Brigham Young University
BYU ScholarsArchive

Theses and Dissertations

2021-12-17

Pentagonal Extensions of the Rationals Ramified at a Single Prime

Pablo Miguel Rodriguez
Brigham Young University

Follow this and additional works at: https://scholarsarchive.byu.edu/etd

 Part of the Physical Sciences and Mathematics Commons

BYU ScholarsArchive Citation

Rodriguez, Pablo Miguel, "Pentagonal Extensions of the Rationals Ramified at a Single Prime" (2021). *Theses and Dissertations*. 9342.
https://scholarsarchive.byu.edu/etd/9342

This Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact ellen_amatangelo@byu.edu.

Pentagonal Extensions of the Rationals Ramified at a Single Prime

Pablo Miguel Rodriguez

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Darrin Doud, Chair
Michael Griffin
Pace Nielsen

Department of Mathematics

Brigham Young University

Copyright © 2021 Pablo Miguel Rodriguez

All Rights Reserved

ABSTRACT

Pentagonal Extensions of the Rationals Ramified at a Single Prime

Pablo Miguel Rodriguez
Department of Mathematics, BYU
Master of Science

In this thesis, we define a certain group of order 160, which we call the hyperpentagonal group, and we prove that every totally real D_5-extension of $\mathbb{Q}$ ramified at only one prime is contained in a hyperpentagonal extension of $\mathbb{Q}$. This generalizes a result of Doud and Childers (originally conjectured by Wong) that every totally real S_3 extension of $\mathbb{Q}$ ramified at only one prime is contained in an S_4 extension.

Keywords: algebraic number theory, number theory, algebra

Acknowledgements

I would like to thank everyone that helped make this thesis happen. To Dr. Griffin for the time he took to read and make comments. To Dr. Nielsen for being an amazing lecturer and furthering my understanding of algebra. A great deal of the content in this thesis relies on all that he taught me in his algebra courses. I also greatly appreciate the time he put in to make several invaluable comments. I would also like to thank my advisor Dr. Doud for all of his help and dedication to me and this work. Were it not for his help and guidance this thesis would not be sitting before you. Lastly, I would like to thank my parents for their endless support in my mathematical endeavors; which ultimately lead to this work.

Contents

Chapter 1. Introduction

In [14], Wong made the following conjecture:

Conjecture 1.1. *Let $K_3/\mathbb{Q}$ be a non-Abelian cubic field such that $|d_{K^3}|$ is a prime power. Then the number of S_4-extensions $K_{24}/\mathbb{Q}$ containing K_3 and with prime-power discriminants is $2^n - 1$ for some integer n. Furthermore, if $K_3/\mathbb{Q}$ is totally real, then $n > 0$.*

This conjecture has two parts: first the claim that the number of S_4 extensions of $\mathbb{Q}$ containing K is of the form $2^n - 1$ for some n, and second that if K is totally real, then $n > 0$, so that $2^n - 1 > 0$ as well.

In [2], Childers and Doud proved both parts of Wong's conjecture. Their proof of the second part (which was the main contribution of [2]) involves finding an extension $K(\sqrt{\pi})/K$ for some $\pi \in \mathfrak{O}_K$ such that $K(\sqrt{\pi})/\mathbb{Q}$ is still unramified outside the prime p, see Figure 1.1. They then examined the possible Galois groups of the Galois closure of L of $K(\sqrt{u})/\mathbb{Q}$, and showed that the only possible Galois group was S_4.

In this thesis, we will generalize the second part of Wong's conjecture to apply to quintic fields K whose Galois closure has Galois group D_5. In place of the group S_4 that Wong uses, we have identified a specific transitive group of degree 10, which we call the hyperpentagonal group. The main theorem that we prove is the following:

Theorem 1.2. *Given any totally real quintic field $K/\mathbb{Q}$ that is ramified at only one prime p and is contained in a D_5 extension of $\mathbb{Q}$, there is an extension $M/\mathbb{Q}$ that contains K, is ramified only at p, and has $\mathrm{Gal}(M/\mathbb{Q})$ isomorphic to a hyperpentagonal group.*

Our proof is similar to that of Childers and Doud. We begin by analyzing how p can factor in K. A detailed study of the units of K allows us to construct a quadratic extension $K(\sqrt{\pi})/K$ that is ramified at a single prime of K lying over p (see Figure 1.2). In order to determine the Galois group of the Galois closure of $K(\sqrt{\pi})/\mathbb{Q}$, we note that this Galois group will be isomorphic to a transitive subgroup of S_{10}. Up to conjugacy, there are 45

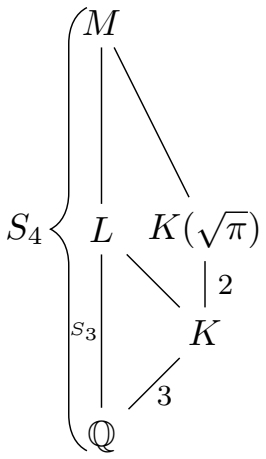

Figure 1.1: The case Wong considered and Childers and Doud proved.

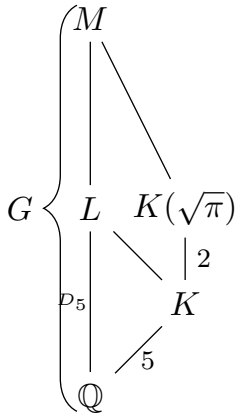

Figure 1.2: The case we will be considering

such groups, and by describing three conditions that $\mathrm{Gal}(M/\mathbb{Q})$ must satisfy, we rule out 43 of these groups. The two remaining subgroups of S_{10} are isomorphic, but not conjugate. We call a group isomorphic to either of them a hyperpentagonal group. In terms of the generalization of Wong's conjecture, it plays the same role for D_5 as the group S_4 plays for $S_3 = D_3$.

Note that the hyperpentagonal group is similar to S_4, in that the hyperpentagonal group has two isomorphic but nonconjugate copies inside S_{10}, while S_4 has two isomorphic but nonconjugate copies inside S_6 [4, page 329].

Chapter 2. Algebraic Number Theory

2.1 Ramification Theorems

Definition 2.1. Let $K \subseteq L$ be an extension of number fields. We denote the ramification index of a prime $\mathfrak{q}$ of L lying over $\mathfrak{p}$ as $e(\mathfrak{q}|\mathfrak{p})$ and the inertial degree as $f(\mathfrak{q}|\mathfrak{p})$.

In an extension of number fields, the inertial degree and ramification index can be used to describe possible factorizations of a prime p in the lower field. We describe some well known relationships between inerital degress and ramification indices of primes in number field extensions.

Theorem 2.2 ([12, Chapter 3, Exercise 10])**.** *Let $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{u}$ be primes of $\mathfrak{O}_K \subset \mathfrak{O}_L \subset \mathfrak{O}_F$ respectively. We then have*

$$e(\mathfrak{u}|\mathfrak{p}) = e(\mathfrak{u}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p}) \tag{2.1}$$

$$f(\mathfrak{u}|\mathfrak{p}) = f(\mathfrak{u}|\mathfrak{q})f(\mathfrak{q}|\mathfrak{p}). \tag{2.2}$$

Theorem 2.3 ([12, Theorem 21])**.** *Let L be an extension of K and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the primes of $\mathfrak{O}_L$ lying over a prime $\mathfrak{p}$ of $\mathfrak{O}_K$. Let $e_i = e(\mathfrak{q}_i|\mathfrak{p})$ and $f_i = f(\mathfrak{q}_i|\mathfrak{p})$, then $\sum_{i=1}^{r} e_i f_i = n$.*

In a Galois extension we have more information as to how a prime can factor:

Theorem 2.4 ([12, Theorem 23])**.** *Let L be a Galois extension of K and let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be two primes of $\mathfrak{O}_L$ lying over the same prime $\mathfrak{p}$ of $\mathfrak{O}_K$. Then for some $\sigma \in \mathrm{Gal}(L/K)$ we have $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$.*

This immediately gives us

Corollary 2.5 ([12, Corollary to Theorem 23])**.** *If L is a Galois extension of K and $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are two primes lying over $\mathfrak{p}$, then $e(\mathfrak{q}_1|\mathfrak{p}) = e(\mathfrak{q}_2|\mathfrak{p})$ and $f(\mathfrak{q}_1|\mathfrak{p}) = f(\mathfrak{q}_2|\mathfrak{p})$.*

Thus in a Galois extension, each prime of $\mathfrak{O}_L$ lying over a prime $\mathfrak{p}$ in $\mathfrak{O}_K$ has the same ramification index and inertial degree. With Corollary 2.5 together with Theorem 2.3 we obtain

Corollary 2.6. *Let L be a Galois extension of K, $\mathfrak{p}$ be a prime of K, $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be all primes of L lying above $\mathfrak{p}$. Then each $e(\mathfrak{q}_i|\mathfrak{p})$ has the same value, which we denote by e. Similarly, each $f(\mathfrak{q}_i|\mathfrak{p})$ has the same value, which we denote by f. We then have $ref = [L : K]$.*

We can use the ramification indices and inertial degrees to determine the exact power of a prime dividing the discriminant of a number field.

Theorem 2.7 ([5, Corollary 4.10.])**.** *Let F be a number field, write $p\mathfrak{O}_F$ as $\prod_{i=1}^{m} \mathfrak{p}_i^{e_i}$ for distinct prime ideals $\mathfrak{p}_i$, set $f_i = f(\mathfrak{p}_i|p)$ and $e_i = e(\mathfrak{p}_i|p)$. If no e_i is a multiple of p then the multiplicity of p in* $\mathrm{disc}(K)$ *is*

$$\sum_{i=1}^{m}(e_i - 1)f_i = n - \sum_{i=1}^{m} f_i. \tag{2.3}$$

2.2 Ramification Groups

We now discuss the ramification groups, which further allow us to determine the possible factorizations of a prime in an extension.

Definition 2.8. Let L be a Galois extension of K and let $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{q}$ be a prime of $\mathfrak{O}_L$. Define the *ramification groups* for $m \geq 0$ as

$$V_m(\mathfrak{q}) = \{\sigma \in G \mid \sigma(\alpha) = \alpha \bmod \mathfrak{q}^{m+1} \quad \forall \alpha \in \mathfrak{O}_L\}. \tag{2.4}$$

We then have the following properties of ramification groups:

Theorem 2.9 ([12, Exercise 4.21])**.** *With the same notation as above we have $V_0(\mathfrak{q})/V_1(\mathfrak{q})$ is cyclic of order dividing $|\mathfrak{O}_L/\mathfrak{q}| - 1$.*

Theorem 2.10 ([12, Exercise 4.23]). *With the same notation as above, $V_1(\mathfrak{q})$ is the Sylow p-subgroup of $V_0(\mathfrak{q})$, where p is the prime of $\mathbb{Z}$ lying under $\mathfrak{q}$. Additionally, if $\mathfrak{p}$ is a prime of $\mathfrak{O}_K$ lying over the prime $p \in \mathbb{Q}$ and under $\mathfrak{q}$, $V_1(\mathfrak{q})$ is nontrivial if and only if $e(\mathfrak{q}|\mathfrak{p})$ is divisible by p.*

2.3 Quadratic Extension

Any quadratic extension L/K of number fields can be constructed as $L = K(\sqrt{u})$ for some $u \in K$. We will be interested in determining which primes of K ramify in such an extension. The following theorem helps us determine this.

Theorem 2.11 ([7, Lemma 5.32]). *Let $L = K(\sqrt{u})$ be a quadratic extension with $u \in \mathfrak{O}_K$, and let $\mathfrak{q}$ be a prime in $\mathfrak{O}_K$.*

(i) If $2u \notin \mathfrak{q}$, then $\mathfrak{q}$ is unramified in L.

(ii) If $2 \in \mathfrak{q}, u \notin \mathfrak{q}$ and $u = b^2 - 4c$ for some $b, c \in \mathfrak{O}_K$, then $\mathfrak{q}$ is unramified in L.

Proof. (i) Suppose $2u \notin \mathfrak{q}$, it follows that $2 \notin \mathfrak{q}$ as well since $u \in \mathfrak{O}_K$ and $\mathfrak{q}$ is an ideal. From this and primality it follows that $4u = 2(2u) \notin \mathfrak{q}$. The minimal polynomial for $\sqrt{u}$ is $f(x) = x^2 - u$. Since the discriminant of $f(x)$ is $4u \notin \mathfrak{q}$ it follows that there are two distinct roots mod $\mathfrak{q}$. It then follows from Proposition 5.11 in [7] that $\mathfrak{q}$ factors into a product of two distinct prime ideals in L and thus does not ramify in L.

(ii) Let $\beta = (-b + \sqrt{u})/2$, clearly $L = K(\beta)$. The polynomial $g(x) = x^2 + bx + c$ has β as a root so the ramification of $\mathfrak{q}$ is determined by factoring $g(x)$ mod $\mathfrak{q}$. Since the discriminant of g is $b^2 - 4c = u \notin \mathfrak{q}$ we then have that g has two distinct roots and so $\mathfrak{q}$ is unramified in L. □

2.4 Exact Sequence

To apply the previous theorem, we need to determine whether u is congruent to a square modulo $4\mathfrak{O}_K$. Hence, we will be interested in the structure of the multiplicative group

$(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. To study this structure, we prove the following general theorem about the structure of $(\mathfrak{O}_K/\mathfrak{p}^2\mathfrak{O}_K)^\times$, for any prime $\mathfrak{p}$ of K.

Theorem 2.12 ([7, Exercise 7.28])**.** *Let K be a quadratic field and let $\mathfrak{p}$ be a prime in $\mathfrak{O}_K$. For $n \geq 2$, there is an exact sequence*

$$1 \longrightarrow \mathfrak{O}_K/\mathfrak{p} \longrightarrow (\mathfrak{O}_K/\mathfrak{p}^n)^\times \longrightarrow (\mathfrak{O}_K/\mathfrak{p}^{n-1})^\times \longrightarrow 1. \tag{2.5}$$

If $n = 2$, then this sequence is split exact.

We have the following lemmas where the notations above are assumed throughout.

Lemma 2.13. *The map $\pi\colon (\mathfrak{O}_K/\mathfrak{p}^n)^\times \to (\mathfrak{O}_K/\mathfrak{p}^{n-1})^\times$ defined by $\alpha + \mathfrak{p}^n \mapsto \alpha + \mathfrak{p}^{n-1}$ is surjective.*

Proof. Let $\beta + \mathfrak{p}^{n-1} \in (\mathfrak{O}_K/\mathfrak{p}^{n-1})^\times$ and let $\alpha + \mathfrak{p}^{n-1}$ be its inverse. Then $\alpha\beta - 1 = \gamma \in \mathfrak{p}^{n-1}$. We then have

$$\beta(\alpha - \alpha\gamma) = \alpha\beta - \alpha\beta\gamma = 1 + \gamma - \gamma - \gamma^2 = 1 - \gamma^2.$$

Since $\gamma^2 \in \mathfrak{p}^{2(n-1)}$, and $2(n-1) = n + (n-2) \geq n$, we see that $\gamma^2 \in \mathfrak{p}^n$, so $\beta(\alpha - \alpha\gamma) = 1 + \mathfrak{p}^n$. By definition we have $\beta \in (\mathfrak{O}_K/\mathfrak{p}^n)^\times$. Then $\pi(\beta + \mathfrak{p}^n) = \beta + \mathfrak{p}^{n-1}$, so π is onto. □

Lemma 2.14. *Let $u \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$, then $[1 + \alpha u] \in (\mathfrak{O}_K/\mathfrak{p}^n)^\times$.*

Proof. Let $\alpha \in \mathfrak{O}_K$ then

$$(1 + \alpha u)(1 - \alpha u) = 1 - \alpha^2 u^2 = 1 \bmod \mathfrak{p}^n,$$

so $1 + \alpha u + \mathfrak{p}^n \in (\mathfrak{O}_K/\mathfrak{p}^n)^\times$. □

Lemma 2.15. *Let $\alpha \in \mathfrak{O}_K$ and $u \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$. Suppose $\alpha u \in \mathfrak{p}^n$, then $\alpha \in \mathfrak{p}$.*

Proof. Suppose for a contradiction that $\alpha \notin \mathfrak{p}$ but $\alpha u \in \mathfrak{p}^n$, then the prime factorization of the ideal is $(\alpha) = \prod \mathfrak{q}_i^{n_i}$ with each $\mathfrak{q}_i \neq \mathfrak{p}$. Since $u \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$ we know $(u) \subseteq \mathfrak{p}^{n-1}$ so

$(u) = \mathfrak{p}^{n-1}\prod \mathfrak{p}_i^{m_i}$ where $\mathfrak{p}_i \neq \mathfrak{p}$. We then have that $(\alpha u) = \mathfrak{p}^{n-1}\prod \mathfrak{p}_i^{n_i}\mathfrak{q}_i^{m_i}$ but $(\alpha u) \subseteq \mathfrak{p}^n$ so $v_{\mathfrak{p}}(\alpha u) \geq n$ but $v_{\mathfrak{p}}(\alpha u) = n-1$ by construction. This is a contradiction so it follows that $\alpha \in \mathfrak{p}$. □

Lemma 2.16. *Let π be the map defined in Lemma 2.13 and $u \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$. If $x + \mathfrak{p}^n \in \ker \pi$ so $x = 1 + \gamma$ for some $\gamma \in \mathfrak{p}^{n-1}$, then $\gamma = au + bv$ for some $v \in \mathfrak{p}^n$, and some $a, b \in \mathfrak{O}_K$.*

Proof. We have that $(u) = \mathfrak{p}^{n-1}\prod \mathfrak{q}_i^{e_i}$ where $\mathfrak{q}_i \neq \mathfrak{p}$ for all i. Since $(\mathfrak{p}, \mathfrak{q}_i) = (1)$ as $\mathfrak{p} \neq \mathfrak{q}_i$ we know by the Chinese Remainder Theorem that the following system has a solution for v:

$$\begin{aligned} v &= 0 \pmod{\mathfrak{p}^n} \\ v &= 1 \pmod{\mathfrak{q}_i}. \end{aligned}$$

Since $v = 1 \bmod \mathfrak{q}_i$ we know $(u, v) = \mathfrak{p}^{n-1}$ as desired. Since $\gamma \in \mathfrak{p}^{n-1}$ there exists $a, b \in \mathfrak{O}_K$ so that $\gamma = au + bv$. □

We now proceed to the proof of Theorem 2.12.

Proof. Let $u \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$, define π to be the map from Lemma 2.13, and define $\varphi\colon \mathfrak{O}_K/\mathfrak{p} \to (\mathfrak{O}_K/\mathfrak{p}^n)^\times$ by $\alpha + \mathfrak{p} \mapsto 1 + \alpha u + \mathfrak{p}^n$. Using this we show that the sequence in (2.5) is exact.

By Lemma 2.13 we know π is surjective, now we show $\ker \varphi$ is trivial. Let $\alpha + \mathfrak{p} \in \ker \varphi$. We then have $1 + \alpha u = 1 \bmod \mathfrak{p}^n$ so $\alpha u \in \mathfrak{p}^n$, by Lemma 2.15 we know $\alpha \in \mathfrak{p}$, so $\ker \varphi$ is trivial as desired.

Finally, we show that $\operatorname{im} \varphi = \ker \pi$. Note that $\operatorname{im} \varphi$ consists of elements of the form $1 + \alpha u + \mathfrak{p}^n$ so

$$\pi(1 + \alpha u + \mathfrak{p}^n) = 1 + \alpha u + \mathfrak{p}^{n-1}$$

and since $u \in \mathfrak{p}^{n-1}$ this is $1 + \mathfrak{p}^{n-1}$. Thus $\operatorname{im} \varphi \subseteq \ker \pi$. Now let $x + \mathfrak{p}^n \in \ker \pi$, we then have $\pi(x + \mathfrak{p}^n) = 1 + \mathfrak{p}^{n-1}$ so $x = 1 + \gamma$ for some $\gamma \in \mathfrak{p}^{n-1}$. From Lemma 2.16 we know $\gamma = au + bv$ for some $v \in \mathfrak{p}^n$. Thus $x = 1 + au + bv$ which implies $x = 1 + au \bmod \mathfrak{p}^{n-1}$. Hence $x \in \operatorname{im} \varphi$ as desired.

Thus (2.5) is exact.

For the split exactness, we note that when $n = 2$, the orders of $\mathfrak{O}_K/\mathfrak{p}$ and $(\mathfrak{O}_K/\mathfrak{p}^{n-1})^\times = (\mathfrak{O}_K/\mathfrak{p})^\times$ are relatively prime, since they differ by 1. The sequence is then split exact by [13, Theorem 6.6.9] thus completing the proof. □

2.5 Structure of $\mathfrak{O}_K/4\mathfrak{O}_K$

From Theorem 2.12 we know (2.5) is split exact when $n = 2$. In Theorem 2.11, we wish to identify whether the elements are squares mod 4, or in other words, are squares in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. Hence we wish to study the structure of $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$.

Theorem 2.17. *If K is a number field of degree n over $\mathbb{Q}$, in which 2 does not ramify, then $2\mathfrak{O}_K = \prod_{i=1}^r \mathfrak{q}_i$ for some primes of $\mathfrak{q}_i$ of K. Denoting the inertial degree of $\mathfrak{q}_i$ over 2 by f_i, we have*

$$(\mathfrak{O}_K/4\mathfrak{O}_K)^\times \cong (\mathbb{Z}/2\mathbb{Z})^n \times \prod_{i=1}^r \mathbb{Z}/(2^{f_i} - 1)\mathbb{Z}. \tag{2.6}$$

Proof. From (2.5) we have, for any prime $\mathfrak{q}$,

$$(\mathfrak{O}_K/\mathfrak{q}^2)^\times \cong (\mathfrak{O}_K/\mathfrak{q}) \times (\mathfrak{O}_K/q)^\times. \tag{2.7}$$

Since 2 does not ramify, $2\mathfrak{O}_K = \prod_{i=1}^r \mathfrak{q}_i$ where the $\mathfrak{q}_i$'s are distinct. Then from Theorem 2.12 and the Chinese Remainder theorem we obtain

$$\begin{aligned}(\mathfrak{O}_K/4\mathfrak{O}_K)^\times &\cong \prod_{i=1}^r (\mathfrak{O}_K/\mathfrak{q}_i^2)^\times \cong \prod_{i=1}^r \left[(\mathfrak{O}_K/\mathfrak{q}_i) \times (\mathfrak{O}_K/\mathfrak{q}_i)^\times\right] \\ &\cong \prod_{i=1}^r (\mathbb{Z}/2\mathbb{Z})^{f_i} \times \prod_{i=1}^r \mathbb{Z}/(2^{f_i} - 1)\mathbb{Z},\end{aligned}$$

and since $\sum f_i = n$, this reduces to

$$(\mathfrak{O}_K/4\mathfrak{O}_K)^\times \cong (\mathbb{Z}/2\mathbb{Z})^n \times \prod_{i=1}^r \mathbb{Z}/(2^{f_i} - 1)\mathbb{Z}. \tag{2.8}$$

Note that this shows that the 2-Sylow subgroup of $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$, and the squares in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$ form a subgroup isomorphic to $\prod \mathbb{Z}/(2^{f_i}-1)\mathbb{Z}$. □

2.6 Dirichlet's Unit Theorem

From [12, Theorem 38] we have the following:

Theorem 2.18. *Let U be the group of units in $\mathfrak{O}_K$. Let r and s be the signature of K. Then $U \cong \mathbb{Z}^{r+s-1} \times W$ where W is a finite cyclic group consisting of the roots of unity in K.*

Definition 2.19. Let r and s be the signature of K and let $m = r+s-1$. There exist units $u_1, \ldots, u_m$ such that every $x \in K^\times$ can be written in a unique way as

$$x = \zeta u_1^{n_1} \cdots u_m^{n_m}$$

with $n_i \in \mathbb{Z}$ and ζ a root of unity of K. The set $\{u_i\}$ is called a *system of fundamental units* of K. Once a system has been chosen, an element of the system is called a *fundamental unit.*

Chapter 3. Class Field Theory

In order to complete our study, we will need to use narrow class fields. We describe them here.

Definition 3.1. Let R be a Dedekind domain with field of fractions K. A *fractional ideal* of K is a set of the form αI for some $\alpha \in K^\times$ and some nonzero ideal I of R.

Definition 3.2. If $A = \alpha I$ and $B = \beta J$ (where $\alpha, \beta \in K^\times$ and I, J are nonzero ideals of R), we define the product

$$AB = (\alpha\beta)IJ.$$

We have the following well known theorem about fractional ideals.

Theorem 3.3. *With the multiplication defined above, the fractional ideals of K form a multiplicative group.*

When we apply the definition of fractional ideals to a number field K, the corresponding Dedekind domain is $\mathfrak{O}_K$. We will denote the group of fractional ideals of a number field K by $\mathcal{I}_K$.

Theorem 3.4 ([12, Chapter 3, Exercise 31])**.** *In a number field K, every fractional ideal has a unique factorization into powers of prime ideals of $\mathfrak{O}_K$ (with negative powers allowed).*

Definition 3.5. Let $\mathfrak{m}$ be an ideal of $\mathfrak{O}_K$. We define $\mathcal{I}_K(\mathfrak{m})$ to be the subgroup of $\mathcal{I}_K$ consisting of fractional ideals relatively prime to $\mathfrak{m}$ (i.e., $A \in I_K$ if and only if no prime divisor of $\mathfrak{m}$ appears in the factorization of A with either a positive or negative exponent).

Definition 3.6. If K is a number field, $\alpha \in K$ is totally positive if every embedding of K into the reals takes α to a positive number. In this case we write $\alpha \gg 0$.

Definition 3.7. Let $\mathfrak{m}$ be an ideal of $\mathfrak{O}_K$. We define $\mathcal{P}^+_{K,\mathfrak{m}}$ to be the subgroup of $\mathcal{I}_K$ generated by the following set of principal ideals:

$$\{(\alpha) : \alpha \in \mathfrak{O}_K, \alpha \equiv 1 \pmod{\mathfrak{m}}, \text{ and } \alpha \gg 0\}. \tag{3.1}$$

We call $\mathcal{P}_{K,\mathfrak{m}}^{+}$ a congruence subgroup of $\mathcal{I}_I$.

We now state the three main theorems of class field theory. In these theorems, $\mathcal{H}$ represents a subgroup of $\mathcal{I}_K$.

Theorem 3.8 (Existence Theorem, [3, p. 61])**.** *For any $\mathcal{H}$, with $\mathcal{P}_{K,\mathfrak{m}}^{+} \leq \mathcal{H} \leq \mathcal{I}_K(\mathfrak{m})$, there is a class field H/K associated to $\mathcal{H}$.*

Theorem 3.9 (Completeness Theorem, [3, p. 61])**.** *For any abelian extension H/K, there is some $\mathfrak{m}$ and some $\mathcal{H}$ with $\mathcal{P}_{K,\mathfrak{m}}^{+} \leq \mathcal{H} \leq \mathcal{I}_K(\mathfrak{m})$ such that H is the class field over K of $\mathcal{H}$.*

Theorem 3.10 (Isomorphy Theorem, [3, p. 61])**.** *When $\mathcal{P}_{K,\mathfrak{m}}^{+} \leq \mathcal{H} \leq \mathcal{I}_K(\mathfrak{m})$, and H is the class field over K of $\mathcal{H}$, we have*

$$\mathcal{I}_K(\mathfrak{m})/\mathcal{H} \cong \mathrm{Gal}(H/K)$$

with the isomorphism being induced by the Artin map.

We will apply these theorems to two specific subgroups; we define $\mathcal{P}_K$ to be the group of all principal fractional ideals, and $\mathcal{P}_K^{+}$ to be the group of all principal fractional ideals with a totally positive generator.

We note that $\mathcal{P}_{K,\mathfrak{O}_K}^{+} = \mathcal{P}_K^{+} \subseteq P_K \subseteq \mathcal{I}_K(\mathfrak{O}_K) = I_K$. Hence, the main theorems of class field theory apply to $\mathcal{P}_K^{+}$ and P_K, yielding the following theorems.

Theorem 3.11. *There is an abelian extension H/K such that*

$$\mathcal{I}_K/\mathcal{P}_K \cong \mathrm{Gal}(H/K),$$

with the isomorphism induced by the Artin map that takes each prime ideal of $\mathfrak{O}_K$ to its Frobenius in $\mathrm{Gal}(H/K)$*. This extension H/K is called the Hilbert Class Field of K, and is unramified at all primes of K (including infinite primes).*

Theorem 3.12. *There is an abelian extension H^+/K such that*

$$\mathcal{I}_K/\mathcal{P}_K^+ \cong \mathrm{Gal}(H^+/K),$$

with the isomorphism induced by the Artin map that takes each prime ideal of $\mathfrak{O}_K$ to its Frobenius in $\mathrm{Gal}(H^+/K)$*. This extension H^+/K is called the Narrow Class Field of K, and is unramified at all finite primes of K (although it may be ramified at the infinite primes of K).*

In this thesis, we will need the following results that follow from Theorem 3.12 above.

Definition 3.13. The narrow class group of K is the group $\mathcal{I}_K/\mathcal{P}_K^+$. The order of the narrow class group is called the narrow class number of K.

Theorem 3.14. *Let K be a number field, and let h be the narrow class number of K.*

(1) If h is even, then there is a quadratic extension of K that is unramified at all finite primes.

(2) For any fractional ideal $\mathfrak{m}$ of K, $\mathfrak{m}^h$ is a principal fractional ideal.

Proof. (1) If h is even then by definition, $|\mathcal{I}_K/\mathcal{P}_K^+| = |\mathrm{Gal}(H^+/K)|$ is even. Let $G = \mathrm{Gal}(H^+/K)$, since G is abelian we know that G has a (normal) subgroup of each order dividing $|G|$. From this we have that G has a subgroup of index 2 which by the fundamental theorem of Galois theory corresponds to a quadratic extension of K. Since H^+ is unramified at all finite primes, it follows that this quadratic extension of K is also unramified at all finite primes.

(2) By Lagrange's theorem we know that since $h = |\mathcal{I}_K/\mathcal{P}_K^+|$, $\mathfrak{m}^h$ will be the identity of $\mathcal{I}_K/\mathcal{P}_K^+$. We then have $\mathfrak{m}^h \in \mathcal{P}_K^+$, by definition of $\mathcal{P}_K^+$, $\mathfrak{m}^h$ is a principal fractional ideal. □

Chapter 4. Group Theory

We are now ready to define the Hyperpentagonal Group.

Theorem 4.1. *There are, up to conjugacy, exactly 2 transitive subgroups G of S_{10} that satisfies the following:*

(i) G has D_5 as a quotient

(ii) G has exactly one subgroup of index 2

(iii) 20 divides $|G|$.

These two subgroups are isomorphic to each other.

Proof. By using Magma [1] we found there are 45 transitive subgroups of S_{10}. Using [8] and [10] we identified each of the groups, using the group names in [6]. For each of these 45 groups, we used Magma to examine the group to determine whether it failed the criteria listed in Theorem 3.1. The results of this examination for each of the 45 groups are contained in Table 4.1 at the end of the section. We now give details on how we eliminated three of the groups.

First, to eliminate Group 18 we use the `NormalSubgroups` command and we obtain the following output in which we have deleted lines indicating the generators of each subgroup.

```
> G := TransitiveGroup(10, 18); NormalSubgroups(G);
Conjugacy classes of subgroups
------------------------------

[1]     Order 1            Length 1
Permutation group acting on a set of cardinality 10
Order = 1
[2]     Order 25           Length 1
```

```
Permutation group acting on a set of cardinality 10
Order = 25 = 5^2
[3]     Order 50          Length 1
Permutation group acting on a set of cardinality 10
Order = 50 = 2 * 5^2
[4]     Order 100         Length 1
Permutation group acting on a set of cardinality 10
Order = 100 = 2^2 * 5^2
[5]     Order 200         Length 1
Permutation group G acting on a set of cardinality 10
Order = 200 = 2^3 * 5^2
```

We see that Group 18 has no normal subgroups of order 20 and so, since the group has order 200, it has no quotient of index 10. This group then cannot have D_5 as a quotient thus failing condition (i).

Second, for Group 28 we have from the `NormalSubgroups` command the following:

```
> G := TransitiveGroup(10, 28); NormalSubgroups(G);
Conjugacy classes of subgroups
------------------------------

[ 1]    Order 1           Length 1
Permutation group acting on a set of cardinality 10
Order = 1
[ 2]    Order 25          Length 1
Permutation group acting on a set of cardinality 10
[ 3]    Order 50          Length 1
Permutation group acting on a set of cardinality 10
Order = 50 = 2 * 5^2
```

```
[ 4]    Order 100          Length 1
Permutation group acting on a set of cardinality 10
Order = 100 = 2^2 * 5^2
[ 5]    Order 100          Length 1
Permutation group acting on a set of cardinality 10
Order = 100 = 2^2 * 5^2
[ 6]    Order 100          Length 1
Permutation group acting on a set of cardinality 10
Order = 100 = 2^2 * 5^2
[ 7]    Order 200          Length 1
Permutation group acting on a set of cardinality 10
Order = 200 = 2^3 * 5^2
[ 8]    Order 200          Length 1
Permutation group acting on a set of cardinality 10
Order = 200 = 2^3 * 5^2
[ 9]    Order 200          Length 1
Permutation group acting on a set of cardinality 10
Order = 200 = 2^3 * 5^2
[10]    Order 400          Length 1
Permutation group acting on a set of cardinality 10
Order = 400 = 2^4 * 5^2
```

Hence we see that Group 28 has two normal subgroups of order 200 (index 2) so it fails condition (ii).

Third, Group 2, isomorphic to D_5, fails condition (iii) since its order is not divisible by 20.

Similar computations work for all but Groups 15 and 16 of the 45 groups. Using the `IdentifyGroup` command in Magma, we find that these two groups are isomorphic (hence,

they have the same name in the table). They are not conjugate in S_{10}, which is why they are listed twice. Note that the copy labeled Group 15 is contained in A_{10}, while the copy labeled Group 16 is not.

Table 4.1: Transitive subgroups of S_{10} and their failed conditions.

Group Number	Group	Order	Failed Conditions
1	C_{10}	10	(i), (ii), (iii)
2	D_5	10	(iii)
3	D_{10}	20	(ii)
4	F_5	20	(i)
5	$C_2 \times F_5$	40	(ii)
6	$C_5 \times D_5$	50	(iii)
7	A_5	60	(i)
8	$C_2^4 \rtimes C_5$	80	(i)
9	D_5^2	100	(ii)
10	$C_5^2 \rtimes C_4$	100	(i)
11	$C_2 \times A_5$	120	(i)
12	S_5	120	(i)
13	S_5	120	(i)
14	$[2^5]5$	160	(i)
15	$[2^4]D_5$	160	
16	$(1/2)[2^5]D_5$	160	
17	$[5^2:4]2$	200	(ii)
18	$[5^2:4]2_2$	200	(i)
19	$[5^2:4_2]2$	200	(ii)
20	$[5^2:4_2]2_2$	200	(ii)
21	$[D(5)^2]2$	200	(ii)

22	$C_2 \times S_5$	240	(ii)
23	$[2^5]D(5)$	320	(ii)
24	$[2^4]F(5)$	320	(i)
25	$(1/2)[2^5]F(5)$	320	(i)
26	A_6	360	(i)
27	$[1/2.F(5)^2]2$	400	(ii)
28	$1/2[F(5)^2]2$	400	(ii)
29	$[2^5]F(5)$	640	(ii)
30	$L(10) : 2$	720	(i)
31	$M(10)$	720	(i)
32	$S_6(10)$	720	(i)
33	$[F(5)^2]2$	800	(ii)
34	$[2^4]A(5)$	960	(i)
35	$L(10).2^2$	1440	(ii)
36	$[2^5]A(5)$	1920	(i)
37	$[2^4]S(5)$	1920	(i)
38	$(1/2)[2^5]S(5)$	1920	(i)
39	$[2^5]S(5)$	3840	(ii)
40	$[A(5)^2]2$	7200	(i)
41	$[(1/2).S(5)^2]2$	14400	(ii)
42	$(1/2)[S(5)^2]2$	14400	(i)
43	$[S(5)^2]2$	28800	(ii)
44	A_{10}	1814400	(i)
45	S_{10}	3628800	(i)

□

Definition 4.2. We define *a hyperpentagonal group* to be the unique (up to isomorphism) group satisfying the conditions of Theorem 4.1.

Chapter 5. Totally Real D_5-Extensions

ramified at one prime p

Let L be a totally real D_5 extension of $\mathbb{Q}$ ramified at one odd prime p and let K be its quintic subfield. Let $p^* = (-1/p) = (-1)^{p-1/2}\, p$. Since L is totally real it has a real quadratic subfield $\mathbb{Q}\big(\sqrt{p^*}\big)$. This is seen in Figure 5.1. It then follows that $p = 1 \bmod 4$. Additionally, from the database in [11] we find there are no D_5 extensions ramified only at 5. We can then further assume that $p > 5$. We now look to see the possible factorizations of p in K.

5.1 Factorization of p in K

From [12, Theorem 24, 34] we know there are no unramified extensions of $\mathbb{Q}$. Since p is the only prime that ramifies in L, it follows that p also ramifies in K. Using Theorem 2.3 we can determine the possible factorizations of p in $\mathfrak{O}_K$.

Theorem 5.1. *Let L, K, and p be as above. Then p factors as $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$ in K.*

We have the following lemmas:

Lemma 5.2. *Let L, K, and p be as above. Then $p\mathfrak{O}_L \neq \mathfrak{q}^{10}$ for any prime $\mathfrak{q}$ of $\mathfrak{O}_L$.*

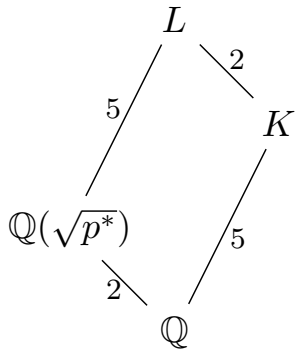

Figure 5.1: A subfield diagram for considering the quadratic extension.

Proof. Suppose for a contradiction that p does factor this way. We then know from Theorem 2.9 that $V_0(\mathfrak{u})/V_1(\mathfrak{u})$ is cyclic. Note that since $p \neq 2, 5$ and from Theorem 2.10, $V_1(\mathfrak{q})$ is the Sylow p-subgroup of $V_0(\mathfrak{q})$. Since $V_0(\mathfrak{q}) \subseteq \mathrm{Gal}(L/\mathbb{Q}) = D_5$ and $p \neq 2, 5$ it follows that $V_1(\mathfrak{q})$ must be trivial. We then have $V_0(\mathfrak{q})$ is a cyclic subgroup of order 10 and thus must be D_5. However D_5 is not cyclic which is a contradiction. Hence p does not factor as $\mathfrak{q}^{10}$ in L. □

Lemma 5.3. *Let L, K, and p be as above. Let $\mathfrak{q}$ be a prime of $\mathfrak{O}_L$ above p. Then 2 divides $e(\mathfrak{q}|p)$.*

Proof. Note that L has a quadratic subfield $\mathbb{Q}(\sqrt{p})$ where we have $(p) = (\sqrt{p})^2$. Hence, there is only one prime $\mathfrak{r}$ of $\mathbb{Q}(\sqrt{p})$ lying over p with $e(\mathfrak{r}|p) = 2$. Thus $\mathfrak{q}$ must lie over $\mathfrak{r}$. Using Theorem 2.2 we then know

$$e(\mathfrak{q}|p) = e(\mathfrak{q}|\mathfrak{r})e(\mathfrak{r}|p) = e(\mathfrak{q}|\mathfrak{r}) \cdot 2.$$

We then see that 2 divides $e(\mathfrak{q}|p)$. □

Theorem 5.4. *Let L, K, and p be as above. Let $\mathfrak{q}$ be a prime of $\mathfrak{O}_L$ lying over p. We have $f(\mathfrak{q}|p) = 1$.*

Proof. Let r be the number of primes in the prime factorization of $p\mathfrak{O}_L$, let $e = e(\mathfrak{q}|p)$, and let $f = f(\mathfrak{q}|p)$. From Corollary 2.5 we know $ref = 10$. Together with Lemma 5.3 we have that e is a multiple of 2 that also divides 10. By Lemma 5.2 we know that $e \neq 10$ so e must be 2. It then follows that $rf = 5$, we show $f \neq 5$ which then shows f must be 1. Suppose for a contradiction that $f = 5$, it then follows that $p\mathfrak{O}_L = \mathfrak{q}^2$. From this we have $p\mathfrak{O}_K = p\mathfrak{O}_L \cap \mathfrak{O}_K = \mathfrak{p}$ for some prime $\mathfrak{p}$ of $\mathfrak{O}_K$ with $f(\mathfrak{p}|p) = 5$. This is impossible since p must ramify in K. Hence $f = 1$ thus completing the proof. □

From this we obtain the following immediate corollaries.

Corollary 5.5. *Let L, K, and p be as above. We have the prime factorization of $p\mathfrak{O}_L$ as $\prod_{i=1}^{5} \mathfrak{q}_i^2$.*

Proof. In the proof of Theorem 5.4 we found $e = 2$, together with $f = 1$ we obtain this factorization. □

Corollary 5.6. *Let L, K, and p be as above. Let $\mathfrak{p}$ be a prime of $\mathfrak{O}_K$ over p. We then have $f(\mathfrak{p}|p) = 1$.*

Proof. Let $\mathfrak{q}$ be a prime of $\mathfrak{O}_L$ lying over $\mathfrak{p}$. We know $f(\mathfrak{q}|p) = 1$ and from Theorem 2.2 that $f(\mathfrak{p}|p)$ must divide 1. It then follows that $f(\mathfrak{p}|p) = 1$. □

Lemma 5.7. *Let L, K, and p be as above. We have $p\mathfrak{O}_K \neq \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4^2$ for $\mathfrak{p}_i$ primes of $\mathfrak{O}_K$.*

Proof. Suppose for a contradiction that this is the case. From [9, page 611], since D_5 is a subgroup of A_5 we need $\text{disc}(K)$ to be a square. Because only one prime ramifies in K we know that $\text{disc}(K)$ is p^k for some even k. Let $e_i = e(\mathfrak{p}_i|p)$, and $f_i = f(\mathfrak{p}_i|p)$. From Lemma 2.7, we know that $k = \sum f_i(e_i - 1)$. We then find $k = 1$, a contradiction. Thus $p\mathfrak{O}_K \neq \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4^2$. □

We now proceed to the proof of Theorem 5.1.

Proof. Let $\mathfrak{p}$ be a ramified prime of K lying over p and let $\mathfrak{q}$ be a prime of $\mathfrak{O}_L$ lying over $\mathfrak{p}$. We have from Corollary 5.5 that $e(\mathfrak{q}|p) = 2$. Together with Theorem 2.2 we know $e(\mathfrak{p}|p)$ divides 2. Since $\mathfrak{p}$ is a prime over p that ramifies we know $e(\mathfrak{p}|p) = 2$. It then follows that the only possible ramification index for a prime that ramifies is 2.

Since the inertial degree of any prime of $\mathfrak{O}_K$ over p must be 1 there are only two options for the factorization of p. If one prime in the factorization has ramification index 2 then this is the case $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4^2$ which is impossible by Lemma 5.7. If there are two primes in the factorization that have ramification index 2 then this is the case $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$. By Theorem 2.3, there cannot be more than 2 primes with ramification index 2. Thus the only possible factorization of p in $\mathfrak{O}_K$ is then $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$. □

Chapter 6. Constructing the Quadratic Extension

Let L be a totally real D_5 extension of $\mathbb{Q}$ ramified at one odd prime p and let K be its quintic subfield as stated in the previous chapter. Since K is totally real we have from Theorem 2.18 that

$$\mathfrak{O}_K^\times = \langle -1, u_1, u_2, u_3, u_4 \rangle$$

where the u_i's are a system of fundamental units. As described in Section 2.5,

$$(\mathfrak{O}_K/4\mathfrak{O}_K)^\times \cong \prod \mathbb{Z}/(2^{f_i}-1)\mathbb{Z} \times \prod (\mathbb{Z}/2\mathbb{Z})^5.$$

Let G_1 be the subgroup of $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$ mapping to $\prod \mathbb{Z}/(2^{f_i}-1)\mathbb{Z}$. Note that G_1 consists of the squares in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. We will prove the following theorem:

Theorem 6.1. *Let p factor in K as $p\mathfrak{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$. Then there exists a $\pi \in \mathfrak{O}_K$ where $K(\sqrt{\pi})/K$ is unramified except possibly at $\mathfrak{p}_3$.*

We first prove the following lemma:

Lemma 6.2. *Let K be a totally real quintic field whose Galois closure has Galois group D_5, and let u_1, u_2, u_3, u_4 be a system of fundamental units of K. Suppose K has odd narrow class number. Let*

$$S_1 = \{\alpha \in \mathfrak{O}_K \mid (\alpha, 2) = \mathfrak{O}_K\},$$

and let $H = (\mathfrak{O}_K/4\mathfrak{O}_K)^\times/G_1$. Let S be the set of all possible products of the form $\prod \pm u_i^{\epsilon_i}$ where ϵ_i is 0 or 1. Define the map $\varphi\colon S_1 \to H$ by $\alpha \mapsto (\alpha + 4\mathfrak{O}_K) \bmod G_1$. Then $\varphi|_S$ is injective.

Proof. Note that for $\alpha \in S_1, \alpha + 4\mathfrak{O}_K \in (\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. Also, $S \subseteq S_1$ so $\varphi|_S$ is defined. Let $s_1, s_2 \in S$ so that $\varphi(s_1) = \varphi(s_2)$. Since s_1 and s_2 are units of $\mathfrak{O}_K$ we know $s_1/s_2 \in \mathfrak{O}_K$, let $s = s_1/s_2$. We then look at the following two cases, if s is a perfect square of K or not.

Case 1. If s is a square then note that the only squares of S are those of the form $\prod u_i^{\delta_i}$ with each δ_i being even. By construction of s, s is of the form $\prod u_i^{\gamma_i}$ with $\gamma_i \in \{-1, 0, 1\}$. If s is a square then it follows that $\gamma_i = 0$ for each i. It then follows that $s_1 = s_2$ so $\varphi|_S$ is injective thus completing the proof.

Case 2. If s is not a perfect square of K then $K(\sqrt{s})$ will be a nontrivial extension of K. Additionally, s maps to the identity in H and thus maps to a square in $(\mathfrak{O}_K/4\mathfrak{O}_K)^\times$. Let $\mathfrak{q} \neq \mathfrak{p}$ be any prime ideal. Note that since s is a unit that $s \notin \mathfrak{q}$. If $2 \notin \mathfrak{q}$ then from (i) of Theorem 2.11 we know $\mathfrak{q}$ is unramified in $K(\sqrt{s})$. If $2 \in \mathfrak{q}$ then from (ii) of Theorem 2.11 we know that since s is a square modulo 4 that $\mathfrak{q}$ is unramified. We then have $K(\sqrt{s})$ is an unramified extension of K. This is a contradiction since the narrow class number of K is odd; there cannot be an unramified quadratic extension of K. It then follows that $\varphi|_S$ is injective. □

We now proceed to the proof of Theorem 6.1.

Proof. We have two cases, if K has odd or even class number.

Case 1. If K has an even narrow class number then by Theorem 3.14 there is an unramified quadratic extension of K. This extension will have the form $K(\sqrt{\pi})$ for some $\pi \in \mathfrak{O}_K$.

Case 2. If K has an odd narrow class number then let h be the narrow class number. Recall that $p\mathfrak{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$, and we know $\mathfrak{p}_3^h$ is principal by the definition of h, say $(\pi_0) = \mathfrak{p}_3^h$. We note that from Equation (2.8) that $|H| = 2^5$ since $[K : \mathbb{Q}] = 5$. Additionally, a simple counting argument shows $|S| = 2^5 = |H|$. Thus since $\varphi|_S$ is injective we have $\varphi|_S$ is surjective as well. Letting $\varphi(\pi_0) = y$, there must exist $u \in S$ so that $\varphi(u) = y$ as well. Then $\varphi(u^{-1}\pi_0)$ equals the identity in H and is thus a square mod 4 as desired. Setting $\pi = u^{-1}\pi_0$, we now consider the extension $K(\sqrt{\pi})$. Let $\mathfrak{q} \neq \mathfrak{p}_3$ be any prime ideal. Note that the only prime ideal of K containing π is $\mathfrak{p}_3$ so $\pi \notin \mathfrak{q}$. If $2 \in \mathfrak{q}$ then since π is a square mod 4 we know $\mathfrak{q}$ will be unramified in $K(\sqrt{\pi})$ by (i) of Theorem 2.11. If $2 \notin \mathfrak{q}$ then we have from (i) of Theorem 2.11 that $\mathfrak{q}$ is unramified. Thus $K(\sqrt{\pi})$ is unramified except possibly at $\mathfrak{p}$ as desired. □

In order to distinguish the fields L and F pictured in Figure 1.2 we require the following Theorem.

Theorem 6.3. *The field $F = K(\sqrt{\pi})$, where π is the element discussed above, is not Galois over $\mathbb{Q}$.*

Proof. We know that p factors in K as $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$ and by construction of F, p ramifies in F as well. Suppose without loss of generality that $\pi \in \mathfrak{p}_3$ and hence $\pi \notin \mathfrak{p}_1, \mathfrak{p}_2$. We then have $\mathfrak{p}_3$ ramifies in F but $\mathfrak{p}_1$ and $\mathfrak{p}_2$ do not. Let $\mathfrak{u}$ be a prime of F lying above $\mathfrak{p}_3$ that ramifies. We then know $e(\mathfrak{u}|p) = 4$. Let $\mathfrak{q}$ be any other prime lying above p in L. Since π was chosen so that no other prime would ramify, we have that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ do not ramify in L. It then follows that $e(\mathfrak{q}|p)$ is either 1 or 2 and not 4. By Theorem 2.5 we know that F is not Galois over K. □

This then gives the following corollary:

Corollary 6.4. *The fields L and F are distinct.*

Proof. Since L/K is Galois but F/K is not it follows that $L \neq F$. □

Letting M be the Galois closure of F, in the next chapter we determine $\mathrm{Gal}(M/\mathbb{Q})$.

Chapter 7. The Galois group of the Galois Closure $M/\mathbb{Q}$ of $F/\mathbb{Q}$

In order to determine $\mathrm{Gal}(M/\mathbb{Q})$ we require a few lemmas.

Lemma 7.1. *The field M contains L.*

Proof. By definition, M is the Galois closure of F, hence the smallest Galois extension of $\mathbb{Q}$ containing F. Note that F contains K and L is the Galois closure of K. By defintion, L is the smallest Galois extension of $\mathbb{Q}$ containing K. L must then be contained in any Galois extension of $\mathbb{Q}$ containing K. Since M is a Galois extension of $\mathbb{Q}$ containing K we then know that M contains L. □

Lemma 7.2. *The degree $[M : \mathbb{Q}]$ is divisible by 20.*

Proof. Let $F = K(\sqrt{\pi})$ be the quadratic extension described above. We then have the composite field $FL \subseteq M$ and by Corollary 6.4, $[FL : \mathbb{Q}] = 20$. Thus 20 divides $[M : \mathbb{Q}]$. □

Lemma 7.3. *The Galois group $\mathrm{Gal}(M/\mathbb{Q})$ has D_5 as a quotient.*

Proof. Since $M/\mathbb{Q}$ contains the D_5 extension L of $\mathbb{Q}$ it follows from the Fundamental Theorem of Galois Theory that $\mathrm{Gal}(M/\mathbb{Q})$ must have D_5 as a quotient. □

Lemma 7.4. *The extension $M/\mathbb{Q}$ has exactly one quadratic subfield.*

Proof. Note that since $M \supset L$ and L has a quadratic subfield we know M does as well. Suppose for a contradiction there are two distinct quadratic subfields namely $\mathbb{Q}(\sqrt{m})$, where m is a square-free integer, and $\mathbb{Q}(\sqrt{p})$. It then follows that a prime divisor of m, other than p, will ramify in $\mathbb{Q}(\sqrt{m})$. Since it is assumed that these extensions are distinct we then have more than one prime ramifying in L contradicting the definition of L. □

Theorem 7.5. *The Galois group $\mathrm{Gal}(M/\mathbb{Q})$ is the hyperpentagonal group.*

Proof. The Galois group $G = \mathrm{Gal}(M/\mathbb{Q})$ must be a transitive subgroup of S_{10}. From Lemma 7.2 and the Fundamental Theorem of Galois Theory we know that $|G| = [M : \mathbb{Q}]$ is divisible by 20. Additionally, since M has exactly one quadratic subfield it follows that G must have exactly one subgroup of index 2. By Lemma 7.3 we know G has D_5 as a quotient. From Theorem 4.1 we know there is only one transitive subgroup (up to isomorphism) of S_{10} that satisfies these properties. Hence G is the hyperpentagonal group. □

We can now provide a proof of Theorem 1.2:

Theorem 1.2. *Given any totally real quintic field $K/\mathbb{Q}$ that is ramified at only one prime p and is contained in a D_5 extension of $\mathbb{Q}$, there is an extension $M/\mathbb{Q}$ that contains K, is ramified only at p, and has $\mathrm{Gal}(M/\mathbb{Q})$ isomorphic to a hyperpentagonal group.*

Proof. By the Fundamental Theorem of Galois Theory, L contains a totally real quintic field $K/\mathbb{Q}$ with Galois closure L. By Theorem 5.1, $p\mathfrak{O}_K$ factors as $\mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$. By Theorem 6.1, there is some $\pi \in \mathfrak{O}_K$ such that $K(\sqrt{\pi})/K$ is ramified only at $\mathfrak{p}_3$. Corollary 6.4 shows that $K(\sqrt{\pi}) \neq L$.

If we let M be the Galois closure of $K(\sqrt{\pi})/\mathbb{Q}$, then Lemma 7.1 tells us that $L \subseteq M$. By [12, Theorem 31] we know that M is ramified at the same primes L is. Additionally, Theorem 7.5 tells us that $\mathrm{Gal}(M/\mathbb{Q})$ is the hyperpentagonal group. Hence, M contains K, is ramified only at p, and has $\mathrm{Gal}(M/\mathbb{Q})$ isomorphic to a hyperpentagonal group. □

Chapter 8. Computational Verification

Using Pari we are able to computationally verify the result of Theorem 1.2 for specific D_5-extensions. From the database associated with [11], we were able to find polynomials that define a totally real D_5 extension with only one ramified prime. Let f be one of these polynomials. The following code computes M and shows that its Galois group is the hyperpentagonal group.

```
{comp(f) =
    \\ initialize number field K
    K = bnfinit(f);

    \\ get the discriminant so we can see what prime ramifies
    d = nfdisc(f);
    p = factor(d)[1,1];

    \\ factor p in K
    ideal_fac = idealprimedec(K, p);

    \\ find which ideal is ramified over p and call it P
    i = 3;
    while(ideal_fac[i][3] != 2, i = i - 1);
    P = ideal_fac[i];

    \\ Get the narrow class number h so that P^h is principal
    h = bnfnarrow(K)[1];

    \\get a root r to describe the fundamental units and pi in terms of r
```

```
r = polroots(f)[1];

\\check to see if the narrow class number is even. If it is then set pi to 1.
if(h % 2 == 0,
    pi = 1;
    \\skips over 1 in the for loop
    start = 2; ,

    \\otherwise in the if then

    \\Make P principal
    Q = idealpow(K, P, h);

    \\ Get the generator for the principal ideal
    gen = bnfisprincipal(K, Q)[2];

    \\ Find what the integral basis to express the generator as a polynomial
    in a root of f
    int_basis = K.zk;
    g = int_basis * gen;

    \\ Use the root of f defined above to describe the generator
    pi = subst(g, x, r);

    \\ Get a polynomial that describes the generator
    poly0 = algdep(pi, 5);
```

```
    \\ Use the polynomial to get the defining polynomial for sqrt(pi)
    poly1 = subst(poly0, x, x^2);

    \\ start checking K(sqrt(u * pi)) at 1
    start = 1;
);
\\compute a system of fundamental units
\\get the fundamental units as polymods
fund_unit = K.fu;

\\make a list of units
u = List([-1]);
for(i = 1, 4,
    \\lift the polymods, plug in r, and obtain the system of fundamental units
    listput(u, subst(lift(fund_unit[i]), x, r))
);

\\computing pi si that K(sqrt(pi)) is unramified except possibly at p_3
\\Create a list to fill with the possibilities for exponents
binary_pos = List();
for(i=0, 31, listput(binary_pos, binary(32 + i)));

\\Check each combination and see which one gets a u so that K(sqrt(u * pi))
is not ramified at 2 or equivalently has odd discriminant
for(i = start, 32,
    pot_exp = binary_pos[i];
    pot_u = prod(k = 2, 6, u[k - 1]^pot_exp[k]);
```

```
        check = nfdisc(subst(algdep(pot_u * pi, 5), x, x^2));
        if(check % 2 == 1,
            good_u = pot_u;
            break;
        );
    );
    new_pi = good_u * pi;
    new_f0 = algdep(new_pi, 5);
    new_f1 = subst(new_f0, x, x^2);
    \\print statement to output the rows of the table
    \\the discriminant, the defining polynomial of K(sqrt(pi)), and the number
    of the Galois group.
    print("$ " p "^" factor(nfdisc(new_f1))[1,2] " $ & ",
        " $ " new_f1 " $ & ",
        polgalois(new_f1)[3], " \\cr \\hline");
}
```

From the database in [11], we obtained defining polynomials for every totally real extension with Galois group D_5 ramified only at one prime p with $p < 30000$. Using our code, we determined a defining polynomial for $K(\sqrt{\pi})$, and verified that its Galois group is the hyperpentagonal group. In the table that follows, for each prime p for which there is a totally real D_5 extension we give a defining polynomial for $K(\sqrt{\pi})$ for the Galois group of the Galois closure. We describe the group by the number in the list of transitive subgroups of S_{10}. In all cases, this number is 15 or 16, the two subgroups of S_{10} that are isomorphic to the hyperpentagonal group.

Disc	Defining Polynomial for $K(\sqrt{\pi})$	Group
401^5	$x^{10} - 38x^8 + 233x^6 + 20x^4 - 1604x^2 - 401$	16
1093^5	$x^{10} + 45x^8 - 2999x^6 - 47613x^4 + 46999x^2 - 1093$	16
1429^5	$x^{10} - 42x^8 + 473x^6 - 541x^4 - 8574x^2 - 1429$	16
2081^5	$x^{10} - 1469x^8 + 30116x^6 + 93785x^4 + 14567x^2 - 2081$	16
2153^5	$x^{10} - 850x^8 + 18447x^6 - 88491x^4 + 40907x^2 - 2153$	16
3121^5	$x^{10} + 78x^8 - 445x^6 - 23063x^4 + 146687x^2 - 3121$	16
3181^5	$x^{10} - 378x^8 + 6617x^6 + 39115x^4 + 31810x^2 - 3181$	16
3253^4	$x^{10} - 2x^8 - 75x^6 - 153x^4 - 26x^2 - 1$	15
4357^5	$x^{10} - 127x^8 - 1831x^6 + 83x^4 + 30499x^2 - 4357$	16
4441^5	$x^{10} - 91x^8 + 2099x^6 - 1696x^4 - 48851x^2 - 4441$	16
4889^4	$x^{10} - 7x^8 + 3x^6 + 57x^4 - 86x^2 - 1$	15
6113^4	$x^{10} + 733x^8 - 4413x^6 - 4255x^4 - 930x^2 - 1$	15
6481^5	$x^{10} - 265x^8 + 7948x^6 - 31351x^4 - 421265x^2 - 6481$	16
6949^5	$x^{10} - 5818x^8 - 321183x^6 + 1090643x^4 - 208470x^2 - 6949$	16
7229^5	$x^{10} + 1690x^8 + 13x^6 - 27481x^4 + 43374x^2 - 7229$	16
7817^5	$x^{10} - 26671x^8 + 339419x^6 - 940564x^4 - 242327x^2 - 7817$	16
8501^5	$x^{10} - 109227x^8 + 30798665x^6 - 57418061x^4 - 2558801x^2 - 8501$	16
8689^5	$x^{10} - 404x^8 + 16780x^6 - 89641x^4 - 295426x^2 - 8689$	16
9181^5	$x^{10} + 66x^8 - 31611x^6 + 1342815x^4 - 2515594x^2 - 9181$	16
9829^5	$x^{10} + 3370x^8 - 2163155x^6 + 3923567x^4 + 19559710x^2 - 9829$	16
10613^5	$x^{10} - 8095x^8 - 4722855x^6 - 465443805x^4 + 22998371x^2 - 10613$	16
10909^5	$x^{10} - 78x^8 + 129x^6 + 25735x^4 + 109090x^2 - 10909$	16
11273^4	$x^{10} + 180x^8 - 3976x^6 + 15143x^4 + 538x^2 - 1$	15
11321^4	$x^{10} + 670x^8 + 29819x^6 - 147083x^4 + 1615x^2 - 1$	15
12041^5	$x^{10} + 317x^8 + 16623x^6 - 1419375x^4 + 2721266x^2 - 12041$	16

12101^4	$x^{10} - 58x^8 + 805x^6 + 847x^4 + 198x^2 - 1$	15
12301^5	$x^{10} - 1067x^8 + 96909x^6 + 75146703x^4 - 565169445x^2 - 12301$	16
13229^5	$x^{10} + 18622x^8 - 5043067x^6 - 62808517x^4 + 2196014x^2 - 13229$	16
13693^5	$x^{10} - 105858x^8 + 1068353x^6 - 2571565x^4 + 1561002x^2 - 13693$	16
13841^5	$x^{10} + 4599x^8 - 13942952x^6 + 8144053x^4 + 9010491x^2 - 13841$	16
14281^5	$x^{10} - 5251x^8 + 6888775x^6 - 1972744x^4 - 1185323x^2 - 14281$	16
15121^5	$x^{10} + 7323x^8 + 3988538x^6 - 13412698x^4 + 1043349x^2 - 15121$	16
15473^4	$x^{10} + 26x^8 - 1249x^6 + 1945x^4 + 2003x^2 - 1$	15
15889^5	$x^{10} - 97195x^8 - 64253x^6 + 1260989x^4 + 603782x^2 - 15889$	16
16001^5	$x^{10} - 37515x^8 + 104293519x^6 + 38346144x^4 + 208013x^2 - 16001$	16
16741^5	$x^{10} + 29882x^8 - 215100151x^6 + 18590310711x^4 + 76640298x^2 - 16741$	16
17033^4	$x^{10} - 174x^8 - 1901x^6 - 5079x^4 - 205x^2 - 1$	15
17737^5	$x^{10} - 38413x^8 + 403144x^6 - 1089783x^4 + 337003x^2 - 17737$	16
18253^5	$x^{10} + 92286x^8 + 218042941x^6 - 337028133x^4 + 111233782x^2 - 18253$	16
18329^5	$x^{10} - 2882x^8 + 1982519x^6 - 16399675x^4 + 1447991x^2 - 18329$	16
18353^5	$x^{10} - 18205478x^8 - 160452403x^6 + 315576392x^4 - 1468240x^2 - 18353$	16
18433^4	$x^{10} + 160x^8 - 1048x^6 + 971x^4 + 642x^2 - 1$	15
18773^5	$x^{10} + 3217x^8 - 763319x^6 + 15408947x^4 + 1633251x^2 - 18773$	16
19477^5	$x^{10} + 257913x^8 - 224782215x^6 + 190134595x^4 + 32390251x^2 - 19477$	16
20089^5	$x^{10} - 22x^8 - 10695x^6 + 186432x^4 - 80356x^2 - 20089$	16
20389^5	$x^{10} - 267x^8 - 40471x^6 - 767933x^4 + 713615x^2 - 20389$	16
21317^5	$x^{10} + 635905x^8 - 656677027x^6 - 236606665x^4 + 157809751x^2 - 21317$	16
22621^4	$x^{10} - 44651x^8 - 82971x^6 - 18845x^4 + 431x^2 - 1$	15
23173^5	$x^{10} - 1542x^8 + 23537x^6 + 5743511x^4 - 135840126x^2 - 23173$	16
23677^5	$x^{10} + 1169x^8 - 324631x^6 + 16713771x^4 + 923403x^2 - 23677$	16
23801^5	$x^{10} - 1096x^8 - 1130980x^6 + 30339327x^4 + 57550818x^2 - 23801$	16

24593^5	$x^{10} - 135x^8 + 4067x^6 + 33028x^4 - 172151x^2 - 24593$	16
25037^4	$x^{10} + 138x^8 - 1315x^6 - 397x^4 + 3622x^2 - 1$	15
25097^5	$x^{10} - 1588074x^8 - 5581080589x^6 + 10097273893x^4 + 676389247x^2 - 25097$	16
25153^5	$x^{10} - 1238133x^8 + 731842312x^6 - 9378819983x^4 - 457507917x^2 - 25153$	16
25601^5	$x^{10} + 12778976x^8 - 1919474356x^6 - 2652695485x^4 + 54120514x^2 - 25601$	16
25621^5	$x^{10} - 7895x^8 + 8077577x^6 - 6230061x^4 + 1204187x^2 - 25621$	16
25741^4	$x^{10} - 5138x^8 + 5237x^6 + 6519x^4 + 38x^2 - 1$	15
26309^4	$x^{10} + 69x^8 - 6911x^6 + 81759x^4 + 1259x^2 - 1$	15
27689^4	$x^{10} + 121x^8 - 157x^6 - 5307x^4 + 150x^2 - 1$	15

Note that some groups are labeled 15 and others are labeled 16. When the discriminant is a perfect square the Galois group must be a subgroup of A_{10}. Although groups 15 and 16 are isomorphic, only 15 is a subgroup of A_{10}.

Bibliography

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[2] Kevin Childers and Darrin Doud, *Octahedral extensions with a given cubic subfield*, J. Number Theory **167** (2016), 141–146. MR 3504039

[3] Nancy Childress, *Class field theory*, Universitext, Springer, New York, 2009. MR 2462595

[4] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206

[5] Keith Conrad, *The different ideal*, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf`.

[6] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, LMS J. Comput. Math. **1** (1998), 1–8. MR 1635715

[7] David A. Cox, *Primes of the form x^2+ny^2*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989, Fermat, class field theory and complex multiplication. MR 1028322

[8] Tim Dokchitser, *Transitive groups of degree up to 15*, `https://people.maths.bris.ac.uk/~matyd/GroupNames/T15.html`.

[9] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR 2286236

[10] John Jones, *Transitive group data*, `https://hobbes.la.asu.edu/Groups/`.

[11] John W. Jones and David P. Roberts, *A database of number fields*, LMS Journal of Computation and Mathematics **17** (2014), no. 1, 595–618.

[12] Daniel A. Marcus, *Number fields*, Universitext, Springer, Cham, 2018, Second edition of [MR0457396], With a foreword by Barry Mazur. MR 3822326

[13] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324

[14] Siman Wong, *Arithmetic of octahedral sextics*, J. Number Theory **145** (2014), 245–272. MR 3253303