

Galois 2-extensions of some split metacyclic extensions

John Jossey,

*Department of Mathematics, University of Illinois, Urbana-Champaign, IL 61801,
USA*

Abstract

Let K be a number field and p be a rational prime. Let $K(p)$ denote the maximal pro- p extension of K unramified outside the primes above p and infinity and $G_K(p)$ denote the Galois group $Gal(K(p)/K)$. We study certain types of split metacyclic extensions K of \mathbb{Q} such that $G_K(p)$ is not free but has a free subgroup of index 2. We will explicitly describe $G_K(p)$ using a result of Herfort-Ribes-Zaleskii on pro- p groups.

Key words: Class number; Free pro- p product; Metacyclic group; Profinite group; Galois group; Virtually free pro- p group

1 Introduction

Let K be a number field and p be a rational prime. Let $K(p)$ denote the maximal pro- p extension of K unramified outside the primes above p and infinity and $G_K(p)$ denote the Galois group $Gal(K(p)/K)$. The main problem is to determine $G_K(p)$. A natural question one could ask is the following:

(\mathcal{Q}_n) : For which K and p , does $G_K(p)$ contains a normal free pro- p subgroup of index p^n ?

There is a characterization for (\mathcal{Q}_0) , i.e., $G_K(p)$ is a free pro- p group [15, Corollary 8.7.10]. Also K.Wingberg [21] has classified when it is Demuškin. Note that this does not address (\mathcal{Q}_n) for any n , because the subgroups of finite index of a Demuškin group are not free(actually, all subgroups of infinite index are free).

Email address: johnjossey@gmail.com (John Jossey).

Markshaitis in [11] gave an explicit description of $G_K(p)$ for $K = \mathbb{Q}$ and $p = 2$, in effect he showed that \mathbb{Q} is a solution of (\mathcal{Q}_1) for $p = 2$. In general, (\mathcal{Q}_1) is unsolved. In [8], the author has shown that certain quadratic extensions of \mathbb{Q} solve (\mathcal{Q}_1) for $p = 2$.

In this paper we will study some split metacyclic extensions of \mathbb{Q} solving (\mathcal{Q}_1) for $p = 2$. In particular we focus on certain types of finite metacyclic extensions; namely split metacyclic groups G which can be written in the form $G' \rtimes M$, with both G' and M being cyclic, where G' indicates the commutator subgroup of G . Under the assumption that K is totally real and there is a unique prime divisor of 2 in K , we get a condition on the class number of K for which $G_K(2)$ is not free but has a free subgroup of index 2. We explicitly describe the structure of $G_K(2)$ using a result of Herfort-Ribes-Zaleskii [3, 22].

1.1 Notations

Let P_K denote a prime divisor of 2 in K . Let S denote the prime divisors of 2 and the infinite primes of K . Let $U_K, Cl(K)$ denote the unit group and the class group of K respectively, also e_2 and f_2 denote the ramification index and the inertial degree of P_K . Let g_2 denote the number of prime divisors of 2. We will study the Galois extensions of K of degree a power of 2, unramified outside S . The composite of these 2-extensions of K unramified outside S is the maximal pro-2 extension of K unramified outside S . Since the cyclotomic 2-extension of \mathbb{Q} unramified outside 2 and infinity is infinite, $G_K(2)$ is an infinite pro-2 group. Let h_K and h_K^+ denote the class number and the extended class number respectively. Let D_{P_K} and I_{P_K} denote the decomposition group and the inertia group respectively for P_K . Denote $o(P_K)$ to be the smallest positive integer n such that P_K^n is principal in \mathcal{O}_K where \mathcal{O}_K is the ring of integers in K . Let $Fix(H)$ denote the fixed field of H . Let $F_2(n)$ be the free pro-2 group on n generators, i.e., $F_2(n) \cong \mathbb{Z}_2 \amalg \cdots \amalg \mathbb{Z}_2$ (n copies of \mathbb{Z}_2)

1.2 Definitions and statement of our main result

Definition 1 *A number field K is said to be 2-rational if $G_K(2)$ is free.*

The notions of p -rational number fields or p -regular number fields were independently introduced by A. Movahhedi, T. Nguyen Quang Do in [14] and by G. Gras, J. F. Jaulent in [2], and their relationships were studied and generalized in [4], [5], [6] and [13]. Their definition of p -rational number field is as follows. Let K be a number field. Let S denote the set of prime divisors of p in K . Then K is called p -rational if the Galois group of the maximal pro- p extension of K unramified outside S is a free pro- p group.

However, the definition we have adapted includes the infinite primes of K in S . Observe that in their definition the infinite primes are not allowed to ramify, hence the infinite primes must split completely, unlike our definition where the infinite primes can ramify or split. Hence both the definitions coincide when K has no real embeddings. However, by our definition \mathbb{Q} is not 2-rational, but by their definition \mathbb{Q} is 2-rational. In [1], G. Gras introduces the concept of primitive ramification. [4, Theorem 3.5] gives a characterization for number fields to be p -rational, using the concept of primitive ramification and descent and lifting theorem on p -rationality. However, for it to hold and to use it is very important to use their definition of p -rationality.

One of our main objectives in this paper is to give an explicit description of $G_K(2)$ using a result of Herfort-Ribes-Zaleskii [3, 22] on virtually free pro-2 extensions and this has not been touched upon by Jaulent and others.

Definition 2 *A number field K is said to be minimal 2-rational if K is 2-rational and if there does not exist any proper, 2-rational, subfield F of K , such that K/F is a 2-extension unramified outside the prime divisors of 2 and the infinite primes of F .*

The following theorem is our main result.

Theorem 3 *Let $Gal(K/\mathbb{Q})$ be a nonabelian group of order pq . Suppose $L = K(i)$ or $K(\sqrt{-2})$.*

- (1) *If h_K^+ is odd, then L is 2-rational, and conversely*
- (2) *If L is 2-rational, then h_K is odd*

Moreover $G_K(2) \cong C_2 \amalg \cdots \amalg C_2 \amalg \mathbb{Z}_2$ with pq copies of C_2 and $G_L(2) \cong F_2(pq + 1)$.

2 Preliminaries

We summarize below definitions and well known results from Group Theory and Number Theory for the convenience of the reader.

2.1 Number Theory

Let L/K be a finite normal extension of number fields. Let \wp be a prime ideal of K and let \mathcal{P} be a prime divisor of \wp in L .

Definition 4 *The subgroup $D_{\mathcal{P}}$ of $Gal(L/K)$ such that $\{\sigma \mid \sigma \in Gal(L/K) :$*

$\sigma(\mathcal{P}) = \mathcal{P}$ is called the **decomposition group** of \mathcal{P} .

Definition 5 The subgroup $I_{\mathcal{P}}$ of $\text{Gal}(L/K)$ such that $\{\sigma \mid \sigma \in \text{Gal}(L/K) : \sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}}\}, \forall \alpha \in \mathcal{O}_L$ is called the **inertia group** of \mathcal{P} .

The inertia group is a normal subgroup of the decomposition group and the quotient group is cyclic of order $f_{\mathcal{P}}$ in L . Let p be the characteristic of the residue field $\mathcal{O}_K/\mathfrak{p}$

Theorem 6 [18, Chapter IV, Corollary 4 to Proposition 7] $I_{\mathcal{P}}$ is the semi direct product of a p -group with a cyclic group of order prime to p .

Theorem 7 [20, Theorem 10.4] Suppose L/K is a Galois extension of number fields and $\text{Gal}(L/K)$ is a p -group, where p is a prime. If there is at most one prime (finite or infinite) which ramifies in L/K . Then if $p|h_L$ then $p|h_K$.

2.2 Group Theory

Definition 8 [7] A finite group G is **metacyclic** if it has a cyclic normal subgroup H such that G/H is cyclic.

Metacyclic group G is called split metacyclic if $G = H \rtimes M$ where H and M are cyclic. If M acts trivially on H then G is abelian. However, not all metacyclic groups are split. For e.g. the quaternion group of order 8. Nevertheless, we have the following inclusion of groups

$$\text{Dihedral} \subset \text{Metacyclic}$$

2.3 Pro- p groups

Let p be a rational prime and G a pro- p group, that is an inverse limit of finite p -groups.

Definition 9 [19, p.121] A pro- p group G is *virtually free* if G has an open free subgroup.

Let $\{G_i \mid i = 1, \dots, n\}$ be a collection of pro- p groups. Let $G^{abs} = G_1 * \dots * G_n$ be the free product of G_1, \dots, G_n considered as abstract groups.

Definition 10 [16, Remark 9.1.3] The free pro- p product $G = G_1 \amalg \dots \amalg G_n$ is the completion of G^{abs} with respect to the topology defined by the collection of all normal subgroups N of finite index in G^{abs} such that $N \cap G_i$ is open in G_i ($i = 1, \dots, n$) and G^{abs}/N is a finite p -group.

The following theorem of Herfort-Ribes-Zaleskii is the group-theoretic fact which we use to deduce the structure of the $G_K(2)$. It is also a generalization of a well-known result of Serre: “A torsion-free virtually free pro- p group is free” [19].

Theorem 11 [3, Theorem 1] and [22] If G is a pro- p group having a free pro- p subgroup F of countable rank and index p then

$$G \cong \left(\prod_{x \in X} (C_p \times H_x) \right) \amalg H$$

is a free product, where C_p denotes the group of order p , H_x, H are free pro- p groups of F and X is the space of conjugacy classes of subgroups of order p in G .

In [3], the above theorem is stated without the restriction of F having a countable rank. In [22], P.A. Zaleskii corrects this error and gives an example of pro-2 group G having a free subgroup F of index 2 with uncountable rank, and G not having the above decomposition.

2.4 B_S

Let G be pro- p group. If $A = \mathbb{F}_p$, then G acts trivially on \mathbb{F}_p . Then

$$H^1(G, \mathbb{F}_p) = \text{Hom}(G, \mathbb{F}_p) = \text{Hom}(G/G^{(1)}, \mathbb{F}_p)$$

Hence the groups $G/G^{(1)}$ and $H^1(G, \mathbb{F}_p)$ are duals of each other. The minimum number of topological generators of G equals the minimum number of generators of $G/G^{(1)}$, by Burnside’s Theorem. Therefore the minimum number of generators of G is $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$. The relation rank of G is $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$ [17].

Let S be the set of prime divisors of a prime p and the infinite primes of K

We have a homomorphism

$$\text{res}^i : H^i(G_K(p), \mathbb{F}_p) \longrightarrow \sum_{\varphi \in S} H^i(G_\varphi, \mathbb{F}_p)$$

where G_φ is Galois group of the maximal p -extension of K_φ and K_φ is the completion of K at φ .

We set

$$\mathfrak{W}^i(G_K(p), \mathbb{F}_p) = \text{Ker}(\text{res}^i)$$

Definition 12 *Let*

$$B_S = (V_S/K^{\times p})^*$$

where

$$V_S = \{\alpha \in K^\times \mid (\alpha) = \mathfrak{a}^p, \alpha \in K_\varphi^p \text{ for } \varphi \in S\}$$

(α) is the principal fractional ideal generated by α , and \mathfrak{a} is some fractional ideal in K and $*$ indicates the dual.

Theorem 13 [9] or [10, Theorem 13.8] Suppose $\mu_p \subset K$. Then $\mathfrak{W}^2(G_K(p), \mathbb{F}_p) \cong B_S$ and there exists a map

$$\sum_{\varphi \in S} H^2(G_\varphi, \mathbb{F}_p) \xrightarrow{inv} \mathbb{F}_p$$

such that the sequence

$$0 \longrightarrow B_S \longrightarrow H^2(G_K(p), \mathbb{F}_p) \longrightarrow \sum_{\varphi \in S} H^2(G_\varphi, \mathbb{F}_p) \longrightarrow \mathbb{F}_p \longrightarrow 0$$

is exact.

Remark 14 *When $B_S = 0$, the map res^2 is injective, hence all the global relations come from the local relations.*

Theorem 15 [15, Theorem 8.7.3]

(1)

$$\dim_{\mathbb{F}_p} H^1(G_K(p), \mathbb{F}_p) = 1 + \sum_{\varphi \in S} \delta_\varphi - \delta + \dim_{\mathbb{F}_p} B_S$$

where

$$\delta = \begin{cases} 1 & \text{if } \mu_p \subseteq K \\ 0 & \text{if } \mu_p \not\subseteq K \end{cases} \quad \text{and} \quad \delta_\varphi = \begin{cases} 1 & \text{if } \mu_p \subseteq K_\varphi \\ 0 & \text{if } \mu_p \not\subseteq K_\varphi \end{cases}$$

Moreover if $\mu_p \subseteq K$, then $\dim_{\mathbb{F}_p} B_S = \dim_{\mathbb{F}_p} Cl_S / Cl_S^p$, where

$$Cl_S = Cl(K) / \langle S \rangle$$

where $\langle S \rangle$ denotes the subgroup of $Cl(K)$ generated by the prime ideals in S .

(2)

$$\dim_{\mathbb{F}_p} H^2(G_K(p), \mathbb{F}_p) = \sum_{\varphi \in S \setminus S_{\mathbb{C}}} \delta_\varphi - \delta + \dim_{\mathbb{F}_p} B_S$$

where $S_{\mathbb{C}}$ is the set of complex primes in K .

The following corollary is crucial for proving Theorem 3.

Corollary 16 *When $p = 2$*

- (1) $G_K(2)$ is free if and only if K is totally imaginary with a unique prime above 2 and $B_S = 0$.
- (2) $B_S = 0$ if either the class number of K is odd or S generates the Sylow 2-subgroup of the class group of K

Proof. (1) Since $p = 2$, $\{\pm 1\}$ belongs to K and K_\wp . Hence $\delta = \delta_\wp = 1$. Using (2) of Theorem 15 we see that $G_K(2)$ is free if and only if $\dim_{\mathbb{F}_2} B_S = 0$ and

$$\sum_{\wp \in S \setminus S_C} \delta_\wp = \delta$$

For the latter equality to hold, K should have a unique prime divisor of 2 and K should have no real embeddings. Hence we demand that there be a unique prime above 2 in K .

(2) Now, by (1) of Theorem 15 we see that $B_S = 0$ if and only if the group Cl_S/Cl_S^2 is trivial, where $Cl_S = Cl(K)/\langle S \rangle$. The group Cl_S/Cl_S^2 is trivial if and only if either h_K is odd or h_K is even and the Sylow 2-subgroup of Cl_S is trivial, which translates into saying that S generates the Sylow 2-subgroup of the class group of K . \square

The following lemma is used in proving Theorem 3.

Lemma 17 *Let L be a finite normal p -extension of a number field K in which at most divisors of p and infinity ramify. Then $G_L(p)$ is a subgroup of $G_K(p)$ and has index $[L : K]$. In particular, if $G_K(p)$ is a free pro- p group, then $G_L(p)$ is a free pro- p group.*

3 Some examples of 2-rational number fields

We first look at a simple example of abelian 2-rational number fields. In [8], the author has given an explicit characterization of all quadratic, biquadratic and degree 4-cyclic 2-rational number fields.

Example 18 *Let $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. Since $h_K = 1$, we have $B_S = 0$ by (2) of Corollary 16. Also, since K is totally imaginary and $g_2 = 1$, hence K is 2-rational by (1) of Corollary 16. Now, by (1) of Theorem 15, $G_K(2)$ has 2 generators. Hence $G_K(2) \cong F_2(2)$.*

Now, let us look at simple examples of nonabelian 2-rational number fields.

Example 19 *Consider a $D_8 (= C_4 \rtimes C_2)$ -extension, namely $L = \mathbb{Q}(\zeta_8, \sqrt[4]{2})$. Note that $h_{\mathbb{Q}(\zeta_8)} = 1$ and 2 is totally ramified in it. Since $L/\mathbb{Q}(\zeta_8)$ is ramified only at one prime, namely, the prime divisor of 2 in $\mathbb{Q}(\zeta_8)$, we have $g_2 = 1$ in*

L and h_L is odd (by Theorem 7). Hence L is 2-rational by Corollary 16 and by (1) of Theorem 15, $G_L(2)$ has 5 generators. Hence, we have $G_L(2) \cong F_2(5)$. However, we can also show the 2-rationality of L using Lemma 17, because $F = \mathbb{Q}(i) \subset L$ is 2-rational and L/F is a 2-extension unramified outside the prime divisors of 2 and infinity in F . Let $M = \mathbb{Q}(2^{\frac{1}{4}}) \subset L$. Since M is not totally imaginary, by (1) of Corollary 16, $G_M(2)$ cannot be free. We will give an explicit description of $G_M(2)$ in example 27.

Example 20 Let L be the splitting field of the polynomial $x^3 - 2$. Then $\text{Gal}(L/\mathbb{Q}) \cong S_3$. $h_L = 1$, $e_2 = 3$ and $f_2 = 2$, hence L is 2-rational. Let $K_1 = \mathbb{Q}(\sqrt[3]{2})$, $K_2 = \mathbb{Q}(\omega\sqrt[3]{2})$, $K_3 = \mathbb{Q}(\omega^2\sqrt[3]{2})$, where ω is a primitive cube root of unity. Let $K_4 = \mathbb{Q}(\sqrt{-3})$. Observe that $G_{K_4}(2) \cong F_2(2)$. Unlike the previous example, L is minimal 2-rational, because 3 is totally ramified in L , hence $G_L(2)$ is not a subgroup of $G_{K_j}(2)$, for any j . We will describe the structure of $G_{K_j}(2)$ in example 28.

4 On split metacyclic extensions

Remark 21 Henceforth, we will assume that K is totally real and $g_2 = 1$ for the rest of the paper.

4.1 Nonabelian extensions of order pq

Let $G = \text{Gal}(K/\mathbb{Q}) \cong C_p \rtimes C_q$ where p and q are primes such that $q \mid p - 1$. It is to be assumed that G is not a direct product, for otherwise G would be abelian.

Lemma 22 $e_2 = p$ in K .

Proof. By remark 21, $D_{P_K} = G$. Suppose that $q = 2$. Applying theorem 6 we see that $e_2 \neq 2$ and $e_2 \neq 2p$, as G has no normal subgroup of order 2. Since G is not cyclic $f_2 \neq 2p$. Hence the only possibility is $e_2 = p$. Therefore $f_2 = 2$. If q is odd, we have $e_2 \neq 1$ and $e_2 \neq pq$ in K , because of theorem 6 and $C_p \rtimes C_q$ being non cyclic. But $e_2 \neq q$ in K because $C_p \rtimes C_q$ has no normal subgroup of order q . Hence $e_2 = p, f_2 = q$ in K . \square

Let F denote the inertia subfield of K for P_K . Now $[F : \mathbb{Q}] = q$. The only finite primes of \mathbb{Q} that could possibly ramify in F are the primes $l \equiv 0, 1 \pmod{q}$. But, $e_q \neq pq$ as $C_p \rtimes C_q$ has no normal subgroup of order q . If l is a prime such that $l \equiv 1 \pmod{q}$, then $e_l \neq pq$ as $C_p \rtimes C_q$ is not cyclic. On the other hand p could be totally ramified in K .

Lemma 23 $o(P_K) = 1$ or p .

Proof. Since 2 is inert in F , we have $P_F = (2)$. Observe that $P_K^p = (2)$. Hence $o(P_K) = p$ or P_K is principal. \square

We are interested in obtaining a 2-extension L of K unramified outside the prime divisor of 2 and infinity in K , such that L is 2-rational. Hence by Corollary 16, we demand that L be totally imaginary and $g_2 = 1$ in L . Observe that P_K will split in the Hilbert 2-class field of K , since P_K has odd order. Hence choose a degree 2-extension L of K such that only P_K and the primes at infinity ramifies. We will assume that $L = K(i)$ or $K(\sqrt{-2})$. Note that L is totally imaginary.

Proof of Theorem 3. Since K is real, K is not 2-rational by Corollary 16. Observe that neither $\mathbb{Q}(i)$ nor $\mathbb{Q}(\sqrt{-2})$ lie in K as K is real. Now, 2 ramifies in $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$ and $e_2 = p$ in K . Hence, we have $e_2 = 2p$ and $f_2 = q$ in L . Note that L/K is unramified outside S .

Suppose h_K^+ is odd. We claim that h_L is odd. The proof given below is similar to the proof of the Theorem 7, but we tailor it to suit our needs. Suppose we assume to the contrary that h_L is even. Let \mathcal{L} be the Hilbert 2-class field of L . Since L/K is Galois, the maximality of \mathcal{L} implies that \mathcal{L}/K is Galois. Let $P_{\mathcal{L}}$ be a prime divisor of P_K in \mathcal{L} . Observe that P_K ramifies in L . Let $I_{P_{\mathcal{L}}}$ denote the inertia group for $P_{\mathcal{L}}$ in $Gal(\mathcal{L}/K)$. Since \mathcal{L}/L is unramified, we have $|I_{P_{\mathcal{L}}}| < |Gal(\mathcal{L}/K)|$. Since $Gal(\mathcal{L}/K)$ is a finite 2-group, there exists a normal subgroup \tilde{G} of $Gal(\mathcal{L}/K)$ of index 2, with $I_{P_{\mathcal{L}}} \subseteq \tilde{G} \subseteq Gal(\mathcal{L}/K)$. The inertia subgroups of other prime divisors of P_K in \mathcal{L} above P_K are conjugates of $I_{P_{\mathcal{L}}}$, hence lie in \tilde{G} . Since P_K is the only finite ramified prime in L , no finite prime of K ramifies from K to fixed field of \tilde{G} . But the fixed field of \tilde{G} is a degree 2 extension of K , so K has an abelian extension in which only the infinite primes ramify, hence h_K^+ is even. A contradiction. Whence h_L is odd. Therefore, by Corollary 16, L is 2-rational. Whence $G_K(2)$ is virtually free (Definition 9), with a free subgroup $G_L(2)$.

Let $N = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$. Observe that even though $N \subset L$ is 2-rational, we cannot conclude that L is 2-rational as L/N is not a 2-extension. In fact it can be seen that L is minimal 2-rational, i.e., there is no subfield J of L , with the property that J is 2-rational and L/J is a 2-extension which is unramified outside P_J and infinity, because odd rational prime(s) ramify in K .

Conversely, suppose that L is 2-rational. We need to show that h_K is odd. If we can show that h_L is odd, then we are done because of the following. Let us assume to the contrary that h_K is even. Let \mathcal{K} denote the Hilbert 2-class field of K . Consider $L\mathcal{K}/L$. Since L/K is totally ramified at P_K , $L\mathcal{K}/L$ is an unramified 2-extension. Hence $2 \mid h_L$. A contradiction.

Since L is 2-rational, by (1) of Corollary 16, we have $B_{\tilde{S}} = 0$, where \tilde{S} is the set of prime divisors of 2 and infinity in L . Recall that by (2) of Corollary 16, the only way $B_{\tilde{S}} = 0$ is if either h_L is odd or P_L generates the Sylow-2 subgroup of the class group of L . Hence to show that h_L is odd, our goal is to show that $o(P_L)$ is odd. We will use the fact that P_N is principal in N .

Now by lemma 23, we know that $o(P_K) = 1$ or p . We claim that $o(P_L) = 1$ or p . Let us denote F_1 to be a degree q -extension of N contained in L . Since $f_2 = q$ in L , we have that P_N is inert in F_1 . Therefore $P_{F_1} = P_N \mathcal{O}_{F_1}$. But P_N is principal in N . Hence P_{F_1} is principal in F_1 . Moreover, $P_L^p = P_{F_1} \mathcal{O}_L$, so $o(P_L) = 1$ or p as L/F_1 is a p -extension.

Next, we determine the structure of $G_K(2)$. Now by Theorem 15, $G_K(2)$ has $pq+1$ generators, pq relations and $G_L(2)$ has $pq+1$ generators and no relations. Since $G_L(2)$ has no relations, it is a free pro-2 group on $pq+1$ generators. Hence $G_L(2) \cong F_2(pq+1)$. Since $G_K(2)/(G_K(2))^{(1)}$ is an elementary abelian 2-group and $G_K(2)$ has $pq+1$ generators, using Burnside's Basis Theorem [9] or [10 Theorem 4.10], we have, $G_K(2)/(G_K(2))^{(1)} \cong C_2 \times \cdots \times C_2$ (with $pq+1$ copies of C_2).

Every number field has a cyclotomic \mathbb{Z}_p -extension for every p . Hence K has a \mathbb{Z}_2 -extension. But, by Leopoldt's conjecture, K has exactly one \mathbb{Z}_2 -extension, since K is totally real. Observe that K actually satisfies Leopoldt's conjecture. This is because, L being 2-rational, satisfies Leopoldt's conjecture by [12]. Now, K being a subfield of L satisfies Leopoldt's conjecture by [15, Proposition 10.3.13].

Hence $G_K(2)^{ab} \cong C_2^{k_1} \times \cdots \times C_2^{k_{pq}} \times \mathbb{Z}_2$, for some $k_i \geq 1, 1 \leq i \leq pq$. Now, $G_K(2)$ has a free subgroup $G_L(2)$ of index 2. Moreover, $G_L(2)$ has rank $pq+1$. Hence, applying Theorem 11, we have that

$$G_K(2) \cong (C_2 \times 1) \amalg \cdots \amalg (C_2 \times 1) \amalg \mathbb{Z}_2$$

or

$$(C_2 \times \mathbb{Z}_2) \amalg \cdots \amalg (C_2 \times 1)$$

and in each case there are pq copies of C_2 . The former group is topologically generated by $\langle a_i, b \mid a_i^2 = 1, 1 \leq i \leq pq \rangle$, where a_i denotes the generator of $C_2 \times 1$, and b denotes the topological generator of \mathbb{Z}_2 . On the other hand, the latter group is topologically generated by $\langle a_i, b \mid a_i^2 = 1, a_1 b = b a_1, 1 \leq i \leq pq \rangle$, where a_1 and b denote the generator of $C_2 \times \mathbb{Z}_2$, with $a_1^2 = 1$ and for $i \geq 2$, a_i denotes the generator of $C_2 \times 1$. It is easy to see that the latter has $pq+1$ relations while the former has only pq relations. But, $G_K(2)$ has pq relations. Whence $G_K(2) \cong C_2 \amalg \cdots \amalg C_2 \amalg \mathbb{Z}_2$ with pq copies of C_2 . [see Remark 24 for further explanations on how we obtained the structure of $G_K(2)$]. Thus $k_i = 1, 1 \leq i \leq pq$ and $G_K(2)$ is a virtually free pro-2 group. Hence these number fields K are a solution of (\mathcal{Q}_1) for $p = 2$. \square

Remark 24 *In the argument given in the proof of Theorem 3 for capturing the structure of $G_K(2)$, we do not consider the case when $G_K(2) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \amalg (C_2 \times 1) \amalg \cdots \amalg (C_2 \times 1)$, with $pq - 1$ copies of C_2 or in general $G_K(2)$ having any other combination of \mathbb{Z}_2 and C_2 satisfying the condition that it has $pq + 1$ generators and pq relations, even though they have the same number of required relations and generators which is exactly what we are after. The reason is the following. Suppose G is a pro- p group and $G = H \amalg F$, where H and F are pro- p groups. Then the abelianisation of G ; namely $G^{ab} = H^{ab} \times F^{ab}$. Note that the free pro- p product becomes a direct product in the abelianisation. Hence if we were to go with the above structure of $G_K(2)$, then $G_K(2)^{ab}$ would have more than one copy of \mathbb{Z}_2 . Which would imply that K has at least 2 independent \mathbb{Z}_2 -extensions. A contradiction.*

Remark 25 *The condition that h_K^+ is odd, implies that h_K is odd. Let F be the inertia field of P_K . Since K/F is totally ramified, we have that h_F is odd. Moreover 2 is inert in F . Now if $q = 2$, then $F = \mathbb{Q}(\sqrt{m})$, where m is a prime congruent to 5 mod 8.*

Example 26 *Let $f(x) = x^6 - 3x^5 - 2x^4 + 9x^3 - 5x + 1$. Let K be the splitting field of $f(x)$. One can verify (using magma) that K is real, $\text{Gal}(K/\mathbb{Q}) \cong C_3 \rtimes C_2 \cong S_3$, $h_K^+ = 1$ and that there is a unique prime above 2. Hence it satisfies the hypotheses of Theorem 3. Hence the set of number fields with the hypotheses of Theorem 3 is not an empty set. Moreover, $\text{Gal}(L/\mathbb{Q}) \cong D_{12}$.*

Example 27 *Now, going back to example 19, we have $M = \mathbb{Q}(2^{\frac{1}{4}})$. Observe that M has a real embedding. In fact M has 2 real embeddings and 2 complex embeddings. Hence M has 2 real places and 1 complex place. By (1) of Theorem 15, $G_M(2)$ has 4 generators. Hence by Burnside Basis Theorem, we have $G_M(2)/(G_M(2))^{(1)} \cong C_2 \times C_2 \times C_2 \times C_2$.*

Now, by Leopoldt's conjecture, M has exactly 2 independent \mathbb{Z}_2 -extensions. Observe that M actually satisfies Leopoldt's conjecture, because L/F is an abelian extension and by [15, Theorem 10.3.16], L satisfies Leopoldt's conjecture. Now, M being a subfield of L , satisfies Leopoldt's conjecture.

Hence $G_M(2)^{ab} \cong C_{2^k} \times C_{2^l} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, for $k, l \geq 1$. $G_M(2)$ has a free subgroup of index 2 because L/M is a 2-extension unramified outside the prime divisors of 2 and infinity and L is 2-rational. Moreover, $G_L(2)$ has 5 generators. Therefore, $G_M(2) \cong (C_2 \times 1) \amalg (C_2 \times 1) \amalg \mathbb{Z}_2 \amalg \mathbb{Z}_2$ or $(C_2 \times \mathbb{Z}_2) \amalg (C_2 \times 1) \amalg \mathbb{Z}_2$ or $(C_2 \times \mathbb{Z}_2) \amalg (C_2 \times \mathbb{Z}_2)$. Now, the first group has 2 relations, the second group has 3 relations and the third group has 4 relations. However, $G_M(2)$ has only 2 relations, whence $G_M(2) \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2 \amalg \mathbb{Z}_2$ and it is virtually free. Hence $k = l = 1$.

Example 28 *Going back to example 20, we will describe $G_{K_j}(2)$ for $1 \leq j \leq$*

3. Now, for $1 \leq j \leq 3$, each K_j has 1 real embedding and 2 complex embeddings, hence 1 real place and 1 complex place. Therefore by (1) of Corollary 16, $G_{K_j}(2)$ cannot be free. Each $G_{K_j}(2)$ has 3 generators. Hence, we have $G_{K_j}(2)/(G_{K_j}(2))^{(1)} \cong C_2 \times C_2 \times C_2$.

By Leopoldt's conjecture, K_j has exactly 2 independent \mathbb{Z}_2 -extensions. Observe that K_j actually satisfies Leopoldt's conjecture, because L/K_4 is an abelian extension, L satisfies Leopoldt's conjecture. Now, each K_j being a subfield of L , satisfies Leopoldt's conjecture. Hence $G_{K_j}(2)^{\text{ab}} \cong C_{2^k} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, for $k \geq 1$.

Note that even though L is 2-rational we cannot conclude that $G_{K_j}(2)$ is virtually free because L/K_j is ramified outside S_j , as 3 is totally ramified in L , where S_j is the set of prime divisors of 2 and the infinite primes of K_j . Hence we need to construct a 2-extension unramified outside S_j . Therefore, define $F = K_j(i); i = \sqrt{-1}$. We claim that $h_{K_j}^+$ is odd. Suppose we assume to the contrary that $h_{K_j}^+$ is even. Then there exists a degree 2-extension L_j of K_j , unramified at every finite place. Since L/K_j is ramified at a finite place, $L_j L/L$ is an unramified extension of L of degree 2. Which implies that h_L is even. A contradiction.

Since $h_{K_j}^+$ is odd, we have h_F is odd by an identical argument used in the proof of Theorem 3. Since $i \in F$, F has no real embedding, hence F is totally imaginary. Moreover, $g_2 = 1$ in F , because 2 is ramified in K_j and in $\mathbb{Q}(i)$. Hence F is 2-rational. Observe that F/K_j is unramified outside S_j , therefore $G_{K_j}(2)$ has a free pro-2 subgroup $G_F(2)$ of index 2. Moreover, $G_F(2)$ has rank 4. Hence, we have $G_{K_j}(2) \cong (C_2 \times 1) \amalg \mathbb{Z}_2 \amalg \mathbb{Z}_2$ or $(C_2 \times \mathbb{Z}_2) \amalg \mathbb{Z}_2$. Now, the first group has 1 relation and the second group has 2 relations. However, $G_{K_j}(2)$ has only 1 relation. Whence $G_{K_j}(2) \cong C_2 \amalg \mathbb{Z}_2 \amalg \mathbb{Z}_2$ and it is virtually free. Hence $k = 1$.

Remark 29 Observe that in Theorem 3, L is obtained as the compositum of K with a quadratic extension of \mathbb{Q} . Let us now look at some degree 2-extensions L of K which are not obtained as compositum of K with degree 2-extensions of \mathbb{Q} . Since $G_K(2)/(G_K(2))^{(1)} \cong C_2 \times \cdots \times C_2$ (with $pq+1$ copies of C_2), there are $pq+1$ independent degree 2-extensions of K which are unramified outside S . Since K is real (by assumption) there are $pq-1$ basis elements of the torsion free part of the units of K . Let $\varepsilon_1, \dots, \varepsilon_{pq}$ be a system of fundamental units and a generator of the cyclic subgroup (the torsion subgroup) of the units of K . Since h_K is odd, we have $P_K^{h_K}$ is principal. Let ε_{pq+1} be a generator of this ideal. Again, since h_K is odd, ε_{pq+1} is not a square in K . Observe that $-1, -2 \in \{\varepsilon_1, \dots, \varepsilon_{pq+1}\}$. Let $L = K(\sqrt{\varepsilon_i})$ be such that L is totally imaginary. Note that totally imaginary L exists, for example, $L = K(i), K(\sqrt{-2})$. Hence we have the following.

Corollary 30 *If h_K^+ is odd, then L is 2-rational*

Proof. Since ε_i is either a unit or a generator of the ideal $P_K^{h_K}$, L/K is unramified outside S_K . Since h_K^+ is odd, by an argument identical to (1) of Theorem 3, we have that h_L is odd. To show that L is 2-rational, all we have to show that there is a unique prime divisor of P_K in L . Suppose we assume to the contrary that P_K is inert or splits in L . Then L/K is an abelian extension, unramified at finite primes. Therefore h_K^+ is even. However, h_K^+ is odd. A contradiction. \square

Remark 31 *Suppose K is imaginary, then $q = 2$ and $F = \mathbb{Q}(\sqrt{-m})$, where $m \equiv 3 \pmod{8}$. If h_K is odd then K is 2-rational.*

4.2 Nonabelian metacyclic extensions of the form $G' \rtimes M$

Let $G = \text{Gal}(K/\mathbb{Q}) = G' \rtimes M$ with G' and M being cyclic, where G' denotes the commutator subgroup of G , where it is assumed that it is not a direct product. Let $|G'| = n > 1$ and $|M| = m$.

Lemma 32 $e_2 \geq n$ in K . Moreover $e_2 = n$ in K if G is not a 2-group.

Proof. Since $G = D_{P_K}$, D_{P_K}/I_{P_K} is cyclic, we have $G' \subseteq I_{P_K}$. Hence $e_2 \geq n$. If n is even and m is odd, then M will act trivially on the Sylow-2 subgroup of G' as the Sylow-2 subgroup of G' is cyclic. Hence, we can assume without loss of generality that either both n and m are of the same parity or just m is even. By Theorem 6 we have that $I_{P_K} = G'$ if G is not a 2-group. \square

Assume that n is odd. Let $L = K(i)$ or $K(\sqrt{-2})$. Then we have the following

Theorem 33 (1) *If h_K^+ is odd, then L is 2-rational, and conversely*
(2) *If L is 2-rational, then h_K is odd*

Hence $G_K(2)$ is virtually free, moreover $G_K(2) \cong C_2 \amalg \cdots \amalg C_2 \amalg \mathbb{Z}_2$ with $|G|$ copies of C_2 and $G_L(2) \cong F_2(|G| + 1)$.

Proof. The proof is identical to the proof of Theorem 3 \square

Now, let n be even. Then we have

Corollary 34 *If h_K^+ is odd, then L is 2-rational and hence $G_K(2)$ is virtually free, moreover $G_K(2) \cong C_2 \amalg \cdots \amalg C_2 \amalg \mathbb{Z}_2$ with $|G|$ copies of C_2 and $G_L(2) \cong F_2(|G| + 1)$.*

4.3 D_8 -extensions

Let $G = \text{Gal}(K/\mathbb{Q}) \cong D_8 (= C_4 \rtimes C_2)$. Observe that D_8 cannot be expressed in the form of section 4.2

Lemma 35 $e_2 = 4$ or 8 in K .

Proof. Since D_8 is not cyclic, $e_2 > 1$. Moreover D_{P_K}/I_{P_K} being cyclic, we have $G' \subseteq I_{P_K}$. But $G' \cong C_2$. However $G/G' \cong C_2 \times C_2$, hence $e_2 \geq 4$. Therefore $e_2 = 4$ or 8 . \square

Let $L = K(i)$ or $K(\sqrt{-2})$. Then we have

Theorem 36 *If h_K^+ is odd, then L is 2-rational and hence $G_K(2)$ is virtually free, moreover $G_K(2) \cong C_2 \amalg \cdots \amalg C_2 \amalg \mathbb{Z}_2$ with 8 copies of C_2 and $G_L(2) \cong F_2(9)$.*

Proof. Proof is identical to the proof of Theorem 3. \square

Suppose L/K is ramified only at the infinite place of K . Then we have the following.

Theorem 37 *If $h_K^+ \equiv 2 \pmod{4}$ and $o(P_K) \geq 2$, then L is 2-rational*

Proof. Since $h_K^+ \equiv 2 \pmod{4}$ then h_K is at most $\equiv 2 \pmod{4}$. If $o(P_K) \geq 2$, then $h_K \equiv 2 \pmod{4}$. Then by (2) of Corollary 16 we have $B_S = 0$.

Now, for the 2-rationality of L , we need to show that $g_2 = 1$ in L , and either h_L is odd or $h_L \equiv 2 \pmod{4}$ and $o(P_L) \geq 2$. Since $g_2 = 1$ in K and $g_2 = 1$ in N , we have $g_2 = 1$ in L , where $N = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$. Moreover, $o(P_K)$ and $o(P_L)$ is a power of 2 since both $[K : \mathbb{Q}]$ and $[L : \mathbb{Q}]$ are powers of 2. Note that L/K is unramified outside S , since N/\mathbb{Q} is unramified outside $\{2, \infty\}$.

Since L/K is ramified only at the infinite place of K , we have that $\mathcal{K}^+ = L$, where \mathcal{K}^+ is the extended Hilbert 2-class field of K . We claim that h_L is odd. Let us assume to the contrary that h_L is even. Let \mathcal{L} be the Hilbert 2-class field of L . Since L/K is Galois, the maximality of \mathcal{L} implies that \mathcal{L}/K is Galois. Note that $\text{Gal}(\mathcal{L}/K)$ is a 2-group of order at least 4. Therefore $\text{Gal}(\mathcal{L}/K)$ has a normal subgroup of index 4. Hence, K has a degree 4 abelian extension contained in \mathcal{L} . This implies that $4 \mid h_K^+$. A contradiction. Hence h_L is odd and by Corollary 16, L is 2-rational. \square

5 On Q_8 -extensions

In this section we look at a nonsplit metacyclic extension. Let $G = \text{Gal}(K/\mathbb{Q}) = Q_8$, the quaternion group of order 8. Note that since every subgroup of order 4 is cyclic with cyclic quotient, so Q_8 is metacyclic but not split, since the cyclic quotients of order 2 do not lift to a complement.

Lemma 38 $e_2 = 4$ or 8 in K .

Proof. Proof is identical to the proof of Lemma 35. \square

Let $L = K(i)$ or $K(\sqrt{-2})$. Then we have

Theorem 39 *If h_K^+ is odd, then L is 2-rational and hence $G_K(2)$ is virtually free, moreover $G_K(2) \cong C_2 \amalg \cdots \amalg C_2 \amalg \mathbb{Z}_2$ with 8 copies of C_2 and $G_L(2) \cong F_2(9)$.*

Proof. Proof is identical to the proof of Theorem 3. \square

Suppose that L/K is ramified only at the infinite place of K .

Theorem 40 *If $h_K^+ \equiv 2 \pmod{4}$ and $o(P_K) \geq 2$, then L is 2-rational*

Proof. Proof is identical to the proof of Theorem 37. \square

6 On A_4 -extensions

In this section we look at a non metacyclic extension. Let $G = \text{Gal}(K/\mathbb{Q}) = A_4 \cong K_4 \rtimes C_3$. Note that A_4 is not metacyclic, as it has no, non trivial, normal cyclic subgroup.

Lemma 41 $e_2 = 4$ in K .

Proof. Since A_4 is not cyclic, $e_2 > 1$. Moreover D_{P_K}/I_{P_K} being cyclic, we have $G' \subseteq I_{P_K}$. But $G' \cong K_4$, hence $e_2 \geq 4$ in K . Observe that A_4 has no subgroup of order 6, hence $e_2 = 4$ or 12 in K .

Now, $\text{Fix}(K_4)/\mathbb{Q}$ is a normal extension of degree 3. Hence $\text{Fix}(K_4) \subseteq \mathbb{Q}(\zeta_m)$, where m is odd. Since we assume that $g_2 = 1$ in K , we have $f_2 = 3$ in $\text{Fix}(K_4)$. Therefore $e_2 = 4$ in K . \square

Let $L = K(i)$ or $K(\sqrt{-2})$. Then we have

Theorem 42 *If h_K^+ is odd, then L is 2-rational and hence $G_K(2)$ is virtually*

free, moreover $G_K(2) \cong C_2 \amalg \cdots \amalg C_2 \amalg \mathbb{Z}_2$ with 8 copies of C_2 and $G_L(2) \cong F_2(9)$.

Proof. Proof is identical to the proof of Theorem 3. \square

Suppose that L/K is ramified only at the infinite place of K .

Theorem 43 *If $h_K^+ \equiv 2 \pmod{4}$ and $o(P_K) \geq 2$, then L is 2-rational*

Proof. Proof is identical to the proof of Theorem 37. \square

References

- [1] G. Gras, Logarithme p -adique et groupes de Galois, *J. reine angew. Math.* **343** (1982), 64-80.
- [2] G. Gras, J.F. Jaulent, Sur les corps de nombres réguliers, *Math. Z.* **202** (1989), no. 3, 343-365.
- [3] W.N. Herfort, L.Ribes, and P.A. Zalesskii, p -Extensions of free pro- p groups, *Forum Mathematicum* (11) (1999), 49-61
- [4] J. F. Jaulent, T. Nguyen Quang Do, Corps p -rationnels, corps p -réguliers et ramification restreinte, *J. Théor. Nombres Bordeaux* **5** (1993), no.2, 343-363.
- [5] J. F. Jaulent, O. Sauzet, Pro- l -extensions de corps de nombres l -rationnels, *J. Number Th.* **65** (1997), 240-267.
- [6] J. F. Jaulent, O. Sauzet, Extensions quadratiques 2-birationnelles de corps de nombres totalement réels, *Pub. Matemtiques* **44** (2000), 343-351.
- [7] D. L. Johnson, *Topics in the Theory of Group Presentations*, Cambridge university press 1980.
- [8] J. Jossey, Galois 2-extensions unramified outside 2. *Journal of Number Theory*, **124** (1):42-56, 2007
- [9] H. Koch, *Galoissche Theorie der p -Erweiterungen*. Deutscher Verlag der Wissenschaften, Berlin 1970.
- [10] H. Koch, *Galois Theory of p -Extensions*, Springer 2002.
- [11] G. N. Markshaitis, On p -extensions with one critical number.(Russian) *Izv. Akad. Nauk SSSR Ser. Mat.* 27 1963 463 – 466.
- [12] H. Miki, On the maximal abelian l -extension of a finite algebraic number field with given ramification, *Nagoya Math. J.* 70 (1978), 183-202.
- [13] A. Movahhedi, Sur les p -extensions des corps p -rationnels. *Math Nachr.* **149** (1990), 163-176.
- [14] A. Movahhedi, T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p -rationnels, *Séminaire de Théorie des Nombres, Paris 1987-88, Prog. Math.*, **89**, (1990) 155-200.
- [15] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Springer 1999.
- [16] L. Ribes, P. Zalesskii, *Profinite Groups*, Springer 2000.
- [17] J.P. Serre, *Galois Cohomology*, Springer 2002.
- [18] J. P. Serre, *Local Fields*, Springer-Verlag 1979.
- [19] J.P. Serre, *Trees*, Springer-Verlag 1980.

- [20] L.C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag 1982.
- [21] K. Wingberg, On Demuskin groups with involution. Ann. Sci. cole Norm. Sup. (4) 22 (1989), no. 4, 555–567.
- [22] P.A. Zalesskii, On virtually projective groups, J. reine angew. Math. 572 (2004), 97-110