UNIVERSITY OF COPENHAGEN

DEPARTMENT OF MATHEMATICAL SCIENCES

Bachelor's Project

Marie Stuhr Kaltoft

Realising Frobenius groups as Galois groups

Date: June 2022

Advisor: Ian Kiming

Abstract

This project will prove some results concerning realisation of Frobenius groups, F_{pl}, as Galois groups. The first half of the project focuses on realising the general case. At the end of this first half, a class of examples for the case $l = \frac{p-1}{2}$ is constructed. In the proof of the general case, we have to make a certain assumption. Hence, we will, in the second half, consider a special case, where we can confirm that the assumption holds. This special case is for $l = 2$, i.e., $F_{2p} = D_p$. The main theorem of this second half is that given a quadratic extension, D_p can be realised in infinitely many different ways. To do this we will need to introduce notions from class field theory. Amongst other things, we will need a formula for the class number, which will be introduced and proven.

Contents

1 Introduction

Given a polynomial over $\mathbb{Q}$, what is its Galois group? We know that a method to answer this question exists. What if we were instead given a group and had to find a polynomial for which it is a Galois group? This is a question that we cannot answer to the full extent. One might wonder why this is. If we imagine the process of finding the Galois group of a polynomial as a function from the set of polynomials to the set of finite groups, then we do not know if this function is surjective (and it is certainly not injective), so there is no easy way of reversing this process. However, in some cases we can actually answer this question of inverse Galois theory.

In this project, we will explore how to realise so-called Frobenius groups (denoted F_{pl}, where p is a prime and $l \mid p-1$) as Galois groups. To do this we will first define semi-direct products and consider the group denoted by $\mathrm{AGL}(1, \mathbb{F}_p)$ called the one-dimensional affine linear group modulo p, which we will show can be considered as a semi-direct product. This will both motivate and help us to begin our work with Frobenius groups.

We will then begin the process of realising general Frobenius groups. First, we assume that a solution to our problem exists, and we analyse the situation. Next, we will use this analysis to show that the field is, in fact, a solution to the problem of realising F_{pl}. Lastly, we will construct a class of examples for a specific l, which will round off this part of the project.

In the construction of the field in the first part, we will need to make a certain assumption. Because of this, we will, in the second half of the project, consider the special case $l = 2$, where $F_{2p} = D_p$. The goal of this part of the project will be to prove that given a quadratic extension, there exist infinitely many different ways to realise the dihedral group $D_p = F_{2p}$ of order $2p$, through an extension of the given quadratic extension. Before we are able to prove this we will need a bit of class field theory. So we will first give some definitions and state a few important results, however, due to the scope of this project we will not prove the majority of these. The last piece needed before we begin the final proof of the project will be a formula for the class number. This theorem (and a lemma preceding it) will be the only result proven in the section on class field theory.

Throughout the project, unless stated otherwise, we will make use of the following notation. Let p be a prime and ζ_p the pth root of unity. In general, we will use the letters L and K to denote number fields, and $N_{L/K}$ will denote the norm of an element (or ideal) in the extension L/K. Recall that the norm is multiplicative.

In this project, we assume that the reader is familiar with group theory, ring theory, introductory Galois theory and basic algebraic number theory. Very basic knowledge of exact sequences of groups is also presumed. The introduction of semi-direct products is based on the theory from [Dummit and Foote, 2003, pp. 175-180]. For the definition of $\mathrm{AGL}(1, \mathbb{F}_p)$ [Cox, 2004] has been used, however, proving that this is isomorphic to a semi-direct product has been produced independently. The definition of Frobenius groups and the first main part of the project, i.e., Section 3, is based on [Kiming, a], which is meant as a supplement to [Jensen et al., 2002, pp. 178-179]. However, through the course of the project, quite a few details (and the example at the very end of Section 3.3) have been added that were not present in these sources. The needed results from class field theory are almost all based on [Cox, 1989]. However, Lemma 4.18, which is left out of the book, has been stated and proven independently. The proof of Theorem 5.1 is based on the one in [Jensen and Yui, 1982], but the authors leave out many details, which will be worked out in this project. Moreover, the paper assumes the formula for the class number, which we, as mentioned, do not.

Acknowledgments

I would like to extend my gratitude to Ian Kiming for his excellent guidance as my advisor, and for introducing me to this wonderful world of algebraic number theory. Thanks to him, I have truly enjoyed the process of writing this project, as well as our weekly meetings. I am also deeply grateful to Rasmus Lemvig and Tim Berland for always being available and taking time to discuss problems with me, big and small. Being able to bounce ideas off of them has made a big difference in the process of writing this project. Lastly, I would like to thank Stig Eilsøe-Madsen for his thorough proofreading, which caught quite a few ambiguities and silly mistakes.

2 Semi-direct products, $\mathrm{AGL}(1,\mathbb{F}_p)$, and Frobenius groups

Before we begin our work in realising Frobenius groups as Galois groups, we must first determine what the Frobenius groups actually look like. We begin by defining the notion of a semi-direct product, and stating some properties of semi-direct products.

Definition 2.1 (Semi-direct product)**.** Let H and K be groups, $\varphi\colon K \to \mathrm{Aut}(H)$ a homomorphism, and $\cdot$ denote the action $K \circlearrowleft_\varphi H$. Set $G = \{\, (h,k) \mid h \in H, k \in K \,\}$, and define multiplication in G as $(h_1,k_1)(h_2,k_2) = (h_1(k_1 \cdot h_2), k_1k_2)$. Then $G =: H \rtimes_\varphi K$ is the *semi-direct product* of H and K with respect to φ. We will often simply write $H \rtimes K$, when there is no confusing which φ induces the group action.

A semi-direct product is, in fact, a group, the properties of which are outlined in the theorem below.

Theorem 2.2 ([Dummit and Foote, 2003, Thm. 5.10])**.** *Let $G = H \rtimes_\varphi K$ be a semi-direct product. Then the following properties hold.*

1. *G is a group of order $|G| = |H||K|$. If either H or K is infinite, then so is G.*
2. *Let $\tilde{H} = \{(h,1) \mid h \in H\}$ and $\tilde{K} = \{(1,k) \mid k \in K\}$. Then $\tilde{H}, \tilde{K} \leq G$, and by the maps $h \mapsto (h,1)$ and $k \mapsto (1,k)$, for $h \in H$ and $k \in K$, respectively, we get the isomorphisms*
$$H \cong \tilde{H} \quad \text{and} \quad K \cong \tilde{K}.$$
By this identification, we further have that
3. *$H \trianglelefteq G$;*
4. *$H \cap K = 1$;*
5. *for all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$.*

This theorem makes it clear that K acts by conjugation on H, when we construct the semi-direct product. The following proposition is another general result about semi-direct products, which we will need later in the section.

Theorem 2.3 ([Dummit and Foote, 2003, Thm. 5.12])**.** *Let G be a group, and H and K subgroups, such that $H \trianglelefteq G$ and $H \cap K = 1$. Then $HK \cong H \rtimes K$. If $G = HK$, with the above, then $G = H \rtimes K$.*

2.1 One-dimensional affine linear group modulo p

Before defining Frobenius groups, we will first consider the one-dimensional affine linear group modulo p, $\mathrm{AGL}(1,\mathbb{F}_p)$. Frobenius groups will, in fact, turn out to by subgroups of $\mathrm{AGL}(1,\mathbb{F}_p)$. It is a well-known result that all Galois groups of irreducible polynomials of degree p are isomorphic to a subgroup of $\mathrm{AGL}(1,\mathbb{F}_p)$ [Cox, 2004, Thm. 14.1.1]. We will not prove this, but it serves as a motivation for considering $\mathrm{AGL}(1,\mathbb{F}_p)$ in the first place.

Definition 2.4 (One-dimensional affine linear group modulo p)**.** For $a,b \in \mathbb{F}_p$ define $\gamma_{a,b}\colon \mathbb{F}_p \to \mathbb{F}_p$ by $\gamma_{a,b}(u) = au + b$. Let $\mathrm{AGL}(1,\mathbb{F}_p) = \left\{\, \gamma_{a,b} \mid (a,b) \in \mathbb{F}_p^\times \times \mathbb{F}_p \,\right\}$ with the composition being composition of maps. This is called the *one-dimensional affine linear group modulo p.*

Proposition 2.5. $\mathrm{AGL}(1,\mathbb{F}_p)$ *is indeed a group.*

Proof. Assume throughout that $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$. For $u \in \mathbb{F}_p$, the composition from the definition above satisfies

$$\begin{aligned}
\gamma_{a,b} \circ \gamma_{c,d}(u) &= \gamma_{a,b}(\gamma_{c,d}(u)) \\
&= \gamma_{a,b}(cu + d) \\
&= a(cu + d) + b \\
&= acu + ad + b \\
&= \gamma_{ac,ad+b}(u).
\end{aligned}$$

Suppose $\gamma_{a,b}(u_1) = \gamma_{a,b}(u_2)$. Then $au_1 + b = au_2 + b$, so $u_1 = u_2$. So $\gamma_{a,b}$ is injective. As $\gamma_{a,b}$ is a map from $\mathbb{F}_p$ to itself, then it must also be surjective. Note that $\gamma_{1,0}$ satisfies the conditions of the neutral element. We have that

$$\begin{aligned}\gamma_{a,b} \circ \gamma_{a^{-1},-a^{-1}b} &= \gamma_{aa^{-1},a(-a^{-1}b)+b}\\ &= \gamma_{1,0},\end{aligned}$$

and

$$\begin{aligned}\gamma_{a^{-1},-a^{-1}b} \circ \gamma_{a,b}(u) &= \gamma_{a^{-1}a,a^{-1}b+(-a^{-1}b)}\\ &= \gamma_{1,0},\end{aligned}$$

so $\gamma_{a^{-1},-a^{-1}b}$ is the inverse of $\gamma_{a,b}$. We also have that

$$\begin{aligned}(\gamma_{a,b} \circ \gamma_{c,d}) \circ \gamma_{e,f} &= \gamma_{ac,ad+b} \circ \gamma_{e,f}\\ &= \gamma_{(ac)e,(ac)f+(ad+b)}\\ &= \gamma_{a(ce),a(cf+d)+b}\\ &= \gamma_{a,b} \circ \gamma_{ce,cf+d},\end{aligned}$$

which shows associativity of the group composition. Thus $\mathrm{AGL}(1, \mathbb{F}_p)$ is, in fact, a group. ■

Not only is $\mathrm{AGL}(1, \mathbb{F}_p)$ a group, it is also isomorphic to a certain semi-direct product. This fact both makes it more intuitive to consider Frobenius groups as subgroups of $\mathrm{AGL}(1, \mathbb{F}_p)$, and also to construct realisations of subgroups of $\mathrm{AGL}(1, \mathbb{F}_p)$ as Galois groups.

Theorem 2.6. *Let $\varphi\colon \mathrm{AGL}(1, \mathbb{F}_p) \to \mathbb{F}_p^\times$ be defined by $\varphi(\gamma_{a,b}) = a$. Then φ induces the isomorphism $\mathrm{AGL}(1, \mathbb{F}_p) \cong \mathbb{F}_p \rtimes \mathbb{F}_p^\times$.*

Proof. We have that

$$\begin{aligned}\varphi(\gamma_{a,b} \circ \gamma_{c,d}) &= \varphi(\gamma_{ac,ad+b})\\ &= ac\\ &= \varphi(\gamma_{a,b})\varphi(\gamma_{c,d}),\end{aligned}$$

so φ is a homomorphism. We must have that $\gamma_{a,b} \in \ker\varphi$ if and only if $a = 1$. Hence,

$$\ker\varphi = \{\, \gamma_{1,b} \mid b \in \mathbb{F}_p \,\} =: T.$$

By the first isomorphism theorem for groups, $\mathrm{AGL}(1, \mathbb{F}_p)/T \cong \mathbb{F}_p^\times$. Clearly, $T \cong \mathbb{F}_p$ be the map $\gamma_{1,b} \mapsto b$. As $T = \ker\varphi$, we have that $\mathbb{F}_p \cong T \trianglelefteq \mathrm{AGL}(1, \mathbb{F}_p)$. Let K be the subgroup of $\mathrm{AGL}(1, \mathbb{F}_p)$, which is isomorphic to $\mathbb{F}_p^\times$. It is clear that such a subgroup exists, and we have that $T \cap K = 1$, so, by Theorem 2.3, $TK \cong \mathbb{F}_p \rtimes \mathbb{F}_p^\times$. As $TK \leq \mathrm{AGL}(1, \mathbb{F}_p)$, and $|\mathrm{AGL}(1, \mathbb{F}_p)| = p(p-1)$, then we must have that $\mathrm{AGL}(1, \mathbb{F}_p) \cong \mathbb{F}_p \rtimes \mathbb{F}_p^\times$. ■

It is well-known that the Galois group of an irreducible polynomial of degree n is a transitive subgroup of S_n. It turns out that $\mathrm{AGL}(1, \mathbb{F}_p)$ can be considered as a transitive subgroup of S_p, which is of course in agreement with the fact, which was previously mentioned, that Galois groups of irreducible polynomials of degree p are all subgroups of $\mathrm{AGL}(1, \mathbb{F}_p)$.

Proposition 2.7. $\mathrm{AGL}(1, \mathbb{F}_p)$ *can be considered as a transitive subgroup of S_p.*

Proof. Let $\psi\colon \mathrm{AGL}(1, \mathbb{F}_p) \to S_p$ be given by the map

$$\gamma_{a,b} \mapsto \begin{pmatrix} 1 & \dots & p \\ [a+b]_p & \dots & [ap+b]_p \end{pmatrix},$$

where $[ai+b]_p$ is the residue class modulo p, but where we write p instead of 0, as we are considering permutations of $\{1,\dots,p\}$. To shorten this notation we let the above permutation be denoted by $\begin{pmatrix} i \\ [ai+b]_p \end{pmatrix}_{1\leq i\leq p}$. Clearly, $[ai+b]_p \neq [aj+b]_p$ for all $i\neq j$. If $\gamma_{a,b},\gamma_{c,d}\in \mathrm{AGL}(1,\mathbb{F}_p)$, then

$$\begin{aligned}\psi\left(\gamma_{a,b}\right)\psi\left(\gamma_{c,d}\right) &= \begin{pmatrix} j \\ [aj+b]_p \end{pmatrix}_{1\leq i\leq p}\begin{pmatrix} i \\ [ci+d]_p \end{pmatrix}_{1\leq i\leq p} = \begin{pmatrix} i \\ [a(ci+d)+b]_p \end{pmatrix}_{1\leq i\leq p} \\ &= \begin{pmatrix} i \\ [aci+ad+b]_p \end{pmatrix}_{1\leq i\leq p} = \psi\left(\gamma_{ac,ad+b}\right) = \psi\left(\gamma_{a,b}\circ\gamma_{c,d}\right),\end{aligned}$$

so ψ is a well-defined homomorphism. If $\psi\left(\gamma_{a,b}\right) = \begin{pmatrix} i \\ i \end{pmatrix}_{1\leq i\leq p}$, then we must have that $a=1$ and $b=0$, so it is also injective. Therefore, $\mathrm{AGL}(1,\mathbb{F}_p)$ is isomorphic to a subgroup of S_p.

Let $x,y\in\{1,\dots,p\}$. Assume without loss of generality that $x\leq y$, as when $y<x$, we can simply find a permutation, which sends y to x, then the inverse of this permutation will send x to y. Then

$$\begin{aligned}\psi\left(\gamma_{1,y-x}\right) &= \begin{pmatrix} i \\ i+(y-x) \end{pmatrix}_{1\leq i\leq p} \\ &= \begin{pmatrix} 1 & \dots & x & \dots & p \\ 1+(y-x) & \dots & x+(y-x) & \dots & p+(y-x) \end{pmatrix} \\ &= \begin{pmatrix} 1 & \dots & x & \dots & p \\ 1+(y-x) & \dots & y & \dots & p+(y-x) \end{pmatrix}.\end{aligned}$$

So there exists an element in $\mathrm{AGL}(1,\mathbb{F}_p)$ which permutes x to y. Hence, $\mathrm{AGL}(1,\mathbb{F}_p)$ can be considered as a transitive subgroup of S_p. ■

2.2 Frobenius groups

The main protagonist of this project is the Frobenius groups, and, as hinted previously, they can be considered as subgroups of $\mathrm{AGL}(1,\mathbb{F}_p)$. We will first give a definition of a Frobenius group, and show that it is isomorphic to a semi-direct product.

Definition 2.8 (Frobenius group)**.** Let l and f be integers, such that $l\mid p-1$, and f has order l modulo p. The *Frobenius group of order pl* is $F_{pl} = \langle \sigma,\tau \mid |\sigma| = p, |\tau| = l, \tau\sigma\tau^{-1} = \sigma^f\rangle$.

Let e be a generator of $\mathbb{F}_p^\times$, then $e^{\frac{p-1}{l}}$ has order l. Thus $f = e^{\frac{p-1}{l}} \bmod p$. It follows that

$$\tau\sigma^{f^{l-1}}\tau^{-1} \overset{(1)}{=} \left(\sigma^f\right)^{f^{l-1}} = \sigma^{f^l} = \sigma^1 = \sigma,$$

where at (1) we note that $\tau\sigma^{f^{l-1}}\tau^{-1} = \tau\sigma\tau^{-1}\tau\cdots\sigma\tau^{-1}\tau\sigma\tau^{-1} = \tau\sigma\tau^{-1}\tau\cdots\sigma\tau^{-1}\sigma^f = \cdots = \left(\sigma^f\right)^{f^{l-1}}$. Thus

$$\tau\sigma^{f^{l-1}} = \tau\sigma^{f^{l-1}}\tau^{-1}\tau = \sigma\tau. \tag{2.1}$$

As $\tau\sigma\tau^{-1} = \sigma^f\in\langle\sigma\rangle$, we have that $\langle\sigma\rangle \trianglelefteq F_{pl}$. Thus the quotient $F_{pl}/\langle\sigma\rangle$ is a group, and is of order l. As $F_{pl} = \langle\sigma,\tau\rangle$, then $F_{pl}/\langle\sigma\rangle \cong \langle\tau\rangle$. Note that $\langle\sigma\rangle\cap\langle\tau\rangle = 1$, and $\langle\sigma\rangle\langle\tau\rangle = F_{pl}$. Thus, by Theorem 2.3, we have that $F_{pl}\cong\langle\sigma\rangle\rtimes\langle\tau\rangle$.

Proposition 2.9. *The Frobenius group of order pl is isomorphic to a subgroup of* $\mathrm{AGL}(1,\mathbb{F}_p)$.

Proof. Identify σ^i in F_{pl} with $\gamma_{1,i}$ in $\mathrm{AGL}(1,\mathbb{F}_p)$, and τ^j in F_{pl} with $\gamma_{f^j,0}$ in $\mathrm{AGL}(1,\mathbb{F}_p)$. Then

$$\gamma_{f,0}\circ\gamma_{1,1}\circ\left(\gamma_{f,0}\right)^{-1} = \gamma_{f,0}\circ\gamma_{1,1}\circ\gamma_{f^{-1},0} = \gamma_{f,0}\circ\gamma_{f^{-1},1} = \gamma_{1,f}.$$

By the identification above, this relation is equivalent to the relation $\tau\sigma\tau^{-1} = \sigma^f$ in F_{pl}. Hence, the generators of F_{pl} satisfy the defining relation, when we consider them as elements of $\mathrm{AGL}(1,\mathbb{F}_p)$. Note that $\gamma_{1,1}$ has order p in $\mathrm{AGL}(1,\mathbb{F}_p)$, and $\gamma_{f,0}$ has order l in $\mathrm{AGL}(1,\mathbb{F}_p)$. Thus F_{pl} can be considered as a subgroup of $\mathrm{AGL}(1,\mathbb{F}_p)$. ■

If $l = p - 1$, then the above gives us that F_{pl} is, in fact, isomorphic to $\mathrm{AGL}(1, \mathbb{F}_p)$. Thus $\mathrm{AGL}(1, \mathbb{F}_p)$ can be considered as a kind of ”maximal” Frobenius group.

3 Realising F_{pl} as a Galois group

Now that we have defined Frobenius groups, we can begin the work to realise them as Galois groups. We will first assume that there exists a field, which is the realisation of F_{pl}, i.e., a solution to our problem, and then work out what this field looks like. The construction of this solution will be quite technical. After this, we will state and prove a theorem, which shows that the field is indeed a solution to our problem of realising F_{pl}. See Figure 1 for a diagram of the construction.

$$\begin{tikzcd}
 & & N := M(\zeta_p) = L(\zeta_p)(\sqrt[p]{\omega}) \arrow[dll, dash] \arrow[drr, dash] & & \\
M = L(\alpha) \arrow[drr, dash, "p"] \arrow[ddrr, dash] & & & & L(\zeta_p) = \mathbb{Q}(\zeta_p) \arrow[dll, dash, "\frac{p-1}{l}"'] \\
 & & L \arrow[d, dash, "l"] & & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

Figure 1: Diagram of the construction.

3.1 Constructing a solution

We want to find a field extension $M/\mathbb{Q}$, such that $\operatorname{Gal}(M/\mathbb{Q}) \cong F_{pl}$. Let L be the unique subfield of $\mathbb{Q}(\zeta_p)$, such that $[L : \mathbb{Q}] = l$. This is unique, because $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of order $p-1$, as p is a prime, so there exists a unique subgroup of index l, which then results in the fixed field L being unique.

It is well known that $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is generated by an element κ with $\kappa\zeta_p = \zeta_p^e$, where e is a generator of $\mathbb{F}_p^\times$. Note that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \varphi(p) = p-1$, where φ is Euler's φ-function [Dummit and Foote, 2003, p. 555]. Clearly, $\langle\kappa^l\rangle \trianglelefteq \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, as $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ can be generated by a single element. So $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})/\langle\kappa^l\rangle$ is a quotient group of order $\frac{p-1}{|\langle\kappa^l\rangle|} = \frac{p-1}{\frac{p-1}{l}} = l$, by Lagrange's theorem. Thus L must be the fixed field of $\langle\kappa^l\rangle$.

Now assume that $M/\mathbb{Q}$ is a solution to our problem, i.e. M is such that $\operatorname{Gal}(M/\mathbb{Q}) \cong F_{pl}$ and $L \subseteq M$. We have that $L \subseteq \mathbb{Q}(\zeta_p)$, so $\operatorname{Gal}(L/\mathbb{Q}) \subseteq \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Therefore, there is a surjective homomorphism $\varphi\colon \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \operatorname{Gal}(L/\mathbb{Q})$ given by $g \mapsto g_{|L}$. As $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \langle\kappa\rangle$, then we must have that $\kappa \mapsto h$, where h is a generator of $\operatorname{Gal}(L/\mathbb{Q})$. As $\operatorname{Gal}(M/\mathbb{Q}) \cong F_{pl}$ and $[L : \mathbb{Q}] = l$, we have that $\operatorname{Gal}(L/\mathbb{Q}) = \langle\tau\rangle$, where we recall that F_{pl} is generated by σ and τ of order p and l, respectively. Thus $\kappa_{|L} = \varphi(\kappa) = h = \tau^a$, where $\gcd(a, l) = 1$. As $l \mid p-1$, we have that $\gcd(a, p-1) = 1$. So we can pick b such that $ab = 1 \bmod p-1$. Then κ^b also generates $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $(\kappa^b)_{|L} = \tau^{ab} = \tau$. By choosing κ this way instead (i.e., as what we just denoted κ^b), we have that $\kappa_{|L} = \tau$, which generates $\operatorname{Gal}(L/\mathbb{Q})$. So τ is the restriction of κ to L.

We know that $[M : \mathbb{Q}] = |F_{pl}| = pl$. So $[M : L] = p$. As $\gcd(pl, p-1) = l$, then, by uniqueness of L, $M \cap \mathbb{Q}(\zeta_p) = L$, so the composite field $M\mathbb{Q}(\zeta_p) = M(\zeta_p) =: N$ must satisfy

$$[N : \mathbb{Q}] = \frac{[M : \mathbb{Q}][\mathbb{Q}(\zeta_p) : \mathbb{Q}]}{[L : \mathbb{Q}]} = \frac{(pl)(p-1)}{l} = p(p-1)$$

[Dummit and Foote, 2003, Corollary 14.20]. Thus

$$[N : L(\zeta_p)] = \frac{[N : \mathbb{Q}]}{[L(\zeta_p) : \mathbb{Q}]} = \frac{[N : \mathbb{Q}]}{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]} = \frac{p(p-1)}{p-1} = p.$$

As any group of prime order is cyclic, $\operatorname{Gal}(N/L(\zeta_p))$ is cyclic of order p. Therefore, there exists an element $\omega \in L(\zeta_p)^\times \setminus (L(\zeta_p)^\times)^p$ (i.e., ω is a nonzero element of $L(\zeta_p)$, which is not a pth power), such that $N = L(\zeta_p)(\sqrt[p]{\omega})$. As $L(\zeta_p) = \mathbb{Q}(\zeta_p)$, we have that $N = \mathbb{Q}(\zeta_p)(\sqrt[p]{\omega})$ for some $\omega \in \mathbb{Q}(\zeta_p)^\times \setminus (\mathbb{Q}(\zeta_p)^\times)^p$. The composite field of M and $\mathbb{Q}(\zeta_p)$ is N, so, by [Dummit and Foote, 2003, Proposition 14.21], we have that $N/\mathbb{Q}$ is Galois with

$$\operatorname{Gal}(N/\mathbb{Q}) \cong \left\{ (g, h) \in F_{pl} \times \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \;\middle|\; g_{|L} = h_{|L} \right\} \leq F_{pl} \times \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}).$$

Note that the elements of F_{pl} are of the form $\sigma^i\tau^j$, where $i \in \mathbb{F}_p$ and $j \in \mathbb{F}_l$. As σ is of order p, $[L:\mathbb{Q}] = l$, and $\gcd(p,l) = 1$, then $\sigma_{|L} = 1$. Thus $(\sigma^i\tau^j)_{|L} = \tau^j$. Recall that L is the fixed field of κ^l, and that $\kappa_{|L} = \tau$. Thus $\tau^k = (\kappa^k)_{|L} = (\kappa^{k'})_{|L} = \tau^{k'}$ exactly when $k = k' \bmod l$, as τ is of order l. So we can more precisely describe the Galois group as $\mathrm{Gal}(N/\mathbb{Q}) = \left\{ (\sigma^i\tau^j, \kappa^k) \mid j = k \bmod l \right\}$. For $i = 1 \bmod p$ and $k = 0 \bmod p-1$, we have $\tilde{\sigma} := (\sigma, 1) = (\sigma^i\tau^j, \kappa^k) \in \mathrm{Gal}(N/\mathbb{Q})$. For $i = 0 \bmod p$ and $j,k = 1 \bmod p-1$, we have $\tilde{\tau} := (\tau, \kappa) = (\sigma^i\tau^j, \kappa^k) \in \mathrm{Gal}(N/\mathbb{Q})$.

Clearly, $|\tilde{\sigma}| = p$ and $|\tilde{\tau}| = p-1$. We have that

$$\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1} = (\tau,\kappa)(\sigma,1)(\tau^{-1},\kappa^{-1}) = (\tau\sigma\tau^{-1}, \kappa\kappa^{-1}) = (\sigma^f, 1) = (\sigma,1)^f = \tilde{\sigma}^f.$$

So, by equation (2.1), $\tilde{\sigma}\tilde{\tau} = \tilde{\tau}\tilde{\sigma}^{f^{l-1}}$ is also satisfied.

By definition, $\tilde{\sigma}_{|\mathbb{Q}(\zeta_p)} = 1$. From this, $[N:\mathbb{Q}] = p(p-1)$, $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$, and $|\tilde{\sigma}| = p$, we have that $\mathbb{Q}(\zeta_p)$ must be the fixed field of $\langle\tilde{\sigma}\rangle$. Thus $\tilde{\sigma}$ cannot fix $\sqrt[p]{\omega}$, as it would then be trivial on N. Hence, we must have that $\tilde{\sigma}\sqrt[p]{\omega} = \zeta_p^m\sqrt[p]{\omega}$ for some integer $1 \leq m < p$. Without loss of generality, we may assume $m = 1$, so $\tilde{\sigma}\sqrt[p]{\omega} = \zeta_p\sqrt[p]{\omega}$.

We would like to know how $\tilde{\tau}$ acts on $\sqrt[p]{\omega}$. For all $g \in \mathbb{N}$

$$\tilde{\sigma}\frac{\tilde{\tau}\sqrt[p]{\omega}}{\sqrt[p]{\omega}^g} = \frac{\tilde{\sigma}\tilde{\tau}\sqrt[p]{\omega}}{\tilde{\sigma}\sqrt[p]{\omega}^g} = \frac{\tilde{\tau}\tilde{\sigma}^{f^{l-1}}\sqrt[p]{\omega}}{(\zeta_p\sqrt[p]{\omega})^g} = \frac{\tilde{\tau}\left(\zeta_p^{f^{l-1}}\sqrt[p]{\omega}\right)}{\zeta_p^g\sqrt[p]{\omega}^g} \overset{(1)}{=} \frac{\zeta_p^{ef^{l-1}}\tilde{\tau}\sqrt[p]{\omega}}{\zeta_p^g\sqrt[p]{\omega}^g}$$

At (1) we note that $\tilde{\tau}_{|\mathbb{Q}(\zeta_p)} = \kappa$. With this information we can now choose $g = ef^{l-1} \bmod p$. Then $\zeta_p^{ef^{l-1}} = \zeta_p^g$, so $\frac{\tilde{\tau}\sqrt[p]{\omega}}{\sqrt[p]{\omega}^g}$ is fixed by $\tilde{\sigma}$. As $\mathbb{Q}(\zeta_p)$ is the fixed field of $\langle\tilde{\sigma}\rangle$, we must have $\frac{\tilde{\tau}\sqrt[p]{\omega}}{\sqrt[p]{\omega}^g} \in \mathbb{Q}(\zeta_p)$, but $\sqrt[p]{\omega} \notin \mathbb{Q}(\zeta_p)$, so there must exist a $y \in \mathbb{Q}(\zeta_p)^\times$ such that $\tilde{\tau}\sqrt[p]{\omega} = y \cdot \sqrt[p]{\omega}^g \in \mathbb{Q}(\zeta_p)$.

As $\tilde{\tau}$ has order $p-1$, then $\tilde{\tau}^l$ has order $\frac{p-1}{l}$, so the fixed field of $\langle\tilde{\tau}^l\rangle$ has degree $\frac{p(p-1)}{\frac{p-1}{l}} = pl$ over $\mathbb{Q}$. We also have that $\tilde{\tau}_{|M} = \tau$, so $(\tilde{\tau}^l)_{|M} = \tau^l = 1$. As $[M:\mathbb{Q}] = pl$, the fixed field of $\langle\tilde{\tau}^l\rangle$ is M.

Define $\alpha := \sum_{i=0}^{\frac{p-1}{l}-1}\tilde{\tau}^{il}\sqrt[p]{\omega}$. As $\tilde{\tau}^{0\cdot l} = \tilde{\tau}^{\frac{p-1}{l}\cdot l}$, we have that

$$\tilde{\tau}^l\alpha = \sum_{i=0}^{\frac{p-1}{l}-1}\tilde{\tau}^l\tilde{\tau}^{il}\sqrt[p]{\omega} = \sum_{i=0}^{\frac{p-1}{l}-1}\tilde{\tau}^{(i+1)l}\sqrt[p]{\omega} = \sum_{i=1}^{\frac{p-1}{l}}\tilde{\tau}^{il}\sqrt[p]{\omega} = \sum_{i=0}^{\frac{p-1}{l}-1}\tilde{\tau}^{il}\sqrt[p]{\omega} = \alpha, \tag{3.1}$$

so $\tilde{\tau}^l$ fixes α.

As $M/\mathbb{Q}$ is Galois, M/L is as well. As the extension is certainly finite, then we have, by The Primitive Element Theorem [Dummit and Foote, 2003, Proposition 14.25], that $M = L(\alpha)$.

We only have left to answer the question, can we always pick ω, such that $\alpha \notin L$? We cannot answer this question in general, but we will later in this section show that such an ω exists in the special case $l = \frac{p-1}{2}$. We will also, in the second half of this project, show that the special case $F_{2p} = D_p$ can be realised.

3.2 Showing $M/\mathbb{Q}$ is a solution

We have shown that if a solution $M/\mathbb{Q}$ to our problem exists, it will look like the construction illustrated in Figure 1 (although α might be different). To show that a solution actually exists, we need to prove the below proposition, which states that such a construction is indeed a solution to our problem.

Proposition 3.1. *Let* $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \langle\kappa\rangle$ *with* $\kappa\zeta = \zeta^e$, *where* ζ *is a primitive pth root of unity and e is a generator of* $\mathbb{F}_p^\times$. *Let* $l > 1$ *such that* $l \mid p-1$, *let* $f = e^{\frac{p-1}{l}} \bmod p$, *and let L be the unique subfield of* $\mathbb{Q}(\zeta_p)$ *with* $[L:\mathbb{Q}] = l$, *i.e., L is the fixed field of* $\langle\kappa^l\rangle$. *Let* $g = ef^{l-1} \bmod p$, *and suppose there exists* $\omega \in \mathbb{Q}(\zeta_p)^\times \setminus (\mathbb{Q}(\zeta_p)^\times)^p$ *and* $x \in \mathbb{Q}(\zeta_p)^\times$, *such that* $\kappa\omega = x^p \cdot \omega^g$.

Then $N := \mathbb{Q}(\zeta_p, \sqrt[p]{\omega})$ *is a Galois extension of* $\mathbb{Q}$, *and* $[N:\mathbb{Q}] = p(p-1)$.

Let, in addition, $\tilde{\tau}$ *be the extension of* κ *to N, and let M be the fixed field of* $\langle\tilde{\tau}^l\rangle$. *Then* $M/\mathbb{Q}$ *is Galois with* $\mathrm{Gal}(M/\mathbb{Q}) \cong F_{pl}$.

Lastly, if $\alpha = \sum_{i=0}^{\frac{p-1}{l}-1}\tilde{\tau}^{il}\sqrt[p]{\omega} \notin L$, *then* $M = L(\alpha)$.

Proof. We first show that $N/\mathbb{Q}$ is Galois. Define $h \in \mathbb{Q}(\zeta_p)[y]$ by $h(y) = (y^p - \omega)(y^p - \kappa\omega)\cdots(y^p - \kappa^{p-2}\omega)$. Then

$$\begin{aligned}
\kappa h(y) &= \kappa\left((y^p - \omega)(y^p - \kappa\omega)\cdots(y^p - \kappa^{p-2}\omega)\right) \\
&= \kappa(y^p - \omega)\kappa(y^p - \kappa\omega)\cdots\kappa(y^p - \kappa^{p-2}\omega) \\
&= (y^p - \kappa\omega)(y^p - \kappa^2\omega)\cdots(y^p - \kappa^{p-2}\omega)(y^p - \kappa^{p-1}\omega) \\
&= (y^p - \kappa\omega)(y^p - \kappa^2\omega)\cdots(y^p - \kappa^{p-2}\omega)(y^p - \omega) \\
&= (y^p - \omega)(y^p - \kappa\omega)\cdots(y^p - \kappa^{p-2}\omega),
\end{aligned}$$

so h is invariant under κ. Thus $h \in \mathbb{Q}[y]$, as $\mathbb{Q}$ is the fixed field of $\langle\kappa\rangle$. We have, by assumption, that $\kappa\omega = x_1^p\omega^g$ for some $x_1 \in \mathbb{Q}(\zeta_p)^\times$. Hence,

$$\kappa^2\omega = \kappa\left(x_1^p\omega^g\right) = (\kappa x_1)^p\,(\kappa\omega)^g = (\kappa x_1)^p\,(x_1^g)^p\,\omega^{g^2}.$$

Let $x_2 = (\kappa x_1)\,(x_1^g)$, then $\kappa^2\omega = x_2^p\omega^{g^2}$. To show that

$$\kappa^j\omega = x_j^p\omega^{g^j} \tag{3.2}$$

holds for appropriate x_j, we will proceed by induction on j. Let $j > 0$, and assume Equation (3.2) holds for j. Then

$$\kappa^{j+1}\omega = \kappa\left(x_j^p\omega^{g^j}\right) = (\kappa x_j)^p\,(\kappa\omega)^{g^j} = (\kappa x_j)^p\left(x_j^{g^j}\right)^p\omega^{g^{j+1}}.$$

By letting $x_{j+1} = (\kappa x_j)\left(x_j^{g^j}\right)$, we have shown the induction step.

Each root of h is, in particular, a root of $y^p - \kappa^i\omega$ for some $0 \leq i \leq p-2$. Thus, by the above induction, we have that $y = \sqrt[p]{\kappa^i\omega} = x^i \cdot \sqrt[p]{\omega}^{g^i}$, and clearly all roots of h must be of this form. As $N = \mathbb{Q}(\zeta_p, \sqrt[p]{\omega})$, the roots of h are in N, so N contains the splitting field of h. Consider the first factor of h, namely $(y^p - \omega)$. A root of this is $y = x^0 \cdot \sqrt[p]{\omega}^{g^0} = \sqrt[p]{\omega}$. Another root of $y^p - \omega$ is $y = \zeta_p\sqrt[p]{\omega}$. So $\sqrt[p]{\omega}$ and ζ_p are both in the splitting field of h, which, therefore, contains N. Thus N is the splitting field of h, hence, N is a Galois extension.

As $\omega \notin \{0\} \cup (\mathbb{Q}(\zeta_p)^\times)^p$, then $\sqrt[p]{\omega} \notin \mathbb{Q}(\zeta_p)$. So $N/\mathbb{Q}(\zeta_p)$ is a nontrivial extension. Thus $[N : \mathbb{Q}(\zeta_p)] = p$, as p is prime, so $\mathrm{Gal}(N/\mathbb{Q}(\zeta_p))$ is cyclic of degree p. Due to $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, and $\gcd(p, p-1) = 1$, we must have that $[N : \mathbb{Q}] = p(p-1)$. This proves the first part of the proposition.

Now, as $\mathrm{Gal}(N/\mathbb{Q}(\zeta_p)) \subseteq \mathrm{Gal}(N/\mathbb{Q})$, there exists a $\tilde{\sigma} \in \mathrm{Gal}(N/\mathbb{Q})$ such that $\langle\tilde{\sigma}\rangle = \mathrm{Gal}(N/\mathbb{Q}(\zeta_p))$. Without loss of generality, we may assume that $\tilde{\sigma}\zeta_p = \zeta_p$, and $\tilde{\sigma}\sqrt[p]{\omega} = \zeta_p\sqrt[p]{\omega}$. Clearly, $\tilde{\sigma}$ must have order p. As $N/\mathbb{Q}$ is Galois, there exists an extension $\tilde{\tau}$ of κ to N. We must have that $\tilde{\tau}\omega = \kappa\omega = x^p\omega^g$. Thus $\tilde{\tau}\sqrt[p]{\omega} = x\sqrt[p]{\omega}^g$ up to a power of ζ_p, so by changing x by the appropriate power of ζ_p we can and will assume that $\tilde{\tau}\sqrt[p]{\omega} = x\sqrt[p]{\omega}^g$. In addition, $\tilde{\tau}\zeta_p = \kappa\zeta_p = \zeta_p^e$. Then we have that

$$\tilde{\sigma}\tilde{\tau}\zeta_p = \tilde{\sigma}\zeta_p^e = \zeta_p^e = \tilde{\tau}\zeta_p = \tilde{\tau}\tilde{\sigma}\zeta_p = \tilde{\tau}\tilde{\sigma}^{f^{l-1}}\zeta_p,$$

and

$$\begin{aligned}
\tilde{\tau}\tilde{\sigma}^{f^{l-1}}\sqrt[p]{\omega} &= \tilde{\tau}\left(\zeta_p^{f^{l-1}}\sqrt[p]{\omega}\right) = \tilde{\tau}\zeta_p^{f^{l-1}}\tilde{\tau}\sqrt[p]{\omega} = \zeta_p^{ef^{l-1}}x\sqrt[p]{\omega}^g \\
&= x\zeta_p^g\sqrt[p]{\omega}^g = x(\zeta_p\sqrt[p]{\omega})^g = \tilde{\sigma}\left(x\sqrt[p]{\omega}^g\right) = \tilde{\sigma}\tilde{\tau}\sqrt[p]{\omega}.
\end{aligned}$$

Thus $\tilde{\sigma}\tilde{\tau} = \tilde{\tau}\tilde{\sigma}^{f^{l-1}}$. Noting that f has order l, we have that

$$\begin{aligned}
\tilde{\sigma}^f &= \left(\tilde{\tau}\tilde{\sigma}^{f^{l-1}}\tilde{\tau}^{-1}\right)^f = \tilde{\tau}\tilde{\sigma}^{f^{l-1}}\tilde{\tau}^{-1}\tilde{\tau}\tilde{\sigma}^{f^{l-1}}\tilde{\tau}^{-1}\ldots\tilde{\tau}\tilde{\sigma}^{f^{l-1}}\tilde{\tau}^{-1} \\
&= \tilde{\tau}\left(\tilde{\sigma}^{f^{l-1}}\right)^f\tilde{\tau}^{-1} = \tilde{\tau}\tilde{\sigma}^{f^l}\tilde{\tau}^{-1} = \tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}.
\end{aligned} \tag{3.3}$$

Therefore $\tilde{\sigma}$ and $\tilde{\tau}$ do not commute, because $\tilde{\sigma} \neq \tilde{\sigma}^f$, as $l > 1$. Therefore, $\mathrm{Gal}(N/\mathbb{Q})$ cannot be cyclic. Then $\tilde{\tau}$ cannot generate $\mathrm{Gal}(N/\mathbb{Q})$, so it cannot have order $[N : \mathbb{Q}] = p(p-1)$. As $\tilde{\tau}$ extends κ, which is of order $p-1$, and $\tilde{\tau}$ cannot have order $[N : \mathbb{Q}]$, we must have that $\tilde{\tau}$ has order $p-1$.

We know that $\mathrm{Gal}(N/\mathbb{Q}(\zeta_p))$ is generated by $\tilde{\sigma}$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is generated by $\tilde{\tau}_{|\mathbb{Q}(\zeta_p)} = \kappa$. Thus $\mathrm{Gal}(N/\mathbb{Q}) = \langle \tilde{\sigma}, \tilde{\tau} \rangle$.

We want to show by induction on $m \in \mathbb{N}$ that

$$\left(\tilde{\sigma}^{f-1}\tilde{\tau}\right)^m = \tilde{\sigma}^{f^m-1}\tilde{\tau}^m. \tag{3.4}$$

For $m = 1$, we have that

$$\left(\tilde{\sigma}^{f-1}\tilde{\tau}\right)^m = \tilde{\sigma}^{f-1}\tilde{\tau} = \tilde{\sigma}^{f^m-1}\tilde{\tau}^m,$$

which shows the induction start. Assume that $\left(\tilde{\sigma}^{f-1}\tilde{\tau}\right)^m = \tilde{\sigma}^{f^m-1}\tilde{\tau}^m$ holds for some $m > 1$. Then

$$\begin{aligned}
\left(\tilde{\sigma}^{f-1}\tilde{\tau}\right)^{m+1} &= \left(\tilde{\sigma}^{f-1}\tilde{\tau}\right)^m \tilde{\sigma}^{f-1}\tilde{\tau} = \left(\tilde{\sigma}^{f^m-1}\tilde{\tau}^m\right)\tilde{\sigma}^{f-1}\tilde{\tau} \\
&= \tilde{\sigma}^{f^m-1}\left(\tilde{\tau}^m\tilde{\sigma}^{f-1}\tilde{\tau}^{-m}\right)\tilde{\tau}^{m+1} = \tilde{\sigma}^{f^m-1}\left(\tilde{\tau}^m\tilde{\sigma}\tilde{\tau}^{-m}\right)^{f-1}\tilde{\tau}^{m+1} \\
&\overset{(1)}{=} \tilde{\sigma}^{f^m-1}\left(\tilde{\sigma}^{f^m}\right)^{f-1}\tilde{\tau}^{m+1} = \tilde{\sigma}^{f^m-1}\tilde{\sigma}^{f^{m+1}-f^m}\tilde{\tau}^{m+1} = \tilde{\sigma}^{f^{m+1}-1}\tilde{\tau}^{m+1},
\end{aligned}$$

where at (1) we apply $\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1} = \tilde{\sigma}^f$ m times. This shows the induction step.

Then we have that

$$\tilde{\sigma}^{-1}\tilde{\tau}^l\tilde{\sigma} \overset{(1)}{=} (\tilde{\sigma}^{-1}\tilde{\tau}\tilde{\sigma})^l = (\tilde{\sigma}^{-1}\tilde{\tau}\tilde{\sigma}\tilde{\tau}^{-1}\tilde{\tau})^l \overset{(2)}{=} (\tilde{\sigma}^{-1}\tilde{\sigma}^f\tilde{\tau})^l = (\tilde{\sigma}^{f-1}\tilde{\tau})^l \overset{(3)}{=} \tilde{\sigma}^{f^l-1}\tilde{\tau}^l \overset{(4)}{=} \tilde{\sigma}^0\tilde{\tau}^l = \tilde{\tau}^l.$$

At (1) we insert $\tilde{\sigma}\tilde{\sigma}^{-1}$ between each pair of $\tilde{\tau}$. At (2) we apply the relation shown in Equation (3.3). At (3) we use Equation (3.4). At (4) recall that $f^l = 1 \bmod p$ and $\tilde{\sigma}$ has order p. So $\tilde{\sigma}$ normalises $\tilde{\tau}^l$. Thus $\langle \tilde{\tau}^l \rangle \trianglelefteq \mathrm{Gal}(N/\mathbb{Q})$. Letting M be the fixed field of $\langle \tilde{\tau}^l \rangle$, we then have, by the Main Theorem of Galois Theory [Dummit and Foote, 2003, Thm. 14.14], that $M/\mathbb{Q}$ is Galois.

As $|\tilde{\tau}| = p-1$, then we must have that $\left|\langle \tilde{\tau}^l \rangle\right| = \frac{p-1}{l}$. It follows from the Main Theorem of Galois Theory that $[M : \mathbb{Q}] = \left|\mathrm{Gal}(N/\mathbb{Q})/\langle \tilde{\tau}^l \rangle\right| = \frac{p(p-1)}{\frac{p-1}{l}} = pl$.

Leting $\sigma = \tilde{\sigma}_{|M}$ and $\tau = \tilde{\tau}_{|M}$, $\mathrm{Gal}(M/\mathbb{Q})$ is generated by σ and τ. And, by equation (3.3), $\sigma^f = \tau\sigma\tau^{-1}$. By this relation, we must have that $\langle \sigma \rangle \trianglelefteq \mathrm{Gal}(M/\mathbb{Q})$, and $\mathrm{Gal}(M/\mathbb{Q})/\langle \sigma \rangle = \langle \tau \rangle$. As $|\tilde{\tau}| = p-1$, then $|\tau| \mid p-1$, and thus $|\tau|$ is prime to p. The order of τ must also be a divisor of $|\mathrm{Gal}(M/\mathbb{Q})| = pl$, so $|\tau| \leq l$. As $|\tilde{\sigma}| = p$, then $|\sigma| = 1, p$. If it was 1, then $\mathrm{Gal}(M/\mathbb{Q})$ would be equal to $\mathrm{Gal}(M/\mathbb{Q})/\langle \sigma \rangle = \langle \tau \rangle$. But we concluded above that $|\tau| \leq l < pl$. So $|\sigma| = p$. Then we have that $|\tau| = l$, as $\frac{|\mathrm{Gal}(M/\mathbb{Q})|}{|\langle \sigma \rangle|} = |\langle \tau \rangle|$. Then $\mathrm{Gal}(M/\mathbb{Q})$ satisfies the properties in the definition of the Frobenius group, so $\mathrm{Gal}(M/\mathbb{Q}) \cong F_{pl}$. This proves the second part of the proposition.

We know that L is the fixed field of κ^l. As $\tilde{\tau}$ is an extension of κ, then $\tilde{\tau}^l$ must also fix L. But M is the fixed field of $\langle \tilde{\tau}^l \rangle$, so $L \subseteq M$. Now let $\alpha = \sum_{i=0}^{\frac{p-1}{l}-1} \tilde{\tau}^{il} \sqrt[p]{\omega} \notin L$. By equation (3.1), $\tilde{\tau}^l$ fixes α, so $\alpha \in M$. As $[M : L] = \frac{[M:\mathbb{Q}]}{[L:\mathbb{Q}]} = p$, so the only intermediate fields of the extension $M/\mathbb{Q}$ are M and L. Hence, by [Dummit and Foote, 2003, Proposition 14.24], $M = L(\alpha)$, which concludes our proof. ■

3.3 Realising $F_{p\frac{p-1}{2}}$ as a Galois group

As remarked earlier, in general, we have to make the assumption that $\alpha \notin L$. However, in concrete cases, we *can* actually show this. Hence, the fitting thing to do next is of course to construct some class of examples, where we can apply Proposition 3.1. The class of examples, which we will construct, involves the Chebyshev polynomial, so we will begin by defining it.

Definition 3.2 (Chebyshev polynomial [Mason and Handscomb, 2002, p. 2])**.** Let $\theta \in \mathbb{R}$, $n \in \mathbb{N}$, and $x = \cos\theta$. Then the relation $T_n(x) = \cos n\theta$ defines the *Chebyshev polynomial of the first kind T_n.*

Remark 3.3. Henceforth, we will refer to T_n simply as the *Chebyshev polynomial.* From the definition it follows immediately that $T_0(x) = 1$, and $T_1(x) = x$. For $n \geq 2$, the recursive relation

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),$$

holds, by [Mason and Handscomb, 2002, p. 2], and we see that T_n is indeed a polynomial.

We will now begin the construction of the class of examples, where $p = 3 \bmod 4$ and $l = \frac{p-1}{2}$. Luckily, we have already carried out a general construction, so we can simply apply this process to our special case.

Let $p = 3 \bmod 4$. From knowledge of Gaussian sums, we have that $\left((-1)^{\frac{p-1}{2}}p\right)^{1/2} = \sum_{a=0}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a$, where $\left(\frac{a}{p}\right)$ is the Legendre symbol. When $p = 3 \bmod 4$, $(-1)^{\frac{p-1}{2}}p = -p$, so $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$, hence, $\mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\zeta_p)$.

As $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$ is Galois, then κ, as in Proposition 3.1, maps $\mathbb{Q}(\sqrt{-p})$ to itself, but cannot do so trivially, as the fixed field of κ is $\mathbb{Q}$. Thus $\kappa\sqrt{-p} = -\sqrt{-p}$.

Define

$$\omega := \frac{1}{2}\left(\frac{a^2+pb^2}{4}\right)^{\frac{p-1}{2}}\left(a + b\sqrt{-p}\right) \in \mathbb{Q}(\sqrt{-p}),$$

where $a, b \in \mathbb{Z}$, not both zero. Then $\kappa\omega = \frac{1}{2}\left(\frac{a^2+pb^2}{4}\right)^{\frac{p-1}{2}}(a - b\sqrt{-p})$, so

$$\begin{aligned}
\omega\kappa\omega &= \left(\frac{1}{2}\left(\frac{a^2+pb^2}{4}\right)^{\frac{p-1}{2}}\left(a + b\sqrt{-p}\right)\right)\left(\frac{1}{2}\left(\frac{a^2+pb^2}{4}\right)^{\frac{p-1}{2}}\left(a - b\sqrt{-p}\right)\right)\\
&= \frac{1}{4}\left(\frac{a^2+pb^2}{4}\right)^{p-1}\left(a + b\sqrt{-p}\right)\left(a - b\sqrt{-p}\right)\\
&= \left(\frac{a^2+pb^2}{4}\right)^{p-1}\frac{1}{4}\left(a^2+pb^2\right)\\
&= \left(\frac{a^2+pb^2}{4}\right)^{p}.
\end{aligned}$$

Assume in addition that $p \nmid ab$. For the sake of clarity, we state and prove the following in the form of a lemma.

Lemma 3.4. *In the above situation, ω is not a pth power in $\mathbb{Q}(\zeta_p)$.*

Proof. Suppose, seeking a contradiction, that there exists $\eta \in \mathbb{Q}(\zeta_p)$, such that $\omega = \eta^p$.

We have that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\sqrt{-p})] = \frac{[\mathbb{Q}(\zeta_p):\mathbb{Q}]}{[\mathbb{Q}(\sqrt{-p}):\mathbb{Q}]} = \frac{p-1}{2}$. Thus $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})}(\omega) = \omega^{\frac{p-1}{2}}$. As η exists, then there also exists a $u \in \mathbb{Q}(\sqrt{-p})$, such that $\omega^{\frac{p-1}{2}} = u^p$. Then

$$\omega^p = \omega\omega^{p-1} = \omega u^{2p},$$

so $\omega = \frac{\omega^p}{u^{2p}} = \left(\frac{\omega}{u^2}\right)^p$, and so ω would also be a pth power in $\mathbb{Q}(\sqrt{-p})$. Then we have that

$$\begin{aligned}
2^p\omega &= 2^p\frac{1}{2}\left(\frac{a^2+pb^2}{4}\right)^{\frac{p-1}{2}}\left(a+b\sqrt{-p}\right)\\
&= 2^p\frac{1}{2}\frac{1}{4^{\frac{p-1}{2}}}\left(a^2+pb^2\right)^{\frac{p-1}{2}}\left(a+b\sqrt{-p}\right)\\
&= 2^p\frac{1}{2^p}\left(a^2+pb^2\right)^{\frac{p-1}{2}}\left(a+b\sqrt{-p}\right)\\
&= \left(a^2+pb^2\right)^{\frac{p-1}{2}}\left(a+b\sqrt{-p}\right)
\end{aligned}$$

would also be a pth power, as $2^p\omega = \left(2\frac{\omega}{u^2}\right)^p$. So for some $c, d \in \mathbb{Q}$ we have that

$$2^p\omega = \left(a^2+pb^2\right)^{\frac{p-1}{2}}\left(a+b\sqrt{-p}\right) = (c+d\sqrt{-p})^p.$$

As $a, b, \frac{p-1}{2} \in \mathbb{Z}$, we have that $\left(a^2+pb^2\right)^{\frac{p-1}{2}} \in \mathbb{Z}$. We have that $\mathcal{O}_{\mathbb{Q}(\sqrt{-p})} = \mathbb{Z}(\sqrt{-p})$, so $\left(a^2+pb^2\right)^{\frac{p-1}{2}}\left(a+b\sqrt{-p}\right)$ is an algebraic integer. As $(c+d\sqrt{-p})^p$ is an algebraic integer, it has a minimal polynomial $m \in \mathbb{Z}[x]$. Then $m(x^p)$ is a monic polynomial having $c+d\sqrt{-p}$ as a root. So $c+d\sqrt{-p}$ is an algebraic integer. As $p = 3 \bmod 4$, then $\{1, \sqrt{-p}\}$ is an integral basis for $\mathbb{Q}(\sqrt{-p})$. Therefore, $c, d \in \mathbb{Z}$. By the binomial formula, we have that

$$\begin{aligned}
(c+d\sqrt{-p})^p &= \sum_{k=0}^{p}\binom{p}{k}c^{n-k}(d\sqrt{-p})^k\\
&= \sum_{k=0}^{p}\left(\binom{p}{2k}c^{n-2k}d^{2k}(-p)^k + \binom{p}{2k+1}c^{n-(2k+1)}d^{2k+1}(-p)^k\sqrt{-p}\right).
\end{aligned}$$

We see from the above that every term, where k is even, is an integer, and every term, where k is odd, is of the form $m\sqrt{-p}$, where $m = \binom{p}{2k+1}c^{n-(2k+1)}d^{2k+1}(-p)^k$ is an integer. When $k = 1$, then $\binom{p}{k} = \frac{p!}{1!(p-1)!}$, so $p \mid m$. When $k > 1$ and odd, then $p \mid m$, as $p \mid (-p)^{\frac{k-1}{2}}$. So the coefficient in front of $\sqrt{-p}$ in the binomial expansion is divisible by p. However, $2^p\omega = \left(a^2+pb^2\right)^{\frac{p-1}{2}}a + \left(a^2+pb^2\right)^{\frac{p-1}{2}}b\sqrt{-p}$, and by assumption $p \nmid ab$, so $p \nmid \left(a^2+pb^2\right)^{\frac{p-1}{2}}b$. But this is a contradiction, so there cannot exist such an η, meaning ω is not a pth power in $\mathbb{Q}(\zeta_p)$. ■

Let L be the unique subfield of $\mathbb{Q}(\zeta_p)$ with $[L : \mathbb{Q}] = \frac{p-1}{2}$. As in the proof of Proposition 3.1, $\tilde{\tau}$ has order $p-1$ and is an extension of κ to the field $N = \mathbb{Q}(\zeta_p, \sqrt[p]{\omega})$. Therefore, $\tilde{\tau}^{\frac{p-1}{2}}$ is an element in $\mathrm{Gal}(N/\mathbb{Q}) \cong F_{p\cdot(p-1)}$ of order 2.

Recall that $(\tilde{\sigma}^a\tilde{\tau}^b)^2 = \tilde{\sigma}^{a(1+f^b)}\tilde{\tau}^{2b}$. If $\tilde{\sigma}^a\tilde{\tau}^b$ is of order 2, then $\tilde{\sigma}^{a(1+f^b)}\tilde{\tau}^{2b}$ is the neutral element. So $2b = 0 \bmod p-1$ and $a(1+f^b) = 0 \bmod p$. So p must divide either a or $1+f^b$. Note that f is of order $\frac{p-1}{2}$ modulo p. Assume, seeking a contradiction, that $p \mid (1+f^b)$. Then $f^b = -1 \bmod p$, so f is of order $2b$ modulo p. But then $\frac{p-1}{2} = 2b$. However, $p = 3 \bmod 4$, so $\frac{p-1}{2}$ is odd. So $\frac{p-1}{2} \neq 2b$, which is a contradiction. Hence, $p \nmid (1+f^b)$. So we must have that $p \mid a$. Then $\tilde{\sigma}^a$ is the neutral element.

Therefore, an element of order 2 has the form $\tilde{\tau}^b$. This can only happen for $b = \frac{p-1}{2} \bmod p-1$. So $\tilde{\tau}^{\frac{p-1}{2}}$ is the unique element of order 2 in $\mathrm{Gal}(N/\mathbb{Q})$. Clearly, complex conjugation is an automorphism of $\mathrm{Gal}(N/\mathbb{Q})$ of order 2. So $\tilde{\tau}^{\frac{p-1}{2}} =: c$ is complex conjugation. It follows that

$$\sqrt[p]{\omega} + c\sqrt[p]{\omega} = \left(\mathrm{Re}(\sqrt[p]{\omega}) + \mathrm{Im}(\sqrt[p]{\omega})\right) + \left(\mathrm{Re}(\sqrt[p]{\omega}) - \mathrm{Im}(\sqrt[p]{\omega})\right) = 2\mathrm{Re}(\sqrt[p]{\omega}).$$

Seeking a contradiction, suppose that $2\mathrm{Re}(\sqrt[p]{\omega}) =: \xi \in L$. We have that

$$\omega c\omega = \omega c_{|\mathbb{Q}(\sqrt{-p})}\omega = \omega\kappa_{|\mathbb{Q}(\sqrt{-p})}\omega = x^p,$$

where $x = \frac{a^2+pb^2}{4}$. Thus $c\sqrt[p]{\omega} = \zeta_p^j x \sqrt[p]{\omega}^{-1}$ for an appropriate j. Note that

$$\begin{aligned}(\sqrt[p]{\omega})^2 - \xi\sqrt[p]{\omega} + \zeta_p^a x &= (\sqrt[p]{\omega})^2 - (\sqrt[p]{\omega} + c\sqrt[p]{\omega})(\sqrt[p]{\omega}) + \zeta_p^a x \\ &= (\sqrt[p]{\omega})^2 - (\sqrt[p]{\omega} + \zeta_p^a x\sqrt[p]{\omega}^{-1})(\sqrt[p]{\omega}) + \zeta_p^a x \\ &= 0.\end{aligned}$$

Hence, $\sqrt[p]{\omega}$ is a root of $y^2 - \xi y + \zeta_p^a x \in \mathbb{Q}(\zeta_p)[y]$. But then $\deg_{\mathbb{Q}(\zeta_p)} \sqrt[p]{\omega} \leq 2$. But we know that $\deg_{\mathbb{Q}(\zeta_p)} \sqrt[p]{\omega} = p$, as $\omega \notin (\mathbb{Q}(\zeta_p)^\times)^p$. So this is a contradiction, meaning there does not exist a $\xi \in L$ of this form. Let $\alpha := \frac{1}{2}(\sqrt[p]{\omega} + c\sqrt[p]{\omega}) = \mathrm{Re}(\sqrt[p]{\omega})$. Then from the above $\alpha \notin L$. As $\omega\kappa\omega = \left(\frac{a^2+pb^2}{4}\right)^p$, then $|\omega| = \left(\frac{a^2+pb^2}{4}\right)^{\frac{p}{2}}$. So if $\omega = \left(\frac{a^2+pb^2}{4}\right)^{\frac{p}{2}}(\cos\theta + i\sin\theta)$ for some $\theta \in \mathbb{R}$, we must have that $\cos\theta + i\sin\theta = \frac{a+b\sqrt{-p}}{\sqrt{a^2+pb^2}}$. So $\cos\theta = \frac{a}{\sqrt{a^2+pb^2}}$ and $i\sin\theta = \frac{b\sqrt{-p}}{\sqrt{a^2+pb^2}}$. Then we know that

$$\sqrt[p]{\omega} = \sqrt[p]{\left(\frac{a^2+pb^2}{4}\right)^{\frac{p}{2}}}\left(\cos\frac{\theta}{p} + i\sin\frac{\theta}{p}\right) = \frac{\sqrt{a^2+pb^2}}{2}\left(\cos\frac{\theta}{p} + i\sin\frac{\theta}{p}\right)$$

so $\alpha = \frac{\sqrt{a^2+pb^2}}{2}\cos\frac{\theta}{p}$. Note that

$$T_p\left(\frac{2\alpha}{\sqrt{a^2+pb^2}}\right) = T_p\left(\frac{2\frac{\sqrt{a^2+pb^2}}{2}\cos\frac{\theta}{p}}{\sqrt{a^2+pb^2}}\right) = T_p\left(\cos\frac{\theta}{p}\right) = \cos\left(\frac{\theta}{p}p\right) = \cos\theta = \frac{a}{\sqrt{a^2+pb^2}}.$$

Hence, $y = \alpha$ is a solution to the equation

$$T_p\left(\frac{2y}{\sqrt{a^2+pb^2}}\right) - \frac{a}{\sqrt{a^2+pb^2}} = 0. \tag{3.5}$$

Let $h(y) = (a^2+pb^2)^{\frac{p}{2}} T_p\left(\frac{2y}{\sqrt{a^2+pb^2}}\right) - a\left(a^2+pb^2\right)^{\frac{p-1}{2}}$. Clearly, $h(\alpha) = 0$, by the above calculations. Let $n \in \mathbb{N}$ and assume $T_n(y) = a_m y^m + a_{m-1}y^{m-1} + \cdots + a_0$ for appropriate $a_i \in \mathbb{Q}$ and $m \in \mathbb{N}$. We have that

$$T_n(\cos(y+\pi)) = \cos(n(y+\pi)) = -\cos(ny),$$

and

$$T_n(\cos(y)) = a_m\cos(y)^m + a_{m-1}\cos(y)^{m-1} + \cdots + a_0.$$

Assuming m is odd, we then have that

$$\begin{aligned}T_n(\cos(y+\pi)) &= a_m\cos(y+\pi)^m + a_{m-1}\cos(y+\pi)^{m-1} + \cdots + a_0 \\ &= -a_m\cos(y)^m + a_{m-1}\cos(y)^{m-1} - \cdots + a_0.\end{aligned}$$

But $-\cos(ny) = -T_n(\cos(y)) = -a_m\cos(y)^m - a_{m-1}\cos(y)^{m-1} - \cdots - a_0$, so the even numbered terms must be 0. Therefore, as T_p is of degree p, and p is odd, we have that T_p has exclusively odd terms. Hence,

$$T_p\left(\frac{2y}{\sqrt{a^2+pb^2}}\right) = a_p\left(\frac{2y}{\sqrt{a^2+pb^2}}\right)^p + a_{p-2}\left(\frac{2y}{\sqrt{a^2+pb^2}}\right)^{p-2} + \cdots + a_1\left(\frac{2y}{\sqrt{a^2+pb^2}}\right).$$

Thus

$$\begin{aligned}\left(a^2+pb^2\right)^{\frac{p}{2}} T_p\left(\frac{2y}{\sqrt{a^2+pb^2}}\right) &= \left(\sqrt{a^2+pb^2}\right)^p T_p\left(\frac{2y}{\sqrt{a^2+pb^2}}\right) \\ &= a_p(2y)^p + a_{p-2}(2y)^{p-2}\left(a^2+pb^2\right) + \cdots + a_1 2y\left(a^2+pb^2\right)^{\frac{p-1}{2}}.\end{aligned}$$

As $p-1$ is even, $\left(a^2+pb^2\right)^{\frac{p}{2}} T_p\left(\frac{2y}{\sqrt{a^2+pb^2}}\right) \in \mathbb{Q}[y]$, so $h \in \mathbb{Q}[y]$. As T_p is of degree p, and h does not in itself contain any variables (apart from the variables in T_p), we have that h is a polynomial of degree p.

Consider now h as a polynomial over L. Then its root α will generate an extension $L(\alpha)/L$. As h is of prime degree, then the minimal polynomial of α is either h (up to normalisation) or a first degree polynomial. So the extension $L(\alpha)/L$ is either trivial or of degree p. But we know that $\alpha \notin L$, so the extension is not trivial. Therefore $[L(\alpha) : L] = p$. As h is of minimal degree, then, by [Dummit and Foote, 2003, Proposition 13.9], h is irreducible over L (and thus also over $\mathbb{Q}$), and up to normalisation it is the minimal polynomial of α.

To conclude the construction we state and prove the following proposition.

Proposition 3.5. *With the above terminology, the splitting field of h is $M := L(\alpha)$, and $\operatorname{Gal}(M/\mathbb{Q}) = F_{p\cdot\frac{p-1}{2}}$.*

Proof. Recall that $\tilde{\tau}$ is the extension of κ to $N = \mathbb{Q}(\zeta_p, \sqrt[p]{\omega})$, and that L is the fixed field of $\kappa^{\frac{p-1}{2}}$. So $\tilde{\tau}^{\frac{p-1}{2}}$ fixes L. We also have that

$$\tilde{\tau}^{\frac{p-1}{2}}\alpha = \frac{1}{2}\left(\tilde{\tau}^{\frac{p-1}{2}}\sqrt[p]{\omega} + \tilde{\tau}^{\frac{p-1}{2}}\tilde{\tau}^{\frac{p-1}{2}}\sqrt[p]{\omega}\right) = \frac{1}{2}\left(\sqrt[p]{\omega} + \tilde{\tau}^{\frac{p-1}{2}}\sqrt[p]{\omega}\right) = \alpha.$$

So $\tilde{\tau}^{\frac{p-1}{2}}$ fixes α. Thus $\langle\tilde{\tau}^{\frac{p-1}{2}}\rangle$ fixes M. We have that $[M : \mathbb{Q}] = p \cdot \frac{p-1}{2}$. As

$$\left|\operatorname{Gal}(N/\mathbb{Q})/\langle\tilde{\tau}^{\frac{p-1}{2}}\rangle\right| = \frac{p(p-1)}{2} = [M : \mathbb{Q}],$$

we have that M is the fixed field of $\langle\tilde{\tau}^{\frac{p-1}{2}}\rangle$. Therefore, by Proposition 3.1, $M/\mathbb{Q}$ is Galois with $\operatorname{Gal}(M/\mathbb{Q}) \cong F_{p\cdot\frac{p-1}{2}}$. Using this, the fact that h is irreducible over $\mathbb{Q}$, and $\alpha \in M$, we get, by [Dummit and Foote, 2003, Theorem 13], that all roots of h are in M. Hence, the splitting field of h is contained in M.

Let $k \in \{0, \dots, p-1\}$. As $\cos(y + 2\pi k) = \cos(y)$, we have that

$$T_p\left(\cos\left(\frac{y+2\pi k}{p}\right)\right) = \cos\left(p\frac{y+2\pi k}{p}\right) = \cos\left(y + 2\pi k\right) = \cos(y).$$

Let $\gamma_k := \frac{\sqrt{a^2+pb^2}}{2}\cos\left(\frac{\theta+2\pi k}{p}\right)$, where $\cos\theta = \frac{a}{\sqrt{a^2+pb^2}}$, as previously. Then

$$T_p\left(\frac{2\gamma_k}{\sqrt{a^2+pb^2}}\right) = T_p\left(\cos\left(\frac{\theta+2\pi k}{p}\right)\right) = \cos\left(p\frac{\theta+2\pi k}{p}\right) = \cos\left(\theta+2\pi k\right) = \cos\theta = \frac{a}{\sqrt{a^2+pb^2}}.$$

So $h(\gamma_k) = 0$. Define

$$\begin{aligned}
\beta &:= \frac{\sqrt{a^2+pb^2}}{2}\cos\left(\frac{\theta+2\pi}{p}\right) + \frac{\sqrt{a^2+pb^2}}{2}\cos\left(\frac{\theta-2\pi}{p}\right) \\
&= \frac{\sqrt{a^2+pb^2}}{2}\cdot\left(\cos\left(\frac{\theta+2\pi}{p}\right) + \cos\left(\frac{\theta-2\pi}{p}\right)\right) \\
&= \frac{\sqrt{a^2+pb^2}}{2}\cdot\left(\cos\left(\frac{\theta}{p}\right)\cos\left(\frac{2\pi}{p}\right) + \cos\left(\frac{\theta}{p}\right)\cos\left(\frac{2\pi}{p}\right)\right) \\
&= \frac{\sqrt{a^2+pb^2}}{2}\cdot 2\cos\left(\frac{\theta}{p}\right)\cos\left(\frac{2\pi}{p}\right),
\end{aligned}$$

where we note that

$$\cos\left(\frac{\theta\pm 2\pi}{p}\right) = \cos\left(\frac{\theta}{p} + \frac{2\pi}{p}\right) = \cos\left(\frac{\theta}{p}\right)\cos\left(\frac{2\pi}{p}\right) \pm \sin\left(\frac{\theta}{p}\right)\sin\left(\frac{2\pi}{p}\right).$$

We see that $\beta = \gamma_1 + \gamma_{-1}$, so β is in the splitting field of h. Therefore, $\frac{\beta}{\alpha} = \cos\left(\frac{2\pi}{p}\right)$ is also in the splitting field of h. Hence, $\mathbb{Q}\left(\alpha, \cos\left(\frac{2\pi}{p}\right)\right)$ is contained in the splitting field of h.

As $M = L(\alpha)$, it is left to show that $L = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$. We know that $[\mathbb{Q}(\zeta_p) : L] = 2$, which means that L is the fixed field of complex conjugation. We see that

$$\frac{\zeta_p + \zeta_p^{-1}}{2} = \frac{\left(\cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right)\right) + \left(\cos\left(\frac{2\pi}{p}\right) - i\sin\left(\frac{2\pi}{p}\right)\right)}{2} = \cos\left(\frac{2\pi}{p}\right).$$

Note that $c(\zeta_p) = \zeta_p^{-1}$, so $\tilde{\tau}^{\frac{p-1}{2}} \cos\left(\frac{2\pi}{p}\right) = \cos\left(\frac{2\pi}{p}\right)$. Therefore, $\cos\left(\frac{2\pi}{p}\right) \in L$. From this calculation we also get that

$$\zeta_p^2 - 2\cos\left(\frac{2\pi}{p}\right)\zeta_p + 1 = \zeta_p^2 - 2\frac{\zeta_p + \zeta_p^{-1}}{2}\zeta_p + 1 = \zeta_p^2 - \zeta_p^2 - 1 + 1 = 0,$$

so ζ_p is a root of $y^2 - 2\cos\left(\frac{2\pi}{p}\right)y + 1$. It follows from this that $\left[\mathbb{Q}(\zeta_p) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] \leq 2$, so

$$\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) : \mathbb{Q}\right] = \frac{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]}{\left[\mathbb{Q}(\zeta_p) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right]} \geq \frac{p-1}{2}.$$

As $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subseteq L$, and $[L : \mathbb{Q}] = \frac{p-1}{2}$, we must have that $L = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$, which concludes the proof. ■

Despite this construction being quite concrete, it can be hard to completely grasp what these fields and polynomials could be. Therefore, we will work out a small example for a specific prime.

Example 3.6. Let $p = 7$. We would like to realise $F_{p\frac{p-1}{2}} = F_{21}$. Some calculations will be made by use of computational software, as they would otherwise be extremely tedious. By Proposition 3.5 and its proof, $M = \mathbb{Q}\left(\cos\left(\frac{2\pi}{7}\right), \alpha\right)$, where $\alpha = \mathrm{Re}(\sqrt[7]{\omega})$ and $\omega = \frac{1}{2}\left(\frac{a^2+7b^2}{4}\right)^3\left(a + b\sqrt{-7}\right)$. Take $a = b = 2$. Then $\omega = 512 + 512\sqrt{-7}$, and $\alpha = \mathrm{Re}\left(\sqrt[7]{512 + 512\sqrt{-7}}\right)$. To find the polynomial h for which M is the splitting field, we must first determine the seventh Chebyshev polynomial. By recursive use of Remark 3.3, we get that

$$T_7(y) = 64y^7 - 112y^5 + 56y^3 - 7y.$$

Then

$$\begin{aligned} h(y) &= \left(2^2 + 7\cdot 2^2\right)^{\frac{7}{2}} T_7\left(\frac{2y}{\sqrt{2^2 + 7\cdot 2^2}}\right) - 2\left(2^2 + 7\cdot 2^2\right)^{\frac{7-1}{2}} \\ &= 8192y^7 - 114688y^5 + 458752y^3 - 458752y - 65536. \end{aligned}$$

If we run h through computational software, we do indeed find that $\mathrm{Gal}(M/\mathbb{Q}) = F_{21}$. ○

4 Results from Class Field Theory

This section will focus on stating some needed results from class field theory. Most results will be blackboxed, however, we will prove an important result about the class number. Let $C(\mathcal{O}_K)$ denote the class group of $\mathcal{O}_K$ (also called the class group of K). One type of Frobenius groups are the dihedral groups of order $2p$. Indeed, by letting $l = 2$, we get that $F_{p\cdot 2} = D_p$. If $L/\mathbb{Q}$ is an extension of degree $2n$ with Galois group D_n, then we call L a *dihedral field* of degree $2n$ over $\mathbb{Q}$. Some dihedral groups are rather easy to realise, as the following example illustrates.

Example 4.1. Let us consider the dihedral group of order six, $D_3 = \langle r, s \mid |r| = 3, |s| = 2, srs = r^{-1} \rangle$. We know that $\mathbb{Q}(i)$ is an extension of degree 2 with $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$, and that $\mathbb{Q}(\sqrt[3]{2})$ is an extension of degree 3 with $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$. By considering the degrees of these field extension, we see that $\mathbb{Q}(i, \sqrt[3]{2})$ is an extension of degree 6, and in fact $\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(i\sqrt[3]{2})$. It turns out that $D_3 \cong \mathrm{Gal}(\mathbb{Q}(i\sqrt[3]{2})/\mathbb{Q})$, and we can easily see that $x^6 + 4$ realises D_3 as a Galois group. ○

However, it is not easy to realise D_p for all primes p. Due to the assumption we had to make in the first half, we will, in this half of the project, show separately that it is actually possible to realise dihedral groups of order $2p$ for all primes p. As these are the type of Frobenius groups, where $l = 2$, it would be intuitive to start our construction with some quadratic extension $K/\mathbb{Q}$. If $L/\mathbb{Q}$ is a dihedral field of order $2p$ with $K \subseteq L$, then $[L : K] = p$, so $\mathrm{Gal}(L/K) = \mathbb{Z}/p\mathbb{Z}$. Hence, the extension L/K is abelian. This leads us to consider the use of class field theory to show that D_p can be realised as a Galois group. To get started, some definitions are required.

Definition 4.2 (Finite and infinite primes)**.** Let K be a number field. A *real infinite prime* is an embedding $\sigma\colon K \to \mathbb{R}$. A *complex infinite prime* is a pair of complex conjugate embedding $\sigma, \overline{\sigma}\colon K \to \mathbb{C}$ with $\sigma \neq \overline{\sigma}$. Prime ideals of $\mathcal{O}_K$ are called *finite primes*.

Definition 4.3 (Unramified extension)**.** Let L/K be an extension of number fields. If L/K is unramified at all primes, then L/K is an *unramified extension*.

With these definitions in place, we state a theorem, which will define the notion of the Hilbert class field.

Theorem 4.4 ([Cox, 1989, Thm. 5.18])**.** *Let K be a number field. Then there is a unique, finite Galois extension L/K, such that*

(i) L is an unramified abelian extension of K.

(ii) Any unramified abelian extension of K lies in L, i.e., L is the maximal unramified extension of K.

Definition 4.5 (Hilbert class field)**.** The field L from Theorem 4.4 is called the *Hilbert class field* of K.

The following important definitions are needed throughout the rest of this section and beyond.

Definition 4.6 ([Cox, 1989, p. 144])**.** Given $m \in \mathbb{N}$, an ideal J of $\mathcal{O}_K$ is *prime to m* if $J + m\mathcal{O}_K = \mathcal{O}_K$.

By the discussion in [Cox, 1989, p. 144], an ideal $\alpha\mathcal{O}_K$ being prime to m is equivalent to the condition that $\alpha = a \bmod m\mathcal{O}_K$ for some $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$.

Definition 4.7 (Fractional ideal [Marcus, 2018, Chap. 3, Exc. 31])**.** Let K be a number field, and let $\mathcal{O}_K$ be the associated number ring. Note that $\mathcal{O}_K$ is a Dedekind domain. A *fractional ideal* of K is a set of the form αI, where $\alpha \in K$ and I is an ideal of $\mathcal{O}_K$, which are both assumed to be nonzero. Given $f \in \mathbb{N}$, let $I_K(f)$ denote the set of fractional ideals of K, which are relatively prime to f.

It can be shown that $I_K(f)$ is a group. Note that $I_K = I_K(1)$, and that $I_K(f) \subseteq I_K$.

Definition 4.8 (Principal fractional ideals [Cox, 1989, p. 160])**.** Let $f \in \mathbb{N}$. Define $P_{K,\mathbb{Z}}(f)$ to be the set of *principal fractional ideals* generated by the principal ideals $\alpha\mathcal{O}_K$ relatively prime to f. In particular, we define $P_{K,1}(f)$ to be the subset of $P_{K,\mathbb{Z}}(f)$, where $a = 1$. We write $P_K = P_{K,1}(1)$. Then $P_{K,\mathbb{Z}}(f) \subseteq P_K \subseteq I_K$.

If K is a number field, it is the field of fractions of $\mathcal{O}_K$, so elements of P_K will be of the form $\alpha\mathcal{O}_K$, where $\alpha \in K$, and, in general, elements of I_K will be of the form αI for an ideal I of $\mathcal{O}_K$ and some $\alpha \in K$.

Remark 4.9. In $\mathcal{O}_K$ all fractional ideals are invertible in the sense that if I is a fractional ideal of K, then there exists some fractional ideal J, such that $IJ = \mathcal{O}_K$. This follows from [**?**, Thm. 15] and the fact that principal fractional ideals are invertible in $\mathcal{O}_K$ (if $x\mathcal{O}_K$ is a fractional ideal, then $\frac{1}{x}\mathcal{O}_K$ is the inverse).

Definition 4.10 (Order of conductor f)**.** Let $K = \mathbb{Q}(\alpha)$ be a quadratic extension, and let $f \in \mathbb{N}$. Then $\mathcal{O}_K = \mathbb{Z} + \alpha\mathbb{Z}$. Define $\mathcal{O} := \mathbb{Z} + f\alpha\mathbb{Z}$, which we call an *order of conductor* f, as $|\mathcal{O}_K/\mathcal{O}| = f$. The *maximal order* of K is the biggest subring of this form, i.e., the ring of integers $\mathcal{O}_K$.

Definition 4.11. Define the *class group of the order* of conductor $f \geq 1$, $\mathcal{O}$, to be $C(\mathcal{O}) := I_K(f)/P_{K,\mathbb{Z}}(f)$.

Remark 4.12. Note that the invertible ideals of $\mathcal{O}$ are exactly the ones, which are relatively prime with f. This is what ties the definition of $C(\mathcal{O})$ together with our definition of $C(\mathcal{O}_K)$. If $f = 1$, then $\mathcal{O} = \mathcal{O}_K$. With these ideas, it can be shown that $C(O_K) = I_K/P_K$. The nontrivial part of proving this equality is showing that I_K/P_K is in fact a group, however, this is simply algebraic number theory, so we leave it out here. From this equality, we see that this definition agrees with our usual definition of the class group.

We now have what is required to define a ring class field, however, the existence of such a field is not at all trivial, but indeed an important result of class field theory. For this project, we will state the theorem without proof.

Theorem 4.13. *Let K be a number field and let $\mathcal{O}$ be an order of K. Then there exists an abelian extension M of K, such that* $\mathrm{Gal}(M/K) \cong C(\mathcal{O})$.

Definition 4.14 (Ring class field)**.** The field M from Theorem 4.13 is called the *ring class field of $\mathcal{O}$*.

Remark 4.15. If $\mathcal{O} = \mathcal{O}_K$, then M is the Hilbert class field of K, i.e., the ring class field of the maximal order is the Hilbert class field.

With this last definition in place, we can state a lemma, which is one of the central tools needed to prove that realising D_p is indeed possible.

Lemma 4.16 ([Cox, 1989, Lem. 9.3])**.** *Let L be the ring class field of $\mathcal{O}$, where $\mathcal{O}$ is an order of K, and K is an imaginary quadratic number field. Then L is a Galois extension of $\mathbb{Q}$, and its Galois group is*

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z}),$$

where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(L/K)$ *by sending an element to its inverse.*

4.1 The Class Number

Another important tool needed to realise D_p is a formula for the class number of an order of conductor f. The class number of $\mathcal{O}_K$ (also called the class number of K) is $h(\mathcal{O}_K) = |C(\mathcal{O}_K)|$. Similarly, the class number of $\mathcal{O}$ is $h(\mathcal{O}) = |C(\mathcal{O})|$. We first define some notation, which we will need in the theorem below.

Definition 4.17. For an odd prime p, we define $\left(\frac{\mathrm{disc}(K)}{p}\right)$ to be the Legendre symbol of the discriminant of a number field K, i.e.,

$$\left(\frac{\mathrm{disc}(K)}{p}\right) := \begin{cases} 0 & \text{if } p \mid \mathrm{disc}(K) \\ 1 & \text{if } p \nmid \mathrm{disc}(K) \text{ and } \mathrm{disc}(K) = a^2 \bmod p \text{ for some } a \in \mathbb{N} \\ -1 & \text{if } p \nmid \mathrm{disc}(K) \text{ and } \mathrm{disc}(K) \neq a^2 \bmod p \text{ for all } a \in \mathbb{N} \end{cases}$$

For $p = 2$, we define $\left(\frac{\mathrm{disc}(K)}{2}\right)$ to be the Kronecker symbol of the discriminant of a number field K, i.e.,

$$\left(\frac{\mathrm{disc}(K)}{2}\right) := \begin{cases} 0 & \text{if } 2 \mid \mathrm{disc}(K) \\ 1 & \text{if } \mathrm{disc}(K) = 1 \bmod 8 \\ -1 & \text{if } \mathrm{disc}(K) = 5 \bmod 8 \end{cases}$$

To make the proof of Theorem 4.19 more clear, we will need the following lemma.

Lemma 4.18. *Let K be an imaginary quadratic number field, and let $f \in \mathbb{N}$. Then*

$$\left|(\mathcal{O}_K/f\mathcal{O}_K)^\times\right| = f^2 \prod_{\substack{p\mid f\\ p \text{ prime}}} \left(1-\frac{1}{p}\right)\left(1-\left(\frac{\operatorname{disc}(K)}{p}\right)\frac{1}{p}\right).$$

Proof. First let $f = p_1^{a_1}\cdots p_k^{a_k}$ be the prime factorisation of f. By the Chinese Remainder Theorem, $\mathcal{O}_K/f\mathcal{O}_K \cong (\mathcal{O}_K/p_1^{a_1}\mathcal{O}_K)\times\cdots\times(\mathcal{O}_K/p_k^{a_k}\mathcal{O}_K)$. We want to show that

$$(\mathcal{O}_K/f\mathcal{O}_K)^\times \cong (\mathcal{O}_K/p_1^{a_1}\mathcal{O}_K)^\times\times\cdots\times(\mathcal{O}_K/p_k^{a_k}\mathcal{O}_K)^\times.$$

This is equivalent to showing that in the isomorphism $\mathcal{O}_K/f\mathcal{O}_K \cong (\mathcal{O}_K/p_1^{a_1}\mathcal{O}_K)\times\cdots\times(\mathcal{O}_K/p_k^{a_k}\mathcal{O}_K)$, the units on the left hand side correspond directly to the units on the right hand side.

Assume first that u is a unit of $\mathcal{O}_K/f\mathcal{O}_K$. Then there exists some $u^{-1}\in\mathcal{O}_K/f\mathcal{O}_K$. Let $u\mapsto(u_1,\dots,u_k)$ and $u^{-1}\mapsto(y_1,\dots,y_k)$. Then $1=uu^{-1}\mapsto(u_1,\dots,u_k)(y_1,\dots,y_k)=(u_1y_1,\dots,u_ky_k)$. But $1\mapsto(1,\dots,1)$, so we must have that $u_iy_i=1$ for all i. Thus the image of u is indeed a unit. Assume conversely that $u_1\in\mathcal{O}_K/p_1^{a_1},\dots,u_k\in\mathcal{O}_K/p_k^{a_k}$ are all units. Then there exists $u_1^{-1}\in\mathcal{O}_K/p_1^{a_1},\dots,u_k^{-1}\in\mathcal{O}_K/p_k^{a_k}$. Let $(u_1,\dots,u_k)\mapsto u$ and $\left(u_1^{-1},\dots,u_k^{-1}\right)\mapsto y$ via the isomorphism. We then have that

$$(1,\dots,1)=\left(u_1u_1^{-1},\dots,u_ku_k^{-1}\right)=(u_1,\dots,u_k)\left(u_1^{-1},\dots,u_k^{-1}\right)\mapsto uy$$

and $(1,\dots,1)\mapsto 1$, so we must have that $uy=1$. Thus u is also a unit. Thus the isomorphism holds.

For each i there are three possibilities for how p_i splits in $\mathcal{O}_K$:

$$p_i^{a_i}\mathcal{O}_K=\begin{cases}(\mathfrak{p}^2)^{a_i} & \text{(case 1)}\\ (\mathfrak{p})^{a_i} & \text{(case 2)}\\ (\mathfrak{p}_1\mathfrak{p}_2)^{a_i} & \text{(case 3),}\end{cases}$$

where $\mathfrak{p},\mathfrak{p}_1,\mathfrak{p}_2$ are all prime ideals of $\mathcal{O}_K$. Let f_i be the inertial degree of the prime(s) lying over p_i (within each case f_i is the same for each of the primes lying over p_i because the extension is Galois). Let $N := N_{K/\mathbb{Q}}$. Recall that the norm of a prime ideal is the underlying prime raised to the inertial degree. We have that

$$N(\mathfrak{p})=p_i^{f_i}=\begin{cases}p_i & \text{(case 1)}\\ p_i^2 & \text{(case 2)}\\ p_i & \text{(case 3).}\end{cases}$$

Before we proceed we must show that

$$\left|(\mathcal{O}_K/\mathfrak{p}^n)^\times\right| = N(\mathfrak{p})^n\left(1-\frac{1}{N(\mathfrak{p}_i)}\right). \tag{4.1}$$

We proceed by induction on n. If $n=1$, then $\mathcal{O}_K/\mathfrak{p}$ is a field, so the only non-unit element is zero. Thus

$$\left|(\mathcal{O}_K/\mathfrak{p})^\times\right| = N(\mathfrak{p})-1 = N(\mathfrak{p})^n\left(1-\frac{1}{N(\mathfrak{p})}\right).$$

Suppose Equation (4.1) holds for some fixed $n-1\geq 1$. We will construct a short exact sequence

$$1\longrightarrow\mathcal{O}_K/\mathfrak{p}\xrightarrow{\varphi}(\mathcal{O}_K/\mathfrak{p}^n)^\times\xrightarrow{\psi}\left(\mathcal{O}_K/\mathfrak{p}^{n-1}\right)^\times\longrightarrow 1 \tag{4.2}$$

from which it will follow that $\left|\left(\mathcal{O}_K/\mathfrak{p}^{n-1}\right)^\times\right||\mathcal{O}_K/\mathfrak{p}| = \left|(\mathcal{O}_K/\mathfrak{p}^n)^\times\right|$. This will prove the induction step.

Note that $\mathfrak{p}^n\subsetneq\mathfrak{p}^{n-1}$, so we can pick $u\in\mathfrak{p}^{n-1}\setminus\mathfrak{p}^n$. Let $\alpha\in\mathcal{O}_K$. We have that $\left[(\alpha u)^2\right]_{\mathfrak{p}^n}=\left[\alpha^2u^2\right]_{\mathfrak{p}^n}=[0]_{\mathfrak{p}^n}$. Thus $1-\alpha u$ is clearly an inverse of $\alpha u+1$, so $\alpha u+1\in(\mathcal{O}/\mathfrak{p}^n)^\times$. We can, therefore, define φ by $\varphi([\alpha]_\mathfrak{p})=[\alpha u+1]_{\mathfrak{p}^n}$ for $\alpha\in\mathcal{O}_K$. For $\alpha,\beta\in\mathcal{O}_K$, we have that

$$\varphi([\alpha]_\mathfrak{p})\varphi([\beta]_\mathfrak{p})=[\alpha u+1]_{\mathfrak{p}^n}[\beta u+1]_{\mathfrak{p}^n}=[\alpha\beta u^2+\alpha u+\beta u+1]_{\mathfrak{p}^n}=[\alpha u+\beta u+1]_{\mathfrak{p}^n}=\varphi([\alpha+\beta]_\mathfrak{p})$$

as $u^2 \in \mathfrak{p}^n$. So φ is a group homomorphism. Define $\psi([\alpha]_{\mathfrak{p}^n}) = [\alpha]_{\mathfrak{p}^{n-1}}$, which is obviously a homomorphism.

We want to show that φ is injective. Let $\alpha \in \ker \varphi$, i.e., $\varphi([\alpha]_{\mathfrak{p}}) = [\alpha u + 1]_{\mathfrak{p}^n} = [1]_{\mathfrak{p}^n}$. Then we must have that $\alpha u \in \mathfrak{p}^n$. As $u \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$, $(u) = \mathfrak{p}^{n-1}A$, where A is an ideal with $\mathfrak{p} \nmid A$. Note that $(\alpha) = \mathfrak{p}^k B$ for appropriate k and some ideal B with $\mathfrak{p} \nmid B$. Then $(\alpha u) = \mathfrak{p}^{n-1}\mathfrak{p}^k AB$. As $\alpha u \in \mathfrak{p}^n$, we must have that $k \geq 1$, so $\alpha \in \mathfrak{p}$. Thus $[\alpha]_{\mathfrak{p}} = [0]_{\mathfrak{p}}$, i.e., $\ker \varphi = 0$. So φ is injective.

Let $\alpha \in (\mathcal{O}_K/\mathfrak{p}^{n-1})^\times$. Then there exists some $\beta \in \mathcal{O}_K$ such that $[\alpha\beta]_{\mathfrak{p}^{n-1}} = [1]_{\mathfrak{p}^{n-1}}$, so there exists some $\gamma \in \mathfrak{p}^{n-1}$ such that $\alpha\beta = 1 + \gamma$. Then

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

As $\gamma \in \mathfrak{p}^{n-1}$, then $-\gamma^2 \in \mathfrak{p}^n$, so

$$[\alpha]_{\mathfrak{p}^n}[\beta - \beta\gamma]_{\mathfrak{p}^n} = [1]_{\mathfrak{p}^n}.$$

Hence, $\alpha \in (\mathcal{O}_K/\mathfrak{p}^n)^\times$, so ψ is surjective.

Letting $\alpha \in \mathcal{O}_K/\mathfrak{p}$, we get that $\psi(\varphi([\alpha]_{\mathfrak{p}})) = \psi([\alpha u + 1]_{\mathfrak{p}^n}) = [\alpha u + 1]_{\mathfrak{p}^{n-1}} = [1]_{\mathfrak{p}^{n-1}}$, so $\mathrm{im}\varphi \subseteq \ker \psi$.

To show that $\ker \psi \subseteq \mathrm{im}\varphi$, we will first consider $u\mathcal{O}_K$. As $u \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$, then $u\mathcal{O}_K = \mathfrak{p}^{n-1} \cdot A\mathcal{O}_K$, where $A \subseteq \mathcal{O}_K$ is an ideal with $\mathfrak{p} \nmid A\mathcal{O}_K$. Then we must have that $\gcd(u\mathcal{O}_K, \mathfrak{p}^n) = \mathfrak{p}^{n-1}$, i.e.,

$$\mathfrak{p}^{n-1} = u\mathcal{O}_K + \mathfrak{p}^n.$$

Let $\alpha \in \ker \psi$. Then there exists $\beta \in \mathfrak{p}^{n-1}$, such that $\alpha = 1 + \beta$, and we must have that $\beta = \gamma u + \theta$ for some $\gamma \in \mathcal{O}_K$ and $\theta \in \mathfrak{p}^n$. It follows that

$$\varphi\left([\gamma]_{\mathfrak{p}}\right) = [\gamma u + 1]_{\mathfrak{p}^n} = [(\gamma u + \theta) + 1]_{\mathfrak{p}^n} = [\beta + 1]_{\mathfrak{p}^n} = [\alpha]_{\mathfrak{p}^n},$$

so $\alpha \in \mathrm{im}\varphi$. Hence, Equation (4.2) is a short exact sequence.

By Equation (4.1), it follows that

$$\left|(\mathcal{O}_K/p_i^{a_i}\mathcal{O}_K)^\times\right| = \begin{cases} N(\mathfrak{p})^{2a_i}\left(1 - \frac{1}{N(\mathfrak{p})}\right) & \text{(case 1)} \\ N(\mathfrak{p})^{a_i}\left(1 - \frac{1}{N(\mathfrak{p})}\right) & \text{(case 2)} \\ N(\mathfrak{p})^{a_i}\left(1 - \frac{1}{N(\mathfrak{p})}\right) N(\mathfrak{p})^{a_i}\left(1 - \frac{1}{N(\mathfrak{p})}\right) & \text{(case 3)} \end{cases}$$

$$= \begin{cases} p_i^{2a_i}\left(1 - \frac{1}{p_i}\right) & \text{(case 1)} \\ p_i^{2a_i}\left(1 - \frac{1}{p_i^2}\right) & \text{(case 2)} \\ p_i^{a_i}\left(1 - \frac{1}{p_i}\right) p_i^{a_i}\left(1 - \frac{1}{p_i}\right) & \text{(case 3)} \end{cases}$$

$$= \begin{cases} p_i^{2a_i}\left(1 - \frac{1}{p_i}\right) & \text{(case 1)} \\ p_i^{2a_i}\left(1 - \frac{1}{p_i^2}\right) & \text{(case 2)} \\ p_i^{2a_i}\left(1 - \frac{1}{p_i}\right)^2 & \text{(case 3).} \end{cases}$$

We note that we are in case 1 if and only if $p \mid \mathrm{disc}(K)$, in case 2 if and only if $\mathrm{disc}(K)$ is not a square modulo p (when p is odd) or $\mathrm{disc}(K) = 5 \bmod 8$ (when $p = 2$), and in case 3 if and only if $\mathrm{disc}(K)$ is a square modulo p (when p is odd) or $\mathrm{disc}(K) = 1 \bmod 8$ (when $p = 2$). Thus

$$\left(\frac{\mathrm{disc}(K)}{p}\right) = \begin{cases} 0 & \text{(case 1)} \\ -1 & \text{(case 2)} \\ 1 & \text{(case 3).} \end{cases}$$

So

$$\left|(\mathcal{O}_K/p_i^{a_i}\mathcal{O}_K)^\times\right| = \begin{cases} (p_i^{a_i})^2\left(\left(1 - \frac{1}{p_i}\right)\left(1 - 0\frac{1}{p_i}\right)\right) & \text{(case 1)} \\ (p_i^{a_i})^2\left(\left(1 - \frac{1}{p_i}\right)\left(1 - (-1)\frac{1}{p_i}\right)\right) & \text{(case 2)} \\ (p_i^{a_i})^2\left(\left(1 - \frac{1}{p_i}\right)\left(1 - 1\frac{1}{p_i}\right)\right) & \text{(case 3).} \end{cases}$$

$$= (p_i^{a_i})^2\left(\left(1 - \frac{1}{p_i}\right)\left(1 - \left(\frac{\mathrm{disc}(K)}{p_i}\right)\frac{1}{p_i}\right)\right).$$

Then

$$\begin{aligned}\left|(\mathcal{O}_K/f\mathcal{O}_K)^\times\right| &= \left|(\mathcal{O}_K/p_1^{a_1}\mathcal{O}_K)^\times\right| \times \cdots \times \left|(\mathcal{O}_K/p_k^{a_k}\mathcal{O}_K)^\times\right| \\ &= \prod_{i=1}^{k} (p_i^{a_i})^2 \left(\left(1-\frac{1}{p_i}\right)\left(1-\left(\frac{\operatorname{disc}(K)}{p_i}\right)\frac{1}{p_i}\right)\right) \\ &= (p_1^{a_1}\cdots p_k^{a_k})^2 \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\left(1-\left(\frac{\operatorname{disc}(K)}{p_i}\right)\frac{1}{p_i}\right) \\ &= f^2 \prod_{\substack{p\mid f \\ p \text{ prime}}} \left(1-\frac{1}{p}\right)\left(1-\left(\frac{\operatorname{disc}(K)}{p}\right)\frac{1}{p}\right).\end{aligned}$$

■

We will now prove a central theorem, which gives a formula for the class number of an order of conductor f. As mentioned, this will play a key role in our later result concerning the realisation of D_p as a Galois group.

Theorem 4.19 ([Cox, 1989, Thm. 7.24])**.** *Let K be an imaginary quadratic number field, and let $\mathcal{O}$ be an order of conductor f, i.e., $\mathcal{O} \subseteq \mathcal{O}_K$, where $|\mathcal{O}_K/\mathcal{O}| = f \in \mathbb{N}$. Then*

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{\substack{p\mid f \\ p \text{ prime}}} \left(1-\left(\frac{\operatorname{disc}(K)}{p}\right)\frac{1}{p}\right).$$

Furthermore, $h(\mathcal{O})$ is always an integer multiple of $h(\mathcal{O}_K)$.

Remark 4.20. We will only prove the theorem for the case, where $\mathcal{O}_K^\times = \{\pm 1\}$. It can be shown that $\mathcal{O}_K^\times \neq \{\pm 1\}$ if and only if $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, and the theorem does in fact also hold in this case. The proof for these cases would require considerations about the additional units.

Proof. To prove the theorem, we first use some exact sequences to reduce the problem to computing the size of $(I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)$. We then construct a helpful homomorphism, which we will show is surjective. By finding the kernel, this leads us to an expression for the size of $(I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)$, which is the part needed to show the theorem.

By the definition of $C(\mathcal{O})$ and Remark 4.12, we have that

$$\begin{aligned} h(\mathcal{O}) &= |C(\mathcal{O})| = |I_K(f)/P_{K,\mathbb{Z}}(f)|, \\ h(\mathcal{O}_K) &= |C(\mathcal{O}_K)| = |I_K/P_K|. \end{aligned}$$

Note that $I_K(f) \subseteq I_K$ and $P_{K,\mathbb{Z}}(f) \subseteq I_K(f) \cap P_K$, so we can consider the diagram below.

$$\begin{tikzcd} 0 \arrow[r] & (I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f) \arrow[r, "g_1"] & I_K(f)/P_{K,\mathbb{Z}}(f) \arrow[r, "g_2"] \arrow[d, "\sim"] & I_K/P_K \arrow[d, "\sim"] \\ & & C(\mathcal{O}) \arrow[r, "g_3"] & C(\mathcal{O}_K) \end{tikzcd}$$

Let g_1 be the inclusion. Let $[x]_{P_{K,\mathbb{Z}}(f)} \in I_K(f)/P_{K,\mathbb{Z}}(f)$. Define g_2 to be the map, which sends this representative to $[x]_{P_K} \in I_K/P_K$. This map is well-defined, as if we take some other representative $y \in [x]_{P_{K,\mathbb{Z}}(f)}$, then there exists an $a \in P_{K,\mathbb{Z}}(f) \subseteq P_K$, such that $y = x \cdot a$.

From [Cox, 1989, Corollary 7.17], it follows that all classes in $C(\mathcal{O}_K)$ contain an ideal of $\mathcal{O}_K$, which has norm relatively prime to f. As $|\mathcal{O}_K/\mathcal{O}| = f$, then, by [Cox, 1989, Proposition 7.20], the restriction of these ideals to $\mathcal{O}$ are ideals of $\mathcal{O}$. So if $A \in C(\mathcal{O}_K)$, then there must be some ideal J in the class A, which has norm relatively prime to f. So we also have that $J \cap \mathcal{O}$ is an ideal of $\mathcal{O}$. Let $B \in C(\mathcal{O})$ be the class, which contains $J \cap \mathcal{O}$. Then define g_3 to be, such that $g_3(B) = A$. So g_3 is surjective. Hence, by the first isomorphism theorem for groups, it follows that $h(\mathcal{O}_K)$ divides $h(\mathcal{O})$.

We will show that the top line of the diagram is an exact sequence. As g_1 is the inclusion, it is injective, which shows exactness at $\left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f)$. Then we must also have that $\operatorname{im}(g_1) = \left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f)$. As $\left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f)$ is a set of principal ideals, we must have that $\left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f) \subseteq \ker(g_2)$. If $A \in \ker(g_2)$, then A must be a principal ideal, as I_K/P_K is just the class group, by Remark 4.12. Of course, $A \in I_K(f)/P_{K,\mathbb{Z}}(f)$, so this means that $A \in \left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f)$. Thus $\ker(g_2) = \operatorname{im}(g_1)$. This proves exactness.

As g_3 is surjective, we can extend our exact sequence to

$$0 \longrightarrow \left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f) \xrightarrow{g_1'} C(\mathcal{O}) \xrightarrow{g_3} C(\mathcal{O}_K) \longrightarrow 0,$$

due to g_3 being surjective, and by composition of the maps g_1 and $I_K(f)/P_{K,\mathbb{Z}}(f) \xrightarrow{\sim} C(\mathcal{O})$, which we will denote by g_1'. Note that g_1' is injective, as g_1 is injective (due to exactness of the sequence), so this is a short exact sequence.

Then, from general knowledge of short exact sequences, we have that $C(\mathcal{O}_K) \cong C(\mathcal{O})/\operatorname{im}(g_1')$. Thus $|C(\mathcal{O}_K)| = \frac{|C(\mathcal{O})|}{|\operatorname{im}(g_1')|}$. Due to injectivity of g_1', it follows that $|C(\mathcal{O}_K)| = \frac{|C(\mathcal{O})|}{|(I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)|}$. Thus

$$\frac{h(\mathcal{O})}{h(\mathcal{O}_K)} = \frac{|C(\mathcal{O})|}{|C(\mathcal{O}_K)|} = \left|\left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f)\right|. \tag{4.3}$$

If $[1] \neq [\alpha] \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$, then $\alpha\mathcal{O}_K$ is prime to f, so $\alpha\mathcal{O}_K \in I_K(f) \cap P_K$. Therefore, we can define

$$\psi\colon (\mathcal{O}_K/f\mathcal{O}_K)^\times \to \left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f),$$

where $\psi([\alpha]) = [\alpha\mathcal{O}_K]$.

Let $[\alpha] \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$ and $\beta \in [\alpha]$. Note that $[\alpha]$ and $[\beta]$ are invertible. Then there exists $u \in \mathcal{O}_K$, such that $u\alpha = 1 \bmod f\mathcal{O}_K$. Thus $u\beta = u\alpha = 1 \bmod f\mathcal{O}_K$. So the ideals $u\alpha\mathcal{O}_K$ and $u\beta\mathcal{O}_K$ are in $P_{K,\mathbb{Z}}(f)$. By [Marcus, 2018, Chap. 3, Exc. 31(a)], it follows that

$$\alpha\mathcal{O}_K \cdot u\beta\mathcal{O}_K = (\alpha u\beta)\mathcal{O}_K = (\beta u\alpha)\mathcal{O}_K = \beta\mathcal{O}_K \cdot u\alpha\mathcal{O}_K,$$

where we use the fact that K is commutative. So $\alpha\mathcal{O}_K = \beta\mathcal{O}_K \bmod P_{K,\mathbb{Z}}(f)$. Hence, $\alpha\mathcal{O}_K$ and $\beta\mathcal{O}_K$ are in the same class in $I_K(f) \cap P_K/P_{K,\mathbb{Z}}(f)$. So ψ is a well-defined homomorphism.

Let $\alpha\mathcal{O}_K \in I_K(f) \cap P_K$. Then there must exist some whole number n, such that $\mathfrak{a} = \alpha\mathcal{O}_K \cdot n\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$, which is prime to f. Then $\mathfrak{b} = n\mathcal{O}_K$ is also prime to f. So $\alpha\mathcal{O}_K = \mathfrak{a}\mathfrak{b}^{-1}$. Let $\overline{\mathfrak{b}}$ denote the ideal consisting of the complex conjugates of the elements of $\mathfrak{b}$. This ideal must also be prime to f. Let $m\mathcal{O}_K = \overline{\mathfrak{b}}\cdot\mathfrak{b}$. Then $\overline{\mathfrak{b}} = m\mathcal{O}_K \cdot \mathfrak{b}^{-1}$, so $m\mathcal{O}_K \cdot \alpha\mathcal{O}_K = \overline{\mathfrak{b}} \cdot \mathfrak{b} \cdot \mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}\overline{\mathfrak{b}}$. This implies that $m\alpha \in \mathcal{O}_K$, and that $m\alpha\mathcal{O}_K$ is prime to f. By definition, $m\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$. Therefore, $[\alpha\mathcal{O}_K] = [m\mathcal{O}_K \cdot \alpha\mathcal{O}_K] = [m\alpha\mathcal{O}_K] = \psi([m\alpha])$. Hence, ψ is surjective.

Henceforth, we will assume that $\mathcal{O}_K^\times = \{\pm 1\}$.

It can be shown that $\mathcal{O}_K^\times = \{\pm 1\}$ whenever $K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(i)$. So our assumption is equivalent to assuming K is neither of these fields. Now we consider the following sequence:

$$1 \longrightarrow (\mathbb{Z}/f\mathbb{Z})^\times \xrightarrow{\gamma} (\mathcal{O}_K/f\mathcal{O}_K)^\times \xrightarrow{\psi} \left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f) \longrightarrow 1,$$

where γ is the obvious injection, and ψ is of course the previously defined homomorphism.

As ψ is surjective the sequence is exact at $\left(I_K(f) \cap P_K\right) / P_{K,\mathbb{Z}}(f)$. From injectivity of γ, it follows that the sequence is exact at $(\mathbb{Z}/f\mathbb{Z})^\times$.

Let $\langle a \bmod f\rangle \subseteq (\mathbb{Z}/f\mathbb{Z})^\times$. Note that $\gcd(a, f) = 1$. Then $\gamma(\langle a \bmod f\rangle) = \langle a \bmod f\mathcal{O}_K\rangle$. So

$$\psi(\gamma(\langle a \bmod f\rangle)) = \psi(\langle a \bmod f\mathcal{O}_K\rangle) = a\mathcal{O}_K,$$

where $a\mathcal{O}_K$ is relatively prime to f, so $a\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$. Thus $\gamma(\langle a \bmod f\mathcal{O}_K\rangle) \in \ker(\psi)$, and hence, $\operatorname{im}(\gamma) \subseteq \ker(\psi)$.

Let $[\alpha] \in \ker(\psi)$. Then, clearly, $\alpha\mathcal{O}_K \in P_{K,\mathbb{Z}}(f) \subseteq I_K(f) \cap P_K$. It was shown above that an element $a\mathcal{O}_K \in I_K(f) \cap P_K$ is of the form $a\mathcal{O}_K = \mathfrak{a}\mathfrak{b}^{-1}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are both relatively prime to f. Hence, $\alpha\mathcal{O}_K = \beta\mathcal{O}_K \cdot \gamma^{-1}\mathcal{O}_K$, where $\beta = b \bmod f\mathcal{O}_K$ and $\gamma = c \bmod f\mathcal{O}_K$ for some $[b], [c] \in (\mathbb{Z}/f\mathbb{Z})^\times$.

As $\alpha\mathcal{O}_K = \beta\mathcal{O}_K \cdot \gamma^{-1}\mathcal{O}_K = (\beta\gamma^{-1})\mathcal{O}_K$, α and $\beta\gamma^{-1}$ are associates. Since $\mathcal{O}_K$ is a Dedekind domain, and so, in particular, an integral domain, then $\alpha = u\beta\gamma^{-1}$ for some $u \in \mathcal{O}_K^\times$. But $\mathcal{O}_K^\times = \{\pm 1\}$, so $\alpha = \pm\beta\gamma^{-1}$. As γ was the injection, then we must have that $\gamma([b][c]^{-1}) = [\beta][\gamma]^{-1} = [\beta\gamma^{-1}] = [\alpha]$. Hence, $[\alpha] \in \operatorname{im}(\gamma)$. Thus $\operatorname{im}(\gamma) = \ker(\psi)$, which proves exactness at $(\mathcal{O}_K/f\mathcal{O}_K)^\times$. Hence, the sequence is exact. By the first isomorphism theorem, we then have that

$$(\mathcal{O}_K/f\mathcal{O}_K)^\times/(\mathbb{Z}/f\mathbb{Z})^\times \cong (\mathcal{O}_K/f\mathcal{O}_K)^\times/\ker(\psi) \cong \operatorname{im}(\psi) = (I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f). \tag{4.4}$$

Let φ be Euler's φ-function. It is well-known that

$$\left|(\mathbb{Z}/f\mathbb{Z})^\times\right| = \varphi(n) = f \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

From Lemma 4.18, we have that

$$\left|(\mathcal{O}_K/f\mathcal{O}_K)^\times\right| = f^2 \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{\operatorname{disc}(K)}{p}\right)\frac{1}{p}\right).$$

Thus

$$\frac{\left|(\mathcal{O}_K/f\mathcal{O}_K)^\times\right|}{\left|(\mathbb{Z}/f\mathbb{Z})^\times\right|} = f \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \left(\frac{\operatorname{disc}(K)}{p}\right)\frac{1}{p}\right).$$

Then, by Equations (4.3) and (4.4), we have that

$$h(\mathcal{O}) = h(\mathcal{O}_K)\left|(I_K(f) \cap P_K)/P_{K,\mathbb{Z}}(f)\right| = h(\mathcal{O}_K) f \prod_{\substack{p \mid f \\ p \text{ prime}}} \left(1 - \left(\frac{\operatorname{disc}(K)}{p}\right)\frac{1}{p}\right).$$

We assumed that $\mathcal{O}_K^\times = \{\pm 1\}$. Clearly, we must then also have that $\mathcal{O}^\times = \{\pm 1\}$, so $[\mathcal{O}_K^\times : \mathcal{O}^\times] = 1$. Hence, the theorem follows for the case where $\mathcal{O}_K^\times = \{\pm 1\}$. ■

5 Realising $F_{2p} = D_p$ as a Galois group

As previously mentioned, the analysis leading up to Proposition 3.1 has a certain assumption. This is one of the reason why we will show separately that realising D_p is possible. It turns out that we can actually realise D_p (by constructing these dihedral fields) in infinitely many different ways, which is another important motivation for the following theorem.

Theorem 5.1 ([Jensen and Yui, 1982, Thm. I.2.1])**.** *For any prime p, and any quadratic field $K = \mathbb{Q}(\sqrt{d})$, there exists infinitely many dihedral fields of degree $2p$, which contain K.*

Remark 5.2. Due to the limited scope of this project, we will only prove the theorem for the case of imaginary quadratic fields, i.e., we will assume that d is strictly negative. We will additionally assume that $d \neq -1, -3$. In the case of $d = -1, -3$ the proof would be slightly different, as these cases involve more units. Another reason for exempting these cases is the fact that we have only proved Theorem 4.19 for $d \neq -1, -3$.

Proof. It follows from Dirichlet's theorem on primes in arithmetic progression that there exist infinitely many primes q, such that

(1) $q = 1 \bmod p$;

(2) q splits completely in K.

Proving Dirichlet's theorem is not at all trivial, however, it requires analytic number theory. Therefore, for this project, we will have to assume that the above statement is true.

Let $\mathcal{O}$ be an order of conductor q, and let M be the ring class field of $\mathcal{O}$, which exists by Theorem 4.13. By the definition of the ring class field, we have that

$$\operatorname{Gal}(M/K) \cong C(\mathcal{O}).$$

So, by Theorem 4.19, we have that

$$|\operatorname{Gal}(M/K)| = |C(\mathcal{O})| = h(\mathcal{O}) = \frac{h(\mathcal{O}_K)q}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{\substack{r \mid q \\ r \text{ prime}}} \left(1 - \left(\frac{\operatorname{disc}(K)}{r}\right)\frac{1}{r}\right).$$

We have, by condition (2) above, that q splits completely in K, so $q\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. By [Kiming, b, Thm. 2], if q is odd, then $\operatorname{disc}(K) = a^2 \bmod p$ for some $a \in \mathbb{N}$, and if $q = 2$, then $\operatorname{disc}(K) = 1 \bmod 8$. From the definition of $\left(\frac{\operatorname{disc}(K)}{q}\right)$, it follows that $\left(\frac{\operatorname{disc}(K)}{q}\right) = 1$ in both cases. Recalling that $[\mathcal{O}_K^\times : \mathcal{O}^\times] = 1$, we have that

$$|\operatorname{Gal}(M/K)| = \frac{h(\mathcal{O}_K)q}{1}\left(1 - \frac{1}{q}\right) = h(\mathcal{O}_K)\left(q - 1\right).$$

As $q = 1 \bmod p$, it follows that p divides $|\operatorname{Gal}(M/K)|$. Due to M being the ring class field, it is, in particular, abelian as an extension of K. It follows, from the structure theorem for abelian groups, that $\operatorname{Gal}(M/K) \cong \mathbb{Z}/p^k\mathbb{Z} \times B$ for appropriate $k \in \mathbb{N}$ and group B.

By Lemma 4.16, we have that $\operatorname{Gal}(M/\mathbb{Q}) \cong \operatorname{Gal}(M/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$, where the nontrivial element τ of $\mathbb{Z}/2\mathbb{Z}$ acts by conjugation on $\operatorname{Gal}(M/K)$, where the conjugation inverts the element, i.e., for $g \in \operatorname{Gal}(M/K)$ the conjugation is $\tau g \tau^{-1} = g^{-1}$.

Let $C \leq \mathbb{Z}/p^k\mathbb{Z}$ be such that $[\mathbb{Z}/p^k\mathbb{Z} : C] = p$, and define $N := C \times B$. As $\mathbb{Z}/p^k\mathbb{Z}$ is abelian, $C \trianglelefteq \mathbb{Z}/p^k\mathbb{Z}$, so $N \trianglelefteq \operatorname{Gal}(M/K)$. Therefore, the quotient $\operatorname{Gal}(M/K)/N$ is well defined, and we must have that $\operatorname{Gal}(M/K)/N \cong \mathbb{Z}/p\mathbb{Z}$. In this quotient we define conjugation by τ of $\overline{g} \in \operatorname{Gal}(M/K)/N$ to be

$$\tau\overline{g}\tau^{-1} = \overline{\tau g \tau^{-1}} = \overline{g^{-1}} = \overline{g}^{-1},$$

which makes it clear that $(\operatorname{Gal}(M/K)/N) \rtimes (\mathbb{Z}/2\mathbb{Z}) \cong D_p$.

As $N \trianglelefteq \operatorname{Gal}(M/K)$ and $\operatorname{Gal}(M/\mathbb{Q})$ is simply $\operatorname{Gal}(M/K)$ together with the conjugates of each of its elements, it follows that $N \trianglelefteq \operatorname{Gal}(M/\mathbb{Q})$. Thus the quotient $\operatorname{Gal}(M/\mathbb{Q})/N$ is well defined and must be of order $2p$, as $|\mathrm{Gal}(M/\mathbb{Q})| = 2\,|\mathrm{Gal}(M/K)|$. From this and our knowledge of conjugation in $\mathrm{Gal}(M/\mathbb{Q})$, we see that $\mathrm{Gal}(M/\mathbb{Q})/N \cong (\mathrm{Gal}(M/K)/N) \rtimes (\mathbb{Z}/2\mathbb{Z})$.

By the Main Theorem of Galois Theory [Dummit and Foote, 2003, Thm. 14.14], the fixed field R of $\mathrm{Gal}(M/\mathbb{Q})/N$ is Galois over $\mathbb{Q}$. So we have found a field, which satisfies $\mathrm{Gal}(R/\mathbb{Q}) \cong D_p$. ■

We have now proven that it is always possible to realise D_p. However, the proof does not give us an answer to the question of *how* to find a polynomial that realises D_p. In Example 4.1, we saw an example for $p = 3$, and the theorem tells us that it is actually possible to realise D_3 in infinitely many different ways. With such a small group it was not extremely difficult to find a realisation. However, it was only easy because we already knew some extensions of degree 2 and 3, respectively. For sufficiently large p, this becomes much harder.

Bibliography

[Cox 1989] Cox, David A.: *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* 1. New York : Wiley, 1989. – ISBN 0471506540

[Cox 2004] Cox, David A.: *Galois Theory.* 1. Wiley, 2004. – ISBN 0-471-43419-1

[Dummit and Foote 2003] Dummit, David S. ; Foote, Richard M.: *Abstract Algebra.* 3. Wiley, 2003. – ISBN 978-0-471-43334-7

[Jensen et al. 2002] Jensen, Christian U. ; Ledet, Arne ; Yui, Noriko: *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem.* 1. Cambridge University Press, 2002. – ISBN 0-521-81998-9

[Jensen and Yui 1982] Jensen, Christian U. ; Yui, Noriko: Polynomials with D_p as Galois Group. In: *Journal of Number Theory* 15 (1982), No. 3, P. 347–375. – URL `https://www.sciencedirect.com/science/article/pii/0022314X82900385`. – ISSN 0022-314X

[Kiming a] Kiming, Ian: *Frobenius and Chebyshev.* Private communication. – Supplement to pp. 178-179 in [Jensen et al., 2002].

[Kiming b] Kiming, Ian: *A theorem of Dedekind on prime decomposition.* Private communication. – Notes distributed in connection with the course on Algebraic Number Theory at University of Copenhagen in 2021.

[Marcus 2018] Marcus, Daniel A.: *Number Fields.* 2. Cham : Springer International Publishing AG, 2018 (Universitext). – ISBN 9783319902326

[Mason and Handscomb 2002] Mason, J.C. ; Handscomb, D.C.: *Chebyshev Polynomials.* CRC Press, 2002. – URL `https://books.google.dk/books?id=g1DMBQAAQBAJ&dq=Chebyshev+polynomials+&pg=PP1&redir_esc=y#v=onepage&q&f=false`. – ISBN 9781420036114