

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 $\text{Gal}(K(p)/K)$.

Markshaitis proved that $G_{\mathbb{Q}}(2)$ is a free product (in the category of pro-2 groups) of a cyclic group of order 2 and a free rank 1 pro-2 group. We will generalize this result to totally imaginary extensions of \mathbb{Q} with odd class number and with a unique prime above 2, and give an elementary proof using his techniques.

We then classify quadratic, biquadratic and degree 4 cyclic 2-rational number fields, where 2-rational number fields K are those for which $G_K(2)$ is free. We use Dirichlet characters to capture the cyclic 2-rational number fields. We also classify those quadratic number fields which are not 2-rational, but have a degree 2-extension, which is Galois over \mathbb{Q} and is 2-rational. Then we give an explicit description of the structure of $G_K(2)$ using a result of Herfort-Ribes-Zaleskii on pro- p groups. We use magma to show the existence of certain degree 4, cyclic, 2-rational number fields with some class number condition.

Finally, we look at some nonabelian, real, Galois extensions K of \mathbb{Q} , such that $G_K(2)$ is not free but has a free subgroup of index 2. In particular we focus on finite split metacyclic extensions and again we explicitly describe the structure of $G_K(2)$.

Table of Contents

| | | |
|------------------|---|-----------|
| Chapter 1 | Introduction | 1 |
| Chapter 2 | Preliminaries | 4 |
| 2.1 | Number Theory | 4 |
| 2.1.1 | Class field theory | 4 |
| 2.1.2 | Genus theory. | 6 |
| 2.1.3 | Class number parity. | 8 |
| 2.1.4 | Leopoldt's conjecture. | 9 |
| 2.1.5 | Dirichlet Characters. | 10 |
| 2.2 | Group Theory | 11 |
| 2.2.1 | Pro- p groups | 12 |
| 2.2.2 | Galois cohomology | 15 |
| 2.2.3 | B_S | 16 |
| Chapter 3 | An extension of a result of Markshaitis | 20 |
| 3.1 | $G(\mathbb{Q}_S(p)/\mathbb{Q})$, where $S = \{q, \infty\}$ | 20 |
| 3.2 | Markshaitis's result | 22 |
| 3.3 | Generalization | 22 |
| Chapter 4 | 2-rational degree 2 and degree 4-extensions | 32 |
| 4.1 | Quadratic extensions | 33 |
| 4.2 | Degree 4-extensions | 34 |
| 4.2.1 | Cyclic extensions | 34 |
| 4.2.2 | Biquadratic extensions | 41 |
| 4.2.3 | Virtually free extensions | 46 |
| 4.2.4 | Minimal 2-rational extensions | 47 |
| 4.2.5 | Cyclic extension revisited | 47 |
| Chapter 5 | Some nonabelian extensions K of \mathbb{Q} with a virtually free $G_K(2)$ | 56 |
| 5.1 | Nonabelian examples of 2-rational number fields | 56 |
| 5.2 | On split metacyclic extensions | 58 |
| 5.2.1 | Nonabelian extensions of order pq | 58 |
| 5.2.2 | Nonabelian metacyclic extensions of the form $G' \rtimes M$ | 64 |
| 5.2.3 | D_8 -extensions | 65 |
| 5.3 | On Q_8 -extensions | 66 |

| | |
|------------------------------------|-----------|
| 5.4 On A_4 -extensions | 67 |
| References | 69 |

Chapter 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 $\text{Gal}(K(p)/K)$. 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 [13, Corollary 8.7.10]. Also K.Wingberg [19] 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).

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 this thesis we find fields solving (\mathcal{Q}_1) for $p = 2$. i.e., number fields K for which $G_K(2)$ is not free but contains a free pro-2 subgroup of index 2. We classify quadratic, biquadratic and degree 4 cyclic number fields whose $G_K(2)$ is free. We also classify those quadratic number fields K for which $G_K(2)$ is not free, but has a degree 2-extension L , which is Galois over \mathbb{Q} and whose $G_L(2)$ is free. In this case we explicitly describe the Galois group of their maximal pro-2 extension unramified outside 2 and infinity using a result of Herfort-Ribes-Zaleskii (Theorem 2.2.6) on pro- p groups. We also find some split metacyclic extensions of \mathbb{Q} solving (\mathcal{Q}_1) for $p = 2$.

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.

In Chapter 3 we generalize a result of Markshaitis. In section 3.2, we state a result of Markshaitis, which describes $G_{\mathbb{Q}}(2)$. In section 3.3, we will extend this result to imaginary extensions of \mathbb{Q} with certain conditions on the class number and on the number of prime divisors of 2 (Theorem 3.3.1), which is the main result in this chapter. We give an elementary proof employing similar techniques as Markshaitis's without appealing to Theorems 2.2.6 and 2.2.13. The reason why the proof works is because the number of generators of certain groups and the degree of extension of certain number fields satisfy the same type of recursive relation.

Our main results are in Chapter 4. In Chapter 4 we classify quadratic, biquadratic and degree 4 cyclic 2-rational (Definition 4.0.5) number fields. We also classify those quadratic number fields which are not 2-rational, but has a degree 2-extension, which is Galois over \mathbb{Q} and is 2-rational. In this case we explicitly describe $G_K(2)$ using a result of Herfort-Ribes-Zaleskii (Theorem 2.2.6) on pro- p groups. We appeal to Corollary 2.2.14, which is crucial in showing the 2-rationality of number fields.

In section 4.1 we classify all the quadratic 2-rational number fields. In section 4.2 we classify all 2-rational biquadratic and cyclic degree 4-extensions of \mathbb{Q} . We use Dirichlet characters, to capture some of the degree 4 cyclic number fields with certain conditions, also we use magma to show the existence of the above fields. Theorems 4.1.1, 4.2.1 and 4.2.2 are the main results in this Chapter.

All the number fields considered in Chapter 4 are abelian. Hence, in Chapter 5 we study some nonabelian extensions K of \mathbb{Q} which are solutions of (\mathcal{Q}_1) for $p = 2$. In particular we concentrate 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 . Let g_2 denote the number of prime divisors of 2.

Under the assumption that $g_2 = 1$ 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. Theorem 5.2.3 is the main result in this chapter.

We also look at a non split metacyclic extension of \mathbb{Q} ; namely Q_8 -extensions (section 5.3). Finally in section 5.4, we look at a non metacyclic extension; namely A_4 .

Chapter 2

Preliminaries

In this chapter, we collect all the definitions and results from group theory and number theory which will be needed later on.

2.1 Number Theory

2.1.1 Class field theory

A number field K is a finite extension of \mathbb{Q} . The ring of integers \mathcal{O}_K of K is the integral closure of \mathbb{Z} in K . It is a Dedekind domain and a free \mathbb{Z} -module. Let U_K denote the group of units of K , i.e., the invertible elements of \mathcal{O}_K . A fractional ideal of K is a finitely generated \mathcal{O}_K -submodule $I \subseteq K$. A non-zero principal fractional ideal is a fractional ideal generated by a single element of K . The fractional ideals form an abelian group $I(K)$ with the operation of ideal multiplication. The principal fractional ideals form a subgroup $P(K)$ of $I(K)$. The ideal class group $Cl(K)$ of K is defined to be the quotient $I(K)/P(K)$.

Theorem 2.1.1. *The abelian group $Cl(K)$ is finite for any number field K .*

Let L/K be a finite extension. Let \wp be a prime ideal of \mathcal{O}_K . Since \mathcal{O}_L is a Dedekind domain, every fractional ideal can be factored uniquely into a product of prime ideals. Suppose we have

$$\wp \mathcal{O}_L = \prod_{i=1}^n \mathcal{P}_i^{e(\mathcal{P}_i)}$$

where \mathcal{P}_i are prime ideals of \mathcal{O}_L . We say that \wp is unramified in L/K , if $e(\mathcal{P}_i) = 1$ for all i .

Theorem 2.1.2. *Let r and $2s$ denote the number of real and non-real embeddings of K in \mathbb{C} . Then $U_K = \mu_K \times V_K$, where μ_K, V_K denote the roots of unity and a free abelian group of rank $r + s - 1$ in K , respectively.*

Proof. See [10, Theorem 38] □

Definition 2.1.3. *A finite extension L/K is unramified if it is unramified at every finite prime \wp of \mathcal{O}_K and also at the completion of L and K with respect to any archimedean valuation of L .*

Since the composite of unramified extensions is unramified and the composite of abelian extensions is abelian, the following is well defined

Definition 2.1.4. *The Hilbert class field \mathcal{K} of a number field K is the maximal abelian unramified extension of K .*

Theorem 2.1.5. *Let \mathcal{K} be the Hilbert class field of a number field K . The Artin reciprocity map induces an isomorphism $Cl(K) \cong \text{Gal}(\mathcal{K}/K)$.*

Let h_K denote the class number of K . Since $Cl(K)$ is finite, we have \mathcal{K}/K is a finite extension. For a rational prime p , we define the p -class group of K to be the Sylow p -subgroup of the abelian group $Cl(K)$. This group is isomorphic to $\text{Gal}(\mathcal{K}_1/K)$, where \mathcal{K}_1 is the maximal unramified abelian p -extension of K also called the Hilbert p -class field of K .

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 2.1.6. *The subgroup $D_{\mathcal{P}}$ of $\text{Gal}(L/K)$ such that $\{\sigma \mid \sigma \in \text{Gal}(L/K) : \sigma(\mathcal{P}) = \mathcal{P}\}$ is called the **decomposition group** of \mathcal{P} .*

Definition 2.1.7. *The subgroup $I_{\mathcal{P}}$ of $\text{Gal}(L/K)$ such that $\{\sigma \mid \sigma \in D_{\mathcal{P}} : \sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}}, \forall \alpha \in \mathcal{O}_L\}$ 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_\wp , the inertial degree of \mathcal{P} in L/K . Let p be the characteristic of the residue field \mathcal{O}_K/\wp

Theorem 2.1.8. *$I_{\mathcal{P}}$ is the semi direct product of a p -group with a cyclic group of order prime to p .*

Proof. See [16, Chapter IV, Corollary 4 to Proposition7] □

Proposition 2.1.9. *Suppose L/K is a totally ramified extension at some prime. Then $h_K|h_L$*

Proof. See [18, Proposition 4.11] Observe that LK/L is an unramified abelian extension of L . Hence $LK \subseteq \mathcal{L}$. Since L/K is totally ramified at some prime, $\mathcal{K} \cap L = K$. Therefore $[\mathcal{K} : K] = [LK : L]$. Hence $h_K|h_L$. □

Theorem 2.1.10. *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 $p|h_K$.*

Proof. See [18, Theorem 10.4]. Suppose $p | h_L$. Let \mathcal{L}_1 be the Hilbert p -class field of L . By maximality of \mathcal{L}_1 over L , \mathcal{L}_1 is Galois over K . Suppose \wp is a prime of K which ramifies in L , and let \mathcal{P} denote a prime divisor of \wp in \mathcal{L}_1 . Let $G = \text{Gal}(\mathcal{L}_1/K)$, and let $I_{\mathcal{P}} \subseteq G$ denote the inertia group for \mathcal{P} . Now, $|I_{\mathcal{P}}| < |G|$. Since G is a p -group, there exists a normal subgroup \tilde{G} of G of index p such that $I_{\mathcal{P}} \subseteq \tilde{G}$. Since the other primes of \mathcal{L}_1 above \wp are conjugate to \mathcal{P} , their inertia groups are conjugates of $I_{\mathcal{P}}$, hence are in \tilde{G} . Let $\text{Fix}(\tilde{G})$ denote the fixed field of \tilde{G} . Now $\text{Fix}(\tilde{G})/K$ is an unramified extension of degree p . Hence $p | h_K$. □

2.1.2 Genus theory.

Definition 2.1.11. *If K is any finite abelian extension of \mathbb{Q} , the genus field \hat{K} of K is the largest abelian extension of \mathbb{Q} contained in the Hilbert class field \mathcal{K} of K . The extended*

genus field $\hat{K}^{(+)}$ of K is the largest abelian extension of \mathbb{Q} contained in the extended Hilbert class field $\mathcal{K}^{(+)}$, where $\mathcal{K}^{(+)}$ is the maximal abelian extension of K unramified at the finite primes of K .

Theorem 2.1.12. *Let $K = \mathbb{Q}(\sqrt{d})$ have discriminant Δ where $|\Delta| = p_1 p_2 \dots p_t$ with $p_2 \dots p_t$ odd primes and p_1 is either an odd prime or a power of 2. Then the extended genus field is*

$$\hat{K}^{(+)} = \mathbb{Q}(\sqrt{d}, \beta_2, \dots, \beta_t)$$

where

$$\beta_i = \begin{cases} \sqrt{p_i} & \text{if } p_i \equiv 1 \pmod{4} \\ \sqrt{-p_i} & \text{if } p_i \equiv 3 \pmod{4} \end{cases}$$

Proof. See [5, Chapter VI, Theorem 3.8] □

Consequently,

Theorem 2.1.13. *If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic extension of \mathbb{Q} and if the discriminant Δ_K is divisible by exactly t different primes, then $[\hat{K}^{(+)} : K] = 2^{t-1}$*

Proof. See [5, Chapter VI, Theorem 3.9] □

Note that $[\hat{K}^{(+)} : \hat{K}] \leq 2$. If K is complex or if K is real and some unit of the ring of algebraic integers of K has norm -1 , then $\hat{K}^{(+)} = \hat{K}$ and then $\text{Gal}(\hat{K}/K) \cong \text{Cl}(K)/\text{Cl}^2(K)$. Hence we have that $h_{\mathbb{Q}(\sqrt{d})}$ is even if $d < 0$ and the discriminant of $\mathbb{Q}(\sqrt{d})$ has more than one prime factor. Therefore $\mathbb{Q}(\sqrt{-p})$ where p is a prime $\equiv 1 \pmod{4}$ or $\mathbb{Q}(\sqrt{-2p})$, where p is an odd prime, have even class number. If $d > 0$ and discriminant of $\mathbb{Q}(\sqrt{d})$ has more than two prime factors then class number of $\mathbb{Q}(\sqrt{d})$ is necessarily even.

More precisely we have the result

Theorem 2.1.14. *The class number of a quadratic number field K is odd if and only if*

1. $K = \mathbb{Q}(\sqrt{-1})$;
2. $K = \mathbb{Q}(\sqrt{p})$, p any prime;
3. $K = \mathbb{Q}(\sqrt{-p})$, p a prime $\equiv 2, 3 \pmod{4}$;
4. $K = \mathbb{Q}(\sqrt{pq})$, p and q distinct primes, $p \equiv 3 \pmod{4}$ and $q \equiv 2, 3 \pmod{4}$.

Proof. See [2, Corollary to Theorem 2.17] or [1, corollary 18.4] □

Theorem 2.1.15. *Let L/\mathbb{Q} be a cyclic extension of \mathbb{Q} of degree l^n , l a prime. Let p_i , $1 \leq i \leq t$ be the finite set of primes, ramified in L , of ramification degrees l^{n_i} , $n_1 \geq n_2 \geq \dots \geq n_t \geq 1$. Then $\text{Gal}(\hat{L}^{(+)} / L)$ is abelian of type $(l^{n_2}, \dots, l^{n_t})$.*

Proof. See [2, Theorem 2.16] □

Let $C(K)$ denote the idele class group of K . If L/K is a finite Galois extension, let $\Phi(L/K)$ denote the character group of $C(K)/N_{L/K}(C(L))$.

Theorem 2.1.16. *Let L/\mathbb{Q} be a cyclic extension of degree 2^n ($n \geq 1$). Then h_L is odd if and only if one of the following conditions hold.*

1. *Precisely one finite rational prime is ramified in L*
2. *L is real and precisely two rational primes p and q are ramified in L of ramification degrees 2^n , and 2, respectively and furthermore either $q \equiv -1 \pmod{4}$, or $q = 2$ and $\phi((-1)_2) = -1$, where ϕ is the generator of $\Phi(L/K)$*

Proof. See [2, Theorem 2.17] □

2.1.3 Class number parity.

Proposition 2.1.17. *Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic extension of \mathbb{Q} . Then $h_K \equiv 2 \pmod{4}$ if and only if*

1. $d = -p, -2p$, where p is prime congruent to $5 \pmod{8}$
2. $d = -2q$ where q is a prime congruent to $3 \pmod{8}$
3. $d = -pq$ with $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = -1$ where p is a prime $\equiv 3 \pmod{4}$ and q is a prime $\equiv 1 \pmod{4}$
- 4.

Proof. See [1, Corollary 19.6] □

Proposition 2.1.18. *For a real quadratic extension $K = \mathbb{Q}(\sqrt{d})$ with fundamental unit of norm -1 , $h_K \equiv 2 \pmod{4}$ if and only if*

1. $d = 2q$, with $q \equiv 5 \pmod{8}$
2. $d = q_1q_2$ with $\left(\frac{q_2}{q_1}\right) = \left(\frac{q_1}{q_2}\right) = -1$

where q, q_1, q_2 are primes $\equiv 1 \pmod{4}$.

Proof. See [1, Corollary 19.8] □

Proposition 2.1.19. *Let $K = \mathbb{Q}(\sqrt{2q})$ or $\mathbb{Q}(\sqrt{q_1q_2})$ with primes $q, q_1, q_2 \equiv 1 \pmod{4}$ satisfying $q \equiv 5 \pmod{8}$ or $\left(\frac{q_2}{q_1}\right) = \left(\frac{q_1}{q_2}\right) = -1$. Then the norm of the fundamental unit of K is -1 .*

Proof. See [1, Proposition 19.9] □

2.1.4 Leopoldt's conjecture.

Let $\{\epsilon_1, \dots, \epsilon_{r+s-1}\}$ be a basis of U_K modulo its torsion subgroup, where r is the number of real places of K and s is the number of complex places of K . Let $\sigma_1, \dots, \sigma_d$ be elements of $\text{Hom}(K, \mathbb{C}_p)$, with $d = [K : \mathbb{Q}]$.

Definition 2.1.20. Regulator matrix

$$\mathcal{R}_p(\epsilon_1, \dots, \epsilon_{r+s-1}) := \begin{pmatrix} \log_p \sigma_1(\epsilon_1) & \cdots & \log_p \sigma_d(\epsilon_1) \\ \vdots & \ddots & \vdots \\ \log_p \sigma_1(\epsilon_{r+s-1}) & \cdots & \log_p \sigma_d(\epsilon_{r+s-1}) \end{pmatrix}$$

where $\log_p : \mathbb{C}_p^\times \rightarrow \mathbb{C}_p^\times$ is the p -adic logarithm.

Conjecture 2.1.21. Leopoldt's conjecture. [13] *For every number field K and every prime number p , the p -adic regulator rank $\text{rr}_p(K) := \text{rank } \mathcal{R}_p(\epsilon_1, \dots, \epsilon_{r+s-1}) = r + s - 1$.*

Another formulation of the Leopoldt's conjecture, which we will be using is that there are exactly $s + 1$ independent \mathbb{Z}_p -extensions of K .

Leopoldt's conjecture has been proved in certain instances.

Theorem 2.1.22. *Assume that the number field K is an abelian extension of \mathbb{Q} or of an imaginary quadratic number field. Then Leopoldt's conjecture holds for K and every prime p .*

Proof. See [13, Theorem 10.3.16] □

Theorem 2.1.23. *Assume that Leopoldt's conjecture is true for the prime number p and the number field K . Then it is also true for p and every subfield F of K .*

Proof. See [13, Proposition 10.3.13] □

2.1.5 Dirichlet Characters.

A Dirichlet character is a multiplicative homomorphism $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. The conductor of χ is the minimal n for which the map χ is defined. If χ is a character defined mod n , then χ is a character of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let K be the fixed field of the kernel of χ . Then K is called the field belonging to χ and $\deg(K/\mathbb{Q}) = \text{order of } \chi$. If $n = \prod p^a$, then we may write any character χ defined mod n as $\chi = \prod \chi_p$, where χ_p is a character defined mod p^a . If X is a group of Dirichlet characters, then denote $X_p = \{\chi_p | \chi \in X\}$. A character is called even if $\chi(-1) = 1$ and odd if $\chi(-1) = -1$. The field belonging to χ is real if and only if χ is even.

Theorem 2.1.24. *Let X be a group of Dirichlet characters and K the associated field. Let p be a prime number with ramification index e_p in K . Then $e_p = \#(X_p)$.*

Proof. See [18, Theorem 3.5]. $K \subseteq \mathbb{Q}(\zeta_n)$, where n is the least common multiple of the conductors of the characters of X . Write $n = p^a m$, where $(p, m) = 1$. Let $L = K(\zeta_m)$. Then the group of characters of L is generated by X_p and the characters of $\mathbb{Q}(\zeta_m)$. Hence $L = F(\zeta_m)$, where $F \subseteq \mathbb{Q}(\zeta_{p^a})$, the field of X_p . Since p is unramified in $\mathbb{Q}(\zeta_m)$, the ramification index of p in K is the same as the ramification index of p in L . Since L/F is unramified for p , $[F : \mathbb{Q}] = e_p = \#(X_p)$. \square

2.2 Group Theory

Definition 2.2.1. [6] *A finite group G is **metacyclic** if it has a cyclic normal subgroup H such that G/H is cyclic.*

Example 2.2.1. *Let $H = \langle h \rangle$ and $M = \langle m \rangle$ be cyclic groups of prime orders p and q respectively such that $q \mid p - 1$. The group $G = H \rtimes_{\theta} M$ is a metacyclic group, where $\theta : M \rightarrow \text{Aut}(H)$ defined by $\theta(m) = \{h \mapsto h^s\}$, where s is an integer such that $p \nmid s - 1$ and $s^q \equiv 1 \pmod{p}$.*

More explicitly, if we denote h for (h, e) , m for (e, m) and e for (e, e) , then $H \rtimes_{\theta} M = \{(h, m) \mid h^p = m^q = e, mh = h^s m\}$ where s is an integer such that $p \nmid s - 1$ and $s^q \equiv 1 \pmod{p}$.

Example 2.2.2. *The dihedral group $D_{2n} = C_n \rtimes_{\theta} C_2$, where $n > 1$ and θ acts by inversion.*

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

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

2.2.1 Pro- p groups

Let p be a rational prime.

Definition 2.2.2. *A profinite group is a Hausdorff, compact, totally disconnected topological group. A pro- p group is a profinite group in which every open subgroup has a power of p index.*

Proposition 2.2.3. *If G is a pro- p group then*

$$G \cong \varprojlim G/U$$

where the limit is taken over all open normal subgroups U of p power index in G . Moreover the isomorphism is also a homeomorphism.

Definition 2.2.4. [17, p.121] *A pro- p group G is virtually free if G has an open free subgroup.*

Let $\{G_i | i = 1, \dots, n\}$ 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 2.2.5. [14, 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 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” [17].

Theorem 2.2.6. *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 subgroups of F and X is the space of conjugacy classes of subgroups of order p in G .

We give an outline of the proof.

Proof. See [4, Theorem 1] and [20]. In [4], the above theorem is stated without the restriction of F having a countable rank. In [20], P.A. Zalesskii 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.

Consider the natural action of G on T , the set of all subgroups of G of order p , on the right given by $tg := t^g$ for $t \in T$ and $g \in G$. Denote the quotient space by T/G , the stabilizer of $t \in T$ by G_t , and the orbit of $t \in T$ by $\dot{t} = tG$.

We say that a system $\{G_t | t \in T\}$ of subgroups of a pro- p group G is continuous if for every open neighborhood U of the identity in G , the set $T(U) = \{t \in T | G_t \subseteq U\}$ is open in T .

The main ingredient of the above theorem is the following result of Mel'nikov.

Theorem 2.2.7. [4, Theorem 4.2] *Let G be a pro- p group, and $\{G_s | s \in S\}$ be a continuous system of subgroups of G , for some boolean space S . Then the following are equivalent:*

1. G is a free pro- p product

$$G = \left(\coprod_{s \in S} G_s \right) \coprod H$$

where H is a free pro- p group.

2. The map

$$\text{Cor} : \bigoplus_{s \in S} H_q(G_s, \mathbb{F}_p) \rightarrow H_q(G, \mathbb{F}_p)$$

is injective for $q = 1$ and surjective for $q = 2$.

The condition 2 of the above theorem is satisfied if there exists a continuous section $\sigma : T/G \hookrightarrow T$.

It is not true that if a profinite group G acts continuously on a boolean space T , then the quotient map $T \rightarrow T/G$ has a continuous section. A major part of [4] is on proving the existence of a continuous section. Hence it can be shown that $G = L \coprod H$, where

$$L = \prod_{i \in T/G} (C_p \times H_{\sigma(i)})$$

□

Let $G^{(1)}$ denote the Frattini subgroup of G , i.e., the intersection of the kernels of the continuous homomorphisms $G \rightarrow \mathbb{F}_p$. Therefore $G^{(1)} = \overline{G^p[G, G]}$ where $\overline{[G, G]}$ denotes the closure of the commutator subgroup of G . If $G^{(i-1)}$ is defined then $G^{(i)} = (G^{(i-1)})^{(1)}$. Since $G^{(i)}$ form a decreasing sequence of closed normal subgroups of G and $\bigcap G^{(i)} = 1$, we have

$$G = \varprojlim G_i$$

where $G_i = G/G^{(i)}$. Since G is pro- p group, each $G^{(i)}$ is a pro- p group. Hence $G^{(i+1)}$ is the smallest normal subgroup N_i of $G^{(i)}$ such that $G^{(i)}/N_i$ is elementary abelian.

Theorem 2.2.8. (*Burnside Basis Theorem*) *Let G be a pro- p group and let $E = \{s_i | i \in I\}$ a subset of G , such that every neighborhood of $1 \in G$ contains almost all elements of E . Then E is a system of generators of G if and only if $\{s_i G^{(1)} | i \in I\}$ generates $G/G^{(1)}$.*

Proof. See [7 or 8 Theorem 4.10]. Assume that $\{s_i G^{(1)} | i \in I\}$ generates $G/G^{(1)}$. Let $F(I)$ denote the free pro- p groups with system of generators $\{s_i | i \in I\}$. Then there exists a morphism $\phi : F(I) \rightarrow G$ corresponding to the system of generators E which induce an epimorphism $\phi^* : F(I)/F(I)^{(1)} \rightarrow G/G^{(1)}$, where the group $F(I)$ is the free pro- p group with system of generators $E = \{s_i | i \in I\}$. Now, we have to show that ϕ is a surjection. Suppose it is not a surjection. Then there exists an open normal subgroup H of G such that $\phi(F(I))H/H \neq G/H$. Hence $\phi(F(I))H/H$ is contained in a normal subgroup G'/H of

index p in G/H . This implies that $G^{(1)} \subseteq G'$ and $\phi^*(F(I)/F(I)^{(1)}) \subseteq G'/G^{(1)}$, i.e., ϕ^* is not a surjection. A contradiction. The converse is obvious. \square

Finally a formula for the rank of a subgroup of finite index in a free pro- p group

Theorem 2.2.9. (*Schreier's Theorem*) *If H is a subgroup of finite index j in a free pro- p group G of finite rank n , then H is also free of rank*

$$k = 1 + j(n - 1)$$

Proof. See [7] or [8] \square

2.2.2 Galois cohomology

Let G be a profinite group and A a (left) G -module. If U is an open subgroup of G , we denote $A^U = \{a \in A \mid ga = a \forall g \in U\}$. We shall consider only G -modules A satisfying the condition $A = \cup A^U$, where the union is taken over all open normal subgroups of G . Then A is called a discrete G -module.

Let $C^n(G, A)$ denote the set of all continuous mappings from G^n into A and define a coboundary $d : C^n(G, A) \rightarrow C^{n+1}(G, A)$ by the formula:

$$(df)(g_1, \dots, g_{n+1}) = g_1 \cdot f(g_2, \dots, g_{n+1}) + \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) + (-1)^{n+1} f(g_1, \dots, g_n)$$

This yields a complex $C^\cdot(G, A)$ and the homology groups of it are the Galois cohomology groups $H^q(G, A)$.

Let G be a 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 $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$ [15].

2.2.3 B_S

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

We have a homomorphism

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

where G_{\wp} is Galois group of the maximal p -extension of K_{\wp} and K_{\wp} is the completion of K at \wp .

We set

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

Definition 2.2.10. *Let*

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

where

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

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

Theorem 2.2.11. *Suppose $\mu_p \subset K$. Then $\mathfrak{W}^2(G_K(p), \mathbb{F}_p) \cong B_S$ and there exists a map*

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

such that the sequence

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

is exact.

Proof. See [7 or 8, Theorem 13.8] □

Remark 2.2.12. When $B_S = 0$, the map res^2 is injective, hence all the global relations come from the local relations.

Theorem 2.2.13. 1.

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

where

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

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.

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

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

Proof. See [13, Theorem 8.7.3] or [7 or 8, Theorem 11.8 and Theorem 11.5] The second assertion follows from Theorem 2.2.11. □

The following corollary is crucial for proving theorems in Chapter 4 and 5.

Corollary 2.2.14. *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_φ . Hence $\delta = \delta_\varphi = 1$. Using (2) of Theorem 2.2.13 we see that $G_K(2)$ is free if and only if $\dim_{\mathbb{F}_2} B_S = 0$ and

$$\sum_{\varphi \in S \setminus S_c} \delta_\varphi = \delta$$

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 2.2.13 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 frequently referred to in Chapter 4 and is used in particular for obtaining the 2-rationality of number fields in Theorem 4.2.2.

Lemma 2.2.15. *Let L be a finite normal p -extension of a number field K in which at most divisors of p and infinity ramify. Let $G_K(p)$ (resp. $G_L(p)$) be $\text{Gal}(K(p)/K)$ (resp. $\text{Gal}(K(p)/K)$) 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.*

Proof. $K(p)$ is the compositum of all normal extensions of K , with p -power degree unramified outside the prime divisors of p and the infinite primes of K , inside a fixed algebraic closure

of K . Now, $K(p)$ is closed with respect to p -extensions, i.e., if F is p -extension of $K(p)$, unramified outside the prime divisors of p and infinity in $K(p)$, then so are the conjugates of F over K . Hence the normal closure N of F/K is a p -extension unramified outside the prime divisors of p and infinity. Therefore $N = F = K(p)$. This implies that for a finite normal p -extension L of K unramified outside the prime divisors of p and infinity, $L(p) = K(p)$. Hence by Galois theory, $G_L(p)$ is a subgroup of $G_K(p)$ and has index $[L : K]$. Moreover if $G_K(p)$ is a free pro- p group, then $G_L(p)$ is a free pro- p group. \square

Definition 2.2.16. [15, p.17] *Let p be a prime number and G a profinite group. One calls the p -cohomological dimension of G , and uses the notation $cd_p(G)$, to denote the lower bound of the integers n which satisfy the following condition: For every $q > n$, the elementary abelian p -group $H^q(G, F_p)$ is zero. One defines the cohomological dimension to be $cd(G) = \sup cd_p(G)$*

Cohomological dimension measures the degree of freeness of a pro- p group. A pro- p group $G \neq 1$ is a free pro- p group if and only if $cd(G) = 1$. If G has an element of order p , then $cd_p(G) = \infty$, hence $cd(G) = \infty$.

Chapter 3

An extension of a result of Markshaitis

In this chapter we extend a result of Markshaitis. In section 3.1, we will describe the Galois group of the maximal pro- p extension of \mathbb{Q} unramified outside $\{q, \infty\}$. In [11], Markshaitis gave an explicit description of $G_{\mathbb{Q}}(2)$ without appealing to Theorem 2.2.6 and Theorem 2.2.13. In section 3.3 we will generalize his result and give an elementary proof using his technique.

Let $S = \{q, \infty\}$. Let $\mathbb{Q}_S(p)$ denote the maximal pro- p extension of \mathbb{Q} unramified outside S , where p and q are primes (not necessarily distinct). Let $G(\mathbb{Q}_S(p)/\mathbb{Q})$ denote the Galois group $\text{Gal}(\mathbb{Q}_S(p)/\mathbb{Q})$.

3.1 $G(\mathbb{Q}_S(p)/\mathbb{Q})$, where $S = \{q, \infty\}$

We have the following relation between p, q and 2.

1. $p \neq q = 2$
2. $p = q \neq 2$
3. $q \neq p = 2$
4. $q \neq p \neq 2$ also $q \neq 2$
5. $p = q = 2$

Let K/\mathbb{Q} be a Galois extension of degree p^n unramified outside the set $\{q, \infty\}$. Observe that when $p \neq q$, q is tamely ramified in K . $G(\mathbb{Q}_S(p)/\mathbb{Q})$ in the first case is trivial due to

the following reason.

Lemma 3.1.1. *The only finite primes of \mathbb{Q} ramifying in K are $q \equiv 0, 1 \pmod{p}$.*

Proof. Suppose $p \neq q$. Let \wp be a prime divisor in K of q . Let K_\wp and \mathbb{Q}_q denote the completion of K and \mathbb{Q} at \wp and q respectively. Let F be the maximal unramified subextension of K_\wp . i.e., $\mathbb{Q}_q \subseteq F \subseteq K_\wp$. Now K_\wp/F is totally ramified. Then $K_\wp = F(\sqrt[e]{\pi\zeta})$, where π is a prime element of \mathbb{Q}_q and ζ is a root of unity coprime to q . If $K_\wp = F(\sqrt[e]{\pi\zeta})$ is to be a normal extension of \mathbb{Q}_q then K_\wp should contain the e -th roots of unity. Here $e = p^l$ for some $0 \leq l \leq n$. If \mathbb{Q}_q and hence K_\wp does not contain the p -th roots of unity, then $e = 1$. Since \mathbb{Q}_q contains the $(q-1)$ -th roots of unity, K_\wp will contain the p -th roots of unity if and only if $p \mid q-1$, i.e., $q \equiv 1 \pmod{p}$. \square

Since 2 is not congruent to $0, 1 \pmod{p}$, $G(\mathbb{Q}_S(p)/\mathbb{Q})$ in case (1) is trivial

In case 2, $G(\mathbb{Q}_S(p)/\mathbb{Q})/(G(\mathbb{Q}_S(p)/\mathbb{Q}))^{(1)} \cong \prod C_p$. But by Kronecker-Weber Theorem, the fixed field of $(G(\mathbb{Q}_S(p)/\mathbb{Q}))^{(1)}$ is contained in $\mathbb{Q}(\zeta_{p^n})$. Since $p \neq 2$, $\text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ is cyclic. Therefore, $G(\mathbb{Q}_S(p)/\mathbb{Q})/(G(\mathbb{Q}_S(p)/\mathbb{Q}))^{(1)}$ is cyclic and hence

$$G(\mathbb{Q}_S(p)/\mathbb{Q})/(G(\mathbb{Q}_S(p)/\mathbb{Q}))^{(1)} \cong C_p$$

Now, by Burnside's theorem, $G(\mathbb{Q}_S(p)/\mathbb{Q})$ is cyclic, hence $G(\mathbb{Q}_S(p)/\mathbb{Q}) \cong \mathbb{Z}_p$.

In cases 3 and 4, $G(\mathbb{Q}_S(p)/\mathbb{Q})/(G(\mathbb{Q}_S(p)/\mathbb{Q}))^{(1)} \cong \prod C_p$. But by Kronecker-Weber theorem, abelian extensions of \mathbb{Q} ramified only at q and infinity are contained in $\mathbb{Q}(\zeta_{q^n})$, which is cyclic since $q \neq 2$. Hence the the fixed field of $(G(\mathbb{Q}_S(p)/\mathbb{Q}))^{(1)}$ is contained in $\mathbb{Q}(\zeta_{q^n})$. Whence $G(\mathbb{Q}_S(p)/\mathbb{Q})/(G(\mathbb{Q}_S(p)/\mathbb{Q}))^{(1)}$ is cyclic and hence

$$G(\mathbb{Q}_S(p)/\mathbb{Q})/(G(\mathbb{Q}_S(p)/\mathbb{Q}))^{(1)} \cong C_p$$

Again, by Burnside's theorem, $G(\mathbb{Q}_S(p)/\mathbb{Q})$ is cyclic, hence $G(\mathbb{Q}_S(p)/\mathbb{Q}) \cong C_{p^a}$, where $p^a \parallel q-1$

The case 5 is (\mathcal{Q}_1) , with $K = \mathbb{Q}$ and $p = 2$ and has been resolved by Markshaitis and we state his result below.

3.2 Markshaitis's result

Theorem 3.2.1. $G_{\mathbb{Q}}(2) \cong C_2 \amalg \mathbb{Z}_2$

Proof. See [11] for an elementary proof without using cohomology, or see Theorem 4.2.6 for a quick proof using cohomology and methods of Chapter 4. We will extend the above result to finite totally imaginary extensions K of \mathbb{Q} with odd class number and with the condition that $g_2 = 1$ in K . □

3.3 Generalization

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). Let P_K denote a prime divisor of 2 in K .

Theorem 3.3.1. *Let K be a finite totally imaginary extension of \mathbb{Q} . Assume that h_K is odd and there is a unique prime P_K above 2 in K . Then $G_K(2) \cong F_2(s + 1)$. (where s is the number of complex places of K)*

Before we dig into the details of the proof, here are a few remarks about the Theorem.

Remark 3.3.2. *There is an easy proof of the above Theorem if we were to invoke Theorem 2.2.13. Since h_K is odd, $B_S = 0$ by (2) of Corollary 2.2.14. Since K is totally imaginary and there is a unique prime divisor of 2 in K , by (1) of Corollary 2.2.14, $G_K(2)$ is a free pro-2 group. There are $s = \frac{[K:\mathbb{Q}]}{2}$ complex places of K . Hence by (1) of Theorem 2.2.13, the generator rank of $G_K(2)$ is $s + 1$. Therefore $G_K(2) \cong F_2(s + 1)$. However, we exhibit an elementary proof without using powerful techniques from cohomology.*

Remark 3.3.3. *By (1) of Corollary 2.2.14, the assumptions that K is totally imaginary and $g_2 = 1$ are necessary for $G_K(2)$ to be free. However, the assumption that h_K be odd is not necessary. There is a way to get around it. Again, using Corollary 2.2.14, one can show that $G_K(2)$ is a free pro-2 group even if h_K is even, provided P_K , the prime divisor of 2 generates the Sylow-2 subgroup of $Cl(K)$. For example, some of the number fields with even class number considered in Theorems 4.1.1, 4.2.1 and 4.2.2.*

Proof. The central idea of the proof is that the number of generators of certain groups and the degree of extensions of certain number fields satisfy the same type of recursive relation; $x_i = 1 + 2^{x_{i-1}}(x_{i-1} - 1)$.

Let $K_0 = K$ and $G_K(2)^{(0)} = G_K(2)$. If K_i is defined then K_{i+1} is the compositum of all quadratic extensions of K_i contained in $K(p)$, which is the maximal pro-2 extension of K unramified outside the prime divisors of p and the infinite primes. Since $G_K(2)^{(i+1)}$ is the smallest normal subgroup N_i of $G_K(2)^{(i)}$ such that $G_K(2)^{(i)}/N_i$ is elementary abelian, it follows that K_{i+1} is the fixed field of $G_K(2)^{(i+1)}$.

Let H be a free pro-2 group on $s + 1$ generators, i.e., $H \cong F_2(s + 1)$. Suppose $G_K(2)$ has $s + 1$ generators. To show that $G_K(2) \cong H$, it is enough to show that $H_i \cong G_K(2)_i$, where $H_i = H/H^{(i)}$. Since both H and $G_K(2)$ have the same number of generators, we may map the generators of H bijectively to the generators of $G_K(2)$. Hence we have a surjective homomorphism from H to $G_K(2)$. Hence there is a surjection between H_i and $G_K(2)_i$, and so we have $|H_i| \geq |G_K(2)_i|$. We need to show that $|H_i| = |G_K(2)_i|$. This will prove the isomorphism between H_i and $G_K(2)_i$. It remains to show that $|H_i| \leq |G_K(2)_i|$. Since $|G_K(2)_i| = [K_i : K_0]$ hence it is enough to show that $|H_i| \leq [K_i : K_0]$.

K_1 is the compositum of all quadratic extensions of K_0 contained in $K(p)$. Hence K_1/K_0 is ramified only at P_{K_0} . We claim that K_1/K_0 is totally ramified and h_{K_1} is odd. Suppose there exists a quadratic extension of K_0 contained in K_1 which is not ramified at P_{K_0} . Then P_{K_0} is either inert or splits in this quadratic sub extension of K_1 , which gives rise to an unramified, abelian, 2-extension of K_0 , which implies that h_{K_0} is even. A contradiction.

Hence K_1/K_0 is totally ramified. Moreover, by Theorem 2.1.10, h_{K_1} is odd. Inductively we observe that each K_i is a totally ramified extension of K_{i-1} , and the class number of each K_i is odd. Let the class number of K_i be h_i . Let P_{K_i} be the unique prime above 2 in K_i . Then $P_{K_i}^{h_i}$ is principal. Let α_i be a generator of this ideal.

Let $\varepsilon_1^{(i)}, \dots, \varepsilon_{t_i}^{(i)}$ be system of fundamental units and a generator of the torsion subgroup of U_{K_i} . Since K is totally imaginary, each K_i is also totally imaginary. Hence $t_i = s_i$, where s_i is the number of complex places of K_i .

Then there does not exist a ζ in K_i for which

$$(\varepsilon_1^{(i)})^{m_1} \dots (\varepsilon_{t_i}^{(i)})^{m_{t_i}} = \alpha_i \zeta^2$$

where $m_j \in \mathbb{Z}$, for $1 \leq j \leq t_i$. This can be verified as follows. Let $v_{P_{K_i}}$ denote the associated valuation of the prime ideal P_{K_i} . Suppose the above equality holds. Apply the valuation to the above equality. Observe that $v_{P_{K_i}}((\varepsilon_1^{(i)})^{m_1} \dots (\varepsilon_{t_i}^{(i)})^{m_{t_i}}) = 0$, because $\varepsilon_j^{(i)}$ for $1 \leq j \leq t_i$ are units. However, since $P_{K_i}^{h_i} = \alpha_i$, we have $v_{P_{K_i}}(\alpha_i \zeta^2) = h_i + 2v_{P_{K_i}}(\zeta)$. Hence we have

$$0 = h_i + 2v_{P_{K_i}}(\zeta)$$

Therefore $v_{P_{K_i}}(\zeta) = -\frac{h_i}{2}$. But h_i is odd, hence $\frac{h_i}{2} \notin \mathbb{Z}$. A contradiction.

Hence

$$K_i(\sqrt{\alpha_i}) \cap K_i(\sqrt{\varepsilon_1^{(i)}}, \dots, \sqrt{\varepsilon_{t_i}^{(i)}}) = K_i$$

Define $L_0 = K_0$, and

$$L_{i+1} = K_i(\sqrt{\varepsilon_1^{(i)}}, \dots, \sqrt{\varepsilon_{t_i}^{(i)}}, \sqrt{\alpha_i})$$

for $i \geq 0$. It is easy to see using Kummer theory that no prime other than the prime above 2 in K_i can ramify in L_{i+1} . Hence

$$L_{i+1} \subseteq K_{i+1}$$

Also

$$[L_{i+1} : L_0] = [K_i(\sqrt{\varepsilon_1^{(i)}}, \dots, \sqrt{\varepsilon_{t_i}^{(i)}}, \sqrt{\alpha_i}) : K_0] = [K_i : K_0]2^{\left(\frac{[K_i:\mathbb{Q}]}{2} + 1\right)}$$

If we can show that $L_{i+1} = K_{i+1}$, or in other words

$$[K_{i+1} : K_0] = [K_i : K_0]2^{\left(\frac{[K_i:\mathbb{Q}]}{2} + 1\right)}$$

then we are done.

Since by Dirichlet's unit theorem, $t_i = \frac{[K_i:\mathbb{Q}]}{2}$, we prove by induction on i that

$$|H_i| = [K_i : K_0]$$

for all $i \geq 1$ and

$$[K_i : K_0] = [K_{i-1} : K_0]2^{\left(\frac{[K_{i-1}:\mathbb{Q}]}{2} + 1\right)}$$

for all $i \geq 1$

Let d_i be the number of generators of $H^{(i)}$. Then by Theorem 2.2.9 (and also by Burnside's Theorem (Theorem 2.2.8)), we have

$$d_i = 1 + 2^{d_{i-1}}(d_{i-1} - 1) \tag{3.1}$$

Here d_0 is the number of generators of $H^{(0)} = H$.

We will see that the fixed fields K_i of $G_K(2)^{(i)}$ satisfy an identical recursive relation.

From

$$L_1 = K_0(\sqrt{\varepsilon_1^{(0)}}, \dots, \sqrt{\varepsilon_{t_0}^{(0)}}, \sqrt{\alpha_0})$$

we deduce that

$$[L_1 : L_0] = [K_0 : K_0]2^{\left(\frac{[K_0:\mathbb{Q}]}{2} + 1\right)}$$

hence

$$[L_1 : L_0] = 2^{s+1}$$

Since H has $s + 1$ generators, again by Burnside's theorem we have

$$|H_1| = 2^{(s+1)}$$

Hence

$$[L_1 : L_0] = |H_1|$$

But

$$[K_1 : K_0] \leq |H_1| = [L_1 : L_0] \leq [K_1 : K_0]$$

this implies that

$$L_1 = K_1$$

and hence

$$[K_1 : K_0] = [K_0 : K_0] 2^{\left(\frac{[K_0:\mathbb{Q}]}{2} + 1\right)}$$

We know that

$$|H_i| \geq [K_i : K_0]$$

and

$$[K_i : K_0] \geq [K_{i-1} : K_0] 2^{\left(\frac{[K_{i-1}:\mathbb{Q}]}{2} + 1\right)}$$

We need to prove that

$$|H_i| \leq [K_i : K_0]$$

and

$$[K_i : K_0] \leq [K_{i-1} : K_0] 2^{\left(\frac{[K_{i-1}:\mathbb{Q}]}{2} + 1\right)}$$

Hence the induction hypothesis are

(a)

$$|H_i| \leq [K_i : K_0]$$

(b)

$$[K_i : K_0] \leq [K_{i-1} : K_0] 2^{\left(\frac{[K_{i-1}:\mathbb{Q}]}{2} + 1\right)}$$

But

$$|H_1| = [L_1 : L_0] = [K_1 : K_0] = [K_0 : K_0] 2^{\left(\frac{[K_0:\mathbb{Q}]}{2} + 1\right)}$$

This proves the first step for induction. Suppose we have proved these inequalities for $i \leq j$.

Now

$$|H_{j+1}| = |H/H^{(j+1)}| = |H/H^{(j)}| |H^{(j)}/H^{(j+1)}|$$

But

$$|H^{(j)}/H^{(j+1)}| = 2^{d_j} = 2^{1+2^{d_{j-1}}(d_{j-1}-1)}$$

Hence

$$|H/H^{(j)}| |H^{(j)}/H^{(j+1)}| = |H_j| 2^{1+2^{d_{j-1}}(d_{j-1}-1)}$$

But by inductive hypothesis

$$|H_j| = [K_j : K_0] = [K_{j-1} : K_0] 2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right)}$$

Also

$$|H_j| = |H_{j-1}| 2^{d_{j-1}}$$

This implies that

$$[K_{j-1} : K_0] 2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right)} = |H_{j-1}| 2^{d_{j-1}}$$

Therefore

$$d_{j-1} = \frac{[K_{j-1} : \mathbb{Q}]}{2} + 1$$

Hence

$$|H_{j+1}| = |H_j| 2^{1+2^{d_{j-1}}(d_{j-1}-1)} = [K_j : K_0] 2^{1+2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right) \frac{[K_{j-1}:\mathbb{Q}]}{2}}} \quad (3.2)$$

Now we know that for all $i \leq j$

$$[K_i : K_0] = [K_{i-1} : K_0] 2^{\left(\frac{[K_{i-1}:\mathbb{Q}]}{2} + 1\right)}$$

But by inductive hypothesis

$$[K_j : K_0] = [K_{j-1} : K_0] 2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right)}$$

$$[K_0 : \mathbb{Q}][K_j : K_0] = [K_0 : \mathbb{Q}][K_{j-1} : K_0] 2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right)}$$

$$[K_j : \mathbb{Q}] = [K_{j-1} : \mathbb{Q}] 2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right)}$$

$$\frac{[K_j : \mathbb{Q}]}{2} = \frac{[K_{j-1} : \mathbb{Q}]}{2} 2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right)}$$

$$1 + \frac{[K_j : \mathbb{Q}]}{2} = 1 + \frac{[K_{j-1} : \mathbb{Q}]}{2} 2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right)} \quad (3.3)$$

Observe that equation 3.3 is identical to equation 3.1 with d_i replaced with $1 + \frac{[K_j:\mathbb{Q}]}{2}$. Hence both the number fields K_i (fixed fields of $G_K(2)^{(i)}$) and the groups $H^{(i)}$ satisfy the same type of recursive relation.

$$2^{\left(1 + \frac{[K_j:\mathbb{Q}]}{2}\right)} = 2^{\left(1 + \frac{[K_{j-1}:\mathbb{Q}]}{2}\right)} 2^{\left(\frac{[K_{j-1}:\mathbb{Q}]}{2} + 1\right)}$$

Hence

$$[K_j : K_0]2^{(1+2^{\lfloor \frac{[K_{j-1}:\mathbb{Q}]}{2} \rfloor + 1} \frac{[K_{j-1}:\mathbb{Q}]}{2})} = [K_j : K_0]2^{\lfloor \frac{[K_j:\mathbb{Q}]}{2} \rfloor + 1} \leq [K_{j+1} : K_0]$$

Hence by equation 3.2 we have

$$|H_{j+1}| \leq [K_{j+1} : K_0]$$

which proves (a) of the inductive hypothesis. But

$$|H_{j+1}| \geq |G_K(2)_{j+1}| = [K_{j+1} : K_0]$$

Therefore

$$|H_{j+1}| = |G_K(2)_{j+1}| = [K_{j+1} : K_0]$$

From the above we have

$$[K_{j+1} : K_0] = [K_j : K_0]2^{\lfloor \frac{[K_j:\mathbb{Q}]}{2} \rfloor + 1}$$

which proves (b) of the inductive hypothesis.

This implies that $|H_i| = |G_K(2)_i|$, therefore $H_i \cong G_K(2)_i$ and hence $H \cong G_K(2)$. Hence $G_K(2)$ is a free pro-2 group on $s + 1$ generators and $G_K(2) \cong F_2(s + 1)$ \square

Remark 3.3.4. *Since K_{i+1} was the maximal elementary abelian 2-extension of K_i unramified outside the set of prime divisors of 2 and the infinite primes of K_i , we showed that $K_{i+1} = K_i(\sqrt{\varepsilon_1^{(i)}}, \dots, \sqrt{\varepsilon_{t_i}^{(i)}}, \sqrt{\alpha_i})$, where $\varepsilon_j^{(i)}$ were units and α_i was the generator of a power of P_{K_i} . Here is an explicit example illustrating the above. Let $K = \mathbb{Q}(\sqrt{15})$. Let S denote the set of prime divisors of 2 and infinity in K . Note that $4 + \sqrt{15}$ is a fundamental unit of K and $h_K = 2$. We will show that the maximal elementary abelian 2-extension of K unramified outside S is $K(\sqrt{4 + \sqrt{15}}, i, \sqrt{2})$, where -1 is the generator of the second roots*

of unity and $P_K^2 = (2)$.

The extended genus field of K is $\mathbb{Q}(\sqrt{3}, \sqrt{5}, i)$. Observe that P_K splits in $K(i)$ and is inert in $K(\sqrt{5})$. Now, $\sqrt{4 + \sqrt{15}} = \frac{\sqrt{10} + \sqrt{6}}{2}$. Hence, $\mathbb{Q}(\sqrt{4 + \sqrt{15}}) = \mathbb{Q}(\sqrt{10}, \sqrt{6}) = K(\sqrt{10})$. Therefore $K(\sqrt{4 + \sqrt{15}}) = K(\sqrt{10})$. Hence it is easy to see that $K(\sqrt{5})$ is not a subfield of $K(\sqrt{4 + \sqrt{15}})$. Hence $K(\sqrt{10}, i, \sqrt{5})$ is contained in the maximal elementary abelian 2-extension of K unramified outside S . However, $K(\sqrt{10}, \sqrt{5}) = K(\sqrt{10}, \sqrt{2})$. Therefore $K(\sqrt{10}, i, \sqrt{5}) = K(\sqrt{10}, i, \sqrt{2}) = K(\sqrt{4 + \sqrt{15}}, i, \sqrt{2})$. Now, we show that this is indeed the maximal elementary abelian 2-extension of K unramified outside S .

Since there are no prime divisors of 15 which are $\equiv \pm 1 \pmod{8}$, there are no algebraic integers of the form $a + b\sqrt{15}$ whose norm is ± 2 , where $a, b \in \mathbb{Z}$. Whence, P_K is not principal. Since, $h_K = 2$, P_K generates the Sylow-2 subgroup of the ideal class group of K . Hence, $B_S = 0$. Now, applying (1) of Theorem 2.2.13, we see that the generator rank of $G_K(2)$ is 3. Hence, by Theorem 2.2.8, $G_K(2)/(G_K(2))^{(1)} \cong C_2 \times C_2 \times C_2$. Therefore, the maximal elementary abelian 2-extension of K unramified outside S is $K(\sqrt{4 + \sqrt{15}}, i, \sqrt{2})$.

Example 3.3.1. Let L be the splitting field of the polynomial $x^3 - 2$. $\text{Gal}(L/\mathbb{Q}) \cong S_3$. There is a unique prime above 2 in L , and $h_L = 1$. Hence $G_L(2) \cong F_2(4)$. Let $F = \mathbb{Q}(\sqrt{-3})$ be the quadratic subfield of L . $h_F = 1$ and $g_2 = 1$ in F . Therefore, $G_F(2) \cong F_2(2)$. Let K_j , $1 \leq j \leq 3$, be the 3 cubic subfields of L . Observe that K_j are not totally imaginary. Hence $G_{K_j}(2)$ cannot be free by (1) of Corollary 2.2.14. We will discuss the structure of $G_{K_j}(2)$ in example 5.2.2.

Example 3.3.2. Let $K = \mathbb{Q}(\zeta_m)$, where $m = 11, 13, 19, 25, 27$. One can check that 2 is inert in K . Moreover, $h_K = 1$ by [18, Theorem 11.1]. Here $G_K(2) \cong F_2(n)$, where $n = 6, 7, 10, 11$ and 10 respectively.

Example 3.3.3. Let $K = \mathbb{Q}(\sqrt{n})$, where $n = -1, -2, -p$ where p is a prime $\equiv 3 \pmod{8}$. Here $G_K(2) \cong F_2(2)$. [See Theorem 4.1.1 for more details].

Example 3.3.4. Let K be any of the following. $\mathbb{Q}(i, \sqrt{2})$, $\mathbb{Q}(i, \sqrt{p})$, $\mathbb{Q}(\sqrt{-2}, \sqrt{p})$, where

p is a prime $\equiv 5 \pmod{8}$ or $\mathbb{Q}(\sqrt{2}, \sqrt{-q})$, $\mathbb{Q}(i, \sqrt{q})$, $\mathbb{Q}(\sqrt{-2}, \sqrt{2q})$ where q is a prime $\equiv 3 \pmod{8}$. Each of these fields have odd class number and have a unique prime above 2. Hence $G_K(2) \cong F_2(3)$.

Example 3.3.5. Consider the two $D_8 (= C_4 \rtimes C_2)$ -extensions, namely $L = \mathbb{Q}(\zeta_8, \sqrt{u})$ or $\mathbb{Q}(\zeta_8, \sqrt[4]{2})$, where $u = 1 - \sqrt{2}$ is the fundamental unit of $\mathbb{Q}(\zeta_8)$. 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 2.1.10). Hence $G_L(2) \cong F_2(5)$. Consider the subfield $K = \mathbb{Q}(2^{\frac{1}{4}})$. Since K is not totally imaginary, by (1) of Corollary 2.2.14, $G_K(2)$ cannot be free, and we will discuss its structure in example 5.1.1.

Chapter 4

2-rational degree 2 and degree 4-extensions

Let S be the set of prime divisors of 2 and the infinite primes in K . Let P_K denote a prime divisor of 2 in K . Let e_2 and f_2 denote the ramification index and the inertial degree of 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 .

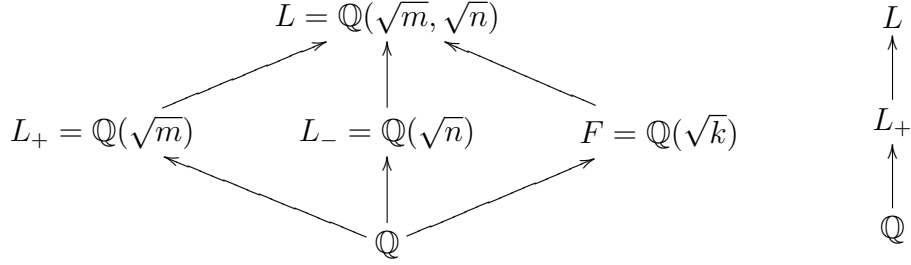
Definition 4.0.5. *A number field K is said to be 2-rational if $G_K(2)$ is free.*

In this chapter we classify quadratic, biquadratic and degree 4 cyclic 2-rational number fields. We also classify those quadratic number fields which are not 2-rational, but has a degree 2-extension, which is Galois over \mathbb{Q} and is 2-rational. In this case we explicitly describe the Galois group of their maximal pro-2 extension unramified outside 2 and infinity using a result of Herfort-Ribes-Zaleskii on virtually free pro- p groups(Definition 2.2.4).

Recall from Corollary 2.2.14, assuming that K is totally imaginary number field and there is a unique prime above 2 in K , to show that K is 2-rational, one has to show that $B_S = 0$ (Definition 2.2.10). Hence all we have to show is that $B_S = 0$ in proving the theorems in this and the next Chapter, which is the main challenge. Now, $B_S = 0$ if either the class number of K is odd or the prime above 2 in K generates the Sylow 2-subgroup of the class group of K . By Genus Theory (Section 2.1.2), for K to satisfy the above class number condition, one cannot have too many ramified primes in K . The most recurring theme of this Chapter, is not to have too many finite ramified primes in K over \mathbb{Q} ; in fact for K to be 2-rational, K cannot have more than 2 finite ramified primes.

Let L be an imaginary biquadratic extension of \mathbb{Q} or an imaginary cyclic extension of \mathbb{Q}

of degree 4 with L_+ as the unique real quadratic subfield. Let $m > 1, n < 0$, be square free integers, $k = \frac{mn}{(m,n)^2}$. We have the following diagram of number fields.



4.1 Quadratic extensions

Theorem 4.1.1. *Let K be a quadratic number field. Then K is 2-rational if and only if K is any imaginary quadratic subfield of $\mathbb{Q}(\zeta_{8p})$ where p is a prime $\equiv \pm 3 \pmod{8}$. More precisely $K = \mathbb{Q}(\sqrt{n})$ is one of the following, $n = -1, -2, -p$ or $-2p$ where p is a prime $\equiv \pm 3 \pmod{8}$. In each of the above cases $G_K(2) \cong F_2(2)$.*

Proof. Recall from Corollary 2.2.14, for K to be 2-rational, K should be totally imaginary, there should be a unique prime divisor of 2 in K , i.e., $g_2 = 1$ in K and $B_S = 0$. Moreover, $B_S = 0$ if either h_K is odd or S generates the Sylow 2-subgroup of $Cl(K)$. Hence, if a number field has a real embedding then it cannot be 2-rational. Therefore, there are no real quadratic 2-rational number fields. For a quadratic number field with even class number, S will generate the Sylow 2-subgroup of the class group of K if and only if P_K is not principal and $h_K \equiv 2 \pmod{4}$.

The genus number of an imaginary L as described in [3] is $\frac{e_1 \cdots e_n}{[L:\mathbb{Q}]}$, where e_1, \dots, e_n are the ramification indices of the ramifying primes p_1, \dots, p_n in L . If more than 2 finite primes ramify in $K = \mathbb{Q}(\sqrt{n})$, then by the Genus formula, $h_K \equiv 0 \pmod{4}$. If $n = -1, -2$, or $-p$, where p is a prime congruent to 3 mod 8, then $h_{\mathbb{Q}(\sqrt{n})}$ is odd. However, if $n = -p$, where p is a prime congruent to 5 mod 8 or $n = -2p$, where p is a prime congruent to 3, 5 mod 8 then $h_{\mathbb{Q}(\sqrt{n})} \equiv 2 \pmod{4}$ by Proposition 2.1.17. Now, we have to show that $P_{\mathbb{Q}(\sqrt{n})}$ is not

principal. Hence, apply the norm to K/\mathbb{Q} . Hence $N_{K/\mathbb{Q}}(a + b\sqrt{-2p}) = a^2 + b^2(2p)$ which should equal $+2$. This cannot happen. Hence there are no algebraic integers of the form $a + b\sqrt{-2p}$ whose norm is 2, where $a, b \in \mathbb{Z}$. Whence $P_{\mathbb{Q}(\sqrt{n})}$ is not principal, and $P_{\mathbb{Q}(\sqrt{n})}$ generates the Sylow 2-subgroup of the class group of $\mathbb{Q}(\sqrt{n})$. Observe that $g_2 = 1$ in all of the above K . Therefore, $G_K(2)$ is a free pro-2 group. Since as $p = 2$, we have $\delta = \delta_\rho = 1$. Moreover, S consists of P_K and a complex place of K . Also, $B_S = 0$. Therefore by (1) of Theorem 2.2.13, $G_K(2)$ has 2 generators. Whence, $G_K(2) \cong F_2(2)$

$g_2 = 1$ in K , if $n = -p$ where $p \equiv 7 \pmod{8}$. Moreover, if $n = -p$ where $p \equiv 1 \pmod{8}$, or $n = -2p$ where $p \equiv 1, 7 \pmod{8}$ then $h_{\mathbb{Q}(\sqrt{n})} \equiv 0 \pmod{4}$ by Theorem 2.1.14 and Proposition 2.1.17. Now, suppose that the only ramifying primes in K are odd, say p and q . Then either 2 is inert in K and $2 \mid h_K$ or $g_2 = 1$ in K . In either case K cannot be 2-rational. \square

4.2 Degree 4-extensions

4.2.1 Cyclic extensions

Let S (resp. S_+) be the set of prime divisors of 2 and infinity in L (resp. L_+). Let P_L be a prime divisor of 2 in L .

Theorem 4.2.1. *Let L be a cyclic extension of degree 4 over \mathbb{Q} with L_+ as the unique quadratic subfield of L . Then L is 2-rational if and only if*

1. *The conductor of L has a unique prime factor and*

(a) *L is the imaginary cyclic extension of \mathbb{Q} contained in $\mathbb{Q}(\zeta_p)$, where p is a prime $\equiv 5 \pmod{8}$.*

(b) *L is the imaginary cyclic extension of \mathbb{Q} contained in $\mathbb{Q}(\zeta_{2^4})$.*

2. *The conductor of L has two prime factors and*

- (a) L is an imaginary cyclic extension of \mathbb{Q} contained in $\mathbb{Q}(\zeta_{2^4 p})$ with $L_+ = \mathbb{Q}(\sqrt{2})$, where p is a prime $\equiv \pm 3 \pmod{8}$ and $h_L \equiv 2 \pmod{4}$.
- (b) L is an imaginary cyclic extension of \mathbb{Q} contained in $\mathbb{Q}(\zeta_{2^4 p})$ with $L_+ = \mathbb{Q}(\sqrt{p})$, where p is a prime $\equiv 5 \pmod{8}$ and $h_L \equiv 2 \pmod{4}$.
- (c) L is an imaginary cyclic extension of \mathbb{Q} contained in $\mathbb{Q}(\zeta_{2^4 p})$ with $L_+ = \mathbb{Q}(\sqrt{2p})$, where p is a prime $\equiv 5 \pmod{8}$ and $2^2 \parallel h_L$.

In each of the above cases $G_L(2) \cong F_2(3)$ and $G_{L_+}(2) \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$.

Proof. Recall from Corollary 2.2.14, for L to be 2-rational, L has to be an imaginary extension of \mathbb{Q} with $g_2 = 1$ in L with the additional condition that $B_S = 0$. Observe that either $f_2 = 4$ or $e_2 \geq 2$ in L . Note that every odd prime is tamely ramified in L . Suppose the conductor of L has a unique prime factor. Hence the conductor is either p or a power of 2. This is the case (1) and is easy to handle, because L is contained in $\mathbb{Q}(\zeta_p)$ or $\mathbb{Q}(\zeta_{2^4})$ respectively. But if L has conductor with two prime factors, then L is contained in $\mathbb{Q}(\zeta_{2^4 p})$ which is the case (2). Here, we need a more subtle analysis. Observe that at least one of the ramifying primes will have ramification index 4. By Genus Theory (Theorem 2.1.15 and Theorem 2.1.16) we know that h_L is even. If $o(P_L) = 1$ or if $8 \mid h_L$, then L cannot be 2-rational. If $o(P_L) = 2$ in $Cl(L)$, then by Corollary 2.2.14, L is 2-rational if and only if $2 \parallel h_L$ and similarly if $o(P_L) = 4$, then L is 2-rational if only if $2^2 \parallel h_L$. Note that if h_{L_+} is odd, then $o(P_L) \leq 2$. If the conductor of L has more than two prime factors, i.e., if more than two finite primes ramify in L , using Genus Theory, it is easy to see that the Sylow 2-subgroup of the class group of L is too large for P_L to generate. We make use of Dirichlet characters to get information about L and L_+ . Examples of fields L which satisfy the class number condition when the conductor has more than one prime factor, lie in $\mathbb{Q}(\zeta_{48})$ and $\mathbb{Q}(\zeta_{80})$. More details can be found in the section 4.2.5.

If L/\mathbb{Q} is a totally imaginary degree 4 cyclic extension, then the unique degree 2 extension L_+/\mathbb{Q} contained in L is totally real, because L_+ is the fixed field of complex conjugation.

(1) Suppose L has conductor with a unique prime factor. Since L/\mathbb{Q} is abelian, by the Kronecker-Weber theorem L is contained in a cyclotomic extension $\mathbb{Q}(\zeta_{p^r})$ for some prime p and $r \geq 1$. Then

$$\text{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) \cong (C_{p_1^{r_1}})^\times$$

Suppose $p \equiv 5 \pmod{8}$. Then $4 \parallel p-1$. Hence there exists a cyclic extension of degree 4 over \mathbb{Q} contained in $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^r})$. The fixed field of the maximal subgroup of odd order in $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a cyclic extension L of degree 4 over \mathbb{Q} . But 2 is inert in $L_+ = \mathbb{Q}(\sqrt{p})$, hence inert in L . Moreover, since L/\mathbb{Q} is a totally imaginary cyclic extension of degree 4 and exactly one rational prime ramifies in L/\mathbb{Q} , h_L is odd by Genus Theory.

If $p \equiv 3, 7 \pmod{8}$, then 4 does not divide $p-1$ and hence there is no extension of degree 4 over \mathbb{Q} contained in $\mathbb{Q}(\zeta_p)$. If $p \equiv 1 \pmod{8}$, $\mathbb{Q}(\zeta_p)$ contains a cyclic extension L of degree 4 over \mathbb{Q} . But 2 factors in L because, $\mathbb{Q}(\sqrt{p}) \subset L \subset \mathbb{Q}(\zeta_p)$.

If the conductor of L is a power of 2, then $L \subset \mathbb{Q}(\zeta_{2^4})$. Here L is the unique imaginary cyclic extension of $\mathbb{Q}(\zeta_{2^4})$ of degree 4. Note that $h_L = 1$.

(2) Now suppose L has conductor with two prime factors. Note that $L_+ = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{2p})$. Therefore L is contained in $\mathbb{Q}(\zeta_{2^4 p})$. Then

$$\text{Gal}(\mathbb{Q}(\zeta_{2^4 p})/\mathbb{Q}) \cong C_2 \times C_4 \times C_{(p-1)}$$

Observe that the above decomposition of the $\text{Gal}(\mathbb{Q}(\zeta_{2^4 p})/\mathbb{Q})$ is not unique. Also, the character group of $\text{Gal}(\mathbb{Q}(\zeta_{2^4 p})/\mathbb{Q})$ is isomorphic to $C_2 \times C_4 \times C_{(p-1)}$. Now we introduce new notation for characters for the sake of convenience. Let χ_1 be a generator of C_2 , χ_2 be a generator of C_4 and χ_p be a generator of $C_{(p-1)}$, chosen in such a way that $\mathbb{Q}(i)$ is the field of χ_1 and $\mathbb{Q}(\zeta_{2^4} + \zeta_{2^4}^{-1})$ is the field of χ_2 . Hence χ_1 is an odd character and χ_2 is an even character, moreover, χ_1 has conductor 4 and χ_2 has conductor 16. Every element of $C_2 \times C_4 \times C_{(p-1)}$ is of the form $\chi_1^a \chi_2^b \chi_p^c$, where $a \in \{0, 1\}$, $b \in \{0, 1, 2, 3\}$ and $c \in \{0, 1, \dots, p-2\}$. Let $2^k \parallel p-1$. Then $C_{(p-1)} \cong C_{2^k} \times C_{\binom{p-1}{2^k}}$.

Since we are interested only in the degree 4, imaginary, cyclic extensions of \mathbb{Q} , we can assume without loss of generality that χ_p is a generator of C_{2^k} . Let the field of χ_p be the fixed field of $C_{\left(\frac{p-1}{2^k}\right)}$, hence χ_p is an odd character with conductor p . We look for odd characters of order 4, with 2 and p as prime factors of the conductor i.e., characters with conductor $4p$, $8p$ or $16p$. Order of χ_1^a can be either 1 or 2, order of χ_2^b can be 1, 2, 4 and order of χ_p^c can be either $1, 2, \dots, 2^k$ with the constraint that $o(\chi_1^a \chi_2^b \chi_p^c) = 4$. Moreover, since we demand that $\chi_1^a \chi_2^b \chi_p^c$ be an odd character, exactly one of χ_1^a or χ_p^c is odd. The following table gives all possible orders of χ_1^a , χ_2^b and χ_p^c to generate degree 4 cyclic extensions of \mathbb{Q} .

| | $o(\chi_1^a)$ | $o(\chi_2^b)$ | $o(\chi_p^c)$ | L_+ |
|-----|---------------|---------------|---------------|--|
| 1. | 2 | 2 | 4 | $\mathbb{Q}(\sqrt{p}), p \equiv 5 \pmod{8}$ |
| 2. | 1 | 2 | 4 | —————”————— |
| 3. | 2 | 1 | 4 | —————”————— |
| 4. | 1 | 1 | 4 | —————”————— |
| 5. | 2 | 4 | 4 | $\mathbb{Q}(\sqrt{2p}), p \equiv 1 \pmod{8}$ |
| 6. | 1 | 4 | 4 | $\mathbb{Q}(\sqrt{2p}), p \equiv 5 \pmod{8}$ |
| 7. | 2 | 4 | 2 | $\mathbb{Q}(\sqrt{2}), p \equiv 5 \pmod{8}$ |
| 8. | 1 | 4 | 2 | $\mathbb{Q}(\sqrt{2}), p \equiv 3 \pmod{8}$ |
| 9. | 2 | 4 | 1 | $\mathbb{Q}(\sqrt{2})$ |
| 10. | 1 | 4 | 1 | $\mathbb{Q}(\sqrt{2})$ |

Character table

We will use the above table to show that certain cases cannot occur. More precisely, for L to be 2-rational with the conductor having two prime factors, any case other than the ones mentioned in 2(a), 2(b) and 2(c) of Theorem 4.2.1 cannot occur. The existence of the number fields L , with the given class number condition in 2 of the Theorem will be shown by giving examples.

Let L_1 , L_2 and L_p denote the field of χ_1^a , χ_2^b and χ_p^c , L_{12} denote the field of $\chi_1^a \chi_2^b$ and let

L denote the field of $\chi_1^a \chi_2^b \chi_p^c$. If $o(\chi_1^a) = 1$, then $L_1 = \mathbb{Q}$ and if $o(\chi_1^a) = 2$, then $L_1 = \mathbb{Q}(i)$. If $o(\chi_2^b) = 2$, then $L_2 = \mathbb{Q}(\sqrt{2})$ and if $o(\chi_2^b) = 4$, then $L_2 = \mathbb{Q}(\zeta_{2^4} + \zeta_{2^4}^{-1})$. Now, if $o(\chi_p^c) = 4$, then L_p is a degree four cyclic extension of \mathbb{Q} contained in $\mathbb{Q}(\zeta_p)$, where $p \equiv 1 \pmod{4}$, and if $o(\chi_p^c) = 2$, then $L_p = \mathbb{Q}(\sqrt{\pm p})$, depending on whether $p \equiv \pm 1 \pmod{4}$.

By Theorem 2.1.24, if $o(\chi_1^a \chi_2^b) = i$, then $e_2 = i$ in L and if $o(\chi_p^c) = j$, then $e_p = j$ in L , where $i, j \in \{1, 2, 4\}$. Moreover, if $e_2 = 4$ and $e_p = 4$, then $L_+ = \mathbb{Q}(\sqrt{2p})$, with $p \equiv 1 \pmod{4}$ and $4 \mid h_L$. If $e_2 = 4$ and $e_p = 2$, then $L_+ = \mathbb{Q}(\sqrt{2})$, $2 \mid h_L$ and in both the cases $L \subset \mathbb{Q}(\zeta_{16p})$. Now, if $e_2 = 2$ and $e_p = 4$, then $L_+ = \mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \pmod{4}$, $2 \mid h_L$ and $L \subset \mathbb{Q}(\zeta_{8p})$. But if $e_2 = 4$ and $e_p = 1$, then $L \subset \mathbb{Q}(\zeta_{2^4})$, and if $e_2 = 1$ and $e_p = 4$, then $L \subset \mathbb{Q}(\zeta_p)$, hence we ignore lines 4, 9 and 10 from the character table. We also ignore lines 1 and 3, because the character $\chi_1^a \chi_2^b \chi_p^c$ is even.

Observe that in Lines 1 through 4 of the character table, $o(\chi_p^c) = 4$. Hence $p \equiv 1 \pmod{4}$. But, if $p \equiv 1 \pmod{8}$, then 2 splits in $L_+ = \mathbb{Q}(\sqrt{p})$. Hence we ignore the case when $p \equiv 1 \pmod{8}$. Moreover, in line 2, observe that $f_2 = 2$ in L , because $L_+ = \mathbb{Q}(\sqrt{p})$. Hence if P_L is not principal and $h_L \equiv 2 \pmod{4}$, we will have 2(b) of the Theorem.

In line 5, since $o(\chi_p^c) = 4$, it implies that $p \equiv 1 \pmod{4}$. If $p \equiv 5 \pmod{8}$, then $o(\chi_p) = 4$ which implies that $\chi_p^c = \chi_p$. Hence the character χ_p^c would be odd. But, χ_1^a is an odd character. Hence we will not consider the case when $p \equiv 5 \pmod{8}$ in line 5. In line 6, since $o(\chi_p^c) = 4$, it implies that $p \equiv 1 \pmod{4}$. Now, χ_1^a and χ_2^b are even. If $p \equiv 1 \pmod{8}$, then the order of χ_p is at least 8. Since $o(\chi_p^c) = 4$, it implies that χ_p^c would be an even power of χ_p . Hence the character χ_p^c would also be even. Hence we will not consider the case when $p \equiv 1 \pmod{8}$ and only consider the case when $p \equiv 5 \pmod{8}$ in line 6.

Now, let us have a closer look at line 5 of the character table. χ_1^a has order 2 and χ_2^b has order 4 and χ_p^c has order 4 hence they yield the following diagram of number fields.

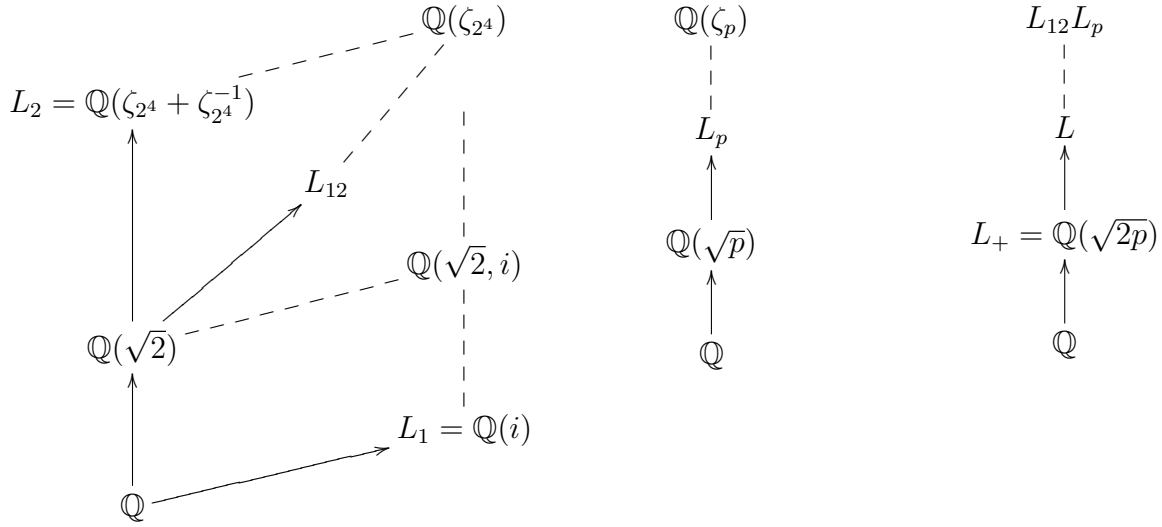


Diagram of number fields corresponding to line 5 of the Character Table

Now χ_1^a is an odd character and χ_p^c is an even character. But, χ_p being an odd character, implies that χ_p^c is an even power of χ_p . Hence the order of χ_p is at least 8. Therefore, $p \equiv 1 \pmod{8}$. Since $o(\chi_1^a \chi_2^b \chi_p^c) = 4$, $\deg(L/\mathbb{Q}) = 4$. However, $\deg(L_{12}L_p/L) = 4$. Observe that $L_{12}L_p/L$ is an unramified extension as 2 is unramified in $\mathbb{Q}(\zeta_p)$ and p is unramified in $\mathbb{Q}(\zeta_{2^4})$, but both 2 and p are totally ramified in L . Observe that $4 \mid h_L$. If $4 \parallel h_L$, then $L_{12}L_p$ is the Hilbert 2-class field of L . But $o(P_L) \leq 2$ as 2 splits in $\mathbb{Q}(\sqrt{p})$ and hence P_L factors in $L_{12}L_p$. Hence we ignore line 5.

Now let us look at line 6 from the character table. Here $L_1 = \mathbb{Q}$. Moreover, $f_2 = 4$ in L_p and $e_2 = 4$ in L . Hence P_L is inert in $L_{12}L_p$. Observe that $\deg(L_{12}L_p/L) = 4$. But, $B_S = 0$ if and only if $o(P_L) = 4$ and $4 \parallel h_L$. Hence we have $2(c)$.

Because of the requirement that $\chi_1^a \chi_2^b \chi_p^c$ be an odd character, in line 7 of the character table, odd primes, whose prime divisors ramify in L/L_+ are $\equiv 1 \pmod{4}$ and similarly $\equiv 3 \pmod{4}$ in line 8. Looking at line 7 of the character table it is easy to see that if $p \equiv 1 \pmod{8}$, then 2 splits in $\mathbb{Q}(\sqrt{p})$, hence P_L factors in $L_{12}L_p$. But $o(P_L) \leq 2$, as $L_+ = \mathbb{Q}(\sqrt{2})$. Observe that $\deg(L_{12}L_p/L) = 2$. If $h_L \equiv 2 \pmod{4}$, then $L_{12}L_p$ is the Hilbert 2-field of L and P_L splits

in $L_{12}L_p$, whence P_L is principal. Hence we will only consider the case when $p \equiv 5 \pmod{8}$ in line 7. Hence we have 2(a) of the Theorem, when $p \equiv 5 \pmod{8}$.

In line 8 of the character table, observe that if $p \equiv 7 \pmod{8}$, then 2 splits in $\mathbb{Q}(\sqrt{-p})$, and hence P_L splits in $L_{12}L_p$. Whence P_L is principal by an argument identical to the previous paragraph. Hence we will only consider the case when $p \equiv 3 \pmod{8}$. Hence if P_L is not principal and $h_L \equiv 2 \pmod{4}$, we will have 2(a) of the Theorem, when $p \equiv 3 \pmod{8}$.

What is remaining is to show that P_L is not principal in L . Now if p is a prime congruent to 5 mod 8 (3 mod 8 respectively), then $2^2 \parallel p - 1$ ($2 \parallel p - 1$ respectively). But 2 is inert in the unique cyclic extension of \mathbb{Q} of degree 4 (degree 2 respectively) contained in $\mathbb{Q}(\zeta_p)$. Note that 2 is unramified in $\mathbb{Q}(\zeta_p)$. Hence 2 can factor in $\mathbb{Q}(\zeta_p)$ into at most $\frac{p-1}{4}$ ($\frac{p-1}{2}$ respectively), both odd number of factors, and so 2 will factor into odd number of factors in $\mathbb{Q}(\zeta_{2^4p})$. Hence P_L cannot be principal in L , for otherwise by the isomorphism of Class group of L with $\text{Gal}(\mathcal{L}/L)$, via the Artin map, where \mathcal{L} is the Hilbert class field of L , P_L will factor in the genus field of L . Now, consider the case when $L_+ = \mathbb{Q}(\sqrt{2p})$. Then $f_2 = 4$ in L_p , but $f_2 = 1$ in L . Hence P_L remains inert in $L_{12}L_p$, if $2^2 \parallel h_L$. Therefore $o(P_L) = 4$.

Suppose the conductor of L has more than two prime factors, then Genus Theory says that at least $4 \mid h_L$. Observe that for at least one of the ramifying primes, the ramification index will be 4. Assuming that $g_2 = 1$ in L , if $e_2 = 2$ in L , then $o(P_L) \leq 2$ and $h_L \equiv 0 \pmod{4}$. But if, $e_2 = 4$ in L , then it is easy to see that either $o(P_L) \leq 2$ and $h_L \equiv 0 \pmod{4}$ or $o(P_L) \leq 4$ and $h_L \equiv 0 \pmod{8}$.

$G_L(2)$ is a free pro-2 group on 3 generators by (1) of Theorem 2.2.13. Therefore

$$G_L(2) \cong F_2(3)$$

The description of the structure of $G_{L_+}(2)$ will be given in Section 4.2.5. □

4.2.2 Biquadratic extensions

Let S_+ (resp. S_- and \tilde{S}) be the set of prime divisors of 2 and infinity in L_+ (resp. L_- and F). Let P_L (resp. P_{L_+}) be a prime divisor of 2 in L (resp. L_+).

Theorem 4.2.2. *Let L be a biquadratic number field, then*

1. L is 2-rational if and only if L is any imaginary biquadratic subfield of $\mathbb{Q}(\zeta_{8p})$, where p is a prime $\equiv \pm 3 \pmod{8}$. More precisely, $L = \mathbb{Q}(\sqrt{n}, \sqrt{m})$, is one of the following
 - (a) $n = -1$ and $m = 2, p$ or $2p$ where p is a prime $\equiv \pm 3 \pmod{8}$
 - (b) $n = -2$ and $m = p$ or $2p$ where p is a prime $\equiv \pm 3 \pmod{8}$
 - (c) $n = -p$, where p is a prime $\equiv \pm 3 \pmod{8}$ and $m = 2$
2. In each of the above cases $G_{L_+}(2) \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$, $G_{L_-}(2) \cong G_F(2) \cong F_2(2)$ and $G_L(2) \cong F_2(3)$.

Proof. Since $g_2 = 1$ in L , then either $e_2 = 2$ or $e_2 = 4$ in L . Hence 2 is ramified in L . Observe that if $f_2 = 4$, then L is a cyclic extension of \mathbb{Q} . Suppose we know that at most 2 finite primes ramify in L . Then L is an imaginary Klein 4-subfield of $\mathbb{Q}(\zeta_{8p})$. The elementary 2-abelian quotient of $\text{Gal}(\mathbb{Q}(\zeta_{8p})/\mathbb{Q})$ has rank 3. Hence there are 7 Klein 4-subfields, one of which is real. The remaining 6 are exactly those of Theorem 4.2.2, if $p \equiv \pm 3 \pmod{8}$.

Unlike Theorem 4.2.1, Theorem 4.2.2 has no class number condition. The reason is because in Theorem 4.2.1 no subfield of L was 2-rational, while every L in Theorem 4.2.2 has a subfield which is 2-rational. Observe that both L_- and $F = \mathbb{Q}(\sqrt{k})$ where $k = \frac{mn}{(m,n)^2}$, are imaginary subfields of L and both are 2-rational by Theorem 4.1.1. But L/L_- is not necessarily unramified outside S_- , as some divisors of odd rational primes may ramify in L/L_- . Hence we cannot conclude that L is 2-rational. However, L/F is unramified outside \tilde{S} . Therefore L is 2-rational by Lemma 2.2.15.

Lemma 4.2.3. $B_{S_+} = 0$ if L_+ is any of the real quadratic subfields of $\mathbb{Q}(\zeta_{8p})$, where p is a prime $\equiv \pm 3 \pmod{8}$.

Proof. If $L_+ = \mathbb{Q}(\sqrt{p})$ where p is any prime, or if $L_+ = \mathbb{Q}(\sqrt{2p})$ where p is a prime $\equiv 3 \pmod{4}$, then h_{L_+} is odd by Theorem 2.1.14.

If $m = 2p$ where $p \equiv 5 \pmod{8}$, then $h_{L_+} \equiv 2 \pmod{4}$ by Proposition 2.1.18 and Proposition 2.1.19. To show that P_{L_+} is not principal we apply norm to L_+/\mathbb{Q} . Suppose P_{L_+} is principal, then $N_{L_+/\mathbb{Q}}(a+b\sqrt{2p}) = a^2 - b^2(2p) = \pm 2$. Which implies that $a^2 \equiv \pm 2 \pmod{p}$. Since $-1 \equiv \square \pmod{p}$, we have $2 \equiv \square \pmod{p}$. But $2 \equiv \square \pmod{p}$ iff $p \equiv \pm 1 \pmod{8}$. A contradiction. Hence there is no algebraic integer of norm ± 2 in L_+ , and hence P_{L_+} is not principal in L_+ . \square

Now we determine the structure of $G_{L_+}(2)$. Observe that there are 3 primes above 2 and infinity in L_+ , namely $\{P_{L_+}, \infty_1, \infty_2\}$. Since $p = 2$, we have $\delta = \delta_\varphi = 1$. Moreover $B_{S_+} = 0$ by Lemma 4.2.3. Hence by the rank formula, (1) of Theorem 2.2.13, $G_{L_+}(2)$ has 3 generators. Therefore, by Theorem 2.2.8, we have $G_{L_+}(2)/G_{L_+}(2)^{(1)} \cong C_2 \times C_2 \times C_2$. Now by a proven case of Leopoldt's conjecture (Theorem 2.1.22), L_+ has a unique \mathbb{Z}_2 -extension. Hence $G_{L_+}(2)^{ab} \cong C_{2^k} \times C_{2^l} \times \mathbb{Z}_2$, for some $k, l \geq 1$.

Since L is 2-rational and L/L_+ is unramified outside S_+ , $G_{L_+}(2)$ has a free subgroup $G_L(2)$, of index 2. Moreover, $G_L(2)$ has rank 3 by (1) of Theorem 2.2.13. Hence, applying Theorem 2.2.6, we have that

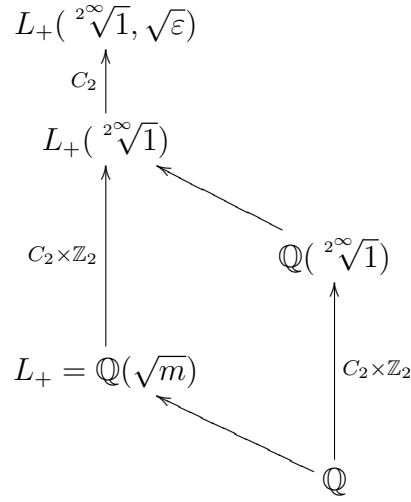
$$G_{L_+}(2) \cong (C_2 \times 1) \amalg (C_2 \times 1) \amalg \mathbb{Z}_2$$

or $(C_2 \times \mathbb{Z}_2) \amalg (C_2 \times 1)$. The former group is topologically generated by $\langle a, b, c \mid a^2 = b^2 = 1 \rangle$, where a denotes the generator of $C_2 \times 1$, b denotes the generator of $C_2 \times 1$ and c denotes the topological generator of \mathbb{Z}_2 . On the other hand, the latter group is topologically generated by $\langle a, b, c \mid a^2 = b^2 = 1, ac = ca \rangle$ where a and c denote the generator of $C_2 \times \mathbb{Z}_2$, with $a^2 = 1$ and b denotes the generator of $C_2 \times 1$. It is easy to see that the latter has 3 relations while the former has only 2. However by (2) of Theorem 2.2.13, G_{S_+} has 2 relations. Whence

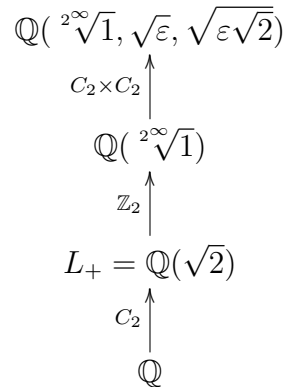
$$G_{L_+}(2) \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$$

[see Remark 4.2.7 for further explanations on how we obtained the structure of $G_{L_+}(2)$]. Thus $k = l = 1$. Since $G_L(2)$ is free, by Lemma 2.2.15, we see that $G_{L_+}(2)$ is a virtually free pro-2 group.

The following diagrams show the number fields corresponding to the abelianisation of G_{S_+} . If m is a prime $\equiv \pm 3 \pmod{8}$ or $m = 2p$ where p is a prime $\equiv \pm 3 \pmod{8}$, and ε is the fundamental unit in L_+ .



If $m = 2$, the fundamental unit in L_+ is $\varepsilon = 1 + \sqrt{2}$, hence $\varepsilon\sqrt{2} = 2 + \sqrt{2}$, therefore $\sqrt{\varepsilon\sqrt{2}} = \sqrt{2 + \sqrt{2}}$. Note that $L_+ \subset \mathbb{Q}(\sqrt[2^\infty]{1})$



To complete the theorem we need the following auxiliary results.

Lemma 4.2.4. *If only two finite primes ramify in L , then L is 2-rational if and only if L*

is one of the imaginary biquadratic subfields of $\mathbb{Q}(\zeta_{8p})$ where $p \equiv \pm 3 \pmod{8}$.

Proof. We have already shown that if L is any one of the imaginary biquadratic subfields of $\mathbb{Q}(\zeta_{8p})$ where $p \equiv \pm 3 \pmod{8}$, then L is 2-rational. To prove the converse, let L be any imaginary biquadratic subfield of $\mathbb{Q}(\zeta_{8p})$ where $p \equiv \pm 1 \pmod{8}$. Then, $F = \mathbb{Q}(\sqrt{-2p})$ or $\mathbb{Q}(\sqrt{-p})$. Now, there are two outcomes. Either $g_2 > 1$ in L or $h_F \equiv 0 \pmod{4}$. In the latter case L/F is totally ramified and hence $h_L \equiv 0 \pmod{4}$. However, P_L^2 is principal. Hence the conditions imposed by Corollary 2.2.14, prevents L from being 2-rational. \square

Proposition 4.2.5. *If more than two finite primes ramify in L , then L is not 2-rational.*

Proof. We are interested only in the imaginary biquadratic fields L in which 2 ramifies and does not factor. If three finite primes 2, p and q ramify in L , then L is contained in $\mathbb{Q}(\zeta_{8pq})$, and L is one of the following biquadratic fields. $\mathbb{Q}(\sqrt{*p}, \sqrt{*q})$, $\mathbb{Q}(\sqrt{*2p}, \sqrt{*q})$, $\mathbb{Q}(\sqrt{*2p}, \sqrt{*2q})$, $\mathbb{Q}(i, \sqrt{*pq})$, $\mathbb{Q}(\sqrt{*2}, \sqrt{*pq})$ where $* = \pm$. If $e_2 = 4$ in L , then the genus number of L is 4 (by the genus number formula given in [3], also used in the proof of Theorem 4.1.1). However, the genus field \hat{L} is a Klein 4-extension of L . Hence P_L cannot generate the 2-part of the class group of L .

However, if $e_2 = 2$ in L , then the genus number of L is 2 and the genus field \hat{L} is a degree 2-extension of L . If $h_L \equiv 0 \pmod{4}$, then P_L cannot generate the 2-part of the class group of L . But, if $h_L \equiv 2 \pmod{4}$, then we need a more subtle analysis. Here we somehow need to show that P_L cannot generate the 2-part of the class group of L . One way to do this is by showing that P_L splits in \hat{L} . Observe that \hat{L} is one of the following subfields of $\mathbb{Q}(\zeta_{8pq})$, namely $L(i)$, $L(\sqrt{*2})$, $L(\sqrt{*p})$ or $L(\sqrt{*q})$ where $* = \pm$. It is easy to see that \hat{L} will contain $\mathbb{Q}(\sqrt{d})$, where $d \equiv 1 \pmod{8}$ and d is either $\pm p$, $\pm q$ or $\pm pq$. Observe that $\mathbb{Q}(\sqrt{d})$ does not lie in L . But 2 splits in $\mathbb{Q}(\sqrt{d})$, where $d \equiv 1 \pmod{8}$, and hence P_L will split in \hat{L} . Then we can show that P_L is principal in L by looking at the Artin map restricted to the Sylow 2-subgroup of the ideal class group of L .

Suppose more than 3 finite primes ramify in L . If $e_2 = 2$ in L , then P_L^2 is principal. Using the genus formula, the genus number of L is a multiple of 4 and hence $h_L \equiv 0 \pmod{4}$. Similarly, if $e_2 = 4$ in L , then the genus number of L is a multiple of 8 and $h_L \equiv 0 \pmod{8}$. \square

Now, we can give a quick proof of Theorem 3.2.1(Markshaitis's result).

Theorem 4.2.6. $G_{\mathbb{Q}}(2) \cong C_2 \amalg \mathbb{Z}_2$

Proof. Let $S = \{2, \infty\}$. Since $h_{\mathbb{Q}} = 1$, we have $B_S = 0$ by (2) of Corollary 2.2.14. Applying (1) of Theorem 2.2.13, we see that $G_{\mathbb{Q}}(2)$ has 2 generators and using (2) of Theorem 2.2.13, we see that $G_{\mathbb{Q}}(2)$ has 1 relation. We know that the maximal elementary abelian 2-extension of \mathbb{Q} unramified outside S is $\mathbb{Q}(i, \sqrt{2})$. Hence, $G_{\mathbb{Q}}(2)/G_{\mathbb{Q}}(2)^{(1)} \cong C_2 \times C_2$. However, we know that $\text{Gal}(\mathbb{Q}(\sqrt[2^{\infty}]{1})/\mathbb{Q}) \cong C_2 \times \mathbb{Z}_2$. Hence $G_{\mathbb{Q}}(2)^{ab} \cong C_2 \times \mathbb{Z}_2$. Since $\mathbb{Q}(i)$ is a degree 2-extension of \mathbb{Q} unramified outside S , we see that $G_{\mathbb{Q}(i)}(2)$ is a subgroup of $G_{\mathbb{Q}}(2)$ by Lemma 2.2.15. Since $h_{\mathbb{Q}(i)} = 1$, we have $B_{\tilde{S}} = 0$, where \tilde{S} is the set of prime divisors of 2 and infinite primes of $\mathbb{Q}(i)$. Hence $G_{\mathbb{Q}(i)}(2)$ is free by Corollary 2.2.14. Therefore $G_{\mathbb{Q}}(2)$ has a free subgroup $G_{\mathbb{Q}(i)}(2)$, of index 2. Moreover, $G_{\mathbb{Q}(i)}(2)$ has rank 2 by (1) of Theorem 2.2.13. Hence, applying Theorem 2.2.6 we have $G_{\mathbb{Q}}(2) \cong (C_2 \times 1) \amalg \mathbb{Z}_2$ or $(C_2 \times \mathbb{Z}_2) \amalg 1$. The latter group is abelian. However $G_{\mathbb{Q}}(2)$ is nonabelian. Hence $G_{\mathbb{Q}}(2) \cong C_2 \amalg \mathbb{Z}_2$ and it is virtually free. Therefore \mathbb{Q} is a solution of (\mathcal{Q}_1) for $p = 2$. \square

Remark 4.2.7. *In the argument given in Theorem 4.2.2 for capturing the structure of $G_{L_+}(2)$, we do not consider the case when $G_{L_+}(2) \cong (C_2 \times \mathbb{Z}_2) \amalg \mathbb{Z}_2$, even though it has 2 relations and 3 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 $G_{L_+}(2)$, then $G_{L_+}(2)^{ab}$ would be $C_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Which would imply that L_+ has 2 independent \mathbb{Z}_2 -extensions. A contradiction.*

Remark 4.2.8. *It is known that the p -rational fields satisfy Leopoldt's conjecture [12]. A natural question is whether the virtually free pro- p fields, i.e., number fields K , for which $G_K(p)$ is virtually free, satisfy Leopoldt's conjecture. The answer is yes. Because, virtually free pro- p fields have a field extension which is p -rational, and by Theorem 2.1.23 if the Leopoldt's conjecture is true for a prime p and a number field K , then it is also true for p and every subfield of K .*

Remark 4.2.9. *If m is a prime congruent to $3 \pmod{8}$ and $n = -1$ or if $m = 2p$ where p is a prime congruent to $3 \pmod{8}$ and $n = -2$, then $G_L(2)$ is the inertia subgroup of $G_{L^+}(2)$ for the prime P_{L^+} . Note that in case (c), $G_L(2)$ is not a subgroup of $G_{L^+}(2)$.*

Remark 4.2.10. *The cohomological dimension of $G_L(2)$ is one, since $G_L(2)$ is a free pro-2 group. But the cohomological dimension of $G_{L^+}(2)$ is infinity, since*

$$G_{L^+}(2) \cong C_2 \amalg C_2 \amalg \mathbb{Z}_2$$

and hence has an element of order 2.

□

4.2.3 Virtually free extensions

Corollary 4.2.11. *Let K be a quadratic number field. Suppose K is not 2-rational. Then K has a degree 2-extension L , such that L is Galois over \mathbb{Q} and is 2-rational if and only if K is any real quadratic subfield of $\mathbb{Q}(\zeta_{8p})$ where p is a prime $\equiv \pm 3 \pmod{8}$ and in each of these cases*

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

where S is the set of prime divisors of 2 and infinite primes of K .

Proof. All the degree 4-extensions of \mathbb{Q} we investigate are normal. Theorems 4.2.1 and 4.2.2 characterize all degree 4 normal extensions of \mathbb{Q} which are 2-rational and contain K , hence

the proof follows. Observe that K is virtually free. Therefore these quadratic number fields are solutions of (\mathcal{Q}_1) for $p = 2$. \square

4.2.4 Minimal 2-rational extensions

Definition 4.2.12. *A number field K is said to be minimal p -rational if K is p -rational and if there does not exist any proper, p -rational, subfield F of K , such that K/F is a p -extension unramified outside \tilde{S} , where \tilde{S} is the set of prime divisors of p and the infinite primes of F .*

Corollary 4.2.13. *The only minimal 2-rational degree 4 normal extensions of \mathbb{Q} are the imaginary cyclic extensions of \mathbb{Q} of Theorem 4.2.1.*

Proof. \mathbb{Q} is not 2-rational, because \mathbb{Q} is real. By Theorem 4.2.2 no biquadratic extension of \mathbb{Q} is minimal 2-rational. Hence any minimal 2-rational degree 4 normal extension of \mathbb{Q} must be cyclic over \mathbb{Q} . Proof of the cyclic case follows from Theorem 4.2.1. \square

4.2.5 Cyclic extension revisited

We will describe the structure of $G_{L_+}(2)$ of Theorem 4.2.1. Observe that except in the case when 2 is the only ramifying prime in L , $G_L(2)$ is not a subgroup of $G_{L_+}(2)$ as divisors of odd primes ramify in L/L_+ . Hence we cannot apply Theorem 2.2.6 directly. However, note that every L_+ of Theorem 4.2.1 is one of the L_+ of Theorem 4.2.2, hence we see that the biquadratic number field L of Theorem 4.2.2 is a degree 2 extension of L_+ which is unramified outside the prime divisors of 2 and infinity. Hence the structure of $G_{L_+}(2)$ of Theorem 4.2.1 is identical to the structure of $G_{L_+}(2)$ of Theorem 4.2.2.

Here is a compiler ready Magma code to show that a number field L exists with the given class number condition in 2(a), 2(b) and 2(c) of Theorem 4.2.1.

```
 $K := CyclotomicField(80);$ 
```

```
 $M := SubfieldLattice(K);$ 
```

```
for ent in M do
```

```

L := NumberField(ent);
if Degree(L) eq 4 then
  N := SubfieldLattice(L);
  for ent in N do
    F := NumberField(ent);
    if Degree(F) eq 2 then
      print " sig = ",Signature(L), " cnum = ",#ClassGroup(L),
      " sig = ",Signature(F), " cnum = ",#ClassGroup(F);
    end if;
  end for;
end if;
end for;

```

The program loops through all the degree 4 extensions L of \mathbb{Q} contained in $\mathbb{Q}(\zeta_{80})$ and then for each L it loops through all the quadratic extensions F of \mathbb{Q} contained in L . The $\text{signature}(L)$ gives the number of real embeddings followed by the number of pairs of complex embeddings of L and the “ $cnum$ ” gives the order of the Class Group. If L is totally imaginary cyclic of degree 4, then it will have only one quadratic (real) subfield F . Observe that if $F = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{5})$, then $h_F = 1$ and by Genus theory h_L is even if the conductor of L has more than one prime factor. If $F = \mathbb{Q}(\sqrt{10})$, then $h_F = 2$ and by Genus theory $4 \mid h_L$.

Now, $\chi_5 : (\mathbb{Z}/5\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$, defined by $\chi_5(2) = i$. Therefore, $o(\chi_5) = 4$ and the field of $\chi_5 = L_5 = \mathbb{Q}(\zeta_5)$. Hence the conductor of χ_5 is 5. Moreover, χ_1 is a generator of $\mathbb{Z}/2\mathbb{Z}$. The field of $\chi_1 = L_1 = \mathbb{Q}(i)$ and hence has conductor 4. The field of $\chi_2 = L_2 = \mathbb{Q}(\zeta_{2^4} + \zeta_{2^4}^{-1})$ and hence has conductor 16. The following set of tables connect the output of Magma with the appropriate field and corresponding generating character set.

| Magma Output | L | generating characters |
|--------------------|---------------------------|------------------------------------|
| sig = 0 2 cnum = 1 | $\mathbb{Q}(\sqrt{2}, i)$ | $\langle \chi_1, \chi_2^2 \rangle$ |
| sig = 0 1 cnum = 1 | | |
| sig = 0 2 cnum = 1 | | |
| sig = 2 0 cnum = 1 | | |
| sig = 0 2 cnum = 1 | | |
| sig = 0 1 cnum = 1 | | |

Table 4.2.1

The first 6 lines of magma output are given in the first column of the above table. The first line “ $sig = 0$ 2 $cnum = 1$ ” says that L has 0 real embeddings and 2 pairs of complex embeddings and $h_L = 1$. Observe that the first, third and the fifth lines are identical. This says that we are looking at the same number field L . The even numbered lines give the signature and the class number of the 3 quadratic subfields of L . The second line says that the quadratic subfield of L has only one pair of complex embedding hence it is imaginary, and its class number is 1. The fourth lines says that the class number of the real quadratic subfield is 1. The sixth line says the third quadratic subfield is imaginary with class number 1. Now, there is only one imaginary biquadratic number field $L \subset \mathbb{Q}(\zeta_{80})$ having class number 1 with the class number of each of its subfields being 1; namely $\mathbb{Q}(\sqrt{2}, i)$ and is generated by the characters $\langle \chi_1, \chi_2^2 \rangle$. The biquadratic number field $L = \mathbb{Q}(\sqrt{2}, i)$ satisfies the hypotheses of 1(a) of Theorem 4.2.2 and hence it is 2-rational.

| Magma Output | L_+ | L | Character |
|--------------------|------------------------|-------------|-------------------|
| sig = 4 0 cnum = 2 | $\mathbb{Q}(\sqrt{2})$ | Real cyclic | $\chi_2 \chi_5^2$ |
| sig = 2 0 cnum = 1 | | | |

Table 4.2.2

The next two lines of magma output are as given in the first column of the above table.

Observe that line 7 which is the first line in the above table and line 9 which is the first line in the next table are different. Hence the number field L described by the first line of the above table has a unique quadratic subfield, hence L is cyclic. The first line of the above table “ $sig = 4\ 0\ cnum = 1$ ” says that L has 4 real embeddings and 0 pairs of complex embeddings and $h_L = 2$ and the second line of the above table says that its real quadratic subfield has class number 1. Now, there are only two real quadratic subfields of $\mathbb{Q}(\zeta_{80})$ with class number 1; namely $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$. If L is real and $h_L = 2$, then by Theorem 2.1.16, $L_+ = \mathbb{Q}(\sqrt{2})$, for otherwise $e_2 = 2$ in L and h_L would be odd. Since the cyclic degree 4 number field L is real, L does not satisfy the hypotheses of Theorem 4.2.1. Hence L is not 2-rational. Hence forth we will ignore the output of magma which deals with degree 4 real subfields of $\mathbb{Q}(\zeta_{80})$

| Magma Output | L_+ | L of $2(a)$ | Character |
|--------------------|------------------------|---------------|------------------------|
| sig = 0 2 cnum = 2 | $\mathbb{Q}(\sqrt{2})$ | Imaginary | $\chi_1\chi_2\chi_5^2$ |
| sig = 2 0 cnum = 1 | | cyclic | |

Table 4.2.3

Since L is imaginary and $h_L = 2$, and $h_{L_+} = 1$, then L is the number field of $2(a)$ or $2(b)$ of Theorem 4.2.1. Hence $L_+ = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{5})$ (Table 4.2.12). Hence the above calculation shows that the imaginary cyclic number field L with $L_+ = \mathbb{Q}(\sqrt{2})$ satisfies the hypotheses $2(a)$ of Theorem 4.2.1 and hence L is 2-rational.

| Magma Output | L_+ | L of $1(a)$ | Character |
|--------------------|------------------------|-----------------------|-----------|
| sig = 0 2 cnum = 1 | $\mathbb{Q}(\sqrt{5})$ | $\mathbb{Q}(\zeta_5)$ | χ_5 |
| sig = 2 0 cnum = 1 | | | |

Table 4.2.4

Since L is imaginary and $h_L = 1$, and $h_{L_+} = 1$, then L is the number field of $1(a)$ or $1(b)$ of Theorem 4.2.1. Hence $L_+ = \mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\sqrt{2})$ (Table 4.2.13). Hence the above calculation

shows that the imaginary cyclic number field L with $L_+ = \mathbb{Q}(\sqrt{5})$ satisfies the hypotheses 1(a) of Theorem 4.2.1 and hence L is 2-rational.

| Magma Output | L | generating characters |
|--------------------|-----------------------------------|---|
| sig = 0 2 cnum = 2 | $\mathbb{Q}(\sqrt{2}, \sqrt{-5})$ | $\langle \chi_2^2, \chi_1 \chi_5^2 \rangle$ |
| sig = 0 1 cnum = 2 | | |
| sig = 0 2 cnum = 2 | | |
| sig = 0 1 cnum = 2 | | |
| sig = 0 2 cnum = 2 | | |
| sig = 2 0 cnum = 1 | | |

Table 4.2.5

There is only one imaginary biquadratic subfield of $\mathbb{Q}(\zeta_{80})$ with its class number being 2 and the class number of both of its imaginary quadratic subfields being 2 and that of its real quadratic subfield being 1. Hence the imaginary biquadratic number field $L = \mathbb{Q}(\sqrt{2}, \sqrt{-5})$ satisfies the hypotheses 1(c) of Theorem 4.2.2 and hence L is 2-rational.

| Magma Output | L | generating characters |
|--------------------|---------------------------|------------------------------------|
| sig = 0 2 cnum = 1 | $\mathbb{Q}(\sqrt{5}, i)$ | $\langle \chi_1, \chi_5^2 \rangle$ |
| sig = 0 1 cnum = 1 | | |
| sig = 0 2 cnum = 1 | | |
| sig = 2 0 cnum = 1 | | |
| sig = 0 2 cnum = 1 | | |
| sig = 0 1 cnum = 2 | | |

Table 4.2.6

There are exactly 3 biquadratic number fields $L \subseteq \mathbb{Q}(\zeta_{80})$, with $h_L = 1$ and the class

number of two of its quadratic subfields being 1 and the third being 2. One of them being real (and hence we will ignore it), and the other two being imaginary, are described in the above table and in Table 4.2.9. The quadratic number field with class number 2 is either $\mathbb{Q}(\sqrt{10})$ (in the real case) or $\mathbb{Q}(\sqrt{-10})$, $\mathbb{Q}(\sqrt{-5})$ (in the imaginary case). The above computation shows that $L = \mathbb{Q}(\sqrt{5}, i)$ satisfies the hypotheses 1(a) of Theorem 4.2.2 and hence L is 2-rational.

| Magma Output | L | generating characters |
|--------------------|----------------------------|---|
| sig = 0 2 cnum = 2 | $\mathbb{Q}(\sqrt{10}, i)$ | $\langle \chi_1, \chi_2^2 \chi_5^2 \rangle$ |
| sig = 0 1 cnum = 1 | | |
| sig = 0 2 cnum = 2 | | |
| sig = 2 0 cnum = 2 | | |
| sig = 0 2 cnum = 2 | | |
| sig = 0 1 cnum = 2 | | |

Table 4.2.7

There are exactly 3 biquadratic number fields $L \subseteq \mathbb{Q}(\zeta_{80})$, with $h_L = 2$ and the class number of two of its quadratic subfields being 2 and the third being 1. One of them has been described in Table 4.2.5, and the other two are described in the above table and in table below (4.2.8). The quadratic number field with class number 1 is either $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$. The above computation shows that $L = \mathbb{Q}(\sqrt{10}, i)$ satisfies the hypotheses 1(a) of Theorem 4.2.2 and hence L is 2-rational.

| Magma Output | L | generating characters |
|--------------------|------------------------------------|--|
| sig = 0 2 cnum = 2 | $\mathbb{Q}(\sqrt{10}, \sqrt{-2})$ | $\langle \chi_1 \chi_2^2, \chi_2^2 \chi_5^2 \rangle$ |
| sig = 0 1 cnum = 1 | | |
| sig = 0 2 cnum = 2 | | |
| sig = 0 1 cnum = 2 | | |
| sig = 0 2 cnum = 2 | | |
| sig = 2 0 cnum = 2 | | |

Table 4.2.8

The above computation shows that $L = \mathbb{Q}(\sqrt{10}, \sqrt{-2})$ satisfies the hypotheses 1(b) of Theorem 4.2.2 and hence L is 2-rational.

| Magma Output | L | generating characters |
|--------------------|-----------------------------------|---|
| sig = 0 2 cnum = 1 | $\mathbb{Q}(\sqrt{5}, \sqrt{-2})$ | $\langle \chi_1 \chi_2^2, \chi_5^2 \rangle$ |
| sig = 0 1 cnum = 1 | | |
| sig = 0 2 cnum = 1 | | |
| sig = 0 1 cnum = 2 | | |
| sig = 0 2 cnum = 1 | | |
| sig = 2 0 cnum = 1 | | |

Table 4.2.9

The above computation shows that $L = \mathbb{Q}(\sqrt{5}, \sqrt{-2})$ satisfies the hypotheses 1(b) of Theorem 4.2.2 and hence L is 2-rational.

| Magma Output | L_+ | L of 2(c) | Character |
|--------------------|-------------------------|-------------|----------------|
| sig = 0 2 cnum = 4 | $\mathbb{Q}(\sqrt{10})$ | Imaginary | $\chi_2\chi_5$ |
| sig = 2 0 cnum = 2 | | cyclic | |

Table 4.2.10

There exactly 2, cyclic, degree 4 number fields $L \subseteq \mathbb{Q}(\zeta_{80})$ such that $4 \parallel h_L$. Both are imaginary, one of them is described in the above table and the other in Table 4.2.11. Now, since $h_{L_+} = 2$, we have $L_+ = \mathbb{Q}(\sqrt{10})$. The above computation shows that L satisfies the hypotheses 2(c) of Theorem 4.2.1.

| Magma Output | L_+ | L of 2(c) | Character |
|---------------------|-------------------------|-------------|------------------|
| sig = 0 2 cnum = 20 | $\mathbb{Q}(\sqrt{10})$ | Imaginary | $\chi_2\chi_5^3$ |
| sig = 2 0 cnum = 2 | | cyclic | |

Table 4.2.11

The above computation shows that L satisfies the hypotheses 2(c) of Theorem 4.2.1.

| Magma Output | L_+ | L of 2(b) | Character |
|--------------------|------------------------|-------------|------------------|
| sig = 0 2 cnum = 2 | $\mathbb{Q}(\sqrt{5})$ | Imaginary | $\chi_2^2\chi_5$ |
| sig = 2 0 cnum = 1 | | cyclic | |

Table 4.2.12

The above computation shows that L satisfies the hypotheses 2(b) of Theorem 4.2.1.

| Magma Output | L_+ | L of 1(b) | Character |
|--------------------|------------------------|-------------|----------------|
| sig = 0 2 cnum = 1 | $\mathbb{Q}(\sqrt{2})$ | Imaginary | $\chi_1\chi_2$ |
| sig = 2 0 cnum = 1 | | cyclic | |

Table 4.2.13

The above computation shows that L in the above table satisfies the hypotheses 1(b) of

Theorem 4.2.1.

The Magma code when L is contained in $\mathbb{Q}(\zeta_{48})$ is identical, replace 80 by 48 in the first line of the code. Here $\chi_3 : (\mathbb{Z}/3\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$, defined by $\chi_3(2) = -1$ and the field of $\chi_3 = L_3 = \mathbb{Q}(\sqrt{-3})$ and hence has conductor 3.

Chapter 5

Some nonabelian extensions K of \mathbb{Q} with a virtually free $G_K(2)$

In this chapter we study some finite nonabelian extensions K of \mathbb{Q} which are solutions of (\mathcal{Q}_1) for $p = 2$. In particular we focus on split metacyclic extensions. Again, we explicitly describe $G_K(2)$ using Theorem 2.2.6.

Remark 5.0.14. *Henceforth, we will assume that $g_2 = 1$ in every number field.*

5.1 Nonabelian examples of 2-rational number fields

We first look at simple examples of nonabelian 2-rational number fields.

Example 5.1.1. *Let L be one of the D_8 -extensions discussed in example 3.3.5; namely $\mathbb{Q}(i, 2^{\frac{1}{4}})$. It was shown that L is 2-rational by using Theorem 3.3.1, however we can also show the 2-rationality using Lemma 2.2.15, 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*

$$K = \mathbb{Q}(2^{\frac{1}{4}}) \subset L$$

Observe that K is not 2-rational as K has a real embedding. In fact K has 2 real embeddings and 2 complex embeddings. Hence K has 2 real places and 1 complex place. By (1) of Theorem 2.2.13, $G_K(2)$ has 4 generators. Hence by Theorem 2.2.8, we have

$$G_K(2)/(G_K(2))^{(1)} \cong C_2 \times C_2 \times C_2 \times C_2$$

Now, by Leopoldt's conjecture, K has exactly 2 independent \mathbb{Z}_2 -extensions. Observe that K actually satisfies Leopoldt's conjecture, because L/F is an abelian extension and by Theorem 2.1.22, L satisfies Leopoldt's conjecture. Now, by Theorem 2.1.23, K being a subfield of L , satisfies Leopoldt's conjecture.

Hence $G_K(2)^{ab} \cong C_{2^k} \times C_{2^l} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, for $k, l \geq 1$. $G_K(2)$ has a free subgroup of index 2 because L/K 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 by (1) of Theorem 2.2.13. Hence we can apply Theorem 2.2.6. Therefore

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

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, by (2) of Theorem 2.2.13, $G_K(2)$ has only 2 relations, whence

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

and it is virtually free. Hence $k = l = 1$.

Example 5.1.2. 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 by Theorem 3.3.1. 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 $G_{K_4}(2) \cong F_2(2)$

by Theorem 3.3.1 or by Theorem 4.1.1. 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 5.2.2.

5.2 On split metacyclic extensions

In this section, we first look at nonabelian extensions of order pq , then extensions of the form $G' \rtimes M$, where both G' and M are cyclic, where G' denotes the commutator subgroup of G . Then we finish this section with a discussion on D_8 -extensions.

5.2.1 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 5.2.1. $e_2 = p$ in K .

Proof. Let D_{P_K} and I_{P_K} denote the decomposition group and the inertia group respectively for P_K . Recall by remark 5.0.14, $D_{P_K} = G$. Suppose that $q = 2$. Applying theorem 2.1.8 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 2.1.8 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 $[F : \mathbb{Q}] = q$. By Lemma 3.1.1 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 5.2.2. $o(P_K) = 1$ 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 2.2.14, we demand that L be totally imaginary. 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. Let h_K^+ denote the extended class number of K .

Theorem 5.2.3. *Let $\text{Gal}(K/\mathbb{Q})$ be a nonabelian group of order pq . If $q = 2$, assume that K is real. Suppose $g_2 = 1$ in K and $L = K(i)$ 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*

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

Proof. K is real if either $q = 2$ (by assumption) or if q is odd, since the order of the Galois group of K is odd. Hence K is not 2-rational by Corollary 2.2.14. 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 2.1.10, but we tailor it to suit our needs. Suppose we assume to the contrary that h_L is even. Let \mathcal{L}_1 be the Hilbert 2-class field of L . Since L/K is Galois, the maximality of \mathcal{L}_1 implies that \mathcal{L}_1/K is Galois. Let $P_{\mathcal{L}_1}$ be a prime divisor of P_K in \mathcal{L}_1 . Observe that P_K ramifies in L . Let $I_{P_{\mathcal{L}_1}}$ denote the inertia group for $P_{\mathcal{L}_1}$ in $\text{Gal}(\mathcal{L}_1/K)$. Since \mathcal{L}_1/L is unramified, we have $|I_{P_{\mathcal{L}_1}}| < |\text{Gal}(\mathcal{L}_1/K)|$. Since $\text{Gal}(\mathcal{L}_1/K)$ is a finite 2-group, there exists a normal subgroup \tilde{G} of $\text{Gal}(\mathcal{L}_1/K)$ of index 2, with $I_{P_{\mathcal{L}_1}} \subseteq \tilde{G} \subseteq \text{Gal}(\mathcal{L}_1/K)$. The inertia

subgroups of other prime divisors of P_K in \mathcal{L}_1 above P_K are conjugates of $I_{P_{\mathcal{L}_1}}$, 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 2.2.14, L is 2-rational. Whence $G_K(2)$ is virtually free, 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}_1 denote the Hilbert 2-class field of K . Consider $L\mathcal{K}_1/L$. Since L/K is totally ramified at P_K , $L\mathcal{K}_1/L$ is an unramified 2-extension. Hence $2 \mid h_L$. A contradiction.

Since L is 2-rational, by (1) of Corollary 2.2.14, we have $B_{\tilde{S}} = 0$, where \tilde{S} is the set of prime divisors of 2 and infinity. Recall that by (2) of Corollary 2.2.14, 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 5.2.2, 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 2.2.13, $G_K(2)$ 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 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 Remark 4.2.8. Now, K being a subfield of L satisfies Leopoldt's conjecture by Theorem 2.1.23.

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 $pq + 1$ by (1) of Theorem 2.2.13. Hence, applying Theorem 2.2.6, we have that

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

or $(C_2 \times \mathbb{Z}_2) \amalg \cdots \amalg (C_2 \times 1)$, 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, by (2) of Theorem 2.2.13, $G_K(2)$ 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 . 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 5.2.4. *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 5.2.1. 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, $\text{Gal}(K/\mathbb{Q}) \cong C_3 \times C_2 \cong S_3$, $h_K^+ = 1$ and that there is a unique prime above 2. Hence it satisfies the hypotheses of Theorem 5.2.3. Hence the set of number fields with the hypotheses of Theorem 5.2.3 is not an empty set. Moreover, $\text{Gal}(L/\mathbb{Q}) \cong D_{12}$.

Example 5.2.2. Going back to example 5.1.2, 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 2.2.14, $G_{K_j}(2)$ cannot be free. By (1) of Theorem 2.2.13, each $G_{K_j}(2)$ has 3 generators. Hence by Theorem 2.2.8, 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 and by Theorem 2.1.22, L satisfies Leopoldt's conjecture. Now, by Theorem 2.1.23, K_j being a subfield of L , satisfies Leopoldt's conjecture. Hence $G_{K_j}(2)^{ab} \cong C_{2^k} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, 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 5.2.3. 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 by Corollary 2.2.14, 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 of index 2. Moreover, $G_F(2)$ has rank 4 by (1) of Theorem 2.2.13. Hence, applying Theorem 2.2.6, 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, by (2) of Theorem 2.2.13, $G_{K_j}(2)$ 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 5.2.5. Observe that in Theorem 5.2.3, 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 5.2.6. 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 5.2.3, 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 5.2.7. *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.*

5.2.2 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 $|M| = m$.

Example 5.2.3. *Any of the groups $\text{Gal}(K/\mathbb{Q})$ considered in section 5.2.1 or let*

$$G = \text{Gal}(K/\mathbb{Q}) \cong C_p \rtimes C_{p-1}$$

Here $G' = C_p$.

Lemma 5.2.8. $e_2 \geq n$ 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 2.1.8 we have that $I_{P_K} = G'$ if G is not a 2-group. \square

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

Theorem 5.2.9. 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 5.2.3 □

Now, let n be even. Then we have

Corollary 5.2.10. *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 $G_L(2) \cong F_2(|G| + 1)$.*

5.2.3 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 5.2.2

Lemma 5.2.11. $e_2 = 4$ 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 . □

Assume K is real and $L = K(i)$ or $K(\sqrt{-2})$. Then we have

Theorem 5.2.12. *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 $G_K(2) \cong F_2(9)$.

Proof. Proof is identical to the proof of Theorem 5.2.3. □

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

Theorem 5.2.13. *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 2.2.14 we have $B_S = 0$.

Now, by Corollary 2.2.14, 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 $\mathcal{K}_1^+ = L$, where \mathcal{K}_1^+ 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}_1 be the Hilbert 2-class field of L . Since L/K is Galois, the maximality of \mathcal{L}_1 implies that \mathcal{L}_1/K is Galois. Note that $\text{Gal}(\mathcal{L}_1/K)$ is a 2-group of order at least 4. Therefore $\text{Gal}(\mathcal{L}_1/K)$ has a normal subgroup of index 4. Hence, K has a degree 4 abelian extension contained in \mathcal{L}_1 . This implies that $4 \mid h_K^+$. A contradiction. Hence h_L is odd and by Corollary 2.2.14, L is 2-rational. \square

5.3 On Q_8 -extensions

In this section we look at a non split 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 5.3.1. $e_2 = 4$ or 8 in K .

Proof. Since Q_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

Assume K is real and $L = K(i)$ or $K(\sqrt{-2})$. Then we have

Theorem 5.3.2. *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 $G_K(2) \cong F_2(9)$.

Proof. Proof is identical to the proof of Theorem 5.2.3. □

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

Theorem 5.3.3. *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 5.2.13. □

5.4 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 5.4.1. *$e_2 = 4$ 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, let $\text{Fix}(K_4)$ be the fixed field of K_4 . Hence $\text{Fix}(K_4)/\mathbb{Q}$ 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 . □

Assume K is real and $L = K(i)$ or $K(\sqrt{-2})$. Then we have

Theorem 5.4.2. *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 $G_K(2) \cong F_2(9)$.

Proof. Proof is identical to the proof of Theorem 5.2.3. □

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

Theorem 5.4.3. *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 5.2.13. □

References

- [1] P. E. Conner, J. Hurrelbrink, Class Number Parity, World Scientific 1988.
- [2] A. Fröhlich, Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields, in “Contemporary Mathematics,” Vol. 24, AMS, 1983.
- [3] Y. Furuta, The genus field and genus number in algebraic number fields, Nagoya Math. J. 29 (1967), 281-285.
- [4] W. N. Herfort, L. Ribes, and P. A. Zalesskii, p -Extensions of free pro- p groups, Forum Mathematicum (11) (1999), 49-61
- [5] G. J. Janusz, Algebraic Number Fields (second edition), American Mathematical Society 1996.
- [6] D. L. Johnson, Topics in the Theory of Group Presentations, Cambridge University Press 1980.
- [7] H. Koch, Galoissche Theorie der p -Erweiterungen. Deutscher Verlag der Wissenschaften, Berlin 1970.
- [8] H. Koch, Galois Theory of p -Extensions, Springer 2002.
- [9] A. G. Kurosh, The Theory of Groups, Volume two, Chelsea publishing company 1960.
- [10] D. A. Marcus, Number Fields, Springer, 1977.
- [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] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Springer 1999.
- [14] L. Ribes, P. Zalesskii, Profinite Groups, Springer 2000.
- [15] J. P. Serre, Galois Cohomology, Springer 2002.
- [16] J. P. Serre, Local Fields, Springer-Verlag 1979.

- [17] J. P. Serre, *Trees*, Springer-Verlag 1980.
- [18] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag 1982.
- [19] K. Wingberg, On Demuskin groups with involution. *Ann. Sci. Ecole Norm. Sup. (4)* 22 (1989), no. 4, 555–567.
- [20] P. A. Zalesskii, On virtually projective groups, *J. reine angew. Math.* 572 (2004), 97-110