LEOPOLDT-TYPE THEOREMS FOR NON-ABELIAN EXTENSIONS OF $\mathbb{Q}$

FABIO FERRI

Abstract. We prove new results concerning the additive Galois module structure of certain wildly ramified finite non-abelian extensions of $\mathbb{Q}$. 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 $G = \text{Gal}(K/F)$. 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. [Leo59] 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 [Let90] gave a simplified and more explicit proof of the same result. We also have the following result of Bergé.

Theorem 1.2. [Ber72] 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 $\text{Gal}(K/\mathbb{Q}) \cong Q_8$, the quaternion group of order 8. Suppose that $K/\mathbb{Q}$ is tamely ramified. Martinet [Mar71] gave two examples of such extensions without and one with a normal integral basis. Moreover, Fröhlich [Fro72] 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. [Mar72] Let $K/\mathbb{Q}$ be a wildly ramified Galois extension with $\text{Gal}(K/\mathbb{Q}) \cong Q_8$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$.

Date: version of 8th April 2022.
In the present article, we prove other Leopoldt-type theorems for certain 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 \( G = \text{Gal}(K/\mathbb{Q}) \). We recall that \( \mathcal{O}_K \) is said to be locally free over \( \mathfrak{A}_{K/\mathbb{Q}} \) at a rational prime \( p \) if \( \mathcal{O}_{K,p} := \mathbb{Z}_p \otimes \mathcal{O}_K \) is free as an \( \mathfrak{A}_{K/\mathbb{Q},p} := \mathbb{Z}_p \otimes \mathfrak{A}_{K/\mathbb{Q}} \)-module. We say that \( \mathcal{O}_K \) is locally free over \( \mathfrak{A}_{K/\mathbb{Q}} \) if this holds for all rational primes \( p \).

Suppose that \( K/\mathbb{Q} \) is tamely ramified. Then \( \mathcal{O}_K \) is locally free over \( \mathbb{Z}[G] \). Moreover, the problem of determining whether \( K/\mathbb{Q} \) has a normal integral basis is well understood thanks to Taylor’s proof of Fröhlich’s conjecture \([\text{Tay}81]\): he determined the class of \( \mathcal{O}_K \) in the locally free class group \( \text{Cl}(\mathbb{Z}[G]) \) in terms of Artin root numbers of the irreducible symplectic characters of \( G \) (see \([\text{Frö}83, \text{I}]\) 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.

If \( K/\mathbb{Q} \) is wildly ramified, then the situation becomes much more difficult, not least because \( \mathcal{O}_K \) need not even be locally free over \( \mathfrak{A}_{K/\mathbb{Q}} \). For instance, Bergé \([\text{Ber}79]\) gave examples of wildly ramified dihedral extensions of \( \mathbb{Q} \) without the local freeness property.

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 \( 2\ell \) for some prime \( \ell \) (see \([3.1]\) 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. More precisely, if \( K/\mathbb{Q} \) is wildly ramified and non-abelian, \( p \) is a rational prime, \( \mathfrak{P} \) a prime of \( K \) above \( p \), and \( \mathcal{O}_{K,\mathfrak{P}} \) is free over \( \mathfrak{A}_{K,\mathfrak{P}/\mathbb{Q}_p} \), then it is not necessarily the case that \( \mathcal{O}_K \) is locally free over \( \mathfrak{A}_{K/\mathbb{Q}} \) at \( p \) (here \( K_\mathfrak{P} \) denotes the completion of \( K \) at \( \mathfrak{P} \)). This is an important obstacle that needs to be overcome in the proofs of the main results of the present article.

We consider the question of whether \( \mathcal{O}_K \) is free over \( \mathfrak{A}_{K/\mathbb{Q}} \) in the case that the locally free class group \( \text{Cl}(\mathbb{Z}[G]) \) is trivial and \( \mathbb{Z}[G] \) has the so-called locally free cancellation property (in fact, the latter condition holds whenever the former holds). In this situation, it is also the case that \( \text{Cl}(\mathfrak{A}_{K/\mathbb{Q}}) \) is trivial and \( \mathfrak{A}_{K/\mathbb{Q}} \) has the locally free cancellation property. Hence it is straightforward to show that the question reduces to whether \( \mathcal{O}_K \) is locally free over \( \mathfrak{A}_{K/\mathbb{Q}} \).

We now briefly describe a straightforward application of this strategy. Suppose that \( G \) is dihedral of order \( 2p^n \) for some prime \( p \) and some positive integer \( n \). In this situation, Keating \([\text{Kea}74]\) gave sufficient conditions for \( \text{Cl}(\mathbb{Z}[G]) \) to be trivial and Bergé \([\text{Ber}79]\) gave necessary and sufficient conditions for \( \mathcal{O}_K \) to be locally free over \( \mathfrak{A}_{K/\mathbb{Q}} \). As a consequence we obtain the following result.

**Theorem 1.4.** 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 \( K/\mathbb{Q} \) is a power of \( p \).

Here \( \mathbb{Q}(\zeta_{p^n})^+ \) denotes the maximal totally real subfield \( \mathbb{Q}(\zeta_{p^n}) \). Using the class number computations of Miller \([\text{Mil}14]\) we obtain the following corollary.

**Corollary 1.5.** 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 \( K/\mathbb{Q} \) is a power of \( p \).

Similar but more complicated results hold when \( p = 2 \) or 3 (see \([5]\)).
LEOPOLDT-TYPE THEOREMS FOR NON-ABELIAN EXTENSIONS OF $\mathbb{Q}$

If $G$ is non-abelian and non-dihedral such that $\text{Cl}(\mathbb{Z}[G])$ is trivial, then a result of Endô and Hironaka [EH79] shows that $G$ is isomorphic to $A_4$, $S_4$ or $A_5$; the converse was already shown by Reiner and Ullom [RU73]. The main results of the present article will be necessary and sufficient conditions for $\mathcal{O}_K$ to be free over $\mathfrak{A}_{K/Q}$ 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 $\mathfrak{A}_{K/Q}$. A key ingredient is the notion of hybrid $p$-adic group rings, introduced by Johnston and Nickel [JN16]; using this tool it is straightforward to show that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/Q}$ 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 rational prime is tamely ramified will mean that some, and hence every, prime of $K$ above $p$ is (at most) tamely ramified in $K/Q$. We shall henceforth abbreviate ‘at most tamely ramified’ to ‘tamely ramified’.

**Theorem 1.6.** Let $K/Q$ be a Galois extension with $\text{Gal}(K/Q) \cong A_4$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/Q}$ 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 $\mathfrak{A}_{K/Q}$ at $p = 2$. This reduces to showing that the lattice $\text{Ind}_D^G \mathfrak{A}_{K_2/Q_2} := \mathbb{Z}_2[G] \otimes_{\mathbb{Z}_2[D]} \mathfrak{A}_{K_2/Q_2}$ is not free over $\mathfrak{A}_{K_2/Q_2}$, where $\mathfrak{p}$ is a fixed prime above 2 and $D$ is its decomposition group. The main theorem used here is Hattori’s result [Hat65] that commutative orders are ‘clean’ (see §6.2).

**Theorem 1.7.** Let $K/Q$ be a Galois extension with $G := \text{Gal}(K/Q) \cong S_4$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/Q}$ if and only if one of the following conditions on $K/Q$ holds:

1. 2 is tamely ramified;
2. 2 has decomposition group equal to the unique subgroup of $G$ of order 12;
3. 2 is wildly and weakly ramified and has full decomposition group; or
4. 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 1.8.** Let $K/Q$ be a Galois extension with $\text{Gal}(K/Q) \cong A_5$. Then $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/Q}$ if and only if all three of the following conditions on $K/Q$ hold:

1. 2 is tamely ramified;
2. 3 is tamely ramified or is weakly ramified with ramification index 6; and
3. 5 is tamely ramified or is weakly ramified with ramification index 10.

In contrast to the proof of Theorem 1.6, the proofs of Theorems 1.7 and 1.8 use the (updated) implementation in MAGMA [BCP97] of the algorithms developed by Bley and Johnston [BJ08] and by Hofmann and Johnston [HJ20].

**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 for helpful discussions, and Werner Bley and Tommy Hofmann for their help with the computer calculations in Appendix A. The author is grateful to the University of Exeter for funding his PhD scholarship.

**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 $O_K$. 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 $ncl_G(H)$ 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 $G$.

2. Associated orders and reduction to the study of local freeness

2.1. Lattices and orders. For further background, we refer the reader to [Rei03] or [CR81]. 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 $\Lambda$ of $A$ (so in particular has the same unity element as $A$) such that $\Lambda$ is a full $R$-lattice in $A$. A $\Lambda$-lattice is a $\Lambda$-module which is also an $R$-module. For any $\Lambda$-module $M$ and $N$, a homomorphism of $\Lambda$-modules $f : M \to N$ is called a homomorphism of $\Lambda$-lattices.

The following well-known lemma follows from [CR81, Exercise 23.2].

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

2.2. Associated orders. Let $\Lambda$ 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 [Rei03 §8]). In particular, it is the largest order $\Lambda$ over which $M$ has a structure of $\Lambda$-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 $\Lambda$ be an $R$-order in $A$ and let $M$ be a free $\Lambda$-lattice of rank 1. Then $FM$ is a free $A$-module of rank 1 and $\Lambda = \mathfrak{A}(A, M)$.

Proof. By hypothesis there exists $\alpha \in M$ such that $M = \Lambda \alpha$ is a free $\Lambda$-module. Thus $FM = \Lambda \alpha$ 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 $\alpha$, 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 $\Lambda$ 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 \( p \) be any maximal ideal of \( R \). Let \( F_p \) denote the completion of \( F \) with respect to a valuation defined by \( p \) and let \( R_p \) be the corresponding valuation ring. For any \( R \)-module \( M \) we write \( M_p \) for \( R_p \otimes_R M \) and \( V_p = F_p \otimes_F V \) for any \( F \)-vector space \( V \). These two notations are consistent as the map \( \lambda \otimes_{O_p} v \mapsto \lambda \otimes_F v \) \((v \in V, \lambda \in O_{R_p})\) is an isomorphism (see [FT93, p. 93]).

Let \( \Lambda \) be an \( R \)-order and let \( M \) be a \( \Lambda \)-lattice in some \( A \)-module \( V \). Then \( \Lambda_p \) is an \( R_p \)-order in \( A_p \) and \( M_p \) is a \( \Lambda_p \)-lattice in \( V_p \). We say that \( M \) is locally free over \( \Lambda \) if \( M_p \) is free over \( \Lambda_p \) for every \( p \).

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 \( R_p[G] \subseteq \mathfrak{A}(F_p[G], M_p) \). Moreover, \( M \) is locally free over \( \mathfrak{A}(F[G], M) \) if \( M_p \) is free over \( \mathfrak{A}(F_p[G], M_p) \) for every \( p \).

2.4. Associated orders of rings of integers. Let \( K/F \) be a finite Galois extension of number fields and let \( G = \text{Gal}(K/F) \). We consider the behaviour of the associated order \( \mathfrak{A}_{K/F} := \mathfrak{A}(F[G], O_K) \) with respect to localisation and induction.

Let \( p \) be a maximal ideal of \( O_F \). Then we have decompositions

\[
K_p := F_p \otimes_F K \cong \prod_{\mathfrak{P} \mid p} K_{\mathfrak{P}} \quad \text{and} \quad O_{K_p} := O_{F_p} \otimes_{O_F} O_K \cong \prod_{\mathfrak{P} \mid p} O_{K_{\mathfrak{P}}},
\]

where \( \{ \mathfrak{P} \mid p \} \) consists of the primes of \( O_K \) above \( p \) (see [FT93, p. 109]). Fix a prime \( \mathfrak{P} \) above \( p \) and let \( D \) be its decomposition group in \( G \). Then as \( G \) acts transitively on \( \{ \mathfrak{P} \mid p \} \) we have

\[
K_p \cong \prod_{s \in G/D} sK_{\mathfrak{P}} \quad \text{and} \quad O_{K_p} \cong \prod_{s \in G/D} sO_{K_{\mathfrak{P}}},
\]

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

\[
O_{K_p} \cong \text{Ind}_D^G O_{K_{\mathfrak{P}}} := O_{F_p}[G] \otimes_{O_{F_p}[D]} O_{K_{\mathfrak{P}}},
\]

and

\[
\mathfrak{A}_{K/F_p} = \mathfrak{A}(F[G], O_K)_p \cong \mathfrak{A}(F_p[G], \text{Ind}_D^G O_{K_{\mathfrak{P}}}),
\]

where the last isomorphism follows from [CR81, Exercise 24.2], for instance. Thus \( O_K \) is locally free over \( \mathfrak{A}_{K/F} \) at \( p \) if and only if \( \text{Ind}_D^G O_{K_{\mathfrak{P}}} \) is free over \( \mathfrak{A}(F_p[G], \text{Ind}_D^G O_{K_{\mathfrak{P}}}) \).

In §6 we will consider the relationship between \( \mathfrak{A}(F_p[G], \text{Ind}_D^G O_{K_{\mathfrak{P}}}) \) and \( \text{Ind}_D^G \mathfrak{A}_{K/F_p} \), as well as conditions under which the implication ‘if \( O_{K_{\mathfrak{P}}} \) is free over \( \mathfrak{A}_{K_{\mathfrak{P}}/F_p} \) then \( O_K \) is locally free over \( \mathfrak{A}_{K/F} \) at \( p \)’ holds.

**Notation.** We henceforth consider the isomorphism \( \mathfrak{A}_{K/F_p} \cong \mathfrak{A}(F_p[G], O_{K_p}) \) as an identification. In particular, we consider \( \mathfrak{A}_{K/F_p} \) as an \( O_{F_p} \)-order in \( F_p[G] \).

2.5. Reduction to the study of local freeness. For a \( \mathbb{Z} \)-order \( \Lambda \) let \( \text{Cl}(\Lambda) \) denote the locally free class group of \( \Lambda \) as defined in [CR87, (39.12)]; further background material can be found in [CR87, §49]. The following proposition underpins the proofs of all the new theorems stated in the introduction.

**Proposition 2.4.** Let \( G \) be a finite group such that \( \text{Cl}(\mathbb{Z}[G]) \) is trivial and let \( K/\mathbb{Q} \) be a Galois extension with \( \text{Gal}(K/\mathbb{Q}) \cong G \). Then \( O_K \) is free over \( \mathfrak{A}_{K/\mathbb{Q}} \) if and only if \( O_K \) is locally free over \( \mathfrak{A}_{K/\mathbb{Q}} \).

**Proof.** One implication is trivial. By [CR87, (49.25)] the inclusion \( \mathbb{Z}[G] \subseteq \mathfrak{A}_{K/\mathbb{Q}} \) induces a surjection \( \text{Cl}(\mathbb{Z}[G]) \twoheadrightarrow \text{Cl}(\mathfrak{A}_{K/\mathbb{Q}}) \), and so \( \text{Cl}(\mathfrak{A}_{K/\mathbb{Q}}) \) is also trivial. Moreover, by [EH79] the triviality of \( \text{Cl}(\mathbb{Z}[G]) \) implies that \( G \) must be abelian, dihedral, or isomorphic to \( A_4, S_4 \) or
A_5 (also see [CR87 (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 [CR87 (51.2)] \( \mathbb{Q}[G] \) satisfies the Eichler condition (see [CR87 (45.4) or §51A]). Thus the Jacobinski cancellation theorem [Jac84] (also see [CR87 (51.24)]) implies that \( \mathfrak{A}_{K/Q} \) has the locally free cancellation property. The non-trivial implication now follows easily. 

\[ \square \]

**Corollary 2.5.** Let \( K/Q \) be a Galois extension with \( \text{Gal}(K/Q) \cong A_5, S_4 \) or \( A_5 \). Then \( \mathcal{O}_K \) is free over \( \mathfrak{A}_{K/Q} \) if and only if \( \mathcal{O}_K \) is locally free over \( \mathfrak{A}_{K/Q} \).

**Proof.** Let \( G = \text{Gal}(K/Q) \). In each case \( \text{Cl}(\mathbb{Z}[G]) \) is trivial, as shown in [RU74]. \( \square \)

3. **Review of results relating to local freeness**

### 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 \( G = \text{Gal}(K/F) \). 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 [Noe32]. In fact, as noted in [Cha96], she only stated and proved the result in the case that \( p \mid |G| \). Complete proofs can be found in [Fr¨ o83], [Kaw86] and [Cha96].

**Theorem 3.3.** Let \( K/F \) be an extension of \( p \)-adic fields such that \( K/Q_p \) is a finite abelian extension. Then \( \mathcal{O}_K \) is free over \( \mathfrak{A}_{K/F} \).

**Theorem 3.4.** Let \( K/Q_p \) be a Galois extension with \( \text{Gal}(K/Q_p) \cong D_{2\ell} \), where \( \ell \) is a prime number. Then \( \mathcal{O}_K \) is free over \( \mathfrak{A}_{K/Q_p} \).

**Theorem 3.5.** Let \( K/Q_p \) be a Galois extension with \( \text{Gal}(K/Q_p) \cong Q_8 \). Then \( \mathcal{O}_K \) is free over \( \mathfrak{A}_{K/Q_p} \).

**Remark 3.6.** Theorem 3.5 is not explicitly stated in [Mar72]. However, the proof of Theorem 3.1 given in loc. cit. also works essentially unchanged in the setting of Theorem 3.5. Alternatively, note that Theorem 3.5 is implied by Theorem 3.1 because for every \( Q_8 \)-extension \( L/Q \) there exists a \( Q_8 \)-extension \( K/Q \) such that \( K_p = L \), where \( p \) is the unique prime of \( K \) above 2; this can be checked using databases of \( p \)-adic and number fields such as [JR06] and [LMF19]. Note that unlike Theorem 3.1 it is not necessary to assume that the extension in question is wildly ramified, thanks to Theorem 3.1.

**Theorem 3.7.** Let \( p, n \) and \( r \) be positive integers such that \( p \) is an odd prime, \( n \) divides \( p - 1 \) and \( r \) is a primitive \( n \)th root modulo \( p \). Let \( G \) be the metacyclic group with the following structure:

\[
G = \langle x, y : x^p = 1, y^n = 1, xy^{-1} = x^r \rangle \cong C_p \rtimes C_n.
\]

Let \( K/Q_p \) be a Galois extension with \( \text{Gal}(K/Q_p) \cong G \). Then \( \mathcal{O}_K \) is free over \( \mathfrak{A}_{K/Q_p} \).

**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 \( G = \text{Gal}(K/F) \). We recall that for an integer \( t \geq -1 \) the \( t \)-th 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 normalized 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.** [Joh15] Let $K/F$ be a weakly ramified finite Galois extension of $p$-adic fields and let $G = \text{Gal}(K/F)$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{K/F}$. Moreover, if $K/F$ is both wildly and weakly ramified then $\mathfrak{A}_{K/F} = \mathcal{O}_K[[\pi_K^{-1}\text{Tr}_{G_0}]]$, where $\pi_K$ is a uniformiser of $\mathcal{O}_K$ and $\text{Tr}_{G_0} = \sum_{\gamma \in G_0} \gamma$ is the sum of the elements of the inertia group $G_0$.

For a subgroup $H$ of $G$ define $\text{Tr}_H = \sum_{h \in H} h \in F[G]$ and $e_H = \frac{1}{|H|} \text{Tr}_H \in F[G]$. Note that $e_H$ is an idempotent. We say that the extension is weakly ramified if $e_H$ is unramified. Let $K/F$, $O_K$ be a finite Galois extension of number fields. Then $O_K$ is free over $A_{K/F}$ if and only if $O_K$ is free over $A_{K/F}$ if and only if either

(i) $K/F$ is almost-maximally ramified, in which case $A_{K/F} = O_F[G][\{e_G\}_{G \geq 1}]$, or

(ii) $K/F$ is not almost-maximally ramified, and the inertia subgroup $G_0$ is dihedral of order $2p$, in which case $A_{K/F} = O_F[G][2e_{G_0}]$.

**Remark 3.11.** Let $H$ be a subgroup of $G$ and let $r$ be a positive integer. We now show how to determine whether $\frac{1}{r}\text{Tr}_H \in A_{K/F}$. 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 $\mathcal{O}_{K/M}$ the different of the extension $K/M$ (see [Ser79, III Proposition 7]) and by $v_p(x)$ the $p$-adic valuation of an integer $x$ (thus $v_p$ is the restriction of $v_{Q_p}$ to $Z$).

$$\frac{1}{r}\text{Tr}_H \in A_{K/F} \iff \frac{1}{r}\text{Tr}_{K/M}(O_K) \subseteq O_M$$

$$\iff \text{Tr}_{K/M}(O_K) \subseteq rO_M$$

$$\iff O_K \subseteq rO_M \mathcal{O}_{K/M}^{-1} \text{ by [Ser79, III Proposition 7]}$$

$$\iff O_{K/M} \subseteq rO_K$$

$$\iff v_K(O_{K/M}) \geq e(K/Q_p)v_p(r)$$

$$\iff \sum_{i=0}^{\infty} (|G_i(K/M)| - 1) \geq e(K/Q_p)v_p(r) \text{ by [Ser79, IV Proposition 4]}.$$

**Remark 3.12.** From Theorem 3.4, Theorem 3.10 and Remark 3.11 (also see [Ber78, Corollaire to Proposition 3]) we deduce that a dihedral extension $K/Q_p$ of degree $2p$ is either almost-maximally ramified or is weakly and totally ramified.

### 3.2. Local freeness results for Galois extensions of number fields.

**Remark 3.13.** Let $K/F$ be a finite Galois extension of number fields. If $O_K$ is free over $A_{F/K}$ then it is clear that $O_K$ is locally free over $A_{F/K}$. In particular, the analogues of Theorems 1.1, 1.2 and 1.3 all hold, with ‘locally free’ in place of ‘free’. Theorems 3.13 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 $G = \text{Gal}(K/F)$ and let $p$ be a prime of $F$ that is tamely ramified in $K/F$. Then $O_{K,p}$ is free over $A_{K/F_p} = O_{F_p}[G]$.

**Theorem 3.15.** [Let98] Let $K/F$ be an extension of number fields such that $K/Q$ is a finite abelian extension. Then $O_K$ is locally free over $A_{K/F}$. 

Remark 3.16. Theorems 3.14 and 3.15 are well-known consequences of Theorems 3.1 and 3.3 respectively. See Remark 3.3 and Corollary 3.6 for instance.

Theorem 3.17. \cite{Jau81} Let $K/Q$ be a Galois extension such that $\text{Gal}(K/Q)$ is metacyclic of type \{3,7\}. Then $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/Q}$.

Theorem 3.18. \cite{Ber79} Théorème] Let $K/Q$ be a finite dihedral extension and let $G = \text{Gal}(K/Q)$. Let $p$ be an odd rational prime that is wildly ramified in $K/Q$ and let $N$ be the unique cyclic subgroup of $G$ of index 2. Then $\mathcal{O}_{K,p}$ is projective over $\mathfrak{A}_{K/Q,p}$ if and only if one of the following conditions holds:

(i) $p$ is almost-maximally ramified in $K/Q$ and $G_1 \subseteq N$, in which case $\mathfrak{A}_{K/Q,p} = \mathbb{Z}_p[G]\{e_{G_1}\}_{i \geq 1}$, or

(ii) $p$ is not almost-maximally ramified, $|G_0| = 2p$ and $|G : G_0| \triangleleft 2$, in which case $\mathfrak{A}_{K/Q,p} = \mathbb{Z}_p[G][e_{G_0}]$.

Remark 3.19. In fact, Theorem 3.18 is \cite{Ber79} 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 to $N$.

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 $e_N x M = e_N e_N x M = e_N x e_N M \subseteq e_N M \subseteq M$. \qed

We now recall the notion of hybrid group ring introduced in \cite{JN16} §2 and further developed in \cite{JN18} §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 [CR81 (27.1)]. In this situation, $\mathfrak{A}(F[G], M) = R[G]$ and thus $M$ is free over $\mathfrak{A}(F[G], M)$ by [Rei03 (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 [JN16, Examples 2.16 and 2.18]. Indeed, we have

$$\mathbb{Z}_3[A_4] \cong \mathbb{Z}_3[C_3] \times M_{3 \times 3}(\mathbb{Z}_3)$$

and

$$\mathbb{Z}_3[S_4] \cong \mathbb{Z}_3[S_3] \times M_{3 \times 3}(\mathbb{Z}_3) \times M_{3 \times 3}(\mathbb{Z}_3),$$

where $M_{3 \times 3}(\mathbb{Z}_3)$ is a maximal $\mathbb{Z}_3$-order by [Rei03 (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 [JN16, 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, $e_N M$ is free over $\mathfrak{A}(F[G/N], e_N M)$ if and only if $M$ is free over $\mathfrak{A}(F[G], M)$.

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 [Rei03 (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 $G = \text{Gal}(K/F)$. Let $p$ be a rational prime and let $p$ 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 $\mathbb{Z}_p[N] \cong \mathfrak{A}(F[G], M) \times (1 - e_N)R[G]$.

Now further suppose that $\mathbb{Z}_p[G]$ is $N$-hybrid. Then

$$\mathfrak{A}(F[G], M) \cong \mathfrak{A}(F[G], M) \times (1 - e_N)\mathbb{Z}_p[G],$$

and $\mathfrak{A}(G, M)$ is free over $\mathfrak{A}(G, M)$ if and only if $\mathfrak{A}(G, M)$ is free over $\mathfrak{A}(G, M)$.

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 $K/Q$ be a finite Galois extension and let $G = \text{Gal}(K/Q)$. 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 $\mathfrak{A}(K/Q, M)$ is free over $\mathfrak{A}(K/Q, M)$.

Proof. Let $M$ be the subfield of $K$ fixed by $N$. Then $\mathfrak{A}(M, M)$ is free over $\mathfrak{A}(M, M)$ by Theorem 1.1 or Theorem 3.11. The result now follows from Proposition 4.1.

Remark 4.9. Jaulent [Jau81] 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 $\text{Gal}(K/\mathbb{Q}) \cong A_4$ 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 2.9 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 $G = \text{Gal}(K/\mathbb{Q})$ 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 $\text{Gal}(L/\mathbb{Q}_2) \cong A_4$. 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 [JR06]. Indeed, $L$ is the Galois closure of the extension of $\mathbb{Q}_2$ generated by the polynomial $x^4 + 2x^3 + 2x^2 + 2$. □

**Proposition 4.12.** Let $K/\mathbb{Q}$ be a Galois extension with $\text{Gal}(K/\mathbb{Q}) \cong A_4$. If 2 is either tamely ramified in $K/\mathbb{Q}$ or has full decomposition group in $\text{Gal}(K/\mathbb{Q})$, 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 $G := \text{Gal}(K/\mathbb{Q})$. 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 

$$
\mathcal{O}_{K,2} \cong \text{Ind}_C^G \mathcal{O}_{K\mathfrak{p}} = \mathcal{O}_{K\mathfrak{p}} \quad \text{and} \quad \mathfrak{A}_{K/\mathbb{Q},2} \cong \mathfrak{A}_{K/\mathbb{Q},2},
$$

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 the introduction.

**Theorem 5.1.** [Ber72] 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 $m$th cyclotomic field $\mathbb{Q}(\zeta_m)$. If $m$ is odd then $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$ and so $\mathbb{Q}(\zeta_{2m})^+ = \mathbb{Q}(\zeta_m)^+$.

**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 $2p^nn$. 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) $p$ is almost-maximally ramified in the extension $K/\mathbb{Q}$;
(iv) the ramification index of $p$ in $K/\mathbb{Q}$ is a power of $p$.

Then we have the following conclusions:

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

Proof. Let $G = \text{Gal}(K/\mathbb{Q})$. By [Was97, Theorem 10.1] the condition on the class number of $\mathbb{Q}(\zeta_{2p^n})^+$ implies that the class number of $\mathbb{Q}(\zeta_{2p^n})^+$ is 1 for every $d \leq n$. This together with the regularity of $p$ implies that the locally free class group $\text{Cl}(\mathbb{Z}[G])$ is trivial: if $p$ is odd this follows from a special case of the main result of [Kea74, Theorem 1] (also see [CR87, (50.28)]), if $p = 2$ this follows from the results of [FKW74] (also see [CR87, (50.31)] and [CR81] (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 2.4. Note that $\mathcal{O}_K$ is locally free over $\mathfrak{A}_{K/\mathbb{Q}}$ at $\ell$ for every rational prime $\ell \neq 2, p$ by Theorem 3.4. 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 Theorem 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 characterization of almost-maximal ramification in dihedral extensions given in [Ber79, 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 [Mill1] 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 $K/\mathbb{Q}$ 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 $K/\mathbb{Q}$ is a power of $p$.

Remark 5.6. In the proof of Theorem 5.2 we could have used [Ber79, 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 [Ber79, §1]. We include some of the proofs for the convenience of the reader. The motivation for this section comes from §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 $\text{Ind}_H^G M$ is the induced module $R[G] \otimes_{R[H]} M \cong \bigoplus_{t \in G/H} sM$, 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 $\mathfrak{A}(F[G], \text{Ind}_H^G M)$ and $\text{Ind}_H^G \mathfrak{A}(F[H], M)$. Note that these both contain the group ring $R[G]$.

Proposition 6.1. [Ber79, §1.3] We have

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

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

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

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

(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 \( \mathfrak{A}(F[G], \text{Ind}_{H}^{G} M) \subseteq \text{Ind}_{H}^{G} \mathfrak{A}(F[H], M) \). Hence \( \text{Ind}_{H}^{G} \mathfrak{A}(F[H], M) \) is an \( \mathfrak{A}(F[G], \text{Ind}_{H}^{G} M) \)-lattice.

Proposition 6.5. If \( M \) is free over \( \mathfrak{A}(F[H], M) \) then \( \text{Ind}_{H}^{G} M \cong \text{Ind}_{H}^{G} \mathfrak{A}(F[H], M) \) as \( \mathfrak{A}(F[G], \text{Ind}_{H}^{G} M) \)-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 \( \text{Ind}_{H}^{G} M \cong \text{Ind}_{H}^{G} \mathfrak{A}(F[H], M) \) of \( R[G] \)-lattices. By Lemma 2.1 this is also an isomorphism of \( \mathfrak{A}(F[G], \text{Ind}_{H}^{G} M) \)-lattices. \( \square \)

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

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

then \( \text{Ind}_{H}^{G} M \) is free over \( \mathfrak{A}(F[G], \text{Ind}_{H}^{G} M) \).

Proof. In case (i) this follows immediately from Proposition 6.5. Clearly, (ii) \( \Rightarrow \) (i). Moreover, (ii) \( \Leftrightarrow \) (iii) by Corollary 6.2. \( \square \)

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

Proposition 6.7. ([Ber79] Proposition 2] If \( \text{Ind}_{H}^{G} M \) is a projective \( \mathfrak{A}(F[G], \text{Ind}_{H}^{G} M) \)-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 6.8. ([Ber79] Proposition 3] Suppose that \( H \) is normal in \( G \). Then

(i) \( \mathfrak{A}^{*}(M) \) is an \( R \)-order in \( F[H] \),
(ii) \( \mathfrak{A}(F[G], \text{Ind}_{H}^{G} M) = \text{Ind}_{H}^{G} \mathfrak{A}^{*}(M) \), and
(iii) \( \text{Ind}_{H}^{G} M \) is a projective \( \mathfrak{A}(F[G], \text{Ind}_{H}^{G} M) \)-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 6.9. Let \( \Lambda \) be an \( R \)-order in a finite dimensional semisimple \( F \)-algebra \( A \). Then \( \Lambda \) is said to be clean if it has the following property: if \( M \) is a projective \( \Lambda \)-lattice such that \( FM \) is free over \( A \) then \( M \) is free over \( \Lambda \).

Theorem 6.10 (Hattori). Commutative \( R \)-orders in finite-dimensional semisimple \( F \)-algebras are clean.
Proof. See \cite{Hat65} or \cite{Rog70} IX Corollary 1.5. \qed

Proposition 6.11. \cite{Ber79} 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) $\text{Ind}_H^G M$ is projective over $\mathfrak{A}(F[G], \text{Ind}_H^G M)$;
(ii) $\text{Ind}_H^G M$ is free over $\mathfrak{A}(F[G], \text{Ind}_H^G M)$;
(iii) $\text{Ind}_H^G \mathfrak{A}(F[H], M)$ is a ring and $\text{Ind}_H^G M$ is free over $\text{Ind}_H^G \mathfrak{A}(F[H], M)$;
(iv) $M$ is free over $\mathfrak{A}(F[H], M)$ and $\mathfrak{A}^*(M) = \mathfrak{A}(F[H], M)$.

Proof. (i)$\Rightarrow$(iv). By Proposition 6.8(iii), $M$ is projective over $\mathfrak{A}^*(M)$. Moreover, $\mathfrak{A}^*(M)$ is a clean order by Theorem 6.10 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)$\Rightarrow$(iii). We have $\text{Ind}_H^G \mathfrak{A}(F[H], M) = \text{Ind}_H^G \mathfrak{A}^*(M) = \mathfrak{A}(F[G], \text{Ind}_H^G M)$, where the second equality is Proposition 6.8(ii). Thus $\text{Ind}_H^G \mathfrak{A}(F[H], M)$ is a ring by Corollary 6.2. Hence $\text{Ind}_H^G M$ is free over $\text{Ind}_H^G \mathfrak{A}(F[H], M)$ by Corollary 6.2(iii).

(iii)$\Rightarrow$(ii). This follows from Corollary 6.2.

(ii)$\Rightarrow$(i). This follows from the general fact that every free module is projective. \qed

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

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

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

Then the following statements hold:

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

LEOPOLDT-TYPE THEOREMS FOR NON-ABELIAN EXTENSIONS OF $\mathbb{Q}$
Proof. Note that if \( \{ h \in G/H \} \) and \( \{ k \in H/P \} \) are two sets of left cosets representatives, then \( \{ hk \} \) is a set of left coset representatives for \( G/P \). Thus we have

\[
\text{Ind}_H^G \mathfrak{A}(F[H], M) = \text{Ind}_H^G \left( R[H] + \left\{ \pi^{-n} \left( \sum_{k \in H/P} a_k k \right) : a_k \in R \right\} \cdot \text{Tr}_P \right)
\]

\[
= R[G] + \left\{ \pi^{-n} \left( \sum_{h \in G/H} h \left( \sum_{k \in H/P} a_h k \right) \right) : a_h \in R \right\} \cdot \text{Tr}_P
\]

\[
= R[G] + \pi^{-n} \left( \sum_{h \in G/H} h \sum_{k \in H/P} a_h k \right) : a_h \in R \right\} \cdot \text{Tr}_P
\]

which proves (i). Moreover, we have

\[
\text{Ind}_H^G \mathfrak{A}(F[H], M) = R[G] + \pi^{-n} R[G/P] \text{Tr}_P
\]

\[
= R[G] + \pi^{-n} \left\{ a_h : \text{a representative of } R/(\pi^n) \right\} \cdot \text{Tr}_P
\]

\[
= \pi^{-n} \left\{ \sum_{\gamma \in G} a_{\gamma} \gamma \in R[G] : \gamma_1^{-1} \gamma_2 \in P \Rightarrow a_{\gamma_1} \equiv a_{\gamma_2} \mod (\pi^n) \right\}.
\]

Thus for every \( g \in G \), we have

\[
g \text{Ind}_H^G \mathfrak{A}(F[H], M) g^{-1} = R[G] + \pi^{-n} R[G/gPg^{-1}] \text{Tr}_{gPg^{-1}}
\]

\[
= \pi^{-n} \left\{ \sum_{\gamma \in G} a_{\gamma} \gamma \in R[G] : \gamma_1^{-1} \gamma_2 \in gPg^{-1} \Rightarrow a_{\gamma_1} \equiv a_{\gamma_2} \mod (\pi^n) \right\}.
\]

Now by Proposition [6.1], we have that

\[
(7.1)
\mathfrak{A}(F[G], \text{Ind}_H^G M) = \bigcap_{g \in G} g \text{Ind}_H^G \mathfrak{A}(F[H], M) g^{-1}
\]

\[
= \pi^{-n} \left\{ \sum_{\gamma \in G} a_{\gamma} \gamma \in R[G] : \gamma_1^{-1} \gamma_2 \in \bigcup_{g \in G} gPg^{-1} \Rightarrow a_{\gamma_1} \equiv a_{\gamma_2} \mod (\pi^n) \right\}
\]

\[
= \pi^{-n} \left\{ \sum_{\gamma \in G} a_{\gamma} \gamma \in R[G] : \gamma_1^{-1} \gamma_2 \in \text{ncl}(P) \Rightarrow a_{\gamma_1} \equiv a_{\gamma_2} \mod (\pi^n) \right\}
\]

\[
= R[G] + \pi^{-n} R[G/\text{ncl}(P)] \text{Tr}_{\text{ncl}(P)}
\]

which proves (ii).

By Corollary [6.2] \( \text{Ind}_H^G \mathfrak{A}(F[H], M) \) is a ring if and only if it is equal to \( \mathfrak{A}(F[G], \text{Ind}_H^G M) \), which by (i) and (ii) is true if and only if \( P = \text{ncl}(P) \). This proves (iii). Part (iv) follows from (iii) and Corollary [6.6]. Part (v) follows from (iii) and Proposition [6.11]. \( \square \)
Remark 7.2. The system of equations (7.1) is justified by the following 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

$$\{a_\gamma \mid \gamma \in G, B : \gamma_1^{-1} \gamma_2 \in A \Rightarrow a_{\gamma_1} = a_{\gamma_2}\} = \{a_\gamma \mid \gamma \in G, B : \gamma_1^{-1} \gamma_2 \in A' \Rightarrow a_{\gamma_1} = a_{\gamma_2}\}.$$ 

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

Corollary 7.3. 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 $A_{K/F_\mathfrak{p}}$.

(ii) Assume further that the decomposition group $D = D(\mathfrak{P}|\mathfrak{p})$ is abelian and normal in $G$. Then $G_0$ is normal in $G$ if and only if $\mathcal{O}_{K_\mathfrak{P}}$ is free over $A_{K/F_\mathfrak{p}}$.

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

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

Hence claims (i) and (ii) follow from parts (iv) and (v) of Theorem 7.1.

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

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

such that

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

Then the following statements hold:

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

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

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

(v) If $H$ is abelian and normal in $G$ and $\text{Ind}_H^G M$ is projective over $A(F[G], \text{Ind}_H^G M)$, then $P_i$ is normal in $G$ for every $i$.

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

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

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

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

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

It remains to show the reverse containment. First note that

\[
\text{Tr}_1 = \pi^{-n_1} \theta \in \mathfrak{A}(F[G], \text{Ind}_H^G M) \subseteq \mathfrak{A}(F[H], M) = \sum_{i=0}^{r} \pi^{-n_i} R[G] \text{Tr}_{P_i},
\]

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

For each integer \( j \) with \( 0 \leq j \leq r \), we shall prove that

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

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

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

Also note that for each \( g \in G \) we have

\[
g^{-1} \pi^{n-1} \theta g \in g^{-1} \pi^{n-1} \mathfrak{A}(F[G], \text{Ind}_H^G M) g = \pi^{n-1} \mathfrak{A}(F[G], \text{Ind}_H^G M) \subseteq \pi^{n-1} \text{Ind}_H^G \mathfrak{A}(F[H], M) \subseteq R[G] + \pi^{n-1-n_r} R[G] \text{Tr}_{P_r}.
\]

Hence

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

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

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

where the equality follows from (7.3) and the containment \( R[G] \text{Tr}_{P_r} \subseteq R[G] \text{Tr}_{P_{r-1}} \), which holds since \( \text{Tr}_{P_r} = \text{Tr}_{P_{r-1}} \text{Tr}_{P_{r-1}} \). 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 \( \sum_{i=j+1}^{r} \pi^{-n_i} R[G] \text{Tr}_{\text{ncl}_G(P_i)} \), we can and do assume without loss of generality that

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

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

\[
\theta \in \sum_{i=0}^{r-j-1} \pi^{-n_i} R[G] \text{Tr}_{P_i} + \pi^{-n_{r-j}} R[G] \text{Tr}_{\text{ncl}_G(P_r-j)}.
\]
As in the base case, for each \( g \in G \) we have
\[
g^{-1} \pi^{n_{r-j-1}} \theta g \in \pi^{n_{r-j-1}-n_{r-j}} R[G] \cap \pi^{n_{r-j-1}} \mathfrak{A}(F[G], \text{Ind}_H^G M) \\
\subseteq \pi^{n_{r-j-1}-n_{r-j}} R[G] \cap \pi^{n_{r-j-1}} \text{Ind}_H^G \mathfrak{A}(F[H], M) \\
\subseteq R[G] + \pi^{n_{r-j-1}-n_{r-j}} R[G] \text{Tr}_{P_{r-j}},
\]
so, by the result for \( r = 1 \), we have
\[
\pi^{n_{r-j-1}} \theta \in R[G] + \pi^{n_{r-j-1}-n_{r-j}} R[G] \text{Tr}_{\text{ncl}_G(P_{r-j})}.
\]
Thus there exists \( \alpha \in R[G] \) such that
\[
\theta - \pi^{-n_{r-j}} \alpha \text{Tr}_{\text{ncl}_G(P_{r-j})} \in \pi^{-n_{r-j}} R[G] \cap \left( \sum_{i=0}^{r-j} \pi^{-n_i} \theta \text{Tr}_{P_i} \right) = \sum_{i=0}^{r-j-1} \pi^{-n_i} R[G] \text{Tr}_{P_i}.
\]
This concludes the induction step. Therefore we deduce that
\[
\mathfrak{A}(F[G], \text{Ind}_H^G M) = \sum_{i=0}^{r} \pi^{-n_i} R[G] \text{Tr}_{\text{ncl}_G(P_i)},
\]
which concludes the proof of part (ii).

We easily see with the same methods that
\[
\text{Ind}_H^G \mathfrak{A}(F[H], M) = \mathfrak{A}(F[G], \text{Ind}_H^G M)
\]
precisely when \( P_i = \text{ncl}_G(P_i) \) for every \( i \), establishing part (iii). Part (iv) follows from part (iii) and Corollary 6.6. Part (v) follows from Proposition 6.11.

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. Moreover, \( P_i \) is normal in \( H \) (to see this, induct from \( H \) to \( H \) and use that \( \mathfrak{A}(F[H], N) \) is a ring) and \( \pi^{n_i} \) divides the order of \( P_i \) for all \( i \).

8. LEOPOLDT-TYPE THEOREMS FOR \( A_4, S_4 \) AND \( A_5 \)-EXTENSIONS OF \( \mathbb{Q} \)

8.1. Galois module structure of \( A_4 \)-extensions of \( \mathbb{Q} \). In this subsection, we shall prove the following result, which is Theorem 1.6 stated in the introduction.

Theorem 8.1. Let \( K/\mathbb{Q} \) be a Galois extension with \( \text{Gal}(K/\mathbb{Q}) \cong A_4 \). 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 [BJ08] §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 [LMF19] 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 \( G := \text{Gal}(K/\mathbb{Q}) \cong A_4 \) of order 4, which 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,
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 $K/\mathbb{Q}$. From the subgroup lattice, we see that it suffices to analyse the cases in which 2 is wildly ramified in $K/\mathbb{Q}$ or $D$ is not dihedral of order 4. Theorem 3.10 implies that $\mathfrak{D}$ is both abelian and normal in $D$. Hence if $D$ is both abelian and normal in $G$, then $D = A_4$. Let $2 \mid e$ denote the number of conjugate subgroups, and is taken to be 1 when omitted (so that the subgroup is normal). 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).

Now suppose that $D = G_0 = V_4$. Then by the database of $p$-adic fields \cite{JR06} we have that $\mathfrak{O}_{K_p}$ is free over $\mathfrak{A}_{K_p/\mathbb{Q}_2}$, 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 3.11 we have $e_{G_2} \in \mathfrak{A}_{K_p/\mathbb{Q}_2}$ 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

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

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

$$\mathfrak{A}_{K_p/\mathbb{Q}_2} = \mathbb{Z}_2[D][e_{G_2}, e_{G_1}] = \mathbb{Z}_2[V_4] + \frac{1}{2}\mathbb{Z}_2[V_4]Tr_{G_2} + \frac{1}{4}\mathbb{Z}_2[V_4]Tr_{V_4}.$$
imply that $\text{Ind}^D_A\mathfrak{A}_{K_p/Q_2}$ is not free over $\mathfrak{A}_{K/Q,2}$. Hence $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/Q,2}$. Note that in the next paragraph we shall use the following fact

$$\text{Ind}^D_A\mathfrak{A}_{K_p/Q_2} = \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\text{Tr}_{G_0} \supseteq \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\text{Tr}_{V_4} = \mathfrak{A}_{K/Q,2},$$

which follows from Theorem 7.1(i)\&(ii).

Finally suppose $D = G_0 \cong C_2$. Then $\mathfrak{A}_{K_p/Q_2}$ 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

$$\mathfrak{A}_{K_p/Q_2} = \mathbb{Z}_2[D] + \frac{1}{2}\mathbb{Z}_2[D]\text{Tr}_D.$$

We cannot directly apply Theorem 7.1(iv)\&(v) as in the previous cases, as $D$ is not normal in $G$, but from Theorem 7.1(i)\&(ii) we have that

$$\text{Ind}^D_A\mathfrak{A}_{K_p/Q_2} = \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\text{Tr}_D \supseteq \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\text{Tr}_{V_4} = \mathfrak{A}_{K/Q,2}.$$

Once we fix a copy of $C_2$ inside $G$, note that $\text{Ind}^D_A\mathfrak{A}_{K_p/Q_2}$ and $\mathfrak{A}_{K/Q,2}$ are exactly the same as in the $(V_4, C_2)$-case of the previous paragraph, where we already showed that $\text{Ind}^D_A\mathfrak{A}_{K_p/Q_2}$ is not free over $\mathfrak{A}_{K/Q,2}$. Therefore $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/Q,2}$. \hfill \Box

8.2. Galois module structure of $S_4$-extensions of $\mathbb{Q}$. In this subsection, we shall prove the following result, which is Theorem 1.7 stated in the introduction.

**Theorem 8.3.** Let $K/\mathbb{Q}$ be a Galois extension with $G := \text{Gal}(K/\mathbb{Q}) \cong S_4$. 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 1.10 $\mathcal{O}_K$ is free over $\mathfrak{A}_{K/\mathbb{Q}}$ if and only if $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/Q,2}$.

We first show that if any of conditions (i)–(iv) hold then $\mathcal{O}_{K,2}$ is free over $\mathfrak{A}_{K/Q,2}$. 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 7.3(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 $\mathfrak{A}_{K/Q,2}$. We shall use the MAGMA implementation of two different algorithms: we use [BJ08 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; we use [HJ20 §8.5], which concerns general lattices in group rings, to prove that $\mathcal{O}_{K,2}$ is not free over $\mathfrak{A}_{K/Q,2}$ in cases when we do have freeness in the corresponding 2-adic extension.
We have the following lattice of the subgroups of $S_4$ up to conjugacy (see, for instance, the GroupNames database \cite{Dok18}).

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 $G := \text{Gal}(K/{\mathbb{Q}}) \cong S_4$ 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.

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 Sylow 2-subgroups of $D$ are not normal, but the wild inertia subgroup $G_1$ must be normal in $D$.

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 \cite{JR06}, we see that there are four possibilities for the completed extension $K_2/{\mathbb{Q}}_2$. By using the updated MAGMA implementation of \cite[Algorithm 3.1(6)]{BJ08} (see \S A.1 for details), which is based on that of \cite[\S 4.2]{BW09}, we can verify that $O_{K_2}$ is not free over $\mathfrak{A}_{K_2}/{\mathbb{Q}}_2$ in either of these cases (for the details on the implementation see \S A.1). Since the decomposition group is full (i.e. $D = G$), this immediately implies that $O_{K_2}$ 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 $D = D_8$. We first treat the case in which $O_{K_2}$ is not free over $\mathfrak{A}_{K_2}/{\mathbb{Q}}_2$. Then $O_{K_2}$ is not projective over $\mathfrak{A}_{K_2}/{\mathbb{Q}}_2$ by Theorem 3.10 and so $O_{K_2}$ is not free over $\mathfrak{A}_{K_2}$ by Proposition 6.7. As an aside, by using the database \cite[Theorem 3.10 and Remark 3.11]{JR06} it is straightforward to check that $O_{K_2}$ is not free over $\mathfrak{A}_{K_2}$ if and only if the ramification jumps of $K_2/{\mathbb{Q}}_2$ are 1, 3 and 5.

Therefore in the remaining cases we can and do assume that $O_{K_2}$ is free over $\mathfrak{A}_{K_2}/{\mathbb{Q}}_2$; 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 $O_{K_2}$ is not free over $\mathfrak{A}_{K_2}/{\mathbb{Q}}_2$ has already been considered in the previous paragraph. As we wish to show that $O_{K_2}$ is not free over $\mathfrak{A}_{K_2}$, by Proposition 6.5 it suffices to show that $\text{Ind}^D_O \mathfrak{A}_{K_2}/{\mathbb{Q}}_2$ is not free over $\mathfrak{A}_{K_2}$. Our strategy will be to determine the possible ramification groups, use this to understand the structure of $\mathfrak{A}_{K_2}$ and then apply Theorem 7.4 to obtain explicit descriptions of $\text{Ind}^D_O \mathfrak{A}_{K_2}$ and $\mathfrak{A}_{K_2}$; we will leave this last step to the end as cases with different $D$ will overlap.
We now return to the case $D = D_8$. We have the following subgroup lattice.

We denote the unique normal subgroup of order 2 in $D_8$ by $V_2$, and note that 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).

Suppose that $K_{P}/Q_2$ is almost-maximally ramified. Then by Theorem 3.10 we have $\mathfrak{A}_{K_p/Q_2} = \mathbb{Z}_2[D] + \sum_{i \geq 1} \frac{1}{2^i} \mathbb{Z}_2[D] \mathfrak{T}_G$, and all quotients of two consecutive different ramification groups are of order 2 (see the database [JLR06], 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 $K_{P}/Q_2$ is 2, then $V_2$ is the unique ramification group. Otherwise, there is a ramification group of order 4, which must be one of $V_4$, $C_2^2$ or $C_4$. Moreover, $D_8$ is a ramification group if and only if the ramification index of $K_{P}/Q_2$ is 8.

Suppose that $K_{P}/Q_2$ is not almost-maximally ramified. Then by Theorem 3.10 we deduce that $G_0 \cong C_2^2$ and $\mathfrak{A}_{K_p/Q_2} = \mathbb{Z}_2[D] + \frac{1}{2} \mathbb{Z}_2[D] \mathfrak{T}_G$. Moreover, by Remark 3.11 we must have that $G_2 = 0$ or $G_2 \cong C_2$ and $G_3 = 0$, 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 [JLR06]); hence $K_{P}/Q_2$ is weakly ramified. Note that $G_0$ is not equal to $V_4$, otherwise we are in case (iv), hence we can assume $G_0 = C_2^2$.

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 $K_{P}/Q_2$ is 2, then $G_0 = V_2$ and by Remark 3.11 $K_{P}/Q_2$ is almost-maximally ramified, and hence $\mathfrak{A}_{K_p/Q_2} = \mathbb{Z}_2[D] + \frac{1}{2} \mathbb{Z}_2[D] \mathfrak{T}_G$ (see Ber78 Corollaire 3 to Théorème 1, for example). If the ramification index is 4, then there must be two ramification jumps; since the upper ramification jumps are integral, Remark 3.11 implies that the extension is almost-maximally ramified and so $\frac{1}{2} \mathfrak{T}_{V_2}$ and $\frac{1}{4} \mathfrak{T}_D$ belong to $\mathfrak{A}_{K_p/Q_2}$. Hence

$$\mathfrak{A}_{K_p/Q_2} = \mathbb{Z}_2[D] + \frac{1}{2} \mathbb{Z}_2[D] \mathfrak{T}_{V_2} + \frac{1}{4} \mathbb{Z}_2[D] \mathfrak{T}_D,$$

where the containment ‘$\subseteq$’ follows from the fact that the right-hand side is the unique maximal order in $\mathbb{Q}_2[D]$ (see Ber78 Proposition 5, for example).

Finally, note that in the cases $D \cong C_2^2$ or $D \cong C_2$, we already computed $\mathfrak{A}_{K_p/Q_2}$ in the proof of Theorem 8.1.

We will denote by $W_2$ a choice of a subgroup of $S_4$ generated by a transposition and contained in $D_8$. We fix the following notation: $\langle 1, \frac{1}{2\pi} \mathfrak{T}_{H_1}, \ldots, \frac{1}{2\pi} \mathfrak{T}_{H_k} \rangle$ is the lattice

$$\mathbb{Z}_2[G] + \frac{1}{2\pi} \mathbb{Z}_2[G] \mathfrak{T}_{H_1} + \cdots + \frac{1}{2\pi} \mathbb{Z}_2[G] \mathfrak{T}_{H_k}.$$

Since we have now determined $\mathfrak{A}_{K_p/Q_2}$ in all the remaining cases, we can use Theorem 7.4(i)&(ii) to determine $\text{Ind}_{D}^D\mathfrak{A}_{K_p/Q_2}$ and $\mathfrak{M}_{K_p/Q_2}$ as listed in Table 1 below.

Hofmann and Johnston [HLJ20, §8.5] described the implementation of an algorithm in Magma that, given a finite group $\Gamma$, 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 [CR81] 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 $\text{Ind}_G^A \mathfrak{A}_{K^p/\mathbb{Q}_2}$ is free over its associated order $\mathfrak{A}_{K/\mathbb{Q},2}$ for each of the cases in Table 1. By Lemma 2.1 this condition is equivalent to $\text{Ind}_G^A \mathfrak{A}_{K^p/\mathbb{Q}_2}$ being isomorphic to $\mathfrak{A}_{K/\mathbb{Q},2}$ as $\mathbb{Z}_2[G]$-lattices. Since $\mathbb{Z}_2[G] + \frac{1}{p^k} \mathbb{Z}_2[G] \text{Tr}_{H_1} + \cdots + \frac{1}{p^k} \mathbb{Z}_2[G] \text{Tr}_{H_k}$ is the completion of $\mathbb{Z}[G] + \frac{1}{p^k} \mathbb{Z}[G] \text{Tr}_{H_1} + \cdots + \frac{1}{p^k} \mathbb{Z}[G] \text{Tr}_{H_k}$, a computation using the aforementioned algorithm shows that $\text{Ind}_G^A \mathfrak{A}_{K^p/\mathbb{Q}_2}$ is not free over $\mathfrak{A}_{K/\mathbb{Q},2}$ in each of the ten cases in Table 1 for the implementation see §A.2.

Remark 8.4. Cases (v) and (ix) from Table 1 can be tackled using Theorem 7.4(v) and cases (vii) and (x) using Theorem 7.4(v) combined with Proposition 6.7. More precisely:

- for (v) we apply Theorem 7.4(v) with $H = V_4$ and $G = S_4$;
- for (vii) we apply Theorem 7.4(v) with $H = C_2^2$ and $G = D_8$ and Proposition 6.7 inducing from $D_8$ to $\text{Gal}(K/\mathbb{Q}) \cong S_4$;
- for (ix) we apply Theorem 7.4(v) with $H = V_4$ and $G = S_4$;
- for (x) we apply Theorem 7.4(v) with $H = W_2$ and $G = D_8$ and Proposition 6.7 inducing from $D_8$ to $\text{Gal}(K/\mathbb{Q}) \cong S_4$.

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 [HJ20] §8.5] we found that $\langle 1, \frac{1}{2} \text{Tr}_{V_4}, \frac{1}{8} \text{Tr}_{D_8} \rangle$ is free over $\langle 1, \frac{1}{2} \text{Tr}_{V_4}, \frac{1}{8} \text{Tr}_{G} \rangle$ (see §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 1.8 stated in the introduction.

**Theorem 8.6.** Let $K/\mathbb{Q}$ be a Galois extension with $\text{Gal}(K/\mathbb{Q}) \cong A_5$. 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;

| Case | Ind$^G_A \mathfrak{A}_{K^p/\mathbb{Q}_2}$ | $\mathfrak{A}_{K/\mathbb{Q},2}$ |
|------|---------------------------------|-------------------------------|
| (i)  | $\langle 1, \frac{1}{2} \text{Tr}_{V_2}, \frac{1}{4} \text{Tr}_{C_4}, \frac{1}{8} \text{Tr}_{D_8} \rangle$ | $\langle 1, \frac{1}{2} \text{Tr}_{V_4}, \frac{1}{8} \text{Tr}_{G} \rangle$ |
| (ii) | $\langle 1, \frac{1}{2} \text{Tr}_{V_2}, \frac{1}{4} \text{Tr}_{C_4}, \frac{1}{8} \text{Tr}_{D_8} \rangle$ | $\langle 1, \frac{1}{2} \text{Tr}_{V_4}, \frac{1}{8} \text{Tr}_{G} \rangle$ |
| (iii) | $\langle 1, \frac{1}{2} \text{Tr}_{V_2}, \frac{1}{4} \text{Tr}_{C_2^2}, \frac{5}{8} \text{Tr}_{D_8} \rangle$ | $\langle 1, \frac{1}{2} \text{Tr}_{V_4}, \frac{1}{8} \text{Tr}_{G} \rangle$ |
| (iv)  | $\langle 1, \frac{1}{2} \text{Tr}_{V_2}, \frac{1}{4} \text{Tr}_{C_4} \rangle$ | $\langle 1, \frac{1}{2} \text{Tr}_{V_4}, \frac{1}{4} \text{Tr}_{G} \rangle$ |
| (v)   | $\langle 1, \frac{1}{2} \text{Tr}_{V_2}, \frac{1}{4} \text{Tr}_{V_4} \rangle$ | $\langle 1, \frac{1}{4} \text{Tr}_{G} \rangle$ |
| (vi)  | $\langle 1, \frac{1}{2} \text{Tr}_{V_2}, \frac{1}{4} \text{Tr}_{C_2^2} \rangle$ | $\langle 1, \frac{1}{2} \text{Tr}_{V_4}, \frac{1}{4} \text{Tr}_{G} \rangle$ |
| (vii) | $\langle 1, \frac{1}{4} \text{Tr}_{C_2^2} \rangle$ | $\langle 1, \frac{1}{2} \text{Tr}_{G} \rangle$ |
| (viii)| $\langle 1, \frac{1}{4} \text{Tr}_{C_2^2} \rangle$ | $\langle 1, \frac{1}{2} \text{Tr}_{G} \rangle$ |
| (ix)  | $\langle 1, \frac{1}{4} \text{Tr}_{V_2} \rangle$ | $\langle 1, \frac{1}{4} \text{Tr}_{V_4} \rangle$ |
| (x)   | $\langle 1, \frac{1}{4} \text{Tr}_{V_2} \rangle$ | $\langle 1, \frac{1}{2} \text{Tr}_{G} \rangle$ |
(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 2.5, \( \mathcal{O}_K \) 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 [Dok18]).

\[ \begin{array}{c}
A_5 \\
\downarrow \\
D_{10} \quad A_4 \\
\downarrow \\
C_5 \quad C_2^2 \\
\downarrow \\
C_2 \\
\downarrow \\
C_1 \\
\end{array} \]

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 \( G := \text{Gal}(K/\mathbb{Q}) \cong A_5 \) 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 \( A_5 \) above \( 2 \) and let \( D(2) \) be its decomposition group. Then \( D(2) \) must be isomorphic to \( A_4, C_2^2 \) or \( C_2 \). Hence in each of these cases \( \mathcal{O}_{K,p} \) is free over \( \mathfrak{A}_{K,p/\mathbb{Q}} \) (if \( D(2) = A_4 \), this follows from Lemma 4.11 and Theorem 3.9; otherwise this follows from Theorem 3.3). By Proposition 6.5 Ind\(_{D(2)}^G \mathfrak{A}_{K,p/\mathbb{Q}} \cong \text{Ind}_{D(2)}^G \mathcal{O}_{K,p} \cong \mathcal{O}_{K,2} \) as \( \mathfrak{A}_{K,2} \)-lattices. Thus we need to analyse when \( \text{Ind}_{D(2)}^G \mathfrak{A}_{K,p/\mathbb{Q}} \) is free over \( \mathfrak{A}_{K,q,2} \). In each of the aforementioned possibilities for \( D(2) \), we already know the structure of \( \mathfrak{A}_{K,p/\mathbb{Q}} \) from the proof of Theorem 8.1. Using Theorem 7.4(i)\&(ii) we can write all the possibilities for \( \text{Ind}_{D(2)}^G \mathfrak{A}_{K,p/\mathbb{Q}} \) and \( \mathfrak{A}_{K,q,2} \). We use the following notation: \( \langle 1, \frac{1}{2} \text{Tr}C_2 \rangle = \mathbb{Z}_2[G] + \frac{1}{2}\mathbb{Z}_2[G]\text{Tr}C_2 \) etc. The results are shown in Table 2 below.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
 & \text{Ind}_{D(2)}^G \mathfrak{A}_{K,p/\mathbb{Q}} \& \mathfrak{A}_{K,q,2} \\
\hline
(i) & \langle 1, \frac{1}{2} \text{Tr}C_2 \rangle & \langle 1, \frac{1}{2} \text{Tr}G \rangle \\
(ii) & \langle 1, \frac{1}{2} \text{Tr}C_2, \frac{1}{2} \text{Tr}C_2^2 \rangle & \langle 1, \frac{1}{2} \text{Tr}G \rangle \\
(iii) & \langle 1, \frac{1}{2} \text{Tr}C_2 \rangle & \langle 1, \frac{1}{2} \text{Tr}G \rangle \\
\hline
\end{tabular}
\end{table}

As in the proof of Theorem 8.3, we can use the MAGMA implementation of the algorithm described in [HJ20] \S8.5. We can hence verify that in none of the above cases \( \text{Ind}_{D(2)}^G \mathfrak{A}_{K,p/\mathbb{Q}} \cong \mathcal{O}_{K,2} \) is free over \( \mathfrak{A}_{K,q,2} \) (see \S8.3 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 $L/Q_3$ such that $\text{Gal}(L/Q_3) \cong A_4$ (one can check this using the database of $p$-adic fields [JR06], for example). Hence $D(p)$ must be isomorphic to either $D_{2p}$ or $C_p$, which implies that $\mathcal{O}_{K_p}$ is free over $\mathfrak{A}_{K_p}/\mathfrak{p}$ by Theorems 3.3 and 3.4. Thus by Proposition 6.5 we have that $\text{Ind}^G_{D(p)}\mathfrak{A}_{K_p}/\mathfrak{p} \cong \text{Ind}^G_{D}\mathcal{O}_{K_p} \cong \mathcal{O}_{K,p}$ as $\mathfrak{A}_{K_p}/\mathfrak{p}$-lattices, so that our goal is to analyse when $\text{Ind}^G_{D(p)}\mathfrak{A}_{K_p}/\mathfrak{p}$ is free over $\mathfrak{A}_{K_p}/\mathfrak{p}$. We use the following notation: $(1, \frac{1}{p}\text{Tr}_{C_p}) = \mathbb{Z}_p[G] + \frac{1}{p}\mathbb{Z}_p[G]\text{Tr}_{C_p}$, etc. If $D(p) \cong C_p$ (in which case we can and do assume that $D(p) = C_p$), then as $\mathfrak{K}_p/\mathfrak{p}$ is wildly ramified this implies that $\mathfrak{A}_{K_p}/\mathfrak{p} = \mathbb{Z}_p[D(p)] + \frac{1}{p}\mathbb{Z}_p[D(p)]\text{Tr}_{C_p}$, 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, $\mathfrak{A}_{K_p}/\mathfrak{p} = \mathbb{Z}_p[D(p)] + \frac{1}{p}\mathbb{Z}_p[D(p)]\text{Tr}_{C_p}$ (which gives the same structure for $\text{Ind}^G_{D(p)}\mathfrak{A}_{K_p}/\mathfrak{p}$ as when $D(p) = C_p$); otherwise, by Remark 3.12 $\mathfrak{K}_p/\mathfrak{p}$ is weakly and totally ramified and $\mathfrak{A}_{K_p}/\mathfrak{p} = \mathbb{Z}_p[D(p)] + \frac{1}{p}\mathbb{Z}_p[D(p)]\text{Tr}_{D(p)}$. Hence there are two possibilities for $\text{Ind}^G_{D(p)}\mathfrak{A}_{K_p}/\mathfrak{p}$ and $\mathfrak{A}_{K_p}/\mathfrak{p}$, shown in Table 3.

| | $\text{Ind}^G_{D(p)}\mathfrak{A}_{K_p}/\mathfrak{p}$ | $\mathfrak{A}_{K_p}/\mathfrak{p}$ |
|---|---|---|
| (i) | $(1, \frac{1}{p}\text{Tr}_{C_p})$ | $(1, \frac{1}{p}\text{Tr}_{G})$ |
| (ii) | $(1, \frac{1}{p}\text{Tr}_{D_{2p}})$ | $(1, \frac{1}{p}\text{Tr}_{G})$ |

We used the MAGMA implementation of the algorithm from [HJ20 §8.5] to verify that $\text{Ind}^G_{D(p)}\mathfrak{A}_{K_p}/\mathfrak{p}$ is free over $\mathfrak{A}_{K_p}/\mathfrak{p}$ if and only if we are in case (ii), that is, precisely when $\mathfrak{K}_p/\mathfrak{p}$ is weakly ramified or, equivalently, when it is not almost maximally-ramified (see §A.3).

Remark 8.7. Note that from the proof of Theorem 8.1 we already knew that neither $\mathbb{Z}_2[A_4] + \frac{1}{2}\mathbb{Z}_2[A_4]\text{Tr}_{C_2}$ nor $\mathbb{Z}_2[A_4] + \frac{1}{2}\mathbb{Z}_2[A_4]\text{Tr}_{C_2} + \frac{1}{4}\mathbb{Z}_2[A_4]\text{Tr}_{C_2}$ are even projective over their associated orders; induction from $A_4$ to $S_4$ and Proposition 6.7 permit us to conclude that $\mathbb{Z}_2[S_4] + \frac{1}{2}\mathbb{Z}_2[S_4]\text{Tr}_{C_2}$ and $\mathbb{Z}_2[S_4] + \frac{1}{2}\mathbb{Z}_2[S_4]\text{Tr}_{C_2} + \frac{1}{4}\mathbb{Z}_2[S_4]\text{Tr}_{C_2}$ are not projective over their associated orders. Thus we can treat cases (i) and (ii) from Table 2 without using the algorithm.

Remark 8.8. Note that for $p = 3$ and $p = 5$ we found that $(1, \frac{1}{p}\text{Tr}_{D_{2p}})$ is free over $(1, \frac{1}{p}\text{Tr}_{G})$ without the two being equal. We also found with the algorithm from [HJ20] that $(1, \frac{1}{p}\text{Tr}_{A_4})$, which does not come from a ring of integers, is free over $(1, \frac{1}{p}\text{Tr}_{G})$ (see §A.3).

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 [BJ08 Algorithm 3.1(6)] to check whether or not $\mathcal{O}_K$ is locally free at 2 over $\mathfrak{A}_{K}/\mathfrak{p}$, or equivalently, whether $\mathcal{O}_{K_p}$ is free over $\mathfrak{A}_{K_p}/\mathfrak{p}$, where $\mathfrak{p}$ is the unique prime of $K$ above 2. We used the database [LMF19] 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 [JR06]. Note that two of these extensions of $\mathbb{Q}_2$ are weakly ramified, and so Corollary 7.3 already shows that $\mathcal{O}_{K_p}$ is free over $\mathfrak{A}_{K_p}/\mathfrak{p}$ in both cases, but we include them anyway as an addition 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 [BJ08]. Note that here we use the updated file `INB.m` from [BJ11] 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);
  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 do not have local freeness at 2
we do not 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 [HJ20, §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 $\mathcal{A}_{K/\mathbb{Q}}$ if $K/\mathbb{Q}$ does not satisfy any of the conditions (i)–(iv) of Theorem 8.3 and $\mathcal{O}_{K_{2}}$ is free over $\mathcal{A}_{K_{2}/\mathbb{Q}_{2}}$, where $\mathcal{P}$ 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 [HJ20] 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, trV4/2, 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, trV4/2, trG/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
LEOPOLDT-TYPE THEOREMS FOR NON-ABELIAN EXTENSIONS OF $\mathbb{Q}$

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 [HJ20, §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 [HJ20] 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

REFERENCES

[BCP97] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478

[Ber72] A.-M. Bergé, Sur l’arithmétique d’une extension diédrale, Ann. Inst. Fourier (Grenoble) 22 (1972), no. 2, 31–59. MR 0371857

[Ber78] ———, Arithmétique d’une extension galoisienne à groupe d’inertie cyclique, Ann. Inst. Fourier (Grenoble) 28 (1978), no. 4, 17–44, ix. MR 513880

[BJ08] W. Bley and H. Johnston, Computing generators of free modules over orders in group algebras, J. Algebra 320 (2008), no. 2, 836–852. MR 2422318

[BJ11] ———, Computing generators of free modules over orders in group algebras II, Math. Comp. 80 (2011), no. 276, 2411–2434. MR 2813368

[BW09] W. Bley and S. M. J. Wilson, Computations in relative algebraic K-groups, LMS J. Comput. Math. 12 (2009), 166–194. MR 2564571

[Cha96] R. J. Chapman, A simple proof of Noether’s theorem, Glasgow Math. J. 38 (1996), no. 1, 49–51. MR 1373957

[CR81] 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)

[CR87] ———, 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)

[Dok18] T. Dokchitser, Group names, https://people.maths.bris.ac.uk/~matyd/GroupNames/ (2018).

[EH79] S. Endô and Y. Hironaka, Finite groups with trivial class groups, J. Math. Soc. Japan 31 (1979), no. 1, 161–174. MR 519042

[FKW74] 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

[Frö72] A. Fröhlich, Artin root numbers and normal integral bases for quaternion fields, Invent. Math. 17 (1972), 143–166. MR 323759
Department of Mathematics, University of Exeter, Rennes Dr, Exeter EX4 4RN, United Kingdom

Email address: ff263@exeter.ac.uk
URL: http://emps.exeter.ac.uk/mathematics/staff/ff263