Unramified Extensions of Number Fields

Trinity Term 2019

Candidate Number 1006289

University of Oxford

MMath Mathematics Part C

CCD Dissertations on a Mathematical Topic

Contents

1 Goal

This dissertation aims to show some of the techniques that have been used to find unramified extensions of number fields, the maximal unramified extension of number fields and also the structure of the Galois group of these extensions. Often, K is taken to be a quadratic number field, and unramified extensions are defined by the splitting field of some polynomial over the integers.

Also, this dissertation will survey the construction of unramified extensions of number fields, both finite and infinite.

This dissertation will focus on three topics: finding finite unramified extensions, infinite unramified extensions and maximal unramified extensions of number fields.

In addition, this dissertation will use computational mathematics packages to find concrete examples of number fields with interesting properties. The packages used are SageMath, Magma http://magma.maths.usyd.edu.au/calc/ and the online database of number fields found at https://hobbes.la.asu.edu/NFDB/ [8]. One important tool in the analysis of unramified extensions is bounds on the discriminant of a number field. Such bounds are given initially from Minkowski and then later from Odlyzko.

Various results from Galois Theory, Algebraic Number Theory and Class Field Theory will be used in this paper.

The reader of this paper is assumed to be familiar with all courses from Prelims, Part A and Part B and Part C. In particular, courses B3.1 Galois Theory, B3.4 Algebraic Number Theory, and all relevant courses on Group Theory.

2 Notation

In the following notation, K denotes a number field.

1. $gcd(a, b)$ denotes the greatest common divisor of a and b.

2. F_n denotes the n^{th} Fibonacci number, where $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

3. L_n denotes the n^{th} Lucas number, where $L_0 = 2$, $L_1 = 1$ and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$.

4. D_n denotes the dihedral group of order $2n$.
5. S_n denotes the symmetrical group on n elements.
6. Q_8 denotes the quaternion group of order 8.
7. $h(K)$ is class number of K and $Cl(K)$ is its ideal class group.
8. d_K or $\Delta(K)$ is the discriminant of K.
9. $disc(f(x))$ denotes the discriminant of the polynomial $f(x)$.
10. K^{ur} is the maximally unramified extension of K.
11. K^{tur} is the maximal tamely unramified extension of K.
12. n_K is the degree of the extension $K : \mathbb{Q}$.
13. $N_{A/B}$ denotes the relative norm for a number field extension A/B.
14. $\bar{K}$ denotes the Galois closure of K.
15. KL denotes the compositum of two number fields K and L.
16. rd_K is the root discriminant of K, $|d_K|^{\frac{1}{n_K}}$.
17. $\mathcal{O}_K$ denotes the ring of integers of K.
18. C_K is the class field group of K.
19. G^{ab} is the abelianisation of a group G, $G/[G, G]$.
20. K_n is the n_{th} term in the sequence defined by $K_0 := K$ and K_{n+1} is the Hilbert class field of K_n.
21. $K_H = \bigcup_i K_i$ is the Hilbert tower of K.
22. ζ_n is the n_{th} root of unity.
23. A number field K is said to be **unramified closed** if K has no non-trivial unramified extensions.
24. A field extension is **strictly unramified** if it is not ramified at any finite or infinite prime.

Note that in general, decimal numbers are rounded to 2 decimal places.

3 Important Results in Group Theory, Algebraic Number Theory and Class Field Theory

First, begin with some definitions and results from related areas of mathematics.

3.1 Group Theory

Lemma 1. Suppose $n \geq 5$. Then A_n and S_n are not solvable.

Lemma 2. Suppose n is prime, and G is a transitive permutation group on n letters containing a transposition. Then G is a symmetric group.

3.2 Algebraic Number Theory

Recall that a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ factors in an extension L of K as $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}_1^{e_1}...\mathfrak{B}_m^{e_m}$, where $\mathfrak{B}_i$ are ideals in $\mathcal{O}_L$ intersecting $\mathcal{O}_K$ at $\mathfrak{p}$.

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, call $\mathfrak{p}$ a **finite prime**. This is in comparison to an **infinite prime**, which is determined by embeddings of K in $\mathbb{C}$.

Each $e_i \geq 1$, and if $e_i > 1$ for some i then say that $\mathfrak{p}$ **ramifies** in L and is unramified otherwise. If $e_i = 1$ for all i then say $\mathfrak{p}$ **splits** in L. If there exists a unique prime $\mathfrak{B}$ lying over $\mathfrak{p}$ with inertial degree 1, then $\mathfrak{p}$ is **totally ramified** in L.

For an extension L/K, an infinite prime $\mathfrak{p}$ in K is ramified in L if it is real but has a complex extension to L. L/K is an **unramified extension** if all primes are unramified, finite or not.

The following theorem motivates the definition of the maximal unramified extension of a number field:

Theorem 1. The compositum of two finite unramified extensions of K is also unramified, and so the union K^{ur} of all unramified extensions is also an unramified extension of K. Furthermore, the residue field $\tilde{k}$ of K^{ur} is the algebraic closure of the residue field k of K.

Proof. Suppose K is a number field and $L, \tilde{L}$ are extensions of K. Let $\mathfrak{p}$ be an ideal unramified in both L and $\tilde{L}$. Let P be a prime lying over $\mathfrak{p}$ in $L\tilde{L}$. Let M be the minimal normal extension of $L\tilde{L}$, i.e. the normal closure. Suppose Q is a prime in M lying over P, then

$$\mathfrak{p} \subseteq P \subseteq Q \tag{1}$$

Now let $E = E(Q|\mathfrak{p})$ denote the inertia group of Q at $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified in L and $\tilde{L}$, it follows that $Q \cap \mathcal{O}_L$ and $Q \cap \mathcal{O}_{\tilde{L}}$ are unramified in L and $\tilde{L}$ respectively. But the inertia field M^E is the largest field in which $\mathfrak{p}$ is unramified, so it follows that $L \subseteq M^E$ and $\tilde{L} \subseteq M^E$, whence $L\tilde{L} \subseteq M^E$ and $\mathfrak{p}$ is unramified in $L\tilde{L}$. $\square$

Following the definition of ramification, the next theorems show whether or not a prime ramifies.

Theorem 2. Suppose that K be a field extension of $\mathbb{Q}$ with discriminant D. Then a prime p ramifies in K if and only if $p|D$.

Note that the discriminant of a number field is finite, hence only finitely many primes ramify over $\mathbb{Q}$. The following is an easy corollary:

Corollary 1. A field extension K of $\mathbb{Q}$ ramifies at precisely one prime iff the absolute value of disc(K) is a prime power.

More generally, suppose L/K is a field extension, and $\mathfrak{p}$ is a prime ideal in K. Then $\mathfrak{p}$ ramifies in L iff it divides the relative discriminant $\Delta_{K/L}$. Also, L/K is unramified iff the relative discriminant is the unit ideal.

Example 1. Suppose $f(x) = x^5 - x^3 - x^2 + x + 1$, and K is the splitting field of f over $\mathbb{Q}$. Then $\Delta(K) = -1609$, and 1609 is prime, hence 1609 is the only prime which ramifies in K over $\mathbb{Q}$. Note that f(x) is an irreducible quintic with precisely three real roots, meaning that $\Gamma(K/\mathbb{Q}) \cong S_5$ and K is an unsolvable extension of $\mathbb{Q}$.

Often it is useful to find the **Galois closure** of a number field K; this is defined to be the smallest extension field, in terms of inclusion, which contains K and is Galois over $\mathbb{Q}$. The following theorem is from Galois theory:

Theorem 3. Suppose $K = \mathbb{Q}(\alpha)$, where α is a root of an irreducible polynomial $f(x) \in \mathbb{Z}[x]$, then $\bar{K} = split(f(x), \mathbb{Q})$.

3.3 Hilbert Class Fields

Analysing the Hilbert class field - and hence the Hilbert class tower - gives information about unramified extensions of number fields. The **class field tower problem** - stated by Hasse in 1925 - asks whether or not this tower is always finite, i.e. terminates in a field with class number one. The answer was shown to be negative when Golod and Shafarevich found a counterexample in 1964.

Definition. The **class field** of the trivial subgroup of C(K) is called the Hilbert class field of K.

Definition. L/K is an **abelian extension** if it is a Galois extension and $\Gamma(L/K)$ is abelian.

The **Hilbert class field** is the maximal abelian extension of K unramified at all primes of K, i.e. it is an unramified abelian extension of K, and contains every other unramified abelian extension of K.

The degree of its extension over K is equal to the class number of K, and its Galois group is isomorphic to the ideal class group of K, taking Frobenius elements as prime ideals of K.

In particular, if K is a unique factorisation domain then K is equal to its own Hilbert class field. Here are three further examples:

Example 2. Suppose K=$\mathbb{Q}$. Then K is its own Hilbert class field.

Example 3. Suppose $K = \mathbb{Q}\left(\sqrt{-15}\right)$, and take $L = \mathbb{Q}\left(\sqrt{-3}, \sqrt{-5}\right)$. $\Delta(K) = -15$ and $\Delta(L) = -15^2$, so L is an degree 2 unramified abelian extension of K. In addition, $h(K) = 2$, so indeed $L = K_1$.

Example 4 (Hasse)**.** Suppose $K = \mathbb{Q}\left(\sqrt{-31}\right)$ with class number 3. Let L be its Hilbert class field. Then $L = \mathbb{Q}(\alpha)$, where α is a root of the polynomial

$$x^3 + \frac{3 + \sqrt{-31}}{2}x^2 + \frac{-3 + \sqrt{-31}}{2}x - 1 = 0. \tag{2}$$

Finally, define the **narrow class field**:

Definition. Suppose K is a $\mathbb{Q}$ - extension. Recall that the class field cl(K) is $C_K = I_K/P_k$, where I_K is the group of fractional ideals of K and P_K is the group of principle fractional ideals of K.

The **narrow class field** C_K^+ is defined by $C_K^+ = I_K/P_K^+$, where P_K^+ is the group of totally positive principal fractional ideals of K, i.e. ideals of the form $a\mathcal{O}_K$, where a is an element of K such that $\sigma(a)$ is positive for every embedding σ :K$\rightarrow \mathbb{R}$.

Note that the **narrow class number** is equal to $|C_K^+|$ and is denoted by $h^+(K)$. The ideal class group is a quotient of the narrow class group, implying that the narrow class number is a multiple of the class number. When the number field is totally complex, they are equal.

3.4 p-class fields

Definitions

The following definitions and corollaries will be useful in determining the structure of the Hilbert class field.

Definition. A **p-group** is a group in which every element has order equal to a power of p.

Definition. A **p-extension** L of a number field K is an extension where the Galois group is a p-group.

Definition. A **Hilbert p-class field** H_K^p of a number field K is the maximal unramified abelian p-extension of K, with the **p-class field tower** defined in a similar way to the definition of the Hilbert tower.

3.4.1 p-class Field Towers

Corollary 2. A number field K can be embedded into a finite field extension with class number coprime to p iff the Hilbert p-class field tower terminates.

Corollary 3. If any p-class field tower over K is infinite, then the class field tower is also infinite. If the p-class tower terminates, then $H_{K_\infty}^p$ is a finite field extension of K and $\Gamma(H_{K_\infty}^p/K)$ is a p-group.

Note that the converse to the first part of Corollary 3 need not hold; a counterexample is given in Schoof [21]. Consider $\mathbb{Q}\left(\sqrt{-239}, \sqrt{4049}\right)$. Then this biquadratic field extension of $\mathbb{Q}$ has an infinite class field tower, but all its p-class field towers are finite.

4 Bounds on Discriminants

4.1 Root Discriminant

One technique for calculating K^{ur} is to use bounds on the root discriminant of a number field. Since unramified extensions have the same root discriminant, these bounds can prove that an unramified extension of a number field with class number one is indeed the maximal unramified extension. Minkowski first found a lower bound for the discriminant using geometry and Odlyzko later improved these bounds. Assuming the Generalised Riemann Hypothesis, even stronger bounds can be achieved.

In Neukirch's Algebraic Number Theory textbook [19], the following theorem for the relative discriminant is stated:

Proposition 1. Let K, L, M be number fields with the inclusions $K \subset$L$\subset M$. Then

$$\Delta_{L/K} = N_{L/K}(\Delta_{L/K})\, \Delta_{L/K}^{[L:K]} \tag{3}$$

Corollary 4. If L is an unramified extension of K, then $\Delta_{L/\mathbb{Q}} = \Delta_{L/\mathbb{Q}}^{[L:K]}$. Furthermore, L and K have the same root discriminant.

Proof. Since L is an unramified extension of K, no prime divides $\Delta_{L/K}$, so $\Delta_{L/K}$ is the unit ideal. But then $N_{K/\mathbb{Q}}(\Delta_{L/K}) = 1$ and so the result follows by the Tower Law and Proposition 1,

$$rd_L = \Delta_{L/\mathbb{Q}}^{\frac{1}{[L:K][K:\mathbb{Q}]}} = \Delta_{K/\mathbb{Q}}^{\frac{1}{[K:\mathbb{Q}]}} = rd_K \tag{4}$$

Hence if L is an unramified extension of K, and rational prime p divides $\Delta(K)$ iff p divides $\Delta(L)$. $\square$

4.2 Minkowski's Bound

Statement

Minkowski's theorem gives another bound for the root discriminant, derived from the geometry of numbers:

Theorem 4. If K is a number field with r_1 real and $2r_2$ complex conjugate fields, and $n = r_1 + 2r_2$ is the degree of the field, then

$$|d_K| \geqslant \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2. \tag{5}$$

Taking n^{th} roots gives a bound for the root discriminant:

$$rd_K \geqslant (\frac{\pi}{4})^{\frac{2r_1}{n}} \frac{n^2}{n!^{\frac{2}{n}}}. \tag{6}$$

Number Fields with No Unramified Extension

As shown in Example 2, every nontrivial field extension of $\mathbb{Q}$ is ramified. Therefore $\mathbb{Q}^{ur} = \mathbb{Q}$. In the answer given by Conrad at [4], Minkowski's bound is used to find more examples of such number fields:

Theorem 5. Suppose K is a number field of degree m, and define $f(n) = \left(\frac{\pi}{4}\right) \frac{n^2}{n!^{\frac{2}{n}}}$. Suppose $rd_K \leq f(2m)$, then K is unramified-closed.

Example 5. Suppose $m = 2$, then $f(4) = 2.57$, and so $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$ all satisfy Theorem 5, so have no nontrivial unramified extensions.

Furthermore, suppose K is a quadratic number field with (wide) class number equal to 1 and with $f(5) > rd_k > f(4)$. Then any unramified extension of K must be a quadratic extension. However, such an extension would be a nontrivial abelian extension unramified at no finite places, with contradiction. This argument shows that $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$ are also unramified-closed.

Example 6. For $m = 3, f(6) = 3.15$. The number fields defined by $x^3 - x^2 + 1$ and $x^3 + x - 1$, which both have Galois groups isomorphic to S_3, also satisfy the theorem and are unramified-closed.

Example 7. For $m = 4, f(8) = 3.55$. Then let K_1 be defined by $x^4 - x^3 - x^2 + x + 1$, K_2 be defined by $x^4 - x^3 + x^2 - x + 1$, K_3 be defined by $x^4 - x^2 + 1$. Then K_1, K_2 and K_3 are all unramified-closed, and have Galois groups isomorphic to D_4, C_4 and V_4 respectively.

As $n \to \infty$, Stirling's formula can estimate $f(n)$, showing that

$$\lim_{n \to \infty} f(n) = \frac{\pi e^2}{4} = 5.80 \tag{7}$$

Furthermore, $f(n)$ is increasing, so this direct argument from Minkowski's bound can only prove that a field is unramified closed if the root discriminant is less than 5.80.

The online database at [8] gives a total of 224 number fields with root discriminant less than $\frac{\pi e^2}{4}$, and the largest degree of all these fields is 8. For $n = 5$, the smallest root discriminant is $4.38 > 3.82 = f(8)$, and Theorem 5 cannot be applied. Similar results hold for $n = 6, 7, 8$. Therefore Theorem 5 cannot be applied directly to any other number fields.

4.3 Odlyzko's Bound

Statement

Odlyzko's bound [20] improved on the Minkowski's bounds for the root discriminant of a number field. It can be stated as

$$rd_K \geqslant 60^{\frac{r_1}{n}} 22^{\frac{r_2}{n}} + o(1) \; as \; n \to \infty \tag{8}$$

Moreno [18] writes this bound explicitly as

$$rd_K \geqslant 60^{\frac{r_1}{n}} 22^{\frac{r_2}{n}} \exp\left(-8.6 n^{-2/3}\right) \tag{9}$$

Furthermore, under the assumption of the Generalised Riemann Hypothesis, this bound can be improved by replacing the numbers 60 and 22 by 188 and 41 respectively.

Using Odlyzko's Bound

Following Yamamura [29], write this bound function as $B(n, r_1, r_2)$. The following theorem will show how to use the lower bound on the root discriminant to prove than an unramified extension of a number field is maximal

Theorem 6. Suppose that K is a degree n number field with r_1 real places and $2r_2$ complex places. Let $B(n, r_1, r_2)$ be the lower bound for rd_K, and suppose L is an unramified normal degree extension of K of degree m. If $h(L) = 1$, and

$$rd_K < B(60 \cdot m \cdot n_K, 60 \cdot m \cdot r_1, 60 \cdot m \cdot r_2), \tag{10}$$

then $K^{ur} = L$.

Proof. Suppose M were an unramified nontrivial normal extension of K. Since the compositum retains closure and unramified extensions, LM is also a normal unramified extension of L. Define $G = \Gamma(LM/L)$ with $|G| = a$.

If G had a normal subgroup H, the Fundamental Theorem of Galois Theory would imply that G/H would correspond to an Abelian unramified extension of L, contradicting $h(L) = 1$. Hence G is unsolvable. This immediately implies that $a \geqslant 60 = |A_5|$ because A_5 is the smallest unsolvable group.

Since LM is also an unramified extension of K,

$$rd_{LM} = rd_K \ < B(60 \cdot m \cdot n_K, 60 \cdot m \cdot r_1, 60 \cdot m \cdot r_2) \leq B(a \cdot m \cdot n_K, a \cdot m \cdot r_1, a \cdot m \cdot r_2) \tag{11}$$

But $LM/\mathbb{Q}$ has $a \cdot r_1 \cdot m$ real places and $2 \cdot a \cdot r_2 \cdot m$ complex places, so $[LM : \mathbb{Q}] = a \cdot m \cdot n$, contradicting Equation (11). Hence L is unramified-closed and $L = K^{ur}$. $\square$

Applying this result to Equation (9) gives the following corollary:

Corollary 5. Suppose K is a degree n number field with signature (r_1, r_2), and L is a degree m unramified extension of K with trivial class group. If

$$rd_K < 60^{\frac{r_1}{n}} 22^{\frac{r_2}{n}} \exp\left(\frac{-8.6}{60 \cdot m \cdot n}\right), \tag{12}$$

then $L = K^{ur}$.

5 Unramified Extensions of Number Fields

Kim [9] showed that given any finite solvable group G, there exist infinitely many abelian extensions $K/\mathbb{Q}$ and Galois extensions $M/\mathbb{Q}$ such that $\Gamma(M/K) \cong G$ and M/K is unramified. However, it is interesting to either find explicit examples of infinite families of number fields with finite solvable extension, or to find number fields with unramified unsolvable extension.

5.1 Kondo's Results

In the paper by Kondo [14], conditions are given for the splitting field of a polynomial to be an unramified extension of the quadratic field defined by the square root of its discriminant.

Theorem 7. Suppose F is a number field with discriminant $\Delta(F)$ of degree n, and K is its Galois closure over $\mathbb{Q}$. Suppose $\Delta(F)$ is not a square, i.e. it is equal to the discriminant of the quadratic number field $\mathbb{Q}(\sqrt{\Delta(F)})$, then

1. $\Gamma(K/\mathbb{Q}) \cong S_n$
2. $K/\mathbb{Q}(\sqrt{\Delta(F)})$ is an unramified extension.

Kondo also gives this theorem:

Theorem 8. The following are equivalent:

1. $\Delta(F)$ is equal to the discriminant of the quadratic number field $\mathbb{Q}(\sqrt{\Delta(F)})$
2. For every prime dividing $\Delta(F)$, its ideal $\mathfrak{p}$ in F has precisely one ramified divisor.

Lemma 3. Furthermore, the following condition is equivalent to conditions of Theorem 8:
The inertia group of every ramified prime of K is a group of order 2 generated by a transposition.

In particular, if F satisfies this condition, then $\Delta(F)$ is equal to $\Delta\left(\mathbb{Q}(\sqrt{\Delta(F)}\right)$.

Proof. This is immediate from a theorem of Van der Waerden [25]. □

Lemma 4. Suppose $\Delta(F) \notin \mathbb{Q}^2$. Then the following are equivalent:

1. K is an unramified extension of $\mathbb{Q}\left(\sqrt{\Delta(F)}\right)$
2. The inertia group of every ramified prime of K is a group of order 2, generated by an odd permutation.

The following examples of unramified extensions of quadratic number fields were found using SageMath:

Example 8. Define $f(x) = x^6 + x^5 - 6x^4 - 4x^3 + 8x^2 + 3x - 2$. Also define $F = \mathbb{Q}(\theta)$, where θ is a root of f, and let K be the splitting field of f over $\mathbb{Q}$. Then $d(f) = \Delta(F) = 7846061 = 17^3 \cdot 1597$.

$$f(x) = (x^3 + 9x^2 + 16x + 7)^2 \, mod \, 17 \tag{13}$$

By Lemma 3 and Lemma 4 indeed K is an unramified extension of $\mathbb{Q}(\sqrt{17^3 \cdot 1597})$. Furthermore, $\Gamma(K/\mathbb{Q})$ is a group of order 72 and is isomorphic to the wreath product of S_3 by C_2.

It follows that $K/\mathbb{Q}(\sqrt{17^3 \cdot 1597})$ is an unramified extension with Galois group isomorphic to the Frobenius group of order 36.

Example 9. Let

$$f(x) = x^7 + 2x^6 - x^5 - x^4 + x^3 - x^2 - x + 1 \tag{14}$$

and F and K be as in Example 9. Then $disc(f) = \Delta(F) = -357911 = -71^3$ and

$$f(x) = (x + 19)(x + 42)^2(x + 59)^2(x + 68)^2 \, mod \, 71. \tag{15}$$

Therefore, by Lemma 4, $K/\mathbb{Q}(\sqrt{-71})$ is unramified. The Galois group of $K/\mathbb{Q}$ is isomorphic to D_7, and so $K/\mathbb{Q}(\sqrt{-71})$ is an unramified extension with Galois group isomorphic to C_7. Since $h(\mathbb{Q}(\sqrt{-71})) = 7$, K is the absolute class field of $\mathbb{Q}(\sqrt{-71})$.

Example 10. Suppose a polynomial f is defined with the following properties:

$$f(x) = x^9 - x^8 - 2x^7 + x^6 + 2x^5 + x^3 + x^2 - x - 1 \tag{16}$$

$$disc(f) = \Delta(F) = 66078977 = 23^3 \cdot 5431 \tag{17}$$

$$f(x) \equiv (x^3 + 8x^2 + 18x + 1)(x^3 + 7x^2 + 3x + 1)^2 \, mod \, 23. \tag{18}$$

Therefore $K/\mathbb{Q}(\sqrt{-23})$ is unramified. $\Gamma(K/\mathbb{Q})$ is isomorphic to the wreath product of S_3 by S_3 and has order $1296 = 2^3 \cdot 3^3$, whence $K/\mathbb{Q}(\sqrt{-23})$ has Galois group of order 648.

5.2 Quintic Polynomials

In [30], Yamamura states the following theorem, which gives a method of finding infinitely many real quadratic number fields with an unramified (and unsolvable) A_5 - extension.

Theorem 9. Suppose S_1 and S_2 are finite sets of primes satisfying $S_1 \cap S_2 = \varnothing$ and $2, 5 \notin S_2$. Then there exist infinitely many real quadratic number fields with the following properties:

1. F is a strictly unramified A_5 - extension.
2. All primes in S_1 are unramified in F.
3. All primes in S_2 are ramified in F.

To prove Theorem 9, Yamamura gives the following five conditions for a quintic polynomial in this lemma:

Lemma 5. Suppose $f(x)$ is of the form

$$f(x) = x^5 - 2ax^3 + bx + c : a, b, c \in \mathbb{Z} \tag{19}$$

and the following conditions hold:

1. f(x) is irreducible over $\mathbb{Q}$.
2. $b \equiv c \equiv 1 \, mod \, 2$.

3. All the roots of $f(x)$ are real.

4. Define $D = disc(f)$, and define $A = 5ac^2(3a^2-5b)+8b^2(a^2-b^2)$ $B = 125ac^2-16b(a^2-b)(6a^2-5b)$. Then any prime factor of (A, B, D) is also a prime factor of $2ac$.

5. $gcd(a, b, 5) = gcd((a^2b - b^2), c, D) = 1$.

Then $\mathbb{Q}(\sqrt{D})$ is a real quadratic number field, and the splitting field K of $f(x)$ is a strictly unramified A_5 - extension of $\mathbb{Q}(\sqrt{D})$.

Example 11. The following example was found using SageMath. Take $a = 81, b = 57, c = 13$. Then $f(x) = x^5 - 162x^3 + 57x + 13$ with splitting field K and

$$D = disc(f) = 19 \cdot 587 \cdot 510172213, \tag{20}$$

whence the splitting field K is an unramified A_5 - extension of $\mathbb{Q}(\sqrt{D})$.

In Yamamura's paper, the following polynomial is defined with certain modularity conditions:

$$f_m(x) = x^5 - 2m^2x^3 + (6m^2 - 1)x - (m - 4) \tag{21}$$

for some integer m. Imposing the modularity conditions on m means that $f_m(x)$ meets criteria (2) and (3) from Theorem 9, thereby producing such a family of quintic polynomials.

Yamamura also gives examples of real quadratic number fields with class number one having either a strictly or weakly unramified A_n - extension which is an S_n - extension of $\mathbb{Q}$ for n equal to 5, 6, and 7.

Example 12. As Hunter shows [5], the minimum possible discriminant of a quintic field with one real and two pairs of imaginary conjugate fields is 1609. Taking $K = \mathbb{Q}(\sqrt{1609})$, $h^+(K) = 1$ and K has a weakly unramified A_5 - extension.

A further sextic example is found by using the database of number fields maintained by Jones and Roberts at [8]:

Example 13. Suppose $K = \mathbb{Q}(\sqrt{592661})$, then K has a strictly ramified A_6 - extension, defined by the splitting field of $x^6 - x^5 - 5x^4 + 4x^3 + 5x^2 - 2x - 1$.

5.3 Unramified Extensions of Number Fields defined by a Trinomial

Uchida [24] gives the following theorem about the ramification of primes in number fields defined by trinomials:

Theorem 10. Suppose K is a number field of finite degree with integers a and b, $f(x) = x^n - ax + b$ and L is the splitting field of $f(x)$ over K. If $(n-1)a$ and nb are relatively prime, the ramification index of any prime ideal of L over K is either 1 or 2.

This theorem has the following easy corollary:

Corollary 6. Suppose $f(x) \in \mathbb{Q}[x]$, with discriminant D, and every prime factor in the factorisation of D appears odd times. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Then $K/\mathbb{Q}\left(\sqrt{D}\right)$ is unramified.

Proof. Suppose p is a rational prime ramified in $K/\mathbb{Q}$. Then $p|D$. However, p ramifies in $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, with ramification index 2. Therefore p is unramified in $K/\mathbb{Q}(\sqrt{D})$. $\square$

Uchida also gives the following examples of unramified extensions of quadratic number fields with Galois group isomorphic to A_n.

Example 14. Define $f_n(x) = x^n - x + 1$ with discriminant $\mathfrak{d}_n$. First note that for all $n \in \mathbb{Z}$, $gcd((n-1)a, nb) = gcd(n-1, n) = 1$. Calculating the discriminant gives

$$disc(x^n - ax + b) = n^n b^{n-1} - (n-1)^{n-1} a^n \tag{22}$$

and so $\mathfrak{d}_n = n^n - (n-1)^{n-1}$. For $n \in \{5, 6, 7\}$, $\mathfrak{d}_n$ is either prime or the product of two primes, hence $f_n(x)$ satisfies the criteria of Theorem 10. Now

$$x^5 - x + 1 \equiv (x^2 - x + 1)(x^3 + x^2 + 1) \, mod \, 2 \tag{23}$$

hence the Galois group defined by $f_5(x)$ is isomorphic to S_5. Similar arguments hold for $n = 6$ and $n = 7$. Therefore there exist unramified extensions of quadratic number fields with D_5, D_6, D_7 or S_5, S_6, S_7 as Galois groups.

In the paper by Uchida [24], further examples of number fields with polynomials which define unramified alternating extensions of quadratic number fields are given; for example $x^7 - x + 1$, $x^9 - x + 1$ and $x^{10} - x + 1$.

Now consider another family of trinomials:

Definition. Define $g_n(x) = x^n - x - 1$ (note the change in sign) for $n \in \mathbb{N}$ with discriminant $\mathfrak{D}_n$ and splitting field L_n.

Selmer [22] shows that for $n \geq 1$, $g_n(x)$ is always irreducible. Furthermore, by Equation (22), $\mathfrak{D}_n = (-(n-1))^{n-1} - (-n)^n$.

Using SageMath, the factorisation of $\mathfrak{D}_n$ is calculated for $2 \leq n \leq 30$. Define G_n be the Galois group defined by $g_n(x)$. Using the Magma package available at `http://magma.maths.usyd.edu.au/calc/`, the Galois group G_n is calculated and the data is presented in the following table:

n	$gcd((n-1)a, nb)$	G_n	Factorisation of $\lvert\mathfrak{D}_n\rvert$
2	1	S_2	5
3	1	S_3	23
4	1	S_4	283
5	1	S_5	$19 \cdot 151$
6	1	S_6	$67 \cdot 743$
7	1	S_7	776887
8	1	S_8	$11 \cdot 1600069$
9	1	S_9	$7 \cdot 11 \cdot 13 \cdot 43 \cdot 79 \cdot 109$
10	1	S_{10}	$173 \cdot 60042893$
11	1	S_{11}	275311670611
12	1	S_{12}	$1237 \cdot 7438489991$
13	1	S_{13}	$28201 \cdot 10423708597$
14	1	S_{14}	$31 \cdot 59 \cdot 1279 \cdot 4879633159$
15	1	S_{15}	$52489 \cdot 418511 \cdot 19428121$
16	1	S_{16}	$227 \cdot 246027323 \cdot 338142271$
17	1	S_{17}	808793517812627212561
18	1	S_{18}	$773 \cdot 1153064743 \cdot 45072130459$
19	1	S_{19}	$5 \cdot 659 \cdot 588489604729898953429$
20	1	S_{20}	$47 \cdot 233 \cdot 443 \cdot 220221742235854057 03$
21	1	S_{21}	$1137694897331 \cdot 5043293621028391$
22	1	S_{22}	$5 \cdot 694540928765211079836055696 01$
23	1	S_{23}	$29 \cdot 53264767 \cdot 1329664622102383847518 1$
24	1	S_{24}	$101 \cdot 2347 \cdot 571454709340397489309477236 9$
25	1	S_{25}	$10667 \cdot 282401201 \cdot 925997749 \cdot 31362479733103$
26	1	S_{26}	$73 \cdot 181 \cdot 2385857 \cdot 32375941061 \cdot 6118709648547401$
27	1	S_{27}	$23 \cdot 3539 \cdot 535391 \cdot 100339188345090206455022514 01$
28	1	S_{28}	$349 \cdot 14769635993383 \cdot 651630200252698335369261 7$
29	1	S_{29}	$41393681953973 \cdot 612301324841360347587968801 21$
30	1	S_{30}	$4421 \cdot 22659339443160463 \cdot 208090623368431916058490 3$

Hence for $2 \leq n \leq 30$, the criteria given in Corollary 6 are fulfilled, and there exist unramified extensions of quadratic number fields with Galois groups isomorphic to A_n or S_n for all such n. For $n \geq 5$, these groups are unsolvable, in contrast to the results from Kim [9].

A Remark on Uchida's Results on Trinomials

Yamamoto [28] gives the following classification of trinomials of the form in Theorem 10:

Theorem 11. Suppose $f(x)$ is trinomial of degree n of the form in Theorem 10 with splitting field L. If the following conditions hold:

1. $(n-1)a$ and nb are relatively prime
2. $\Gamma(L/\mathbb{Q}) \cong S_n$.

Then K is an A_n - extension of $\mathbb{Q}\left(\sqrt{disc(f)}\right)$ which is unramified at all finite primes.

Uchida [24] gives the following proposition:

Proposition 2. Suppose $f(x) = x^n + ax + b$ is a trinomial with splitting field L, and

1. n is prime.
2. $gcd((n-1)a, nb) = 1$.
3. $f(x)$ is irreducible.

Then $\Gamma(L/\mathbb{Q}) \cong S_n$.

Putting together the remark from Selmer [22] that $x^n - x - 1$ is irreducible, Theorem 11 and Proposition 2, the following corollary can be stated:

Corollary 7. Suppose $g_p(x) = x^p - x - 1$ is in Section 5.3 with p prime, and with splitting field L_p. Then $G_p \cong S_p$ and $\Gamma\left(L_p/\mathbb{Q}\left(\sqrt{\mathfrak{D}_p}\right)\right) \cong A_p$. Thus for $p \geq 5$, g_p defines a family of unramified unsolvable extensions of imaginary quadratic number fields.

5.4 Yamamoto's Constructions of Unramified Extensions of Number Fields Defined by Trinomials

In addition, Yamamoto states another theorem:

Theorem 12. If there exist primes p_1, p_2, p_3 such that

- $f(x)$ is irreducible modulo p_1
- $f(x)$ is the product of a degree 1 irreducible polynomial and a degree $n-1$ irreducible polynomial modulo p_2
- $f(x)$ is the product of $n-2$ distinct degree 1 polynomials and a degree 2 irreducible polynomials modulo p_3

Then the Galois group defined by the splitting field of f is isomorphic to S_n.

Example 15. Set $f(x) = x^5 + 51x - 95$ with discriminant D, then $f(x)$ is irreducible modulo 1979, i.e.

$$f(x) \equiv x^5 + 51x - 9 \; mod \; 979 \tag{24}$$

$$f(x) \equiv (x + 357)(x^4 + 1642x^3 + 1512x^2 + 1945x + 1338) \; mod \; 1999, \tag{25}$$

$$f(x) \equiv (x + 194)(x + 384)(x + 1332)(x^2 + 1832x + 950) \; mod \; 1871 \tag{26}$$

Let L be the splitting field of f, and $K = \mathbb{Q}\left(\sqrt{disc(f)}\right)$. Note that

$$gcd((n-1)a, nb) = gcd(204, -475) = 1 \tag{27}$$

and

$$D = 342859667381 = 7^3 \cdot 11 \cdot 1567 \cdot 57991. \tag{28}$$

Therefore $\Gamma(L, \mathbb{Q}) \cong S_5$ and L is an A_5 - extension of K unramified at all finite primes.

Using SageMath, additional examples were found. For instance:

Example 16. Set $f(x) = x^6 - 23x - 58$ with D, K and L as in Example 15, and p_1, p_2, p_3 are equal to 1999, 1987, 1861 respectively.

Calculating:

$gcd((n-1)a, nb) = gcd(-115, -324) = 1$, $f(x)$ is irreducible mod 1999,

$$f(x) \equiv (x + 1818)(x^5 + 169x^4 + 743x^3 + 386x^2 + 1650x + 647)\ mod\ 1987 \tag{29}$$

$$f(x) \equiv (x + 37)(x + 406)(x + 1265)(x + 1396)(x^2 + 618 + 1485)\ mod\ 1861 \tag{30}$$

Also $D = 31085593520933 = 7 \cdot 617 \cdot 7197405307$.

Therefore, $\Gamma(L/\mathbb{Q}) \cong S_6$ and L is an A_6 - extension of K, unramified at all finite primes.

5.5 Infinite Family of Real Quadratic Fields with Class Number a Multiple of 3

Applying Theorem 10 in the case that $n = 3$, Uchida also uses unramified extensions to prove that there exist infinitely many real quadratic number fields with class numbers divisible by 3:

Proof. Suppose $f(x) = x^3 + ax + b$ is an irreducible cubic with splitting field K and discriminant D, such that $\Gamma(K/\mathbb{Q}) \cong S_3$. Then $K/\mathbb{Q}(\sqrt{d})$ is unramified and the class number of $\mathbb{Q}(\sqrt{d})$ is divisible by 3.

Fixing $b = 1$, it suffices to find infinitely many different $\mathbb{Q}(\sqrt{D})$ with positive D. Picking a prime $p \equiv 2$ mod 3 with $a_1 \equiv 1$ mod 3 and $a_1 > 2$ such that $p|4a_1^3 - 27$ will generate the required fields. Examples of such fields have been calculated using SageMath and are tabulated below. Note that for $D = 9410521, 32969605$, the class group is not cyclic.

p	a_1	D	$Cl(\mathbb{Q}(\sqrt{D}))$
5	7	1345	C_6
11	16	16357	C_3
17	46	389317	C_{12}
23	70	1371973	C_3
29	10	3973	C_6
41	28	87781	C_{12}
47	55	665473	C_{21}
53	133	9410521	$C_6 \times C_2$
59	175	21437473	C_6
71	109	5180089	C_3
83	241	55990057	C_6
89	202	32969605	$C_{18} \times C_2$

$\square$

5.6 Unramified Cyclic Quintic Extensions of Imaginary Quadratic Number Fields

Kishi [12] finds an infinite family of imaginary quadratic number fields with class number a multiple of 5, and also a family of unramified cyclic quintic extensions of these fields. Recall the notation for Fibonacci numbers F_n and Lucas number L_n.

Begin with the well-known statement about Fibonacci numbers:

Lemma 6. If n, m are positive integers, and $d = gcd(n, m)$, then $gcd(F_n, F_m) = F_d$.

Then the proposition follows:

Proposition 3. The following set is infinite:

$$\{\mathbb{Q}\left(\sqrt{-F_{50s+25}}\right) : s \geq 0\} \tag{31}$$

Now for a non-negative integer m, define

- $k_m = \mathbb{Q}(\sqrt{-F_{2m+1}})$
- $g_m(x) = x^5 - 10x^3 - 20x^2 + 5(20F_{2m+1}^2 - 3)x + 40F_{2m+1}^2((-1)^m L_{2m+1} + 1) - 4$

Using Proposition 3, Kishi formulates an infinite set of cyclic quintic unramified extensions of imaginary quadratic number fields:

Theorem 13. Let m be a non-negative integer and define $E = split(g_m, \mathbb{Q})$. Then E is a D_5 - extension of $\mathbb{Q}$ containing k_m. Furthermore, if $m \equiv 12\ (mod\ 25)$, then E is an unramified cyclic quintic extension of k_m. Therefore, if $m = 25s + 12$ for some non-negative integer s, 5 divides the class number of the quadratic field $\mathbb{Q}(\sqrt{-F_{50s+25}})$.

Here is such an example of an imaginary quadratic number field with an unramified cyclic quintic extension:

Example 17. Suppose $s = 1, m = 37$. Then $F_{75} = 2111485077978050 = 2 \cdot 5^2 \cdot 61 \cdot 3001 \cdot 230686501$. Define $K = \mathbb{Q}(\sqrt{-F_{75}})$, and

$$g_{37} = x^5 - 10x^3 - 20x^2 + 445836923452397188907628180249985x - 841994090120605132670921957520010040515272300004$$

with discriminant

$$2^{24} \cdot 5^{20} \cdot 13^2 \cdot 61^6 \cdot 109^2 \cdot 139^2 \cdot 3001^6 \cdot 464419^2 \cdot 10772623^2 \cdot 230686501^6 \cdot 29020995417137^2 \cdot 460045379989033^2.$$

Note that g_{37} has precisely one real root. Using Magma, the class group of K was calculated. The factoring was done using SageMath. So $Cl(K) \cong C_{40}$ and $h(K) = 40$ which is divisible by 5. Let L be the splitting field of $g_{37}(x)$. Then L is an unramified C_5 - extension of K.

Kishi gives examples for the class group when $s = 0, 1, 2, 3$. Using Magma, the class group for $s = 4$ is calculated:

Example 18. Suppose $s = 4$,

$$d = F_{225} = 2 \cdot 5^2 \cdot 17 \cdot 61 \cdot 3001 \cdot 109441 \cdot 230686501 \cdot 11981661982050957053616001. \quad (32)$$

Define $K = \mathbb{Q}(\sqrt{-d})$. Then $h(K) = 22968615048297879813120$ which is a multiple of 5, and

$$cl(K) \cong C_2 \times C_2 \times C_2 \times C_2 \times C_4 \times C_{358884610129654372080}. \quad (33)$$

5.6.1 Smith's Family of Cyclic Quintic Extensions

Smith [23] also gives a method to find several families of imaginary quadratic number fields with unramified cyclic extensions using Lucas numbers and Fibonacci numbers.

First recall the well-known result that $L_n^2 = 5F_n^2 + 4(-1)^n$, therefore $\sqrt{5 \cdot L_n^2 + 20} = 5F_n \in \mathbb{Z}$ for odd n. Furthermore for $m, n \in \mathbb{Z}$, $m|n$ iff $F_m|F_n$. Since $F_5 = 5$, it follows that $5|F_n$ when n is a multiple of 5, and therefore when n is an odd multiple of 5,

$$\frac{L_n^2 + 4}{125} = \frac{F_n^2}{25} \in \mathbb{Z} \quad (34)$$

Also for $t = 2L_{20i-15}$ and $i \in \mathbb{Z}$,

$$\sqrt{\frac{t^2 + 16}{500}} = \frac{F_{20i-15}}{5} \in \mathbb{Z}. \quad (35)$$

The following three theorems describe infinite families of imaginary quadratic number fields with unramified cyclic quintic extension. For each theorem, an example of field with unramified cyclic quintic extension was calculated using SageMath.

Theorem 14. Suppose $t = 2L_{20i-5}$ for some $i \in \mathbb{Z}$. Define

$$f_t(x) = x^5 + 10x^3 - 5tx^2 - 15x - t^2 + t - 16 \quad (36)$$

with splitting field L_t. Furthermore define

$$d_t = -\sqrt{\frac{t^2 + 16}{500}},\ K_t = \mathbb{Q}(\sqrt{d_t}). \quad (37)$$

If $f_t(x)$ is irreducible, $L_t(x)$ defines an unramified C_5 - extension of K_t.

Example 19. Let $i = 1$. Then $t = 2L_{15} = 2728$,

$$f_t(x) = x^5 + 10x^3 - 13640x^2 - 15x - 7439272, \quad (38)$$

$$K_t = \mathbb{Q}\left(\sqrt{-2 \cdot 61}\right) \quad (39)$$

and $disc(f) = 2^{14} \cdot 5^{20} \cdot 11^2 \cdot 61^6$. Then L_t is an unramified C_5 - extension of K_t.

Theorem 15. Suppose $t = L_{4i-1}$ for some $i \in \mathbb{Z}$. Define

$$f_t(x) = x^5 - 10x^3 - 5x^2t^2 + 5(t^3 + 2t^2 + 4t + 5)x - (t^3 + 2t^2 + 5t + 8), \tag{40}$$

with splitting field L_t. Furthermore define

$$d_t = -t(t+2)(\sqrt{5t^2 + 20}),\ K_t = \mathbb{Q}(\sqrt{d_t}). \tag{41}$$

If $f_t(x)$ is irreducible, $L_t(x)$ defines an unramified C_5 - extension of K_t.

Example 20. Let $i = 2$. Then $t = L_7 = 29$,

$$f_t(x) = x^5 - 10x^3 - 4205x^2 + 130960x - 760496, \tag{42}$$

$$K_t = \mathbb{Q}\left(\sqrt{-5 \cdot 13 \cdot 29 \cdot 31}\right) \tag{43}$$

and $disc(f) = 2^6 \cdot 5^{10} \cdot 13^6 \cdot 29^2 \cdot 31^6$. Then L_t is an unramified C_5 - extension of K_t.

Theorem 16. Suppose either $t = L_{20i-15}$ or $t = L_{100i-25}$ for some $i \in \mathbb{Z}$. Define

$$f_t(x) = (x+4)(x-1)^4 + 20(x-1)^2t + (10x^2 - 20x + 26)t^2 + (5x^2 - 10x + 13)t^3 + (-5x+6)t^4 + 2t^5, \tag{44}$$

with splitting field L_t. Furthermore define

$$d_t = -t(t+2)\left(\sqrt{\frac{t^2+4}{125}}\right),\ K_t = \mathbb{Q}(\sqrt{d_t}). \tag{45}$$

If $f_t(x)$ is irreducible, $L_t(x)$ defines an unramified C_5 - extension of K_t.

Example 21. Let $i = 1$. Then $t = L_5 = 11$,

$$f_t(x) = x^5 - 10x^3 + 8105x^2 - 89390x + 430621,\ K_t = \mathbb{Q}\left(\sqrt{-11 \cdot 13}\right), \tag{46}$$

and $disc(f) = 5^{20} \cdot 11^6 \cdot 13^6$. Then L_t is an unramified C_5 - extension of K_t.

For each of these polynomials, $f_t(x)$ is irreducible for all but finitely many values of t, giving three infinite families of unramified cyclic extensions of imaginary quadratic number fields.

5.7 Unramified Extensions of Cyclic Cubic Fields

Wong [26] also gives examples of a cyclic cubic field with an unsolvable unramified extension. First the following lemma from Galois Theory is useful:

Lemma 7. Let such a field be L, and have Galois closure S. Then if K is a cyclic cubic field, SK is an A_5 - extension of K.

Proof. From the Fundamental Theorem of Galois Theory, any A_5 - extension cannot contain a C_3 - sub-extension. Hence $K \cap S = \mathbb{Q}$ and the result follows. $\square$

The online database of [8] is then used to find a totally real quintic number field ramified at precisely one prime:

Example 22. Let K be the cyclic cubic field by $f(x) = x^3 - x^2 - 3422x + 1521$, with discriminant $disc(f) = 3^2 \cdot 13^2 \cdot 10267^2$, $\Delta(K) = 10367^2$. Also define L to be the splitting field of the quintic polynomial $g(x) = x^5 - 25x^3 - 7x^2 + 116x - 45$. Then L is an A_5 - extension of $\mathbb{Q}$, and the compositum LK is an unramified (and unsolvable) A_5 - extension of K.

5.8 Yamamura's Results for the First Imaginary Quadratic Field with Unramified Unsolvable extension

Yamamura [32] found several more examples of unsolvable unramified extensions.

Example 23. Yamamura proves that $\mathbb{Q}(\sqrt{-1507})$ is the first imaginary quadratic field with an unramified A_5 - extension over $\mathbb{Q}$. In fact, defining $L = split\,(x^5 - 5x^3 + 5x^2 + 24x + 5, \mathbb{Q})$ gives such an A_5 - extension of K.

Example 24. Define $K = \mathbb{Q}(\sqrt{-14731})$, $L = split(x^6 + 3x^5, 5x^4 + 4x^3 + 3x^2 + 2x + 1, \mathbb{Q})$. Then L is an unramified A_6 - extension of K and is an S_6 - extension of $\mathbb{Q}$.

Example 25. Define $K = \mathbb{Q}(\sqrt{-30759})$, $L = split(x^7 + 2x^6 - 3x^4 - x^3 - x^2 - x + 2, \mathbb{Q})$. Then L is an unramified PSL(2,7) - extension of K and is an $PSL(2,7) \times C_2$ - extension of $\mathbb{Q}$.

5.9 Hoelscher's Results for Abelian Unramified Extensions

Hoelscher gives the following theorem for an unramified sub-extension of a Galois group:

Theorem 17. Let K be a finite Galois extension of $\mathbb{Q}$ ramified only at a single finite prime $p > 2$, where Galois group $G = \Gamma(K/\mathbb{Q})$ is solvable. Let $K_0/\mathbb{Q}$ be an intermediate abelian extension of $K/\mathbb{Q}$. Let $N = \Gamma(K/K_0)$ and $p(N)$ be the quasi-p part of N. Then either

1. $N/p(N) \subset \mathbb{Z}/(p-1)$, or
2. there is a non-trivial abelian unramified sub-extension $L/K_0(\zeta_p)$ of $K(\zeta_p)/K_0(\zeta_p)$ of degree prime to p, with L Galois over $\mathbb{Q}$.

Using the paper by Jones and Roberts, [7], it is shown that the prime $p = 239$ is tamely ramified for

$$G = S_3,\ G^{ab} = C_2,\ p_w = 3 \tag{47}$$

and also

$$G = D_5,\ G^{ab} = C_2. \tag{48}$$

This means that Theorem 17 from Hoelscher can be applied with

$$N = G = D_5,\ K_0 = \mathbb{Q} \tag{49}$$

Then the first condition doesn't hold, because

$$N/p(N) = D_5 \not\subset \mathbb{Z}/(p-1) = \mathbb{Z}_{238}. \tag{50}$$

The following diagram shows the field extensions in this situation:

$$\begin{tikzcd}
 & K(\zeta_{239}) \arrow[d, dash] \arrow[ddl, dash] \\
 & L \arrow[d, dash] \\
K \arrow[d, dash, "D_5"'] & \mathbb{Q}(\zeta_{239}) \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q} \arrow[d, dash] & \mathbb{Q}(\zeta_{239}) \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}$$

Where the field extension L is a non-trivial abelian unramified sub-extension of degree prime to p, with L Galois over $\mathbb{Q}$.

Hoelscher also gives the following theorem about the divisibility of the order of Galois groups:

Theorem 18. Let G be the Galois group of some number field, ramified only at 3 and possibly ∞. Then

- If $2 \nmid |G|$ and $27 \nmid |G|$, then G is cyclic.
- If G is a solvable quasi-3 group, and $27 \nmid |G|$, then G is cyclic.

The online database at [8] lists 22 number fields ramified only at 3. Note that the converse of this theorem is not true: [8] gives three counterexamples of number fields where G is cyclic, but 2 divides $|G|$.

Example 26. Let $f(x) = x^2 - x + 1$. Then $disc(f) = -3$, $G \cong C_2$.

Example 27. Let $f(x) = x^6 - x^3 + 1$. Then $disc(f) = -(3^9)$, $G \cong C_6$.

Example 28. Let $f(x) = x^{18} - x^9 + 1$. Then $disc(f) = -(3^{45})$, $G \cong C_{18}$.

5.10 Lesseni's Results on Degree 9 Number Fields

Lesseni [15] proves that there is no primitive number field ramified at only one prime $p < 11$. Suppose $K = \mathbb{Q}(\theta)$ is a number field where θ is a root of an irreducible polynomial of degree 9, and let L represent the Galois closure of K.

Definition. A degree 9 number field K is said to be **primitive** if it has no cubic subfields.

The following theorem is given:

Theorem 19. Suppose GRH holds. Then L cannot be ramified over K only at $p = 5$. Now suppose GRH doesn't hold. Then $5\mathcal{O}_K$ is equal to one of the following:

- $\mathfrak{p}_1^5\mathfrak{p}_2^4$
- $\mathfrak{p}_1^5\mathfrak{p}_2^3\mathfrak{p}_3$
- $\mathfrak{p}_1^5\mathfrak{p}_2^2\mathfrak{p}_3^2$
- $\mathfrak{p}_1^5\mathfrak{p}_2^2$

whence the discriminant d_K is equal to 5^{11} or 5^{12}.

Similar theorems hold for $p = 3$ and $p = 7$. Using a computer search for primitive number fields defined by a degree 9 polynomial, for a prime $p < 11$ there were only 13 distinct number fields found which ramify precisely at 3, and none of these number fields ramify at 2,5 or 7. In addition, none of these number fields are primitive, leading to the following conclusion:

Theorem 20. There is no primitive degree 9 number field ramified at only one prime p, $p < 11$.

Corollary 8. Suppose K is a degree 9 number field which is ramified at only one prime p, $p < 11$. Then the Galois group of its Galois closure is solvable.

Searching the database of number fields at [8] confirms this result.

6 Infinite Unramified Extensions

6.1 Imaginary Quadratic Extensions

Martinet [17] gives the following example of a totally real number field of degree 10 with infinite unramified extension:

Example 29. Suppose $K = \mathbb{Q}\left(\cos(\frac{2\pi}{11}), \sqrt{2}\right)$. Then $[K : \mathbb{Q}] = 10$ and $rd_K = 92.37$. Genus theory and Golod-Shafarevich together show that K has an infinite unramified 2-tower.

In fact, K has the smallest root discriminant of any known number field with an infinite unramified extension. However, if the number field is imaginary quadratic, several examples of infinite unramified extensions have been found.

The following is a fact from Algebraic Number Theory: there are 9 imaginary quadratic fields with class number 1, and there are 47 imaginary biquadratic number fields with class number 1.

One natural question to ask is: "What are the unramified extensions of imaginary quadratic number fields"? Discriminant bounds are one way of attacking this question. Applying Odlyzko's bounds gives this lemma:

Lemma 8. All imaginary quadratic number fields with class number one are unramified-closed, and therefore have no infinite unramified extension.

Proof. Suppose K is a imaginary quadratic number field with class number one. Then $rd_K \leq \sqrt{163} = 12.77 < 17.02 = B(120, 0, 60)$. So K is unramified-closed by a previous theorem. $\square$

Such a method does not work for all imaginary biquadratic number fields with trivial class group. Consider the field $K = \mathbb{Q}(\sqrt{-67}, \sqrt{-163})$ which has root discriminant equal to 104.50.

6.2 Biquadratic Number Fields with Infinite Unramified Extension

In a paper by Hajir and Maire [3], an unpublished paper by Martinet is referenced with the following examples:

Example 30. Define $K_1 = \mathbb{Q}\left(\sqrt{-263}, \sqrt{-35}\right)$,$K_1 = \mathbb{Q}\left(\sqrt{-607}, \sqrt{-15}\right)$. Then K_1 and K_2 have infinite unramified extensions. Furthermore, $rd_{K_1} = 95.94$, $rd_{K_2} = 95.42$.

These biquadratic number fields have root discriminant only slightly larger than the degree 10 number field given by Martinet in Example 29.

Suppose now that K is a class field with trivial class group, i.e. $h(K) = 1$. Then K has no abelian (and hence no solvable) non-trivial unramified Galois extension. Despite this, K may have a unsolvable unramified extension. Brink [1] gives such an example:

Example 31. Suppose

$$K = \mathbb{Q}(\sqrt{29}, \sqrt{4967}) \tag{51}$$

$$L = split(x^7 - 11x^5 + 17x^3 - 5x + 1, \mathbb{Q}) \tag{52}$$

Then K has class number 1 and L is a $PSL(2,7)$ - extension of K.

Maire [16] showed that there exist biquadratic number fields with class number one with an infinite unramified extension. Here is another example from Maire:

Example 32. Suppose $K = \mathbb{Q}(\sqrt{17601097}, \sqrt{17380678572159893})$. Then $h(K) = 1$ and K has an infinite unramified Galois extension.

Theorem 21. Brink [1] gives the following construction for biquadratic number fields with infinite unramified extension. Suppose that

1. $f \in \mathbb{Z}[x]$ is an irreducible quintic with five real roots.
2. $D = disc(f)$ is prime and $\mathbb{Q}(\sqrt{D})$ has class number 1.
3. p and q are two primes such that $\mathbb{Q}(\sqrt{p.q})$ has class number 1 and $\mathbb{Q}\left(\sqrt{(D.p.q}\right)$ has class number 2.
4. $f(x)$ has five simple roots modulo p and $f(x)$ factors modulo q into polynomials of degrees, as a tuple μ of the form (1,1,1,1,1), (1,1,1,3), (1,2,2) or (1,1,3).

Then the field $L = \mathbb{Q}\left(\sqrt{D}, \sqrt{p \cdot q}\right)$ has class number 1 and infinite unramified extension.

Proof. A result from Kondo [14] shows that the splitting field K of f is an S_5 - extension of $\mathbb{Q}$ and an unramified A_5 - extension of $\mathbb{Q}(\sqrt{D})$. Hence $M = K\left(\sqrt{p \cdot q}\right)$ is an unramified A_5 - extension of L. In fact, since M has a finite 2-Hilbert tower, the class group of M must be a 2-group. Furthermore, K has class number 1, as demonstrated in the following diagram.

$$\begin{tikzcd}[arrows=dash]
 & & M = K(\sqrt{p \cdot q}) \arrow[dl, "C_2"'] \arrow[dr, "A_5"] & & \\
 & K = split(f, \mathbb{Q}) \arrow[dl, "A_5"'] \arrow[dd, "S_5"] & & L = \mathbb{Q}(\sqrt{D}, \sqrt{p \cdot q}) \arrow[ddll] \arrow[d] \arrow[dr] & \\
\mathbb{Q}(\sqrt{D}) \arrow[dr] & & & \mathbb{Q}(\sqrt{p \cdot q}) \arrow[dll] & \mathbb{Q}(\sqrt{D \cdot p \cdot q}) \arrow[dlll] \\
 & \mathbb{Q} & & &
\end{tikzcd}$$

Let r be the number of primes $\mathfrak{p}$ in L ramified in M, and let θ be a root of f, $T = \mathbb{Q}(\theta)$. Martinet [17] shows that M has an infinite 2-class field tower if $r \geq 155$. By assumption p splits completely in T and therefore also in L; furthermore q decomposes in T as $q = \mathfrak{p}_1 ... \mathfrak{p}_r$, with inertia degrees

$$(deg(\mathfrak{p}_1), ...deg(\mathfrak{p}_r)) = \mu \tag{53}$$

Write $Z_{\mathfrak{B}} \subseteq \Gamma(L/\mathbb{Q}) = S_5$ as the decomposition group of $\mathfrak{B}$ where $\mathfrak{B}$ is a prime in L dividing q. Since q is unramified, this group is cyclic, and Martinet [17] shows that $Z_{\mathfrak{B}}$ has order at most 3. It now follows that L has 120 primes dividing p and at least 40 primes dividing q. Then $r \geq 160$ since they all ramify in M, and Theorem 21 follows. $\square$

Using SageMath, the following polynomial and primes were found:

$$f(x) = x^5 + 4x^4 - 6x^2 - x + 1, \; p = 1531, \; q = 71, 151, 227, \; disc(f) = 170701 \tag{54}$$

$$f(x) = x^5 - 4x^4 + 12x^2 - 8x + 1,\ p = 1987,\ q = 31, 107, 211, 239,\ disc(f) = 186037 \quad (55)$$

These polynomials satisfy the criteria of the Theorem 21 and therefore describe fields with infinite unramified extensions. Furthermore, the class number of the splitting fields of each of these polynomials is 1, meaning that they are equal to their own Hilbert class fields.

Example 33. Using the notation as defined in Theorem 21,

$$f(x) = x^5 - 2x^4 - 20x^3 + 6x^2 + 89x + 67 \quad (56)$$

$$p = 2003, q = 499, disc(f) = 4906992917 \quad (57)$$

Using Magma, the class group of K is isomorphic to V_4. Due to the Fundamental Theorem of Galois Theory, there must exist an intermediate field isomorphic to C_2 between K and its Hilbert class field. Furthermore, the Hilbert class field of K is isomorphic to the splitting field of

$x^{20} - 2874x^{18} + 2391847x^{16} - 471345876x^{14} + 29106648697x^{12} - 550807754260x^{10} + 4307861945767x^8 - 14829016524058x^6 + 23545104859585x^4 - 16530672769260x^2 + 4009653817744.$

Example 34. Using the notation as defined in Theorem 21,

$$f(x) = x^5 - 2x^2 - 20x^3 + 6x^2 + 89x + 67 \quad (58)$$

$$p = 811, q = 59, disc(f) = 8996154317 \quad (59)$$

Using Magma, the class group of K is isomorphic to C_2. There is no intermediate field between K and its Hilbert class field. Furthermore, the Hilbert class field of K is isomorphic to the splitting field of

$x^{10} - 375x^8 + 5121x^6 - 4084x^4 + 928x^2 - 64.$

The splitting field of this polynomial has class group isomorphic to V_4.

6.3 Golod and Shafaverich

Golod and Shafaverich [2] found a number field with an infinite class tower. This relies on the following theorem:

Theorem 22. Let G be a finite p-group, and define $d = dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$, $r = dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$. Then $r > d^2/4$.

There is also the theorem from Shafaverich,1963:

Theorem 23. Let $G = \Gamma(H^p_{K_\infty}/K)$ where K is an imaginary quadratic number field. If G is finitely generated as a pro-p group, then $r - d \leq 1$. If p is an odd prime, $r = d$.

The inequalities in Theorem 22 and Theorem 23 give a contradiction for $d \geq 5$ if all such G are assumed to be finite p-groups. Hence there must be a number field with an infinite 2-class field tower, so not all number fields have a finite field extension with class number 1:

Example 35. Define $K = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23})$. Then 6 odd primes ramify in K over $\mathbb{Q}$, and so K has an infinite 2-class field tower.

Furthermore, Schoof [21] shows that $\mathbb{Q}\left(\sqrt{-191 \cdot 773}\right)$ has an infinite 2-class field tower, and that there are infinitely many real quadratic number fields of the form $\mathbb{Q}(\sqrt{p_1 \cdot p_2})$ possessing infinite class field towers, where p_1 and p_2 are prime,

6.4 Infinite Unramified Extensions of Cyclic Cubic Fields

Wong [26] also gives a method to find a cyclic cubic field with infinite class field tower and infinite unramified extension. Use the following result from Roquette (see [13]):

Theorem 24. Suppose K is a normal degree n number field, r is the number of infinite places over K, and $e(p)$ be the nonzero exponent of a prime p in the factorisation of n. Let t_p be the number of primes ramified in K with p dividing their ramification index, and δ_p is 1 if the p-th roots of unity are in K, and 0 otherwise. Then K has an infinite class tower if

$$t_p \geqslant 2 + e(p)\delta_p + \frac{r-1}{p-1} + 2\sqrt{r + \delta_p} \tag{60}$$

If K is a cyclic cubic field, $n = r = p = 3$, $e(p) = 1$, $\delta_3 = 0$. Therefore if $t_3 \geq 3+2\sqrt{3} = 6.46$, K has an infinite class tower.

Hence if K is a cyclic cubic field, with at least 7 ramified primes, K has an infinite class field tower. Given seven primes which are all $1 \, mod \, 3$, the algorithm given in the proof of Theorem 2.7 in Wong [26] finds a cyclic cubic field, ramifying at these seven primes, with infinite class field tower and infinite unramified extension:

Example 36. Suppose the discriminant of $\Delta(K)$ is specified to be $3^4 \cdot 7^2 \cdot 13^2 \cdot 19^2 \cdot 31^2 \cdot 37^2 \cdot 61^2$. Using SageMath to follow the algorithm given by Wong, an appropriate polynomial was found. Define

$$f(x) = x^3 - 362918829x + 18285423253279. \tag{61}$$

Then

$$disc(f) = -1 \cdot 3^5 \cdot 7^2 \cdot 13^2 \cdot 19^2 \cdot 31^2 \cdot 37^2 \cdot 61^2 \cdot 157 \cdot 15826849. \tag{62}$$

Thus the cyclic cubic field K defined by $f(x)$ has 7 ramified primes. Therefore K has an infinite class field tower and infinite unramified extension.

6.5 Maire's Results for Infinite Unramified Extension

Construction of Quadratic Field with Finite Hilbert Tower and Infinite Unramified Extension

Maire [16], uses a theorem from Kummer Theory is used to find a quadratic field with finite Hilbert tower and infinite unramified extension:

Theorem 25 (Kummer Theory)**.** Suppose $K/\mathbb{Q}$ is a cyclic extension of degree p, unramified at p, and $L/\mathbb{Q}$ is an extension of degree n. Suppose also that for all places $\mathfrak{Q}$ in L, the ramification index of $\mathbb{Q}$ in $L/\mathbb{Q}$ divides the ramification index of $\mathfrak{q} = \mathbb{Q} \cap \mathfrak{Q}$ in $K/\mathbb{Q}$.

Then the extension $LK/\mathbb{Q}$ is unramified at all finite places. In particular, $\bar{L}K/K$ is also unramified at all finite places.

Construction of Suitable Number Field

Maire gives a construction of such a number field:

Proposition 4. Suppose K is a totally real number field of degree n over $\mathbb{Q}$, and q_1, q_2 are distinct prime numbers with the following criteria:

- $disc(K)$ is equal to some prime l.
- There are precisely $n-2$ unramified places above l in $K/\mathbb{Q}$.
- $q_1 \equiv q_2 \equiv 3$ modulo 4.
- q_1 splits completely in K.
- There are precisely $n-1$ unramified places above q_2 in $K/\mathbb{Q}$.

Also write $k = \mathbb{Q}(\sqrt{l \cdot q_1 \cdot q_2})$ and $M = Kk$. Then k_H/k is finite and k_∞/k is infinite.

Using Theorem 25, all places above q_1 and q_2, as well as the $n-2$ places above l are ramified in M/K. Using the theorem from Golod and Shafaverich, for $n \geq 7$, M has some infinite 2-Hilbert tower, denoted by M_2. Furthermore, M/k is unramified. This implies that $k = \mathbb{Q}(l \cdot q_1 \cdot q_2) \subset M \subset M_2$.

M_2 is an infinite unramified extension of k. But then $\bar{M}_2$ is an infinite unramified Galois extension of k. Maire also shows the following:

Theorem 26. k_H/k is finite.

Proof. Suppose k_1, k_2 and $k = k_3$ are quadratic fields with discriminant l, $l \cdot q_1$, $l \cdot q_1 \cdot q_2$ respectively, (with l, q_1, q_2 as above), and define $F = k_1 k_2$. Since $l \equiv q_1 q_2 \equiv 1 \bmod 4$, F/k_3 is unramified. In addition, if $h(k_1) = h(k_2) = 1$, and $h(k_3) = 2$, then $k_H = F$. Also remark that $h(F) = 1$ and that F/k is unramified, so LF/F is an infinite unramified extension. $\square$

Examples of Quadratic Fields with Finite Hilbert Tower and Infinite Unramified Extension

Using SageMath, the following polynomial and primes were found:

Example 37.

$$f(x) = x^7 - 3x^6 - 5x^5 + 17x^4 + x^3 - 14x^2 + 3x + 1, l = disc(f) = 8980833629 \tag{63}$$

Also define $K = split(P, \mathbb{Q})$. Modulo l,

$$\begin{aligned} P(x) &= (x + 2040911047)(x + 3097257563) \\ &\quad (x + 3210721157)(x + 6041496066) \\ &\quad (x + 6737752038)(x + 7397598321)^2 \end{aligned}$$

Now specify values for q_1 and q_2:

$$q_1 = 17471, q_2 \in \{443, 919, 1627, 2803, 3691, 5231, 5867, 9391\} \tag{64}$$

Then indeed $q_1 \equiv q_2 \equiv 3(4)$. Also, q_1 splits completely in K, and there are $n-1$ places lying above q_2 in $K/\mathbb{Q}$.

This can be restated as a theorem:

Theorem 27. Suppose K is a quadratic field of the form $\mathbb{Q}(\sqrt{8980833629 \cdot 17471 \cdot q_2})$, where

$$q_2 \in \{443, 919, 1627, 2803, 3691, 5231, 5867, 9391\} \tag{65}$$

then

1. K_H/K is finite.
2. K_∞/K is finite.

6.6 Maire's Results for infinite non Galois unramified extension

Following from Maire [16][5.1], there exist infinitely many (imaginary or real) quadratic fields with a finite 2-Hilbert tower, but having an infinite ramified extension of 2^∞. The following methodology was implemented in SageMath to find suitable polynomials:

1. Pick 8 real numbers close to 0 and define $\tilde{P}(x)$ to be the polynomial with these roots. This is done to increase the probability that P(x) will also have 8 real roots.
2. Find a polynomial P(x) which is near to $\tilde{P}(x)$.
3. Check that the P(x) is irreducible, has 8 real roots and has prime discriminant.
4. Search for primes 3 mod 4 which totally decompose in the splitting field of P.

The following polynomial was found:

$$f(x) = x^8 - 3x^7 - 16x^6 + 31x^5 + 74x^4 - 40x^3 - 56x^2 + 17x + 3 \tag{66}$$

where

$$l = disc(f) = 76363470193820546413 \tag{67}$$

Put

$$q_1 = 219823, q_2 = 931363, K = split(P, \mathbb{Q}). \tag{68}$$

Here q_1 and q_2 are totally decomposed in $K/\mathbb{Q}$, the Galois closure of P.
Use the following definitions:

- $N = K\mathbb{Q}(\sqrt{l})$. Note q_1 and q_2 decompose completely in $N/\mathbb{Q}$, an extension of degree 16.
- $E = N(\sqrt{q_1 . q_2})$
- E_2 is the infinite 2-Hilbert tower of E.

In the following diagram, all extensions are unramified 2-extensions.

$$\begin{array}{c} E_2 \\ | \\ \mathrm{E} \\ | \\ \mathbb{Q}\left(\sqrt{l}, \sqrt{q_1 \cdot q_2}\right) \\ | \\ \mathbb{Q}(\sqrt{l . q_1 . q_2}) \end{array}$$

In fact, $E_2/\mathbb{Q}(\sqrt{l \cdot q_1 \cdot q_2})$ is an unramified field extension of degree 2^∞. Furthermore, the choices of q_1 and q_2 guarantee that the 2-part of $cl(\mathbb{Q}(\sqrt{q_1 \cdot q_2}))$ will be cyclic, and that the 2-Hilbert tower stops at the first extension.

Theorem 28 (Cebotarev's Density Criterion)**.** Let L/K be a finite extension of number fields with Galois group G, and let $\mathcal{C}$ be a conjugacy class in G. Then the set of prime ideals of K such that $(\mathfrak{p}, L/K) = \mathcal{C}$ has density $|\mathcal{C}|/|G|$ in the set of all prime ideals of K. If G is abelian, then, for a fixed $\sigma \in G$, the set of prime ideals $\mathfrak{p}$ of K with $\{\mathfrak{p} : (\mathfrak{p}, L/K) = \sigma\} = (G : 1)$.

Corollary 9. If a polynomial $f \in K[x]$ splits into linear factors modulo $\mathfrak{p}$ for all but finitely prime ideals $\mathfrak{p}$ in K, then it splits in $K[x]$.

Proof. Apply the theorem to the splitting field of f. □

Applying Corollary 9 to Proposition 4 proves that there are infinitely many such q_1 and q_2 satisfying the conditions. Finally, for an imaginary quadratic number field with the same properties, keep the same K and q_1, and put $q_2 = -1$, and using $\mathbb{Q}(\sqrt{l \cdot q_1 \cdot q_2})$.

7 Maximal Unramified Extensions of Number Fields

7.1 P-adics

For p-adic fields, it is relatively easy to calculate the maximal unramified extension. To find $\mathbb{Q}_p^{ur}$, it is necessary to define an unramified extension of a local field K. Local Field Theory gives the following results:

Definition. Suppose $L : K$ is a local field extension. Then $L : K$ is unramified if $[L : K] = [l : k]$, where $l = \mathcal{O}_L \pi_L$ and $k = \mathcal{O}_K \pi_K$, where π_L, π_K are the uniformisers of L, K. This is equivalent to saying that π_k is inert in L.

Theorem 29. Fix a local field K with perfect residue field k.. Then there is an equivalence of categories between the extensions of k and the unramified extensions of K.

Example 38. Consider the unramified extensions of $\mathbb{Q}_p$. By Theorem 29, these are in 1-1 correspondence with finite extensions of $\mathbb{F}_p$. For every $n \in \mathbb{N}$, there exists a unique field extension of degree n of $\mathbb{F}_p$, isomorphic to the splitting field of $x^{p^n} - x$.

Therefore $\mathbb{Q}_p$ has a unique field extension of degree n, obtained by adjoining all $(p^n - 1)$-th roots of unity. Furthermore, $\mathbb{Q}_p^{ur}$ is isomorphic to the algebraic closure of $\mathbb{F}_p$, which is obtained by joining the $(p^n - 1)$-th roots of unity for all $n \in \mathbb{N}$. For any n prime to p, $p^{\phi(n)} - 1 \equiv 0 \bmod n$, so

$$\mathbb{Q}_p^{ur} = \mathbb{Q}_p(\{\zeta_n : (n, p) = 1\}) \tag{69}$$

7.2 Yamamura's First Tables of Quadratic Number Fields with Small Conductor

Yamamura [32] defines the structure of $\Gamma(K^{ur}/K)$ where K is an imaginary quadratic number field with small conductors. Note that for all number fields with conductor < 1000, K^{ur} is one of K_1, K_2 or K_3.

Let $K = \mathbb{Q}(\sqrt{d})$ for some integer d. Using Odlyzko's bound Equation (8), the degree $[K^{ur} : K]$ is finite for $|d| \leq 499$, and assuming GRH, replace 499 with 2003. It is known that if $[K^{ur} : K_H] < 60$, then $K^{ur} = K_H$. However this is difficult to prove; for example for $d = -423$, $K_H = K_1$. It is necessary to find the degree $[K_H : \mathbb{Q}]$.

One way is to use the Tower Law from Galois theory. Suppose $\Delta(K) = d_1 d_2 ... d_n$, where $\Delta(K)$ is the discriminant of K, then the genus field of K satisfies $K_g = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, ...\sqrt{d_n})$. Therefore there is the list of inclusions

$$\mathbb{Q} \subseteq K \subseteq K_g \subseteq K_1 \subseteq (K_g)_1 \subseteq K_2 \tag{70}$$

and the tower law gives

$$[K_2 : q] = [K_2 : (K_g)_1] h(K_g) [(K_g)_1 : \mathbb{Q}] \tag{71}$$

Here is an explicit example:

Example 39. Let $d = -1 \cdot 5 \cdot 51 = -255 \equiv 1 \, mod \, 4$. Therefore $|\Delta(K)| = |d| = 255$, and $K_g = \mathbb{Q}(\sqrt{5}, \sqrt{51}$. Computer verification gives that $h(K_g) = 2$, and so

$$[K_2 : \mathbb{Q}] = [K_2 : (K_g)_1]h(K_g)[(K_g)_1 : \mathbb{Q}] = 3 \cdot 2 \cdot 4 = 24 \tag{72}$$

For $d = -255$, $K_H = K_2$. Then calculating shows that $cl(K) \cong C_6 \times C_2$,

$$K_1 = K\left(\sqrt{5}, \sqrt[3]{(9+\sqrt{85})/2}\right), K_2 = K_1\left(\sqrt{2+\sqrt{5}(5+2\sqrt{-3})}\right) \tag{73}$$

In conclusion, Yamamura shows that $\Gamma(K^{ur}/K) \cong Q_8 \times C_3$.

7.3 Imaginary Quadratic Number Fields with Class Number Two

Yamamura [31] gives the following result for imaginary quadratic number fields with class number two.

Theorem 30. Suppose K is an imaginary quadratic number field with class number 2, i.e. $K = \mathbb{Q}(\sqrt{-d}))$, where $d = 15, 20, 24, 35, 40, 51, 52, 88, 91, 115, 123, 148, 187, 232, 235, 267, 403$, or 427. Then

- Except for $d = 115, 235, 403$, $K^{ur} = K_1$
- For $d = 115, 235, 403$, $K^{ur} = K_2$, and $\Gamma(K^{ur}/K)$ can be explicitly calculated.

Lemma 9. By genus theory, $d = d_1 d_2$, where d_1 and d_2 are fundamental prime discriminants. Then $K_1 = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.

Proof. When $d \notin 115, 235, 403$, $h(F) = 1$ and therefore $K_1 = \mathbb{Q}\left(\sqrt{-d_1}, \sqrt{-d_2}\right)$ is an imaginary biquadratic number field with class number one by Lemma 9. Since K_1/K is unramified, $rd_{K_1} = rd_K \leq 267 = 16.340$, and if $d = 427$, and $rd_{K_1} = rd_K = 427 = 20.663$. Now $B(240, 0, 120) = 18.788$, $B(240, 0, 120) = 23.575$ under GRH. Hence under GRH, K_1 is unramified-closed and $K^{ur} = K_1$ □

Corollary 10. Assume GRH. Define $G = \Gamma\left(\mathbb{Q}(\sqrt{-d})^{ur}/\mathbb{Q}(\sqrt{-d})\right)$. Then there are three situations:

- If $d \neq 115, 235, 403$, then have $G \cong C_2$
- If $d = 115, 403$ then $G \cong D_3$.
- If $d = 235$, $G \cong D_5$.

Yamamura also gives the following theorem:

Theorem 31. Suppose K is an imaginary quadratic number field and $G = \Gamma(K^{ur}/K)$. Then unless G is isomorphic to one of C_2, C_3 or D_5, $G^{ab} \ncong C_2$.

These next two lemmata from Group Theory are useful for finding the abelianisation dihedral groups and symmetric groups:

Lemma 10. Suppose $n > 5$ is odd. By Group Theory, $D_n^{ab} \cong C_2$. Then $G \ncong D_n$ for any imaginary quadratic number field.

Lemma 11. Suppose $n > 2$. Then $[S_n] \cong D_n$, meaning that $S_n^{ab} \cong C_2$. By Theorem 31, $G \ncong S_n$ for any imaginary quadratic number field.

Until the paper by Wong [27], GRH was needed to find the maximal unramified extension in the case $d = 427$. Wong removed this dependency. In addition, the following are proved:

- Unconditionally, the number field $\mathbb{Q}(\sqrt{-7}, \sqrt{-61})$ is unramified-closed.
- Assuming GRH, the degree 14 subfield of the cyclotomic field $\mathbb{Q}(\zeta_{49})$ is also unramified-closed.

7.4 More Maximal Unramified Extensions of Quadratic Number Fields

In another paper by Yamamura [33], the table for the $\mathbb{Q}(\sqrt{-d}))^{ur}$ is updated for the missing 19 of the missing 23 values of d, apart from $d = -883, -907, -947$. However, if it can be verified that $K^{ur} \neq K_1$ for these fields, then $\Gamma(K^{ur}/K) \cong PSL(2,7) \times cl(K)$. A previous paper by Yamamura [32] gave the following proposition:

Proposition 5. For $d = 1507 = 11 \cdot 137$, define $f(x) = x^5 - 5x^3 + 5x^2 + 24x + 4$, $disc(f) = 581388544 = 2^8 \cdot 11^2 \cdot 137^2$. Then $\mathbb{Q}(\sqrt{-1507})$ is the first imaginary quadratic number field with an unramified A_5 - extension which is normal over $\mathbb{Q}$, given by the splitting field of f.

Consider now the quadratic number fields defined by

$$-d = 723, 763, 772, 787, 808, 843, 904, 932, 939, 964, 971, 979 \tag{74}$$

which all have Hilbert class tower of length 1.

Proposition 6. For these fields, if K has odd class number, then $K^{ur} = K_1$.

Proof. Conditional Odlyzko bounds give that $[K^{ur} : K_1] < 168 = |PSL(2,7)|$, and by results on group extensions from Group Theory, it is sufficient to show that K_1 does not have a unramified A_5 - extension, normal over $\mathbb{Q}$.

Suppose that K_1 had such an extension, denoted by L. Then $\Gamma(L/K) \cong \Gamma(K_1/K) \times A_5$, and so K would have an unramified A_5 - extension, normal over $\mathbb{Q}$, contradicting Proposition 5. Hence $K^{ur} = K_1$. □

For fields with even class number, for example when

$$-d = 924 = 2^2 \cdot 241,\ h(\mathbb{Q}\left(\sqrt{-924}\right) = |C_2 \times C_6| = 12, \tag{75}$$

existing data for quintic polynomials is used. For K_1 to have an unramified A_5 - extension, normal over $\mathbb{Q}$, it is necessary to find a quintic number field with discriminant $-2^2, 241, -2^2 \cdot 241$ or $2^4 \cdot 241$. Such a field does not exist, as can be verified by the online database at [8]. Therefore $K^{ur} = K_1$, and the proof for other number fields with even class number are similar.

Yamamura also gives the following example.

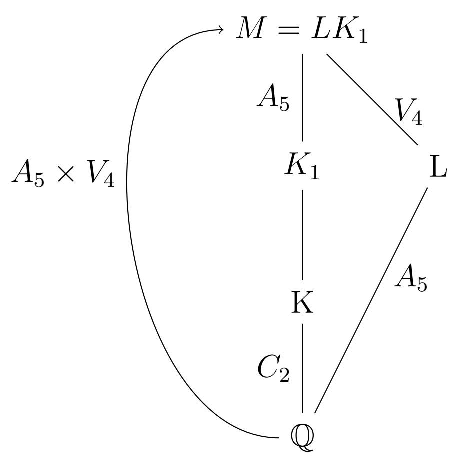
Example 40. Suppose $f(x) = x^7 - x^6 - 3x^5 - x^4 + 2x^3 + 4x^2 + 4x + 1$, E is a defined by a root of f, and $L = \bar{E}$ is the splitting field of f. In addition, define $K = \mathbb{Q}(\sqrt{-3983})$. Noting that $3983 = 7 \cdot 569$, and checking the ramification the rational primes 7 and 569 in E, it can be verified that KE/K is unramified, whence KL/K is also unramified. Therefore KL is an unramified $PSL(2,7)$ - extension of K.

7.5 Kim and Koenig's Results for Maximal Unramified Extensions

Maximal Unramified Extension for the Quadratic Number Field = 22268

Kim and Koenig [11] use Odlyzko's bounds and results from Group Theory to show the following:

Theorem 32. Define $K = \mathbb{Q}(\sqrt{22268})$, noting $22268 = 76 \cdot 293$.
Also define $L = split(x^6 - 10x^4 - 7x^3 + 15x^2 + 14x + 3, \mathbb{Q})$. Then $K \subset K_1 = \mathbb{Q}(\sqrt{76}, \sqrt{293})$, and computer calculation shows that $h(K_1) = 1$, thus K_1 has no nontrivial unsolvable extensions. Define $M = LK_1$. Then $M = K^{ur}$, $\Gamma(K^{ur}/K \cong A_5)$, and the extensions are shown in the following diagram:



Maximal Unramified Extension for the Quadratic Number Field = -1567

Kim and Koenig also calculate the maximal unramified extension of an imaginary quadratic number field, where $d = -1567$. Define $K = \mathbb{Q}(\sqrt{-1567})$ and

$$L = split(x^9 - 2x^8 + 10x^7 - 25x^6 + 34x^5 - 40x^4 + 52x^3 - 45x^2 + 20x - 4, \mathbb{Q}) \tag{76}$$

The following lemma is a useful result in class field theory and will be applied here:

Lemma 12 (Abhyankar's Lemma)**.** Suppose F is a local field, and E_1 and E_2 are finite extensions of F with degrees e_1 and e_2 respectively. In addition, suppose E_2 is tamely ramified and $e_2 | e_1$. Then E_1E_2 is an unramified extension of E_1.

Then the following theorem is used:

Theorem 33. Write $G = PSL_2(\mathbb{F}_8)$. Then L is a G - extension of $\mathbb{Q}$ and 1567 is the only prime in this field which is ramified with index 2. Abhyankar's Lemma shows that LK/K is unramified at every prime. Since G is a non-abelian simple group, it follows that $L \cap K_1 = \mathbb{Q}$. Therefore $\Gamma(LK_1/K_1) \cong \Gamma(L/\mathbb{Q}) \cong G$. Following on from this, $\Gamma(LK_1/\mathbb{Q} \cong G \times D_{15}$.

The field extensions are shown in this diagram:

$$\begin{tikzcd}
 & LK_1 \arrow[d, dash, "G"'] \arrow[dr, dash, "D_{15}"] & \\
 & K_1 \arrow[d, dash] & L \arrow[ddl, dash, "G"] \\
 & K \arrow[d, dash, "C_2"'] & \\
 & \mathbb{Q} \arrow[uuu, bend left=80, "G \times D_{15}"] \arrow[uu, bend left=60, "D_{15}"'] &
\end{tikzcd}$$

7.6 Real Quadratic Number Fields with Unsolvable Maximal Unramified Extension

In this section, GRH is assumed. Under this assumption, Kim [10] shows that for $d \in \{13613, 16621, 16701\}$, $\Gamma(\mathbb{Q}(\sqrt{d})^{ur}/\mathbb{Q}(\sqrt{d}))$ is isomorphic to an unsolvable finite group.

Definitions

The following definitions are from Group Theory

Definition. Suppose G is a group. The **automorphism group** $Aut(G)$ is the group consisting of all the automorphisms of G.

Definition. Suppose N and Q are two groups. G is an **extension** of Q by N if there exists a short exact sequence

$$1 \to N \to G \to Q \to 1 \tag{77}$$

Such an extension is called a **central extension** if the centre of G contains N.

Definition. A **p-group** for a given prime number p is a group in which every element has order a power of p.

The following proposition from Group Theory is relevant:

Proposition 7. Let H be an abelian 2-group. Suppose that $1 \to H \to G \to A_5 \to 1$ is a central extension of A_5 by H. If $|H| > 2$ then G has a non-trivial abelian quotient, whereas if $|H| = 2$, then G is isomorphic either to $C_2 \times A_5$ or to $SL_2(F_5)$.

Calculation of the Maximal Unramified Extension of Certain Fields

Kim also gives several examples for the determination of the maximal unramified extension of certain quadratic number fields: Let $K = \mathbb{Q}(\sqrt{13613})$, and let L be the splitting field of $f(x) = x^6 - 13x^4 - 7x^3 + 44x^2 + 40x - 9$, and E be a number field defined by a root of f, so L is the Galois closure of E. Then f has a discriminant of 163^2 and factorises as

$$(x + 4519)(x + 6371)^2(x + 10315)(x + 13438)^2 \, mod \, 13613. \tag{78}$$

Therefore L is an A_5 - extension of $\mathbb{Q}$ unramified only at 13613 with ramification index 2. By Abhyankar's Lemma, LK/K is unramified at all primes. A_5 is an non-abelian simple group, so $L \cap$K$= \mathbb{Q}$ and $\Gamma(LK/K) \cong \Gamma(L/\mathbb{Q}) \cong A_5$, whence LK is an unramified A_5 - extension of K.

Now write $M = LK$. Since M/K is unramified at all places, M and K have the same root discriminant, $rd_M = rd_K = \sqrt{13613} = 116.67 < 121.11 = B(2400, 2400, 0)$. Therefore $[K^{ur} : M] < 20$.

Now define $N = KE$, and N is a subfield of M, so N/K is unramified. Following the known fact that $N/M \cong D_5$, the Fundamental Theorem of Galois Theory shows that there must exist some intermediate field F, $M/F/N$ with $\Gamma(M/F) \cong A_5$ and $\Gamma(F/N) \cong C_2$.

Calculation gives that $h(N) = 4$ and $cl(N) \cong C_4$, whence M has some unramified C_2 - extension T with closure $S = \bar{T}$. Therefore S/M is an unramified extension with Galois group $\Gamma(S/M) \cong (C_2)^n$ for some $1 \leq n \leq 4$.

For $n = 2$, $|Aut((C_2)^2)| = |C_2| = 2$, and for $n = 3$, $|Aut((C_2)^3)| = |PSL(3, 2)| = 168$. In either case, the order is not divisible by 60, so $\Gamma(M/K)$ acts trivially on $\Gamma(S/M)$. By proposition 7, $\Gamma(S/K)$ has an abelian quotient, contradicting $h(K) = 1$.

Now suppose that $n = 4$. If $\Gamma(M/K)$ acts trivially on $\Gamma(S/M)$, applying Proposition 7 will lead to a contradiction. Let $\tilde{N}$ denote the unique intermediate field in $N_2/\tilde{N}/N$, and $\Gamma(N_2/\tilde{N})$ is an abelian quotient of $\Gamma(S/\tilde{N})$.
Noting that $\Gamma(S/\tilde{N})$ is a C_5 - extension of $\Gamma(M/\tilde{N})$ by $\Gamma(S/M) \cong (C_2)^4$. Since $\Gamma(M/\tilde{N})$ acts non-trivially on $\Gamma(S/M)$ and it follows that $\Gamma(S/\tilde{N})$ does not have C_2 as a quotient, with contradiction.

Therefore, $m = 1$, implying that $S = T$ and $\Gamma(T/M) = \Gamma(S/M) \cong C_2$. By the proposition 7, $\Gamma(T/K) \cong A_5 \times C_2$ or $\cong SL_2(\mathbb{F}_5)$ However, $A_5 \times C_2$ has an abelian quotient. Therefore, $SL_2(F_5)$ is the only possibility. Since T is a $\mathbb{Q}$ - extension of degree 240, $[K^{ur} : T] < 10$.

7.6.1 p-class Groups of T

Let T^p be the Hilbert p-class field of T. Since T is Galois over $\mathbb{Q}$, so is T^p.

Lemma 13. There does not exist a group G with $|G| < 10$ such that $Aut(G)$ contains a subgroup isomorphic to A_5 or $SL_2(\mathbb{F}_5)$

Proof. Easy check. □

Corollary 11. $\Gamma(T/K) \cong (SL_2(\mathbb{F}_5))$ acts trivially on $\Gamma(T^p/K)$. Therefore $\Gamma(T^p/K)$ is a central extension of $SL_2(\mathbb{F}_5)$ by $\Gamma(T^p/T)$.

Since $\Gamma(T/M) \cong C_2$, $\Gamma(T^p/M)$ is abelian and $\Gamma(T^p/K)$ is a central extension of $\Gamma(M/K) \cong A_5$ by some abelian group $\Gamma(T^p/M)$.

By Proposition 7 and Corollary 11, $\Gamma(T^p/K)$ has an abelian quotient, contradicting $h(K) = 1$.

Therefore $\Gamma(K^{ur}/T)$ is trivial and so $\Gamma(K^{ur}/K) \cong SL_2(\mathbb{F}_5)$. Note that $SL_2(\mathbb{F}_5)$ is an unsolvable group.

Here are two more examples of the maximal unramified extension of quadratic number fields from Kim:

Example 41. Suppose $K = \mathbb{Q}(\sqrt{16621})$ and $f(x) = x^6 - 13x^4 - 4x^3 + 36x^2 + 3x - 22$. Then $disc(f) = 11^2 \cdot 1511^2 = 16621^2$. Let L be the splitting field of f, and so L is an unramified A_5 - extension of K and similar to the previous example, $\Gamma(K^{ur}/K) \cong SL_2(\mathbb{F}_5)$.

Example 42. Let K be the real quadratic field $\mathbb{Q}(\sqrt{16701})$. Then, under the assumption of GRH, $\Gamma(K^{ur}/K) \cong A_5 \times C_2$. Since A_5 is a subgroup of $A_5 \times C_2$, and A_5 is not solvable, $A_5 \times C_2$ is also not solvable.

7.7 Serre's Calculation of Maximal Unramified Extensions of Quadratic number Fields

Maximal Unramified Extension for d = -23

Serre [6] gives two examples of the maximal unramified extension of a quadratic number field: Consider the polynomial

$$f(x) = x^3 - x - 1,\ disc(f) = -23 \tag{79}$$

Note f has one real root and two imaginary roots. Let L denote its splitting field. Then $\Gamma(L/\mathbb{Q}) \cong S_3$ and it is a degree three extension of the quadratic field $K = \mathbb{Q}(\sqrt{-23})$. Now $h(K) = 3$ so using Odlyzko's bounds proves that L is the maximal unramified abelian extension of K, and Martinet shows that indeed $L = K^{ur}$. The relationships between fields are shown in the diagram below:

$$\begin{tikzcd}
L = K^{ur} \arrow[d, dash] \\
\mathrm{K} \arrow[d, dash, "C_2"] \\
\mathbb{Q} \arrow[uu, bend left=60, "S_3"]
\end{tikzcd}$$

7.8 Maximal Unramified Extension for d = -283

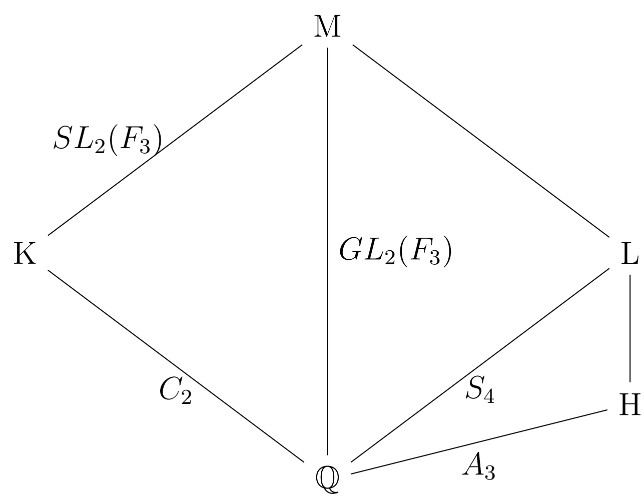
Note that this result is also tabulated in Yamamura's paper [32]. Define

$$f(x) = x^4 - x - 1,\ disc(f) = -283 \tag{80}$$

First observe that f has two real and two imaginary roots. Define $L = split(f, \mathbb{Q})$ and note that $\Gamma(L/\mathbb{Q}) \cong S_4$. By the Fundamental Theorem of Galois Theory, there exists an intermediate field H corresponding to the normal subgroup V_4 of S_4. Now L^H is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-283})$ and $h(K) = 3$.

Now define a further field extension of M/L such that M is unramified over L (and hence also over K) and M is a Galois extension of $\mathbb{Q}$. A construction (given by Tate) is that $M = L(\sqrt{4 - 7\theta^2})$, where θ is a root of f in L.

Martinet proved that M is the maximal unramified extension of K, and $\Gamma(M/K) \cong SL_2(\mathbb{F}_3)$, of order 24. In addition, the Galois group of $M/\mathbb{Q}$ is isomorphic to $GL_2(\mathbb{F}_3)$. The relationships between fields are shown in the diagram below:



7.9 Maximal Unramified Extensions of Cyclic Cubic Fields

The maximal unramified extensions of quadratic number fields have been well-studied, and some examples have been given in this section already. In the paper by Wong [26], examples of maximal unramified extensions of cyclic cubic number fields are given.

Let $K = \mathbb{Q}(\theta)$ where θ is the root of a cubic polynomial $f(x)$. If $\Gamma(K/\mathbb{Q}) \cong A_3$, call K a **cyclic cubic field**.

Proposition 8 (Galois Theory)**.** Then K is a cyclic cubic field iff disc(f) is a square.

If K is a totally real cubic number field, the unconditional bound for the root discriminant given by Odlyzko (and published by Martinet) is 46.42. Assuming GRH can increase this value to 72.55. Wong [26] tabulates the all cyclic cubic fields ramified at one prime with trivial class group.

Theorem 34. The first 28 (47 under GRH) cyclic cubic fields with class number 1 have trivial maximal unramified extension.

Example 43. Let $f = x^3 - x^2 - 2x + 1$. Then $\Delta(K) = 7^2$, $rd_k = 3.66$ and h(K)=1. Then unconditionally, K does not have an unsolvable unramified extension and $\Gamma(K/\mathbb{Q}) \cong C_3$.

Example 44. $f(x) = x^3 - x^2 - 110x + 49$, $\Delta(K) = 331^2$, $72.55 > rd_K = 47.85 > 46.42$. Therefore under the assumption of GRH, K does not have an unsolvable unramified extension, $\Gamma(K/\mathbb{Q}) \cong C_3$, but without this assumption, Odlyzko's bound is not strong enough to conclude this.

Wong also gives examples of how to calculate the maximal unramified extension of a cyclic cubic field with nontrivial class group.

Example 45. $f = x^3 - x^2 - 54x + 169$, disc(K)=$163^2$, $rd_k = 29.84$. Here the class number $h(K) = 4$. Define $g(x) = x^6 - 3x^5 - 11x^4 + 27x^3 - 3x^2 - 11x + 1$. Then the online database at [8] gives $L = split(g, \mathbb{Q})$ with $\Delta(K_1) = 163^4$.

Firstly $\Gamma(L/\mathbb{Q}) \cong A_4$, and 163 is unramified in L/K. Hence indeed $L = K_1$. It is known that $\Gamma(L/K) \cong V_4$ which is a normal subgroup of A_4. Now h(L)=1 and $rd_K < 54.62$ which is the lower bound for the root discriminant of totally real fields of degree 720, certainly $\Gamma(K^{ur}/K) \cong V_4$ and $\Gamma(K^{ur}/\mathbb{Q}) \cong A_4$.

Example 46. K is the cyclic cubic field defined by $x^3 - x^2 - 104x - 371$ with $d_K = 313^2$ and $rd_K = 46.10$. Now h(K)=7. Define $g(x) = x^7 - x^6 - 15x^5 + 20x^4 + 33x^3 - 22x^2 - 32x + 8$.

Calculation shows that $K_1 = split(g, \mathbb{Q})$ with field discriminant 313^4, $h(K_1) = 1$ and $rd_K = 46.10 < 56.47$. Since 56.47 is the lower bound for totally real fields of degree 1260, indeed $K^{ur} = K_1$. In this case, $\Gamma(K^{ur}/K) \cong C_7$ and $\Gamma(K^{ur}/\mathbb{Q}) \cong F_{21}$.

References

[1] David Brink. Remark on infinite unramified extensions of number fields with class number one. *Journal of Number Theory*, 130(2):304 – 306, 2010.

[2] I.R. Shafarevich" "E.S. Golod. "on the class field tower". *"Izv. Akad. Nauk SSSR Ser. Mat."*, 28:261–272, 1964.

[3] Farshid Hajir and Christian Maire. Tamely ramified towers and discriminant bounds for number fields—ii. *Journal of Symbolic Computation*, 33(4):415 – 423, 2002.

[4] KConrad (https://mathoverflow.net/users/3272/kconrad). Is there a ring of integers except for z, such that every extension of it is ramified? MathOverflow. URL:https://mathoverflow.net/q/26504 (version: 2016-12-01).

[5] John Hunter. The minimum discriminants of quintic fields. *Proceedings of the Glasgow Mathematical Association*, 3(2):57–67, 1957.

[6] Serre Jean-Pierre. On a theorem of jordan. *Bulletin (New Series) of the American Mathematical Society*, 40, 08 2003.

[7] John Jones and David Roberts. Number fields ramified at one prime. volume 5011, pages 226–239, 05 2008.

[8] John W. Jones and David P. Roberts. A database of number fields. *LMS Journal of Computation and Mathematics*, 17(1):595–618, 2014.

[9] Kwang-Seob Kim. Construction of unramified extensions with a prescribed galois group. *Osaka J. Math.*, 52(4):1039–1051, 10 2015.

[10] Kwang-Seob Kim. Some examples of real quadratic fields with finite nonsolvable maximal unramified extensions. *Journal of Number Theory*, 166:235 – 249, 2016.

[11] Kwang-Seob Kim and Joachim König. Some examples of quadratic fields with finite nonsolvable maximal unramified extensions ii, 2017.

[12] Yasuhiro Kishi. A new family of imaginary quadratic fields whose class number is divisible by five. *Journal of Number Theory*, 128(8):2450 – 2458, 2008.

[13] Helmut Koch. *Number Theory: Algebraic Numbers and Functions (Graduate Studies in Mathematics)*. American Mathematical Society, 2000.

[14] Takeshi Kondo. Algebraic number fields with the discriminant equal to that of a quadratic number field. *J. Math. Soc. Japan*, 47(1):31–36, 01 1995.

[15] Sylla Lesseni. Nonsolvable nonic number fields ramified only at one small prime. *Journal de théorie des nombres de Bordeaux*, 18(3):617–625, 2006.

[16] Christian Maire. On infinite unramified extensions. *Pacific Journal of Mathematics*, 192, 01 2006.

[17] Jacques Martinet. Tours de corps de classes et estimations de discriminants. *Séminaire de Théorie des Nombres de Bordeaux*, pages 1–4, 1976.

[18] Carlos Julio Moreno. *Advanced Analytic Number Theory: L-functions (AMS Mathematical Surveys and Monographs, Volume 115)*. American Mathematical Society, 2005.

[19] Jürgen Neukirch. *Algebraic Number Theory (Grundlehren der mathematischen Wissenschaften) (v. 322)*. Springer, 1999.

[20] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions : a survey of recent results. *Journal de théorie des nombres de Bordeaux*, 2(1):119–141, 1990.

[21] René Schoof. Infinite class field towers of quadratic fields. *Journal für die reine und angewandte Mathematik*, 372:209–220, 1986.

[22] Ernst S. Selmer. The irreducibility of certain trinomials. *Mathematica Scandinavica*, 4(2):287–302, 1957.

[23] Gene Ward Smith. Families of unramified extensions of number fields, 2012.

[24] Kôji Uchida. Unramified extensions of quadratic number fields, i. *Tohoku Math. J. (2)*, 22(1):138–141, 1970.

[25] B.L. van der Waerden. Die zerlegungs- und trägheitsgruppe als permutationsgruppen. *Mathematische Annalen*, 111:731–733, 1935.

[26] Ka Lun Wong. Maximal unramified extensions of cyclic cubic fields. 2011.

[27] Siman Wong. The maximal unramified extensions of certain complex abelian number fields. 2015.

[28] Yoshihiko Yamamoto. On unramified galois extensions of quadratic number fields. *Osaka J. Math.*, 7(1):57–76, 1970.

[29] Ken Yamamura. On infinite unramified galois extensions of algebraic number fields with many primes decomposing almost completely. *J. Math. Soc. Japan*, 38(4):599–605, 10 1986.

[30] Ken Yamamura. On unramified galois extensions of real quadratic number fields. *Osaka J. Math.*, 23(2):471–478, 1986.

[31] Ken Yamamura. The maximal unramified extensions of the imaginary quadratic number fields with class number two. *Journal of Number Theory*, 60(1):42 – 50, 1996.

[32] Ken Yamamura. Maximal unramified extensions of imaginary quadratic number fields of small conductors. *Proc. Japan Acad. Ser. A Math. Sci.*, 73(4):67–71, 1997.

[33] Ken Yamamura. Maximal unramified extensions of imaginary quadratic number fields of small conductors, ii. *Journal de théorie des nombres de Bordeaux*, 13(2):633–649, 2001.