EXTENSIONS OF TOTALLY REAL DIHEDRAL FIELDS RAMIFIED AT ONLY ONE PRIME

DARRIN DOUD AND PABLO RODRIGUEZ

Abstract. We prove that under certain conditions on an odd prime ℓ, every totally real $D_{2\ell}$-extension $L/\mathbb{Q}$ that is ramified at only one prime is contained in a $W \rtimes D_{2\ell}$-extension that is also ramified at only one prime, where W is the deleted permutation module for $D_{2\ell}$ over $\mathbb{F}_2$. If the degree ℓ subextension of $L/\mathbb{Q}$ has odd narrow class number, then our theorem holds regardless of the value of ℓ.

1. Introduction

In [9], Wong conjectures that any totally real S_3-extension of $\mathbb{Q}$ that is ramified at a single prime is contained in an S_4-extension of $\mathbb{Q}$ that is ramified only at that prime. This conjecture was proved in [3]. We note that S_3 is isomorphic to the dihedral group D_6 of order 6, and that S_4 can be described as a semidirect product $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes D_6$.

In [7], a similar result was proved: if D_{10} is the dihedral group of order 10, then any totally real D_{10}-extension $L/\mathbb{Q}$ that is ramified at a single prime is contained in a Galois extension $M/\mathbb{Q}$ that is ramified at only one prime and has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4 \rtimes D_{10}$, where D_{10} acts on $(\mathbb{Z}/2\mathbb{Z})^4$ in a specific way independent of L.

In this paper, we generalize the results of [3] and [7]. Our main theorem is as follows:

Theorem 1.1. *Fix a prime $\ell > 2$, and let $L/\mathbb{Q}$ be any totally real Galois extension that is ramified at only one prime $p \nmid 2\ell$ and has $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2\ell}$ (the dihedral group of order 2ℓ). Let $K/\mathbb{Q}$ be a degree ℓ subfield of L. If*

(1) K has odd narrow class number, or
(2) 2 is a primitive root modulo ℓ, or
(3) 2 has order $(\ell-1)/2$ modulo ℓ and $\ell \equiv 3 \pmod 4$,

then there is a Galois extension $M/\mathbb{Q}$ that is ramified only at p and contains L, and

$$\mathrm{Gal}(M/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{\ell-1} \rtimes D_{2\ell},$$

where the action of $D_{2\ell}$ on $(\mathbb{Z}/2\mathbb{Z})^{\ell-1}$ makes $(\mathbb{Z}/2\mathbb{Z})^{\ell-1}$ isomorphic as an $\mathbb{F}_2 D_{2\ell}$-module to the quotient W (defined in Definition 5.2) of the permutation $D_{2\ell}$-module by its unique trivial submodule.

For $\ell = 3$ or $\ell = 5$, Theorem 1.1 yields the results of [3] and [7] mentioned above, since 2 is a primitive root modulo ℓ for both of these values of ℓ. The primes below

Date: August 10, 2026 16:48.

100 which satisfy conditions (2) or (3) are

$$\ell = 3, 5, 7, 11, 13, 19, 23, 29, 37, 47, 53, 59, 61, 67, 71, 79, 83.$$

For these primes, every totally real $D_{2\ell}$-extension ramified only at a single prime is contained in a $W \rtimes D_{2\ell}$-extension of $\mathbb{Q}$ ramified only at that same prime. The primes below 100 which do not satisfy conditions (2) or (3) are

$$\ell = 17, 31, 41, 43, 73, 89, 97.$$

2. $D_{2\ell}$-extensions ramified at one prime

Throughout this paper, we fix a prime $\ell > 2$ and a prime p not dividing 2ℓ, and let $L/\mathbb{Q}$ be a totally real $D_{2\ell}$-extension of $\mathbb{Q}$ ramified only at p. We denote by $K/\mathbb{Q}$ a fixed degree ℓ subextension of $L/\mathbb{Q}$. Since $L/\mathbb{Q}$ is totally real, ramified only at p, and has a unique quadratic subfield, this quadratic subfield must be $\mathbb{Q}(\sqrt{p})$, and we see that we must have $p \equiv 1 \pmod 4$.

Since $p \nmid 2\ell$, we see that p is tamely ramified in $L/\mathbb{Q}$, so for any prime $\mathfrak{p}$ of L lying over p, the inertia group of $\mathfrak{p}/p$ in $\mathrm{Gal}(L/\mathbb{Q})$ must be cyclic. Since p has ramification index 2 in $\mathbb{Q}(\sqrt{p})$, this inertia group must have order 2. Since the inertia group is normal in the decomposition group, we see that $\mathfrak{p}/p$ must have inertial degree 1. Thus, in $L/\mathbb{Q}$, p splits into ℓ primes with ramification index 2 and inertial degree 1.

Using this information, we now describe the decomposition of p into primes in $K/\mathbb{Q}$.

Theorem 2.1. *With ℓ, p, and K as above, we have the prime decomposition*

$$p\mathfrak{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2 \cdots \mathfrak{p}_r^2$$

with $r = 1 + (\ell - 1)/2$, where each $\mathfrak{p}_i$ is a prime of K lying over p with inertial degree 1.

Proof. We note that all ℓ elements of order 2 in $D_{2\ell}$ are conjugate in $D_{2\ell}$. Thus, each element of $\mathrm{Gal}(L/\mathbb{Q})$ having order 2 generates the decomposition group of a unique prime of L lying over p. Hence, $\mathrm{Gal}(L/K)$ is the decomposition group for exactly one prime $\mathfrak{p}$ of L lying over p. Let $\mathfrak{p}_1 = \mathfrak{p} \cap K$. Then $\mathfrak{p}_1$ is a prime of K lying over p with ramification index 1. All other primes $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ of K lying over p must have ramification index 2 over p since their decomposition groups do not intersect $\mathrm{Gal}(L/K)$ nontrivially. Thus, the decomposition of p in $\mathfrak{O}_K$ is

$$p\mathfrak{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2 \cdots \mathfrak{p}_r^2.$$

Letting e_i and f_i be the ramification index and inertial degree of $\mathfrak{p}_i$ over p, and using the facts that each $f_i = 1$ and

$$\sum_{i=1}^{r} e_i f_i = \deg(K/\mathbb{Q}) = \ell,$$

we see easily that $r = 1 + (\ell - 1)/2$. □

Finally, we remark that since $K/\mathbb{Q}$ is totally real of degree ℓ, any system of fundamental units of K consists of $\ell - 1$ units.

3. Preliminary Lemmas

We wish to construct a quadratic extension of K with prescribed ramification. To do this, we will need to know the structure of $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. This will be accomplished using the following lemmas, which are true for general number fields $F/\mathbb{Q}$.

Lemma 3.1. *Let F be a degree n extension of $\mathbb{Q}$ in which 2 is unramified. Write the prime decomposition of $2\mathfrak{O}_F$ as*

$$2\mathfrak{O}_F = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

and for each i, denote the inertial degree of $\mathfrak{q}_i$ by f_i, and note that the sum of the f_i equals n. Then we have an isomorphism of abelian groups

$$(\mathfrak{O}_F/4\mathfrak{O}_F)^\times \cong (\mathbb{Z}/2\mathbb{Z})^n \times \prod_{i=1}^{s} \mathbb{Z}/(2^{f_i}-1)\mathbb{Z}.$$

Proof. By [4, Prop. 4.2.12], we see that each

$$(\mathfrak{O}_F/\mathfrak{q}_i^2)^\times \cong (\mathbb{Z}/2\mathbb{Z})^{f_i} \times \mathbb{Z}/(2^{f_i}-1)\mathbb{Z}.$$

Combining these via the Chinese Remainder Theorem, we find that

$$\begin{aligned}(\mathfrak{O}_F/4\mathfrak{O}_F)^\times &\cong \prod_{i=1}^{s}(\mathbb{Z}/2)^{f_i} \times \prod_{i=1}^{s} \mathbb{Z}/(2^{f_i}-1)\mathbb{Z} \\ &\cong (\mathbb{Z}/2\mathbb{Z})^n \times \prod_{i=1}^{s} \mathbb{Z}/(2^{f_i}-1)\mathbb{Z}.\end{aligned}$$

□

Since each $2^{f_i}-1$ is odd, the following corollary is immediate.

Corollary 3.2. *With notation as above, let S be the subgroup of squares in $(\mathfrak{O}_F/4\mathfrak{O}_F)^\times$. Then*

$$(\mathfrak{O}_F/4\mathfrak{O}_F)^\times/S \cong (\mathbb{Z}/2\mathbb{Z})^n.$$

The following lemma, proved in [5], allows us to construct quadratic extensions of a number field F with controlled ramification.

Lemma 3.3. [5, Lemma 5.32] *Let F be a number field, let $M = F(\sqrt{\alpha})$ be a quadratic extension of F with $\alpha \in \mathfrak{O}_F$, and let $\mathfrak{q}$ be a prime ideal of $\mathfrak{O}_F$.*

i If $2\alpha \notin \mathfrak{q}$, then $\mathfrak{q}$ is unramified in M.

ii If $2 \in \mathfrak{q}$, $\alpha \notin \mathfrak{q}$, and $\alpha = \beta^2 - 4\gamma$ for some $\beta, \gamma \in \mathfrak{O}_F$, then $\mathfrak{q}$ is unramified in M.

4. Existence of a quadratic extension of K

Using Lemmas 3.1 and 3.3, we prove the following two propositions. Both are proved for $\ell = 5$ in [7]; the proofs, which generalize easily to the case of arbitrary prime ℓ, are included here for completeness.

Proposition 4.1. *Let $u_1, \ldots, u_{\ell-1}$ be a system of fundamental units of K, and let*

$$T = \left\{ \pm \prod_{i=1}^{\ell-1} u_i^{\epsilon_i} : \text{ each } \epsilon_i \in \{0,1\} \right\}.$$

If the narrow class number of K is odd, then there is a surjective map $\Phi : T \to (\mathfrak{O}_K/4\mathfrak{O}_K)^\times/S \cong (\mathbb{Z}/2\mathbb{Z})^\ell$.

Proof. Suppose that the narrow class number of K is odd. Since elements of $\mathfrak{O}_K^\times$ are relatively prime to 2, we can define the natural homomorphism $\Psi : \mathfrak{O}_K^\times \to (\mathfrak{O}_K/4\mathfrak{O}_K)^\times/S$ taking $\alpha \in \mathfrak{O}_K^\times$ to $(\alpha + 4\mathfrak{O}_K) \pmod S$. We will show that the restriction $\Phi = \Psi|_T$ of this homomorphism is the desired surjection.

We note that $|T| = |(\mathfrak{O}_K/4\mathfrak{O}_K)^\times/S| = 2^\ell$, so to prove that the given map is surjective, it suffices to prove that it is injective. Suppose then that $\alpha_1, \alpha_2 \in T$ and $\Phi(\alpha_1) = \Phi(\alpha_2)$. Then $\Psi(\alpha_1) = \Psi(\alpha_2)$, and since Ψ is a homomorphism, $\Psi(\alpha_1/\alpha_2)$ is the identity. Let $\alpha = \alpha_1/\alpha_2$. We note that we can write

$$\alpha = \pm \prod_{i=1}^{\ell-1} u_i^{\gamma_i},$$

where each $\gamma_i \in \{-1, 0, 1\}$.

If α is not a square in K, then we can construct the quadratic extension $K(\sqrt{\alpha})/K$. Since α is a unit, by Lemma 3.3 this extension can only be ramified at 2. However, since $\Psi(\alpha) = (\alpha + 4\mathfrak{O}_K) \pmod S$ is the identity, we see that $\alpha + 4\mathfrak{O}_K$ must be an element of S, and so $\alpha + 4\mathfrak{O}_K$ is equal to some $\beta^2 + 4\mathfrak{O}_K$. Hence, α is congruent to a square modulo $4\mathfrak{O}_K$. Then by Lemma 3.3, we see that $K(\sqrt{\alpha})/K$ is unramified at primes above 2. Thus, $K(\sqrt{\alpha})/K$ is an unramified quadratic extension of K, which cannot exist (since the narrow class number of K is odd). Hence, α must be a square in K.

Since α is a square in K, we see that each $\gamma_i = 0$ and the sign on α is positive. In this case, we must have $\alpha_1 = \alpha_2$, proving that Φ is injective. □

Proposition 4.2. *Let $L/\mathbb{Q}$ be a totally real Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{2\ell}$ for some prime ℓ. Assume that $L/\mathbb{Q}$ is ramified only at the rational prime p, and let $K/\mathbb{Q}$ be a degree ℓ subextension of L. Then there is an element $\pi \in \mathfrak{O}_K$ such that $K(\sqrt{\pi})$ is a quadratic extension of K not equal to L and $K(\sqrt{\pi})/\mathbb{Q}$ is unramified outside p.*

Proof. We break the proof into two cases.

Case 1: Assume that the narrow class number of K is even.

Then there is a quadratic extension of K that is unramified over K. This extension has the form $K(\sqrt{\pi})$ for some $\pi \in \mathfrak{O}_K$, and is clearly ramified over $\mathbb{Q}$ only at the primes that ramify in K, namely at p. Since the primes in K lying over p do not all have the same ramification indices, neither do the primes in $K(\sqrt{\pi})$, so $K(\sqrt{\pi})$ is not Galois, and thus not equal to L.

Case 2: Assume that the narrow class number of K is odd.

Denote by h the narrow class number of K. As described in Theorem 2.1, we see that the prime factorization of $p\mathfrak{O}_K$ is

$$p\mathfrak{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2 \cdots \mathfrak{p}_r^2$$

with $r = 1 + (\ell - 1)/2$. Then $\mathfrak{p}_r^h$ is the identity in the narrow class group, and is hence principal. Let $\tau \in \mathfrak{O}_K$ be a generator of $\mathfrak{p}_r^h$. Then τ is relatively prime to 4, and so gives rise to an element $\bar{\tau} \in (\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. Then $\tau + 4\mathfrak{O}_K \equiv \alpha + 4\mathfrak{O}_K \pmod S$ for some $\alpha \in T$. Then we see that $\tau\alpha^{-1} + 4\mathfrak{O}_K = \beta^2 + 4\mathfrak{O}_K$ for some $\beta \in \mathfrak{O}_K$. Since α is a unit in $\mathfrak{O}_K$, we see that $\pi = \tau\alpha^{-1} \in \mathfrak{O}_K$ is also a generator of $\mathfrak{p}_r^h$. Applying Lemma 3.3, we then see that $K(\sqrt{\pi})/K$ is a quadratic extension of K unramified outside $\mathfrak{p}_r$. Since the narrow class number of K is odd, we see that, in fact, $K(\sqrt{\pi})/K$ must be ramified at $\mathfrak{p}_r$. As in the even class number case, we

see that the primes in $K(\sqrt{\pi})$ have different ramification indices over $\mathbb{Q}$, so $K(\sqrt{\pi})$ is not Galois, and thus not equal to L. □

From this point on, we will denote by M the Galois closure of $K(\sqrt{\pi})/\mathbb{Q}$, with π as described above. The following facts about M are easily observed:

(1) M/L is a Galois extension and $\mathrm{Gal}(M/L)$ is an elementary abelian 2-group.
(2) $M/\mathbb{Q}$ is ramified only at p.

In the next sections, we will (under certain conditions) determine $\mathrm{Gal}(M/\mathbb{Q})$.

5. Computing the Galois group

5.1. **Galois groups for small ℓ.** Theorem 1.1 is proven in [3] for $\ell = 3$ and in [7] for $\ell = 5$ by examining tables of transitive subgroups of $S_{2\ell}$. The idea is that $K(\sqrt{\pi}) = \mathbb{Q}(\sqrt{\pi})$ (since $K = \mathbb{Q}(\pi)$), and $\sqrt{\pi}$ has degree 2ℓ over $\mathbb{Q}$. Hence, we know that $\mathrm{Gal}(M/\mathbb{Q})$ is a transitive group of degree 2ℓ. It must have order divisible by 4ℓ, since it contains $L(\sqrt{\pi})$, which has degree 4ℓ over $\mathbb{Q}$. In addition, it has exactly one subgroup of index 2 (since $M/\mathbb{Q}$ is only ramified at $p > 2$, and so must have at most one quadratic subfield, but M contains L, which has a quadratic subfield), and it has $D_{2\ell}$ as a quotient. By examining tables of transitive groups of degree 2ℓ, [3, 7] find that there is a unique (up to isomorphism) group satisfying these conditions when $\ell = 3$ or $\ell = 5$. Using tables of transitive groups of degree 2ℓ contained in Magma [1], we can similarly prove Theorem 1.1 for $\ell = 7, 11, 13, 19, 23$ (note that each of 7, 11, 13, 19, and 23 satisfies either condition (2) or condition (3) of Theorem 1.1). Since these tables do not extend to arbitrary degree, they cannot be used to prove the theorem for arbitrarily large primes. Because our methods below will include all of these cases, we omit any further detail about this method.

5.2. **Some $\mathbb{F}_2 D_{2\ell}$-modules.** In preparation for studying $\mathrm{Gal}(M/\mathbb{Q})$, we define a specific $\mathbb{F}_2 D_{2\ell}$-module, and record some of its properties. As generators for $D_{2\ell}$, we take the permutations $a = (1, 2, \ldots, \ell)$ and $b = (2, \ell)(3, \ell - 1) \cdots ((\ell + 1)/2, 1 + (\ell + 1)/2)$. Let $C_\ell = \langle a \rangle$ be the cyclic subgroup of order ℓ in $D_{2\ell}$. We will identify $D_{2\ell}$ with $\mathrm{Gal}(L/\mathbb{Q})$ via an isomorphism that makes K the fixed field of b.

Definition 5.1. For a prime ℓ, let V be the standard permutation module for $D_{2\ell}$ over $\mathbb{F}_2$. It has basis $v_1, \ldots, v_\ell$, with $\sigma \in D_{2\ell}$ acting via $\sigma v_i = v_{\sigma i}$.

We note that V has a unique one-dimensional submodule that is fixed by $D_{2\ell}$.

Definition 5.2. Let W be the quotient of V by its unique trivial submodule, and let $\pi : V \to W$ be the quotient map. We take as a basis for W the elements $w_i = \pi(v_i)$, for $1 \le i \le \ell - 1$.

One checks easily that with this notation, $\pi(v_\ell) = w_1 + \cdots + w_{\ell-1}$. In terms of this basis for W, the left action of $D_{2\ell}$ is given by

$$a \mapsto \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \end{bmatrix} = A, \quad b \mapsto \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 1 & 1 & \cdots & 0 & 0 \end{bmatrix} = B.$$

Let $W^* = \hom(W, \mathbb{F}_2)$ be the dual module of W. The action of $g \in D_{2\ell}$ is given on $f \in \hom(W, \mathbb{F}_2)$ by $(gf)(w) = f(g^{-1}w)$.

Lemma 5.3. *There is an isomorphism $W \cong W^*$ of $\mathbb{F}_2 D_{2\ell}$-modules.*

Proof. The action of $D_{2\ell}$ on W^* is given (in terms of the standard dual basis) by the matrices $A' = {}^tA^{-1}$ and $B' = {}^tB^{-1}$. It then suffices to find a change of basis matrix on W^* that conjugates A' to A and B' to B. This matrix is the tridiagonal matrix $P = (p_{ij})$ with

$$p_{ij} = \begin{cases} 1 & \text{if } |i-j| = 1 \\ 0 & \text{otherwise.} \end{cases}.$$

Note that P is invertible, since ℓ is odd. It is a simple (but tedious) matrix calculation to show that $P^{-1}A'P = A$ and $P^{-1}B'P = B$. □

Lemma 5.4. *W contains no nonzero elements fixed by the action of $C_\ell \subset D_{2\ell}$.*

Proof. Any such element would span a one-dimensional space on which $a \in D_{2\ell}$ acts with eigenvalue one. However, the matrix representing a has no eigenvalue equal to one. □

Definition 5.5. Let N be the set of quadratic extensions of L contained in M, together with L itself. We put an abelian group structure on N in the standard way; for distinct quadratic extensions L_1/L and L_2/L, we define their product to be the third quadratic subfield contained in L_1L_2/L. If we also define $L_1L_1 = L$, and $L_1L = L_1$, then N is an elementary abelian 2-group, or in other words, an $\mathbb{F}_2$-vector space. We define an action of $D_{2\ell}$ on N as follows: for $\sigma \in D_{2\ell}$ and $L_1 = L(\sqrt{\alpha})$ with $\alpha \in L$, we define $\sigma L_1 = L(\sqrt{\sigma\alpha})$. With these definitions it is easy to check that N is an $\mathbb{F}_2 D_{2\ell}$-module.

Definition 5.6. Let $G = \mathrm{Gal}(M/L)$. Then G is an $\mathbb{F}_2$-vector space. If we let $D_{2\ell} \cong \mathrm{Gal}(L/\mathbb{Q})$ act on it via conjugation in the standard way, then G becomes a left $\mathbb{F}_2 D_{2\ell}$-module.

Theorem 5.7. *There is an isomorphism $N \cong G^*$ of $\mathbb{F}_2 D_{2\ell}$-modules.*

Proof. There is a bijection between elements of N (field extensions of L of degree 1 or 2) and subgroups of G of index 1 or 2, with the field $L' \in N$ corresponding to the subgroup $\mathrm{Gal}(M/L')$.

Further, there is a bijection between subgroups of G of index 1 or 2 and elements of $G^* = \hom(G, \mathbb{F}_2)$, with a subgroup H corresponding to the unique homomorphism $\phi : G \to \mathbb{F}_2$ with kernel equal to H.

Composing these gives a bijection from N to G^*. Given two elements L_1 and L_2 corresponding to homomorphisms ϕ_1 and ϕ_2, with kernels H_1 and H_2, we note that the subgroup H_3 corresponding to the product L_3 (in N) of L_1 and L_2 consists of all elements of G that fix either both of L_1 and L_2, or neither. Thus, the homomorphism ϕ_3 corresponding to L_3 is the sum of ϕ_1 and ϕ_2. Hence, the given bijection is a homomorphism of groups.

For $L' \in N$, let H' be the corresponding subgroup of G, and ϕ' the corresponding element of G^*. Then for $x \in D_{2\ell}$, the field xL' corresponds to $xH'x^{-1}$. We note that for $g \in G$, $x\phi'(g) = \phi'(x^{-1} \cdot g) = \phi'(x^{-1}gx)$ has kernel $xH'x^{-1}$. Thus xL' maps to $x\phi'$, and we see that $N \cong G^*$. □

Lemma 5.8. *N is a quotient of the $D_{2\ell}$-module W defined in Definition 5.2.*

Proof. It is clear that as an abelian group, N is generated by the ℓ conjugates of $L(\sqrt{\pi})$. These conjugates are of the form $L_i = L(\sqrt{a^{i-1}\pi})$, and we see that for $\sigma \in D_{2\ell}$, we have $\sigma L_i = L_{\sigma i}$. Thus, there is a surjective module homomorphism θ from the standard permutation module V to N defined by $v_i \mapsto L_i$. The sum of the L_i in N is $L(\sqrt{\prod_i a^i\pi}) = L(\sqrt{N_{\mathbb{Q}}^K(\pi)})$. Let $\alpha = N_{\mathbb{Q}}^K(\pi) \in \mathbb{Q}$. Then the sum of the L_i is an extension of L of degree 1 or 2, unramified outside p, and contains $\mathbb{Q}(\sqrt{\alpha})$. Since $\mathbb{Q}(\sqrt{\alpha})/\mathbb{Q}$ must then be unramified outside p, we see that $\mathbb{Q}(\sqrt{\alpha}) \subseteq \mathbb{Q}(\sqrt{p}) \subseteq L$. Thus the sum of the L_i is equal to the identity element L in N.

Since the sum of the v_i maps to the identity under θ, we see that θ factors through W, yielding a surjective homomorphism from W to N, as desired. □

5.3. **The Hochschild–Serre spectral sequence.**

Lemma 5.9. *Let A be a finite-dimensional $\mathbb{F}_2 D_{2\ell}$-module on which the unique normal subgroup of $D_{2\ell}$ of order ℓ acts with no nonzero fixed elements. Then $H^2(D_{2\ell}, A) = 0$.*

Proof. We use the Lyndon-Hochschild-Serre spectral sequence [8, 6.8.2], denoting the normal subgroup of order ℓ in $D_{2\ell}$ by C_ℓ and the quotient $D_{2\ell}/C_\ell$ by C_2.

We have the spectral sequence

$$H^p(C_2, H^q(C_\ell, A)) \implies H^{p+q}(D_{2\ell}, A).$$

Of the three terms on the E_2 page of this sequence with $p + q = 2$, the two with $q > 0$ are zero since C_ℓ and A have relatively prime order [2, Corollary III.10.2]. The third (with $q = 0$) is zero since A has no nonzero fixed element under the action of C_ℓ. Hence, $H^2(D_{2\ell}, A) = 0$. □

Corollary 5.10. *We have*

$$\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{Gal}(M/L) \rtimes \mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r \rtimes D_{2\ell}$$

where r is the rank of $\mathrm{Gal}(M/L)$ *as an elementary abelian 2-group, and the action of $D_{2\ell}$ on $(\mathbb{Z}/2\mathbb{Z})^r$ is induced by the conjugation action of* $\mathrm{Gal}(L/\mathbb{Q})$ *on* $\mathrm{Gal}(M/L)$.

Proof. By Lemma 5.8, N is a quotient of W. Then $\mathrm{Gal}(M/L) \cong N^*$ is isomorphic to a submodule of W^*. By Lemma 5.3, W is self-dual, so $\mathrm{Gal}(M/L)$ is isomorphic to a submodule of W. Since W has no nontrivial fixed elements, neither does $\mathrm{Gal}(M/L)$.

Thus,

$$H^2(D_{2\ell}, \mathrm{Gal}(M/L)) = 0$$

by Lemma 5.9, so the sequence

$$1 \to \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \to 1$$

splits, giving the desired semidirect product decomposition. □

6. Proof of Theorem 1.1 assuming condition (1)

In this section, we will assume that K has odd narrow class number. In this case, by Proposition 4.2, we obtain a quadratic extension $K(\sqrt{\pi})/K$ in which a single prime $\mathfrak{p} = \mathfrak{p}_r$ of K having ramification index 2 over $\mathbb{Q}$ further ramifies in $K(\sqrt{\pi})/K$. Since $\mathfrak{p}$ already has ramification index 2 over $\mathbb{Q}$, and the inertial degree of the primes of L lying over p is 1, we see that $\mathfrak{p}$ must split in L. Thus, in L, there

must be two primes lying over the prime $\mathfrak{p}$ of K, each of which ramifies in $L(\sqrt{\pi})$. The other $\ell-2$ primes of L lying over p will be unramified in $L(\sqrt{\pi})/L$, since they lie over a prime of K that is unramified in $K(\sqrt{\pi})/K$ (see [6, Exercise 4.10(c)]).

Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be the two primes of L lying over the prime $\mathfrak{p}$ in K. Since $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{p}))$ acts transitively on the primes of L lying above p, we can choose an ℓ-cycle $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. Number the remaining primes of L lying over p as $\mathfrak{q}_3, \ldots, \mathfrak{q}_\ell$ such that $\sigma(\mathfrak{q}_i) = \mathfrak{q}_{i+1}$ for $1 \leq i \leq \ell$, where we reduce the indices modulo ℓ. Then for each $0 \leq i \leq \ell-1$, we see that $\sigma^i(\mathfrak{q}_1) = q_{i+1}$ and $\sigma^i(\mathfrak{q}_2) = \mathfrak{q}_{i+2}$ are the primes of L lying over the prime $\sigma^i(\mathfrak{p})$ in $\sigma^i(K)$. Then $L(\sqrt{\sigma^i(\pi)})/L$ is ramified only at $\mathfrak{q}_{i+1}$ and $\mathfrak{q}_{i+2}$.

Recall that N is the elementary abelian 2-group of quadratic extensions of L inside M, which is generated by the $L(\sqrt{\sigma^i(\pi)})$, with $0 \leq i \leq \ell-1$. Let $E = \mathbb{F}_2^\ell$ be the standard ℓ-dimensional vector space over $\mathbb{F}_2$, with standard basis $e_1, \ldots, e_\ell$.

We define a map $\psi : N \to E$ by

$$\psi(L') = \sum_{i=1}^{\ell} \epsilon_i e_i,$$

where $\epsilon_i = 0$ if $\mathfrak{q}_i$ is unramified in L'/L and $\epsilon_i = 1$ if $\mathfrak{q}_i$ is ramified in L'/L. Using the operation in N, one sees easily that this map is a linear transformation, since a prime $\mathfrak{q}_i$ is ramified in the product of two quadratic extensions if and only if it is ramified in exactly one of the two extensions. With the numbering as chosen above, the image of ψ is generated by $e_1+e_2, e_2+e_3, \ldots, e_{\ell-1}+e_\ell, e_\ell+e_1$. The first $\ell-1$ of these are clearly linearly independent, and the last is the sum of all the others. Hence, the dimension of the image is $\ell-1$. Now $\dim_{\mathbb{F}_2} N \geq \ell-1$, since N has a homomorphic image of dimension $\ell-1$. However, $\dim_{\mathbb{F}_2} N \leq \dim_{\mathbb{F}_2} W = \ell-1$, since, by Lemma 5.8, N is the homomorphic image of W as an $\mathbb{F}_2 D_{2\ell}$-module. Thus, $\dim_{\mathbb{F}_2}(N) = \ell-1$, and we see that $N \cong W$ as $\mathbb{F}_2 D_{2\ell}$-modules. Then $G \cong N^* \cong W^* \cong W$ by Theorem 5.7 and Lemma 5.3. Hence,

$$\mathrm{Gal}(M/\mathbb{Q}) \cong W \rtimes D_{2\ell},$$

as desired. This completes the proof of Theorem 1.1 when condition (1) holds.

7. Proof of Theorem 1.1 assuming condition (2) or (3)

If K has even narrow class number, then the extension $K(\sqrt{\pi})/K$ described by Proposition 4.2 may be unramified everywhere. In this case $L(\sqrt{\pi})/L$ is unramified everywhere, and we cannot proceed as in Section 6. Instead, we will show that either condition (2) or condition (3) of Theorem 1.1 guarantees that W is an irreducible $\mathbb{F}_2 D_{2\ell}$-module, and thus that $N \cong W$, since N is a nontrivial quotient of W.

Theorem 7.1. *W is an irreducible $\mathbb{F}_2 D_{2\ell}$-module if one of the following conditions holds:*

(1) 2 is a primitive root modulo ℓ.
(2) 2 has order $(\ell-1)/2$ modulo ℓ and $\ell \equiv 3 \pmod 4$.

Proof. Let $C_\ell = \langle a \rangle \subset D_{2\ell}$. By Maschke's theorem, W is a direct sum of irreducible $\mathbb{F}_2 C_\ell$-modules. Since the characteristic polynomial of a acting on W is the ℓth cyclotomic polynomial, the irreducible $\mathbb{F}_2 C_\ell$-constituents in W correspond to the irreducible factors of the ℓth cyclotomic polynomial over $\mathbb{F}_2$. Since the ℓth cyclotomic polynomial has no repeated roots in characteristic 2, these factors are

distinct. It is well known that they all have the same degree, namely the multiplicative order of 2 modulo ℓ, which we denote by $d = \mathrm{ord}_\ell(2)$. Thus, W decomposes into a direct sum of $(\ell-1)/d$ nonisomorphic irreducible $\mathbb{F}_2C_\ell$-modules, each having dimension d.

If we assume that 2 is a primitive root modulo ℓ, then $d = \mathrm{ord}_\ell(2) = \ell-1$. Thus, W is an irreducible $\mathbb{F}_2C_\ell$-module, hence also an irreducible $\mathbb{F}_2D_{2\ell}$-module.

If we assume that 2 has multiplicative order $(\ell-1)/2$ modulo ℓ and that $\ell \equiv 3 \pmod 4$, then the ℓth cyclotomic polynomial has two irreducible factors of degree $(\ell-1)/2$, and W is a direct sum of two nonisomorphic irreducible $\mathbb{F}_2C_\ell$-modules of dimension $(\ell-1)/2$, one for each factor. Since $\ell \equiv 3 \pmod 4$, the dimension of each of these modules is odd. Denote these submodules by M and M', and note that they are the only proper nontrivial $\mathbb{F}_2C_\ell$-submodules of W. Assume by way of contradiction that M is stable under the action of $b \in D_{2\ell}$. Let $\widetilde{M} = M \otimes_{\mathbb{F}_2} \bar{\mathbb{F}}_2$ be the module obtained from M by extending scalars to $\bar{\mathbb{F}}_2$. Now $\widetilde{M}$ is a direct sum of its nontrivial eigenspaces under a, each of which will have dimension 1. Since $ab = ba^{-1}$, multiplication by b will take an eigenspace of a with eigenvalue ζ to an eigenspace with eigenvalue ζ^{-1}. Since $\bar{\mathbb{F}}_2^\times$ has no elements of order 2, the nontrivial eigenvalues of a acting on M must come in pairs, implying that the dimension of $\widetilde{M}$ (and thus the dimension of M) must be even. This is a contradiction, so M cannot be stable under the action of b, and is not an $\mathbb{F}_2D_{2\ell}$-submodule of W. Similarly, M' is not an $\mathbb{F}_2D_{2\ell}$-submodule of W. Since M and M' are the only nontrivial proper $\mathbb{F}_2\mathbb{C}_\ell$-submodules of W, we see that W must be irreducible as an $\mathbb{F}_2D_{2\ell}$-module. □

In cases where ℓ satisfies the conditions in parts (2) or (3) of Theorem 1.1, we see that the conclusion of Theorem 1.1 holds, since the extension $M/\mathbb{Q}$ described at the end of Section 4 has Galois group $G \rtimes D_{2\ell}$, where $G^* \cong N$, and N is a quotient of W, which is irreducible by Theorem 7.1. Thus, $G^* \cong N \cong W$, and by Lemma 5.3, $G \cong W^* \cong W$. Hence,

$$\mathrm{Gal}(M/\mathbb{Q}) \cong W \rtimes D_{2\ell},$$

as desired.

References

1. Wieb Bosma, John Cannon, and Catherine 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 MR1484478
2. Kenneth S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994, Corrected reprint of the 1982 original. MR 1324339
3. Kevin Childers and Darrin Doud, *Octahedral extensions with a given cubic subfield*, J. Number Theory **167** (2016), 141–146. MR 3504039
4. Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR 1728313
5. David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR 3236783
6. Daniel A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York-Heidelberg, 1977. MR 457396
7. Pablo Miguel Rodriguez, *Pentagonal extensions of the rationals ramified at a single prime*, Master's thesis, Brigham Young University, Provo, Utah, December 2021, Available at `https://scholarsarchive.byu.edu/etd/9342`.

8. Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324
9. Siman Wong, *Arithmetic of octahedral sextics*, J. Number Theory **145** (2014), 245–272. MR 3253303

Brigham Young University, Provo, UT 84602
Email address: doud@mathematics.byu.edu

Brigham Young University, Provo, UT 84602
Email address: pablor@mathematics.byu.edu