of (iii) is immediate from (ii). We now prove the first equality, that is, $e_N \mathfrak{A}(F[G], M) = \mathfrak{A}(F[G], M) \cap e_N F[G]$. Since $e_N \in R[G] \subseteq \mathfrak{A}(F[G], M)$, we easily have that $e_N \mathfrak{A}(F[G], M) \subseteq \mathfrak{A}(F[G], M) \cap e_N F[G]$. The other containment follows from the fact that $e_N^2 = e_N$; hence, any element in $\mathfrak{A}(F[G], M) \cap e_N F[G]$, with the harmless multiplication by e_N, can be written as an element in $e_N \mathfrak{A}(F[G], M)$.

We now prove that $\mathfrak{A}(F[G], M) \cap e_N F[G] = \mathfrak{A}(e_N F[G], e_N M)$. Consider $e_N x \in \mathfrak{A}(F[G], M) \cap e_N F[G]$ for a certain $x \in F[G]$; we have to prove that $e_N x$ preserves $e_N M$. Since $e_N M \subseteq M$ and $e_N x \in \mathfrak{A}(F[G], M)$, we have that $e_N x e_N M \subseteq M$. Hence, $e_N x e_N M = e_N e_N x e_N M \subseteq e_N M$. Conversely, let us consider an element $e_N x \in \mathfrak{A}(e_N F[G], e_N M)$, thus such that $e_N x e_N M \subseteq e_N M$. We must prove that $e_N x \in \mathfrak{A}(F[G], M)$, which is automatic since $e_N x M = e_N e_N x M = e_N x e_N M \subseteq e_N M \subseteq M$. □

We now recall the notion of hybrid group ring introduced in [21, §2] and further developed in [22, §2].

Definition 4.2. *Let N be a normal subgroup of G. We say that $R[G]$ is N-hybrid if $|N| \in R^\times$ and $(1 - e_N)R[G]$ is a maximal R-order in $(1 - e_N)F[G]$.*

Remark 4.3. *The group ring $R[G]$ is a maximal R-order if and only if $|G| \in R^\times$ if and only if $R[G]$ is G-hybrid, where the first equivalence is given by [9, Proposition (27.1)]. In this situation, $\mathfrak{A}(F[G], M) = R[G]$, and thus, M is free over $\mathfrak{A}(F[G], M)$ by [35, Theorem (18.10)].*

Example 4.4. *Let $G = A_4$ or S_4 and let N be its unique normal subgroup of order 4. Then, $\mathbb{Z}_3[G]$ is N-hybrid as shown in [21, Examples 2.16 and 2.18]. Indeed, we have*

$$\mathbb{Z}_3[A_4] \cong \mathbb{Z}_3[C_3] \times M_{3\times3}(\mathbb{Z}_3) \quad \text{and} \quad \mathbb{Z}_3[S_4] \cong \mathbb{Z}_3[S_3] \times M_{3\times3}(\mathbb{Z}_3) \times M_{3\times3}(\mathbb{Z}_3),$$

where $M_{3\times3}(\mathbb{Z}_p)$ is a maximal $\mathbb{Z}_p$-order by [35, Theorem (8.7)].

Example 4.5. *Let n be an odd positive integer and let N_n be the unique subgroup of index 2 in D_{2n}. Then, $\mathbb{Z}_2[D_{2n}]$ is N_n-hybrid as shown in [21, Example 2.14].*

Proposition 4.6. *Suppose $R[G]$ is N-hybrid. Then,*

$$\mathfrak{A}(F[G], M) = e_N \mathfrak{A}(F[G], M) \times (1 - e_N)R[G] \cong \mathfrak{A}(F[G/N], e_N M) \times (1 - e_N)R[G].$$

Moreover, M is free over $\mathfrak{A}(F[G], M)$ if and only if $e_N M$ is free over $\mathfrak{A}(F[G/N], e_N M)$.

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Proof. The first claim follows from Proposition 4.1, Definition 4.2, and the fact that $R[G] \subseteq \mathfrak{A}(F[G], M)$. Since $(1-e_N)R[G]$ is a maximal R-order, $(1-e_N)M$ is free over $(1-e_N)R[G]$ by [35, Theorem (18.10)]. The second claim now follows from the decomposition $M \cong e_N M \oplus (1-e_N)M$. □

4.2. Applications to local freeness for extensions of number fields

Proposition 4.7. *Let K/F be a finite Galois extension of number fields and let $G = \mathrm{Gal}(K/F)$. Let p be a rational prime and let $\mathfrak{p}$ be a prime of F above p. Let N be a normal subgroup of G such that $p \nmid |N|$ and let M be the subfield of K fixed by N. Then, we have an identification $e_N\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{M,\mathfrak{p}}$. Moreover, via this identification, the structure of $e_N\mathcal{O}_{K,\mathfrak{p}}$ as an $e_N\mathcal{O}_{F_\mathfrak{p}}[G]$-module coincides with the structure of $\mathcal{O}_{M,\mathfrak{p}}$ as an $\mathcal{O}_{F_\mathfrak{p}}[G/N]$-module under the canonical identification $G/N \cong \mathrm{Gal}(M/F)$. In particular,*

$$e_N\mathfrak{A}(F_\mathfrak{p}[G], \mathcal{O}_{K,\mathfrak{p}}) = \mathfrak{A}(F_\mathfrak{p}[G], \mathcal{O}_{K,\mathfrak{p}}) \cap e_N F[G] \cong \mathfrak{A}(F_\mathfrak{p}[G/N], \mathcal{O}_{M,\mathfrak{p}}).$$

Now further suppose that $\mathcal{O}_{F_\mathfrak{p}}[G]$ is N-hybrid. Then,

$$\mathfrak{A}_{K/F,\mathfrak{p}} \cong \mathfrak{A}_{M/F,\mathfrak{p}} \times (1-e_N)\mathcal{O}_{F_\mathfrak{p}}[G],$$

and $\mathcal{O}_{K,\mathfrak{p}}$ is free over $\mathfrak{A}_{K/F,\mathfrak{p}}$ if and only if $\mathcal{O}_{M,\mathfrak{p}}$ is free over $\mathfrak{A}_{M/F,\mathfrak{p}}$.

Proof. The claims regarding the identifications are clear. The remaining claims are then specialisations of Propositions 4.1 and 4.6. □

Corollary 4.8. *Let $K/\mathbb{Q}$ be a finite Galois extension and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Let N be a normal subgroup of G and such that G/N is abelian or metacyclic of type (3.1). Let p be a rational prime. If $\mathbb{Z}_p[G]$ is N-hybrid, then $\mathcal{O}_{K,p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$.*

Proof. Let M be the subfield of K fixed by N. Then, $\mathcal{O}_{M,p}$ is free over $\mathfrak{A}_{M/\mathbb{Q},p}$ by Theorem 1.1 or Theorem 3.17. The result now follows from Proposition 4.7. □

Remark 4.9. *Jaulent [20] developed similar arguments to Corollary 4.8, but restricted to the case that G is metacyclic of type (3.1).*

4.3. Preliminary results on A_4 and S_4-extensions of $\mathbb{Q}$

Proposition 4.10. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$ or S_4. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$.*

Proof. By Corollary 2.7, it suffices to show that $\mathcal{O}_{K,p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$ for each rational prime $p \geq 3$. For $p \geq 5$, this follows from Theorem 3.14. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and let N be its unique normal subgroup of order 4. By Example 4.4, the group ring $\mathbb{Z}_3[G]$ is N-hybrid. Moreover, $G/N \cong C_3$ or S_3 (note that $S_3 \cong D_6$ is metacyclic of type (3.1)). Thus by Corollary 4.8, we have that $\mathcal{O}_{K,3}$ is free over $\mathfrak{A}_{K/\mathbb{Q},3}$. □

Lemma 4.11. *There is a unique Galois extension $L/\mathbb{Q}_2$ with $\mathrm{Gal}(L/\mathbb{Q}_2) \cong A_4$. Moreover, this extension is wildly and weakly ramified, and the inertia subgroup is equal to the unique (normal) subgroup of order 4.*

Proof. This can easily be checked by, for instance, using the database of p-adic fields [24] (which is now accessible via the database [30]). Indeed, L is the Galois closure of the extension of $\mathbb{Q}_2$ generated by the polynomial $x^4 + 2x^3 + 2x^2 + 2$. □

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Proposition 4.12. *Let $K/\mathbb{Q}$ be a Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$*. If* 2 *either is tamely ramified in $K/\mathbb{Q}$ or has full decomposition group in* $\mathrm{Gal}(K/\mathbb{Q})$*, then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Proof. By Proposition 4.10, it suffices to show that $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$. If 2 is tamely ramified in $K/\mathbb{Q}$, then this follows from Theorem 3.14. Now suppose that 2 has full decomposition group in $G := \mathrm{Gal}(K/\mathbb{Q})$. Then, 2 is weakly ramified in $K/\mathbb{Q}$ by Lemma 4.11. Let $\mathfrak{P}$ be the unique prime of K above 2. Then,

$$\mathcal{O}_{K,2} \cong \mathrm{Ind}_G^G \mathcal{O}_{K_\mathfrak{P}} = \mathcal{O}_{K_\mathfrak{P}} \quad \text{and} \quad \mathfrak{A}_{K/\mathbb{Q},2} \cong \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2},$$

so the result now follows from Theorem 3.9. □

5. Leopoldt-type theorems for certain dihedral extensions of $\mathbb{Q}$

We first recall the following theorem of Bergé stated in the introduction.

Theorem 5.1. [2] *Let p be a prime number and let $K/\mathbb{Q}$ be a dihedral extension of degree* $2p$*. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

In the following theorem and corollaries, we consider other dihedral extensions of $\mathbb{Q}$. For a positive integer m, let $\mathbb{Q}(\zeta_m)^+$ denote the maximal totally real subfield of the mth cyclotomic field $\mathbb{Q}(\zeta_m)$. If m is odd, then $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$ and so $\mathbb{Q}(\zeta_{2m})^+ = \mathbb{Q}(\zeta_m)^+$. We recall that we abbreviate 'at most tamely ramified' to 'tamely ramified'.

Theorem 5.2. *Let p be a prime and let $n \geq 2$ be an integer. Let $K/\mathbb{Q}$ be a dihedral extension of degree* $2p^n$*. Suppose that p is a regular prime such that the class number of* $\mathbb{Q}(\zeta_{2p^n})^+$ *is* 1*. Consider the following assertions:*

(i) $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$;
(ii) $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at p;
(iii) p tamely ramified or is almost-maximally ramified in the extension $K/\mathbb{Q}$;
(iv) the ramification index of p in $K/\mathbb{Q}$ either is coprime to p or is a power of p.

Then, we have the following conclusions:

(i) (i) and (ii) are equivalent;
(ii) if p is odd, then (i), (ii) and (iii) are equivalent;
(iii) if p is odd, then (iv) implies (i), (ii) and (iii);
(iv) if $p \geq 5$, then (i), (ii), (iii) and (iv) are equivalent.

Proof. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. By [40, Theorem 10.1] the condition on the class number of $\mathbb{Q}(\zeta_{2p^n})^+$ implies that the class number of $\mathbb{Q}(\zeta_{2p^d})^+$ is 1 for every $d \leq n$. This together with the regularity of p implies that the locally free class group $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial: if p is odd this follows from a special case of the main result of [26, Theorem 1] (also see [10, (50.28)]), if $p = 2$ this follows from the results of [13] (also see [10, Theorem (50.31)] and [9, Example (7.39)]). Therefore, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ by Proposition 2.6. Note that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at ℓ for every rational prime $\ell \neq 2, p$ by Theorem 3.14. Moreover, if p is odd then Example 4.5 implies that $\mathbb{Z}_2[G]$ is N-hybrid where N is the unique subgroup of G of index 2, and so $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at $\ell = 2$ by Corollary 4.8. Thus we have proven claim (a).

Claim (b) now follows from Theorems 3.14 and 3.18 (note that case (ii) of Theorem 3.18 cannot occur when p is odd and $n \geq 2$). Finally, claims (c) and (d) follow from the definition of tame ramification and

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

the characterisation of almost-maximal ramification in dihedral extensions given in [4, Corollaire to Proposition 6]. □

Remark 5.3. *Let p be a prime and let n be a positive integer. It is well known that p is regular if $p < 37$. Moreover, by the results of [33] the class number of $\mathbb{Q}(\zeta_{2p^n})^+$ is 1 whenever (p, n) is $(2, 6)$, $(3, 4)$, $(5, 3)$, $(7, 2)$, $(11, 2)$, or the same pairs with a smaller choice of $n \geq 2$. Hence, the hypotheses of Theorem 5.2 hold for these values. In particular, we obtain the following corollaries.*

Corollary 5.4. *Let $K/\mathbb{Q}$ be a dihedral extension of degree $2 \cdot 3^n$ where $n = 2, 3$ or 4. If the ramification index of 3 in $K/\mathbb{Q}$ either is coprime to 3 or is a power of 3 then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.*

Corollary 5.5. *Let $K/\mathbb{Q}$ be a dihedral extension of degree $2p^n$ where (p, n) is $(5, 2)$, $(5, 3)$, $(7, 2)$ or $(11, 2)$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if the ramification index of p in $K/\mathbb{Q}$ either is coprime to p or is a power of p.*

Remark 5.6. *In the proof of Theorem 5.2, we could have used [4, Théorème] to establish local freeness at $\ell = 2$ instead of Example 4.5 and Corollary 4.8.*

6. Review of results on induction of lattices and associated orders

In this section, we shall give an exposition of Bergé's results contained in [4, §I]. We include some of the proofs for the convenience of the reader. The motivation for this section comes from Section 2.4.

6.1. Associated orders and induction

Let R be a Dedekind domain with field of fractions F. Let H be a subgroup of a finite group G and let M be an $R[H]$-lattice such that FM is free of rank 1 over $F[H]$.

We recall that $\mathrm{Ind}_H^G M$ is the induced module $R[G] \otimes_{R[H]} M \cong \bigoplus_{s \in G/H} sM$, where on the right-hand side we choose a system of representatives in G of the left cosets G/H and the left $R[G]$-module structure is given by the relation $gs = th$ for some coset representative t and $h \in H$. We wish to understand the relationship between $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ and $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$. Note that these both contain the group ring $R[G]$.

Proposition 6.1 ([4, §1.3]). *We have*

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) = \bigcap_{g \in G} g\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) g^{-1}.$$

Corollary 6.2. $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is a ring if and only if it is equal to* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$.

Proof. If $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is a ring, then $g\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) g^{-1} = \mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ for all $g \in G$ and thus $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ by Proposition 6.1. Conversely, if $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$ then the left-hand side is a ring since the right-hand side is an associated order and thus a ring. □

Remark 6.3. *In general,* $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *need not be a ring. However, it is straightforward to deduce from the above that* $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is a ring in the following cases:*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

(i) *there exists a subgroup $K \leq G$ such that $G \cong H \times K$,*
(ii) *H is contained in the centre of G, or*
(iii) *$\mathfrak{A}(F[H], N) = R[H]$.*

Remark 6.4. *Proposition 6.1 implies that $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \subseteq \mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$. Hence $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is an $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-lattice.*

Proposition 6.5. *If M is free over $\mathfrak{A}(F[H], M)$, then $\mathrm{Ind}_H^G M \cong \mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ as $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-lattices.*

Proof. Since $R[H] \subseteq \mathfrak{A}(F[H], M)$ and M is free (necessarily of rank 1) over $\mathfrak{A}(F[H], M)$, we see that M and $\mathfrak{A}(F[H], M)$ are isomorphic as $R[H]$-lattices. Extension of scalars gives an isomorphism $\mathrm{Ind}_H^G M \cong \mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ of $R[G]$-lattices. By Lemma 2.1, this is also an isomorphism of $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-lattices. □

Corollary 6.6. *Suppose that M is free over $\mathfrak{A}(F[H], M)$. If*

(i) *$\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is free over $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$,*
(ii) *$\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$, or*
(iii) *$\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is a ring,*

then $\mathrm{Ind}_H^G M$ is free over $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$.

Proof. In case (i) this follows immediately from Proposition 6.5. Clearly, (ii) ⇒ (i). Moreover, (ii) ⇔ (iii) by Corollary 6.2. □

Remark 6.7. *In the proofs of the main theorems of the present article, Corollary 6.6 will be used to show that certain primes are not decomposition obstructions (see Definition 1.4).*

The following is a partial converse to Corollary 6.6(i).

Proposition 6.8 ([4, Proposition 2]). *If $\mathrm{Ind}_H^G M$ is a projective $\mathfrak{A}(F[G], \mathrm{Ind}_H^G N)$-lattice, then M is a projective $\mathfrak{A}(F[H], M)$-lattice.*

If H is normal in G, then we define $\mathfrak{A}^*(M) = \bigcap_{g \in G} g\mathfrak{A}(F[H], M)g^{-1}$.

Proposition 6.9 ([4, Proposition 3]). *Suppose that H is normal in G. Then,*

(i) *$\mathfrak{A}^*(M)$ is an R-order in $F[H]$,*
(ii) *$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) = \mathrm{Ind}_H^G \mathfrak{A}^*(M)$, and*
(iii) *$\mathrm{Ind}_H^G M$ is a projective $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$-lattice if and only if M is a projective $\mathfrak{A}^*(M)$-lattice.*

6.2. Clean orders and induction

Let R be a discrete valuation ring with field of fractions F of characteristic zero and suppose that the residue field of R is finite.

Definition 6.10. *Let Λ be an R-order in a finite-dimensional semisimple F-algebra A. Then, Λ is said to be clean if it has the following property: if M is a projective Λ-lattice such that FM is free over A then M is free over Λ.*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Theorem 6.11 (Hattori). *Commutative R-orders in finite-dimensional semisimple F-algebras are clean.*

Proof. See [17] or [36, IX Corollary 1.5]. □

Proposition 6.12 ([4, Corollaire to Proposition 3]). *Let H be a normal abelian subgroup of a finite group G and let M be an $R[H]$-lattice such that FM is free of rank 1 over $F[H]$. Then, the following are equivalent:*

(i) $\mathrm{Ind}_H^G M$ *is projective over* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$*;*
(ii) $\mathrm{Ind}_H^G M$ *is free over* $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$*;*
(iii) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is a ring and* $\mathrm{Ind}_H^G M$ *is free over* $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$*;*
(iv) M *is free over* $\mathfrak{A}(F[H], M)$ *and* $\mathfrak{A}^*(M) = \mathfrak{A}(F[H], M)$.

Proof. (i)⇒(iv). By Proposition 6.9(iii), M is projective over $\mathfrak{A}^*(M)$. Moreover, $\mathfrak{A}^*(M)$ is a clean order by Theorem 6.11 and thus M is in fact free over $\mathfrak{A}^*(M)$. Hence $\mathfrak{A}^*(M) = \mathfrak{A}(F[H], M)$ by Proposition 2.2.

(iv)⇒(iii). We have $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathrm{Ind}_H^G \mathfrak{A}^*(M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$, where the second equality is Proposition 6.9(ii). Thus, $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is a ring by Corollary 6.2. Hence, $\mathrm{Ind}_H^G M$ is free over $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ by Corollary 6.6(iii).

(iii)⇒(ii). This follows from Corollary 6.2.

(ii)⇒(i). This follows from the general fact that every free module is projective. □

Remark 6.13. *Let $K/\mathbb{Q}$ be a finite Galois extension, let $\mathfrak{P}$ be a prime of K above the rational prime p, let $M = \mathcal{O}_{K_{\mathfrak{P}}}$, let $H = D(\mathfrak{P}|p)$ be the decomposition group and let $R = \mathbb{Z}_p$. If H is normal and abelian in G and $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$, Proposition 6.12 tells us that p is a decomposition obstruction for K unless $\mathrm{Ind}_H^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p} = \mathfrak{A}_{K/\mathbb{Q},p}$. This observation is crucial in the proofs in Section 8.*

7. Induction for orders of a certain structure

Let R be a discrete valuation ring with field of fractions F of characteristic zero and suppose that the residue field of R is finite. Let G be a finite group and let H be a subgroup of G. In Section 6, we reviewed some general induction properties of the associated order $\mathfrak{A}(F[H], M)$ (with weaker hypotheses on R for some results). In this section, we prove new results concerning inductions of orders of a certain form and then consider arithmetic applications such as the study of weakly ramified extensions.

Let π be a uniformiser of R. For a subgroup P of G, let $\mathrm{ncl}_G(P)$ denote the normal closure of P in G and let $\mathrm{Tr}_P = \sum_{k \in P} k \in R[G]$.

Theorem 7.1. *Let M be an $R[H]$-lattice such that FM is free of rank 1 over $F[H]$. Suppose that there exists a positive integer n and a subgroup P of H such that*

$$\mathfrak{A}(F[H], M) = R[H] + \pi^{-n} R[H] \mathrm{Tr}_P.$$

Then, the following statements hold:

(i) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = R[G] + \pi^{-n} R[G] \mathrm{Tr}_P$.
(ii) $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) = R[G] + \pi^{-n} R[G] \mathrm{Tr}_{\mathrm{ncl}_G(P)}$.
(iii) $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ *is a ring if and only if P is normal in G.*
(iv) *If P is normal in G and M is free over $\mathfrak{A}(F[H], M)$, then $\mathrm{Ind}_H^G \mathfrak{A}(F[H], M)$ is free over $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$.*
(v) *If H is abelian and normal in G and $\mathrm{Ind}_H^G M$ is projective over $\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$, then P is normal in G.*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Proof. Note that if h runs through a set of coset representatives of G/H and k runs through a set of coset representatives of H/P, then hk runs through a set of left coset representatives of G/P. Thus, we have

$$\begin{aligned}\mathrm{Ind}_H^G\mathfrak{A}(F[H],M) &= \mathrm{Ind}_H^G\left(R[H]+\left\{\pi^{-n}\left(\sum_{k\in H/P}a_k k\right):a_k\in R\right\}\cdot\mathrm{Tr}_P\right)\\ &= R[G]+\left\{\sum_{h\in G/H}\pi^{-n}h\left(\sum_{k\in H/P}a_{h,k}k\right):a_{h,k}\in R\right\}\cdot\mathrm{Tr}_P\\ &= R[G]+\left\{\pi^{-n}\left(\sum_{h\in G/H}\sum_{k\in H/P}a_{h,k}hk\right):a_{h,k}\in R\right\}\cdot\mathrm{Tr}_P\\ &= R[G]+\pi^{-n}R[G]\mathrm{Tr}_P,\end{aligned}$$

which proves (i). Moreover, we have

$$\begin{aligned}\mathrm{Ind}_H^G\mathfrak{A}(F[H],M) &= R[G]+\pi^{-n}R[G/P]\mathrm{Tr}_P\\ &= R[G]+\left\{\pi^{-n}\left(\sum_{h\in G/P}a_h h\right):a_h \text{ is a representative of } R/(\pi^n)\right\}\cdot\mathrm{Tr}_P\\ &= \pi^{-n}\left\{\sum_{\gamma\in G}a_\gamma\gamma\in R[G]:\gamma_1^{-1}\gamma_2\in P\Rightarrow a_{\gamma_1}\equiv a_{\gamma_2} \bmod (\pi^n)\right\}.\end{aligned}$$

Thus for every $g\in G$, we have

$$\begin{aligned}g\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)g^{-1} &= R[G]+\pi^{-n}R[G/gPg^{-1}]\mathrm{Tr}_{gPg^{-1}}\\ &= \pi^{-n}\left\{\sum_{\gamma\in G}a_\gamma\gamma\in R[G]:\gamma_1^{-1}\gamma_2\in gPg^{-1}\Rightarrow a_{\gamma_1}\equiv a_{\gamma_2} \bmod (\pi^n)\right\}.\end{aligned}$$

We will now use the following general fact. Let G be a group, let B be any set, let A be a subset of G and let A' be the subgroup of G generated by A. Then from the description of the elements of A' in terms of products of elements of A and their inverses, we have

$$\begin{aligned}&\left\{\{a_\gamma\}_{\gamma\in G}\in\textstyle\prod_{\gamma\in G}B:\gamma_1^{-1}\gamma_2\in A\Rightarrow a_{\gamma_1}=a_{\gamma_2}\right\}\\ &\qquad\qquad=\left\{\{a_\gamma\}_{\gamma\in G}\in\textstyle\prod_{\gamma\in G}B:\gamma_1^{-1}\gamma_2\in A'\Rightarrow a_{\gamma_1}=a_{\gamma_2}\right\}.\end{aligned}$$

This said, by Proposition 6.1, we have that

$$\begin{aligned}\mathfrak{A}(F[G],\mathrm{Ind}_H^G M) &= \bigcap_{g\in G}g\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)g^{-1}\\ &= \pi^{-n}\left\{\sum_{\gamma\in G}a_\gamma\gamma\in R[G]:\gamma_1^{-1}\gamma_2\in\bigcup_{g\in G}gPg^{-1}\Rightarrow a_{\gamma_1}\equiv a_{\gamma_2} \bmod (\pi^n)\right\}\\ &= \pi^{-n}\left\{\sum_{\gamma\in G}a_\gamma\gamma\in R[G]:\gamma_1^{-1}\gamma_2\in \mathrm{ncl}_G(P)\Rightarrow a_{\gamma_1}\equiv a_{\gamma_2} \bmod (\pi^n)\right\}\\ &= R[G]+\pi^{-n}R[G/\mathrm{ncl}_G(P)]\mathrm{Tr}_{\mathrm{ncl}_G(P)},\\ &= R[G]+\pi^{-n}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P)},\end{aligned}$$

which proves (ii).

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

By Corollary 6.2, $\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)$ is a ring if and only if it is equal to $\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$, which by (i) and (ii) is true if and only if $P=\mathrm{ncl}(P)$. This proves (iii). Part (iv) follows from (iii) and Corollary 6.6(iii). Part (v) follows from (iii) and Proposition 6.12(i)⇒(iii). □

We have the following application to the understanding of local freeness in weakly ramified extensions of number fields.

Corollary 7.2. *Let K/F be a finite Galois extension of number fields with Galois group G and let $\mathfrak{P}|\mathfrak{p}$ be two primes of K/F such that $K_{\mathfrak{P}}/F_{\mathfrak{p}}$ is wildly and weakly ramified.*

- *(i) If the inertia group $G_0=G_0(\mathfrak{P}|\mathfrak{p})$ is normal in G, then $\mathcal{O}_{K,\mathfrak{p}}$ is free over $\mathfrak{A}_{K/F,\mathfrak{p}}$.*
- *(ii) Suppose that the decomposition group $D=D(\mathfrak{P}|\mathfrak{p})$ is abelian and normal in G. Then, $\mathcal{O}_{K,\mathfrak{p}}$ is free over $\mathfrak{A}_{K/F,\mathfrak{p}}$ if and only if G_0 is normal in G.*

Proof. Let π be any uniformiser of $\mathcal{O}_{F_{\mathfrak{p}}}$. Then by Theorem 3.9, we have

$$\mathfrak{A}(F_{\mathfrak{p}}[D],\mathcal{O}_{K_{\mathfrak{P}}})=\mathfrak{A}_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}=\mathcal{O}_{F_{\mathfrak{p}}}[D][\pi^{-1}\mathrm{Tr}_{G_0}]=\mathcal{O}_{F_{\mathfrak{p}}}[D]+\pi^{-1}\mathcal{O}_{F_{\mathfrak{p}}}[D]\mathrm{Tr}_{G_0}$$

and $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}(F_{\mathfrak{p}}[D],\mathcal{O}_{K_{\mathfrak{P}}})$. Hence claim (i) follows from Theorem 7.1(iv). Claim (ii) follows from Theorem 7.1(v) for one direction and from claim (i) for the other direction. □

Remark 7.3. *Note that by using Corollary 7.2(ii), databases such as [30], and a computational algebra system such as Magma to determine whether certain subgroups are normal, we can easily read off examples of number fields K and decomposition obstructions for K. For instance, let K be the splitting field of $x^4-x^2-4x-11$ over $\mathbb{Q}$. Then, K is an S_4-extension of $\mathbb{Q}$, for which the prime 2 is weakly ramified, has normal decomposition group isomorphic to C_2^2 and (non-normal) inertia group isomorphic to C_2: in other words, 2 is a decomposition obstruction for K (this case is in fact covered in the proof of Theorem 8.3: it lies on the entry (5) of Table 1).*

We now prove the following generalisation of Theorem 7.1.

Theorem 7.4. *Let M be an $R[H]$-lattice such that FM is free of rank 1 over $F[H]$. Suppose that there exist integers $0=n_0<n_1<\cdots<n_r$ and subgroups*

$$\{e\}=P_0\subsetneq P_1\subsetneq P_2\subsetneq\cdots\subsetneq P_r\subseteq H\subseteq G$$

such that

$$\mathfrak{A}(F[H],M)=\sum_{i=0}^{r}\pi^{-n_i}R[H]\mathrm{Tr}_{P_i}. \tag{7.1}$$

Then, the following statements hold:

- *(i)* $\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)=\sum_{i=0}^{r}\pi^{-n_i}R[G]\mathrm{Tr}_{P_i}$.
- *(ii)* $\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)=\sum_{i=0}^{r}\pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}$.
- *(iii) $\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)$ is a ring if and only if P_i is normal in G for every i.*
- *(iv) If P_i is normal in G for every i and M is free over $\mathfrak{A}(F[H],M)$, then $\mathrm{Ind}_H^G\mathfrak{A}(F[H],M)$ is free over $\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$.*
- *(v) If H is abelian and normal in G and $\mathrm{Ind}_H^G M$ is projective over $\mathfrak{A}(F[G],\mathrm{Ind}_H^G M)$, then P_i is normal in G for every i.*

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Proof. The proof of part (i) is exactly as for Theorem 7.1(i).

We already know from Theorem 7.1 that (ii) holds if $r = 1$. So suppose that $r > 1$. Note that, since each $\mathrm{ncl}_G(P_i)$ is normal in G, for each $g \in G$ we have that

$$g^{-1}\pi^{-n_i}\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}g = \pi^{-n_i}\mathrm{Tr}_{\mathrm{ncl}_G(P_i)} = \mathrm{Tr}_{\mathrm{ncl}_G(P_i)/P_i}\pi^{-n_i}\mathrm{Tr}_{P_i} \in \mathrm{Ind}_H^G\mathfrak{A}(F[H], M),$$

where $\mathrm{Tr}_{\mathrm{ncl}_G(P_i)/P_i}$ is the sum over any fixed choice of coset representatives of $\mathrm{ncl}_G(P_i)/P_i$. Hence for each $g \in G$ we have $\pi^{-n_i}\mathrm{Tr}_{\mathrm{ncl}_G(P_i)} \in g\mathrm{Ind}_H^G\mathfrak{A}(F[H], M)g^{-1}$. Together with Proposition 6.1, this implies that $\pi^{-n_i}\mathrm{Tr}_{\mathrm{ncl}_G(P_i)} \in \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$. Therefore

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \supseteq \sum_{i=0}^{r} \pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}.$$

It remains to show the reverse containment. First note that

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \subseteq \mathrm{Ind}_H^G\mathfrak{A}(F[H], M) = \sum_{i=0}^{r} \pi^{-n_i}R[G]\mathrm{Tr}_{P_i}, \tag{7.2}$$

where the containment follows from Remark 6.4 and the equality is part (i). Let $\theta \in \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$. Then, we can write $\theta = \sum_{i=0}^{r} \pi^{-n_i}\theta_i\mathrm{Tr}_{P_i}$, where $\theta_i \in R[G]$ for each i. For each integer j with $0 \le j \le r$, we shall prove that

$$\theta \in \sum_{i=0}^{r-j-1} \pi^{-n_i}R[G]\mathrm{Tr}_{P_i} + \sum_{i=r-j}^{r} \pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}.$$

We proceed by induction on j and first consider the base case $j = 0$. We have that

$$\pi^{n_{r-1}}\theta = \sum_{i=0}^{r} \pi^{n_{r-1}-n_i}\theta_i\mathrm{Tr}_{P_i} \in R[G] + \pi^{n_{r-1}-n_r}R[G]\mathrm{Tr}_{P_r}.$$

Also note that for each $g \in G$, we have

$$\begin{aligned} g^{-1}\pi^{n_{r-1}}\theta g &\in g^{-1}\pi^{n_{r-1}}\mathfrak{A}(F[G], \mathrm{Ind}_H^G M)g \\ &= \pi^{n_{r-1}}\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \\ &\subseteq \pi^{n_{r-1}}\mathrm{Ind}_H^G\mathfrak{A}(F[H], M) \\ &\subseteq R[G] + \pi^{n_{r-1}-n_r}R[G]\mathrm{Tr}_{P_r}. \end{aligned}$$

Hence,

$$\pi^{n_{r-1}}\theta \in \bigcap_{g\in G} g\left(R[G] + \pi^{n_{r-1}-n_r}R[G]\mathrm{Tr}_{P_r}\right)g^{-1} = R[G] + \pi^{n_{r-1}-n_r}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_r)},$$

where the equality follows from the case $r = 1$. Thus there exists $\alpha \in R[G]$ such that

$$\theta - \pi^{-n_r}\alpha\mathrm{Tr}_{\mathrm{ncl}_G(P_r)} \in \pi^{-n_{r-1}}R[G] \cap \mathrm{Ind}_H^G\mathfrak{A}(F[H], M) = \sum_{i=0}^{r-1} \pi^{-n_i}R[G]\mathrm{Tr}_{P_i},$$

where the equality follows from (7.2) and the containment $R[G]\mathrm{Tr}_{P_r} \subseteq R[G]\mathrm{Tr}_{P_{r-1}}$, which holds since $\mathrm{Tr}_{P_r} = \mathrm{Tr}_{P_r/P_{r-1}}\mathrm{Tr}_{P_{r-1}}$. This completes the base case $j = 0$.

We now proceed with the induction step. Suppose our claim is valid for $j - 1$, and let us prove it for j. Using the inductive hypothesis and subtracting an appropriate element of $\sum_{i=j+1}^{r} \pi^{-n_i}R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)}$, we can and do assume without loss of generality that

$$\theta = \sum_{i=0}^{r-j} \pi^{-n_i}\theta_i\mathrm{Tr}_{P_i} \in \mathfrak{A}(F[G], \mathrm{Ind}_H^G M),$$

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

for some $\theta_i \in R[G]$. Hence, it remains to show that

$$\theta \in \sum_{i=0}^{r-j-1} \pi^{-n_i} R[G]\mathrm{Tr}_{P_i} + \pi^{-n_{r-j}} R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_{r-j})}.$$

As in the base case, for each $g \in G$ we have

$$\begin{aligned} g^{-1}\pi^{n_{r-j-1}}\theta g &\in \pi^{n_{r-j-1}-n_{r-j}} R[G] \cap \pi^{n_{r-j-1}} \mathfrak{A}(F[G], \mathrm{Ind}_H^G M) \\ &\subseteq \pi^{n_{r-j-1}-n_{r-j}} R[G] \cap \pi^{n_{r-j-1}} \mathrm{Ind}_H^G \mathfrak{A}(F[H], M) \\ &\subseteq R[G] + \pi^{n_{r-j-1}-n_{r-j}} R[G]\mathrm{Tr}_{P_{r-j}}, \end{aligned}$$

so, by the result for $r = 1$, we have

$$\pi^{n_{r-j-1}}\theta \in R[G] + \pi^{n_{r-j-1}-n_{r-j}} R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_{r-j})}.$$

Thus, there exists $\alpha \in R[G]$ such that

$$\theta - \pi^{-n_{r-j}}\alpha\mathrm{Tr}_{\mathrm{ncl}_G(P_{r-j})} \in \pi^{-n_{r-j-1}} R[G] \cap \left(\sum_{i=0}^{r-j} \pi^{-n_i}\theta_i \mathrm{Tr}_{P_i}\right) = \sum_{i=0}^{r-j-1} \pi^{-n_i} R[G]\mathrm{Tr}_{P_i}.$$

This concludes the induction step. Therefore, we deduce that

$$\mathfrak{A}(F[G], \mathrm{Ind}_H^G M) = \sum_{i=0}^{r} \pi^{-n_i} R[G]\mathrm{Tr}_{\mathrm{ncl}_G(P_i)},$$

which concludes the proof of part (ii).

We easily see with the same methods that

$$\mathrm{Ind}_H^G \mathfrak{A}(F[H], M) = \mathfrak{A}(F[G], \mathrm{Ind}_H^G M)$$

precisely when $P_i = \mathrm{ncl}_G(P_i)$ for every i, establishing part (iii). Part (iv) follows from part (iii) and Corollary 6.6(iii). Part (v) follows from Proposition 6.12(i)⇒(iii). □

Remark 7.5. *It follows from the proof of Theorem 7.4 that the subgroups P_i and the numbers n_i are uniquely determined by $\mathfrak{A}(F[H], M)$. Moreover, P_i is normal in H (a way to see this from what we already proved is the following:* $\mathrm{Ind}_H^H \mathfrak{A}(F[H], M) = \mathfrak{A}(F[H], M)$ *is a ring, so that we can apply (iii) with $G = H$) and π^{n_i} divides the order of P_i for all i.*

8. Leopoldt-type theorems for A_4, S_4 and A_5-extensions of $\mathbb{Q}$

In this section, we prove Theorems 1.7, 1.8 and 1.9 from the introduction. We first give an overview of our methods. Let $K/\mathbb{Q}$ be a finite Galois extension, let $G = \mathrm{Gal}(K/\mathbb{Q})$, and suppose that $G \cong A_4$, S_4 or A_5. As proven in Corollary 2.7, the only property to check is local freeness. By Proposition 4.10, if G is isomorphic to A_4 or S_4 then we only have to check for local freeness at 2, while freeness in the $G \cong A_5$-case only happens if we have local freeness simultaneously at 2, 3 and 5.

If $G \cong A_4$ or S_4, let $p = 2$. If $G \cong A_5$, let $p \in \{2, 3, 5\}$. Let $\mathfrak{P}$ be a prime of K above p, with decomposition group $D = D(\mathfrak{P}|p)$. We will first apply the techniques of the previous sections to compute $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$ and determine whether $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$.

When $G \cong A_4$ or S_4, in some cases it will suffice to directly apply results such as Theorem 3.14, Lemma 4.11, Proposition 4.12 or Corollary 7.2(i). We will study these cases at the beginning of each of the proofs. In the remaining cases, the analysis will be somewhat more complicated.

It could be the case that $\mathcal{O}_{K_{\mathfrak{P}}}$ is not even free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$. In general, this does not necessarily imply that $\mathcal{O}_{K,p}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},p}$. However, this will occur only when $G \cong S_4$ and in two specific cases:

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

- $D = G$, which guarantees that $\mathcal{O}_{K,p} = \mathcal{O}_{K_\mathfrak{P}}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},p} = \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$: we will use [5, Algorithm 3.1(6)] to verify that in four specific S_4-extensions of $\mathbb{Q}_2$ the ring of integers is not free over its associated order;
- D is dihedral of order 8, in which case, by Theorem 3.10, $\mathcal{O}_{K_\mathfrak{P}}$ is not even projective over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$, which allows us to conclude that $\mathcal{O}_{K,p}$ cannot be free over $\mathfrak{A}_{K/\mathbb{Q},p}$ by Proposition 6.8.

We call this method 'the non-freeness method'.

In all the remaining cases, we have that $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$. We will see that the structure of $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ will always satisfy the hypotheses of Theorem 7.4 (in some cases its simpler version, i.e. Theorem 7.1). We can then apply Theorem 7.4(i) and (ii) to compute $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ and $\mathfrak{A}_{K/\mathbb{Q},p}$. By Proposition 6.5, we are reduced to verifying whether $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$. In all cases of $G \cong A_4$ with predicted non-freeness of $\mathcal{O}_K$ over $\mathfrak{A}_{K/\mathbb{Q}}$, we can reduce to the case in which D is normal in G and abelian, hence apply Theorem 7.4(v). We call this method 'the theoretical freeness method'; this can also be applied to some cases when $G \cong S_4$.

When the above strategy cannot be followed, the structure of $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ allows us to construct both $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ and $\mathfrak{A}_{K/\mathbb{Q},p}$ in Magma. Hofmann and Johnston [18, §8.5] described the implementation of an algorithm in Magma that, given a finite group Γ, a rational prime p, and $\mathbb{Z}[\Gamma]$-lattices X and Y contained in $\mathbb{Q}[\Gamma]$, determines whether the localisations X_p and Y_p are isomorphic over $\mathbb{Z}_{(p)}[\Gamma]$. Note that by [9, Proposition (30.17)], this is equivalent to checking whether the p-adic completions are isomorphic over $\mathbb{Z}_p[\Gamma]$. In present situation, we are interested in understanding whether $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ is free over its associated order $\mathfrak{A}_{K/\mathbb{Q},p}$. By Lemma 2.1 this condition is equivalent to $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ being isomorphic to $\mathfrak{A}_{K/\mathbb{Q},p}$ as $\mathbb{Z}_p[G]$-lattices. Since both lattices will be of the form $\mathbb{Z}_p[G] + \frac{1}{p^{n_1}}\mathbb{Z}_p[G]\mathrm{Tr}_{H_1} + \cdots + \frac{1}{p^{n_k}}\mathbb{Z}_p[G]\mathrm{Tr}_{H_k}$, which is the completion of $\mathbb{Z}[G] + \frac{1}{p^{n_1}}\mathbb{Z}[G]\mathrm{Tr}_{H_1} + \cdots + \frac{1}{p^{n_k}}\mathbb{Z}[G]\mathrm{Tr}_{H_k}$, the aforementioned algorithm will tell us if $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$. We call this method 'the algorithmic freeness method'.

With both freeness methods we will mostly find that $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_p}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},p}$, that is, p is a decomposition obstruction for K.

Notation. *Let G be a finite group, let $H_1, \ldots, H_k$ be subgroups of G and let $n_1, \cdots, n_k$ be integers. We will denote by $\langle 1, \frac{1}{p^{n_1}}\mathrm{Tr}_{H_1}, \cdots, \frac{1}{p^{n_k}}\mathrm{Tr}_{H_k}\rangle_G^p$ the lattice*

$$\mathbb{Z}_p[G] + \frac{1}{p^{n_1}}\mathbb{Z}_p[G]\mathrm{Tr}_{H_1} + \cdots + \frac{1}{p^{n_k}}\mathbb{Z}_p[G]\mathrm{Tr}_{H_k}.$$

8.1. Galois module structure of A_4-extensions of $\mathbb{Q}$

In this subsection, we shall prove the following result, which is Theorem 1.7 stated in the introduction.

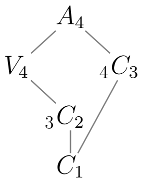
Theorem 8.1. *Let $K/\mathbb{Q}$ be a Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong A_4$. *Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if* 2 *is tamely ramified or has full decomposition group.*

Remark 8.2. *After considering computational evidence, in [5, §8] the authors raised the question of whether it is always the case that $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ for every A_4-extension $K/\mathbb{Q}$. Theorem 8.1 shows that this is false. Indeed, one can use the database of number fields [30] to verify that every possible decomposition group of* 2 *of even order can be realised by an A_4-extension $K/\mathbb{Q}$ in which* 2 *is wildly ramified.*

Proof of Theorem 8.1. We already showed the 'if' direction in Proposition 4.12. Now we prove that if 2 is wildly ramified in $K/\mathbb{Q}$ and does not have full decomposition group then $\mathcal{O}_K$ is not (locally) free (at 2) over $\mathfrak{A}_{K/\mathbb{Q}}$. Let V_4 denote the unique normal subgroup of $G := \mathrm{Gal}(K/\mathbb{Q}) \cong A_4$ of order 4, which

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

is isomorphic to $C_2 \times C_2$. Recall that $A_4 \cong V_4 \rtimes C_3$ and we have the following lattice of the subgroups of A_4 up to conjugacy (see, for instance, the GroupNames database [11]).



Here the subscript on the left denotes the number of conjugate subgroups and is taken to be 1 when omitted (so that the subgroup is normal).

Let $\mathfrak{P}$ be a prime of K above 2, let $D = D(\mathfrak{P}|2)$ be the decomposition group and let $G_0 = G_0(\mathfrak{P}|2)$ be the inertia group of $K/\mathbb{Q}$. Since 2 is wildly ramified, D has even order. Thus, since D is a proper subgroup of G, the subgroup lattice implies that either $D = V_4$ or $D \cong C_2$. More precisely, there are three possibilities for the pair (D, G_0) up to isomorphism: (V_4, V_4), (V_4, C_2) and (C_2, C_2). Since D is abelian in each of these cases, we have that $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ by Theorem 3.3. Thus by Proposition 6.5 we have that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} \cong \mathrm{Ind}_D^G \mathcal{O}_{K_{\mathfrak{P}}} \cong \mathcal{O}_{K,2}$ as $\mathfrak{A}_{K/\mathbb{Q},2}$-lattices. Therefore, it suffices to show that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ in each of the three cases; in other words, we will show that 2 is a decomposition obstruction for K. We will apply the 'theoretical freeness method' in all cases.

First suppose that $D = G_0 = V_4$. Then from the database of p-adic fields [24], we see that there are four possible extensions $K_{\mathfrak{P}}/\mathbb{Q}_2$, each of which has 1 and 3 as (lower) ramification jumps. Let F denote the subfield of $K_{\mathfrak{P}}$ fixed by G_2. Then by Remark 3.12, we have $e_{G_2} \in \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ since

$$\sum_{i=0}^{\infty}(|G_i(K_{\mathfrak{P}}/F)|-1) = 1+1+1+1 = 4 \geq 4 = |G_0(K_{\mathfrak{P}}/\mathbb{Q}_2)| \cdot v_2(|G_2|).$$

Similarly, we have $e_{V_4} = e_{G_1} \in \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ since

$$\sum_{i=0}^{\infty}(|G_i(K_{\mathfrak{P}}/\mathbb{Q}_2)|-1) = 3+3+1+1 = 8 \geq 8 = |G_0(K_{\mathfrak{P}}/\mathbb{Q}_2)| \cdot v_2(|V_4|).$$

Thus, $K_{\mathfrak{P}}/\mathbb{Q}_2$ is almost-maximally ramified, and so by Theorem 3.10(i) we have that

$$\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \mathbb{Z}_2[D][e_{G_2}, e_{G_1}] = \langle 1, \frac{1}{2}\mathrm{Tr}_{G_2}, \frac{1}{4}\mathrm{Tr}_{V_4}\rangle_D^2.$$

Since $G_2 \cong C_2$ is not normal in G and D is both abelian and normal in G, Theorem 7.4(v) implies that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Hence $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. As an aside, using Theorem 7.4(i) and (ii) and the fact that $\mathrm{ncl}_G(G_2) = V_4$, we note that in this case we have

$$\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \left\langle 1, \frac{1}{2}\mathrm{Tr}_{G_2}, \frac{1}{4}\mathrm{Tr}_{V_4}\right\rangle_G^2 \supseteq \left\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}\right\rangle_G^2 = \mathfrak{A}_{K/\mathbb{Q},2}.$$

Now suppose that $D = V_4$ and $G_0 \cong C_2$. Since $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ and $G_0 = G_1$ is not dihedral of order 4, Theorem 3.10 implies that $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \mathbb{Z}_2[D][e_{G_0}] = \langle 1, \frac{1}{2}\mathrm{Tr}_{G_0}\rangle_D^2$. (Alternatively, we can use the database of p-adic fields [24] to check for almost-maximal ramification as in the previous case; the ramification jump turns out to be 1 or 2). Since D is both abelian and normal in G and G_0 is not normal in G, Theorem 7.1(v) implies that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Hence, $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Note that in the next paragraph, we shall use that

$$\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \left\langle 1, \frac{1}{2}\mathrm{Tr}_{G_0}\right\rangle_G^2 \supseteq \left\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}\right\rangle_G^2 = \mathfrak{A}_{K/\mathbb{Q},2},$$

which follows from Theorem 7.1(i) and (ii).

Finally, suppose $D = G_0 \cong C_2$. Then, $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ is a $\mathbb{Z}_2$-order in $\mathbb{Q}_2[D] \cong \mathbb{Q}_2[C_2]$ strictly containing $\mathbb{Z}_2[D]$. As there is only one such order, we must have $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \langle 1, \frac{1}{2}\mathrm{Tr}_D\rangle_D^2$. Since D is not normal in

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

G, we cannot directly apply Theorem 7.1(v) as in the previous cases. Instead, Theorem 7.1(i) and (ii) implies that

$$\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \left\langle 1, \frac{1}{2}\mathrm{Tr}_D \right\rangle_G^2 \supseteq \left\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4} \right\rangle_G^2 = \mathfrak{A}_{K/\mathbb{Q},2}.$$

Once we fix a copy of C_2 inside G, note that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ and $\mathfrak{A}_{K/\mathbb{Q},2}$ are exactly the same as in the (V_4, C_2)-case of the previous paragraph, where we already showed that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Therefore $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. □

8.2. *Galois module structure of S_4-extensions of $\mathbb{Q}$*

In this subsection, we shall prove the following result, which is Theorem 1.8 stated in the introduction.

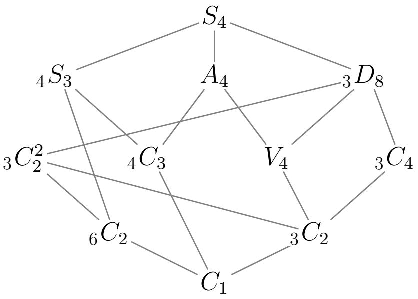
Theorem 8.3. *Let $K/\mathbb{Q}$ be a Galois extension with $G := \mathrm{Gal}(K/\mathbb{Q}) \cong S_4$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if one of the following conditions on $K/\mathbb{Q}$ holds:*

(i) *2 is tamely ramified;*
(ii) *2 has decomposition group equal to the unique subgroup of G of order* 12*;*
(iii) *2 is wildly and weakly ramified and has full decomposition group; or*
(iv) *2 is wildly and weakly ramified, has decomposition group of order* 8 *in G, and has inertia subgroup equal to the unique normal subgroup of order* 4 *in G.*

Proof. By Proposition 4.10, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$.

We first show that if any of conditions (i)–(iv) hold then $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$. In case (i), this follows from Theorem 3.14. In case (ii), Lemma 4.11 shows that 2 is wildly and weakly ramified in $K/\mathbb{Q}$ and has inertia group equal to the unique normal subgroup of order 4 in G (note that A_4 is the unique subgroup of S_4 of order 12). Therefore in cases (ii), (iii) and (iv), 2 is wildly and weakly ramified in $K/\mathbb{Q}$ and its inertia group is normal in G, and so the desired result follows from Corollary 7.2(i).

It now remains to show that if we are not in any of the cases (i)–(iv) then $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. We have the following lattice of the subgroups of S_4 up to conjugacy (see, for instance, the GroupNames database [11]).



Here the subscript on the left denotes the number of conjugate subgroups and is taken to be 1 when omitted (so that the subgroup is normal). In particular, the only normal subgroups are C_1, V_4, A_4 and S_4. (Recall that $V_4 \cong C_2 \times C_2$.)

We fix an isomorphism $G := \mathrm{Gal}(K/\mathbb{Q}) \cong S_4$ and denote by A_4, D_8, S_3, C_2^2, V_4, C_4 a choice of subgroups of G in such a way that whenever there is a containment between choices of conjugates of two such subgroups, one of the subgroups is in fact contained in the other.

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

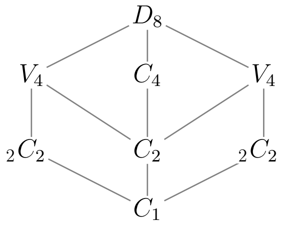
Suppose that $K/\mathbb{Q}$ does not satisfy any of the conditions (i)–(iv). Let $\mathfrak{P}$ be a prime of K above 2 and let $D = D(\mathfrak{P}|2)$ be the decomposition group. In particular, 2 is wildly ramified in $K/\mathbb{Q}$ and so D must be of even order. We cannot have $D = A_4$ as this corresponds to case (ii). Moreover, we cannot have $D = S_3$ since the subgroups of D of order 2 are not normal, but the wild inertia subgroup G_1 must be normal in D.

We will start by applying the 'non-freeness method' in those cases in which $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$. By Theorem 3.3, we are in the case in which D is not abelian. Suppose that $D = S_4$. Since we are not in case (iii), this implies that 2 is wildly but not weakly ramified in $K/\mathbb{Q}$. From the database of p-adic fields [24], we see that there are four possibilities for the completed extension $K_{\mathfrak{P}}/\mathbb{Q}_2$. By using the updated Magma implementation of [5, Algorithm 3.1(6)], which is based on that of [7, §4.2], we can verify that $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ in any of these cases (for the details on the implementation see Section A.1). Since the decomposition group is full, this immediately implies that $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$.

Now suppose that $D \cong D_8$; without loss of generality, we can and do assume that $D = D_8$. Since we are assuming $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$, we have that $\mathcal{O}_{K_{\mathfrak{P}}}$ is not projective over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ by Theorem 3.10, and so $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ by Proposition 6.8. As an aside, by using the database [24], Theorem 3.10 and Remark 3.12, it is straightforward to check that $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ if and only if the ramification jumps of $K_{\mathfrak{P}}/\mathbb{Q}_2$ are 1, 3 and 5.

Therefore in the remaining cases, we can and do assume that $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$, since either D is abelian (in which case we can apply Theorem 3.3) or $D = D_8$ (in which case the situation in which $\mathcal{O}_{K_{\mathfrak{P}}}$ is not free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ has already been considered in the previous paragraph). For these cases, we will apply the 'algorithmic freeness method'. As we wish to show that $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ (so that 2 is a decomposition obstruction for K), by Proposition 6.5 it suffices to show that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Our strategy will be to determine the possible ramification groups, use this to derive the explicit structure of $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ and then apply Theorem 7.4(i) and (ii) to obtain explicit descriptions of $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ and $\mathfrak{A}_{K/\mathbb{Q},2}$, which will be listed in Table 1 below. For instance, if $D = D_8$ and $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_4}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle^2_{D_8}$ (where V_2 is the subgroup of C_4 of order 2), then by Theorem 7.4(i) the same groups will appear in $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$, so that $\mathrm{Ind}_D^G \mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_4}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle^2_G$. The normal closure of C_4 and D_8 in G is G, while the normal closure of V_2 is V_4; by Theorem 7.4(ii), this tells us that $\mathfrak{A}_{K/\mathbb{Q},2} = \langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_G\rangle^2_G$ (in fact, this will be entry (1) of Table 1).

We first consider the case $D = D_8$. We have the following subgroup lattice.



Note that D_8 has a unique normal subgroup of order 2, which we denoted by V_2, and, as a subgroup of S_4, this is generated by a double transposition and contained in C_4. (Also note that under D_8-conjugation we have three conjugacy classes of subgroups of order 2 compared to two in the S_4-lattice).

We now find $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ using Theorem 3.10, which determines the structure of the associated order depending upon whether $K_{\mathfrak{P}}/\mathbb{Q}_2$ is almost-maximally ramified or not. We recall we are assuming $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$. Suppose that $K_{\mathfrak{P}}/\mathbb{Q}_2$ is almost-maximally ramified. Then by Theorem 3.10(i), we have $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \mathbb{Z}_2[D] + \sum_{t\geq 1} \frac{1}{|G_t|}\mathbb{Z}_2[D]\mathrm{Tr}_{G_t}$ and all quotients of two consecutive different ramification groups are of order 2 (see the database [24], for example). We have that V_2 must be among the ramification groups since they are all normal in D_8. Thus if the ramification index of $K_{\mathfrak{P}}/\mathbb{Q}_2$ is 2, then V_2 is the unique ramification group. Otherwise, there is a ramification group of order 4, which must be one of V_4,

Table 1. *Local freeness at 2 in S_4-extensions.*

	$\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$	$\mathfrak{A}_{K/\mathbb{Q},2}$
(1)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_4}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_G\rangle_G^2$
(2)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle_G^2$	$\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_G\rangle_G^2$
(3)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_G\rangle_G^2$
(4)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_4}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{4}\mathrm{Tr}_G\rangle_G^2$
(5)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{V_4}\rangle_G^2$	$\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}\rangle_G^2$
(6)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}, \frac{1}{4}\mathrm{Tr}_G\rangle_G^2$
(7)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{W_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}\rangle_G^2$	$\langle 1, \frac{1}{4}\mathrm{Tr}_G\rangle_G^2$
(8)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2^2}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_G\rangle_G^2$
(9)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_{V_4}\rangle_G^2$
(10)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{W_2}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_G\rangle_G^2$

C_2^2 or C_4. Moreover, D_8 is a ramification group if and only if the ramification index of $K_\mathfrak{P}/\mathbb{Q}_2$ is 8. This case contributes to entries (1), (2), (3), (4), (5), (6) and (9) of Table 1.

Suppose that $K_\mathfrak{P}/\mathbb{Q}_2$ is not almost-maximally ramified. Then by Theorem 3.10(ii), we deduce that $G_0 \cong C_2^2$ and $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \langle 1, \frac{1}{2}\mathrm{Tr}_{G_0}\rangle_G^2$. Moreover, by Remark 3.12 we must have that $G_2 = \{1\}$ or $G_2 \cong C_2$ and $G_3 = \{1\}$, but in the latter case the upper ramification jumps are not integral, which is not possible by Hasse-Arf theorem (alternatively, just use the database [24]); hence, $K_\mathfrak{P}/\mathbb{Q}_2$ is weakly ramified. Note that G_0 is not equal to V_4; otherwise, we are in case (iv) of the statement of Theorem 8.3; hence, we can assume $G_0 = C_2^2$. This contributes to entry (8) of Table 1.

Now suppose that $D \cong C_4$; without loss of generality, we can and do assume that $D = C_4$. If the ramification index of $K_\mathfrak{P}/\mathbb{Q}_2$ is 2, then $G_0 = V_2$ and by Remark 3.12 $K_\mathfrak{P}/\mathbb{Q}_2$ is almost-maximally ramified, and hence $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \langle 1, \frac{1}{2}\mathrm{Tr}_{G_0}\rangle_D^2$ (see [3, Corollaire 3 to Théorème 1], for example), which contributes to entry (9) of Table 1. If the ramification index is 4, then there must be two ramification jumps; since the upper ramification jumps are integral, Remark 3.12 implies that the extension is almost-maximally ramified and so $\frac{1}{2}\mathrm{Tr}_{V_2}$ and $\frac{1}{4}\mathrm{Tr}_D$ belong to $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$. Hence $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} = \langle 1, \frac{1}{2}\mathrm{Tr}_{V_2}, \frac{1}{4}\mathrm{Tr}_D\rangle_D^2$, where the containment '$\subseteq$' follows from the fact that the right-hand side is the unique maximal order in $\mathbb{Q}_2[D]$ (see [3, Proposition 5], for example). This corresponds to entry (4) of Table 1.

Finally, in the cases $D \cong C_2^2$ or $D \cong C_2$, we already computed $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ in the proof of Theorem 8.1. Note that in the present proof and notation the case $D \cong C_2^2$ corresponds to either $D = V_4$ (which contributes to entry (5) of Table 1) or $D = C_2^2$ (entries (6) and (7), where we denote by W_2 a choice of a subgroup of S_4 generated by a transposition and contained in D_8). The case $D \cong C_2$ corresponds to $D = V_2$ (entry (9)) or $D = W_2$ (entry (10)).

As anticipated, all the possible values of $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ and $\mathfrak{A}_{K/\mathbb{Q},2}$ are listed in Table 1.

We conclude the application of the 'algorithmic freeness method' by using the algorithm [18, §8.5], as explained in the overview at the beginning of this section. We find that $\mathrm{Ind}_D^G\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ in each of the ten cases in Table 1 (for the implementation see Section A.2). □

Remark 8.4. *In some of the cases, we can apply the 'theoretical freeness method': cases (5) and (9) from Table 1 can be tackled using Theorem 7.4(v) and cases (7) and (10) using Theorem 7.4(v) combined with Proposition 6.8. More precisely:*

- *for (5) we apply Theorem 7.4(v) with $H = V_4$ and $G = S_4$;*
- *for (7) we apply Theorem 7.4(v) with $H = C_2^2$ and $G = D_8$ and Proposition 6.8 inducing from D_8 to* $\mathrm{Gal}(K/\mathbb{Q}) \cong S_4$;
- *for (9) we apply Theorem 7.4(v) with $H = V_4$ and $G = S_4$;*
- *for (10) we apply Theorem 7.4(v) with $H = W_2$ and $G = D_8$ and Proposition 6.8 inducing from D_8 to* $\mathrm{Gal}(K/\mathbb{Q}) \cong S_4$.

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Note that here G is not necessarily the Galois group and H is not necessarily one of the decomposition groups.

Remark 8.5. *The computations in the proof of Theorem 8.3 show that each of the lattices considered is free over its associated order if and only if the lattice is a ring if and only if the lattice is equal to its associated order. However, with the algorithm of [18, §8.5] we found that $\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{D_8}\rangle_G^2$ is free over $\langle 1, \frac{1}{4}\mathrm{Tr}_{V_4}, \frac{1}{8}\mathrm{Tr}_{G}\rangle_G^2$ (see Section A.2 for the implementation).*

8.3. Galois module structure of A_5-extensions of $\mathbb{Q}$

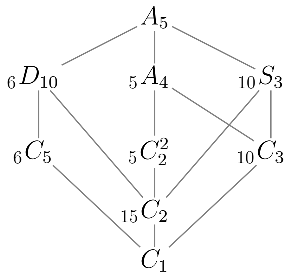
In this subsection, we shall prove the following result, which is Theorem 1.9 stated in the introduction.

Theorem 8.6. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$. Then, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if all three of the following conditions on $K/\mathbb{Q}$ hold:*

(i) *2 is tamely ramified;*
(ii) *3 is tamely ramified or is weakly ramified with ramification index* 6; *and*
(iii) *5 is tamely ramified or is weakly ramified with ramification index* 10.

Proof of Theorem 8.6. By Corollary 2.7, $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_{K,p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$ for every rational prime p. If p is tamely ramified in $K/\mathbb{Q}$ then $\mathcal{O}_{K,p}$ is indeed free over $\mathfrak{A}_{K/\mathbb{Q},p}$ by Theorem 3.14. Thus, it remains to consider the situation in which at least one of the primes $p = 2, 3, 5$ is wildly ramified in $K/\mathbb{Q}$.

We have the following lattice of the subgroups of A_5 up to conjugacy (see, for instance, the GroupNames database [11]).



Here the subscript on the left denotes the number of conjugate subgroups. Recall that A_5 is simple and note that the subgroup lattice shows that isomorphic subgroups must be conjugate. Moreover, since A_5 is not soluble, no prime can have full decomposition group. We fix an isomorphism $G := \mathrm{Gal}(K/\mathbb{Q}) \cong A_5$ and denote by A_4, D_{10} etc. a choice of subgroups of G in such a way that whenever there is a containment between choices of conjugates of two such subgroups, one of the subgroups is in fact contained in the other.

Suppose that $p = 2$ is wildly ramified in $K/\mathbb{Q}$. Let $\mathfrak{P}$ be a prime of K above 2 and let $D(2)$ be its decomposition group. Then, $D(2)$ must be isomorphic to A_4, C_2^2 or C_2, since for every other subgroup H of A_5 there is no normal non-trivial 2-subgroup in H. Hence in each of these cases $\mathcal{O}_{K_\mathfrak{P}}$ is free over $\mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ (if $D(2) = A_4$, this follows from Lemma 4.11 and Theorem 3.9; otherwise, this follows from Theorem 3.3). We will apply the 'algorithmic freeness method' for every such case. By Proposition 6.5, $\mathrm{Ind}_{D(2)}^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2} \cong \mathrm{Ind}_{D(2)}^G \mathcal{O}_{K_\mathfrak{P}} \cong \mathcal{O}_{K,2}$ as $\mathfrak{A}_{K/\mathbb{Q},2}$-lattices. Thus we need to analyse when $\mathrm{Ind}_{D(2)}^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$. Note that, by Lemma 4.11, Theorem 3.9 and Theorem 7.1(i), the structure of $\mathrm{Ind}_{D(2)}^G \mathfrak{A}_{K_\mathfrak{P}/\mathbb{Q}_2}$ in the case $D(2) = A_4$ is covered by the proof of Theorem 8.1. Hence, in each of the aforementioned

Table 2. *Local freeness at 2 in A_5-extensions.*

	$\mathrm{Ind}_{D(2)}^{G}\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$	$\mathfrak{A}_{K/\mathbb{Q},2}$
(1)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_G\rangle_G^2$
(2)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}\rangle_G^2$	$\langle 1, \frac{1}{4}\mathrm{Tr}_G\rangle_G^2$
(3)	$\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2^2}\rangle_G^2$	$\langle 1, \frac{1}{2}\mathrm{Tr}_G\rangle_G^2$

Table 3. *Local freeness at 3 and 5 in A_5-extensions.*

	$\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$	$\mathfrak{A}_{K/\mathbb{Q},p}$
(1)	$\langle 1, \frac{1}{p}\mathrm{Tr}_{C_p}\rangle_G^p$	$\langle 1, \frac{1}{p}\mathrm{Tr}_G\rangle_G^p$
(2)	$\langle 1, \frac{1}{p}\mathrm{Tr}_{D_{2p}}\rangle_G^p$	$\langle 1, \frac{1}{p}\mathrm{Tr}_G\rangle_G^p$

possibilities for $D(2)$, we already know $\mathrm{Ind}_{D(2)}^{G}\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ and $\mathfrak{A}_{K/\mathbb{Q},2}$ from the proof of Theorem 8.1, using Theorem 7.4(i) and (ii). The results are shown in Table 2.

We now use the Magma implementation of the algorithm described in [18, §8.5]. We can hence verify that in none of the above cases $\mathrm{Ind}_{D(2)}^{G}\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2} \cong \mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/\mathbb{Q},2}$ (see Section A.3 for the implementation).

Now suppose that $p = 3$ or 5 and that p is wildly ramified in $K/\mathbb{Q}$. Let $\mathfrak{P}$ be a choice of a prime of K above p and let $D(p)$ be its decomposition group. There is no Galois extension $L/\mathbb{Q}_3$ such that $\mathrm{Gal}(L/\mathbb{Q}_3) \cong A_4$ (since the subgroups of A_4 of order 3 are not normal). Hence, $D(p)$ must be isomorphic to either D_{2p} or C_p, which implies that $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$ by Theorems 3.3 and 3.4. Again we can use the 'algorithmic freeness method', so that our goal is to analyse when $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$. If $D(p) \cong C_p$ (in which case we can and do assume that $D(p) = C_p$), then as $K_{\mathfrak{P}}/\mathbb{Q}_p$ is wildly ramified this implies that $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p} = \langle 1, \frac{1}{p}\mathrm{Tr}_{D(p)}\rangle_{D(p)}^p$, which is the unique maximal order in $\mathbb{Q}_p[D(p)]$. If $D(p) \cong D_{2p}$ (in which case we can and do assume that $D = D_{2p}$), we can use Theorem 3.10: in case of almost-maximal ramification, $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p} = \langle 1, \frac{1}{p}\mathrm{Tr}_{C_p}\rangle_{D(p)}^p$ (which gives the same structure for $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$ as when $D(p) = C_p$); otherwise, by Remark 3.13, $K_{\mathfrak{P}}/\mathbb{Q}_p$ is weakly and totally ramified and $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p} = \langle 1, \frac{1}{p}\mathrm{Tr}_{D(p)}\rangle_{D(p)}^p$. Hence there are two possibilities for $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$ and $\mathfrak{A}_{K/\mathbb{Q},p}$, shown in Table 3.

We used the Magma implementation of the algorithm from [18, §8.5] to verify that $\mathrm{Ind}_{D(p)}^{G}\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_p}$ is free over $\mathfrak{A}_{K/\mathbb{Q},p}$ if and only if we are in case (2), that is, precisely when $K_{\mathfrak{P}}/\mathbb{Q}_p$ is weakly ramified or, equivalently, when it is not almost-maximally ramified (see Section A.3). □

Remark 8.7. *Note that from the proof of Theorem 8.1, we already knew that neither $\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2}\rangle_{A_4}^2$ nor $\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}\rangle_{A_4}^2$ are even projective over their associated orders; induction from A_4 to S_4 and Proposition 6.8 permit us to conclude that $\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2}\rangle_G^2$ and $\langle 1, \frac{1}{2}\mathrm{Tr}_{C_2}, \frac{1}{4}\mathrm{Tr}_{C_2^2}\rangle_G^2$ are not projective over their associated orders. Thus we can treat cases (1) and (2) from Table 2 without using the algorithm.*

Remark 8.8. *Note that for $p = 3$ and $p = 5$ we found that $\langle 1, \frac{1}{p}\mathrm{Tr}_{D_{2p}}\rangle_G^p$ is free over $\langle 1, \frac{1}{p}\mathrm{Tr}_G\rangle_G^p$ without the two being equal. We also found with the algorithm from [18] that $\langle 1, \frac{1}{2}\mathrm{Tr}_{A_4}\rangle_G^p$, which does not come from a ring of integers, is free over $\langle 1, \frac{1}{2}\mathrm{Tr}_G\rangle_G^p$ (see Section A.3).*

Acknowledgments. This work is part of the author's PhD thesis at the University of Exeter. The author wishes to thank his PhD supervisor, Henri Johnston, for his encouragement and valuable comments, Nigel Byott and Christian Wuthrich for helpful comments and discussions, and Werner Bley and Tommy Hofmann for their help with the computer calculations in Appendix A. Finally, the author is grateful to the anonymous referee for a number of helpful comments, which led to an improved exposition.

The author is grateful to the University of Exeter for funding his PhD scholarship; he was subsequently supported by an LMS Early Career Fellowship and then by EPSRC grant EP/W52265X/1.

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

Data availability statement. Data sharing is not applicable to this article, as no datasets were generated or analysed during the present work.

References

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symb. Comput.* **24**(3-4) (1997), 235–265. Computational algebra and number theory (London, 1993). MR 1484478.

[2] A.-M. Bergé, Sur l'arithmétique d'une extension diédrale, *Ann. Inst. Fourier (Grenoble)* **22**(2) (1972), 31–59. MR 0371857.

[3] A.-M. Bergé, Arithmétique d'une extension galoisienne à groupe d'inertie cyclique, *Ann. Inst. Fourier (Grenoble)* **28**(4) (1978), 17–44, ix. MR 513880.

[4] A.-M. Bergé, Projectivite des anneaux d'entiers sur leurs ordres associes, *Astérisque* **61** (1979), 15–28 (French).

[5] W. Bley and H. Johnston, Computing generators of free modules over orders in group algebras, *J. Algebra* **320**(2) (2008), 836–852. MR 2422318.

[6] W. Bley and H. Johnston, Computing generators of free modules over orders in group algebras II, *Math. Comput.* **80**(276) (2011), 2411–2434. MR 2813368.

[7] W. Bley and S. M. J. Wilson, Computations in relative algebraic K-groups, *LMS J. Comput. Math.* **12** (2009), 166–194. MR 2564571.

[8] R. J. Chapman, A simple proof of Noether's theorem, *Glasgow Math. J.* **38**(1) (1996), 49–51. MR 1373957.

[9] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*, Pure and Applied Mathematics (John Wiley & Sons Inc., New York, 1981). With applications to finite groups and orders, A Wiley-Interscience Publication. MR 632548 (82i:20001).

[10] C. W. Curtis and I. Reiners, *Methods of representation theory. Vol. II*, Pure and Applied Mathematics (John Wiley & Sons Inc., New York, 1987). With applications to finite groups and orders, A Wiley-Interscience Publication. MR 892316 (88f:20002).

[11] T. Dokchitser, *Group names*. 2018. https://people.maths.bris.ac.uk/~matyd/GroupNames/

[12] S. Endô and Y. Hironaka, Finite groups with trivial class groups, *J. Math. Soc. Jpn.* **31**(1) (1979), 161–174. MR 519042.

[13] A. Fröhlich, M. E. Keating and S. M. J. Wilson, The class groups of quaternion and dihedral 2-groups, *Mathematika* **21** (1974), 64–71. MR 360531.

[14] A. Fröhlich, Artin root numbers and normal integral bases for quaternion fields, *Invent. Math.* **17** (1972), 143–166. MR 323759.

[15] A. Fröhlich, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. **1** (Springer-Verlag, Berlin, 1983). MR 717033.

[16] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. **27** (Cambridge University Press, Cambridge, 1993). MR 1215934.

[17] A. Hattori, *Rank element of a projective module*, *Nagoya Math. J.* **25** (1965), 113–120. MR 0175950.

[18] T. Hofmann and H. Johnston, *Computing isomorphisms between lattices*, math 2020, **no. 326**, Comp. **89**, 2931–2963.MR 4136552.

[19] H. Jacobinski, Genera and decompositions of lattices over orders, *Acta Math.* **121** (1968), 1–29. MR 251063.

[20] J.-F. Jaulent, *Sur la l-structure galoisienne des idéaux ambiges dans une extension métacyclique de degré nl sur le corps des rationnels*, Number Theory, 1979-1980 and 1980-1981, Publ. Math. Fac. Sci. Besançon (Univ. Franche-Comté, Besançon, 1981). Exp. No. 3, 20. MR 748000.

[21] H. Johnston and A. Nickel, On the equivariant Tamagawa number conjecture for Tate motives and unconditional annihilation results, *Trans. Am. Math. Soc.* **368**(9) (2016), 6539–6574. MR 3461042.

[22] H. Johnston and A. Nickel, Hybrid Iwasawa algebras and the equivariant Iwasawa main conjecture, *Am. J. Math.* **140**(1) (2018), 245–276. MR 3749195.

[23] H. Johnston, Explicit integral Galois module structure of weakly ramified extensions of local fields, *Proc. Am. Math. Soc.* **143**(12) (2015), 5059–5071. MR 3411126.

[24] J. W. Jones and D. P. Roberts, A database of local fields, *J. Symb. Comput.* **41**(1) (2006), 80–97. MR 2194887.

[25] F. Kawamoto, On normal integral bases of local fields, *J. Algebra* **98**(1) (1986), 197–199. MR 825142.

[26] M. E. Keating, Class groups of metacyclic groups of order $p^r q$, p a regular prime, *Mathematika* **21** (1974), 90–95. MR 0357591.

[27] H.-W. Leopoldt, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, *J. Reine Angew. Math.* **201** (1959), 119–149. MR 0108479.

[28] G. Lettl, The ring of integers of an abelian number field, *J. Reine Angew. Math.* **404** (1990), 162–170. MR 1037435.

[29] G. Lettl, Relative Galois module structure of integers of local abelian fields, *Acta Arith.* **85**(3) (1998), 235–248. MR 1627831.

[30] The LMFDB Collaboration, *The L-functions and modular forms database*. 2019. Available at http://www.lmfdb.org (accessed 30 October 2019).

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

[31] J. Martinet, Modules sur l'algèbre du groupe quaternionien, *Ann. Sci. École Norm. Sup. (4)* **4** (1971), 399–408. MR 0291208.

[32] J. Martinet and C. R. Acad Sci, Sur les extensions à groupe de Galois quaternionien, *C. R. Acad. Sci. Paris Sér. A-B* **274** (1972), A933–A935. MR 299593.

[33] J. C. Miller, Class numbers of real cyclotomic fields of composite conductor, *LMS J. Comput. Math.* **17**(suppl. A) (2014), 404–417. MR 3240817.

[34] E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, *J. Reine Angew. Math.* **167** (1932), 147–152. MR 1581331.

[35] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. **28** (The Clarendon Press, Oxford University Press, Oxford, 2003). Corrected reprint of the 1975 original, With a foreword by M. J. Taylor. MR 1972204

[36] K. W. Roggenkamp, *Lattices over orders. II*, Lecture Notes in Mathematics, vol. **142** (Springer-Verlag, Berlin/New York, 1970). MR 0283014.

[37] I. Reiner and S. Ullom, *Remarks on class groups of integral group rings*, Symposia Mathematica, Vol. XIII (Convegno di Gruppi e loro Rappresentazioni, INDAM, Rome, 1972) (1974), 501–516. MR 0367043.

[38] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. **67** (Springer-Verlag, New York/Berlin, 1979). Translated from the French by Marvin Jay Greenberg. MR 554237.

[39] M. J. Taylor, On Fröhlich's conjecture for rings of integers of tame extensions, *Invent. Math.* **63**(1) (1981), 41–79. MR 608528.

[40] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. **83**, 2nd edition (Springer-Verlag, New York, 1997). MR 1421575.

Appendix A: Computer calculations

A.1. Determining freeness for S_4-extensions of $\mathbb{Q}_2$

Let $K/\mathbb{Q}$ be an S_4-extension with full decomposition group that is wildly ramified. Here we describe how to use the Magma implementation of [5, Algorithm 3.1(6)] to check whether or not $\mathcal{O}_K$ is locally free at 2 over $\mathfrak{A}_{K/\mathbb{Q}}$, or equivalently, whether $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$, where $\mathfrak{P}$ is the unique prime of K above 2. We used the database [30] to find six number fields, each of which has a completion at 2 equal to one of the six wildly ramified S_4-extensions of $\mathbb{Q}_2$ listed in the database of p-adic fields [24]. Note that two of these extensions of $\mathbb{Q}_2$ are weakly ramified, and so Corollary 7.2(ii) already shows that $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ in both cases, but we include them anyway as an additional check. The files `RelAlgKTheory.m` and `INB.m` referred to below are available on Werner Bley's website `https://www.mathematik.uni-muenchen.de/~bley/pub.php`

We refer to the sample file `sample.m` from the article [5]. Note that here we use the updated file `INB.m` from [6] rather than the original file `ao.m`.

```
Attach("RelAlgKTheory.m");
Attach("INB.m");
P <x> := PolynomialRing(IntegerRing());
Polynomials := [ x^6 + x^4 + x^2 - 1,
x^6 - x^4 + 3*x^2 - 1,
x^6 + 3*x^4 + 11*x^2 + 11,
x^6 + 7*x^4 + 15*x^2 + 11,
x^6 - x^4 - 2*x^3 - x^2 + 1,
x^6 - 2*x^5 + 2*x^4 - 4*x^3 + 4*x^2 - 2*x + 2 ];
for i in [1..6] do
  L := NormalClosure(NumberField(Polynomials[i]));
  G, Aut, h := AutomorphismGroup(L);
  h := map <Domain(h)-> Codomain(h) | g:-> h(g^-1)> ;
  OL := MaximalOrder(L);
  theta := NormalBasisElement(OL, h);
  Ath := ComputeAtheta(OL, h, theta);
  QG := GroupAlgebra(Rationals(), G);
```

https://doi.org/10.1017/S0017089523000460 Published online by Cambridge University Press

```
  AssOrd := ModuleConductor(QG, Ath, Ath);
  rho := RegularRep(QG);
  M := ZGModuleInit(Ath`hnf, rho);
  isfree, w := IsLocallyFree(QG, AssOrd, M, 2);
  if isfree then
   print "we have local freeness at 2";
  else
   print "we do not have local freeness at 2";
  end if;
end for;
we do not have local freeness at 2
we do not have local freeness at 2
we do not have local freeness at 2
we do not have local freeness at 2
we have local freeness at 2
we have local freeness at 2
```

A.2. Determining local freeness at 2 for S_4-extensions of $\mathbb{Q}$

Here we describe how to use the Magma implementation of [18, §8.5] to show that for an S_4-extension $K/\mathbb{Q}$ we have that $\mathcal{O}_K$ is not locally free at 2 over $\mathfrak{A}_{K/\mathbb{Q}}$ if $K/\mathbb{Q}$ does not satisfy any of the conditions (i)–(iv) of Theorem 8.3 and $\mathcal{O}_{K_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$, where $\mathfrak{P}$ is a prime of K above 2 (see Table 1). Moreover, we also prove the freeness claim of Remark 8.5. The files `Iso.m`, `Lattices.m` and `Iso.spec` referred to below are contained in `Iso.zip`, available in the link to [18] on Tommy Hofmann's website `https://www.thofma.com`

```
AttachSpec("Iso.spec");
G := Sym(4);
W2 := sub <G | G!(1, 3)> ;
V2 := sub <G | G!(1, 3)(2, 4)> ;
C4 := sub <G | G!(1, 2, 3, 4)> ;
V4 := sub <G | G!(1, 3)(2, 4),(1, 2)(3, 4)> ;
C22 := sub <G | G!(1, 3),(2, 4)> ;
D8 := sub <G | G!(1, 2, 3, 4),(1, 3)> ;
QG := GroupAlgebra(Rationals(), G);
trW2 := &+[ QG!h : h in W2];
trV2 :=&+[ QG!h : h in V2];
trC4 := &+[ QG!h : h in C4];
trV4 := &+[ QG!h : h in V4];
trC22 := &+[ QG!h : h in C22];
trD8 := &+[ QG!h : h in D8];
trG := &+[ QG!h : h in G];
ZG := Order(Integers(), Basis(QG));
M1 := rideal < ZG | 1, trV2/2, trC4/4,trD8/8> ;
A1 := rideal < ZG | 1, trV4/2, trG/8> ;
IsLocallyIsomorphic(QG, BasisMatrix(M1), BasisMatrix(A1), 2);
false
M2 := rideal < ZG | 1, trV2/2, trV4/4,trD8/8> ;
A2 := rideal < ZG | 1, trV4/4, trG/8> ;
IsLocallyIsomorphic(QG, BasisMatrix(M2), BasisMatrix(A2), 2);
false
```

```
M3 := rideal < ZG | 1, trV2/2, trC22/4,trD8/8> ;
IsLocallyIsomorphic(QG, BasisMatrix(M3), BasisMatrix(A1), 2);
false
M4 := rideal < ZG | 1, trV2/2, trC4/4> ;
A4 := rideal < ZG | 1, trV4/2, trG/4> ;
IsLocallyIsomorphic(QG, BasisMatrix(M4), BasisMatrix(A4), 2);
false
M5 := rideal < ZG | 1, trV2/2, trV4/4> ;
A5 := rideal < ZG | 1, trV4/4> ;
IsLocallyIsomorphic(QG, BasisMatrix(M5), BasisMatrix(A5), 2);
false
M6 := rideal < ZG | 1, trV2/2, trC22/4> ;
IsLocallyIsomorphic(QG, BasisMatrix(M6), BasisMatrix(A4), 2);
false
M7 := rideal < ZG | 1, trW2/2, trC22/4> ;
A7 := rideal < ZG | 1, trG/4> ;
IsLocallyIsomorphic(QG, BasisMatrix(M7), BasisMatrix(A7), 2);
false
M8 := rideal < ZG | 1, trC22/2> ;
A8 := rideal < ZG | 1, trG/2> ;
IsLocallyIsomorphic(QG, BasisMatrix(M8), BasisMatrix(A8), 2);
false
M9 := rideal < ZG | 1, trV2/2> ;
A9 := rideal < ZG | 1, trV4/2> ;
IsLocallyIsomorphic(QG, BasisMatrix(M9), BasisMatrix(A9), 2);
false
M10 := rideal < ZG | 1, trW2/2> ;
IsLocallyIsomorphic(QG, BasisMatrix(M10), BasisMatrix(A8), 2);
false
M11 := rideal < ZG | 1, trV4/4, trD8/8> ;
A11 := rideal < ZG | 1, trV4/4, trG/8> ;
IsLocallyIsomorphic(QG, BasisMatrix(M11), BasisMatrix(A11), 2);
true -31/4*Id(G) + (1, 4, 3, 2) + 5/4*(1, 3)(2, 4) - 5*(2, 3)
+ 5/4*(1, 2, 4) + 1/4*(1, 4, 3)+ (1, 3, 4, 2) + (2, 4, 3)+ (1, 4, 2, 3)
+ (1, 2, 3) + 5/4*(2, 3, 4) + 1/4*(1, 3, 2) + (2, 4) + 5/4*(1, 2)(3, 4)
+ 1/4*(1, 4)(2, 3)
```

A.3. Determining local freeness for A_5-extensions of $\mathbb{Q}$

Here we describe how to use the Magma implementation of [18, §8.5] to check local freeness in A_5-extensions of $\mathbb{Q}$ at the wildly ramified primes (see Tables 2 and 3). Moreover, we also prove the second freeness claim of Remark 8.8. The files `Iso.m`, `Lattices.m` and `Iso.spec` referred to below are contained in `Iso.zip`, available in the link to [18] on Tommy Hofmann's website `https://www.thofma.com`

When `IsLocallyIsomorphic(QG, BasisMatrix(M), BasisMatrix(A), 2)` is 'true', we suppress the full output, which includes an element $x \in \mathbb{Q}[G]$ such that $x(\mathbb{Z}_2 \otimes_{\mathbb{Z}} M) = \mathbb{Z}_2 \otimes_{\mathbb{Z}} A$ (whose existence is in our case equivalent to $\mathbb{Z}_2 \otimes_{\mathbb{Z}} M$ being free over $\mathbb{Z}_2 \otimes_{\mathbb{Z}} A$).

```
AttachSpec("Iso.spec");
G:=Alt(5);
C2 := sub <G | G!(1, 2)(3, 4)> ;
C22 := sub <G | G!(1, 2)(3, 4),(1, 3)(2, 4)> ;
```

```
C3 := sub <G | G!(1, 2, 3)> ;
D6 := sub <G | G!(1, 2)(4, 5),(1, 2, 3)> ;
C5 := sub <G | G!(1, 2, 3, 4, 5)> ;
D10 := sub <G | G!(2,5)(3, 4),(1, 2, 3, 4, 5)> ;
Alt4 := sub <G | G!(1,2)(3, 4),(1, 2, 3)> ;
QG := GroupAlgebra(Rationals(), G);
trC2 := &+[ QG!h : h in C2];
trC22 := &+[ QG!h : h in C22];
trC3 := &+[ QG!h : h in C3];
trD6 := &+[ QG!h : h in D6];
trC5 := &+[ QG!h : h in C5];
trD10 := &+[ QG!h : h in D10];
trAlt4 := &+[ QG!h : h in Alt4];
trG := &+[ QG!h : h in G];
ZG := Order(Integers(), Basis(QG));
M1 := rideal < ZG | 1, trC2/2> ;
A1 := rideal < ZG | 1, trG/2> ;
IsLocallyIsomorphic(QG, BasisMatrix(M1), BasisMatrix(A1), 2);
false
M2 := rideal < ZG | 1, trC2/2, trC22/4> ;
A2 := rideal < ZG | 1, trG/4> ;
IsLocallyIsomorphic(QG, BasisMatrix(M2), BasisMatrix(A2), 2);
false
M3 := rideal < ZG | 1, trC22/2> ;
IsLocallyIsomorphic(QG, BasisMatrix(M3), BasisMatrix(A1), 2);
false
M4 := rideal < ZG | 1, trC3/3> ;
A4 := rideal < ZG | 1, trG/3> ;
IsLocallyIsomorphic(QG, BasisMatrix(M4), BasisMatrix(A4), 3);
false
M5 := rideal < ZG | 1, trD6/3> ;
IsLocallyIsomorphic(QG, BasisMatrix(M5), BasisMatrix(A4), 3);
true
M6 := rideal < ZG | 1, trC5/5> ;
A6 := rideal < ZG | 1, trG/5> ;
IsLocallyIsomorphic(QG, BasisMatrix(M6), BasisMatrix(A6), 5);
false
M7 := rideal < ZG | 1, trD10/5> ;
IsLocallyIsomorphic(QG, BasisMatrix(M7), BasisMatrix(A6), 5);
true
M8 := rideal < ZG | 1, trAlt4/2> ;
IsLocallyIsomorphic(QG, BasisMatrix(M8), BasisMatrix(A1), 2);
true
```