11-24-2015 12:00 AM

Galois 2-Extensions

Masoud Ataei Jaliseh, *The University of Western Ontario*

Supervisor: Jan Minac, *The University of Western Ontario*
Joint Supervisor: Eric Schost, *The University of Western Ontario*
A thesis submitted in partial fulfillment of the requirements for the Doctor of Philosophy degree in Mathematics

GALOIS 2-EXTENSIONS
(Thesis format: Monograph)

by

Masoud Ataei Jaliseh

Graduate Program in Mathematics

A thesis submitted in partial fulfillment
of the requirements for the degree of
PhD

The School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

Abstract

The inverse Galois problem is a major question in mathematics. For a given base field F and a given finite group G, one would like to list all Galois extensions L/F such that the Galois group of L/F is G.

In this work we shall solve this problem for all fields F, and for group G of unipotent 4×4 matrices over $\mathbb{F}_2$. We also list all 16 $U_4(\mathbb{F}_2)$-extensions of $\mathbb{Q}_2$. The importance of these results is that they answer the inverse Galois problem in some specific cases.

This is joint work with Ján Mináč and Nguyen Duy Tân.

Keywords: Galois Theory, Class Field Theory, Massey Products, Galois Extensions of Local Fields.

Co-Authorship Statement

Chapter 3 of this thesis incorporates material that is the result of joint research with Professor Ján Mináč and Dr. Nguyễn Duy Tân. Results are available in arXiv:1508.05540 [math.NT] and are submitted for publication soon.

Acknowledgments

My sincere thanks first of all go to Professor Ján Mináč for his joint work with me and with Nguyễn Duy Tân, related to my thesis, as well as for valuable and essential discussions with Ján Mináč, along with plenty of great encouragement, enthusiasm. I would like to also thank Nguyễn Duy Tân for his advice and generous help. Additionally it is a pleasure to warmly thank Professor Éric Schost, my co-supervisor, for having given me the opportunity to pursue this research, and for having provided many interesting and valuable discussions along the way. Additionally I am also very grateful to my other colleagues and friends including Armin Jamshidpey, Michael Rogelstad, Javad Rastegari and Marina Palaisti, for their great help with the exposition of this thesis.

Also I would like to thank Western University and the Department of Mathematics for providing essential financial support which was crucial for the completion of my Ph.D. I would like to also thank Professor Dan Christensen and the other members of the Graduate Committee for their help with issues concerning my graduate studies at Western. And I am very grateful to Janet Williams for her kind help with the various administrative tasks related to my graduate studies at Western over these past few years.

I would like to thank my examiners, Professors John Bell, Masoud Khalkhali, Stuart Rankin, and Andrew Schultz, for their careful study of my thesis and for their suggestions on improving the exposition.

And last but not least I would like to thank my wife, Mahshad, and my parents for their strong support and supreme patience during the course of my studies.

Contents

Introduction

Let G be a finite group, and let F be an arbitrary field. A fundamental problem in Galois theory is to describe all Galois extensions L/F whose Galois groups are isomorphic to group G. It is desirable to describe such families of extensions using invariants of L/F which depend only on the base field F. If G is abelian then this is possible by the theories of Kummer and Artin-Schreier extension, and classical work of A. Albert and D. J. Saltman. Moreover this description is elegant, simple and useful. It is known that there are some other very interesting and useful explicit constructions of Galois extensions L/F with prescribed Galois group G. See for example, [Jar11], [JLY02, Chapters 5-6], [Led05, Chapters 2,5-7], [Mas87], [MNQD77], [MZ11], [Sal82]. However the simplicity and generality of the descriptions of Kummer and Artin-Schreier extension seem to be unmatched.

Recall that for each natural number n, $U_n(\mathbb{F}_p)$ is the group of upper triangular $n\times n$-matrices with entries in $\mathbb{F}_p$ and diagonal entries 1. In a recent development of Massey products in Galois cohomology, it was recognized that Galois extensions L/F with $Gal(L/F) \simeq U_n(\mathbb{F}_p)$ play a very special role in Galois theory of p-extensions. (See [Efr14], [EM14], [HW15], [Dwy75], [LMS03], [MT13, MT15a, MT14b, MT15b]). Moreover the works above reveal some surprising depth and simplicity of analysis of these extensions.

In this thesis we show that there exists a very simple description of the families of Galois extensions L/F with $Gal(L/F) \simeq U_4(\mathbb{F}_2)$ over any given field F. The key difference from the results in [MT15a] is that in this thesis we describe all Galois extensions with $Gal(L/F) \simeq U_4(\mathbb{F}_2)$. We also show that a similar description is valid for Galois $U_3(\mathbb{F}_2)$-extensions over an arbitrary field.

Beside of their intrinsic value, these simple descriptions of Galois extensions L/F with $Gal(L/F) \simeq U_4(\mathbb{F}_p)$ are expected to play a significant role in an induction approach to the construction of Galois extensions L/F with $Gal(L/F) \simeq U_n(\mathbb{F}_2)$ for $n \geq 2$, and for a possible proof of the Vanishing n-Massey Conjecture for absolute Galois groups of fields (see [MT13, MT15b]). Also this description should be useful for establishing the Kernel n-Unipotent Conjecture for absolute Galois groups of fields and $p = 2$. This would be a very interesting extension of the work of [MS96], [Vil]. (See also [EM11], [MT15a].) Further possible applications of this work can be related to an extension of the study of Redei symbols (see [Ama14]) and also the study of 2-Hilbert towers (see [McL08]).

Main results in this thesis are in: Theorem 3.1.1, Theorem 3.1.2, Theorem 2.3.1 and Theorem 2.3.2.

In Chapter 1, I start with a definition of Massey products especially triple Massey products and explain the connection between Massey products and some embedding problems. Specifically, I will discuss the Heisenberg extensions and $U_4(\mathbb{F}_p)-$Galois extensions.

In Chapter 2, we recover the result of Hirotada Naito [Nai95] on dihedral extensions of $\mathbb{Q}_2$. We will separately discuss the cases $p \neq 2$ and $p = 2$ of dihedral extensions of $\mathbb{Q}_p$. In the case $p \neq 2$, there is only one D_4-extension for $p \equiv 3(mod 4)$ and there is no D_4-extension for $p \equiv 1(mod 4)$ over $\mathbb{Q}_p$. In the case $p = 2$, there is a constructive method to build up all 18 D_4-extensions of $\mathbb{Q}_2$, which are listed at the end of this chapter.

Chapter 3 contains my results with Professor Jan Mináč and Dr Nguyễn Duy Tân. We provide a description of Galois $U_4(\mathbb{F}_2)$-extensions over any given field [AMT15]. We then use this description to count the number of Galois $U_4(\mathbb{F}_2)$-extensions over a field which is a finite extension of $\mathbb{Q}_2$. For this result, we used the construction method of Mináč and Tân for $U_4(\mathbb{F}_p)-$extensions, which is explained in Chapter 1, and the construction method of Naito for D_4-extensions, which is explained in Chapter 2, to make a list of all 16 distinct $U_4(\mathbb{F}_2)$ Galois extensions over $\mathbb{Q}_2$. This list is provided in this chapter.

I quote results and preliminary material from available sources with precise references.

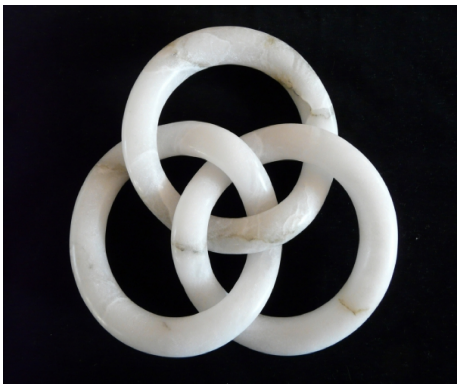
Chapter 1

Massey Products

1.1 Introduction

Massey products have a lot of influence on several rather distinct parts of mathematics. Here I would like to point out some of these aspects. Massey products originated from topology in an effort to produce finer topological invariants than those which existed before. W. S. Massey [Mas58] introduced this product which generalizes the usual cup product.

The complement of Borromean rings gives an example where triple Massey product is defined and non-zero.



In the complement of Borromean rings the linking number of any two rings is zero while all three are linked, showing Borromean rings are an example of a non-trivial Massey product.

In the middle of the 1970s, it was recognized that the non-vanishing of Massey products could be viewed as an obstruction to determination of the homotopy type of some topological spaces from their cohomology rings. P. Deligne, P. Griffiths, J. Morgan and D. Sullivan [DGMS75] in their paper on “Real homotopy theory of Kähler manifolds" using the concept of vanishing Massey products showed real homotopy type of Kähler manifolds follows from its real cohomology ring. Given two spaces X and Y it is said they are homotopy equivalent or of the same homotopy type, if there exist continuous maps $f : X \longrightarrow Y$ and $g : Y \longrightarrow X$

such that $g \circ f$ is homotopic to the id_X and $f \circ g$ is homotopic to id_Y. For more information, please go to [DGMS75].

In 1975, W. G. Dwyer [Dwy75] discovered a crucial link between unipotent representations of groups and a certain vanishing of Massey product. Let $G_K(p)$ be the maximal pro-p-quotient of an absolute Galois group G_K of a field K, and let $\mathbb{U}_4(\mathbb{F}_p)$ be upper triangular unipotent 4 by 4 matrices with entries in $\mathbb{F}_p$. By Dwyer's work, every surjective homomorphism from $G_K(p)$ to $\mathbb{U}_4(\mathbb{F}_p)$ determines a defined triple Massey product which in fact contains zero. This will be discussed in details later.

1.2 Massey products

Let G be a profinite group and p a prime number. Consider the finite field $\mathbb{F}_p$ as a trivial discrete G-module. Let $C^\bullet = (C^\bullet(G, \mathbb{F}_p), \delta, \cup)$ be the differential graded algebra of inhomogenous continuous cochain of G with coefficients in $\mathbb{F}_p$ [NSW13, Chapter I, Section 2] .

Assume $H^\bullet(G, \mathbb{F}_p)$ be the corresponding cohomology groups, and $Z^1(G, \mathbb{F}_p)$ the subgroup of $C^1(G, \mathbb{F}_p)$ consisting of all 1-cocycles. Because we use the trivial action on the coefficients $\mathbb{F}_p$, $Z^1(G, \mathbb{F}_p) = H^1(G, \mathbb{F}_p) = Hom(G, \mathbb{F}_p)$. In this section we review Massey products in $H^\cdot(G, \mathbb{F}_p)$ and their relations to certain types of embedding problems, which will be needed in the sequel. (See [MT13] and [MT15a]).

Let $n \geq 3$ be an integer. Let $a_1, \cdots, a_n$ be elements in $H^1(G, \mathbb{F}_p) = Z^1 \subseteq C^1(G, \mathbb{F}_p)$.

Definition 1.2.1. *A collection $\mathcal{M} = \{a_{ij} | 1 \leq i < j \leq n+1, (i,j) \neq (1, n+1)\}$ of elements a_{ij} of $C^1(G, \mathbb{F}_p)$ is called a defining system for the n−fold Massey product $\langle a_1, \cdots, a_n \rangle$ if the following conditions are fulfilled:*

(1) $a_{i,i+1} = a_i$ for all $i = 1, 2, \cdots n$.

(2) $\delta a_{i,j} = \sum_{l=i+1}^{j-1} a_{il} \cup a_{lj}$ for all $i + 1 < j$.

Then $\sum_{k=2}^{n} a_{1,k} \cup a_{k,n+1}$ is a 2-cycle. Its cohomology class in H^2 is called the value of the product relative to the defining system $\mathcal{M}$ and it is denoted by $\langle a_1, \cdots, a_n \rangle_{\mathcal{M}}$. The product $\langle a_1, \cdots, a_n \rangle$ itself is the subset of $H^2(G, \mathbb{F}_p)$ consisting of all elements which can be written in the form $\langle a_1, \cdots, a_n \rangle_{\mathcal{M}}$ for some defining system $\mathcal{M}$.

As observed by Dwyer [Dwy75] in the discrete context (see also [Efr14, Section 8] in the profinite case), a defining system for Massey products can be interpreted in terms of upper-triangular unipotent representations of G, as follows.

Let $\mathbb{U}_{n+1}(\mathbb{F}_p)$ be a group of all upper-triangular unipotent $(n+1) \times (n+1)-$matrices with entries in $\mathbb{F}_p$. Let Z be the subgroup of all such a matrices with all off-diagonal entries being zero

except at position $(1, n+1)$. We may identify $\mathbb{U}_{n+1}(\mathbb{F}_p)/Z$ with the group $\overline{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ of all upper triangular unipotent $(n+1)\times(n+1)-$matrices with entries over $\mathbb{F}_p$ with the $(1, n+1)-$ entries omitted. For any representation $\rho : G \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ and $1 \leq i < j \leq n+1$, let $\rho_{ij} : G \to \mathbb{F}_p$ be the composition of ρ with the projection from $\mathbb{U}_{n+1}(\mathbb{F}_p)$ to its $(i, j)-$coordinate. We use similar notation for representations $\overline{\rho} : G \to \overline{\mathbb{U}}_{n+1}(\mathbb{F}_p)$.

Assume that

$$\mathcal{M} = \{a_{ij} | 1 \leq i < j \leq n+1, (i,j) \neq (1, n+1)\}$$

is a defining system for an $n-$fold Massey product $\langle a_1, \cdots, a_n\rangle$. We denote a map $\overline{\rho}_{\mathcal{M}} : G \to \overline{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ by $(\overline{\rho}_{\mathcal{M}}) = -a_{ij}$. Then one can check that $\overline{\rho}_{\mathcal{M}}$ is a (continuous) group homomorphism.

Moreover, $\langle a_1, \cdots, a_n\rangle = 0$ if and only if $\overline{\rho}_{\mathcal{M}}$ can be lifted to the group homomorphism $G \to \mathbb{U}_{n+1}(\mathbb{F}_p)$. On the other hand, if $\overline{\rho} : G \to \overline{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ is a group homomorphism, then

$$\{-\overline{\rho}_{ij} | 1 \leq i < j \leq n+1, (i,j) \neq (1, n+1)\}$$

is defining system for

$$\langle -\overline{\rho}_{12}, \cdots - \overline{\rho}_{n,n+1}\rangle.$$

(See [Dwy75, Theorem 2.4].)

1.3 Embedding problem

A weak embedding problem $\mathcal{E}$ for a profinite group G is a diagram

$$\mathcal{E} := \quad \begin{array}{ccc} & & G \\ & & \downarrow \varphi \\ \mathcal{U} & \xrightarrow{f} & \overline{\mathcal{U}} \end{array}$$

which consists of profinite groups $\mathcal{U}$ and $\overline{\mathcal{U}}$ and homomorphisms $\varphi : G \to \overline{\mathcal{U}}$, $f : \mathcal{U} \to \overline{\mathcal{U}}$ with f being surjective. If in addition φ is also surjective, we call $\mathcal{E}$ an *embedding problem*.

A *weak solution* of $\mathcal{E}$ is a homomorphism $\psi : G \to \mathcal{U}$ such that $f\psi = \varphi$. We call $\mathcal{E}$ a *finite* weak embedding problem if group $\mathcal{U}$ is finite. The *kernel* of $\mathcal{E}$ is defined to be $M := ker(f)$. We denote by $Sol(\mathcal{E})$ the set of weak solutions of $\mathcal{E}$.

Assume now the kernel M is abelian. The conjugation action of $\mathcal{U}$ on M is trivial while restricting to $M \subseteq \mathcal{U}$. Hence this induces an $\overline{\mathcal{U}}-$module structure on M. We consider M as a G-module via φ and the conjugation action of $\mathcal{U}$ on M. we denote by M_φ this $G-$module. The following result is well known:

Lemma 1.3.1. *Let $\mathcal{E}(G, f, \varphi)$ be a weak embedding problem with a finite abelian kernel M which has a weak solution. Then $Sol(\mathcal{E})$ is a principal homogeneous space over the group of 1-cycles $Z^1(G, M_\varphi)$.*

In particular, any weak solution θ of $\mathcal{E}$ induces an bijection

$$Sol(\mathcal{E}) \cong Z^1(G, M_\varphi).$$

Proof. See [NSW13, Proof of 3.5.11]

1.4 Heisenberg extensions

Let F be a field containing a primitive $p-$th root of unity ζ. For any element $a \in F^\times$, we write χ_a for the character corresponding to a via the Kummer map [CF67, Chapter 3]

$$F^\times \to H^1(G_F, \mathbb{Z}/p\mathbb{Z}) = Hom(G_F, \mathbb{Z}/p\mathbb{Z})$$

where G_F is the absolute Galois group of the field F. Assume $a \notin (F^\times)^p$. So the extension $F(\sqrt[p]{a})/F$ is a Galois extension with the Galois group $\langle\sigma_a\rangle \cong \mathbb{Z}/p\mathbb{Z}$, where σ_a satisfies $\sigma_a(\sqrt[p]{a}) = \zeta\sqrt[p]{a}$.

The character χ_a defines a homomorphism $\chi^a \in Hom(G_F, \frac{1}{p}\mathbb{Z}/\mathbb{Z}) \subseteq Hom(G_F, \mathbb{Q}/\mathbb{Z})$ by the formula

$$\chi^a = \frac{1}{p}\chi_a.$$

Let b be any element in $F^\times$. Then norm residue symbol may be defined as

$$(a, b) := (\chi^a, b) := b \cup \delta\chi^a.$$

Here δ is a coboundary homomorphism $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ associated to the short exact sequence of trivial G-modules

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

The cup product $\chi_a \cup \chi_b \in H^2(G_F, \mathbb{Z}/p\mathbb{Z})$ can be interpreted as the norm residue symbol (a, b). More precisely, we consider the exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to F_s^\times \xrightarrow{x\mapsto x^p} F_s^\times \to 1,$$

where $\mathbb{Z}/p\mathbb{Z}$ has been identified with the group of $p-$th roots of unity μ_p via the choice of ζ. As $H^1(G_F, F_s^\times) = 0$, we obtain

$$0 \to H^2(G_F, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{i} H^2(G_F, F_s^\times) \xrightarrow{\times p} H^2(G_F, F_s^\times).$$

Then one has $i(\chi_a \cup \chi_b) = (a, b) \in H^2(G_F, F_s^\times)$. (See [Ser13, Chapter XIV, Proposition 5].)

Assume that a, b are elements in $F^\times$, which are linearly independent modulo $(F^\times)^p$. Let $K = F(\sqrt[p]{a}, \sqrt[p]{b})$. Then K/F is a Galois extension whose Galois group is generated by σ_a and σ_b. Here

$$\sigma_a(\sqrt[p]{b}) = \sqrt[p]{b}, \sigma_a(\sqrt[p]{a}) = \zeta\sqrt[p]{a}, \sigma_b(\sqrt[p]{a}) = \sqrt[p]{a}, \sigma_b(\sqrt[p]{b}) = \zeta\sqrt[p]{b}.$$

We consider a map $\mathbb{U}_3(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^2$ which sends

$$\begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \mapsto (x, y).$$

Then we have the following embedding problem

$$\begin{array}{ccccccccc} & & & & & & & & G_F \\ & & & & & & & & \downarrow \overline{\rho} \\ 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^2 & \longrightarrow & 1, \end{array}$$

where $\overline{\rho}$ is the map

$$(\chi_a, \chi_b) : G_F \to Gal(K/F) \cong (\mathbb{Z}/p\mathbb{Z})^2$$

and the last isomorphism is the one which sends σ_a to $(1, 0)$ and σ_b to $(0, 1)$.

Assume that $\chi_a \cup \chi_b = 0$. Then the norm residue symbol (a, b) is trivial. Hence there exists $\alpha \in F(\sqrt[p]{a})$ such that $N_{F(\sqrt[p]{a})/F}(\alpha) = b$, (see [Ser13, Chapter XIV, Proposition 4(iii)]). We set

$$A_0 = \alpha^{p-1}\sigma_a(\alpha^{p-2}) \cdots \sigma_a^{p-2}(\alpha) = \prod_{i=0}^{p-2} \sigma_a^i(\alpha^{p-i-1}) \in F(\sqrt[p]{a}).$$

Lemma 1.4.1. *Let f_a be an element in $F^\times$. Let $A = f_a A_0$. Then we have*

$$\frac{\sigma_a(A)}{A} = \frac{Nm_{F(\sqrt[p]{a})/F}(\alpha)}{\alpha^p} = \frac{b}{\alpha^p}.$$

Proof. [MT15b] Observe that $\frac{\sigma_a(A)}{A} = \frac{\sigma_a(A_0)}{A_0}$. The lemma then follows from the identity

$$(s-1)\sum_{i=0}^{p-2}(p-i-1)s^i = \sum_{i=0}^{p-1} s^i - ps^0$$

We may use multiplicative version of above equality to prove this lemma.

$$\begin{aligned} \frac{\sigma_a(A)}{A} &= \frac{\sigma_a(\alpha^{p-1})\sigma_a^2(\alpha^{p-2}) \cdots \sigma_a^{p-1}(\alpha)}{\alpha^{p-1}\sigma_a(\alpha^{p-2}) \cdots \sigma_a^{p-2}(\alpha)} \\ &= \frac{\sigma_a(\alpha)\sigma_a^2(\alpha) \cdots \sigma_a^{p-1}(\alpha)}{\alpha^{p-1}} \\ &= \frac{Nm_{F(\sqrt[p]{a})/F}(\alpha)}{\alpha^p} = \frac{b}{\alpha^p}. \end{aligned}$$

□

Proposition 1.4.2. *Assume that $\chi_a \cup \chi_b = 0$. Let f_a be an element in $F^\times$. Let $A = f_a A_0$ be defined as above. Then the homomorphism $\overline{\rho} := (\chi_a, \chi_b) : G_F \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ lifts to a Heisenberg extension $\rho : G_F \to \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$.*

Sketch of Proof. [MT15b] Let $L := K(\sqrt[p]{A})/F$. Then L/F is Galois extension. Let $\tilde{\sigma}_a \in Gal(L/K)$ (resp. $\tilde{\sigma}_b \in Gal(L/K)$) be an extension of σ_a (resp. σ_b). Since $\sigma_b(A) = A$, we have $\tilde{\sigma}_b(\sqrt[p]{A}) = \zeta^j \sqrt[p]{A}$, for some $j \in \mathbb{Z}$. Hence $\tilde{\sigma}_b^p(\sqrt[p]{A}) = \sqrt[p]{A}$. This implies that $\tilde{\sigma}_b$ is of order p.

On the other hand, we have $\tilde{\sigma}_a((\sqrt[p]{A})^p) = \sigma_a(A) = A\frac{b}{\alpha^p}$. Hence $\tilde{\sigma}_a(\sqrt[p]{A}) = \zeta^i \sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha}$, for some $i \in \mathbb{Z}$. Then $\tilde{\sigma}_a^p(\sqrt[p]{A}) = \sqrt[p]{A}$. Thus $\tilde{\sigma}_a$ is of order p.

If we set $\sigma_A := [\tilde{\sigma}_a, \tilde{\sigma}_b]$ then $\sigma_A(\sqrt[p]{A}) = \zeta\sqrt[p]{A}$. This implies that σ_A is of order p. Also one can check that

$$[\tilde{\sigma}_a, \sigma_A] = [\tilde{\sigma}_b, \sigma_A] = 1$$

We can define an isomorphism $\varphi : Gal(L/F) \to \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ by letting

$$\sigma_a \mapsto x := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \sigma_b \mapsto y := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \sigma_A \mapsto z := \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then the composition $\rho : G_F \to Gal(L/F) \xrightarrow{\varphi} \mathbb{U}_3(\mathbb{Z}/p\mathbb{Z})$ is the desired lifting of $\overline{\rho}$.

Note that $[L : F] = p^3$. Hence there are exactly p extensions of $\sigma_a \in Gal(E/F)$ to the automorphism in $Gal(L/F)$ since $[L : E] = p^3/p^2 = p$. Therefore for later use, we can choose an extension, still denoted by $\sigma_a \in Gal(L/F)$, of $\sigma_a \in Gal(K/F)$ in such a way that $\sigma_a(\sqrt[p]{A}) = \sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha}$. ⊡

1.5 Triple Massey product

When $n = 3$, in the last section, we will speak about a triple Massey product. Note that in this case, the triple Massey product $\langle a_1, a_2, a_3\rangle$ is defined if and only if $a_1 \cup a_2 = a_2 \cup a_3 = 0$ in $H^2(G, \mathbb{F}_p)$. Then there exist cochains a_{12} and a_{23} in $C^1(G, \mathbb{F}_p)$ such that

$$\delta a_{12} = x \cup y \text{ and } \delta a_{23} = y \cup z,$$

in $C^2(G, \mathbb{F}_p)$. Then we say that $D := \{x, y, z, a_{12}, a_{23}\}$ is a defining system for triple Massey product $\langle x, y, z\rangle$. Observe that

$$\delta(x \cup a_{23} + a_{12} \cup z) = 0.$$

Hence, $x \cup a_{23} + a_{12} \cup z$ is a 2-cocycle. We define the value $\langle x, y, z\rangle_D$ of the triple Massey product $\langle x, y, z\rangle$ with respect to the defining system D to be the cohomology class $[x \cup a_{23} + a_{12} \cup z]$ in $H^1(G, \mathbb{F}_p)$. The set of all values $\langle x, y, z\rangle_D$ when D runs over the set of all defining systems, is called the triple Massey product $\langle x, y, z\rangle \subseteq H^1(G, \mathbb{F}_p)$. Note that we always have

$$\langle x, y, z\rangle = \langle x, y, z\rangle_D + x \cup H^1(G, \mathbb{F}_p) + z \cup H^1(G, \mathbb{F}_p).$$

We also have the following result.

Lemma 1.5.1. *If the triple Massey products $\langle x, y, z\rangle$ and $\langle x, y', z\rangle$ are defined then the triple Massey product $\langle x, y + y', z\rangle$ is defined too, and*

$$\langle x, y + y', z\rangle = \langle x, y, z\rangle + \langle x, y', z\rangle.$$

Proof. [MT15b] Let $\{x, y, z, a_{12}, a_{23}\}$ (respectively, $\{x, y', z, a'_{12}, a'_{23}\}$) be a defining system for $\langle x, y, z\rangle$ (respectively $\langle x, y', z\rangle$). Then $\{x, y+y', z, a_{12}+a'_{12}, a_{23}+a'_{23}\}$ is a defining system for $\langle x, y + y', z\rangle$. We also have

$$\begin{aligned}\langle x, y, z\rangle + \langle x, y', z\rangle &= [x \cup a_{23} + a_{12} \cup z] + x \cup H^1(G, \mathbb{F}_p) + z \cup H^1(G, \mathbb{F}_p)\\ &\quad + [x \cup a'_{23} + a'_{12} \cup z] + x \cup H^1(G, \mathbb{F}_p) + z \cup H^1(G, \mathbb{F}_p)\\ &= [x \cup (a_{23} + a'_{23}) + (a_{12} + a'_{12}) \cup z] + x \cup H^1(G, \mathbb{F}_p) + z \cup H^1(G, \mathbb{F}_p)\\ &= \langle x, y + y', z\rangle.\end{aligned}$$

⊡

For the following proposition, I assume the Theorem 1.6.4 which is originally from [MT15b, Theorem 3.6]and [MT15b, Theorems 3.8 and 4.2].

Proposition 1.5.2. *Let F be an arbitrary field. Let χ_1, χ_2, χ_3 be elements in $Hom(G_F, \mathbb{F}_p)$. We assume that χ_1, χ_2, χ_3 are $\mathbb{F}_p$-linearly independent. If the triple Massey product $\langle \chi_1, \chi_2, \chi_3\rangle$ is defined then it contains 0.*

Proof. [MT15b] Let F^s be a separable closure of F and L be the fixed field of F^s under the kernel of the surjection $(\chi_1, \chi_2, \chi_3) : G_F \to (\mathbb{F}_p)^3$. Then the Theorems 3.6, 3.8 and 4.2 [MT15b] imply that L/F can be embedded in a Galois $\mathbb{U}_4(\mathbb{F}_p)$-extension M/F. More over there exist $\sigma_1, \sigma_2, \sigma_3 \in Gal(M/F)$ such that they generate $Gal(M/F)$, and

$$\chi_1(\sigma_1) = 1, \chi_1(\sigma_2) = 0, \chi_1(\sigma_3) = 0;$$

$$\chi_2(\sigma_1) = 0, \chi_2(\sigma_2) = 1, \chi_2(\sigma_3) = 0;$$

$$\chi_3(\sigma_1) = 0, \chi_3(\sigma_2) = 0, \chi_3(\sigma_3) = 1.$$

(Note that for each $i = 1, 2, 3$, χ_i is trivial on $Gal(M/M_0)$, hence $\chi_i(\sigma_j)$ make sense for every $j = 1, 2, 3$.) An explicit isomorphism $\varphi : Gal(M/F) \to \mathbb{U}_4(\mathbb{F}_p)$ can be defined as

$$\sigma_1 \mapsto \begin{bmatrix}1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}, \quad \sigma_2 \mapsto \begin{bmatrix}1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}, \quad \sigma_3 \mapsto \begin{bmatrix}1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}.$$

Let ρ be the composite homomorphism $\rho : G_F \to Gal(M/F) \cong \mathbb{U}_4(\mathbb{F}_p)$. Then one can check that

$$\rho_{12} = \chi_1, \rho_{23} = \chi_2, \rho_{34} = \chi_3.$$

(Since all the maps $\rho, \chi_1, \chi_2, \chi_3$ factor through $Gal(M/F)$, it is enough to check these equalities on the elements $\sigma_1, \sigma_2, \sigma_3$.) This implies that $\langle -\chi_1, -\chi_2, -\chi_3 \rangle$ contains 0 by [Dwy75, Theorem 2.4]. Hence $\langle \chi_1, \chi_2, \chi_3 \rangle$ also contains 0. ⊡

For each x in Field F, denote $[x]_F$ be the image of x in F/F^p.

Proposition 1.5.3. *Assume that $dim_{\mathbb{F}_p}\langle [a]_F, [b]_F, [c]_F \rangle \leq 2$. If the triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ is defined, then it contains 0.*

Proof. For $char(F) = 2$ see [MT13] and for $char(F) \neq 2$ [MT15b]. ⊡

Theorem 1.5.4. *Let p be an arbitrary prime and F any field. Then the following statements are equivalent.*

(1) There exists χ_1, χ_2, χ_3 in $Hom(G_F, \mathbb{F}_p)$ such that they are $\mathbb{F}_p-$linearly independent and if $char(F) \neq p$ then $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$.

(2) There exists a Galois extension M/F such that $Gal(M/F) \cong \mathbb{U}_4(\mathbb{F}_p)$.

Moreover, assume that (1) *holds, and let L be a fixed field of $(F)^s$ under the kernel of the surjection $(\chi_1, \chi_2, \chi_3) : G_F \to (\mathbb{F}_p)^3$. Then in* (2) *we can construct M/F explicitly such that L is embedded in M.*

If F contains a primitive $p-$th root of unity, then the two above conditions are also eqivalent to the following condition.

(3) There exist $a, b, c \in F^\times$ such that $[F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c}) : F] = p^3$ and $(a, b) = (b, c) = 0$.

If F be of characteristic p then conditions (1), (2) *above are also equivalent to the following condition.*

(3') There exist $a, b, c \in F^\times$ such that $[F(\theta_a, \theta_b, \theta_c) : F] = p^3$.

Proof. See [MT15b]. ⊡

Definition 1.5.5. *We say G has the triple Massey product property with respect to $\mathbb{F}_p$ if every defined triple Massey product $\langle a_1, a_2, a_3 \rangle$, where $a_1, a_2, a_3 \in H^1(G, \mathbb{F}_p)$, necessarily contains 0.*

1.6 $U_4(\mathbb{F}_p)-$Extensions

Assume F is a field containing a primitive p-th root ζ of unity, and let $a, b, c \in F^\times$ such that a, b and c are linearly independent modulo $(F^\times)^p$ and that $(a, b) = (b, c) = 0$. We shall construct that Galois $\mathbb{U}_4(\mathbb{F}_p)$-extension M/F such that M contains $F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$.

First note that $F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F$ is a Galois extension with $Gal(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F)$ generate by $\sigma_a, \sigma_b, \sigma_c$. Here

$$\sigma_a(\sqrt[p]{a}) = \zeta\sqrt[p]{a}, \quad \sigma_a(\sqrt[p]{b}) = \sqrt[p]{b}, \quad \sigma_a(\sqrt[p]{c}) = \sqrt[p]{c}$$
$$\sigma_b(\sqrt[p]{a}) = \sqrt[p]{a}, \quad \sigma_b(\sqrt[p]{b}) = \zeta\sqrt[p]{b}, \quad \sigma_b(\sqrt[p]{c}) = \sqrt[p]{c}$$
$$\sigma_c(\sqrt[p]{a}) = \sqrt[p]{a}, \quad \sigma_c(\sqrt[p]{b}) = \sqrt[p]{b}, \quad \sigma_c(\sqrt[p]{c}) = \zeta\sqrt[p]{c}$$

Let $E = F(\sqrt[p]{a}, \sqrt[p]{c})$. Since $(a, b) = (b, c) = 0$, there are $\alpha \in F(\sqrt[p]{a})$ and $\gamma \in F(\sqrt[p]{c})$ (see [Ser13, Chapter XIV, Proposition 4(iii)]) such that

$$Nm_{E/F(\sqrt[p]{c})}(\alpha) = b = Nm_{E/F(\sqrt[p]{a})}(\gamma)$$

Let G be the Galois group $Gal(E/F)$. Then $G = \langle \sigma_a, \sigma_c \rangle$ where $\sigma_a \in G$ (respectively $\sigma_c \in G$) is the restriction of $\sigma_a \in Gal(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F)$ (respectively $\sigma_c \in Gal(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F)$).

Our goal is to find an element $\delta \in E^\times$ such that the Galois closure of $E(\sqrt[p]{\delta})$ is our desired $\mathbb{U}_4(\mathbb{F}_p)$-extension of F. We define

$$C_0 = \prod_{i=0}^{p-2} \sigma_c^i(\gamma^{p-i-1}) \in F(\sqrt[p]{c}),$$

and define $B := \gamma/\alpha$. Then we have the following result which follow from Lemma 1.4.1.

Lemma 1.6.1. *We have*

(1) $\frac{\sigma_a(A_0)}{A_0} = Nm_{\sigma_c}(B)$.

(2) $\frac{\sigma_c(C_0)}{C_0} = Nm_{\sigma_a}(B)^{-1}$.

Proof. [MT15b] Using the Lemma 1.4.1, we have

$$\frac{\sigma_a(A_0)}{A_0} = \frac{b}{\alpha^p} = \frac{Nm_{\sigma_c}(\gamma)}{Nm_{\sigma_c}(\alpha)} = Nm_{\sigma_c}(B)$$

and

$$\frac{\sigma_c(C_0)}{C_0} = \frac{b}{\gamma^p} = \frac{Nm_{\sigma_a}(\alpha)}{Nm_{\sigma_a}(\gamma)} = Nm_{\sigma_a}(B)^{-1}$$

□

Lemma 1.6.2. *Assume that there exist $C_1, C_2 \in E^\times$ such that*

$$B = \frac{\sigma_a(C_1)}{C_1}\frac{C_2}{\sigma_c(C_2)}$$

Then $Nm_{\sigma_c}(C_1)/A_0$ and $Nm_{\sigma_a}(C_2)/C_0$ are in $F^\times$. Moreover, if we let

$$A = Nm_{\sigma_c}(C_1) \in F(\sqrt[p]{a})^\times$$

and

$$C = Nm_{\sigma_a}(C_2) \in F(\sqrt[p]{c})^\times,$$

then there exists $\delta \in E^\times$ *such that*

$$\frac{\sigma_c(\delta)}{\delta} = AC_1^{-p}$$
$$\frac{\sigma_a(\delta)}{\delta} = CC_2^{-p}$$

Proof. [MT15b] By lemma 1.6.1, and the fact that $Nm_{\sigma_c}(C_2) = Nm_{\sigma_c}(\sigma_c(C_2))$, we have

$$\frac{\sigma_a(A_0)}{A_0} = Nm_{\sigma_c}(B) = Nm_{\sigma_c}\Big(\frac{\sigma_a(C_1)}{C_1}\Big)Nm_{\sigma_c}\Big(\frac{C_2}{\sigma_c(C_2)}\Big) = \frac{\sigma_a(Nm_{\sigma_c}(C_1))}{Nm_{\sigma_c}(C_1)}.$$

This implies that

$$\frac{Nm_{\sigma_c}(C_1)}{A_0} = \sigma_a\Big(\frac{Nm_{\sigma_c}(C_1)}{A_0}\Big).$$

Because $\frac{Nm_{\sigma_c}(C_1)}{A_0}$ is fixed by both σ_a and σ_c, we have

$$\frac{Nm_{\sigma_c}(C_1)}{A_0} \in F(\sqrt[p]{c})^\times \cap F(\sqrt[p]{a})^\times = F^\times.$$

Using the same procedure, by the same lemma (lemma 1.6.1), we have

$$\frac{\sigma_c(C_0)}{C_0} = Nm_{\sigma_a}(B^{-1}) = Nm_{\sigma_a}\Big(\frac{C_1}{\sigma_a(C_1)}\Big)Nm_{\sigma_a}\Big(\frac{\sigma_c(C_2)}{C_2}\Big) = \frac{\sigma_c(Nm_{\sigma_a}(C_2))}{Nm_{\sigma_a}(C_2)}.$$

This implies that

$$\frac{Nm_{\sigma_a}(C_2)}{C_0} = \sigma_c\Big(\frac{Nm_{\sigma_a}(C_2)}{C_0}\Big).$$

Hence

$$\frac{Nm_{\sigma_a}(C_2)}{C_0} \in F(\sqrt[p]{a})^\times \cap F(\sqrt[p]{c})^\times = F^\times.$$

Clearly, one has

$$Nm_{\sigma_a}(CC_2^{-p}) = Nm_{\sigma_a}(C_2)^p Nm_{\sigma_a}(C_2)^{-p} = 1$$
$$Nm_{\sigma_c}(AC_1^{-p}) = Nm_{\sigma_c}(C_1)^p Nm_{\sigma_c}(C_1^{-p}) = 1.$$

We also have

$$\begin{aligned}\frac{\sigma_a(AC_1^{-p})}{AC_1^{-p}}\frac{CC_2^{-p}}{\sigma_c(CC_2^{-p})} &= \frac{\sigma_a(A)}{A}\Big(\frac{\sigma_a(C_1)}{C_1}\Big)^{-p}\frac{C}{\sigma_c(C)}\Big(\frac{C_2}{\sigma_c(C_2)}\Big)^{-p}\\ &= \frac{b}{\alpha^p}\frac{\gamma^p}{b}B^{-p}\\ &= 1.\end{aligned}$$

Hence, we have

$$\frac{\sigma_a(AC_1^{-p})}{AC_1^{-p}} = \frac{\sigma_c(CC_2^{-p})}{CC_2^{-p}}.$$

From [Con65, Page 756] (a variant of Hilbert's Theorem 90) we see that there exists $\delta \in E^\times$ such that

$$\frac{\sigma_c(\delta)}{\delta} = AC_1^{-p},$$
$$\frac{\sigma_a(\delta)}{\delta} = CC_2^{-p}.$$

□

The next lemma is used in order to apply lemma 1.6.2 in theorem 1.6.4. Furthermore, this lemma is used in Section 1.7.

Lemma 1.6.3. *There exists $e \in E^\times$ such that $B = \frac{\sigma_a\sigma_c(e)}{e}$. Furthermore, the following statements are true.*

(1) If we set $C_1 := \sigma_c(e) \in E^\times$, $C_2 = e^{-1} \in E^\times$, then $B = \frac{\sigma_a(C_1)}{C_1}\frac{C_2}{\sigma_c(C_2)}$.

(2) If we set $C_1 := e \in E^\times$, $C_2 := (eB)\sigma_c(eB)\cdots\sigma_c^{p-2}(eB) \in E^\times$, then $B = \frac{\sigma_a(C_1)}{C_1}\frac{C_2}{\sigma_c(C_2)}$.

Proof. [MT15b] We have

$$Nm_{\sigma_a\sigma_c}(B) = \frac{Nm_{\sigma_a\sigma_c}(\alpha)}{Nm_{\sigma_a\sigma_c}(\gamma)} = \frac{Nm_{\sigma_a}(\alpha)}{Nm_{\sigma_c}(\gamma)} = \frac{b}{b} = 1.$$

Hence by Hilbert's Theorem 90, there exists $e \in E^\times$ such that $B = \frac{\sigma_a\sigma_c(e)}{e}$.

In the first case, we have

$$\frac{\sigma_a(C_1)}{C_1}\frac{C_2}{\sigma_c(C_2)} = \frac{\sigma_a(\sigma_c(e))}{\sigma_c(e)}\frac{e^{-1}}{\sigma_c(e^{-1})} = \frac{\sigma_a\sigma_c(e)}{e} = B.$$

And in the second case, from $B = \frac{\sigma_a\sigma_c(e)}{e}$, we have $eB = \sigma_a\sigma_c(e)$. Therefore $\sigma_c^{p-1}(eB) = \sigma_a(e)$. Hence

$$B = \frac{\sigma_a(e)}{e}\frac{eB}{\sigma_c^{p-1}(eB)} = \frac{\sigma_a(C_1)}{C_1}\frac{C_2}{\sigma_c(C_2)}.$$

□

Theorem 1.6.4. *Let the notation and assumption be as in Lemma 1.6.2. Let $M := E(\sqrt[p]{\delta}, \sqrt[p]{A}, \sqrt[p]{C}, \sqrt[p]{b})$. Then M/F is a Galois extension, M contains $F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})$ and $Gal(M/F) \cong \mathbb{U}_4(\mathbb{F}_p)$.*

Proof. [MT15b] Let W be a $\mathbb{F}_p$-vector space in $E^\times/(E^\times)^p$ generated by $[b]_E, [A]_E, [C]_E$ and $[\delta]_E$. Here for any $x \neq 0$ in a field L, we denote $[x]_L$ the image of x in $L^\times/L^\times$. Since

$$\sigma_c(\delta) = \delta AC_1^{-p},$$
$$\sigma_a(\delta) = \delta CC_2^{-p},$$
$$\sigma_a(A) = A\frac{b}{\alpha^p} \quad \text{(by lemma 1.4.1)},$$
$$\sigma_c(C) = C\frac{b}{\gamma^p} \quad \text{(by lemma 1.4.1)},$$

we see that W is in fact an $\mathbb{F}_p[G]$-module where $G = Gal(E/F)$. Hence M/F is a Galois extension by Kummer theory.

Claim: $dim_{\mathbb{F}_p}(W) = 4$. Hence $[L : F] = [L : E][E : F] = p^4 p^2 = p^6$.

Proof of Claim: From our hypothesis that $dim_{\mathbb{F}_p}\langle [a]_F, [b]_F, [c]_F\rangle = 3$, we see that $\langle [b]_E\rangle \cong \mathbb{F}_p$.

Clearly $\langle [b]_E\rangle \subseteq W^G$. From the relation

$$[\sigma_a(A)]_E = [A]_E[b]_E$$

we see that $[A]_E$ is not in W^{σ_a}. Hence $dim_{\mathbb{F}_p}\langle [b]_E, [A]_E\rangle = 2$.

From the relation

$$[\sigma_c(C)]_E = [C]_E[b]_E,$$

we see that $[C]_E$ is not in W^{σ_c}. But we have $\langle [b]_E, [A]_E\rangle \subseteq W^{\sigma_c}$. Hence

$$dim_{\mathbb{F}_p}\langle [b]_E, [A]_E, [C]_E\rangle = 3.$$

Observe that the element $(\sigma_a - 1)(\sigma_c - 1)$ annihilates the $\mathbb{F}_p[G]-$ module $\langle [b]_E, [A]_E, [C]_E\rangle$, while

$$(\sigma_a - 1)(\sigma_c - 1)[\delta]_E = \frac{\sigma_a([A]_E)}{[A]_E} = [b]_E,$$

we see that

$$dim_{\mathbb{F}_p} W = dim_{\mathbb{F}_p}\langle [b]_E, [A]_E, [C]_E, [\delta]_E\rangle = 4.$$

Let $H^{a,b} = F(\sqrt[p]{a}, \sqrt[p]{A}, \sqrt[p]{b})$ and $H^{b,c} = F(\sqrt[p]{c}, \sqrt[p]{C}, \sqrt[p]{b})$. Let

$$N := H^{a,b}H^{b,c} = F(\sqrt[p]{a}, \sqrt[p]{c}, \sqrt[p]{b}, \sqrt[p]{A}, \sqrt[p]{C}) = E(\sqrt[p]{b}, \sqrt[p]{A}, \sqrt[p]{C}).$$

Then N/F is a Galois extension of order p^5. This is because $Gal(N/E)$ is dual to the $\mathbb{F}_p[G]-$submodule $\langle [b]_E, [A]_E, [C]_E\rangle$ via Kummer theory, and the proof of the claim above shows that

$$dim_{\mathbb{F}_p}\langle [b]_E, [A]_E, [C]_E\rangle = 3.$$

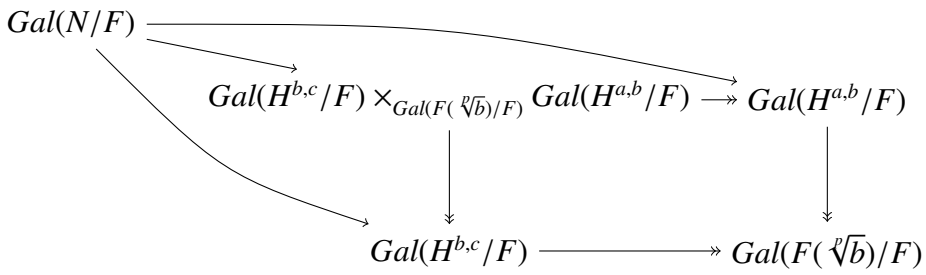
We have the following commutative diagram

$$\begin{array}{ccc} Gal(N/F) & \twoheadrightarrow & Gal(H^{a,b}/F) \\ \downarrow & & \downarrow \\ Gal(H^{b,c}/F) & \twoheadrightarrow & Gal(F(\sqrt[p]{b})/F) \end{array}$$

So we have a homomorphism η from $Gal(N/F)$ to the pull-back $Gal(H^{b,c}/F) \times_{Gal(F(\sqrt[p]{b})/F)} Gal(H^{a,b}/F)$:

$$\eta : Gal(N/F) \to Gal(H^{b,c}/F) \times_{Gal(F(\sqrt[p]{b})/F)} Gal(H^{a,b}/F)$$

which makes the following diagram commute.



We claim that η is injective. Indeed, let σ be an element in $ker(\eta)$. Then $\sigma|_{H^{a,b}} = 1$ in $Gal(H^{a,b}/F)$ and $\sigma|_{H^{b,c}} = 1$ in $Gal(H^{b,c}/F)$. Since N is the compositum of $H^{a,b}$ and $H^{b,c}$, this implies that $\sigma = 1$.

Since $|Gal(H^{b,c}/F) \times_{Gal(F(\sqrt[p]{b})/F)} Gal(H^{a,b}/F)| = p^5 = |Gal(N/F)|$, we see then η is an isomorphism. As in proof of Proposition 1.4.2 we can choose an extension $\sigma_a \in Gal(H^{a,b}/F)$ of $\sigma_a \in Gal(F(\sqrt[p]{a}, \sqrt[p]{b})/F)$ in such a way that

$$\sigma_a(\sqrt[p]{A}) = \sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha}.$$

Since the commutative diagram above is a pull-back, we can choose an extension $\sigma_a \in Gal(N/F)$ of $\sigma_a \in Gal(H^{a,b}/F)$ in such a way that

$$\sigma_a|_{H^{b,c}} = 1.$$

Now we can choose any extension $\sigma_a \in Gal(M/F)$ of $\sigma_a \in Gal(N/F)$. Then we have

$$\sigma_a(\sqrt[p]{A}) = \sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha} \text{ and } \sigma_a|_{H^{b,c}} = 1.$$

Similarly, we can choose an extension $\sigma_c \in Gal(M/F)$ of $\sigma_c \in Gal(F(\sqrt[p]{b}, \sqrt[p]{c})/F)$ in such a way that

$$\sigma_c(\sqrt[p]{C}) = \sqrt[p]{C}\frac{\sqrt[p]{b}}{\gamma} \text{ and } \sigma_c|_{H^{a,b}} = 1.$$

Claim: The order of σ_a is p.

Proof of claim. As in the proof of Proposition 1.4.2, we see that $\sigma_a^p(\sqrt[p]{A}) = \sqrt[p]{A}$. Since $\sigma_a(\delta) = \delta C C_2^{-p}$, we have $\sigma_a(\sqrt[p]{\delta}) = \zeta^i \sqrt[p]{\delta}\sqrt[p]{C}C_2^{-1}$ for some $i \in \mathbb{Z}$. This implies that

$$\begin{aligned}\sigma_a^2(\sqrt[p]{\delta}) &= \zeta^i \sigma_a(\sqrt[p]{\delta})\sigma_a(\sqrt[p]{C})\sigma_a(C_2^{-1}) \\ &= \zeta^{2i}\sqrt[p]{\delta}(\sqrt[p]{C})^2 C_2^{-1}\sigma_a(C_2^{-1}).\end{aligned}$$

Inductively we obtain

$$\begin{aligned}\sigma_a^p(\sqrt[p]{\delta}) &= \zeta^{pi}\sqrt[p]{\delta}(\sqrt[p]{C})^p Nm_{\sigma_a}(C_2)^{-1} \\ &= \sqrt[p]{\delta}\cdot(C)\cdot Nm_{\sigma_a}(C_2)^{-1} \\ &= \sqrt[p]{\delta}.\end{aligned}$$

Therefore, we can conclude that $\sigma_a^p = 1$ and σ_a is of order p.

Claim: The order of σ_c is p.

Proof of claim. As in the proof of Proposition 1.4.2, we see that $\sigma_c^p(\sqrt[p]{C}) = \sqrt[p]{C}$. Since $\sigma_c(\delta) = \delta A C_1^{-p}$, we have $\sigma_c(\sqrt[p]{\delta}) = \zeta^j \sqrt[p]{\delta}\sqrt[p]{A}C_1^{-1}$ for some $j \in \mathbb{Z}$. This implies that

$$\begin{aligned}\sigma_c^2(\sqrt[p]{\delta}) &= \zeta^j \sigma_c(\sqrt[p]{\delta})\sigma_c(\sqrt[p]{A})\sigma_c(C_1^{-1}) \\ &= \zeta^{2j}\sqrt[p]{\delta}(\sqrt[p]{A})^2 C_1^{-1}\sigma_a(C_1^{-1}).\end{aligned}$$

Inductively we obtain

$$\begin{aligned}\sigma_c^p(\sqrt[p]{\delta}) &= \zeta^{pj}\sqrt[p]{\delta}(\sqrt[p]{A})^p Nm_{\sigma_c}(C_1)^{-1} \\ &= \sqrt[p]{\delta}\cdot(A)\cdot Nm_{\sigma_c}(C_1)^{-1} \\ &= \sqrt[p]{\delta}.\end{aligned}$$

Therefore, we can conclude that $\sigma_a^p = 1$ and σ_a is of order p.

Claim: $[\sigma_a, \sigma_c] = 1$.

Proof of claim: It is enough to check that $\sigma_a\sigma_c(\sqrt[p]{\delta}) = \sigma_c\sigma_a(\sqrt[p]{\delta})$. We have

$$\begin{aligned}\sigma_a\sigma_c(\sqrt[p]{\delta}) &= \sigma_a(\zeta^j\sqrt[p]{\delta}\sqrt[p]{A}C_1^{-1}) \\ &= \zeta^j\sigma_a(\sqrt[p]{\delta})\sigma_a(\sqrt[p]{A})\sigma_a(C_1)^{-1} \\ &= \zeta^j\zeta^i\sqrt[p]{\delta}\sqrt[p]{C}C_2^{-1}\sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha}\sigma_a(C_1)^{-1} \\ &= \zeta^{i+j}\sqrt[p]{\delta}\sqrt[p]{C}\sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha}(\sigma_a(C_1)C_2)^{-1} \\ &= \zeta^{i+j}\sqrt[p]{\delta}\sqrt[p]{C}\sqrt[p]{A}\frac{\sqrt[p]{b}}{\alpha}\frac{(C_1\sigma_c(C_2))^{-1}}{B} \\ &= \zeta^{i+j}\sqrt[p]{\delta}\sqrt[p]{C}\sqrt[p]{A}\frac{\sqrt[p]{b}}{\gamma}(C_1\sigma_c(C_2))^{-1}.\end{aligned}$$

On the other hand, we have:

$$\begin{aligned}\sigma_c\sigma_a(\sqrt[p]{\delta}) &= \sigma_c(\zeta^i\sqrt[p]{\delta}\sqrt[p]{C}C_2^{-1}) \\ &= \zeta^i\sigma_c(\sqrt[p]{\delta})\sigma_c(\sqrt[p]{C})\sigma_c(C_2)^{-1} \\ &= \zeta^i\zeta^j\sqrt[p]{\delta}\sqrt[p]{A}C_1^{-1}\sqrt[p]{C}\frac{\sqrt[p]{b}}{\gamma}\sigma_c(C_2)^{-1} \\ &= \zeta^{i+j}\sqrt[p]{\delta}\sqrt[p]{A}\sqrt[p]{C}\frac{\sqrt[p]{b}}{\gamma}(C_1\sigma_a(C_2))^{-1}.\end{aligned}$$

Hence $\sigma_a\sigma_c(\sqrt[p]{\delta}) = \sigma_c\sigma_a(\sqrt[p]{\delta})$.

We define $\sigma_b \in Gal(M/K)$ to be the element which is dual to $[b]_E$ via Kummer theory. In other words, we require that

$$\sigma_b(\sqrt[p]{b}) = \zeta\sqrt[p]{b},$$

and σ_b acts trivially on $\sqrt[p]{A}$, $\sqrt[p]{C}$ and $\sqrt[p]{\delta}$. We consider σ_b as an element in $Gal(M/F)$ then it is clear that σ_b is an extension of $\sigma_b \in Gal(F(\sqrt[p]{a}, \sqrt[p]{b}, \sqrt[p]{c})/F)$.

Let $W^* = Gal(M/E)$, and let $H = Gal(M/F)$ then we have the following exact sequence

$$1 \to W^* \to H \to G \to 1.$$

By Kummer theory, W^* is dual to W, hence $W \cong (\mathbb{Z}/p\mathbb{Z})^4$. In particular, we have $|H| = p^6$.

Claim: $[\sigma_a, [\sigma_a, \sigma_b]] = [\sigma_b, [\sigma_a, \sigma_b]] = 1$.

Proof of claim. Since G is abelian, it follows that $[\sigma_a, \sigma_b]$ is in W^*. Hence

$$[\sigma_b, [\sigma_a, \sigma_b]] = 1.$$

To see $[\sigma_a, [\sigma_a, \sigma_b]] = 1$, observe Heisenberg group $\mathbb{U}_3(\mathbb{F}_p)$ is a nilpotent group of nilpotent length 2, we see that $[\sigma_a, [\sigma_a, \sigma_b]] = 1$ on $H^{a,b}$ and $H^{b,c}$. So it is enough to check that $[\sigma_a, [\sigma_a, \sigma_b]](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$.

By definition of σ_b, we see that

$$\sigma_b\sigma_a(\sqrt[p]{\delta}) = \sigma_a(\sqrt[p]{\delta}) = \sigma_a\sigma_b(\sqrt[p]{\delta}).$$

Hence $[\sigma_a, \sigma_b](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$. Since σ_a and σ_b act trivially on $\sqrt[p]{C}$, and σ_b acts trivially on E, we see that

$$[\sigma_a, \sigma_b](\sqrt[p]{C}) = \sqrt[p]{C}, \text{ and } [\sigma_a, \sigma_b](C_2^{-1}) = C_2^{-1}.$$

Hence,

$$\begin{aligned}
[\sigma_a, \sigma_b]\sigma_a(\sqrt[p]{\delta}) &= [\sigma_a, \sigma_b](\zeta^i\sqrt[p]{\delta}\sqrt[p]{C}C_2^{-1}) \\
&= \zeta^i[\sigma_a, \sigma_b](\sqrt[p]{\delta})[\sigma_a, \sigma_b](\sqrt[p]{C})[\sigma_a, \sigma_b](C_2)^{-1} \\
&= \zeta^i\sqrt[p]{\delta}\sqrt[p]{C}C_2^{-1} \\
&= \sigma_a(\sqrt[p]{\delta}) \\
&= \sigma_a[\sigma_a, \sigma_b](\sqrt[p]{\delta}).
\end{aligned}$$

Thus $[\sigma_a, [\sigma_a, \sigma_b]](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$.

Claim: $[\sigma_b, [\sigma_b, \sigma_c]] = [\sigma_c, [\sigma_b, \sigma_c]] = 1$.

Proof of claim. Since G is abelian, it follows that $[\sigma_b, \sigma_c]$ is in W^*. Hence

$$[\sigma_b, [\sigma_b, \sigma_c]] = 1.$$

To see $[\sigma_c, [\sigma_b, \sigma_c]] = 1$, observe that the Heisenberg group $\mathbb{U}_3(\mathbb{F}_p)$ is a nilpotent group of nilpotent length 2, we see that $[\sigma_c, [\sigma_b, \sigma_c]] = 1$ on $H^{a,b}$ and $H^{b,c}$. So it is enough to check that $[\sigma_c, [\sigma_b, \sigma_c]](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$.

By definition of σ_b, we see that

$$\sigma_b\sigma_c(\sqrt[p]{\delta}) = \sigma_c(\sqrt[p]{\delta}) = \sigma_c\sigma_b(\sqrt[p]{\delta}).$$

Hence $[\sigma_b, \sigma_c](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$. Since σ_b and σ_c act trivially on $\sqrt[p]{A}$, and σ_b acts trivially on E, we see that

$$[\sigma_b, \sigma_c](\sqrt[p]{A}) = \sqrt[p]{A}, \text{ and } [\sigma_b, \sigma_c](C_1^{-1}) = C_1^{-1}.$$

Hence,

$$\begin{aligned}
[\sigma_b, \sigma_c]\sigma_c(\sqrt[p]{\delta}) &= [\sigma_b, \sigma_c](\zeta^j \sqrt[p]{\delta}\sqrt[p]{A}C_1^{-1}) \\
&= \zeta^i[\sigma_b, \sigma_c](\sqrt[p]{\delta})[\sigma_b, \sigma_c](\sqrt[p]{A})[\sigma_b, \sigma_c](C_1)^{-1} \\
&= \zeta^j \sqrt[p]{\delta}\sqrt[p]{A}C_1^{-1} \\
&= \sigma_c(\sqrt[p]{\delta}) \\
&= \sigma_c[\sigma_b, \sigma_c](\sqrt[p]{\delta}).
\end{aligned}$$

Thus $[\sigma_c, [\sigma_b, \sigma_c]](\sqrt[p]{\delta}) = \sqrt[p]{\delta}$.

Claim: $[[\sigma_a, \sigma_b], [\sigma_b, \sigma_c]] = 1$.

Proof of claim. Since G is abelian, $[\sigma_a, \sigma_b]$ and $[\sigma_b, \sigma_c]$ are in W^*. Hence $[[\sigma_a, \sigma_b], [\sigma_b, \sigma_c]] = 1$ because W^* is abelian.

Since σ_a, σ_b and σ_c generate $Gal(M/F)$ and $|Gal(M/F)| = p^6$, we see that $Gal(M/F) \cong \mathbb{U}_4(\mathbb{F}_p)$ by [BD01, Theorem 1].

An explicit isomorphism $\varphi : Gal(M/F) \to \mathbb{U}_4(\mathbb{F}_p)$ may be defined as

$$\sigma_a \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_b \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_c \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

$\square$

1.7 Explicit form of $U_4(\mathbb{F}_2)$−Extensions

Let the notation and assumption be as in Lemma 1.6.2. Let us consider the case $p = 2$ [MT15b]. In Lemma 1.6.3, we can choose $e = \frac{\alpha}{\alpha+\gamma}$. (Observe that $\alpha + \gamma \neq 0$.) Since $\alpha\overline{\alpha} = \gamma\overline{\gamma} = b$ where $\overline{\alpha} = \sigma_a(\alpha)$ and $\overline{\gamma} = \sigma_c(\gamma)$, we have

$$\begin{aligned}\sigma_a\sigma_c(\frac{\alpha}{\alpha+\gamma}) &= \frac{\overline{\alpha}}{\overline{\alpha}+\overline{\gamma}}\\ &= \frac{1}{1+\overline{\gamma}/\overline{\alpha}}\\ &= \frac{1}{1+\alpha/\gamma}\\ &= \frac{\gamma}{\alpha+\gamma}\\ &= \frac{\gamma}{\alpha}\frac{\alpha}{\alpha+\gamma}.\end{aligned}$$

If we choose $C_1 = \sigma_c(e)$ and $C_2 = e^{-1}$, then by Lemma 1.6.3 part (1), we have

$$A = Nm_{\sigma_c}(C_1) = Nm_{\sigma_c}(\sigma_c(e)) = Nm_{\sigma_c}(e) = \frac{\alpha^2\gamma}{(\alpha+\gamma)(\alpha\gamma+b)},$$

$$C = Nm_{\sigma_a}(C_2) = Nm_{\sigma_a}(e^{-1}) = \frac{(\alpha+\gamma)(\alpha\gamma+b)}{b\alpha}.$$

In Lemma 1.6.2, we can choose $\delta = e^{-1} = \frac{\alpha+\gamma}{\alpha}$. In fact, we have

$$\frac{\sigma_c(\delta)}{\delta} = \sigma_c(e)^{-1}e = \sigma_c(e)^{-2}e\sigma_c(e) = C_1^{-2}Nm_{\sigma_c}(e) = AC_1^{-2},$$

$$\frac{\sigma_a(\delta)}{\delta} = \sigma_a(e)^{-1}e = e^{-1}\sigma_a(e)^{-1}e^2 = Nm_{\sigma_a}(e^{-1}) = CC_2^{-2}.$$

Therefore

$$\begin{aligned}M &= F(\sqrt{b}, \sqrt{A}, \sqrt{C}, \sqrt{\delta})\\ &= F(\sqrt{b}, \sqrt{\frac{\alpha^2\gamma}{(\alpha+\gamma)(\alpha\gamma+b)}}, \sqrt{\frac{(\alpha+\gamma)(\alpha\gamma+b)}{b\alpha}}, \sqrt{\frac{\alpha+\gamma}{\alpha}})\\ &= F(\sqrt{b}, \sqrt{\frac{\alpha+\gamma}{\alpha}}, \sqrt{(\alpha\gamma+b)}, \sqrt{\alpha\gamma}).\end{aligned}$$

Now by Lemma 1.6.3 part (2), if we choose $C_1 = e = \frac{\alpha}{\alpha+\gamma}$ and $C_2 = eB = \frac{\gamma}{\alpha+\gamma}$, then we have

$$A = Nm_{\sigma_c}(C_1) = Nm_{\sigma_c}(e) = \frac{\alpha^2\gamma}{(\alpha+\gamma)(\alpha\gamma+b)},$$

$$C = Nm_{\sigma_a}(C_2) = Nm_{\sigma_a}(eB) = \frac{\alpha\gamma^2}{(\alpha+\gamma)(\alpha\gamma+b)}.$$

In Lemma 1.6.2, we choose $\delta = (\alpha+\gamma)^{-1}$. In fact, we have

$$\frac{\sigma_c(\delta)}{\delta} = \frac{\gamma(\alpha+\gamma)}{\alpha\gamma+b} = AC_1^{-2},$$

$$\frac{\sigma_a(\delta)}{\delta} = \frac{\alpha(\alpha+\gamma)}{\alpha\gamma+b} = CC_2^{-2}.$$

Therefore

$$M = F(\sqrt{b}, \sqrt{A}, \sqrt{C}, \sqrt{\delta}) = F(\sqrt{b}, \sqrt{\frac{\alpha^2\gamma}{\alpha\gamma+b}}, \sqrt{\frac{\alpha\gamma^2}{\alpha\gamma+b}}, \sqrt{\alpha+\gamma}).$$

Observe also that M is the Galois closure of $E(\sqrt{\delta}) = F(\sqrt{a}, \sqrt{c}, \sqrt{\alpha+\gamma})$.

1.8 Kummer theory and local class field theory

1.8.1 Abelian Kummer theory

Let K be a field containing an $n-$th root of unity. Let L/K be a Galois extension which is abelian of exponent n i.e. for all $\sigma \in Gal(L/K)$ we have $\sigma^n = id_L$ then $L = K(\sqrt[n]{W})$ for some subgroup $K^{\times n} \subset W \subset K^\times$. In particular Kummer theory tells us that within a fixed algebraic closure there is a bijection

$$\{W | K^{\times n} \subset W \subset K^\times\} \rightleftharpoons \{L/K \text{ abelian of exponent } n \text{ inside } \overline{K}\}$$

where the bijection is given by

$$W \mapsto K(\sqrt[n]{W})$$

and

$$(L^\times)^n \cap K^\times \hookleftarrow L.$$

In this case if W is a subgroup of $K^\times$ corresponding to L/K by above correspondence, we have a perfect pairing

$$\begin{aligned} Gal(L/K) \times W/K^{\times n} &\to \langle \zeta_n \rangle \\ (\sigma, a) &\mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}. \end{aligned}$$

To see the proof of the above facts, see [Jac64, Chapter III, Theorem 7 and Theorem 8] or [Lan13, Theorem 8.1 and Theorem 8.2].

When we deal with abelian extensions of exponent p equal to the characteristic, then we have to develop an additive theory.

If K is a field, we define an operator $\wp$ by

$$\wp(x) = x^p - x$$

for $x \in K$. Then $\wp$ is an additive homomorphism of K into itself. The subgroup $\wp(K)$ plays the same role as the subgroup $K^{\times p}$ in multiplicative theory, whenever p is a prime number.

Now we assume K has characteristic p. A root of polynomial $X^p - X - a$ with $a \in K$ will be denoted by $\wp^{-1}(a)$. If B is a subgroup of K containing $\wp(K)$ we let $L_B = K(\wp^{-1}(B))$ be the field obtained by adjoining $\wp^{-1}(a)$ to K for all $a \in B$. We emphasize the fact that B is an additive subgroup of K.

In this case, the map $B \mapsto K(\wp^{-1}(B))$ is a bijection between the subgroups of K containing $\wp(K)$ and abelian extensions of K of exponent p. Let $L = L_B = K(\wp^{-1}(B))$, and let G be its Galois group. If $\sigma \in G$ and $a \in B$ and $\wp(\alpha) = a$, let $\langle \sigma, a \rangle = \sigma(\alpha) - \alpha$. Then we have a bilinear map

$$G \times B \to \mathbb{Z}/p\mathbb{Z}$$

given by

$$(\sigma, a) \mapsto \langle \sigma, a \rangle.$$

The kernel on the left is 1 and the kernel on the right is $\wp(K)$. The extension L/K is finite if and only if $[B : \wp(K)]$ is finite and if that is the case then

$$[L : K] = [B : \wp(K)].$$

For proof see [Lan13, Theorem 8.3].

1.8.2 Local class field theory

In characteristic zero, a local field is either $\mathbb{C}$ or $\mathbb{R}$ or a complete discrete valued field with a finite residue field. In characteristic $p > 0$, they are formal power series in one variable with coefficient in a finite field.

Now Let K be a local field and K^{ab} be the maximal abelian extensions of K in a fixed separable closure of K. Local class field theory says that there is a homomorphism

$$\theta : K^{\times} \to Gal(K^{ab}/K)$$

called the local Artin homomorphism that induces an isomorphism of topological groups

$$\hat{K}^{\times} \to Gal(K^{ab}/K)$$

where

$$\hat{K}^{\times} = \varprojlim K^{\times}/U$$

with U ranges over the finite index open normal subgroups of the group $K^{\times}$.

Let L be a finite extension of K. Let $Nm_{L/K} : L^{\times} \to K^{\times}$ be the norm map. Let θ_L and θ_K be the local Artin homomorphism associated to L and K, respectively. Let

$$res : Gal(L^{ab}/L) \to Gal(K^{ab}/K)$$

be the homomorphism mapping an automorphism σ of L^{ab} to its restriction $\sigma|_{K^{ab}}$. Then the following diagram commutes.

$$\begin{array}{ccc} L^\times & \xrightarrow{\theta_L} & Gal(L^{ab}/L) \\ \downarrow{\scriptstyle Nm_{L/K}} & & \downarrow{\scriptstyle res} \\ K^\times & \xrightarrow{\theta_K} & Gal(K^{ab}/K) \end{array}$$

Now let L be a finite abelian extension of K in a fixed separable closure of K. The subgroup $Nm_{L/K}$ of the group $K^\times$ corresponds to the subgroup $Gal(L/K)$ of the group $Gal(K^{ab}/K)$. Also the composition

$$K^\times \to Gal(K^{ab}/K) \overset{res}{\twoheadrightarrow} Gal(L/K)$$

is surjective with kernel $Nm_{L/K}(L^\times)$.

The precise definition of θ and the proof of the above facts can be found in [Sha72, Chapter V] and [CF67, Chapter VI].

Chapter 2

Dihedral Extensions over Rational p-adic Fields

Let $\mathbb{Q}_p$ be the rational p-adic field for a prime p. It is well-known that there exist only finitely many extensions of a fixed degree over $\mathbb{Q}_p$ in a fixed algebraic closure of $\mathbb{Q}_p$ [Wei95, p. 208]. Yamagishi [Yam95] computed the number of extensions K over a finite extension $k/\mathbb{Q}_p$ whose Galois group $Gal(K/k)$ is isomorphic to a fixed finite p-group.

In this chapter, I will exhibit all extensions M over $\mathbb{Q}_p$ whose Galois group is isomorphic to the dihedral group D_4 of order 8 [Nai95]. We will see that there exists no such extension for $p \equiv 1 \pmod 4$, one extension for $p \equiv 3 \pmod 4$ and 18 extensions for $p = 2$.

Definition 2.0.1. *Let K be a field of characteristic not 2, and let $a, b \in K^\times$. We define quaternion algebra (a, b) to be the $K-$algebra on two generators i, j with defining relations*

$$i^2 = a,\ j^2 = b,\ \text{and } ij = -ji$$

2.1 Non-dyadic fields

It is known that there is a D_4-extension of field K with $char(K) \neq 2$ if and only if there are $a, b \in K$, which are independent modulo squares, such that quaternion algebra (a, b) is split [MS90, Theorem 1.6]. When $p \equiv 3 \pmod 4$, then -1 is not square and by [Lam05, Theorem 2.2], the only split quaternion algebra, in the form (a, b) where a and b are linearly independent, is $(p, -p)$. Hence for $p \equiv 3 \pmod 4$ there is just one dihedral extension of $\mathbb{Q}_p$.

When $p \equiv 1 \pmod 4$, again by [Lam05, Theorem 2.2], there is a $u \in \mathbb{Z}_p$ such that u is not square and (u, p) is non-split quaternion algebra and there is no split quaternion algebra (a, b) where a and b are linearly independent module squares in this case. Hence for $p \equiv 1 \pmod 4$ there is no dihedral extension of $\mathbb{Q}_p$.

Also the following is an alternative proof for $p \neq 2$ using W-groups. Let K be a field with $char(K) \neq 2$. Define

$$K^{(2)} = K(\sqrt{a} : a \in K^\times),$$

also define

$$\mathcal{E} = \{y \in K^{(2)} : K^{(2)}(\sqrt{y})/K \quad \text{is Galois}\}$$

and

$$K^{(3)} = K(\sqrt{y} : y \in \mathcal{E}).$$

It is known that $Gal(K^{(2)}/K) \cong \prod_{i\in I} \mathbb{Z}/2\mathbb{Z}$, where I is smallest index set with $\{a_i \in K : i \in I\}$, is a basis of $K^\times/K^{\times 2}$. The field $K^{(3)}$ is called the *Witt Closure* of K and the group $Gal(K^{(3)}/K)$ is called the W-group. Observe that all D_4-extensions of K are subfields of $K^{(3)}$ and by [MS96, Example 4.2 and 4.3], we have

$$Gal(\mathbb{Q}_p^{(3)}/\mathbb{Q}_p) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \qquad \text{when} \qquad p \equiv 1(\text{mod } 4)$$

and

$$Gal(\mathbb{Q}_p^{(3)}/\mathbb{Q}_p) \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} \qquad \text{when} \qquad p \equiv 3(\text{mod } 4)$$

where $\sigma_1\sigma_2\sigma_1^{-1} = \sigma_2^{-1}$ is the action in the latter case. Observe that there is no subgroup of $Gal(\mathbb{Q}_p^{(3)}/\mathbb{Q}_p)$ that is isomorphic to D_4 for $p \equiv 1(\text{mod } 4)$ and there is exactly one subgroup for $p \equiv 3(\text{mod } 4)$.

And second alternative proof from [Nai95] is the following. Let $M/\mathbb{Q}_p$ be a D_4-extension. $M/\mathbb{Q}_p$ has four intermediate fields N_1, N_1', N_2 and N_2' of degree 4 which are not Galois extensions over $\mathbb{Q}_p$.

We see they are totally and tamely ramified: totally ramified because $\|\cdot\|_{\mathfrak{p}} = |Nm(\cdot)|_p^{1/4}$ which corresponds to decomposition of p in these degree 4 extensions as $p = \mathfrak{p}^4$ and tamely ramified because p is an odd prime. We see by Serre [Ser78] that $\mathbb{Q}_p$ has four totally and tamely ramified extensions of degree 4. Therefore we see that $\mathbb{Q}_p$ has at most one D_4-extension.

In the case $p \equiv 1 \pmod 4$, then -1 is square in $\mathbb{Q}_p$. So we see that $\mathbb{Q}_p$ has no D_4-extension, because $\mathbb{Q}_p(\sqrt[4]{p})/\mathbb{Q}_p$ is a totally and tamely ramified Galois extension of degree 4. Also $Gal(\mathbb{Q}_p(\sqrt[4]{p})/\mathbb{Q}_p)$ is a cyclic group of order 4. Because there is no cyclic quotient of order 4 in dihedral group of order 8, therefore, there is no D_4-extension like $M/\mathbb{Q}_p$ such that $\mathbb{Q}_p(\sqrt[4]{p}) \subset M$. In the case $p \equiv 3 \pmod 4$, we see that $\mathbb{Q}_p(\sqrt{-1}, \sqrt[4]{p})$ is the only D_4-extension over $\mathbb{Q}_p$.

2.2 Dyadic fields

Let $M/\mathbb{Q}_2$ be Galois extension of degree 8. We know that the Galois group of $M/\mathbb{Q}_2$ is isomorphic to D_4 if and only if M contains an intermediate field of degree 4 which is not a Galois extension over $\mathbb{Q}_2$.

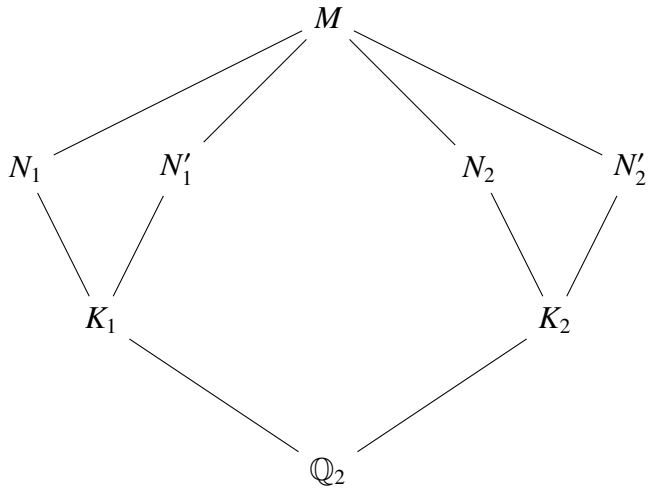
Let K be a quadratic extension over $\mathbb{Q}_2$ such that M/K is a cyclic extension of degree 4. Also assume K_1 and K_2 are two other quadratic extensions over $\mathbb{Q}_p$. It is sufficient to construct all quadratic extensions over K_1 and K_2 which are not Galois extensions over $\mathbb{Q}_2$.

2.2.1 Construction method

For every K_i with $i = 1, 2$ we can generate two quadratic extensions N_i and N_i' such that $N_i/\mathbb{Q}_2$ and $N_i'/\mathbb{Q}_2$ are non-Galois extensions of $\mathbb{Q}_2$ as follows:

We get $N_i = K_i(\sqrt{\epsilon})$ and $N_i' = K_i(\sqrt{\epsilon^\sigma})$ for an $\epsilon \in K_i^\times$ such that $\epsilon^\sigma/\epsilon \notin K_i^{\times 2}$ where σ is the generator of the Galois group $K_i/\mathbb{Q}_2$.

So $M = K_i(\sqrt{\epsilon}, \sqrt{\epsilon^\sigma})$. Now examine a representative system of $K_i^\times/K_i^{\times 2}$. Take all pairs $(\epsilon,\epsilon^\sigma)$ of the system such that $\epsilon \not\equiv \epsilon^\sigma \bmod K_i^{\times 2}$. By putting $M = K_i(\sqrt{\epsilon}, \sqrt{\epsilon^\sigma})$, we get all D_4-extensions $M/\mathbb{Q}_2$.



Lemma 2.2.1. *(1) 2-adic unit x is square in $\mathbb{Q}_2$ if and only if $x \equiv 1$ mod 8,*

(2) The set $\{-1, 2, 5\}$ forms a $\mathbb{F}_2$-basis for $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.

(3) The unique quaternion division algebra is $(-1, -1) = (2, 5)$.

Proof. [Lam05, Corollary 2.24] □

So by the above Lemma, all quadratic extensions over $\mathbb{Q}_2$ are

$$\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{5}), \mathbb{Q}_2(\sqrt{-5}), \mathbb{Q}_2(\sqrt{2}), \mathbb{Q}_2(\sqrt{-2}), \mathbb{Q}_2(\sqrt{10}), \mathbb{Q}_2(\sqrt{-10})$$

Part One: $m = \pm 2$ and ± 10:

Let $K_i = \mathbb{Q}_2(\sqrt{m})$ for $m = \pm 2$ or ± 10. In this case, we have $\mathfrak{p} = (\sqrt{m})$ is the prime ideal of K_i which lies over 2 . Also observe $\mathfrak{p}^5 = 4\mathfrak{p}$ and by [Lam05, Theorem 2.19], all elements of $1 + \mathfrak{p}^5$ are squares in K_i. Therefore we get

$$\frac{K_i^\times}{K_i^{\times 2}} \cong \frac{(\sqrt{m})}{(m)} \times \frac{O^\times}{(1 + m + 2\sqrt{m}, 1 + \mathfrak{p}^5)}$$

where $1 + m + 2\sqrt{m} = (1 + \sqrt{m})^2$. Observe there is a natural isomorphism $K_i \cong (\sqrt{m}) \times O^\times$ and we have $K_i^\times / K_i^{\times 2} \cong (\sqrt{m})/(m) \times O^\times / O^{\times 2}$. On the other hand there is a surjective map

$$\frac{O^\times}{O^{\times 2}} \to \frac{O^\times}{(1 + m + 2\sqrt{m}, 1 + \mathfrak{p}^5)}$$

and since the size of the left hand side is equal to the size of the right hand side (by following lemma), we have

$$\frac{O^\times}{O^{\times 2}} \cong \frac{O^\times}{(1 + m + 2\sqrt{m}, 1 + \mathfrak{p}^5)}.$$

Lemma 2.2.2. *If K is a finite extension of degree n over $\mathbb{Q}_2$, then $|K^\times / K^{\times 2}| = 2^{n+2}$.*

Proof. [Lam05, Corollary 2.23]. □

So,

$$|\frac{K_i^\times}{K_i^{\times 2}}| = 2^4 \quad \text{and} \quad |\frac{(\sqrt{m})}{(m)} \times \frac{O^\times}{(1 + m + 2\sqrt{m}, 1 + \mathfrak{p}^5)}| = 2 \times 2 \times 4 = 2^4.$$

Also for any $x \in O^\times$, write $x^{-1} = a' + b'\sqrt{m}$, and choose $a \equiv a'(mod 8)$ and $b \equiv b'(mod 4)$. Then it is easy to see that $x(a + b\sqrt{m}) \in 1 + 8O + 4\mathfrak{p} \subseteq O^2$ (since $1 + 8O \subseteq (O^\times)^2$). So

$$x + y\sqrt{m} \equiv x' + y'\sqrt{m} \pmod{\mathfrak{p}^5} \quad \Leftrightarrow \quad x \equiv x' \pmod 8 \text{ and } y \equiv y' \pmod 4$$

Hence, for constructing D_4-extensions, it is sufficient to examine elements ϵ and $\epsilon\sqrt{m}$ where $\epsilon = a + b\sqrt{m}$ for $a = 1, 2, 3, 4, 5, 6, 7, 8$ and $b = 0, 1, 2, 3$. But when a is even we can replace ϵ by $\epsilon\sqrt{m}/2$; therefore it is enough to check for $a = 1, 3, 5, 7$ and $b = 0, 1, 2, 3$. We take ϵ such that

1) ϵ
2) ϵ^σ
3) $\epsilon(1 + m + 2\sqrt{m})$
4) $\epsilon^\sigma(1 + m + 2\sqrt{m})$

are different modulo $\mathfrak{p}^5$ from each other and take $\epsilon\sqrt{m}$, such that

1) ϵ
2) $-\epsilon^\sigma$
3) $\epsilon(1 + m + 2\sqrt{m})$
4) $-\epsilon^\sigma(1 + m + 2\sqrt{m})$

are different modulo $\mathfrak{p}^5$ from each other, for number 2) and 4) we use the fact that $(\epsilon\sqrt{m})^\sigma = -\epsilon^\sigma\sqrt{m}$. Then we get D_4-extensions as follows:

$$
\begin{aligned}
A_1 =&\{\mathbb{Q}_2(\sqrt{1+\sqrt{2}},\sqrt{-1}),\mathbb{Q}_2(\sqrt{3+\sqrt{2}},\sqrt{-1}),\\
&\mathbb{Q}_2(\sqrt{\sqrt{2}},\sqrt{-1}),\mathbb{Q}_2(\sqrt{3\sqrt{2}},\sqrt{-1})\}\\
A_2 =&\{\mathbb{Q}_2(\sqrt{\sqrt{-2}},\sqrt{-1}),\mathbb{Q}_2(\sqrt{3\sqrt{-2}},\sqrt{-1})\}\\
B_1 =&\{\mathbb{Q}_2(\sqrt{1+\sqrt{-2}},\sqrt{-5}),\mathbb{Q}_2(\sqrt{5+\sqrt{-2}},\sqrt{-5}),\}\\
C_1 =&\{\mathbb{Q}_2(\sqrt{\sqrt{-2}(1+\sqrt{-2})},\sqrt{5}),\mathbb{Q}_2(\sqrt{\sqrt{-2}(1+3\sqrt{-2})},\sqrt{5}),\}\\
C_2 =&\{\mathbb{Q}_2(\sqrt{\sqrt{-10}(1+\sqrt{-10})},\sqrt{5}),\mathbb{Q}_2(\sqrt{\sqrt{-10}(1+3\sqrt{-10})},\sqrt{5}),\}\\
D_1 =&\{\mathbb{Q}_2(\sqrt{1+\sqrt{10}},\sqrt{-1}),\mathbb{Q}_2(\sqrt{3+\sqrt{10}},\sqrt{-1}),\\
&\mathbb{Q}_2(\sqrt{\sqrt{10}},\sqrt{-1}),\mathbb{Q}_2(\sqrt{3\sqrt{10}},\sqrt{-1})\}\\
D_2 =&\{\mathbb{Q}_2(\sqrt{\sqrt{-10}},\sqrt{-1}),\mathbb{Q}_2(\sqrt{3\sqrt{-10}},\sqrt{-1})\}\\
E_1 =&\{\mathbb{Q}_2(\sqrt{1+\sqrt{-10}},\sqrt{-5}),\mathbb{Q}_2(\sqrt{5+\sqrt{-10}},\sqrt{-5}),\}
\end{aligned}
$$

To check that the above method (Naito's method) gives us distinct D_4-extensions in each set, we can use the following method.

We begin with a biquadratic extension $\mathbb{Q}_2(\sqrt{a},\sqrt{b})$ of order 4 over $\mathbb{Q}$. Let $M_1=\mathbb{Q}_2(\sqrt{\alpha_1},\sqrt{b})$ and $M_2=\mathbb{Q}_2(\sqrt{\alpha_2},\sqrt{b})$ be two extensions in the above list where α_1 and α_2 are in $\mathbb{Q}_2(\sqrt{a})$ and

$$Nm_{\mathbb{Q}_2(\sqrt{a})/\mathbb{Q}_2}\left(\frac{\alpha_1}{\alpha_2}\right)\in\mathbb{Q}_2^2.$$

We will show that α_1 and α_2 are not in the same square class, i.e. α_1/α_2 is not square in $E:=\mathbb{Q}_2(\sqrt{a},\sqrt{b})$. Hence M_1 and M_2 are distinct.

In set A_1, let $M_1=\mathbb{Q}_2(\sqrt{1+\sqrt{2}},\sqrt{-1})$ and $M_2=\mathbb{Q}_2(\sqrt{3+\sqrt{2}},\sqrt{-1})$. Since $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(1+\sqrt{2})=-1$ and $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(3+\sqrt{2})=7$, we have

$$Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\frac{\sqrt{-7}(1+\sqrt{2})}{3+\sqrt{2}})=1.$$

Note that $-7\equiv 1 \pmod 8$ and so -7 is square in $\mathbb{Q}_2$. Now, by an explicit version of Hilbert 90 for quadratic extensions we can find a relation between $1+\sqrt{2}$ and $\frac{3+\sqrt{2}}{\sqrt{-7}}$ modulo squares in $E=\mathbb{Q}_2(\sqrt{-1},\sqrt{2})$.

Let

$$t = \frac{\sqrt{-7}(1 + \sqrt{2})}{3 + \sqrt{2}}$$

and

$$l = t + 1 = \frac{(3 + \sqrt{-7}) + (1 + \sqrt{-7})\sqrt{2}}{3 + \sqrt{2}}.$$

Now assume $1 \neq \sigma \in Gal(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)$, so we have

$$\begin{aligned} \sigma(l) &= \sigma(t + 1) \\ &= \sigma(t) + 1 \\ &= \sigma(t) + t\sigma(t) \\ &= (t + 1)\sigma(t) = l\sigma(t). \end{aligned} \tag{2.1}$$

Therefore

$$\frac{\sigma(l)}{l} = \sigma(t)$$

and by applying σ on both sides we have

$$\frac{l}{\sigma(l)} = t.$$

Hence

$$t = \frac{l^2}{Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(l)}.$$

So in the above case,

$$t = \frac{\sqrt{-7}(1 + \sqrt{2})}{3 + \sqrt{2}} = \left(\frac{(3 + \sqrt{-7}) + (1 + \sqrt{-7})\sqrt{2}}{3 + \sqrt{2}}\right)^2 \frac{1}{2 + \frac{2}{\sqrt{-7}}}$$

and since $\frac{1}{\sqrt{-7}(2+\frac{2}{\sqrt{-7}})} = 2^{-3} + 2^{-2} + 1 + 2 + 2^3 + \cdots \in \mathbb{Q}_2$, we have

$$\frac{1}{\sqrt{-7}(2 + \frac{2}{\sqrt{-7}})} \notin E^2 \cap \mathbb{Q}_2 = \mathbb{Q}_2^2 \cup (2)\mathbb{Q}_2^2 \cup (-1)\mathbb{Q}_2^2 \cup (-2)\mathbb{Q}_2^2.$$

Hence $1 + \sqrt{2}$ and $3 + \sqrt{2}$ are not in the same square class of E, and $M_1 \neq M_2$.

Let $M_3 = \mathbb{Q}_2(\sqrt{\sqrt{2}}, \sqrt{-1})$ and $M_4 = \mathbb{Q}_2(\sqrt{3\sqrt{2}}, \sqrt{-1})$. For M_3 and M_4 we have E as above and

$$\frac{Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\sqrt{2})}{Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(3\sqrt{2})} \in \mathbb{Q}_2^2.$$

So, $3\sqrt{2}/\sqrt{2} = 3 \notin E^2$ implies $M_3 \neq M_4$.

For the last step in A_1, we need to check M_1 and $M_2 \notin \{M_3, M_4\}$. $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(1+\sqrt{2})$ and $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(3+\sqrt{2})$ are in the square class of -1 denoted by $[-1]$ in $\mathbb{Q}_2$, and $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\sqrt{2})$ and $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(3\sqrt{2})$ are in the square class of $[-2]$ in $\mathbb{Q}_2$. Also since $[-1] \neq [-2]$ in $\mathbb{Q}_2$, we have M_1 and $M_2 \notin \{M_3, M_4\}$.

For A_2, we have $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(\sqrt{-2}) = 2$ and $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(3\sqrt{-2}) = 18$, and $[2] = [18]$ in $\mathbb{Q}_2$. So $3\sqrt{-2}/\sqrt{-2} = 3 \notin E^2 = \mathbb{Q}_2(\sqrt{-2}, \sqrt{-1})^2$ implies

$$\mathbb{Q}_2(\sqrt{\sqrt{-2}}, \sqrt{-1}) \neq \mathbb{Q}_2(\sqrt{3\sqrt{-2}}, \sqrt{-1}).$$

In B_1, we have $E = \mathbb{Q}_2(\sqrt{-2}, \sqrt{-5})$ and $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(1+\sqrt{-2}) = 3$ as well as $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(5+\sqrt{-2}) = 27$. Also we have $[3] = [27] = [-5]$ in $\mathbb{Q}_2$. So we need to use the explicit version of Hilbert 90 for quadratic extensions to find a relation between $1+\sqrt{-2}$ and $5+\sqrt{-2}$.

Let

$$t = \frac{3(1+\sqrt{-2})}{5+\sqrt{-2}} \quad \text{and} \quad l = t+1 = \frac{8+4\sqrt{-2}}{5+\sqrt{-2}}.$$

Therefore

$$\frac{3(1+\sqrt{-2})}{5+\sqrt{-2}} = t = \frac{l^2}{Nm(l)} = \left(\frac{8+4\sqrt{-2}}{5+\sqrt{-2}}\right)^2 \frac{32}{9}.$$

This concludes $(1+\sqrt{-2})/(5+\sqrt{-2}) = 6e^2$ where $e \in E$. Since $6 \notin E^2 \cap \mathbb{Q}_2$, $1+\sqrt{-2}$ and $5+\sqrt{-2}$ are in different square classes of E. Hence

$$\mathbb{Q}_2(\sqrt{1+\sqrt{-2}}, \sqrt{-5}) \neq \mathbb{Q}_2(\sqrt{5+\sqrt{-2}}, \sqrt{-5}).$$

In C_1, we have $E = \mathbb{Q}_2(\sqrt{-2}, \sqrt{5})$ and $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(\sqrt{-2}(1+\sqrt{-2})) = 6$ as well as $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(\sqrt{-2}(1+3\sqrt{-2})) = 38$. Also we have $[6] = [38] = [-10] = [-2][5]$ in $\mathbb{Q}_2$. So we need to use the explicit version of Hilbert 90 for quadratic extensions to find a relation between $\sqrt{-2}(1+\sqrt{-2})$ and $\sqrt{-2}(1+3\sqrt{-2})$.

Let

$$t = \sqrt{\frac{19}{3}}\left(\frac{1+\sqrt{-2}}{1+3\sqrt{-2}}\right) \quad \text{and} \quad l = t+1 = \frac{(1+\sqrt{19/3})+(3+\sqrt{19/3})\sqrt{-2}}{1+3\sqrt{-2}}.$$

Therefore

$$\sqrt{\frac{19}{3}}\left(\frac{1+\sqrt{-2}}{1+3\sqrt{-2}}\right) = t = \frac{l^2}{Nm(l)} = \left(\frac{(1+\sqrt{19/3})+(3+\sqrt{19/3})\sqrt{-2}}{1+3\sqrt{-2}}\right)^2 \frac{1}{2+\frac{14}{19}\sqrt{\frac{19}{3}}}.$$

This concludes

$$\frac{\sqrt{-2}(1+\sqrt{-2})}{\sqrt{-2}(1+3\sqrt{-2})} = \frac{1}{\sqrt{\frac{19}{3}}\left(2+\frac{14}{19}\sqrt{\frac{19}{3}}\right)}e^2$$

where $e \in E$. Since

$$\left[\frac{1}{\sqrt{\frac{19}{3}}\left(2+\frac{14}{19}\sqrt{\frac{19}{3}}\right)}\right] = [-5]$$

in $\mathbb{Q}_2$ and since $-5 \notin E^2 \cap \mathbb{Q}_2$, $\sqrt{-2}(1+\sqrt{-2})$ and $\sqrt{-2}(1+3\sqrt{-2})$ are in different square classes of E. Hence

$$\mathbb{Q}_2(\sqrt{\sqrt{-2}(1+\sqrt{-2})},\ \sqrt{5}) \neq \mathbb{Q}_2(\sqrt{\sqrt{-2}(1+3\sqrt{-2})},\ \sqrt{5}).$$

In C_2, we have $E = \mathbb{Q}_2(\sqrt{-10},\ \sqrt{5})$ and $Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(\sqrt{-10}(1+\sqrt{-10})) = 110$ as well as $Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(\sqrt{-10}(1+3\sqrt{-10})) = 910$. Also we have $[110] = [910] = [-2] = [-10][5]$ in $\mathbb{Q}_2$. So we need to use the explicit version of Hilbert 90 for quadratic extensions to find a relation between $\sqrt{-10}(1+\sqrt{-10})$ and $\sqrt{-10}(1+3\sqrt{-10})$.

Let

$$t = \sqrt{\frac{91}{11}}\left(\frac{1+\sqrt{-10}}{1+3\sqrt{-10}}\right) \quad \text{and} \quad l = t+1 = \frac{(1+\sqrt{91/11})+(3+\sqrt{91/11})\sqrt{-10}}{1+3\sqrt{-10}}.$$

Therefore

$$\sqrt{\frac{91}{11}}\left(\frac{1+\sqrt{-10}}{1+3\sqrt{-10}}\right) = t = \frac{l^2}{Nm(l)} = \left(\frac{(1+\sqrt{91/11})+(3+\sqrt{91/11})\sqrt{-10}}{1+3\sqrt{-10}}\right)^2 \frac{1}{2+\frac{62}{91}\sqrt{\frac{91}{11}}}.$$

This concludes

$$\frac{\sqrt{-10}(1+\sqrt{-10})}{\sqrt{-10}(1+3\sqrt{-10})} = \frac{1}{\sqrt{\frac{91}{11}}\left(2+\frac{62}{91}\sqrt{\frac{91}{11}}\right)}e^2$$

where $e \in E$. Since

$$\left[\frac{1}{\sqrt{\frac{91}{11}}\left(2+\frac{62}{91}\sqrt{\frac{91}{11}}\right)}\right] = [-5]$$

in $\mathbb{Q}_2$ and since $-5 \notin E^2 \cap \mathbb{Q}_2$, we have $\sqrt{-10}(1+\sqrt{-10})$ and $\sqrt{-10}(1+3\sqrt{-10})$ are in different square classes of E. Hence

$$\mathbb{Q}_2(\sqrt{\sqrt{-10}(1+\sqrt{-10})},\ \sqrt{5}) \neq \mathbb{Q}_2(\sqrt{\sqrt{-10}(1+3\sqrt{-10})},\ \sqrt{5}).$$

For D_1, assume

$$M_1 = \mathbb{Q}_2(\sqrt{1+\sqrt{10}},\ \sqrt{-1}), \qquad M_2 = \mathbb{Q}_2(\sqrt{3+\sqrt{10}},\ \sqrt{-1}),$$

$$M_3 = \mathbb{Q}_2(\sqrt{\sqrt{10}},\ \sqrt{-1}), \qquad M_4 = \mathbb{Q}_2(\sqrt{3\sqrt{10}},\ \sqrt{-1}).$$

In this case, we have $E = \mathbb{Q}_2(\sqrt{10}, \sqrt{-1})$. We want to show $M_1 \neq M_2$. We have $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(1+\sqrt{10}) = -9$ and $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(3+\sqrt{10}) = -1$. Since $[-9] = [-1]$ in $\mathbb{Q}_2$, we can find a relation between $1+\sqrt{10}$ and $3+\sqrt{10}$ using Hilbert 90.

Let

$$t = \frac{3(1+\sqrt{10})}{(3+\sqrt{10})} \quad \text{and} \quad l = t+1 = \frac{6+4\sqrt{10}}{3+\sqrt{10}}.$$

Therefore

$$\frac{3(1+\sqrt{10})}{3+\sqrt{10}} = t = \frac{l^2}{Nm(l)} = \left(\frac{6+4\sqrt{10}}{3+\sqrt{10}}\right)^2 \frac{(4)(49)}{-1}.$$

This concludes $(1+\sqrt{10})/(3+\sqrt{10}) = -e^2$ where $e \in E$. Since $-1 \notin E^2 \cap \mathbb{Q}_2$, we have $1+\sqrt{10}$ and $3+\sqrt{10}$ are in different square classes of E. Hence $M_1 \neq M_2$.

To see $M_3 \neq M_4$, observe

$$Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}\left(\frac{3\sqrt{10}}{\sqrt{10}}\right) = 9$$

and

$$\left[\frac{3\sqrt{10}}{\sqrt{10}}\right] = [3] = [-5]$$

in $\mathbb{Q}_2$. Also observe $-5 \notin E^2 \cap \mathbb{Q}_2$. Therefore $\sqrt{10}$ and $3\sqrt{10}$ are in different classes of E. Hence $M_3 \neq M_4$.

For the last step in D_1, we need to check M_1 and $M_2 \notin \{M_3, M_4\}$. We have $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(1+\sqrt{10})$ and $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(3+\sqrt{10})$ are in the square class of -1 in $\mathbb{Q}_2$ and $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(\sqrt{10})$ and $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(3\sqrt{10})$ are in the square class of $[-10] = [10][-1]$ in $\mathbb{Q}_2$. Also since $[-1] \neq [-10]$ in $\mathbb{Q}_2$, we have M_1 and $M_2 \notin \{M_3, M_4\}$.

For D_2, we have $Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(\sqrt{-10}) = 10$ and $Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(3\sqrt{-10}) = 90$, and $[10] = [90]$ in $\mathbb{Q}_2$. So $3\sqrt{-10}/\sqrt{-10} = 3 \notin E^2 = \mathbb{Q}_2(\sqrt{-10}, \sqrt{-1})^2$ implies

$$\mathbb{Q}_2(\sqrt{\sqrt{-10}}, \sqrt{-1}) \neq \mathbb{Q}_2(\sqrt{3\sqrt{-10}}, \sqrt{-1}).$$

In E_1, we have $E = \mathbb{Q}_2(\sqrt{-10}, \sqrt{-5})$ and $Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(1+\sqrt{-10}) = 11$ as well as $Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(5+\sqrt{-10}) = 35$. Also we have $[11] = [35] = [-5]$ in $\mathbb{Q}_2$. So we need to use explicit version of Hilbert 90 for quadratic extensions to find a relation between $1+\sqrt{-10}$ and $5+\sqrt{-10}$.

Let

$$t = \sqrt{\frac{35}{11}}\left(\frac{1+\sqrt{-10}}{5+\sqrt{-10}}\right) \quad \text{and} \quad l = t+1 = \frac{(5+\sqrt{35/11}) + (1+\sqrt{35/11})\sqrt{-10}}{5+\sqrt{-10}}.$$

Therefore

$$\sqrt{\frac{35}{11}}\left(\frac{1+\sqrt{-10}}{5+\sqrt{-10}}\right) = t = \frac{l^2}{Nm(l)} = \left(\frac{(5+\sqrt{35/11})+(1+\sqrt{35/11})\sqrt{-10}}{5+\sqrt{-10}}\right)^2 \frac{1}{2+\frac{6}{7}\sqrt{\frac{35}{11}}}.$$

This concludes

$$\frac{1+\sqrt{-10}}{5+\sqrt{-10}} = \frac{1}{\sqrt{\frac{35}{11}}\left(2+\frac{6}{7}\sqrt{\frac{35}{11}}\right)}e^2$$

where $e \in E$. Since

$$\left[\frac{1}{\sqrt{\frac{35}{11}}\left(2+\frac{6}{7}\sqrt{\frac{35}{11}}\right)}\right] = [-2]$$

in $\mathbb{Q}_2$ and since $-2 \notin E^2 \cap \mathbb{Q}_2$, we have $1+\sqrt{-10}$ and $5+\sqrt{-10}$ are in different square classes of E. Hence

$$\mathbb{Q}_2(\sqrt{1+\sqrt{-10}},\sqrt{-5}) \neq \mathbb{Q}_2(\sqrt{5+\sqrt{-10}},\sqrt{-5}).$$

Part Two: $m = -1, -5$:

Let $K_i = \mathbb{Q}_2(\sqrt{m})$ for $m = -1, -5$. In this case, $\mathfrak{p} = (1+\sqrt{m})$ is the prime ideal of K_i which lies over p. We see that all elements of $1+\mathfrak{p}^5$ are square in K_i (same as part one for any $x \in 1+\mathfrak{p}^5$ we have $Nm(x) \equiv 1(mod 8)$).

For $K_i = \mathbb{Q}_2(\sqrt{-1})$, we have

$$\frac{K_i^\times}{K_i^{\times 2}} \cong \frac{(1+\sqrt{-1})}{(2\sqrt{-1})} \times \frac{O^\times}{(7, 1+\mathfrak{p}^5)}$$

since $7 \equiv (\sqrt{-1})^2 \pmod{\mathfrak{p}^5}$. We examine elements ϵ and $\epsilon(1+\sqrt{-1})$ where $\epsilon = a+b(1+\sqrt{-1})$ for $a = 1, 3, 5, 7$ and $b = 0, 1, 2, 3$. We take ϵ such that

1) ϵ
2) ϵ^σ
3) 7ϵ
4) $7\epsilon^\sigma$

are different modulo $\mathfrak{p}^5$ from each other and take $\epsilon(1+\sqrt{-1})$, such that

1) ϵ
2) $-\sqrt{-1}\epsilon^\sigma$
3) 7ϵ
4) $\sqrt{-1}\epsilon^\sigma$

are different modulo $\mathfrak{p}^5$ from each other. Then we get D_4-extensions as follows:

$$\begin{aligned} A_3 &= \{\mathbb{Q}_2(\sqrt{1+\sqrt{-1}},\sqrt{2}), \mathbb{Q}_2(\sqrt{3(1+\sqrt{-1})},\sqrt{2})\} \\ D_3 &= \{\mathbb{Q}_2(\sqrt{1+3\sqrt{-1}},\sqrt{10}), \mathbb{Q}_2(\sqrt{1+5\sqrt{-1}},\sqrt{10})\} \\ F_2 &= \{\mathbb{Q}_2(\sqrt{3+2\sqrt{-1}},\sqrt{5}), \mathbb{Q}_2(\sqrt{2+\sqrt{-1}},\sqrt{5}),\} \end{aligned}$$

Next, consider $K_i = \mathbb{Q}_2(\sqrt{-5})$. We get:

$$\frac{K_i^\times}{K_i^{\times 2}} \cong \frac{(1+\sqrt{-5})}{(-4+2\sqrt{-5})} \times \frac{O^\times}{(3, 1+\mathfrak{p}^5)}$$

since $3 \equiv (\sqrt{-5})^2 \pmod{\mathfrak{p}^5}$. We examine element ϵ and $\epsilon(1+\sqrt{-5})$ where $\epsilon = a + b(1+\sqrt{-5})$ for $a = 1, 3, 5, 7$ and $b = 0, 1, 2, 3$. We take ϵ such that

1) ϵ
2) ϵ^σ
3) 3ϵ
4) $3\epsilon^\sigma$

are different modulo $\mathfrak{p}^5$ from each other and take $\epsilon(1+\sqrt{-5})$, such that

1) ϵ
2) $\epsilon^\sigma(2+5\sqrt{-5})$
3) 3ϵ
4) $3\epsilon^\sigma(2+5\sqrt{-5})$

are different modulo $\mathfrak{p}^5$ from each other. Then we get D_4-extensions as follow:

$$\begin{aligned} B_2 &= \{\mathbb{Q}_2(\sqrt{-1+5\sqrt{-5}},\sqrt{-2}), \mathbb{Q}_2(\sqrt{3+5\sqrt{-5}},\sqrt{-2})\} \\ E_2 &= \{\mathbb{Q}_2(\sqrt{1+\sqrt{-5}},\sqrt{2}), \mathbb{Q}_2(\sqrt{5(1+\sqrt{-5})},\sqrt{2})\} \\ F_3 &= \{\mathbb{Q}_2(\sqrt{3+2\sqrt{-5}},\sqrt{-1}), \mathbb{Q}_2(\sqrt{4+\sqrt{-5}},\sqrt{-1}),\} \end{aligned}$$

Now we are going to check the distinction of the extensions in each set using the explicit version of Hilbert 90 for quadratic extensions.

For A_3, we have $Nm_{\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2}(1+\sqrt{-1}) = 2$ and $Nm_{\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2}(3(1+\sqrt{-1})) = 18$, and $[2] = [18]$ in $\mathbb{Q}_2$. So $3(1+\sqrt{-1})/(1+\sqrt{-1}) = 3 \notin E^2 = \mathbb{Q}_2(\sqrt{-1},\sqrt{2})^2$ implies

$$\mathbb{Q}_2(\sqrt{1+\sqrt{-1}},\sqrt{2}) \neq \mathbb{Q}_2(\sqrt{3(1+\sqrt{-1})},\sqrt{2}).$$

In D_3, we have $E = \mathbb{Q}_2(\sqrt{10}, \sqrt{-1})$ and $Nm_{\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2}(1+3\sqrt{-1}) = 10$ as well as $Nm_{\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2}(1+5\sqrt{-1}) = 26$. Also we have $[10] = [26]$ in $\mathbb{Q}_2$. So we need to use the explicit version of Hilbert 90 for quadratic extensions to find a relation between $1 + 3\sqrt{-1}$ and $1 + 5\sqrt{-1}$.

Let

$$t = \sqrt{\frac{13}{5}}\left(\frac{1+3\sqrt{-1}}{1+5\sqrt{-1}}\right) \quad \text{and} \quad l = t+1 = \frac{(1+\sqrt{13/5}) + (5+3\sqrt{13/5})\sqrt{-1}}{1+5\sqrt{-1}}.$$

Therefore

$$\sqrt{\frac{13}{5}}\left(\frac{1+3\sqrt{-1}}{1+5\sqrt{-1}}\right) = t = \frac{l^2}{Nm(l)} = \left(\frac{(1+\sqrt{13/5}) + (5+3\sqrt{13/5})\sqrt{-1}}{1+5\sqrt{-1}}\right)^2 \frac{1}{2+\frac{16}{13}\sqrt{\frac{13}{5}}}.$$

This concludes

$$\frac{1+3\sqrt{-1}}{1+5\sqrt{-1}} = \frac{1}{\sqrt{\frac{13}{5}}\left(2+\frac{16}{13}\sqrt{\frac{13}{5}}\right)}e^2$$

where $e \in E$. Since

$$\left[\frac{1}{\sqrt{\frac{13}{5}}\left(2+\frac{16}{13}\sqrt{\frac{13}{5}}\right)}\right] = [-2]$$

in $\mathbb{Q}_2$ and since $-2 \notin E^2 \cap \mathbb{Q}_2$, we have $1 + 3\sqrt{-1}$ and $1 + 5\sqrt{-1}$ are in different square classes of E. Hence

$$\mathbb{Q}_2(\sqrt{1+\sqrt{-1}}, \sqrt{10}) \neq \mathbb{Q}_2(\sqrt{1+5\sqrt{-1}}, \sqrt{10}).$$

In F_2, we have $E = \mathbb{Q}_2(\sqrt{5}, \sqrt{-1})$ and $Nm_{\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2}(3+2\sqrt{-1}) = 13$ as well as $Nm_{\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2}(2+\sqrt{-1}) = 5$. Also we have $[13] = [5]$ in $\mathbb{Q}_2$. So we need to use the explicit version of Hilbert 90 for quadratic extensions to find a relation between $3 + 2\sqrt{-1}$ and $2 + \sqrt{-1}$.

Let

$$t = \sqrt{\frac{5}{13}}\left(\frac{3+2\sqrt{-1}}{2+\sqrt{-1}}\right) \quad \text{and} \quad l = t+1 = \frac{(2+3\sqrt{5/13}) + (1+2\sqrt{5/13})\sqrt{-1}}{2+\sqrt{-1}}.$$

Therefore

$$\sqrt{\frac{5}{13}}\left(\frac{3+2\sqrt{-1}}{2+\sqrt{-1}}\right) = t = \frac{l^2}{Nm(l)} = \left(\frac{(2+3\sqrt{5/13}) + (1+2\sqrt{5/13})\sqrt{-1}}{2+\sqrt{-1}}\right)^2 \frac{1}{2+\frac{16}{5}\sqrt{\frac{5}{13}}}.$$

This concludes

$$\frac{3+2\sqrt{-1}}{2+\sqrt{-1}} = \frac{1}{\sqrt{\frac{5}{13}}\left(2+\frac{16}{5}\sqrt{\frac{5}{13}}\right)}e^2$$

where $e \in E$. Since

$$\left[\frac{1}{\sqrt{\frac{5}{13}}\left(2+\frac{16}{5}\sqrt{\frac{5}{13}}\right)}\right] = [-10]$$

in $\mathbb{Q}_2$ and since $-10 \notin E^2 \cap \mathbb{Q}_2$, $3+2\sqrt{-1}$ and $2+\sqrt{-1}$ are in different square classes of E. Hence

$$\mathbb{Q}_2(\sqrt{3+2\sqrt{-1}},\sqrt{5}) \neq \mathbb{Q}_2(\sqrt{2+\sqrt{-1}},\sqrt{5}).$$

In B_2, we have $E = \mathbb{Q}_2(\sqrt{-5},\sqrt{-2})$ and $Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(-1+5\sqrt{-5}) = 126$ as well as $Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(3+5\sqrt{-5}) = 134$. Also we have $[126] = [-2]$ and $[134] = [-10] = [-2][5]$ in $\mathbb{Q}_2$. So 5 is square in $\mathbb{Q}_2(\sqrt{3+5\sqrt{-5}},\sqrt{-2})$ but not in $\mathbb{Q}_2(\sqrt{-1+5\sqrt{-5}},\sqrt{-2})$. Hence they are distinct.

For E_2, we have $Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(1+\sqrt{-5}) = 6$ and $Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(5(1+\sqrt{-5})) = 6(5)^2$, and $[6] = [-10]$ in $\mathbb{Q}_2$. So $5(1+\sqrt{-5})/(1+\sqrt{-5}) = 5 \notin E^2 = \mathbb{Q}_2(\sqrt{-5},\sqrt{2})^2$ implies

$$\mathbb{Q}_2(\sqrt{1+\sqrt{-5}},\sqrt{2}) \neq \mathbb{Q}_2(\sqrt{5(1+\sqrt{-5})},\sqrt{2}).$$

In F_3, we have $E = \mathbb{Q}_2(\sqrt{-5},\sqrt{-1})$ and $Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(3+2\sqrt{-5}) = 29$ as well as $Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(4+\sqrt{-5}) = 21$. Also we have $[29] = [21] = [5]$ in $\mathbb{Q}_2$. So we need to use the explicit version of Hilbert 90 for quadratic extensions to find a relation between $3+2\sqrt{-5}$ and $4+\sqrt{-5}$.

Let

$$t = \sqrt{\frac{21}{29}}\left(\frac{3+2\sqrt{-5}}{4+\sqrt{-5}}\right) \quad \text{and} \quad l = t+1 = \frac{(4+3\sqrt{29/21})+(1+2\sqrt{29/21})\sqrt{-5}}{4+\sqrt{-5}}.$$

Therefore

$$\sqrt{\frac{21}{29}}\left(\frac{3+2\sqrt{-5}}{4+\sqrt{-5}}\right) = t = \frac{l^2}{Nm(l)} = \left(\frac{(4+3\sqrt{21/29})+(1+2\sqrt{21/29})\sqrt{-5}}{4+\sqrt{-5}}\right)^2 \frac{1}{2+\frac{44}{21}\sqrt{\frac{21}{29}}}.$$

This concludes

$$\frac{3+2\sqrt{-5}}{4+\sqrt{-5}} = \frac{1}{\sqrt{\frac{21}{29}}\left(2+\frac{44}{21}\sqrt{\frac{21}{29}}\right)}e^2$$

where $e \in E$. Since

$$\left[\frac{1}{\sqrt{\frac{21}{29}}\left(2+\frac{44}{21}\sqrt{\frac{21}{29}}\right)}\right] = [2]$$

in $\mathbb{Q}_2$ and since $2 \notin E^2 \cap \mathbb{Q}_2$, we have $3+2\sqrt{-5}$ and $4+\sqrt{-5}$ are in different square classes of E. Hence

$$\mathbb{Q}_2(\sqrt{3+2\sqrt{-5}},\sqrt{-1}) \neq \mathbb{Q}_2(\sqrt{4+\sqrt{-5}},\sqrt{-1}).$$

Part Three: $m = 5$:

By [Coh08, Lemma 4.4.26], we have $K_i = \mathbb{Q}_2(\sqrt{5})$ is the only unramified extension of $\mathbb{Q}_2$. Take $\mathfrak{p} = (2)$ which is the prime ideal of K_i. We see that all elements of $1 + \mathfrak{p}^3$ are square in K_i since they are congruent to 1 modulo 8.

Let $\theta = (1 + \sqrt{5})/2$, we see that

$$1 + \theta, 2 + 3\theta, 5, 5(1 + \theta), 5(2 + 3\theta)$$

are square in K_i since $Nm(1+\theta) = Nm(\frac{3+\sqrt{5}}{2}) = 1$, $Nm(2+3\theta) = Nm(\frac{7+3\sqrt{5}}{2}) = 1$ and $5 = (\sqrt{5})^2$.

We examine elements ϵ and 2ϵ where $\epsilon = a + b\theta$ for $0 \leq a \leq 7$ and $0 \leq b \leq 7$ such that either a or b is odd. We take ϵ or 2ϵ such that

1) $\epsilon\eta$
2) $\epsilon^{\sigma}\eta$

are different modulo $\mathfrak{p}^3$ each other where η runs over

$$\{1, 1 + \theta, 2 + 3\theta, 5, 5(1 + \theta), 2 + 7\theta\}.$$

Then we get D_4-extensions over $\mathbb{Q}_2$ as follow:

$$\begin{aligned} F_1 \quad = \quad & \{\mathbb{Q}_2(\sqrt{2 + \sqrt{5}}, \sqrt{-1}), \mathbb{Q}_2(\sqrt{4 + \sqrt{5}}, \sqrt{-1}), \\ & \mathbb{Q}_2(\sqrt{2(2 + \sqrt{5})}, \sqrt{-1}), \mathbb{Q}_2(\sqrt{2(4 + \sqrt{5})}, \sqrt{-1})\} \end{aligned}$$

Now we would like to check that the extensions in set F_1 are distinct.

Let

$$M_1 = \mathbb{Q}_2(\sqrt{2 + \sqrt{5}}, \sqrt{-1}) \qquad M_2 = \mathbb{Q}_2(\sqrt{4 + \sqrt{5}}, \sqrt{-1})$$
$$M_3 = \mathbb{Q}_2(\sqrt{2(2 + \sqrt{5})}, \sqrt{-1}) \qquad M_4 = \mathbb{Q}_2(\sqrt{2(4 + \sqrt{5})}, \sqrt{-1})$$

Since $2(2 + \sqrt{5})/(2 + \sqrt{5}) = 2 \notin E^2 = \mathbb{Q}_2(\sqrt{5}, \sqrt{-1})^2$, we conclude $M_1 \neq M_3$. Also for the same reason, $M_2 \neq M_4$. In addition we have $Nm_{\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2}(2 + \sqrt{5}) = -1$ and $Nm_{\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2}(4 + \sqrt{5}) = 11$. Also we know $[11] = [-5] \neq [-1]$ in $\mathbb{Q}_2$, hence $M_1, M_3 \notin \{M_2, M_4\}$.

Part Four: Removing extra counted extensions:

We get all D_4-extensions over $\mathbb{Q}_2$ as above. But we doubly counted the number of dihedral extensions L, because $K_1(\sqrt{\epsilon}, \sqrt{\epsilon^{\sigma}})$ coincides with $K_2(\sqrt{\xi}, \sqrt{\xi^{\tau}})$ for a suitable $\xi \in K_2^{\times}$ where τ is the generator of the Galois group of $K_2/\mathbb{Q}_2$. Therefore $N = K_i(\sqrt{\epsilon\epsilon^{\sigma}})$ are other quadratic extensions K of $\mathbb{Q}_2$ in D_4-extensions other than K_1 and K_2. Thus we have the following equalities.

$A_1 = A_2 \cup A_3$ where $E = \mathbb{Q}_2(\sqrt{-1}, \sqrt{2})$ and $K = \mathbb{Q}_2(\sqrt{-1})$ in A_2 and $K = \mathbb{Q}_2(\sqrt{-2})$ in A_3 respectively.

$B_1 = B_2$ where $E = \mathbb{Q}_2(\sqrt{-2}, \sqrt{-5})$ and $K = \mathbb{Q}_2(\sqrt{10})$.

$C_1 = C_2$ where $E = \mathbb{Q}_2(\sqrt{-2}, \sqrt{5})$ and $K = \mathbb{Q}_2(\sqrt{5})$.

$D_1 = D_2 \cup D_3$ where $E = \mathbb{Q}_2(\sqrt{-1}, \sqrt{10})$ and $K = \mathbb{Q}_2(\sqrt{-1})$ in D_2 and $K = \mathbb{Q}_2(\sqrt{-10})$ in D_3 respectively.

$E_1 = E_2$ where $E = \mathbb{Q}_2(\sqrt{2}, \sqrt{-5})$ and $K = \mathbb{Q}_2(\sqrt{2})$.

$F_1 = F_2 \cup F_3$ where $E = \mathbb{Q}_2(\sqrt{-1}, \sqrt{5})$ and $K = \mathbb{Q}_2(\sqrt{-5})$ in F_2 and $K = \mathbb{Q}_2(\sqrt{-1})$ in F_3 respectively.

Hence, all 18 distinct D_4-extensions are as follows:

$$\mathbb{Q}_2(\sqrt{1+\sqrt{2}}, \sqrt{-1}) \qquad \mathbb{Q}_2(\sqrt{1+\sqrt{-2}}, \sqrt{-5})$$
$$\mathbb{Q}_2(\sqrt{3+\sqrt{2}}, \sqrt{-1}) \qquad \mathbb{Q}_2(\sqrt{5+\sqrt{-2}}, \sqrt{-5})$$
$$\mathbb{Q}_2(\sqrt{\sqrt{2}}, \sqrt{-1}) \qquad \mathbb{Q}_2(\sqrt{\sqrt{-2}(1+\sqrt{-2})}, \sqrt{5})$$
$$\mathbb{Q}_2(\sqrt{3\sqrt{2}}, \sqrt{-1}) \qquad \mathbb{Q}_2(\sqrt{\sqrt{-2}(1+3\sqrt{-2})}, \sqrt{5})$$

$$\mathbb{Q}_2(\sqrt{1+\sqrt{10}}, \sqrt{-1}) \qquad \mathbb{Q}_2(\sqrt{2+\sqrt{5}}, \sqrt{-1})$$
$$\mathbb{Q}_2(\sqrt{3+\sqrt{10}}, \sqrt{-1}) \qquad \mathbb{Q}_2(\sqrt{4+\sqrt{5}}, \sqrt{-1})$$
$$\mathbb{Q}_2(\sqrt{\sqrt{10}}, \sqrt{-1}) \qquad \mathbb{Q}_2(\sqrt{2(2+\sqrt{5})}, \sqrt{-1})$$
$$\mathbb{Q}_2(\sqrt{3\sqrt{10}}, \sqrt{-1}) \qquad \mathbb{Q}_2(\sqrt{2(4+\sqrt{5})}, \sqrt{-1})$$

$$\mathbb{Q}_2(\sqrt{1+\sqrt{-10}}, \sqrt{-5}),$$
$$\mathbb{Q}_2(\sqrt{5+\sqrt{-10}}, \sqrt{-5}),$$

2.3 Description of Galois D_4-extensions

In this section, we describe all dihedral extensions over all fields.

2.3.1 The case of characteristic not 2

Let F be a field of characteristic not 2.

Definition 2.3.1. *An unordered pair $\{[b]_F, [a]_F\}$, where a and b are in $F^\times$ is admissible if $(b, a) = 0$ and $\dim_{\mathbb{F}_2}(\langle [a]_F, [b]_F\rangle) = 2$.*

Lemma 2.3.2. *Assume that $\{[b]_F, [a]_F\}$ is admissible. Let $E = F(\sqrt{a}, \sqrt{b})$. Then there exists $\delta_1 \in F(\sqrt{a})$ such that*

$$[Nm_{F(\sqrt{a})/F}(\delta_1)]_F = [b]_F.$$

Furthermore for any such δ_1, there exists δ_2 in $F(\sqrt{b})$ such that $[\delta_1]_E = [\delta_2]_E$ and

$$[Nm_{F(\sqrt{b})/F}(\delta_2)]_F = [a]_F.$$

Proof. As $(a, b) = 0$ there exists $\delta_1 \in F(\sqrt{a})$ ([Ser13, Chapter XIV, Proposition 4]) such that

$$[Nm_{F(\sqrt{a})/F}(\delta_1)]_F = [b]_F.$$

Now let δ be any element in $F(\sqrt{a})$ such that $[Nm_{F(\sqrt{a})/F}(\delta)]_F = [b]_F$. We write $\delta = x + y\sqrt{a}$, where $x, y \in F^\times$. Then $x^2 = y^2a + bd^2$, for some $d \in F^\times$. Hence

$$(x + y\sqrt{a} + d\sqrt{b})^2 = 2(x + y\sqrt{a})(x + d\sqrt{b}).$$

Set $\delta_2 = 2(x + d\sqrt{b}) \in F(\sqrt{b})$. Then $[\delta_1]_E = [\delta_2]_E$ and $[Nm_{F(\sqrt{b})/F}(\delta_2)]_F = [4(x^2 - bd^2)]_F = [4y^2a]_F = [a]_F$. □

The above lemma shows that the following definition is well-defined.

Definition 2.3.3. *Let $P = \{[b]_F, [a]_F\}$ be an admissible unordered pair. Let $E = F(\sqrt{a}, \sqrt{b})$. A one dimensional $\mathbb{F}_2$-subspace W of $E^\times/(E^\times)^2$ is said to be compatible with P if W is generated by a $\delta \in F(\sqrt{a})$ with $[Nm_{F(\sqrt{a})/F}(\delta)]_F = [b]_F$. In this case we say that (P, W) is admissible.*

The construction of Galois D_4-extensions over fields of characteristic not 2 is known. See for example [JLY02, Theorem 2.2.7]. Here we make a description of all Galois D_4-extensions over a given field, which is similar to the description of Galois $U_4(\mathbb{F}_2)$ extensions in Theorem 3.1.1.

Theorem 2.3.1. *Let F be a field of characteristic not 2. There is a natural one-one correspondence between the set of admissible pairs $(\{[a]_F, [b]_F\}, W)$ and the set of Galois D_4 extensions L/F.*

Proof. Let $(\{[b]_F, [a]_F\}, W)$ be admissible. Let $E = F(\sqrt{a}, \sqrt{b})$. Let $L = E(\sqrt{W})$. Then L/F is a Galois D_4-extension. (See for example [MT14a, Subsection 2.2].)

Now let L/F be a Galois D_4-extension. We identify D_4 with $U_3(\mathbb{F}_2)$. Let $\rho\colon Gal(L/F) \to U_3(\mathbb{F}_2)$ be any isomorphism. Set $\sigma_1 = \rho^{-1}(E_{12})$, and $\sigma_2 = \rho^{-1}(E_{23})$. Then the commutator subgroup $\Phi = [Gal(L/F), Gal(L/F)]$ is $\langle [\sigma_1, \sigma_2]\rangle$.

Let M be the fixed field of Φ. Then M/F is a 2-elementary abelian extension of F, and $Gal(M/F)$ is the internal direct sum

$$Gal(M/F) = \langle \sigma_1|_M \rangle \oplus \langle \sigma_2|_M \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2.$$

Let $[a]_F, [b]_F$ be elements in $F^\times/(F^\times)^2$ which are dual to $\sigma_1|_M, \sigma_2|_M$ respectively via the Kummer theory. Explicitly we require that

$$\sigma_1(\sqrt{a}) = -\sqrt{a}, \sigma_1(\sqrt{b}) = \sqrt{b};$$
$$\sigma_2(\sqrt{a}) = \sqrt{a}, \sigma_2(\sqrt{b}) = -\sqrt{b}.$$

Claim: $\{[b]_F, [a]_F\}$ does not depend on the choice of ρ.

Proof of Claim: Suppose that $\rho' : Gal(L/F) \to U_3(\mathbb{F}_2)$ is another isomorphism. We define $\sigma_1' = \rho'^{-1}(E_{12})$, and $\sigma_2' = \rho'^{-1}(E_{23})$. We need to show that $\{\sigma_1|_M, \sigma_2|_M\} = \{\sigma_1'|_M, \sigma_2'|_M\}$. We first note that Φ is the centre of $Gal(L/F)$.

Because $\sigma_2'|_M$ is in $Gal(M/F) = \langle \sigma_1|_M \rangle \oplus \langle \sigma_2|_M \rangle$, we have that modulo the subgroup Φ, σ_2' is equal to one of the following elements σ_1, σ_2, or $\sigma_1\sigma_2$.

If $\sigma_2' = \sigma_1\sigma_2$ modulo Φ, then $\sigma_2'^2 = (\sigma_1\sigma_2)^2 \neq 1$, a contradiction. Similarly σ_1' cannot be $\sigma_1\sigma_2$ modulo Φ.

Case 1: $\sigma_2' = \sigma_1$ modulo Φ. In this case σ_1' cannot be σ_1 modulo Φ. Otherwise it would lead to a contradiction that $1 \neq [\sigma_1', \sigma_2'] = [\sigma_1, \sigma_1] = 1$. Hence $\sigma_1' = \sigma_2$ modulo Φ.

Case 2: $\sigma_2' = \sigma_2$ modulo Φ. In this case σ_1' cannot be σ_2 modulo Φ. Otherwise it would lead to a contradiction that $1 \neq [\sigma_1', \sigma_2'] = [\sigma_2, \sigma_2] = 1$. Hence $\sigma_1' = \sigma_1$ modulo Φ.

In both cases we have $\{\sigma_1|_M, \sigma_2|_M\} = \{\sigma_1'|_M, \sigma_2'|_M\}$, as desired.

We have an exact sequence

$$1 \to Gal(L/F(\sqrt{a})) \to Gal(L/F) \to Gal(F(\sqrt{a})/F) \to 1.$$

Then $Gal(L/F(\sqrt{a})$ is an $\mathbb{F}_2[Gal(F(\sqrt{a})/F)]$-module where the action is by conjugation. We also have the $Gal(F(\sqrt{a})/F)$-equivariant Kummer pairing

$$\frac{F(\sqrt{a}) \cap (L^\times)^2}{(F(\sqrt{a})^\times)^2} \times Gal(L/F(\sqrt{a})) \to \mathbb{F}_2.$$

As an $\mathbb{F}_2$-vector space $Gal(L/F(\sqrt{a}))$ has a basis consisting of σ_2, $[\sigma_1, \sigma_2]$. Let δ be the element dual to $[\sigma_1, \sigma_2]$. Then $Nm_{F(\sqrt{a})/F}(\delta) \equiv b \bmod (F(\sqrt{a})^\times)^2$. Hence $Nm_{F(\sqrt{a})/F}(\delta)$ is in $b(F^\times)^2 \cup ba(F^\times)^2$.

Suppose that $Nm_{F(\sqrt{a})/F}(\delta) = baf^2$, for some $f \in F^\times$. From $\sigma_1(\delta)/\delta = ba(f/\delta)^2$, we see that

$$\sigma_1(\sqrt{\delta}) = (\pm)\sqrt{\delta}\sqrt{ba}f/\delta.$$

Hence

$$\begin{aligned}\sigma_1^2(\sqrt{\delta}) &= (\pm)\sigma_1(\sqrt{\delta})\sigma_1(\sqrt{ba})(f/\sigma_1(\delta)) \\ &= (\pm)^2\sqrt{\delta}\sqrt{ba}(f/\delta)\sqrt{b}(-\sqrt{a})(f/\sigma_1(\delta)) \\ &= -\sqrt{\delta}.\end{aligned}$$

This implies that σ_1 is not of order 2, a contradiction. Hence we have $[Nm_{E/F}(\delta)]_F = [b]_F$. Let W be the one dimensional $\mathbb{F}_2$-subspace of $M^\times/(M^\times)^2$ generated by $[\delta]_M$. Then W is compatible with $\{[a]_F, [b]_F\}$. Also since $L = M(\sqrt{W})$, we see that W does not depend on the choice of ρ. □

Lemma 2.3.4. *Assume that F is a finite extension of $\mathbb{Q}_2$ of degree n. Let q be the highest power of 2 such that F contains a primitive q-th root of unity. Then the number N of admissible unordered pairs $\{[a]_F, [b]_F\}$ is*

$$\begin{cases}(2^{n+2}-1)(2^n-1) & \text{if } q \neq 2, \\ (2^{n+1}-1)^2 & \text{if } q = 2.\end{cases}$$

Proof. Let N' be the number of $([a]_F, [b]_F)$ such that $(a, b) = 0$ and that $\dim_{\mathbb{F}_2}\langle [a]_F, [b]_F\rangle = 2$. Then $N = N'/2$. On the other hand, by [MT15a, Remark 3.9], we have

$$N' = \begin{cases}(2^{n+2}-1)(2^{n+1}-2) & \text{if } q \neq 2, \\ 2(2^{n+1}-1)^2 & \text{if } q = 2.\end{cases}$$

The result then follows. □

Lemma 2.3.5. *Assume that F is a finite extension of $\mathbb{Q}_2$ of degree n. Let us fix an unordered admissible pair $\{[a]_F, [b]_F\}$. Then the number of admissible pairs $(\{[a]_F, [b]_F\}, W)$ is 2^n.*

Proof. By local class field theory we have an isomorphism

$$\frac{F^\times}{Nm_{F(\sqrt{a})/F}(F(\sqrt{a})^\times)} \simeq Gal(F(\sqrt{a})/F) = \mathbb{Z}/2\mathbb{Z}.$$

Since $G := Gal(F(\sqrt{a})/F)$ is of exponent 2, we see that $\dfrac{F^\times}{Nm_{F(\sqrt{a})/F}(F(\sqrt{a})^\times)}$ is also of exponent 2. Hence

$$(F^\times)^2 \subseteq Nm_{F(\sqrt{a})/F}(F(\sqrt{a})^\times) \subseteq F^\times.$$

Since $|G| = 2$, we have

$$2 = \left|\frac{F^\times}{Nm_{F(\sqrt{a})/F}(F(\sqrt{a})^\times)}\right| = \left[\frac{F^\times}{(F^\times)^2} : \frac{Nm_{F(\sqrt{a})/F}(F(\sqrt{a})^\times)}{(F^\times)^2}\right].$$

By [Neu99, Chapter II, §5, Corollary 5.8], one has $|F^\times/(F^\times)^2| = 2^{n+2}$. Hence

$$\frac{Nm_{F(\sqrt{a})/F}(E^\times)}{(F^\times)^2} = \left|\frac{F^\times}{(F^\times)^2}\right|/2 = 2^{n+1}.$$

Consider the homomorphism $Nm\colon \dfrac{F(\sqrt{a})^\times}{(F(\sqrt{a})^\times)^2} \to \dfrac{F^\times}{(F^\times)^2}$. Then $\mathrm{im}(Nm) = \dfrac{Nm_{E/F}(E^\times)}{(F^\times)^2}$. By [Neu99, Chapter II, §5, Corollary 5.8], one has $|F(\sqrt{a})^\times/(F(\sqrt{a})^\times)^2| = 2^{2n+2}$. Hence we have

$$|\ker Nm| = \left|\frac{F(\sqrt{a})^\times}{(F(\sqrt{a})^\times)^2}\right|/|\mathrm{im}(Nm)| = 2^{2n+2}/2^{n+1} = 2^{n+1}.$$

Hence

$$|\{[\delta]_{F(\sqrt{a})}\colon [Nm_{F(\sqrt{a})/F}(\delta)]_F = [b]_F\}| = |\ker Nm| = 2^{n+1}.$$

Therefore the number of W such that $(\{[b]_F, [a]_F\}, W)$ is admissible, is $2^{n+1}/2 = 2^n$. □

We recover the following result, which was also obtained in [Yam95, Theorem 2.2] (see also [MNQD77, Theorem 11], [MT14a, Remark 3.9]).

Corollary 2.3.6. *Assume that F is a finite extension of $\mathbb{Q}_2$ of degree n. Let q be the highest power of 2 such that F contains a primitive q-th root of unity. Then the number of Galois D_4-extensions of F is*

$$\begin{cases} 2^n(2^{n+2}-1)(2^n-1) & \text{if } q \neq 2, \\ 2^n(2^{n+1}-1)^2 & \text{if } q = 2. \end{cases}$$

Proof. This follows from Theorem 2.3.1, Lemma 2.3.4 and Lemma 2.3.5. □

2.3.2 The case of characteristic 2

Let F be a field of characteristic 2. We define the class of $a \in F^+$ in $F^+/\wp(F^+)$ as $[a]_F$.

Definition 2.3.7. *An unordered pair $\{[b]_F, [a]_F\}$, where a and b are in $F^\times$ is admissible if* $\dim_{\mathbb{F}_2}(\langle [a]_F, [b]_F\rangle) = 2$.

Lemma 2.3.8. *Assume that $\{[b]_F, [a]_F\}$ is admissible. Let $E = F(\theta_a, \theta_b)$ where $\theta_a \in \wp^{-1}(a)$ and $\theta_b \in \wp^{-1}(b)$. Then there exists $\delta_1 \in F(\theta_a)$ such that*

$$[\mathrm{Tr}_{F(\theta_a)/F}(\delta_1)]_F = [b]_F.$$

Furthermore for any such δ_1, there exists δ_2 in $F(\theta_b)$ such that $[\delta_1]_E = [\delta_2]_E$ and

$$[\mathrm{Tr}_{F(\theta_b)/F}(\delta_2)]_F = [a]_F.$$

Proof. As the trace map $\mathrm{Tr}_{F(\theta_a)/F}$ is surjective, there exists $\delta_1 \in F(\theta_a)$ such that

$$[\mathrm{Tr}_{F(\theta_a)/F}(\delta_1)]_F = [b]_F.$$

Now let δ_1 be any element in $F(\theta_a)$ such that $[\mathrm{Tr}_{F(\theta_a)/F}(\delta_1)]_F = [b]_F$. We write $\delta_1 = x + y\theta_a$, where $x, y \in F$. Then $y = b + \wp(d)$, for some $d \in F$. We have

$$\begin{aligned}\delta_1 + x + a\theta_b + ab + ad^2 &= x + (b + \wp(d))\theta_a + x + a\theta_b + ab + ad^2 \\ &= [b\theta_a + a\theta_b + ab] + [\wp(d)\theta_a + ad^2] \\ &= [(\theta_a\theta_b)^2 - \theta_a\theta_b] + [(d\theta_a)^2 - d\theta_a].\end{aligned} \quad .$$

Set $\delta_2 = x + a\theta_b + ab + ad^2 \in F(\theta_b)$. Then $[\delta_1]_E = [\delta_2]_E$ and $[\mathrm{Tr}_{F(\theta_b)/F}(\delta_2)]_F = [a]_F$. □

The above lemma shows that the following definition is well-defined.

Definition 2.3.9. *Let $P = \{[b]_F, [a]_F\}$ be an admissible unordered pair. Let $E = F(\theta_a, \theta_b)$.*

A one dimensional $\mathbb{F}_2$-subspace W of $E/\wp(E)$ is said to be compatible with P if W is generated by a $\delta \in F(\theta_a)$ with $[\mathrm{Tr}_{F(\theta_a)/F}(\delta)]_F = [b]_F$. In this case we say that (P, W) is admissible.

Lemma 2.3.10. *Let $\{[a]_F, [b]_F\}$ be an admissible unordered pair Let $E = F(\theta_a, \theta_b)$. Let $\delta \in F(\theta_a)$ with $[\mathrm{Tr}_{F(\theta_a)/F}(\delta)]_F = [b]_F$. Then $E(\theta_\delta)/F$ is a Galois D_4-extension.*

Proof. The extension E/F is Galois with Galois group generated by σ_a, σ_b, where σ_a and σ_b are defined by the conditions:

$$\begin{aligned}\sigma_a(\theta_a) = \theta_a + 1, \sigma_a(\theta_b) = \theta_b, \\ \sigma_b(\theta_a) = \theta_a, \sigma_(\theta_b) = \theta_b + 1,\end{aligned}$$

Since $\mathrm{Tr}_{F(\theta_a)/F}(\delta) = b + \wp(d)$ for some $d \in F$, we have

$$\sigma_a(\delta) = \delta + b + \wp(d).$$

Clearly we have

$$\sigma_b(\delta) = \delta.$$

Then [MT14a, Proof of Proposition 4.1] shows that $L = E(\theta_\delta)/F$ is Galois and its Galois group is isomorphic to D_4. Furthermore, we can choose an extension, still denoted σ_a in $Gal(L/F)$, of σ_a such that $\sigma_a(\theta_\delta) = \theta_\delta + \theta_b + d$. □

Theorem 2.3.2. *Let F be a field of characteristic 2. There is a natural one-one correspondence between the set of admissible pairs $(\{[a]_F, [b]_F\}, W)$ and the set of Galois D_4 extensions L/F.*

Proof. Let $(\{[b]_F, [a]_F\}, W)$ be admissible. Let $E = F(\sqrt{a}, \sqrt{b})$. Let $L = E(\sqrt{W})$. Then L/F is a Galois D_4-extension. (See [MT14a, Subsection 4.2].)

Now let L/F be a Galois D_4-extension. We identify D_4 with $U_3(\mathbb{F}_2)$. Let $\rho\colon Gal(L/F) \to U_3(\mathbb{F}_2)$ be any isomorphism. Set $\sigma_1 = \rho^{-1}(E_{12})$, and $\sigma_2 = \rho^{-1}(E_{23})$. Then the commutator subgroup $\Phi = [Gal(L/F), Gal(L/F)]$ is $\langle[\sigma_1, \sigma_2]\rangle$.

Let M be the fixed field of Φ. Then M/F is an 2-elementary abelian extension of F, and $Gal(M/F)$ is the internal direct sum

$$Gal(M/F) = \langle\sigma_1|_M\rangle \oplus \langle\sigma_2|_M\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2.$$

Let $[a]_F, [b]_F$ be elements in $F/\wp(F)^2$ which are dual to $\sigma_1|_M, \sigma_2|_M$ respectively via the Artin-Schreier theory. Explicitly we require that

$$\sigma_1(\theta_a) = \theta_a + 1, \sigma_1(\theta_b) = \theta_b;$$
$$\sigma_2(\theta_a) = \theta_a, \sigma_2(\theta_b) = -\theta_b.$$

Claim: $\{[b]_F, [a]_F\}$ does not depend on the choice of ρ.

Proof of Claim: Suppose that $\rho' : Gal(L/F) \to U_4(\mathbb{F}_2)$ is another isomorphism. We define $\sigma_1' = \rho'^{-1}(E_{12})$, and $\sigma_2' = \rho'^{-1}(E_{23})$. We need to show that $\{\sigma_1|_M, \sigma_2|_M\} = \{\sigma_1'|_M, \sigma_2'|_M\}$. We first note that Φ is the center of $Gal(L/F)$.

Because $\sigma_2'|_M$ is in $Gal(M/F) = \langle\sigma_1|_M\rangle \oplus \langle\sigma_2|_M\rangle$, we have that modulo the subgroup Φ, σ_2' is equal to one of the following elements σ_1, σ_2, or $\sigma_1\sigma_2$.

If $\sigma_2' = \sigma_1\sigma_2$ modulo Φ, then $\sigma_2'^2 = (\sigma_1\sigma_2)^2 \neq 1$, a contradiction. Similarly σ_1' cannot be $\sigma_1\sigma_2$ modulo Φ.

Case 1: $\sigma_2' = \sigma_1$ modulo Φ. In this case σ_1' cannot be σ_1 modulo Φ. Otherwise it would lead to a contradiction that $1 \neq [\sigma_1', \sigma_2'] = [\sigma_1, \sigma_1] = 1$. Hence $\sigma_1' = \sigma_2$ modulo Φ.

Case 2: $\sigma_2' = \sigma_2$ modulo Φ. In this case σ_1' cannot be σ_2 modulo Φ. Otherwise it would lead to a contradiction that $1 \neq [\sigma_1', \sigma_2'] = [\sigma_2, \sigma_2] = 1$. Hence $\sigma_1' = \sigma_1$ modulo Φ.

In both cases we have $\{\sigma_1|_M, \sigma_2|_M\} = \{\sigma_1'|_M, \sigma_2'|_M\}$, as desired.

We have an exact sequence

$$1 \to Gal(L/F(\theta_a)) \to Gal(L/F) \to Gal(F(\theta_a)/F) \to 1.$$

Then $Gal(L/F(\theta_a)$ is an $\mathbb{F}_2[Gal(F(\theta_a)/F)]$-module where the action is by conjugation. We also have the $Gal(F(\theta_a)/F)$-equivariant Artin-Schreier pairing

$$\frac{F(\theta_a) \cap \wp(L)}{\wp(F(\theta_a))} \times Gal(L/F(\theta_a)) \to \mathbb{F}_2.$$

As an $\mathbb{F}_2$-vector space $Gal(L/F(\theta_a))$ has a basis consisting of σ_2, $[\sigma_1, \sigma_2]$. Let δ be the element dual to $[\sigma_1, \sigma_2]$. Then $\mathrm{Tr}_{F(\theta_a)/F}(\delta) \equiv b \bmod (\wp(F(\theta_a))$. Hence $Nm_{F(\theta_a)/F}(\delta)$ is in $b + \wp(F) \cup b + a + \wp(F)$.

Suppose that $\mathrm{Tr}_{F(\theta_a)/F}(\delta) = b + a + \wp(f)$, for some $f \in F$. Then $\sigma_1(\delta) = \delta + b + a + \wp(f)$. Thus

$$\sigma_1(\theta_\delta) = \theta_\delta + \theta b + \theta_a + f + i,$$

for some $i \in \{0, 1\}$. Hence

$$\begin{aligned}\sigma_1^2(\theta_\delta) &= \sigma_1(\theta_\delta) + \sigma_1(\theta_b) + \sigma_1(\theta_a) + f + i \\ &= \theta_\delta + \theta_b + \theta + a + f + i\theta_b + \theta_a + 1 + f + i \\ &= \theta_\delta + 1.\end{aligned}$$

This implies that σ_1 is not of order 2, a contradiction. Hence we have $[\mathrm{Tr}_{E/F}(\delta)]_F = [b]_F$. Let W be the one dimensional $\mathbb{F}_2$-subspace of $M^\times/(M^\times)^2$ generated by $[\delta]_M$. Then W is compatible with $\{[a]_F, [b]_F\}$. Also since $L = M(\theta_W)$, we see that W does not depend on the choice of ρ. □

Using the correspondence in Theorem 2.3.1, we can rearrange Naito's list of D_4-extensions in the following table.

$\{[a],[b]\}$	Naito's list of D_4-extensions
$\{[-1],[2]\}$	$\mathbb{Q}_2(\sqrt{1+\sqrt{2}},\sqrt{-1})$ $\quad$ $\mathbb{Q}_2(\sqrt{3+\sqrt{2}},\sqrt{-1})$ $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(1+\sqrt{2})=-1$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(3+\sqrt{2})=7$
$\{[-1],[5]\}$	$\mathbb{Q}_2(\sqrt{2+\sqrt{5}},\sqrt{-1})$ $\quad$ $\mathbb{Q}_2(\sqrt{2(2+\sqrt{5})},\sqrt{-1})$ $Nm_{\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2}(2+\sqrt{5})=-1$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2}(2(2+\sqrt{5}))=-4$
$\{[-1],[10]\}$	$\mathbb{Q}_2(\sqrt{1+\sqrt{10}},\sqrt{-1})$ $\quad$ $\mathbb{Q}_2(\sqrt{3+\sqrt{10}},\sqrt{-1})$ $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(1+\sqrt{10})=-9$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(3+\sqrt{2})=-1$
$\{[-2],[2]\}$	$\mathbb{Q}_2(\sqrt{\sqrt{2}},\sqrt{-1})$ $\quad$ $\mathbb{Q}_2(\sqrt{3\sqrt{2}},\sqrt{-1})$ $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\sqrt{2})=-2$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(3\sqrt{2})=-18$
$\{[-5],[5]\}$	$\mathbb{Q}_2(\sqrt{4+\sqrt{5}},\sqrt{-1})$ $\quad$ $\mathbb{Q}_2(\sqrt{2(4+\sqrt{5})},\sqrt{-1})$ $Nm_{\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2}(4+\sqrt{5})=11$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2}(2(4+\sqrt{5}))=44$

$\{[-2],[-10]\}$	$\mathbb{Q}_2(\sqrt{\sqrt{-2}(1+\sqrt{-2})},\sqrt{5})$ $\quad$ $\mathbb{Q}_2(\sqrt{\sqrt{-2}(1+3\sqrt{-2})}$ $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(\sqrt{-2}(1+\sqrt{-2}))=6$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(\sqrt{-2}(1+3\sqrt{-2}))=38$
$\{[-10],[10]\}$	$\mathbb{Q}_2(\sqrt{\sqrt{10}},\sqrt{-1})$ $\quad$ $\mathbb{Q}_2(\sqrt{3\sqrt{10}},\sqrt{-1})$ $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(\sqrt{10})=-10$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(3\sqrt{10})=-90$
$\{[-5],[-10]\}$	$\mathbb{Q}_2(\sqrt{1+\sqrt{-10}},\sqrt{-5})$ $\quad$ $\mathbb{Q}_2(\sqrt{5+\sqrt{-10}},\sqrt{-5})$ $Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(1+\sqrt{-10})=11$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(5+\sqrt{-10})=35$
$\{[-2],[-5]\}$	$\mathbb{Q}_2(\sqrt{1+\sqrt{-2}},\sqrt{-5})$ $\quad$ $\mathbb{Q}_2(\sqrt{5+\sqrt{-2}},\sqrt{-5})$ $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(1+\sqrt{-2})=3$ $\quad$ $Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(5+\sqrt{-2})=27$

Chapter 3

$U_4(\mathbb{F}_2)$-Extensions

In the last chapter we saw the list of all D_4−extensions of rational 2-adic fields. In this chapter, we use the technique of Mináč and Tân [MT15b], which is introduced in chapter 1, to write the list of all $U_4(\mathbb{F}_2)$−extensions of $\mathbb{Q}_2$.

3.1 Description of Galois $U_4(\mathbb{F}_2)$-extensions over fields

For any field F of characteristic not 2 and for any element $a \in F^\times$, we denote $[a]_F$ the image of a in $F^\times/(F^\times)^2$. For any field L of characteristic 2 and for any element $a \in L$, we denote $[a]_L$ the image of a in $L/\wp(L)$.

For $1 \leq i, j \leq n$, let e_{ij} denote the n-by-n matrix with the 1 of $\mathbb{F}_p$ in the position (i, j) and 0 elsewhere, and let $E_{ij} = I + e_{ij}$ where I is identity matrix of order n.

3.1.1 The case of characteristic not 2

Let F be a field of characteristic different from 2.

Definition 3.1.1. *A pair $([b]_F, V)$, where b is in $F^\times$ and $V \subseteq F^\times/(F^\times)^2$, is admissible if $\dim_{\mathbb{F}_2}(V) = 2$, $\dim_{\mathbb{F}_2}(\langle V, [b]_F\rangle) = 3$ and $(b, v) = 0$ for every $[v]_F \in V$.*

Lemma 3.1.2. *Assume that $([b]_F, V)$ is admissible. Let $E = F(\sqrt{V})$. Then there exists $\delta \in E$ such that $[Nm_{E/F}(\delta)]_F = [b]_F$.*

Proof. We have $V = \langle [a]_F, [c]_F\rangle$ for some $a, c \in F^\times$. Then $(a, b) = (b, c) = 0$. By [MT13, Section 5], there exists $\delta \in E$ such that $Nm_{E/F}(\delta) = bd^2$ for some $d \in F^\times$. □

Definition 3.1.3. *Assume that $([b]_F, V)$ is admissible. Let $E = F(\sqrt{V})$. Then a triple $([b]_F, V, W)$, where W is a free $\mathbb{F}_2[Gal(E/F)]$-submodule of $E^\times/(E^\times)^2$, is admissible if W is generated by an element $[\delta]_E$ with $[Nm_{E/F}(\delta)]_F = [b]_F$.*

Lemma 3.1.4. *Let K be a field of characteristic $p > 0$. Let G be a finite p-group. Then every non-zero left ideal in the group ring $K[G]$ contains the element $\sum_{\sigma\in G} \sigma$.*

Proof. Let I be any non-zero left ideal in $K[G]$. Then I contains a minimal non-zero left ideal J. As a $K[G]$-module, J is simple. We know that over $K[G]$ there is up to isomorphism only one simple module, which is K with trivial action. Let n be any element in J which generates J as a $K[G]$-module. Then n is fixed under all elements of G. Hence $n = a\sum_{\sigma\in G}\sigma$, for some $a \in K^\times$. This implies that $\sum_{\sigma\in G}\sigma$ is in J. □

Lemma 3.1.5. *Let $([b]_F, V, W)$ be an admissible triple. Assume that $V = \langle [a]_F, [c]_F\rangle$. Let $E = F(\sqrt{V})$. Assume that W is generated by $[\delta]_E$ as a free $\mathbb{F}_2[Gal(E/F)]$-module with $[Nm_{E/F}(\delta)]_F = [b]_F$. Let $A = Nm_{E/F(\sqrt{a})}(\delta)$ and $C = Nm_{E/F(\sqrt{c})}(\delta)$. Then every generator of W as a free $\mathbb{F}_2[Gal(E/F)]$-module is of the form*

$$[\delta']_E = [\delta A^{\epsilon_A} C^{\epsilon_C} b^{\epsilon_b}]_E,$$

where $\epsilon_A, \epsilon_C, \epsilon_b \in \{0, 1\}$.

Furthermore for any generator $[\delta']_E$ of W as a free $\mathbb{F}_2[Gal(E/F)]$-module, we have $[Nm_{E/F}(\delta')]_F = [b]_F$. In particular, this implies that the pair (V, W) uniquely determines $[b]_F$.

Proof. Let $G = Gal(E/F)$. As an $\mathbb{F}_2$-vector space, W is generated by $[\delta]_E, [A]_E, [C]_E, [b]_E$. Let $[\delta']_E$ be an arbitrary generator of the free $\mathbb{F}_2[G]$-module. Then

$$[\delta']_E = [\delta^{\epsilon_\delta} A^{\epsilon_A} C^{\epsilon_C} b^{\epsilon_b}]_E,$$

for some $\epsilon_\delta, \epsilon_A, \epsilon_C, \epsilon_b \in \{0, 1\}$. Suppose that $\epsilon_\delta = 0$, then we see that $(\sum_{\sigma\in G}\sigma)([\delta']_E)$ is trivial in $E^\times/((E^\times)^2)$, a contradiction. Hence $\epsilon_\delta = 1$. Furthermore, we have

$$[Nm_{E/F}(\delta')]_F = [b]_F.$$

This implies that $[b]_F$ is uniquely determined by V and W.

Conversely, assume that $[\delta']_E = [\delta A^{\epsilon_A} C^{\epsilon_C} b^{\epsilon_b}]_E$, for some $\epsilon_A, \epsilon_C, \epsilon_b \in \{0, 1\}$. Let W' be the $\mathbb{F}_2[G]$-module generated by $[\delta']_E$. Then we have $W' \subseteq W$. It is then enough to show that W' is a free $\mathbb{F}_2[G]$-module. Suppose that W' is not free. Then there would exist a non-zero ideal $I \subseteq \mathbb{F}_2[G]$ such that I would annihilate δ'. By Lemma 3.1.4 any non-zero ideal of $\mathbb{F}_2[G]$ contains the element $\sum_{\sigma\in G}\sigma =: N$. Therefore N would annihilate $[\delta']_E$. This contradicts the fact that

$$N([\delta']_E)] = [Nm_{E/F}(\delta')]_E = [b]_E \neq 1 \in E^\times/(E^\times)^2.$$ □

Proposition 3.1.6. *Let $([b]_F, V, W)$ be an admissible triple. Let $E = F(\sqrt{V})$. Let $L = E(\sqrt{W})$. Then L/F is a Galois $U_4(\mathbb{F}_2)$-extension.*

Proof. Suppose that $V = \langle [a]_F, [c]_F\rangle$ and that W is generated by δ with $Nm_{E/F}(\delta) = bd^2$. Let $A = Nm_{E/F(\sqrt{a})}(\delta)$ and $C = Nm_{E/F(\sqrt{c})}(\delta)$. We first note that $F(\sqrt{a}, \sqrt{b}, \sqrt{c})/F$ is an abelian 2-elementary extension with Galois group generated by $\sigma_a, \sigma_b, \sigma_c$, where

$$\begin{aligned}
\sigma_a(\sqrt{a}) &= -\sqrt{a}, \sigma_a(\sqrt{b}) = \sqrt{b}, \sigma_a(\sqrt{c}) = \sqrt{c};\\
\sigma_b(\sqrt{a}) &= \sqrt{a}, \sigma_b(\sqrt{b}) = -\sqrt{b}, \sigma_b(\sqrt{c}) = \sqrt{c};\\
\sigma_c(\sqrt{a}) &= \sqrt{a}, \sigma_c(\sqrt{b}) = \sqrt{b}, \sigma_c(\sqrt{c}) = -\sqrt{c}.
\end{aligned}$$

Clearly we have

$$\sigma_c(\delta) = \delta A \delta^{-2},$$
$$\sigma_a(\delta) = \delta C \delta^{-2},$$
$$\sigma_a(A) = A\frac{bd^2}{A^2},$$
$$\sigma_c(C) = C\frac{bd^2}{C^2},$$

and

$$\frac{C}{A} = \frac{\sigma_a(\delta)}{\delta}\frac{\delta}{\sigma_c(\delta)}.$$

Then [MT14a, Section 3] implies that L/F is a Galois $U_4(\mathbb{F}_2)$-extension. Moreover an explicit isomorphism $\rho\colon Gal(L/F) \to U_4(\mathbb{F}_2)$ is given by

$$\sigma_a \mapsto \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_b \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_c \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

for suitable extensions $\sigma_a, \sigma_b, \sigma_c \in Gal(L/F)$ of $\sigma_a, \sigma_b, \sigma_c$. □

Proposition 3.1.7. *There is a natural way to associate an admissible triple* $([b]_F, V, W)$ *to any given Galois* $U_4(\mathbb{F}_2)$*-extension* L/F.

Proof. Assume that L/F is a Galois $U_4(\mathbb{F}_2)$-extension. Let $\rho\colon Gal(L/F) \to U_4(\mathbb{F}_2)$ be any isomorphism. Set $\sigma_1 = \rho^{-1}(E_{12})$, $\sigma_2 = \rho^{-1}(E_{23})$, and $\sigma_3 = \rho^{-1}(E_{34})$. Then the commutator subgroup $\Phi = [Gal(L/F), Gal(L/F)]$ is the internal direct sum

$$\Phi = \langle [\sigma_1, \sigma_2] \rangle \oplus \langle [\sigma_2, \sigma_3] \rangle \oplus \langle [[\sigma_1, \sigma_2], \sigma_3] \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^3.$$

Let M be the fixed field of Φ. Then M/F is an abelian 2-elementary extension of F, and $Gal(M/F)$ is the (internal) direct sum

$$Gal(M/F) = \langle \sigma_1|_M \rangle \oplus \langle \sigma_2|_M \rangle \oplus \langle \sigma_3|_M \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^3.$$

Let $[a]_F, [b]_F, [c]_F$ be elements in $F^\times/(F^\times)^2$ which are dual to $\sigma_1|_M, \sigma_2|_M, \sigma_3|_M$ respectively via Kummer theory. Explicitly we require that

$$\sigma_1(\sqrt{a}) = -\sqrt{a}, \sigma_1(\sqrt{b}) = \sqrt{b}, \sigma_1(\sqrt{c}) = \sqrt{c};$$
$$\sigma_2(\sqrt{a}) = \sqrt{a}, \sigma_2(\sqrt{b}) = -\sqrt{b}, \sigma_2(\sqrt{c}) = \sqrt{c};$$
$$\sigma_3(\sqrt{a}) = \sqrt{a}, \sigma_3(\sqrt{b}) = \sqrt{b}, \sigma_3(\sqrt{c}) = -\sqrt{c}.$$

Let $E = F(\sqrt{a}, \sqrt{c})$. Then E is fixed under σ_2, $[\sigma_1, \sigma_2]$, $[\sigma_2, \sigma_3]$ and $[[\sigma_1, \sigma_2], \sigma_3]$. Hence E is fixed under a subgroup H of Gal(L/F) which is generated by σ_2, $[\sigma_1, \sigma_2]$, $[\sigma_2, \sigma_3]$ and $[[\sigma_1, \sigma_2], \sigma_3]$. We have $[L^H : F] = |Gal(L/F)|/|H| = 4$, and $[E : F] = 4$. Therefore $E = L^H$.

Claim: E does not depend on the choice of ρ.

Proof of Claim: Suppose that $\rho' : Gal(L/F) \to U_4(\mathbb{F}_2)$ is another isomorphism. We define $\sigma_1' = \rho'^{-1}(E_{12})$, $\sigma_2' = \rho'^{-1}(E_{23})$, and $\sigma_3' = \rho'^{-1}(E_{34})$. Let H' be the group generated by σ_2', $[\sigma_1', \sigma_2']$, $[\sigma_2', \sigma_3']$ and $[[\sigma_1', \sigma_2'], \sigma_3']$. We need to show that $H = H'$. We first note that σ_2 and σ_2' commute with every element in Φ.

We have $\sigma_2'|_M$ is in $Gal(M/F) = \langle \sigma_1|_M \rangle \oplus \langle \sigma_2|_M \rangle \oplus \langle \sigma_3|_M \rangle$.

Hence modulo the subgroup Φ, σ_2' is equal to one of the following element $\sigma_1, \sigma_2, \sigma_3$, $\sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_3, \sigma_1\sigma_2\sigma_3$.

If $\sigma_2' = \sigma_1$, or $\sigma_1\sigma_2$, or $\sigma_1\sigma_3$, or $\sigma_1\sigma_2\sigma_3$ modulo Φ, then

$$[[\sigma_2, \sigma_3], \sigma_2'] = [[\sigma_2, \sigma_3], \sigma_1],$$

which is impossible since $[[\sigma_2, \sigma_3], \sigma_1]$ is nontrivial but $[[\sigma_2, \sigma_3], \sigma_2']$ is trivial.

If $\sigma_2' = \sigma_3$, or $\sigma_2\sigma_3$ modulo Φ, then

$$[[\sigma_1, \sigma_2], \sigma_2'] = [[\sigma_1, \sigma_2], \sigma_3],$$

which is impossible since $[[\sigma_1, \sigma_2], \sigma_3]$ is nontrivial but $[[\sigma_1, \sigma_2], \sigma_2']$ is trivial.

From the above discussion we see that $\sigma_2' \equiv \sigma_2 \bmod \Phi$. This implies that $H' = H$. Thus E does not depend on the choice of ρ.

We have an exact sequence

$$1 \to Gal(L/E) \to Gal(L/F) \to Gal(E/F) = G \to 1.$$

Then $Gal(L/E)$ is an $\mathbb{F}_2[G]$-module where the action is by conjugation. We also have the G-equivariant Kummer pairing ([Wat94, Section 1])

$$\frac{E \cap (L^\times)^2}{(E^\times)^2} \times Gal(L/E) \to \mathbb{F}_2.$$

As an $\mathbb{F}_2$-vector space, $Gal(L/E)$ has a basis consisting of σ_2, $[\sigma_1, \sigma_2]$, $[\sigma_2, \sigma_3]$ and $[[\sigma_1, \sigma_2], \sigma_3]$. Let $[\delta]_E$ be an element dual to $[[\sigma_1, \sigma_2], \sigma_3]$. Then $Nm_{E/F}(\delta) \equiv b \bmod (E^\times)^2$. Hence $Nm_{E/F}(\delta)$ is in $b(F^\times)^2 \cup ba(F^\times)^2 \cup bc(F^\times)^2 \cup bac(F^\times)^2$.

Let $A = Nm_{E/F(\sqrt{a})}(\delta)$ and $C = Nm_{E/F(\sqrt{c})}(\delta)$. Suppose that $Nm_{E/F}(\delta) \equiv ba \mod (F^\times)^2$. Then $Nm_{F(\sqrt{a})/F}(A) = baf^2$ for some $f \in F^\times$. From $\sigma_1(A)/A = ba(f/A)^2$, we see that

$$\sigma_1(\sqrt{A}) = (\pm)\sqrt{A}\sqrt{ba}f/A.$$

Hence

$$\begin{aligned}\sigma_1^2(\sqrt{A}) &= (\pm)\sigma_1(\sqrt{A})\sigma_1(\sqrt{ba})(f/\sigma_1(A)) \\ &= (\pm)^2\sqrt{A}\sqrt{ba}(f/A)\sqrt{b}(-\sqrt{a})(f/\sigma_1(A)) \\ &= -\sqrt{A}.\end{aligned}$$

This implies that σ_1 is not of order 2, a contradiction. Hence we have $Nm_{E/F}(\delta)$ is not in $ba(F^\times)^2$.

Similarly we can show that $Nm_{E/F}(\delta)$ is not in $bc(F^\times)^2 \cup ba(F^\times)^2$. Therefore

$$Nm_{E/F}(\delta) \equiv b \bmod (F^\times)^2.$$

We set $V = \langle [a]_F, [c]_F \rangle$. Then V does not depend on the choice of ρ. Since

$$Nm_{F(\sqrt{a})/F}(A) = Nm_{E/F}(\delta) = b \bmod (F^\times)^2,$$

we have $(a, b) = 0$. Similarly, we have $(b, c) = 0$. Therefore $(b, v) = 0$ for every $v \in V$, and the pair $([b]_F, V)$ is admissible. Let W be the $\mathbb{F}_2[G]$-submodule of $E^\times/(E^\times)^2$ which is dual via the Kummer theory to $Gal(L/E)$. Then W does not depend on choice of ρ, and W is free and generated by δ. Since $[Nm_{E/F}(\delta)]_F = [b]_F$, we see that the triple $([b]_F, V, W)$ is admissible. Since V and W determine $[b]_F$ uniquely, we see that $[b]_F$ does not depend on the choice of ρ. □

Theorem 3.1.1. *Let F be a field of characteristic not 2. There is a natural one-one correspondence between the set of admissible triples $([b]_F, V, W)$ and the set of Galois $U_4(\mathbb{F}_2)$-extensions L/F.*

Proof. By Proposition 3.1.6 we have a map μ from the set of admissible triples $([b]_F, V, W)$ to the set of Galois $U_4(\mathbb{F}_2)$-extensions L/F. By Proposition 3.1.7 we have a map η from the set of Galois $U_4(\mathbb{F}_2)$-extensions L/F to the set of admissible triples $([b]_F, V, W)$. We show that μ and η are inverses of each other.

Let $([b]_F, V, W)$ be an admissible triple. Via the map μ we obtain a $U_4(\mathbb{F}_2)$-extension L/F. Explicitly, if $V = \langle [a]_F, [c]_F \rangle$ and $E = F(\sqrt{a}, \sqrt{c})$, then $L = E(\sqrt{W})$ and there is an isomorphism $\rho\colon Gal(L/F) \simeq U_4(\mathbb{F}_2)$ such that $\rho^{-1}(E_{12}) = \sigma_a$, $\rho^{-1}(E_{23}) = \sigma_b$, $\rho^{-1}(E_{34}) = \sigma_c$. (Here $\sigma_a, \sigma_b, \sigma_c$ are defined as in Proposition 3.1.6.) We apply the construction in Proposition 3.1.7 with this isomorphism ρ. Then we obtain back the admissible triple $([b]_F, V, W)$.

Now let L/F be a $U_4(\mathbb{F}_2)$-extension. Then via the map η we obtain an admissible triple $([b]_F, V, W)$. Since $L = F(\sqrt{V})(W)$, we see that μ sends the triple $([b]_F, V, W)$ back to the extension L/F. □

We apply the theorem above to count the number of Galois $U_4(\mathbb{F}_2)$-extensions over a 2-adic field.

Lemma 3.1.8. *Assume that F is a finite extension of $\mathbb{Q}_2$ of degree n. Let q be the highest power of 2 such that F contains a primitive q-th root of unity. Then the number N of admissible pairs $([b]_F, V)$ is*

$$\begin{cases} \dfrac{4(2^{n+2}-1)(2^n-1)(2^{n-1}-1)}{3} & \text{if } q \neq 2, \\ \dfrac{4(2^{n+1}-1)(2^n-1)^2}{3} & \text{if } q = 2. \end{cases}$$

Proof. Let N' be the number of $([a]_F, [b]_F, [c]_F)$ such that $(a,b) = (b,c) = 0$ and that $\dim_{\mathbb{F}_2}\langle [a]_F, [b]_F, [c]_F\rangle = 3$. Then $N = N'/6$. This is because for each given V such that $([b]_F, V)$ is admissible, since there are 3 possibilities for $[a]_F$ and 2 possibilities $[b]_F$, there are precisely 6 choices of choosing $([a]_F, [c]_F)$ with $V = \langle [a]_F, [c]_F\rangle$. On the other hand, by [MT15a, Lemma 3.6 and Proposition 3.4], we have

$$N' = \begin{cases} (2^{n+2}-1)(2^{n+1}-2)(2^{n+1}-4) & \text{if } q \neq 2, \\ (2^{n+1}-1)(2^{n+1}-2)(2^{n+2}-4) & \text{if } q = 2. \end{cases}$$

The result then follows. □

Lemma 3.1.9. *Assume that F is a finite extension of $\mathbb{Q}_2$ of degree n. Let us fix an admissible pair $([b]_F, V)$. Then the number of admissible triples $([b]_F, V, W)$ is 2^{3n-1}.*

Proof. Let $E = F(\sqrt{V})$. By local class field theory we have an isomorphism

$$\frac{F^\times}{Nm_{E/F}(E^\times)} \simeq Gal(E/F) = G.$$

Since G is of exponent 2, we see that $\dfrac{F^\times}{Nm_{E/F}(E^\times)}$ is also of exponent 2. Hence

$$(F^\times)^2 \subseteq Nm_{E/F}(E^\times) \subseteq F^\times.$$

Since $|G| = 4$, we have

$$4 = \left|\frac{F^\times}{Nm_{E/F}(E^\times)}\right| = \left[\frac{F^\times}{(F^\times)^2} : \frac{Nm_{E/F}(E^\times)}{(F^\times)^2}\right].$$

By [Neu99, Chapter II, §5, Corollary 5.8], one has $|F^\times/(F^\times)^2| = 2^{n+2}$. Hence

$$\left|\frac{Nm_{E/F}(E^\times)}{(F^\times)^2}\right| = \left|\frac{F^\times}{(F^\times)^2}\right|/4 = 2^n.$$

Consider the homomorphism $Nm\colon \dfrac{E^\times}{(E^\times)^2} \to \dfrac{F^\times}{(F^\times)^2}$. Then $\mathrm{im}(Nm) = \dfrac{Nm_{E/F}(E^\times)}{(F^\times)^2}$. By [Neu99, Chapter II, §5, Corollary 5.8], one has $|E^\times/(E^\times)^2| = 2^{4n+2}$. Hence we have

$$|\ker Nm| = \left|\frac{E^\times}{(E^\times)^2}\right|/|\mathrm{im}(Nm)| = 2^{4n+2}/2^n = 2^{3n+2}.$$

Hence

$$|\{[\delta]_E\colon [Nm_{E/F}(\delta)]_F = [b]_F\}| = |\ker Nm| = 2^{3n+2}.$$

Therefore by Lemma 3.1.5 the number of W such that $([b]_F, V, W)$ is admissible, is $2^{3n+2}/8 = 2^{3n-1}$. □

We recover the following result, which was also obtained in [MT15a, Theorem 3.8].

Corollary 3.1.10. *Assume that F is a finite extension of $\mathbb{Q}_2$ of degree n. Let q be the highest power of 2 such that F contains a primitive q-th root of unity. Then the number of Galois $U_4(\mathbb{F}_2)$-extensions of F is*

$$\begin{cases} \dfrac{(2^{n+2}-1)(2^n-1)(2^{n-1}-1)2^{3n+1}}{3} & \text{if } q \neq 2, \\ \dfrac{(2^{n+1}-1)(2^n-1)^2 2^{3n+1}}{3} & \text{if } q = 2. \end{cases}$$

Proof. This follows from Theorem 3.1.1, Lemma 3.1.8 and Lemma 3.1.9. □

3.1.2 The case of characteristic 2

Let F be a field of characteristic 2.

Definition 3.1.11. *A pair $([b]_F, V)$ where b is in F and $V \subseteq F/\wp(F)$ is admissible if* $\dim_{\mathbb{F}_2}(V) = 2$ *and* $\dim_{\mathbb{F}_2}(\langle V, [b]_F\rangle) = 3$.

Lemma 3.1.12. *Assume that $([b]_F, V)$ is admissible. Let $E = F(\wp^{-1}(V))$. Then there exists $\delta \in E$ such that $[Tr_{E/F}(\delta)]_F = [b]_F$.*

Proof. It is clear since we know that the trace map $Tr_{E/F}$ is surjective. □

Definition 3.1.13. *Assume that $([b]_F, V)$ is admissible. Let $E = F(\wp^{-1}(V))$. Then a triple $([b]_F, V, W)$ where W is a free $\mathbb{F}_2[Gal(E/F)]$-submodule of $E/\wp(E)$, is admissible if W is generated by an element $[\delta]_E$ with $[Tr_{E/F}(\delta)]_F = [b]_F$.*

Lemma 3.1.14. *Let $([b]_F, V, W)$ be an admissible triple. Assume that $V = \langle [a]_F, [c]_F\rangle$. Let $E = F(\wp^{-1}(V))$. Assume that W is generated by $[\delta]_E$ as a free $\mathbb{F}_2[Gal(E/F)]$-module with $[Tr_{E/F}(\delta)]_F = [b]_F$. Let $A = Tr_{E/F(\theta_a)}(\delta)$ and $C = Tr_{E/F(\theta_c)}(\delta)$. Then every generator of W as a free $\mathbb{F}_2[Gal(E/F)]$-module is of the form*

$$[\delta']_E = [\delta]_E + \epsilon_A[A]_E + \epsilon_C[C]_E + \epsilon_b[b]_E,$$

where $\epsilon_A, \epsilon_C, \epsilon_b \in \{0, 1\}$.

Furthermore for any generator $[\delta']_E$ of W as a free $\mathbb{F}_2[Gal(E/F)]$-module, we have $[Tr_{E/F}(\delta')]_F = [b]_F$. In particular, this implies that the pair (V, W) determines uniquely $[b]_F$.

Proof. Let $G = Gal(E/F)$. As an $\mathbb{F}_2$-vector space, W is generated by $[\delta]_E, [A]_E, [C]_E, [b]_E$. Let $[\delta']_E$ be an arbitrary generator of the free $\mathbb{F}_2[G]$-module. Then

$$[\delta']_E = \epsilon_\delta[\delta]_E + \epsilon_A[A]_E + \epsilon_C[C]_E + \epsilon_b[b]_E,$$

for some $\epsilon_\delta, \epsilon_A, \epsilon_C, \epsilon_b \in \{0, 1\}$. Suppose that $\epsilon_\delta = 0$, then we see that $(\sum_{\sigma\in G}\sigma)([\delta']_E)$ is trivial in $E/\wp((E))$, a contradiction. Hence $\epsilon_\delta = 1$.

Conversely, assume that $[\delta']_E = [\delta]_E + \epsilon_A[A]_E + \epsilon_C[C]_E + \epsilon_b[b]_E$, for some $\epsilon_A, \epsilon_C, \epsilon_b \in \{0, 1\}$. Let W' be the $\mathbb{F}_2[G]$-module generated by $[\delta']_E$. Then we have $W' \subseteq W$. It is then enough to show that W' is a free $\mathbb{F}_2[G]$-module. Suppose that W' is not free. Then there exists a non-zero ideal $I \subseteq \mathbb{F}_2[G]$ such that I annihilates δ'. But it is known that any non-zero ideal of $\mathbb{F}_2[G]$ contains the element $\sum_{\sigma\in G}\sigma =: N$. Therefore N annihilates $[\delta']_E$. This contradicts the fact that

$$N([\delta']_E)] = [Tr_{E/F}(\delta')]_E = [b]_E \neq 0 \in E/\wp(E). \qquad \square$$

Proposition 3.1.15. *Let $([b]_F, V, W)$ be an admissible triple. Let $E = F(\wp^{-1}V)$. Let $L = E(\wp^{-1}W)$. Then L/F is a Galois $U_4(\mathbb{F}_2)$-extension.*

Proof. Suppose that $V = \langle [a]_F, [c]_F\rangle$ and that W is generated by δ with $Tr_{E/F}(\delta) = b + \wp(d)$, for some $d \in F$. Let $A = Tr_{E/F(\theta_a)}(\delta)$ and $C = Tr_{E/F(\theta_c)}(\delta)$. We first note that $F(\theta_a, \theta_b, \theta_c)/F$ is an abelian 2-elementary extension with Galois group generated by $\sigma_a, \sigma_b, \sigma_c$, where

$$\begin{aligned}
&\sigma_a(\theta_a) = \theta_a + 1, \sigma_a(\theta_b) = \theta_b, \sigma_a(\theta_c) = \theta_c;\\
&\sigma_b(\theta_a) = \theta_a, \sigma_b(\theta_b) = \theta_b + 1, \sigma_b(\theta_c) = \theta_c;\\
&\sigma_c(\theta_a) = \theta_a, \sigma_c(\theta_b) = \theta_b, \sigma_c(\theta_c) = \theta_c + 1.
\end{aligned}$$

Clearly we have

$$\begin{aligned}
\sigma_c(\delta) &= \delta + A,\\
\sigma_a(\delta) &= \delta + C,\\
\sigma_a(A) &= A + b + \wp(d),\\
\sigma_c(C) &= C + b + \wp d.
\end{aligned}$$

Then [MT14a, Proof of Theorem 4.2] show that L/F is a Galois $U_4(F_p)$-extension. Moreover an explicit isomorphism $\rho\colon Gal(L/F) \to U_4(\mathbb{F}_2)$ is given by

$$\sigma_a \mapsto \begin{bmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}, \quad \sigma_b \mapsto \begin{bmatrix}1&0&0&0\\0&1&1&0\\0&0&1&0\\0&0&0&1\end{bmatrix}, \quad \sigma_c \mapsto \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&1\\0&0&0&1\end{bmatrix},$$

for suitable extensions $\sigma_a, \sigma_b, \sigma_c \in Gal(L/F)$ of $\sigma_a, \sigma_b, \sigma_c$. $\square$

Proposition 3.1.16. *There is a natural way to associate an admissible triple $([b]_F, V, W)$ to any given Galois $U_4(\mathbb{F}_2)$-extension L/F.*

Proof. Let $\rho\colon Gal(L/F) \to U_4(\mathbb{F}_2)$ be any isomorphism. Set $\sigma_1 = \rho^{-1}(E_{12})$, $\sigma_2 = \rho^{-1}(E_{23})$, and $\sigma_3 = \rho^{-1}(E_{34})$. Then the commutator subgroup $\Phi = [Gal(L/F), Gal(L/F)]$ is the internal direct sum

$$\Phi = \langle[\sigma_1, \sigma_2]\rangle \oplus \langle[\sigma_2, \sigma_3]\rangle \oplus \langle[[\sigma_1, \sigma_2], \sigma_3]\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^3.$$

Let M be the fixed field of Φ. Then M/F is an abelian 2-elementary extension of F, and $Gal(M/F)$ is the (internal) direct sum

$$Gal(M/F) = \langle\sigma_1|_M\rangle \oplus \langle\sigma_2|_M\rangle \oplus \langle\sigma_3|_M\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^3.$$

Let $[a]_F, [b]_F, [c]_F$ be elements in $F/\wp(F)$ which is dual to $\sigma_1|_M, \sigma_2|_M, \sigma_3|_M$ respectively via the Artin-Schreier theory. Explicitly we require that

$$\sigma_1(\theta_a) = \theta_a + 1, \sigma_1(\theta_b) = \theta_b, \sigma_1(\theta_c) = \theta_c;$$
$$\sigma_2(\theta_a) = \theta_a, \sigma_2(\theta_b) = \theta_b + 1, \sigma_2(\theta_c) = \theta_c;$$
$$\sigma_3(\theta_a) = \theta_a, \sigma_3(\theta_b) = \theta_b, \sigma_3(\theta_c) = \theta_c + 1;$$

Let $E = F(\theta_a, \theta_c)$. Then E is fixed under σ_2, $[\sigma_1, \sigma_2]$, $[\sigma_2, \sigma_3]$ and $[[\sigma_1, \sigma_2], \sigma_3]$. Hence E is fixed under a subgroup H of Gal(L/F) which is generated by σ_2, $[\sigma_1, \sigma_2]$, $[\sigma_2, \sigma_3]$ and $[[\sigma_1, \sigma_2], \sigma_3]$. We have $[L^H : F] = |Gal(L/F)|/|H| = 4$, and $[E : F] = 4$. Therefore $E = L^H$.

Claim: E does not depend on the choice of ρ.

Proof of Claim: Suppose that $\rho' : Gal(L/F) \to U_4(\mathbb{F}_2)$ is another isomorphism. We define $\sigma'_1 = \rho'^{-1}(E_{12})$, $\sigma'_2 = \rho'^{-1}(E_{23})$, and $\sigma'_3 = \rho'^{-1}(E_{34})$. Let H' be the group generated by σ'_2, $[\sigma'_1, \sigma'_2]$, $[\sigma'_2, \sigma'_3]$ and $[[\sigma'_1, \sigma'_2], \sigma'_3]$. We need to show that $H = H'$. We first note that σ_2 and σ'_2 commute with every element in Φ.

We have $\sigma'_2|_M$ is in $Gal(M/F) = \langle \sigma_1|_M \rangle \oplus \langle \sigma_2|_M \rangle \oplus \langle \sigma_3|_M \rangle$.

Hence modulo the subgroup Φ, σ'_2 is equal to one of the following element $\sigma_1, \sigma_2, \sigma_3$, $\sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_3, \sigma_1\sigma_2\sigma_3$.

If $\sigma'_2 = \sigma_1$, or $\sigma_1\sigma_2$, or $\sigma_1\sigma_3$, or $\sigma_1\sigma_2\sigma_3$ modulo Φ, then

$$[[\sigma_2, \sigma_3], \sigma'_2] = [[\sigma_2, \sigma_3], \sigma_1],$$

which is impossible since $[[\sigma_2, \sigma_3], \sigma_1]$ is non trivial but $[[\sigma_2, \sigma_3], \sigma'_2]$ is trivial.

If $\sigma'_2 = \sigma_3$, or $\sigma_2\sigma_3$ modulo Φ, then

$$[[\sigma_1, \sigma_2], \sigma'_2] = [[\sigma_1, \sigma_2], \sigma_3],$$

which is impossible since $[[\sigma_1, \sigma_2], \sigma_3]$ is non trivial but $[[\sigma_1, \sigma_2], \sigma'_2]$ is trivial.

From the above discussion we see that $\sigma'_2 \equiv \sigma_2 \bmod \Phi$. This implies that $[b]_F$ does not depend on the choice of ρ and that $H' = H$. Thus E does not depend on the choice of ρ also.

We have an exact sequence

$$1 \to Gal(L/E) \to Gal(L/F) \to Gal(E/F) = G \to 1.$$

Then $Gal(L/E)$ is an $\mathbb{F}_2[G]$ module where the action is by conjugation. We also have the G-equivariant Artin-Schreier pairing

$$\frac{E \cap \wp(L)}{\wp(E)} \times Gal(L/E) \to \mathbb{F}_2.$$

As an $\mathbb{F}_2$-vector space $Gal(L/E)$ has a basis consisting of σ_2, $[\sigma_1, \sigma_2]$, $[\sigma_2, \sigma_3]$ and $[[\sigma_1, \sigma_2], \sigma_3]$. Let $[\delta]_E$ be an element dual to $[[\sigma_1, \sigma_2], \sigma_3]$. Then $Tr_{E/F}(\delta) \equiv b \bmod \wp(E)$. Hence $Tr_{E/F}(\delta)$ is in $(b + \wp(F)) \cup (b + a + \wp(F)) \cup (b + c + \wp(F)) \cup (b + a + c + \wp(F)^2)$.

Let $A = Tr_{E/F(\theta_a)}(\delta)$ and $C = Tr_{E/F(\theta_c)}(\delta)$. Suppose that $Tr_{E/F}(\delta) \equiv b + a \mod \wp(F)$. Then $Tr_{F(\theta_a)/F}(A) = b + a + \wp(f)$ for some $f \in F$. Hence $\sigma_1(A) = A + b + a + \wp(f)$. Thus

$$\sigma_1(\theta_A) = \theta_A + \theta_b + \theta_a + f + i,$$

for some $i \in \{0, 1\}$. Therefore

$$\begin{aligned}\sigma_1^2(\theta_A) &= \sigma_1(\theta_A) + \sigma_1(\theta_b) + \sigma_1(\theta_a) + f + i \\ &= \theta_A + \theta_b + \theta_a + f + i + \theta_b + \theta_a + 1 + f + i \\ &= \theta_A + 1.\end{aligned}$$

This implies that σ_1 is not of order 2, a contradiction. Hence we have $Nm_{E/F}(\delta)$ is not in $b + a + \wp(F)$.

Similarly we can show that $Nm_{E/F}(\delta)$ is not in $(b + c + \wp(F)) \cup (b + a + \wp(F)$. Therefore

$$Tr_{E/F}(\delta) \equiv b \bmod \wp(F).$$

We set $V = \langle [a]_F, [c]_F \rangle$. Then V does not depend on the choice of ρ, and the pair $([b]_F, V)$ is admissible. Let W be the $\mathbb{F}_2[G]$-submodule of $E/\wp(E)$ which is dual via the Artin-Schreier theory to $Gal(L/E)$. Then W is does not depend on choice of ρ, and W is free and generated by δ. Since $[Tr_{E/F}(\delta)]_F = [b]_F$, we see that the triple $([b]_F, V, W)$ is admissible. Since $[b]_F$ is uniquely determined by (V, W), we see that $[b]_F$ does not depend on the choice of ρ.

□

Theorem 3.1.2. *Let F be a field of characteristic 2. There is a natural one-one correspondence between the set of admissible triples $([b]_F, V, W)$ and the set of Galois $U_4(\mathbb{F}_2)$ extensions L/F.*

Proof. By Proposition 3.1.15 we have a map μ from the set of admissible triples $([b]_F, V, W)$ to the set of Galois $U_4(\mathbb{F}_2)$-extensions L/F. By Proposition 3.1.7 we have a map η from the set of Galois $U_4(\mathbb{F}_2)$-extensions L/F to the set of admissible triples $([b]_F, V, W)$. We show that μ and η are the inverses of each other.

Let $([b]_F, V, W)$ be an admissible triple. Via the map μ we obtain a $U_4(\mathbb{F}_2)$-extension L/F. Explicitly, if $V = \langle [a]_F, [c]_F \rangle$ and $E = F(\sqrt{a}, \sqrt{c})$, then $L = E(\sqrt{W})$ and there is an isomorphism $\rho\colon Gal(L/F) \simeq U_4(\mathbb{F}_2)$ such that $\rho^{-1}(E_{12}) = \sigma_a$, $\rho^{-1}(E_{23}) = \sigma_b$, $\rho^{-1}(E_{34}) = \sigma_c$. (Here $\sigma_a, \sigma_b, \sigma_c$ are defined as in Proposition 3.1.6.) We apply the construction in Proposition 3.1.16 with this isomorphism ρ. Then we obtain back the admissible triple $([b]_F, V, W)$.

Now let L/F be a $U_4(\mathbb{F}_2)$-extension. Then via the map η we obtain an admissible triple $([b]_F, V, W)$. Since $L = F(\sqrt{V})(W)$, we see that μ sends the triple $([b]_F, V, W)$ back to the extension L/F □

Lemma 3.1.17. *Assume that* $\dim_{\mathbb{F}_2}(F/\wp(F)) = n < \infty$. *Then the number N of admissible pairs* $([b]_F, V)$ *is* $\dfrac{4(2^n-1)(2^{n-1}-1)(2^{n-2}-1)}{3}$.

Proof. Recall that the Gaussian binomial coefficients are defined by

$$\binom{n}{r}_q = \begin{cases} \dfrac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-r+1}-1)}{(q-1)(q^2-1)\cdots(q^r-1)} & \text{if } r \le n \\ 0 & \text{if } r > n. \end{cases}$$

Every admissible pair $([b]_F, V)$ can be obtained as follows. First, we choose a three dimensional $\mathbb{F}_2$-subspace V' of $F/\wp(F)$. The number of choices of such V' is $\binom{n}{3}_2$. Then we choose a two dimensional $\mathbb{F}_2$-subspace V of V'. The number of choices of such V is $\binom{3}{2}_2$. Finally, we choose a vector $[b]_F$ in $V' \setminus V$. The number of choices of such b is $8 - 4 = 4$. Therefore we have

$$N = \binom{n}{3}_2 \times \binom{3}{2}_2 \times 4 = \frac{4(2^n-1)(2^{n-1}-1)(2^{n-2}-1)}{3}. \qquad \square$$

Lemma 3.1.18. *Assume that* $\dim_{\mathbb{F}_2}(F/\wp(F)) = n < \infty$. *Let* $([b]_F, V)$ *be a fixed admissible pair. Then* $n \ge 3$ *and the number of admissible triples* $([b]_F, V, W)$ *is* 2^{3n-6}.

Proof. Since there exists at least one admissible pair, namely $([b]_F, V)$, we see that $n \ge 3$.

It is known that for a field L of characteristic 2, then the maximal pro-2-quotient $G_L(2)$ of the absolute Galois group of L is free of rank $\dim_{\mathbb{F}_2}(L/\wp(L))$. (See [Koc02, Theorem 9.1].)

Let $E = F(\wp^{-1}(V))$. Then $G_E(2)$ is a (closed) subgroup of index 4 in the free pro-2-group $G_F(2)$ of rank n. Thus $G_E(2)$ is also free and of rank $4n - 3$.

Consider the surjective homomorphism $Tr\colon \dfrac{E}{\wp(E)} \to \dfrac{F}{\wp(F)}$. We have

$$|\ker(Tr)| = \left|\frac{E}{\wp(E)}\right| \Big/ \left|\frac{F}{\wp(F)}\right| = 2^{4n-3}/2^n = 2^{3n-3}.$$

Hence

$$|\{[\delta]_E \colon [Tr_{E/F}(\delta)]_F = [b]_F\}| = |\ker Tr| = 2^{3n-3}.$$

Therefore the number of W such that $([b]_F, V, W)$ is admissible, is $2^{3n-3}/8 = 2^{3n-6}$. $\square$

Corollary 3.1.19. *Assume that* $\dim_{\mathbb{F}_2}(F/\wp(F)) = n < \infty$. *Then the number of Galois* $U_4(\mathbb{F}_2)$*-extensions* L/F *is* $\dfrac{(2^n-1)(2^{n-1}-1)(2^{n-2}-1)2^{3n-4}}{3}$.

In the next proposition we show in particular that for each natural number n there exists a field satisfying the hypothesis of the above corollary.

Proposition 3.1.20. *Let p a prime number. Then for each cardinal number C there exists a field K of characteristic p such that* $[K : \wp(K)] = C$.

Proof. Consider any $\mathbb{F}_p$-vector space V such that $\dim_{\mathbb{F}_p}(V)$ is C. Let $V^* = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ be the Pontrjagin dual of V. Then V^* is a profinite (abelian) group. By [Wat74, Theorem 2] there exists a field F of characteristic p such that F admits a Galois extension L/F with $Gal(L/F) = V^*$. By the Artin-Schreier theory we conclude that $\mathrm{Hom}_{cont}(V^*, \mathbb{F}_p) = H^1(V^*, \mathbb{F}_p)$, which is isomorphic canonically with V via Pontrjagin duality, is isomorphic to $A/\wp(F)$,where A is some subgroup of F containing $\wp(F)$. Hence the $\mathbb{F}_2$-dimension of $A/\wp(F)$ is C.

Now consider a maximal Galois extension K/F in the maximal p-extension $F(p)$ of F such that: (*) the natural map $A/\wp(F) \to K/\wp(K)$ is an injection.

Claim 1: Such an extension K/F exists.

Proof: Let $\mathcal{S}$ be the set of all field extensions K over F in $F(p)$ satisfying the condition (*). Then $\mathcal{S}$ is not empty since it contains at least F. This set is partially ordered by set inclusion. We shall apply apply Zorn's lemma. We take a non-empty totally ordered subset $\mathcal{T}$ of $\mathcal{S}$. Let K be the union of all fields K_i in $\mathcal{T}$. Clearly K/F is a field extension and $K \subseteq F(p)$. Consider the natural map $A\wp(K) \to K/\wp(K)$. Suppose that this map is not injective. Then $A \cap \wp(K)$ is strictly larger than $\wp(F)$. However $A \cap \wp(K) = \bigcup_{K_i \in \mathcal{T}}(A \cap \wp(K_i))$. Thus there exists a field $K_i \in \mathcal{T}$ such that $A \cap \wp(K_i)$ is strictly larger than $\wp(F)$. This implies that the natural map $A/\wp(F) \to K_i/\wp(K_i)$ is not injective, which contradicts to the condition that K_i satisfies (*). Therefore the map $A\wp(K) \to K/\wp(K)$ is injective and K is in $\mathcal{T}$. Clearly K is greater than every element in $\mathcal{T}$. The Claim then follows from Zorn's lemma.

Claim 2: The above injection $A/\wp(F) \to K/\wp(K)$ is an isomorphism.

Proof: If the injection is not an isomorphism, then there exists an element u in K such that $u \not\equiv a \bmod \wp(K)$ for every $a \in A$. We have $A \cap (iu + \wp(K)) = \emptyset$ for every $i = 1, 2 \ldots, p-1$. Let $T = K(\theta_u)$. Then T is strictly larger than K and $T \subseteq F(p)$. We have

$$A \cap \wp(T) = A \cap (K \cap \wp(T)) = A \cap [\bigcup_{i=0}^{p-1}(iu + \wp(K))] = A \cap \wp(K) = \wp(F).$$

We consider the natural map $\eta\colon A/\wp(F) \to T/\wp(T)$. Then $\ker(\eta) = \dfrac{A \cap \wp(T)}{\wp(F)} = 0$. Thus η is injective. This contradicts the maximality of K. □

3.2 The case $F = \mathbb{Q}_2$

In this section we consider some fixed algebraic separable closure of $\mathbb{Q}_2$ and all following Galois extensions live inside this separable closure.

There are exactly 16 $U_4(\mathbb{F}_2)$-extensions of $\mathbb{Q}_2$ [MT14a, Theorem 3.7]. By [MT15b],

$$\mathbb{Q}_2\left(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{A}, \sqrt{C}, \sqrt{\delta}\right)$$

is a $U_4(\mathbb{F}_2)-$extension of $\mathbb{Q}_2$ with a, b and c in the field $\mathbb{Q}_2$ such that $(a,b) = (b,c) = 0$ (norm residue symbol, Section 1.4), also $\alpha \in \mathbb{Q}_2(\sqrt{a})$ and $\gamma \in \mathbb{Q}_2(\sqrt{c})$ such that

$$Nm_{\mathbb{Q}_2(\sqrt{a})/\mathbb{Q}_2}(\alpha) = b = Nm_{\mathbb{Q}_2(\sqrt{c})/\mathbb{Q}_2}(\gamma).$$

In addition A, C and δ are as follows. By section 1.7, assume $e = \frac{\alpha}{\alpha+\gamma}$ and $B = \gamma/\alpha$, so we have

$$A = Nm_{\sigma_c}(e) = \frac{\alpha^2\gamma}{(\alpha+\gamma)(\alpha\gamma+b)},$$
$$C = Nm_{\sigma_a}(eB) = \frac{\alpha\gamma^2}{(\alpha+\gamma)(\alpha\gamma+b)},$$

and

$$\delta = \alpha + \beta.$$

Lemma 3.2.1. *There is an $f \in \mathbb{Q}_2$ such that*

$$A = N_{\sigma_c}(e) = f\alpha$$

and

$$C = N_{\sigma_a}(eB) = f\gamma.$$

In particular,

$$f = \frac{\alpha\gamma}{(\alpha+\gamma)(\alpha\gamma+b)} \in \mathbb{Q}_2$$

Proof: Since $\alpha, \gamma \neq 0$, we have

$$f = \frac{\alpha\gamma}{(\alpha+\gamma)(\alpha\gamma+b)} = \frac{1}{(\alpha/\gamma+1)(\gamma+b/\alpha)} = \frac{1}{\alpha+\bar{\alpha}+\gamma+\bar{\gamma}} \in \mathbb{Q}_2.$$

Also, because all elements of $\mathbb{Q}_2$ are square in $\mathbb{Q}_2\left(\sqrt{a},\ \sqrt{b},\ \sqrt{c}\right)$, we have

$$\mathbb{Q}_2\left(\sqrt{a},\ \sqrt{b},\ \sqrt{c},\ \sqrt{A},\ \sqrt{C},\ \sqrt{\delta}\right) = \mathbb{Q}_2\left(\sqrt{a},\ \sqrt{b},\ \sqrt{c},\ \sqrt{\alpha},\ \sqrt{\gamma},\ \sqrt{\alpha+\gamma}\right)$$

□

By lemma 2.2.1 (or similarly [Lam05, Corollary 2.24]), $\{-1, 2, 5\}$ is an $\mathbb{F}_2-$basis of $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$, so

$$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} = \{1, -1, 2, 5, -2, -5, 10, -10\}.$$

The unique quaternion division algebra corresponds to $(-1,-1) = (2,5) = 1$ (see lemma 2.2.1), so the rest of the following possibilities correspond to $(\mathbb{Z}/2\mathbb{Z})^3-$extensions of $\mathbb{Q}_2$.

$$A_1 = \{(2,-1) = (-1,5) = 0, (2,-1) = (-1,10) = 0, (5,-1) = (-1,10) = 0\}$$
$$A_2 = \{(2,-2) = (-2,-10) = 0, (2,-2) = (-2,-5) = 0, (-10,-2) = (-2,-5) = 0\}$$
$$A_3 = \{(5,-5) = (-5,-10) = 0, (5,-5) = (-5,-2) = 0, (-10,-5) = (-5,-2) = 0\}$$
$$A_4 = \{(-2,-10) = (-10,10) = 0, (-2,-10) = (-10,-5) = 0, (10,-10) = (-10,-5) = 0\}$$

Since each set A_i for $i = 1, 2, 3, 4$ generates the same $(\mathbb{Z}/2\mathbb{Z})^3-$extensions of $\mathbb{Q}_2$, by Theorem 3.1.1, they generate the same $U_4(\mathbb{F}_2)-$extensions. Hence, there are four cases for b; $b = -1, -2, -5$ and -10.

3.2.1 $b = -1$

For $b = -1$, a and c can be as follows: $(a = 2, c = 10)$, $(a = 2, c = 5)$ or $(a = 10, c = 5)$. These three possibilities for a and c generate the same $U_4(\mathbb{F}_2)$-extensions of $\mathbb{Q}_2$. Assume $(a = 2, b = -1, c = 10)$.

Let $\epsilon_1 = 1 + \sqrt{2}$, $\epsilon_2 = 3 + \sqrt{2}$, $\epsilon_3 = 1 + \sqrt{10}$ and $\epsilon_4 = 3 + \sqrt{10}$. We have:

$$Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\epsilon_1) = -1$$
$$Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\epsilon_2) = 7 = (-7)(-1)$$
$$Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(\epsilon_3) = -9 = (9)(-1)$$
$$Nm_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}(\epsilon_4) = -1.$$

Note: -7 and 9 are squares in $\mathbb{Q}_2$. Set

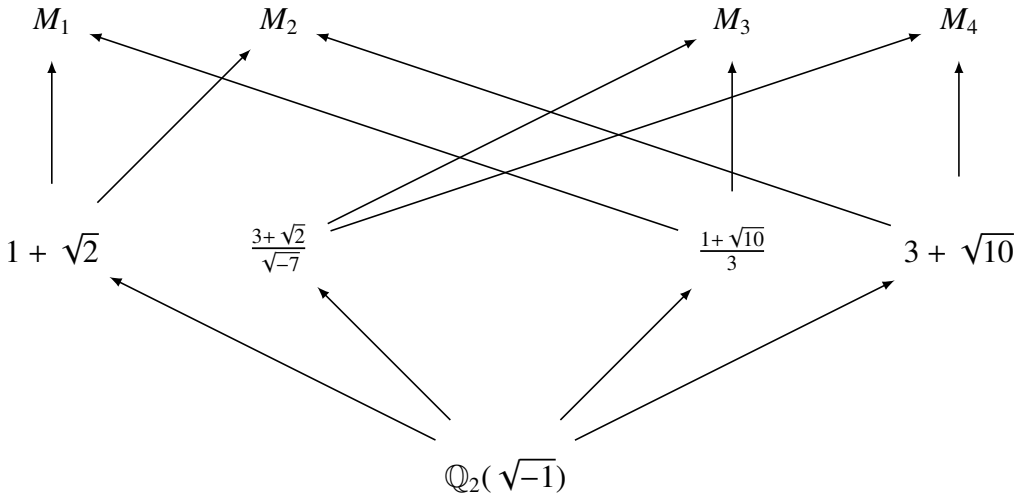
$$\alpha = 1 + \sqrt{2}, \qquad \alpha' = \frac{3 + \sqrt{2}}{\sqrt{-7}};$$
$$\gamma = 3 + \sqrt{10}, \qquad \gamma' = \frac{1 + \sqrt{10}}{3};$$

where $\sqrt{-7} = 1 + 2^2 + 2^4 + 2^5 + \cdots \in \mathbb{Q}_2$. We define

$$\delta_1 := \alpha + \gamma; \quad \delta_2 := \alpha + \gamma'; \quad \delta_3 := \alpha' + \gamma; \quad \delta_4 := \alpha' + \gamma';$$

and

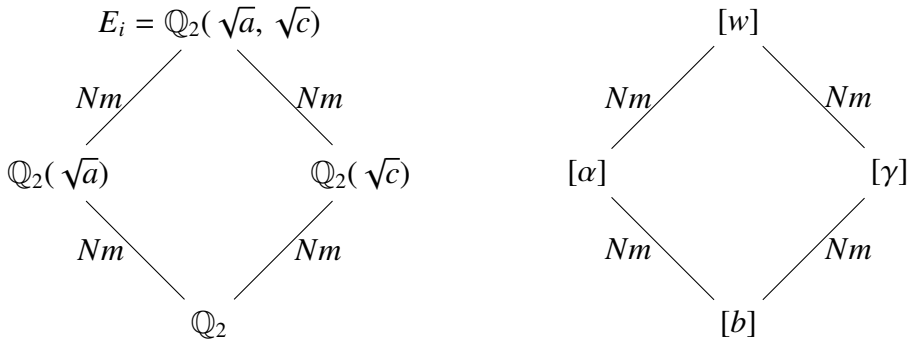
$$M_1 := \mathbb{Q}_2(\sqrt{2}, \sqrt{-1}, \sqrt{10}, \sqrt{\alpha}, \sqrt{\gamma}, \sqrt{\delta_1}),$$
$$M_2 := \mathbb{Q}_2(\sqrt{2}, \sqrt{-1}, \sqrt{10}, \sqrt{\alpha}, \sqrt{\gamma'}, \sqrt{\delta_2}),$$
$$M_3 := \mathbb{Q}_2(\sqrt{2}, \sqrt{-1}, \sqrt{10}, \sqrt{\alpha'}, \sqrt{\gamma}, \sqrt{\delta_3}),$$
$$M_4 := \mathbb{Q}_2(\sqrt{2}, \sqrt{-1}, \sqrt{10}, \sqrt{\alpha'}, \sqrt{\gamma'}, \sqrt{\delta_4}).$$



Distinction of M_1, M_2, M_3 and M_4

Notation: Denote by $[a]$, the square class of a in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ and by $[a]_F$, the square class of a in $F^\times/F^{\times 2}$ (unless specified).

We have the following diagram for each M_i:



for some $w \in W_i$ with $W_i = \langle [\delta_i], [\alpha_i], [\gamma_i], [b] \rangle$ is a $\mathbb{F}_2(Gal(E_i/\mathbb{Q}_2))-$module in $E_i^\times/E_i^{\times 2}$. By [MT15b], we have $M_i = E_i(\sqrt{W_i})$. Also by Kummer theory and Theorem 3.1.1, we have $M_i^{\times 2} \cap E_i = W_i$; therefore

$$M_i = M_j \Rightarrow W_i = W_j.$$

Now if $W_i = W_j$ then we can write δ_i as follows:

$$\delta_i = \delta_j^{\epsilon_1} \alpha_j^{\epsilon_2} \gamma_j^{\epsilon_3} b^{\epsilon_4} e^2$$

where $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$.

The strategy to show $M_i \neq M_j$ for $i \neq j$ is to assume $W_i = W_j$ and to find a contradiction using norm of the last equality.

Claim: $M_1 \neq M_2$

For M_1, we have $b = -1$, $\alpha_1 = 1 + \sqrt{2}$, $\gamma_1 = (1 + \sqrt{10})/3$ and $\delta_1 = (4 + 3\sqrt{2} + \sqrt{10})/3$, therefore

$$W_1 = \langle [\delta_1], [1 + \sqrt{2}], [(1 + \sqrt{10})/3], [-1] \rangle.$$

For M_2, we have $b = -1$, $\alpha_2 = 1 + \sqrt{2}$, $\gamma_2 = 3 + \sqrt{10}$ and $\delta_2 = 4 + \sqrt{2} + \sqrt{10}$, therefore

$$W_2 = \langle [\delta_2], [1 + \sqrt{2}], [3 + \sqrt{10}], [-1] \rangle.$$

We assume $W_1 = W_2$, then we can write $\delta_1 = \delta_2^{\epsilon_1} \alpha_2^{\epsilon_2} \gamma_2^{\epsilon_3} b^{\epsilon_4} e^2$ for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. Therefore

$$Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_1) = Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_2)^{\epsilon_1} Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\alpha_2)^{\epsilon_2} Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\gamma_2)^{\epsilon_3} Nm_{E/\mathbb{Q}_2(\sqrt{2})}(b)^{\epsilon_4} Nm_{E/\mathbb{Q}_2(\sqrt{2})}(e^2)$$

On the other hand, we have $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_1) = 8/3(1+\sqrt{2})$ and $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_2) = 8(1+\sqrt{2})$, also $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\alpha_2) = (1+\sqrt{2})^2$, $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\gamma_2) = -1$ and $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(b) = b^2$. Therefore

$$\frac{8/3(1+\sqrt{2})}{(8(1+\sqrt{2}))^{\epsilon_1}(-1)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{2})^{\times 2}.$$

For $\epsilon_1 = 0$ from the last equation, we have $\pm 1/3(1+\sqrt{2}) \in \mathbb{Q}_2(\sqrt{2})^{\times 2}$, but this is a contradiction. Also, for $\epsilon_1 = 1$ from the last equation, we have $\pm 1/3 \in \mathbb{Q}_2(\sqrt{2})^{\times 2}$, but this is a contradiction too. Hence $W_1 \neq W_2$, and we conclude $M_1 \neq M_2$.

Claim: $M_2 \neq M_3$

W_2 is as above. For M_3, we have $b = -1$, $\alpha_3 = (3+\sqrt{2})/\sqrt{-7}$, $\gamma_3 = (1+\sqrt{10})/3$ and $\delta_3 = 3(3+\sqrt{2}) + \sqrt{-7}(1+\sqrt{10})$, therefore

$$W_1 = \langle [\delta_1], [(3+\sqrt{2})/\sqrt{-7}], [(1+\sqrt{10})/3], [-1] \rangle.$$

If we assume $W_2 = W_3$ then we can write $\delta_2 = \delta_3^{\epsilon_1}\alpha_3^{\epsilon_2}\gamma_3^{\epsilon_3}b^{\epsilon_4}e^2$ for some $\epsilon_1, \cdots \epsilon_4 \in \{0,1\}$ and $e \in E^\times$. Now take norms, $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\delta_2) = 8(3+\sqrt{10})$ and $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\delta_3) = \frac{18\sqrt{-7}-14}{-21}\frac{1+\sqrt{10}}{3}$, also $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\alpha_3) = -1$, $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\gamma_3) = (1+\sqrt{10})^2/9$ and $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(b) = b^2$. Therefore

$$\frac{8(3+\sqrt{10})}{\left(\frac{18\sqrt{-7}-14}{-21}\cdot\frac{1+\sqrt{10}}{3}\right)^{\epsilon_1}(-1)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{10})^{\times 2}.$$

For $\epsilon_1 = 0$ from the last equation, we have $\pm 8(3+\sqrt{10}) \in \mathbb{Q}_2(\sqrt{10})^{\times 2}$, but this is a contradiction. Also, for $\epsilon_1 = 1$ from the last equation, we have

$$\pm\frac{1}{8(3+\sqrt{10})}\cdot\frac{18\sqrt{-7}-14}{-21}\cdot\frac{1+\sqrt{10}}{3} \in \mathbb{Q}_2(\sqrt{10})^{\times 2}.$$

On the other hand, because

$$N_{\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2}\left(\frac{1+\sqrt{10}}{3(3+\sqrt{10})}\right) = 1,$$

we know that

$$\frac{1+\sqrt{10}}{3(3+\sqrt{10})} = f\cdot k^2 \qquad \text{for some} \qquad f \in \mathbb{Q}_2 \text{ and } k \in \mathbb{Q}_2(\sqrt{10}).$$

Let us find f and k as above. Set

$$t := \frac{1+\sqrt{10}}{3(3+\sqrt{10})} \qquad \text{and} \qquad l := t+1 = \frac{10+4\sqrt{10}}{3(3+\sqrt{10})}.$$

Therefore $\sigma(l) = l\sigma(t)$ for some $1 \neq \sigma \in Gal(\mathbb{Q}_2(\sqrt{10})/\mathbb{Q}_2)$. So we have $\sigma(l)/l = \sigma(t)$ and $l/\sigma(l) = l$, therefore

$$\frac{1+\sqrt{10}}{3(3+\sqrt{10})} = t = \frac{l^2}{Nm(l)} = \left(\frac{10+4\sqrt{10}}{3(3+\sqrt{10})}\right)^2\cdot\frac{9}{60}.$$

Therefore,

$$\pm\frac{18\sqrt{-7}-14}{8(-21)}\cdot\frac{9}{60}=\pm\frac{9\sqrt{-7}-7}{5}\cdot\left(\frac{1}{4\sqrt{-7}}\right)^2\in\mathbb{Q}_2(\sqrt{10})^{\times 2},$$

but with the choice of $\sqrt{-7}=1+2^2+2^4+2^5\cdots$, we have $\frac{9\sqrt{-7}-7}{5}=1+2+2^3+2^5+\cdots\notin(\pm1)\mathbb{Q}_2(\sqrt{10})^{\times 2}$, and this is a contradiction too. Hence $W_2\neq W_3$, and we conclude $M_2\neq M_3$.

Claim: $M_3\neq M_4$

W_3 is as above. For M_4, we have $b=-1$, $\alpha_4=(3+\sqrt{2})/\sqrt{-7}$, $\gamma_4=3+\sqrt{10}$ and $\delta_4=3+\sqrt{2}+\sqrt{-7}(1+\sqrt{10})$, therefore

$$W_4=\langle[\delta_4],[(3+\sqrt{2})/\sqrt{-7}],[3+\sqrt{10}],[-1]\rangle.$$

we assume $W_3=W_4$, then we can write $\delta_3=\delta_4^{\epsilon_1}\alpha_4^{\epsilon_2}\gamma_4^{\epsilon_3}b^{\epsilon_4}e^2$ for some $\epsilon_1,\cdots\epsilon_4\in\{0,1\}$ and $e\in E^\times$. Now take norms, $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\delta_3)=\frac{18\sqrt{-7}-14}{-21}\frac{1+\sqrt{10}}{3}$ and $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\delta_4)=\frac{6+6\sqrt{-7}}{\sqrt{-7}}(3+\sqrt{10})$, also $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\alpha_3)=-1$, $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\gamma_3)=(3+\sqrt{10})^2$ and $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(b)=b^2$. Therefore

$$\frac{\frac{18\sqrt{-7}-14}{-21}\cdot\frac{1+\sqrt{10}}{3}}{\left(\frac{6+6\sqrt{-7}}{\sqrt{-7}}(3+\sqrt{10})\right)^{\epsilon_1}(-1)^{\epsilon_3}}\in\mathbb{Q}_2(\sqrt{10})^{\times 2}.$$

For $\epsilon_1=0$, from the last equation, we have $\pm\frac{18\sqrt{-7}-14}{-21}\cdot\frac{1+\sqrt{10}}{3}\in\mathbb{Q}_2(\sqrt{10})^{\times 2}$, but this is a contradiction. Also, for $\epsilon_1=1$, from the last equation, we have

$$\pm\frac{\sqrt{-7}}{6+6\sqrt{-7}}\cdot\frac{18\sqrt{-7}-14}{-21}\cdot\frac{1+\sqrt{10}}{3(3+\sqrt{10})}\in\mathbb{Q}_2(\sqrt{10})^{\times 2}.$$

Therefore,

$$\pm\frac{\sqrt{-7}}{6+6\sqrt{-7}}\cdot\frac{18\sqrt{-7}-14}{-21}\cdot\frac{9}{60}\in\mathbb{Q}_2(\sqrt{10})^{\times 2},$$

so,

$$\frac{1}{3}(-7+\sqrt{-7})\in\mathbb{Q}_2(\sqrt{10})^{\times 2},$$

but $1/3(-7+\sqrt{-7})=2+2^3+2^4+\cdots\notin(\pm1)\mathbb{Q}_2(\sqrt{10})^{\times 2}$ and this is a contradiction too. Hence $W_3\neq W_4$, and we conclude $M_3\neq M_4$.

Claim: $M_1\neq M_3$

Assume $W_1=W_3$ then we can write $\delta_1=\delta_3^{\epsilon_1}\alpha_3^{\epsilon_2}\gamma_3^{\epsilon_3}b^{\epsilon_4}e^2$ for some $\epsilon_1,\cdots\epsilon_4\in\{0,1\}$ and $e\in E^\times$. Now take norms, $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_1)=8/3(1+\sqrt{2})$ and $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_3)=\frac{-14+18\sqrt{-7}}{-21}\cdot\frac{3+\sqrt{2}}{\sqrt{-7}}$, also $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\alpha_3)=-1$, $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\gamma_3)=(1+\sqrt{10})^2/9$ and $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(b)=b^2$.

Since

$$Nm_{E/\mathbb{Q}_2(\sqrt{2})}\left(\frac{3+\sqrt{2}}{\sqrt{-7}(1+\sqrt{2})}\right)=1,$$

we have

$$\frac{3+\sqrt{2}}{\sqrt{-7}(1+\sqrt{2})} = f \cdot k^2 \qquad \text{for some} \qquad f \in \mathbb{Q}_2 \text{ and } k \in \mathbb{Q}_2(\sqrt{2}).$$

Let us find f and k as above. Set

$$t := \frac{3+\sqrt{2}}{\sqrt{-7}(1+\sqrt{2})} \qquad \text{and} \qquad l := t+1 = \frac{3+\sqrt{-7}+(1+\sqrt{-7})\sqrt{2}}{\sqrt{-7}(1+\sqrt{2})}.$$

Therefore $\sigma(l) = l\sigma(t)$ for some $1 \neq \sigma \in Gal(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)$. So we have $\sigma(l)/l = \sigma(t)$ and $l/\sigma(l) = l$, therefore

$$\frac{3+\sqrt{2}}{\sqrt{-7}(1+\sqrt{2})} = t = \frac{l^2}{Nm(l)} = \left(\frac{3+\sqrt{-7}+(1+\sqrt{-7})\sqrt{2}}{\sqrt{-7}(1+\sqrt{2})}\right)^2 \cdot \frac{7}{14+2\sqrt{-7}}.$$

Therefore

$$\frac{(-1/21)(-14+18\sqrt{-7})(1/\sqrt{-7})(3+\sqrt{2})}{(8/3(1+\sqrt{2}))^{\epsilon_1}(-1)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{2})^{\times 2}.$$

For $\epsilon_1 = 0$, from the last equation, we have $\pm\frac{-14+18\sqrt{-7}}{-21} \cdot \frac{3+\sqrt{2}}{\sqrt{-7}} \in \mathbb{Q}_2(\sqrt{2})^{\times 2}$, but this is a contradiction. Also, for $\epsilon_1 = 1$, from the last equation, we have

$$\pm\frac{-14+18\sqrt{-7}}{-21} \cdot \frac{3+\sqrt{2}}{\sqrt{-7}} \frac{3}{8(1+\sqrt{2})} \in \mathbb{Q}_2(\sqrt{2})^{\times 2}.$$

Therefore,

$$\pm\sqrt{-7}-2 \in \mathbb{Q}_2(\sqrt{2})^{\times 2}.$$

but $\sqrt{-7}-2 = 1+2+2^4+\cdots \notin (\pm 1)\mathbb{Q}_2(\sqrt{2})^{\times 2}$ and this is a contradiction too. Hence $W_1 \neq W_3$, and we conclude $M_1 \neq M_3$.

Claim: $M_1 \neq M_4$

Assume $W_1 = W_4$ then we can write $\delta_1 = \delta_4^{\epsilon_1}\alpha_4^{\epsilon_2}\gamma_4^{\epsilon_3}b^{\epsilon_4}e^2$ for some $\epsilon_1, \cdots \epsilon_4 \in \{0,1\}$ and $e \in E^\times$. Now take norms, $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\delta_1) = 8/9(1+\sqrt{10})$ and $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\delta_4) = \frac{6+6\sqrt{-7}}{\sqrt{-7}} \cdot (3+\sqrt{10})$, also $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\alpha_4) = -1$, $Nm_{E/\mathbb{Q}_2(\sqrt{10})}(\gamma_4) = (3+\sqrt{10})^2$ and $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(b) = b^2$.
Therefore

$$\frac{8/9(1+\sqrt{10})}{\left((1/\sqrt{-7})(6+6\sqrt{-7})(3+\sqrt{10})\right)^{\epsilon_1}(-1)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{10})^{\times 2}.$$

For $\epsilon_1 = 0$, from the last equation, we have $\pm 8/9(1+\sqrt{10}) \in \mathbb{Q}_2(\sqrt{10})^{\times 2}$, but this is a contradiction. Also, for $\epsilon_1 = 1$, from the last equation and

$$\frac{1+\sqrt{10}}{3(3+\sqrt{10})} = \left(\frac{10+4\sqrt{10}}{3(3+\sqrt{10})}\right)^2 \cdot \frac{9}{60}.$$

we have

$$\pm\frac{6+6\sqrt{-7}}{\sqrt{-7}}\cdot(3+\sqrt{10})\cdot\frac{9}{8(1+\sqrt{10})}\in\mathbb{Q}_2(\sqrt{10})^{\times 2}.$$

Therefore,

$$\pm 3/2(\sqrt{-7}-7)\in\mathbb{Q}_2(\sqrt{10})^{\times 2}.$$

but $3/2(\sqrt{-7}-7)=1+2^2+2^8+\cdots\notin(\pm 1)\mathbb{Q}_2(\sqrt{10})^{\times 2}$ and this is a contradiction too. Hence $W_1\neq W_4$, and we conclude $M_1\neq M_4$.

Claim: $M_2\neq M_4$

Assume $W_2=W_4$ then we can write $\delta_2=\delta_4^{\epsilon_1}\alpha_4^{\epsilon_2}\gamma_4^{\epsilon_3}b^{\epsilon_4}e^2$ for some $\epsilon_1,\cdots\epsilon_4\in\{0,1\}$ and $e\in E^\times$. Now take norm, $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_2)=8(1+\sqrt{2})$ and $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_4)=\frac{6+6\sqrt{-7}}{\sqrt{-7}}\cdot\frac{3+\sqrt{2}}{\sqrt{-7}}$, also $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\alpha_4)=(3+\sqrt{2})^2$, $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\gamma_4)=-1$ and $Nm_{E/\mathbb{Q}_2(\sqrt{2})}(b)=b^2$.
Therefore

$$\frac{8(1+\sqrt{2})}{\left((-1/7)(6+6\sqrt{-7})(3+\sqrt{2})\right)^{\epsilon_1}(-1)^{\epsilon_3}}\in\mathbb{Q}_2(\sqrt{2})^{\times 2}$$

For $\epsilon_1=0$, from the last equation, we have $\pm 8(1+\sqrt{2})\in\mathbb{Q}_2(\sqrt{2})^{\times 2}$, but this is a contradiction. Also, for $\epsilon_1=1$, from the last equation and

$$\frac{3+\sqrt{2}}{\sqrt{-7}(1+\sqrt{2})}=\left(\frac{3+\sqrt{-7}+(1+\sqrt{-7})\sqrt{2}}{\sqrt{-7}(1+\sqrt{2})}\right)^2\cdot\frac{7}{14+2\sqrt{-7}}$$

we have

$$\pm\frac{(6+6\sqrt{-7})(3+\sqrt{2})}{-7}\cdot\frac{1}{8(1+\sqrt{2})}\in\mathbb{Q}_2(\sqrt{2})^{\times 2}.$$

Therefore,

$$\pm 3\in\mathbb{Q}_2(\sqrt{2})^{\times 2}.$$

and this is a contradiction too. Hence $W_2\neq W_4$, and we conclude $M_2\neq M_4$.

3.2.2 $b=-5$

For $b=-5$, a and c can be 2 and -10 respectively. Assume $\epsilon_1=1+\sqrt{-2}$, $\epsilon_2=-1+\sqrt{-2}$, $\epsilon_3=-1+\sqrt{-10}$ and $\epsilon_4=5+\sqrt{-10}$, we have

$$Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\epsilon_1)=3$$

$$Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\epsilon_2)=3,$$

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(\epsilon_3)=11$$

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(\epsilon_4)=35$$

Note: $-5/3=1+O(2^3)\equiv 1\pmod 8$, $-5/11=1+O(2^4)\equiv 1\pmod 8$ and $-5/35=1+O(2^3)\equiv 1\pmod 8$, so 3, 11 and 35 are in the same square class as -5.

Set

$$\alpha = \sqrt{\frac{-5}{3}}(1 + \sqrt{-2}), \qquad \alpha' = \sqrt{\frac{-5}{3}}(-1 + \sqrt{-2});$$
$$\gamma = \sqrt{\frac{-5}{11}}(-1 + \sqrt{-10}), \qquad \gamma' = \sqrt{\frac{-5}{35}}(5 + \sqrt{-10});$$

where

$$\sqrt{-5/3} = 1 + 2 + 2^4 + 2^5 + 2^6 + 2^7 + 2^9 + \cdots \in \mathbb{Q}_2,$$
$$\sqrt{-5/11} = 1 + 2^3 + 2^6 + 2^7 + 2^{10} + 2^{12} + \cdots \in \mathbb{Q}_2$$

and

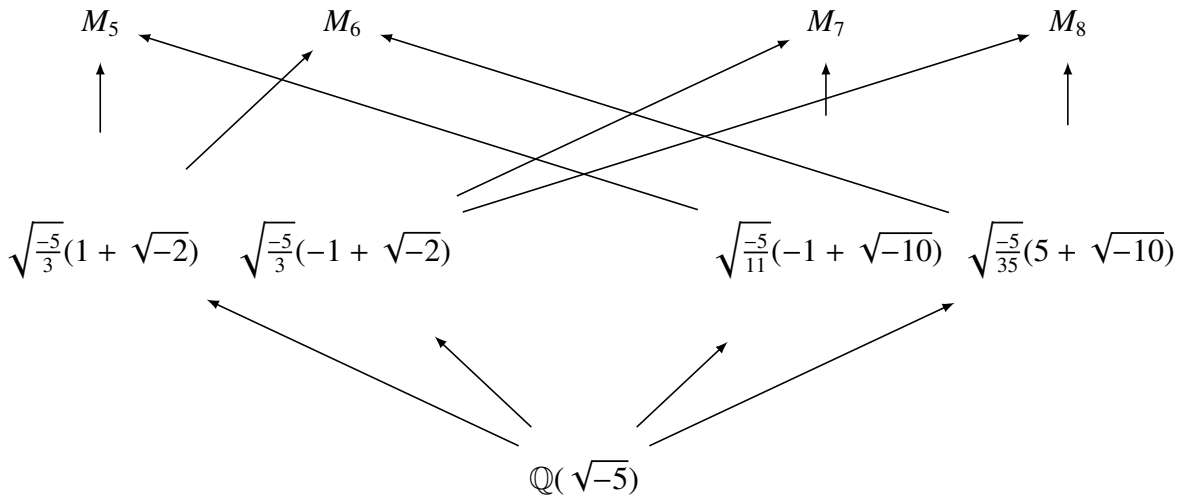
$$\sqrt{-5/35} = 1 + 2 + 2^5 + 2^6 + 2^9 + 2^{12} + \cdots \in \mathbb{Q}_2.$$

We define

$$\delta_1 := \alpha + \gamma; \quad \delta_2 := \alpha + \gamma'; \quad \delta_3 := \alpha' + \gamma; \quad \delta_4 := \alpha' + \gamma';$$

and

$$M_1 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{-5}, \sqrt{-10}, \sqrt{\alpha}, \sqrt{\gamma}, \sqrt{\delta_1}),$$
$$M_2 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{-5}, \sqrt{-10}, \sqrt{\alpha}, \sqrt{\gamma'}, \sqrt{\delta_2}),$$
$$M_3 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{-5}, \sqrt{-10}, \sqrt{\alpha'}, \sqrt{\gamma}, \sqrt{\delta_3}),$$
$$M_4 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{-5}, \sqrt{-10}, \sqrt{\alpha'}, \sqrt{\gamma'}, \sqrt{\delta_4}).$$



Distinction of M_5, M_6, M_7 and M_8

Claim: $M_5 \neq M_6$

For M_5, we have

$$b = -5, \alpha_5 = \sqrt{-5/3}(1 + \sqrt{-2}), \gamma_5 = \sqrt{-5/11}(-1 + \sqrt{-10})$$

and

$$\delta_5 = \sqrt{-5/3}(1+\sqrt{-2}) + \sqrt{-5/11}(-1+\sqrt{-10}),$$

therefore

$$W_5 = \langle [\delta_5], [\sqrt{-5/3}(1+\sqrt{-2})], [\sqrt{-5/11}(-1+\sqrt{-10})], [-5]\rangle.$$

For M_6, we have

$$b = -5, \alpha_6 = \sqrt{-5/3}(1+\sqrt{-2}), \gamma_6 = \sqrt{-5/35}(5+\sqrt{-10})$$

and

$$\delta_6 = \sqrt{-5/3}(1+\sqrt{-2}) + \sqrt{-5/35}(5+\sqrt{-10}),$$

therefore

$$W_6 = \langle [\delta_6], [\sqrt{-5/3}(1+\sqrt{-2})], [\sqrt{-5/35}(5+\sqrt{-10})], [-5]\rangle.$$

Assume $W_5 = W_6$, we can write

$$\delta_5 = \delta_6^{\epsilon_1}\alpha_6^{\epsilon_2}\gamma_6^{\epsilon_3}b^{\epsilon_4}e^2 \tag{3.1}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0,1\}$ and $e \in E^\times$ where $E = \mathbb{Q}_2(\sqrt{-2}, \sqrt{-10})$. Let

$$f_5 = 2(\sqrt{-5/3} - \sqrt{-5/11}) \in \mathbb{Q}_2$$

and

$$f_6 = 2(\sqrt{-5/3} + 5\sqrt{-5/35}) \in \mathbb{Q}_2.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_5) = f_5\alpha_5$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_6) = f_6\alpha_6.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\alpha_6) = \alpha_6^2, Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\gamma_6) = -5 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(b) = b^2.$$

Therefore from (3.1) we have

$$\frac{f_5\alpha_5}{(f_6\alpha_6)^{\epsilon_1}(-5)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}. \tag{3.2}$$

But for $\epsilon_1 = 0$,

$$\frac{f_5\alpha_5}{(-5)^{\epsilon_3}} \notin \mathbb{Q}_2(\sqrt{-2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}\left(\frac{f_5\alpha_5}{(-5)^{\epsilon_3}}\right) = \frac{1}{25^{\epsilon_2}}f_5^2(-5) \notin \mathbb{Q}_2^{\times 2} \cup (-2)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.2), we have

$$\frac{f_5\alpha_5}{f_6\alpha_6(-5)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}.$$

Using the fact that $\alpha_5 = \alpha_6$ and by multiplying 1 to above, we need to check whether $(-5)^{\epsilon_3} f_5 f_6$ is square in $\mathbb{Q}_2(\sqrt{-2})$. By fixed choice of

$$\sqrt{-5/3} = 1 + 2 + 2^4 + 2^5 + 2^6 + 2^7 + 2^9 + \cdots \in \mathbb{Q}_2,$$

$$\sqrt{-5/11} = 1 + 2^3 + 2^6 + 2^7 + 2^{10} + 2^{12} + \cdots \in \mathbb{Q}_2$$

and

$$\sqrt{-5/35} = 1 + 2 + 2^5 + 2^6 + 2^9 + 2^{12} + \cdots \in \mathbb{Q}_2,$$

we have

$$f_5 f_6 = 2^4(1 + 2^2 + 2^6 + 2^8 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2) f_5 f_6 = 2^4(2 + 2^2 + 2^4 + 2^5 + 2^6 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-5) f_5 f_6 = 2^4(1 + 2 + 2^2 + 2^5 + 2^7 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)(-5) f_5 f_6 = 2^4(2 + 2^4 + 2^5 + 2^7 + 2^{11} + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_5 \neq W_6$, and we conclude $M_5 \neq M_6$.

Claim: $M_7 \neq M_8$

For M_7, we have

$$b = -5, \alpha_7 = \sqrt{-5/3}(-1 + \sqrt{-2}), \gamma_7 = \sqrt{-5/11}(-1 + \sqrt{-10})$$

and

$$\delta_7 = \sqrt{-5/3}(-1 + \sqrt{-2}) + \sqrt{-5/11}(-1 + \sqrt{-10}),$$

therefore

$$W_7 = \langle [\delta_7], [\sqrt{-5/3}(-1 + \sqrt{-2})], [\sqrt{-5/11}(-1 + \sqrt{-10})], [-5] \rangle.$$

For M_8, we have

$$b = -5, \alpha_8 = \sqrt{-5/3}(-1 + \sqrt{-2}), \gamma_8 = \sqrt{-5/35}(5 + \sqrt{-10})$$

and

$$\delta_8 = \sqrt{-5/3}(-1 + \sqrt{-2}) + \sqrt{-5/35}(5 + \sqrt{-10}),$$

therefore

$$W_8 = \langle [\delta_8], [\sqrt{-5/3}(-1 + \sqrt{-2})], [\sqrt{-5/35}(5 + \sqrt{-10})], [-5] \rangle.$$

Assume $W_7 = W_8$, we can write

$$\delta_7 = \delta_8^{\epsilon_1} \alpha_8^{\epsilon_2} \gamma_8^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.3}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. Let

$$f_7 = 2(-\sqrt{-5/3} - \sqrt{-5/11}) \in \mathbb{Q}_2$$

and

$$f_8 = 2(-\sqrt{-5/3} + 5\sqrt{-5/35}) \in \mathbb{Q}_2.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_7) = f_7\alpha_7$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_8) = f_8\alpha_8.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\alpha_8) = \alpha_8^2, Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\gamma_8) = -5 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(b) = b^2.$$

Therefore from (3.3) we have

$$\frac{f_7\alpha_7}{(f_8\alpha_8)^{\epsilon_1}(-5)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}. \tag{3.4}$$

But for $\epsilon_1 = 0$,

$$\frac{f_7\alpha_7}{(-5)^{\epsilon_3}} \notin \mathbb{Q}_2(\sqrt{-2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}\left(\frac{f_7\alpha_7}{(-5)^{\epsilon_3}}\right) = \frac{1}{25^{\epsilon_3}} f_7^2(-5) \notin \mathbb{Q}_2^{\times 2} \cup (-2)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.4), we have

$$\frac{f_7\alpha_7}{f_8\alpha_8(-5)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}.$$

Using the fact that $\alpha_7 = \alpha_8$, we have

$$\frac{f_7}{f_8(-5)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}.$$

So, we need to check whether $(-5)^{\epsilon_3} f_7 f_8$ is square in $\mathbb{Q}_2(\sqrt{-2})^{\times}$. By fixed choice of $\sqrt{-5/3}$, $\sqrt{-5/11}$ and $\sqrt{-5/35}$ we have

$$f_7 f_8 = 2^6(1 + 2 + 2^2 + 2^3 + 2^5 + 2^{11} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-5)f_7 f_8 = 2^6(1 + 2^2 + 2^4 + 2^8 + 2^9 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-2)f_7 f_8 = 2^6(2 + 2^5 + 2^7 + 2^8 + 2^9 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)(-5)f_7 f_8 = 2^6(2 + 2^2 + 2^4 + 2^6 + 2^7 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_7 \neq W_8$, and we conclude $M_7 \neq M_8$.

Claim: $M_6 \neq M_7$

Assume $W_6 = W_7$, we can write

$$\delta_6 = \delta_7^{\epsilon_1} \alpha_7^{\epsilon_2} \gamma_7^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.5}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. we have

$$f_6 = 2(\sqrt{-5/3} + 5\sqrt{-5/35}) \in \mathbb{Q}_2.$$

and

$$f_7 = 2(-\sqrt{-5/3} - \sqrt{-5/11}) \in \mathbb{Q}_2$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_6) = f_6\gamma_6$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_7) = f_7\gamma_7.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\alpha_7) = -5, Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\gamma_7) = \gamma_7 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(b) = b^2.$$

Therefore from (3.5) we have

$$\frac{f_6\gamma_6}{(f_7\gamma_7)^{\epsilon_1}(-5)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}. \tag{3.6}$$

But for $\epsilon_1 = 0$,

$$\frac{f_6\gamma_6}{(-5)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-10})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}\left(\frac{f_6\gamma_6}{(-5)^{\epsilon_2}}\right) = \frac{1}{25^{\epsilon_2}} f_6^2(-5) \notin \mathbb{Q}_2^{\times 2} \cup (-10)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.6), we have

$$\frac{f_6\gamma_6}{f_7\gamma_7(-5)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}.$$

Now we need to find a relation between γ_6 and γ_7 modulo squares in $\mathbb{Q}_2(\sqrt{-10})$. Since

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\frac{\gamma_6}{\gamma_7}) = 1,$$

we can follow the same method we used in section 3.2.1. So take

$$t = \frac{\gamma_6}{\gamma_7} \quad \text{and} \quad l = t + 1 = \frac{\gamma_6 + \gamma_7}{\gamma_7}.$$

Therefore

$$\frac{\gamma_6}{\gamma_7} = t = \frac{l^2}{Nm(l)} = \left(\frac{\gamma_6+\gamma_7}{\gamma_7}\right)^2 (2 + 2\sqrt{-5/11}\sqrt{-5/35}). \tag{3.7}$$

So, we have

$$\frac{(2 + 2\sqrt{-5/11}\sqrt{-5/35})f_6}{f_7(-5)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}.$$

So, we need to check whether $(2 + 2\sqrt{-5/11}\sqrt{-5/35})(-5)^{\epsilon_2} f_6 f_7$ is square in $\mathbb{Q}_2(\sqrt{-10})^{\times}$. By fixed choice of $\sqrt{-5/3}$, $\sqrt{-5/11}$ and $\sqrt{-5/35}$ we have

$$(2 + 2\sqrt{-5/11}\sqrt{-5/35})f_6 f_7 = 2^8(1 + 2 + 2^2 + 2^3 + 2^5 + 2^6 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(2 + 2\sqrt{-5/11}\sqrt{-5/35})(-5)f_6 f_7 = 2^8(1 + 2^2 + 2^4 + 2^6 + 2^7 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-10)(2 + 2\sqrt{-5/11}\sqrt{-5/35})f_6 f_7 = 2^8(2 + 2^3 + 2^5 + 2^7 + 2^8 + 2^{11} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)(2 + 2\sqrt{-5/11}\sqrt{-5/35})(-5)f_6 f_7 = 2^8(2 + 2^2 + 2^3 + 2^5 + 2^7 + 2^8 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_6 \neq W_7$, and we conclude $M_6 \neq M_7$.

Claim: $M_5 \neq M_7$

Assume $W_5 = W_7$, we can write

$$\delta_5 = \delta_7^{\epsilon_1}\alpha_7^{\epsilon_2}\gamma_7^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.8}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^{\times}$. Let

$$f_5 = 2(\sqrt{-5/3} - \sqrt{-5/11}) \in \mathbb{Q}_2$$

and

$$f_7 = 2(-\sqrt{-5/3} - \sqrt{-5/11}) \in \mathbb{Q}_2$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_5) = f_5\alpha_5$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_7) = f_7\alpha_7.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\alpha_7) = \alpha_7^2, Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\gamma_7) = -5 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(b) = b^2.$$

Therefore from (3.8) we have

$$\frac{f_5\alpha_5}{(f_7\alpha_7)^{\epsilon_1}(-5)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}. \tag{3.9}$$

But for $\epsilon_1 = 0$,

$$\frac{f_5\alpha_5}{(-5)^{\epsilon_3}} \notin \mathbb{Q}_2(\sqrt{-2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}\left(\frac{f_5\alpha_5}{(-5)^{\epsilon_3}}\right) = \frac{1}{25^{\epsilon_3}} f_5^2(-5) \notin \mathbb{Q}_2^{\times 2} \cup (-2)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.9), we have

$$\frac{f_5\alpha_5}{f_7\alpha_7(-5)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}.$$

Now we need to find a relation between α_5 and α_7 module squares in $\mathbb{Q}_2(\sqrt{-2})$. Since

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\frac{\alpha_5}{\alpha_7}) = 1,$$

we can follow the same method we used in section 3.2.1. So take

$$t = \frac{\alpha_5}{\alpha_7} \quad \text{and} \quad l = t + 1 = \frac{\alpha_5 + \alpha_7}{\alpha_7}.$$

Therefore

$$\frac{\alpha_5}{\alpha_7} = t = \frac{l^2}{Nm(l)} = \left(\frac{\alpha_5 + \alpha_7}{2\alpha_7}\right)^2 \frac{3}{2}. \tag{3.10}$$

So, we need to check whether $3/2(-5)^{\epsilon_3} f_5 f_7$ is square in $\mathbb{Q}_2(\sqrt{-2})$. By fixed choice of $\sqrt{-5/3}$, $\sqrt{-5/11}$ and $\sqrt{-5/35}$ we have

$$(\frac{3}{2}) f_5 f_7 = 2^4(1 + 2 + 2^2 + 2^3 + 2^5 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(\frac{3}{2})(-5) f_5 f_7 = 2^4(1 + 2 + 2^2 + 2^5 + 2^7 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-2)(\frac{3}{2}) f_5 f_7 = 2^4(2 + 2^2 + 2^4 + 2^5 + 2^6 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)(\frac{3}{2})(-5) f_5 f_7 = 2^4(2 + 2^4 + 2^5 + 2^7 + 2^{11} + 2^{13} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

So this is a contradiction. Hence $W_5 \neq W_7$, and we conclude $M_5 \neq M_7$.

Claim: $M_5 \neq M_8$

Assume $W_5 = W_8$, we can write

$$\delta_5 = \delta_8^{\epsilon_1}\alpha_8^{\epsilon_2}\gamma_8^{\epsilon_3}b^{\epsilon_4}e^2 \tag{3.11}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. Let

$$f_5 = 2(\sqrt{-5/3} - \sqrt{-5/11}) \in \mathbb{Q}_2$$

and

$$f_8 = 2(-\sqrt{-5/3} + 5\sqrt{-5/35}) \in \mathbb{Q}_2.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_5) = f_5\gamma_5$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_8) = f_8\gamma_8.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\alpha_8) = -5, Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\gamma_8) = \gamma_8^2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(b) = b^2.$$

Therefore from (3.11) we have

$$\frac{f_5\gamma_5}{(f_8\gamma_8)^{\epsilon_1}(-5)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}. \tag{3.12}$$

But for $\epsilon_1 = 0$,

$$\frac{f_5\gamma_5}{(-5)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-10})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(\frac{f_5\gamma_5}{(-5)^{\epsilon_2}}) = \frac{1}{25^{\epsilon_2}}f_5^2(-5) \notin \mathbb{Q}_2^{\times 2} \cup (-10)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.12) we have

$$\frac{f_5\gamma_5}{f_8\gamma_8(-5)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}.$$

Using the fact that $\gamma_5 = \gamma_7$, by (3.7) we have

$$\frac{\gamma_5}{\gamma_8} = \left(\frac{\gamma_5 + \gamma_8}{\gamma_8}\right)^2 \frac{1}{2 + 2\sqrt{-5/11}\sqrt{-5/35}}.$$

So, we need to check whether $(2 + 2\sqrt{-5/11}\sqrt{-5/35})(-5)^{\epsilon_2}f_5f_8$ is square in $\mathbb{Q}_2(\sqrt{-10})^\times$. By fixed choice of $\sqrt{-5/3}$, $\sqrt{-5/11}$ and $\sqrt{-5/35}$ we have

$$(2 + 2\sqrt{-5/11}\sqrt{-5/35})f_5f_8 = 2^8(1 + 2^2 + 2^5 + 2^8 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(2 + 2\sqrt{-5/11}\sqrt{-5/35})(-5)f_5f_8 = 2^8(1 + 2 + 2^2 + 2^6 + 2^9 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-10)(2 + 2\sqrt{-5/11}\sqrt{-5/35})f_5f_8 = 2^8(2 + 2^2 + 2^3 + 2^7 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)(2 + 2\sqrt{-5/11}\sqrt{-5/35})(-5)f_5f_8 = 2^8(2 + 2^3 + 2^4 + 2^5 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

So this is a contradiction. Hence $W_5 \neq W_8$, and we conclude $M_5 \neq M_8$.

Claim: $M_6 \neq M_8$

Assume $W_6 = W_8$, we can write

$$\delta_6 = \delta_8^{\epsilon_1}\alpha_8^{\epsilon_2}\gamma_8^{\epsilon_3}b^{\epsilon_4}e^2 \tag{3.13}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. We have

$$f_6 = 2(\sqrt{-5/3} + 5\sqrt{-5/35}) \in \mathbb{Q}_2.$$

and

$$f_8 = 2(-\sqrt{-5/3} + 5\sqrt{-5/35}) \in \mathbb{Q}_2.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_6) = f_6\alpha_6$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_8) = f_8\alpha_8.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\alpha_8) = \alpha_8^2, Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\gamma_8) = -5 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(b) = b^2.$$

Therefore from (3.13) we have

$$\frac{f_6\alpha_6}{(f_8\alpha_8)^{\epsilon_1}(-5)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}. \tag{3.14}$$

But for $\epsilon_1 = 0$,

$$\frac{f_6\alpha_6}{(-5)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}\left(\frac{f_6\alpha_6}{(-5)^{\epsilon_3}}\right) = \frac{1}{25^{\epsilon_3}}f_6^2(-5) \notin \mathbb{Q}_2^{\times 2} \cup (-2)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.14) and the fact that $\alpha_6 = \alpha_5$ and $\alpha_8 = \alpha_7$, we have

$$\frac{3f_6}{2f_8(-5)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}.$$

So, we need to check whether $(3/2)(-5)^{\epsilon_2} f_6 f_8$ is square in $\mathbb{Q}_2$. By fixed choice of $\sqrt{-5/3}$, $\sqrt{-5/11}$ and $\sqrt{-5/35}$ we have

$$(3/2)f_6 f_8 = 2^4(1 + 2^2 + 2^3 + 2^5 + 2^6 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(3/2)(-5)f_6 f_8 = 2^4(1 + 2 + 2^2 + 2^3 + 2^4 + 2^6 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

as well as

$$(-2)(3/2)f_6 f_8 = 2^4(2 + 2^2 + 2^5 + 2^8 + 2^{11} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)(3/2)(-5)f_6 f_8 = 2^4(2 + 2^6 + 2^9 + 2^{12} + 2^{15} + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_6 \neq W_8$, and we conclude $M_6 \neq M_8$.

3.2.3 $b = -2$

For $b = -2$, a and c can be 2 and -10. Assume $\epsilon_1 = \sqrt{2}$, $\epsilon_2 = 4 + \sqrt{2}$, $\epsilon_3 = 2 + \sqrt{-10}$ and $\epsilon_4 = 2 + 3\sqrt{-10}$.

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(\epsilon_1) = -2$$
$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}(\epsilon_2) = 14$$
$$Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(\epsilon_3) = 14$$
$$Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(\epsilon_4) = 94$$

(Note: $-2/14 = 1 + O(2^3) \equiv 1 \pmod 8$ and $-2/94 = 1 + O(2^3) \equiv 1 \pmod 8$, so 14 and 94 are in the same square class as -2)

Set

$$\alpha = \sqrt{2}, \qquad \alpha' = \sqrt{\frac{-2}{14}}(4 + \sqrt{2});$$
$$\gamma = \sqrt{\frac{-2}{14}}(2 + \sqrt{-10}), \qquad \gamma' = \sqrt{\frac{-2}{94}}(2 + 3\sqrt{-10});$$

where

$$\sqrt{-2/14} = 1 + 2^2 + 2^3 + 2^4 + 2^7 + 2^8 + 2^{10} + \cdots \in \mathbb{Q}_2,$$

and

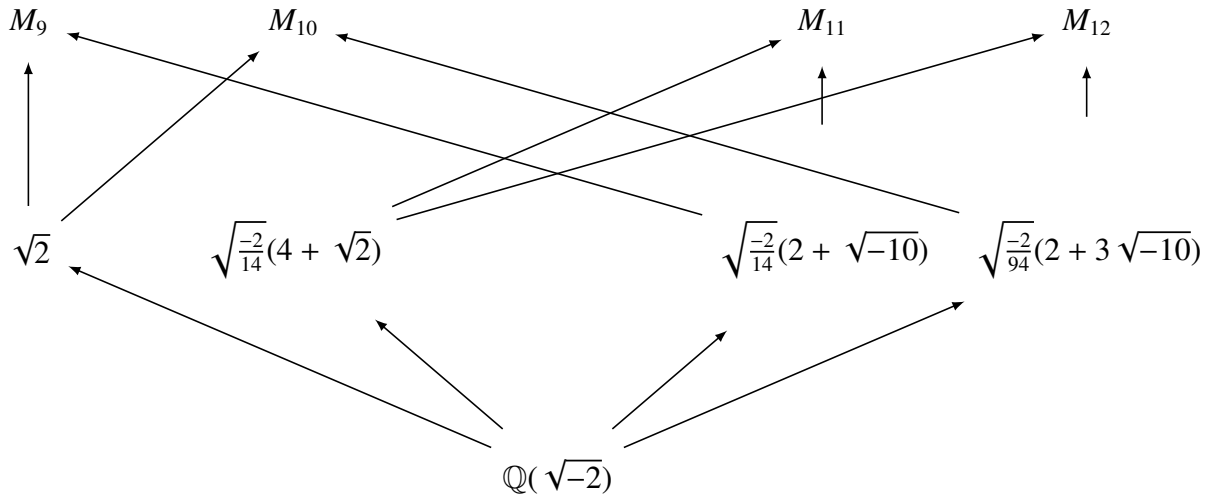
$$\sqrt{-2/94} = 1 + 2^3 + 2^4 + 2^5 + 2^6 + 2^{14} + 2^{16} + \cdots \in \mathbb{Q}_2,$$

We define

$$\delta_1 := \alpha + \gamma; \quad \delta_2 := \alpha + \gamma'; \quad \delta_3 := \alpha' + \gamma; \quad \delta_4 := \alpha' + \gamma';$$

and

$$M_1 := \mathbb{Q}_2(\sqrt{2}, \sqrt{-2}, \sqrt{-10}, \sqrt{\alpha}, \sqrt{\gamma}, \sqrt{\delta_1}),$$
$$M_2 := \mathbb{Q}_2(\sqrt{2}, \sqrt{-2}, \sqrt{-10}, \sqrt{\alpha}, \sqrt{\gamma'}, \sqrt{\delta_2}),$$
$$M_3 := \mathbb{Q}_2(\sqrt{2}, \sqrt{-2}, \sqrt{-10}, \sqrt{\alpha'}, \sqrt{\gamma}, \sqrt{\delta_3}),$$
$$M_4 := \mathbb{Q}_2(\sqrt{2}, \sqrt{-2}, \sqrt{-10}, \sqrt{\alpha'}, \sqrt{\gamma'}, \sqrt{\delta_4}).$$



Distinction of M_9, M_{10}, M_{11} and M_{12}

Claim: $M_9 \neq M_{10}$

For M_9, we have

$$b = -2, \alpha_9 = \sqrt{2}, \gamma_9 = \sqrt{-2/14}(2 + \sqrt{-10})$$

and

$$\delta_9 = \sqrt{2} + \sqrt{-2/14}(2 + \sqrt{-10}),$$

therefore

$$W_9 = \langle [\delta_9], [\sqrt{2}], [\sqrt{-2/14}(2 + \sqrt{-10})], [-2] \rangle.$$

For M_{10}, we have

$$b = -2, \alpha_{10} = \sqrt{2}, \gamma_{10} = \sqrt{-2/94}(2 + 3\sqrt{-10})$$

and

$$\delta_{10} = \sqrt{2} + \sqrt{-2/94}(2 + 3\sqrt{-10}),$$

therefore

$$W_{10} = \langle [\delta_{10}], [\sqrt{2}], [\sqrt{-2/94}(2 + 3\sqrt{-10})], [-2] \rangle.$$

Assume $W_9 = W_{10}$ then we can write

$$\delta_9 = \delta_{10}^{\epsilon_1} \alpha_{10}^{\epsilon_2} \gamma_{10}^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.15}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$ where $E = \mathbb{Q}_2(\sqrt{2}, \sqrt{-10})$. Let

$$f_9 = 4\sqrt{-2/14}$$

and

$$f_{10} = 4\sqrt{-2/94}.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_9) = f_9\alpha_9$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_{10}) = f_{10}\alpha_{10}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\alpha_{10}) = \alpha_{10}^2, Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\gamma_{10}) = -2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{2})}(b) = b^2.$$

Therefore from (3.15) we have

$$\frac{f_9\alpha_9}{(f_{10}\alpha_{10})^{\epsilon_1}(-2)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{2})^{\times 2}. \tag{3.16}$$

But for $\epsilon_1 = 0$,

$$\frac{f_9\alpha_9}{(-2)^{\epsilon_3}} \notin \mathbb{Q}_2(\sqrt{2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}\left(\frac{f_9\alpha_9}{(-2)^{\epsilon_3}}\right) = \frac{1}{4^{\epsilon_3}}f_9^2(-2) \notin \mathbb{Q}_2^{\times 2} \cup 2\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.16) and the fact that $\alpha_9 = \alpha_{10}$, we have

$$\frac{f_9}{f_{10}(-2)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{2})^{\times 2}.$$

So, we need to check whether $(-2)^{\epsilon_3}f_9f_{10}$ is square in $\mathbb{Q}_2(\sqrt{2})$. By fixed choice of

$$\sqrt{-2/14} = 1 + 2^2 + 2^3 + 2^4 + 2^7 + 2^8 + 2^{10} + \cdots \in \mathbb{Q}_2,$$

and

$$\sqrt{-2/94} = 1 + 2^3 + 2^4 + 2^5 + 2^6 + 2^{14} + 2^{16} + \cdots \in \mathbb{Q}_2,$$

we have

$$f_9f_{10} = 2^4(1 + 2^2 + 2^4 + 2^5 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)f_9f_{10} = 2^4(2 + 2^2 + 2^4 + 2^7 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(2)f_9f_{10} = 2^4(2 + 2^3 + 2^5 + 2^6 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(2)(-2)f_9f_{10} = 2^6(1 + 2 + 2^3 + 2^6 + 2^7 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_9 \neq W_{10}$, and we conclude $M_9 \neq M_{10}$.

Claim: $M_{10} \neq M_{11}$

Let W_{10} be as above. For M_{11}, we have

$$b = -2, \alpha_{11} = \sqrt{-2/14}(4 + \sqrt{2}), \gamma_{11} = \sqrt{-2/14}(2 + \sqrt{-10})$$

and

$$\delta_{11} = \sqrt{-2/14}(4 + \sqrt{2}) + \sqrt{-2/14}(2 + \sqrt{-10}),$$

therefore

$$W_{11} = \langle [\delta_{11}], [\sqrt{-2/14}(4 + \sqrt{2})], [\sqrt{-2/14}(2 + \sqrt{-10})], [-2] \rangle.$$

Assume $W_{10} = W_{11}$ then we can write

$$\delta_{10} = \delta_{11}^{\epsilon_1} \alpha_{11}^{\epsilon_2} \gamma_{11}^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.17}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. Let

$$f_{10} = 4\sqrt{-2/94}$$

and

$$f_{11} = 12\sqrt{-2/14}.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_{10}) = f_{10}\gamma_{10}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_{11}) = f_{11}\gamma_{11}$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\alpha_{11}) = -2, Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\gamma_{11}) = \gamma_{11}^2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(b) = b^2.$$

Therefore from (3.17) we have

$$\frac{f_{10}\gamma_{10}}{(f_{11}\gamma_{11})^{\epsilon_1}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}. \tag{3.18}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{10}\gamma_{10}}{(-2)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-10})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}\left(\frac{f_{10}\gamma_{10}}{(-2)^{\epsilon_2}}\right) = \frac{1}{4^{\epsilon_2}} f_{10}^2(-2) \notin \mathbb{Q}_2^{\times 2} \cup (-10)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.18), we have

$$\frac{f_{10}\gamma_{10}}{f_{11}\gamma_{11}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-5})^{\times 2}.$$

Now we need to find a relation between γ_{10} and γ_{11} module squares in $\mathbb{Q}_2(\sqrt{-10})$. Since

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\frac{\gamma_{10}}{\gamma_{11}}) = 1,$$

we can follow the same method we used in section 3.2.1. So take

$$t = \frac{\gamma_{10}}{\gamma_{11}} \quad \text{and} \quad l = t + 1 = \frac{\gamma_{10} + \gamma_{11}}{\gamma_{11}}.$$

Therefore

$$\frac{\gamma_{10}}{\gamma_{11}} = t = \frac{l^2}{Nm(l)} = \left(\frac{\gamma_{10} + \gamma_{11}}{\gamma_{11}}\right)^2 (2 - 34\sqrt{-2/14}\sqrt{-2/94}). \tag{3.19}$$

So, we need to check whether $(2 - 34\sqrt{-2/14}\sqrt{-2/94})(-2)^{\epsilon_2} f_9 f_{10}$ is square in $\mathbb{Q}_2(\sqrt{-10})$. By fixed choice of $\sqrt{-2/14}$ and $\sqrt{-2/94}$, we have

$$(2 - 34\sqrt{-2/14}\sqrt{-2/94}) f_{10} f_{11} = 2^6(2 + 2^9 + 2^{10} + 2^{11} + 2^{12} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(2 - 34\sqrt{-2/14}\sqrt{-2/94})(-2) f_{10} f_{11} = 2^8(1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-10)(2 - 34\sqrt{-2/14}\sqrt{-2/94}) f_{10} f_{11} = 2^8(1 + 2 + 2^3 + 2^4 + 2^5 + 2^6 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)(2 - 34\sqrt{-2/14}\sqrt{-2/94})(-2) f_{10} f_{11} = 2^8(2 + 2^3 + 2^9 + 2^{10} + 2^{12} + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_{10} \neq W_{11}$, and we conclude $M_{10} \neq M_{11}$.

Claim: $M_{11} \neq M_{12}$

Let W_{11} be as above. For M_{12}, we have

$$b = -2, \alpha_{12} = \sqrt{-2/14}(4 + \sqrt{2}), \gamma_{12} = \sqrt{-2/94}(2 + 3\sqrt{-10})$$

and

$$\delta_{12} = \sqrt{-2/14}(4 + \sqrt{2}) + \sqrt{-2/94}(2 + 3\sqrt{-10}),$$

therefore

$$W_{12} = \langle [\delta_{12}], [\sqrt{-2/14}(4 + \sqrt{2})], [\sqrt{-2/94}(2 + 3\sqrt{-10})], [-2] \rangle.$$

Assume $W_{11} = W_{12}$ then we can write

$$\delta_{11} = \delta_{12}^{\epsilon_1} \alpha_{12}^{\epsilon_2} \gamma_{12}^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.20}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. Let

$$f_{11} = 12\sqrt{-2/14}$$

and

$$f_{12} = 2(4\sqrt{-2/14} + 2\sqrt{-2/94}).$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_{11}) = f_{11}\alpha_{11}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\delta_{12}) = f_{12}\alpha_{12}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\alpha_{12}) = \alpha_{12}^2, Nm_{E/\mathbb{Q}_2(\sqrt{2})}(\gamma_{12}) = -2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{2})}(b) = b^2.$$

Therefore from (3.20) we have

$$\frac{f_{11}\alpha_{11}}{(f_{12}\alpha_{12})^{\epsilon_1}(-2)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{2})^{\times 2}. \tag{3.21}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{11}\alpha_{11}}{(-2)^{\epsilon_3}} \notin \mathbb{Q}_2(\sqrt{2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}\left(\frac{f_{11}\alpha_{11}}{(-2)^{\epsilon_3}}\right) = \frac{1}{4^{\epsilon_3}} f_{11}^2(-2) \notin \mathbb{Q}_2^{\times 2} \cup 2\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.21) and the fact that $\alpha_{11} = \alpha_{12}$, we have

$$\frac{f_{11}}{f_{12}(-2)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{2})^{\times 2}.$$

So, we need to check whether $(-2)^{\epsilon_3} f_{11} f_{12}$ is square in $\mathbb{Q}_2(\sqrt{2})$. By fixed choice of $\sqrt{-2/14}$ and $\sqrt{-2/94}$ we have

$$f_{11}f_{12} = 2^4(1 + 2^2 + 2^4 + 2^6 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)f_{11}f_{12} = 2^4(2 + 2^2 + 2^4 + 2^6 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-10)f_{11}f_{12} = 2^4(2 + 2^3 + 2^5 + 2^7 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)(-2)f_{11}f_{12} = 2^6(1 + 2 + 2^3 + 2^5 + 2^7 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_{11} \neq W_{12}$, and we conclude $M_{11} \neq M_{12}$.

Claim: $M_9 \neq M_{11}$

Assume $W_9 = W_{11}$ then we can write

$$\delta_9 = \delta_{11}^{\epsilon_1}\alpha_{11}^{\epsilon_2}\gamma_{11}^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.22}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. We have

$$f_9 = 4\sqrt{-2/14}$$

and

$$f_{11} = 12\sqrt{-2/94}.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_9) = f_9\gamma_9$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_{11}) = f_{11}\gamma_{11}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\alpha_{11}) = -2, Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\gamma_{11}) = \gamma_{11} \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(b) = b^2.$$

Therefore from (3.22) we have

$$\frac{f_9\gamma_9}{(f_{11}\gamma_{11})^{\epsilon_1}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}. \tag{3.23}$$

But for $\epsilon_1 = 0$,

$$\frac{f_9\gamma_9}{(-2)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-10})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}\left(\frac{f_9\gamma_9}{(-2)^{\epsilon_2}}\right) = \frac{1}{4^{\epsilon_2}} f_9^2(-2) \notin \mathbb{Q}_2^{\times 2} \cup (-10)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.23), we have

$$\frac{f_9\gamma_9}{f_{11}\gamma_{11}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}.$$

Using the fact $\gamma_9 = \gamma_{11}$, we need to check whether $(-2)^{\epsilon_2} f_9 f_{11}$ is square in $\mathbb{Q}_2(\sqrt{-10})$. By fixed choice of $\sqrt{-2/14}$ and $\sqrt{-2/94}$ we have

$$f_9 f_{11} = 2^4(1 + 2 + 2^3 + 2^4 + 2^6 + 2^7 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)f_9 f_{11} = 2^4(2 + 2^3 + 2^6 + 2^9 + 2^{12} + 2^{15} + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-10)f_9 f_{11} = 2^4(2 + 2^4 + 2^5 + 2^6 + 2^8 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)(-2)f_9 f_{11} = 2^6(1 + 2 + 2^2 + 2^6 + 2^9 + 2^{12} + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_9 \neq W_{11}$, and we conclude $M_9 \neq M_{11}$.

Claim: $M_9 \neq M_{12}$

Assume $W_9 = W_{12}$ then we can write

$$\delta_9 = \delta_{12}^{\epsilon_1}\alpha_{12}^{\epsilon_2}\gamma_{12}^{\epsilon_3}b^{\epsilon_4}e^2 \tag{3.24}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. We have

$$f_9 = 4\sqrt{-2/14}$$

and

$$f_{12} = 2(4\sqrt{-2/14} + 2\sqrt{-2/94}).$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_9) = f_9\gamma_9$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_{12}) = f_{12}\gamma_{12}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\alpha_{12}) = -2, Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\gamma_{12}) = \gamma_{12}^2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(b) = b^2.$$

Therefore from (3.24) we have

$$\frac{f_9\gamma_9}{(f_{12}\gamma_{12})^{\epsilon_1}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}. \tag{3.25}$$

But for $\epsilon_1 = 0$,

$$\frac{f_9\gamma_9}{(-2)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-10})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}\left(\frac{f_9\gamma_9}{(-2)^{\epsilon_2}}\right) = \frac{1}{4^{\epsilon_2}}f_9^2(-2) \notin \mathbb{Q}_2^{\times 2} \cup (-10)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.25), we have

$$\frac{f_9\gamma_9}{f_{12}\gamma_{12}(-2)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-5})^{\times 2}.$$

Using the fact that $\gamma_9 = \gamma_{11}$ and $\gamma_{12} = \gamma_{10}$, by (3.19) we have

$$\frac{\gamma_9}{\gamma_{12}} = \left(\frac{\gamma_{11}}{\gamma_{10} + \gamma_{11}}\right)^2 \frac{1}{2 - 34\sqrt{-2/14}\sqrt{-2/94}}.$$

So, we need to check whether $(2 - 34\sqrt{-2/14}\sqrt{-2/94})(-2)^{\epsilon_2}f_9f_{12}$ is square in $\mathbb{Q}_2(\sqrt{-10})$. By fixed choice of $\sqrt{-2/14}$ and $\sqrt{-2/94}$ we have

$$(2 - 34\sqrt{-2/14}\sqrt{-2/94})f_9f_{12} = 2^6(2 + 2^4 + 2^5 + 2^7 + 2^8 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(2 - 34\sqrt{-2/14}\sqrt{-2/94})(-2)f_9f_{12} = 2^8(1 + 2 + 2^2 + 2^5 + 2^{13} + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-10)(2 - 34\sqrt{-2/14}\sqrt{-2/94})f_9f_{12} = 2^8(1 + 2 + 2^6 + 2^7 + 2^{13} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)(2 - 34\sqrt{-2/14}\sqrt{-2/94})(-2)f_9f_{12} = 2^8(2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_9 \neq W_{12}$, and we conclude $M_9 \neq M_{12}$.

Claim: $M_{10} \neq M_{12}$

Assume $W_{10} = W_{12}$ then we can write

$$\delta_{10} = \delta_{12}^{\epsilon_1}\alpha_{12}^{\epsilon_2}\gamma_{12}^{\epsilon_3}b^{\epsilon_4}e^2 \tag{3.26}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. We have

$$f_{10} = 4\sqrt{-2/94}$$

and

$$f_{12} = 2(4\sqrt{-2/14} + 2\sqrt{-2/94}).$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_{10}) = f_{10}\gamma_{10}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\delta_{12}) = f_{12}\gamma_{12}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\alpha_{12}) = -2, Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(\gamma_{12}) = \gamma_{12}^2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-10})}(b) = b^2.$$

Therefore from (3.26) we have

$$\frac{f_{10}\gamma_{10}}{(f_{12}\gamma_{12})^{\epsilon_1}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}. \tag{3.27}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{10}\gamma_{10}}{(-2)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-10})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-10})/\mathbb{Q}_2}\left(\frac{f_{10}\gamma_{10}}{(-2)^{\epsilon_2}}\right) = \frac{1}{4^{\epsilon_2}}f_{10}^2(-2) \notin \mathbb{Q}_2^{\times 2} \cup (-10)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.27) and the fact that $\gamma_{10} = \gamma_{12}$, we have

$$\frac{f_{10}}{f_{12}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-10})^{\times 2}.$$

So, we need to check whether $(-2)^{\epsilon_2} f_{10} f_{12}$ is square in $\mathbb{Q}_2(\sqrt{-10})$. By fixed choice of $\sqrt{-2/14}$ and $\sqrt{-2/94}$ we have

$$f_{10} f_{12} = 2^4(1 + 2 + 2^3 + 2^4 + 2^7 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2) f_{10} f_{12} = 2^4(2 + 2^3 + 2^6 + 2^7 + 2^{12} + 2^{14} + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-10) f_{10} f_{12} = 2^4(2 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)(-2) f_{10} f_{12} = 2^6(1 + 2 + 2^2 + 2^9 + 2^{10} + 2^{12} + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_{10} \neq W_{12}$, and we conclude $M_{10} \neq M_{12}$.

3.2.4 $b = -10$

For $b = -10$, a and c can be -2 and -5. Let $\epsilon_1 = 6 + \sqrt{-2}$, $\epsilon_2 = 2 + \sqrt{-2}$, $\epsilon_3 = -1 + \sqrt{-5}$ and $\epsilon_4 = 5 + 3\sqrt{-5}$.

$$Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(\epsilon_1) = 38$$

$$Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}(\epsilon_2) = 6$$

$$Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(\epsilon_3) = 6$$

$$Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}(\epsilon_4) = 70$$

Note: $-10/38 = 1 + O(2^3) \equiv 1 \pmod 8$, $-10/6 = 1 + O(2^3) \equiv 1 \pmod 8$ and $-10/70 = 1 + O(2^3) \equiv 1 \pmod 8$, so 38, 6 and 70 are in the same square class as -10.

Set

$$\alpha = \sqrt{\frac{-10}{38}}(6 + \sqrt{-2}), \qquad \alpha' = \sqrt{\frac{-10}{6}}(2 + \sqrt{-2});$$

$$\gamma = \sqrt{\frac{-10}{6}}(-1 + \sqrt{-5}), \qquad \gamma' = \sqrt{\frac{-10}{70}}(5 + 3\sqrt{-5});$$

where

$$\sqrt{-10/38} = 1 + 2 + 2^3 + 2^7 + 2^8 + 2^9 + 2^{14} + \cdots \in \mathbb{Q}_2,$$

$$\sqrt{-10/6} = 1 + 2 + 2^4 + 2^5 + 2^6 + 2^7 + 2^9 + \cdots \in \mathbb{Q}_2$$

and

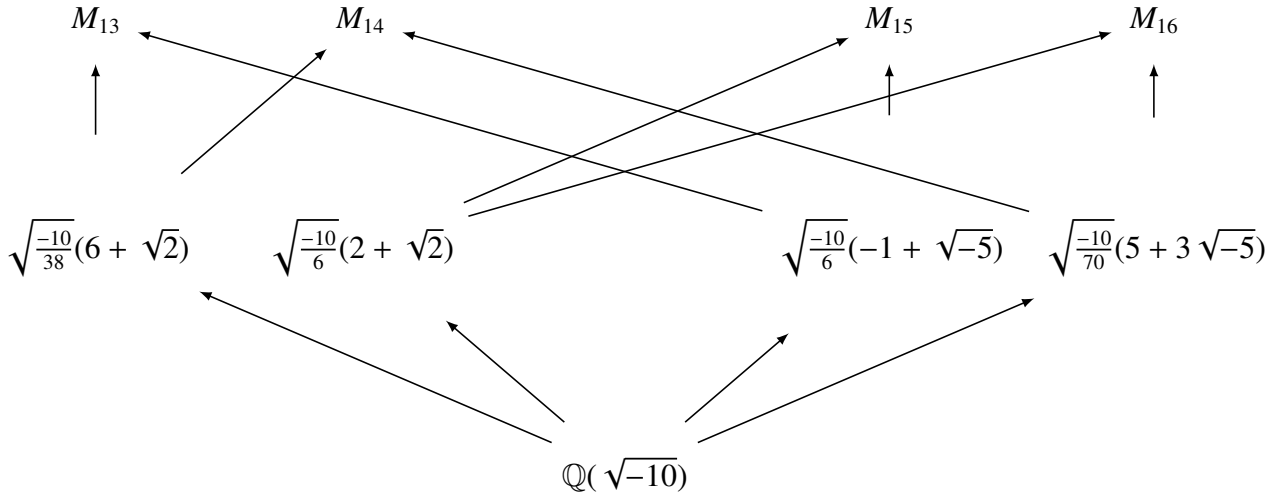
$$\sqrt{-10/70} = 1 + 2 + 2^5 + 2^6 + 2^9 + 2^{12} + 2^{14} + \cdots \in \mathbb{Q}_2.$$

We define

$$\delta_1 := \alpha + \gamma; \quad \delta_2 := \alpha + \gamma'; \quad \delta_3 := \alpha' + \gamma; \quad \delta_4 := \alpha' + \gamma';$$

and

$$M_1 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{-10}, \sqrt{-5}, \sqrt{\alpha}, \sqrt{\gamma}, \sqrt{\delta_1}),$$
$$M_2 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{-10}, \sqrt{-5}, \sqrt{\alpha}, \sqrt{\gamma'}, \sqrt{\delta_2}),$$
$$M_3 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{-10}, \sqrt{-5}, \sqrt{\alpha'}, \sqrt{\gamma}, \sqrt{\delta_3}),$$
$$M_4 := \mathbb{Q}_2(\sqrt{-2}, \sqrt{-10}, \sqrt{-5}, \sqrt{\alpha'}, \sqrt{\gamma'}, \sqrt{\delta_4}).$$



Distinction of M_{13}, M_{14}, M_{15} and M_{16}

Claim: $M_{13} \neq M_{14}$

For M_{13}, we have

$$b = -10, \alpha_{13} = \sqrt{-10/38}(6+\sqrt{-2}), \gamma_{13} = \sqrt{-10/6}(-1+\sqrt{-5})$$

and

$$\delta_{13} = \sqrt{-10/38}(6+\sqrt{-2}) + \sqrt{-10/6}(-1+\sqrt{-5}),$$

therefore

$$W_{13} = \langle [\delta_{13}], [\sqrt{-10/38}(6+\sqrt{-2})], [\sqrt{-10/6}(-1+\sqrt{-5})], [-10] \rangle.$$

For M_{14}, we have

$$b = -10, \alpha_{14} = \sqrt{-10/38}(6+\sqrt{-2}), \gamma_{14} = \sqrt{-10/70}(5+3\sqrt{-5})$$

and

$$\delta_{14} = \sqrt{-10/38}(6+\sqrt{-2}) + \sqrt{-10/70}(5+3\sqrt{-5}),$$

therefore

$$W_{14} = \langle [\delta_{14}], [\sqrt{-10/38}(6+\sqrt{-2})], [\sqrt{-10/70}(5+3\sqrt{-5})], [-10] \rangle.$$

Assume $W_{13} = W_{14}$ then we can write

$$\delta_{13} = \delta_{14}^{\epsilon_1}\alpha_{14}^{\epsilon_2}\gamma_{14}^{\epsilon_3}b^{\epsilon_4}e^2 \tag{3.28}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$ where $E = \mathbb{Q}_2(\sqrt{-2}, \sqrt{-5})$. Let

$$f_{13} = 2(6\sqrt{-10/38} - \sqrt{-10/6}$$

and

$$f_{14} = 2(6\sqrt{-10/38} + 5\sqrt{-10/70}).$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_{13}) = f_{13}\alpha_{13}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_{14}) = f_{14}\alpha_{14}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\alpha_{14}) = \alpha_{14}^2, Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\gamma_{14}) = -10 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(b) = b^2.$$

Therefore from (3.28) we have

$$\frac{f_{13}\alpha_{13}}{(f_{14}\alpha_{14})^{\epsilon_1}(-2)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}. \tag{3.29}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{13}\alpha_{13}}{(-10)^{\epsilon_3}} \notin \mathbb{Q}_2(\sqrt{-2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}\left(\frac{f_{13}\alpha_{13}}{(-10)^{\epsilon_3}}\right) = \frac{1}{100^{\epsilon_3}}f_{13}^2(-10) \notin \mathbb{Q}_2^{\times 2} \cup (-2)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.29) and the fact that $\alpha_{13} = \alpha_{14}$, we have

$$\frac{f_{13}}{f_{14}(-2)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}.$$

So, we need to check whether $(-2)^{\epsilon_3}f_{13}f_{14}$ is square in $\mathbb{Q}_2$. By fixed choice of

$$\sqrt{-10/38} = 1 + 2 + 2^3 + 2^7 + 2^8 + 2^9 + 2^{14} + \cdots \in \mathbb{Q}_2,$$

$$\sqrt{-10/6} = 1 + 2 + 2^4 + 2^5 + 2^6 + 2^7 + 2^9 + \cdots \in \mathbb{Q}_2$$

and

$$\sqrt{-10/70} = 1 + 2 + 2^5 + 2^6 + 2^9 + 2^{12} + 2^{14} + \cdots \in \mathbb{Q}_2,$$

we have

$$f_{13}f_{14} = 2^2(1 + 2 + 2^2 + 2^3 + 2^4 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)f_{13}f_{14} = 2^2(2 + 2^3 + 2^6 + 2^7 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-2)f_{13}f_{14} = 2^2(2 + 2^6 + 2^7 + 2^8 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)(-10)f_{13}f_{14} = 2^4(1 + 2 + 2^3 + 2^4 + 2^7 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_{13} \neq W_{14}$, and we conclude $M_{13} \neq M_{14}$.

Claim: $M_{14} \neq M_{15}$

Let W_{14} be as above. For M_{15}, we have

$$b = -10, \alpha_{15} = \sqrt{-10/6}(2 + \sqrt{-2}), \gamma_{15} = \sqrt{-10/6}(-1 + \sqrt{-5})$$

and

$$\delta_{15} = \sqrt{-10/6}(2 + \sqrt{-2}) + \sqrt{-10/6}(-1 + \sqrt{-5}),$$

therefore

$$W_{15} = \langle [\delta_{15}], [\sqrt{-10/6}(2 + \sqrt{-2})], [\sqrt{-10/6}(-1 + \sqrt{-5})], [-10] \rangle.$$

Assume $W_{14} = W_{15}$ then we can write

$$\delta_{14} = \delta_{15}^{\epsilon_1}\alpha_{15}^{\epsilon_2}\gamma_{15}^{\epsilon_3}b^{\epsilon_4}e^2 \tag{3.30}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. Let

$$f_{14} = 2(6\sqrt{-10/38} + 5\sqrt{-10/6})$$

and

$$f_{15} = 2\sqrt{-10/6}.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\delta_{14}) = f_{14}\gamma_{14}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\delta_{15}) = f_{15}\gamma_{15}$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\alpha_{15}) = -10, Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\gamma_{15}) = \gamma_{15}^2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(b) = b^2.$$

Therefore from (3.30) we have

$$\frac{f_{14}\gamma_{14}}{(f_{15}\gamma_{15})^{\epsilon_1}(-10)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-5})^{\times 2}. \tag{3.31}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{14}\gamma_{14}}{(-10)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-5})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}\left(\frac{f_{14}\gamma_{14}}{(-10)^{\epsilon_2}}\right) = \frac{1}{100^{\epsilon_2}} f_{14}^2(-10) \notin \mathbb{Q}_2^{\times 2} \cup (-5)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.31), we have

$$\frac{f_{14}\gamma_{14}}{f_{15}\gamma_{15}(-10)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-5})^{\times 2}.$$

Now we need to find a relation between γ_{14} and γ_{15} module squares in $\mathbb{Q}_2(\sqrt{-5})$. Since

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\frac{\gamma_{14}}{\gamma_{15}}) = 1,$$

we can follow the same method we used in section 3.2.1. So take

$$t = \frac{\gamma_{14}}{\gamma_{15}} \quad \text{and} \quad l = t + 1 = \frac{\gamma_{14} + \gamma_{15}}{\gamma_{15}}.$$

Therefore

$$\frac{\gamma_{14}}{\gamma_{15}} = t = \frac{l^2}{Nm(l)} = \left(\frac{\gamma_{14} + \gamma_{15}}{\gamma_{15}}\right)^2 (2 + 2\sqrt{-10/6}\sqrt{-10/70}). \tag{3.32}$$

So, we need to check whether $(2+2\sqrt{-10/6}\sqrt{-10/70})(-10)^{\epsilon_2} f_{14}f_{15}$ is square in $\mathbb{Q}_2(\sqrt{-5})$. By fixed choice of $\sqrt{-10/38}$, $\sqrt{-10/6}$ and $\sqrt{-10/70}$, we have

$$(2 + 2\sqrt{-10/6}\sqrt{-10/70})f_{14}f_{15} = 2^4(1 + 2 + 2^2 + 2^4 + 2^5 + 2^6 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(2 + 2\sqrt{-10/6}\sqrt{-10/70})(-10)f_{14}f_{15} = 2^4(2 + 2^3 + 2^4 + 2^6 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-2)(2 + 2\sqrt{-10/6}\sqrt{-10/70})f_{14}f_{15} = 2^4(1 + 2^2 + 2^3 + 2^5 + 2^7 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)(2 + 2\sqrt{-10/6}\sqrt{-10/70})(-10)f_{14}f_{15} = 2^4(2 + 2^2 + 2^3 + 2^4 + 2^5 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_{14} \neq W_{15}$, and we conclude $M_{14} \neq M_{15}$.

Claim: $M_{15} \neq M_{16}$

Let W_{15} be as above. For M_{16}, we have

$$b = -10, \alpha_{16} = \sqrt{-10/6}(2 + \sqrt{-2}), \gamma_{16} = \sqrt{-10/70}(5 + 3\sqrt{-5})$$

and

$$\delta_{16} = \sqrt{-10/6}(2 + \sqrt{-2}) + \sqrt{-10/70}(5 + 3\sqrt{-5}),$$

therefore

$$W_{16} = \langle [\delta_{16}], [\sqrt{-10/6}(2 + \sqrt{-2})], [\sqrt{-10/70}(5 + 3\sqrt{-5})], [-10] \rangle.$$

Assume $W_{15} = W_{16}$ then we can write

$$\delta_{15} = \delta_{16}^{\epsilon_1} \alpha_{16}^{\epsilon_2} \gamma_{16}^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.33}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. Let

$$f_{15} = 2\sqrt{-10/6}$$

and

$$f_{16} = 2(2\sqrt{-10/6} + 5\sqrt{-10/70}).$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_{15}) = f_{15}\alpha_{15}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_{16}) = f_{16}\alpha_{16}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\alpha_{16}) = \alpha_{16}^2, Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\gamma_{16}) = -10 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(b) = b^2.$$

Therefore from (3.33) we have

$$\frac{f_{15}\alpha_{15}}{(f_{16}\alpha_{16})^{\epsilon_1}(-10)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}. \tag{3.34}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{15}\alpha_{15}}{(-10)^{\epsilon_3}} \notin \mathbb{Q}_2(\sqrt{-2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}\left(\frac{f_{15}\alpha_{15}}{(-10)^{\epsilon_3}}\right) = \frac{1}{100^{\epsilon_3}} f_{15}^2(-10) \notin \mathbb{Q}_2^{\times 2} \cup (-3)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.34), we have

$$\frac{f_{15}}{f_{16}(-10)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}.$$

So, we need to check whether $(-10)^{\epsilon_3} f_{15} f_{16}$ is square in $\mathbb{Q}_2(\sqrt{-2})$. By fixed choice of $\sqrt{-10/6}$, $\sqrt{-10/70}$ and $\sqrt{-10/38}$ we have

$$f_{15}f_{16} = 2^2(1 + 2 + 2^2 + 2^3 + 2^5 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-10)f_{15}f_{16} = 2^2(2 + 2^3 + 2^5 + 2^{13} + 2^{17} + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-2)f_{15}f_{16} = 2^2(2 + 2^5 + 2^7 + 2^8 + 2^{11} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)(-10)f_{15}f_{16} = 2^4(1 + 2 + 2^3 + 2^5 + 2^6 + 2^7 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_{15} \neq W_{16}$, and we conclude $M_{15} \neq M_{16}$.

Claim: $M_{13} \neq M_{15}$

Assume $W_{13} = W_{15}$ then we can write

$$\delta_{13} = \delta_{15}^{\epsilon_1}\alpha_{15}^{\epsilon_2}\gamma_{15}^{\epsilon_3}b^{\epsilon_4}e^2 \tag{3.35}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. We have

$$f_{13} = 2(6\sqrt{-10/38} - \sqrt{-10/6}$$

and

$$f_{15} = 2\sqrt{-10/6}.$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_{13}) = f_{13}\alpha_{13}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\delta_{15}) = f_{15}\alpha_{15}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\alpha_{15}) = \alpha_{15}^2, Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\gamma_{15}) = -10 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(b) = b^2.$$

Therefore from (3.35) we have

$$\frac{f_{13}\alpha_{13}}{(f_{15}\alpha_{15})^{\epsilon_1}(-10)^{\epsilon_3}} \in \mathbb{Q}_2(\sqrt{-2})^{\times 2}. \tag{3.36}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{13}\alpha_{13}}{(-10)^{\epsilon_3}} \notin \mathbb{Q}_2(\sqrt{-2})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-2})/\mathbb{Q}_2}\left(\frac{f_{13}\alpha_{13}}{(-10)^{\epsilon_3}}\right) = \frac{1}{100^{\epsilon_3}}f_{13}^2(-10) \notin \mathbb{Q}_2^{\times 2} \cup (-2)\mathbb{Q}_2^{\times 2}.$$

Now we need to find a relation between α_{13} and α_{15} module squares in $\mathbb{Q}_2(\sqrt{-2})$. Since

$$Nm_{E/\mathbb{Q}_2(\sqrt{-2})}(\frac{\alpha_{13}}{\alpha_{15}}) = 1,$$

we can follow the same method we used in section 3.2.1. So take

$$t = \frac{\alpha_{13}}{\alpha_{15}} \quad \text{and} \quad l = t + 1 = \frac{\alpha_{13} + \alpha_{15}}{\alpha_{15}}.$$

Therefore

$$\frac{\alpha_{13}}{\alpha_{15}} = t = \frac{l^2}{Nm(l)} = \left(\frac{\alpha_{13} + \alpha_{15}}{\alpha_{15}}\right)^2 (2 - (14/5)\sqrt{-10/6}\sqrt{-10/38}). \tag{3.37}$$

So, we need to check whether $(2 - (14/5)\sqrt{-10/6}\sqrt{-10/38})(-10)^{\epsilon_3} f_{13} f_{15}$ is square in $\mathbb{Q}_2(\sqrt{-2})$. By fixed choice of $\sqrt{-10/6}$, $\sqrt{-10/70}$ and $\sqrt{-10/38}$ we have

$$(2 - (14/5)\sqrt{-10/6}\sqrt{-10/38}) f_{13} f_{15} = 2^4(1 + 2 + 2^2 + 2^3 + 2^4 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(2 - (14/5)\sqrt{-10/6}\sqrt{-10/38})(-10) f_{13} f_{15} = 2^4(2 + 2^3 + 2^6 + 2^{10} + 2^{12} + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

as well as

$$(-2)(2 - (14/5)\sqrt{-10/6}\sqrt{-10/38}) f_{13} f_{15} = 2^4(2 + 2^6 + 2^8 + 2^9 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-2)(2 - (14/5)\sqrt{-10/6}\sqrt{-10/38})(-10) f_{13} f_{15} = 2^6(1 + 2 + 2^3 + 2^4 + 2^6 + 2^7 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_{11} \neq W_{12}$, and we conclude $M_{11} \neq M_{12}$.

Claim: $M_{13} \neq M_{16}$

Assume $W_{13} = W_{16}$ then we can write

$$\delta_{13} = \delta_{16}^{\epsilon_1} \alpha_{16}^{\epsilon_2} \gamma_{16}^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.38}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. we have

$$f_{13} = 2(6\sqrt{-10/38} - \sqrt{-10/6}$$

and

$$f_{16} = 2(2\sqrt{-10/6} + 5\sqrt{-10/70}).$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\delta_{13}) = f_{13}\gamma_{13}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\delta_{16}) = f_{16}\gamma_{16}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\alpha_{16}) = -10, Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\gamma_{16}) = \gamma_{16}^2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(b) = b^2.$$

Therefore from (3.38) we have

$$\frac{f_{13}\gamma_{13}}{(f_{16}\gamma_{16})^{\epsilon_1}(-10)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-5})^{\times 2}. \tag{3.39}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{13}\gamma_{13}}{(-10)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-5})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}\left(\frac{f_{13}\gamma_{13}}{(-10)^{\epsilon_2}}\right) = \frac{1}{100^{\epsilon_2}} f_{13}^2(-10) \notin \mathbb{Q}_2^{\times 2} \cup (-5)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.39), we have

$$\frac{f_{13}\gamma_{13}}{f_{16}\gamma_{16}(-10)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-5})^{\times 2}.$$

Using the fact that $\gamma_{13} = \gamma_{15}$ and $\gamma_{16} = \gamma_{14}$, also by (3.32), we have

$$\frac{\gamma_{13}}{\gamma_{16}} = \left(\frac{\gamma_{13} + \gamma_{16}}{\gamma_{16}}\right)^2 \frac{1}{2 + 2\sqrt{-10/6}\sqrt{-10/70}}.$$

So, we need to check whether $(2 + 2\sqrt{-10/6}\sqrt{-10/70})(-10)^{\epsilon_2} f_{13} f_{16}$ is square in $\mathbb{Q}_2(\sqrt{-5})$. By fixed choice of $\sqrt{-10/6}$, $\sqrt{-10/70}$ and $\sqrt{-10/38}$ we have

$$(2 + 2\sqrt{-10/6}\sqrt{-10/70}) f_{13} f_{16} = 2^2(1 + 2 + 2^2 + 2^3 + 2^6 + 2^7 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(2 + 2\sqrt{-10/6}\sqrt{-10/70})(-10) f_{13} f_{16} = 2^4(2 + 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + \cdots) \notin \mathbb{Q}_2^{\times 2},$$

as well as

$$(-5)(2 + 2\sqrt{-10/6}\sqrt{-10/70}) f_{13} f_{16} = 2^2(1 + 2^2 + 2^4 + 2^5 + 2^6 + 2^7 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-5)(2 + 2\sqrt{-10/6}\sqrt{-10/70})(-10) f_{13} f_{16} = 2^4(2 + 2^2 + 2^3 + 2^5 + 2^6 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_9 \neq W_{12}$, and we conclude $M_9 \neq M_{12}$.

Claim: $M_{14} \neq M_{16}$

Assume $W_{14} = W_{16}$ then we can write

$$\delta_{14} = \delta_{16}^{\epsilon_1} \alpha_{16}^{\epsilon_2} \gamma_{16}^{\epsilon_3} b^{\epsilon_4} e^2 \tag{3.40}$$

for some $\epsilon_1, \cdots \epsilon_4 \in \{0, 1\}$ and $e \in E^\times$. Let

$$f_{14} = 2(6\sqrt{-10/38} + 5\sqrt{-10/6})$$

and

$$f_{16} = 2(2\sqrt{-10/6} + 5\sqrt{-10/70}).$$

Now we take the norm of both sides. So, we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\delta_{14}) = f_{14}\gamma_{14}$$

and

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\delta_{16}) = f_{16}\gamma_{16}.$$

Also we have

$$Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\alpha_{16}) = -10, Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(\gamma_{16}) = \gamma_{16}^2 \text{ and } Nm_{E/\mathbb{Q}_2(\sqrt{-5})}(b) = b^2.$$

Therefore from (3.40) we have

$$\frac{f_{14}\gamma_{14}}{(f_{16}\gamma_{16})^{\epsilon_1}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-5})^{\times 2}. \tag{3.41}$$

But for $\epsilon_1 = 0$,

$$\frac{f_{14}\gamma_{14}}{(-10)^{\epsilon_2}} \notin \mathbb{Q}_2(\sqrt{-5})^{\times 2}$$

because

$$Nm_{\mathbb{Q}_2(\sqrt{-5})/\mathbb{Q}_2}\left(\frac{f_{14}\gamma_{14}}{(-10)^{\epsilon_2}}\right) = \frac{1}{100^{\epsilon_2}} f_{14}^2(-10) \notin \mathbb{Q}_2^{\times 2} \cup (-5)\mathbb{Q}_2^{\times 2}.$$

For $\epsilon_1 = 1$, from (3.41) and the fact that $\gamma_{14} = \gamma_{16}$, we have

$$\frac{f_{14}}{f_{16}(-2)^{\epsilon_2}} \in \mathbb{Q}_2(\sqrt{-5})^{\times 2}.$$

So, we need to check whether $(-10)^{\epsilon_2} f_{14} f_{16}$ is square in $\mathbb{Q}_2(\sqrt{-5})$. By fixed choice of $\sqrt{-10/6}$, $\sqrt{-10/70}$ and $\sqrt{-10/38}$ we have

$$f_{14}f_{16} = 2^2(1 + 2^2 + 2^6 + 2^7 + 2^9 + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-5)f_{14}f_{16} = 2^2(1 + 2 + 2^2 + 2^5 + 2^9 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

as well as

$$(-10)f_{14}f_{16} = 2^2(2 + 2^2 + 2^3 + 2^6 + 2^{10} + \cdots) \notin \mathbb{Q}_2^{\times 2}$$

and

$$(-5)(-10)f_{14}f_{16} = 2^2(2 + 2^3 + 2^4 + 2^5 + 2^6 + \cdots) \notin \mathbb{Q}_2^{\times 2}.$$

So this is a contradiction. Hence $W_{14} \neq W_{16}$, and we conclude $M_{14} \neq M_{16}$.

3.2.5 Conclusion

Theorem 3.2.2. *$M_1, M_2, \cdots, M_{16}$ are all $U_4(\mathbb{F}_2)$-Galois extensions of $\mathbb{Q}_2$.*

Proof. By [MT14a, Theorem 3.7], we know that there are only 16 $U_4(\mathbb{F}_2)$-Galois extensions of $\mathbb{Q}_2$. Also by [MT15b] all of the extensions $M_1, \cdots, M_{16}$ are Galois extensions of $\mathbb{Q}_2$ and their Galois groups are isomorphic to $U_4(\mathbb{F}_2)$.

The only part remaining is to show $M_1, \cdots, M_{16}$ are distinct. In the sections 3.2.1, 3.2.2, 3.2.3 and 3.2.4, we already showed that $|\{M_i, M_{i+1}, M_{i+2}, M_{i+3}\}| = 4$ for $i = 1, 5, 9, 13$. So now, we need to show, for a fixed $i, j = 1, 5, 9, 13$ and $i \neq j$, we have

$$\{M_i, M_{i+1}, M_{i+2}, M_{i+3}\} \cap \{M_j, M_{j+1}, M_{j+2}, M_{j+3}\} = \phi.$$

All dihedral extensions of $M_1, \cdots, M_4$ contain $\sqrt{-1}$, but there are some dihedral extensions in $M_5, \cdots, M_{16}$ such that they don't contain $\sqrt{-1}$. So

$$M_5, \cdots, M_{16} \notin \{M_1, M_2, M_3, M_4\}.$$

Similarly, all dihedral extensions of $M_5, \cdots, M_8$ contain $\sqrt{-5}$, but there are some dihedral extensions in $M_1, \cdots, M_4$ and $M_9, \cdots, M_{16}$ such that they don't contain $\sqrt{-5}$. So

$$M_1, \cdots, M_4, M_9, \cdots, M_{16} \notin \{M_5, M_6, M_7, M_8\}.$$

Also, all dihedral extensions of $M_9, \cdots, M_{12}$ contain $\sqrt{-2}$, but there are some dihedral extensions in $M_1, \cdots, M_8$ and $M_{13}, \cdots, M_{16}$ such that they don't contain $\sqrt{-2}$. So

$$M_1, \cdots, M_8, M_{13}, \cdots, M_{16} \notin \{M_9, M_{10}, M_{11}, M_{12}\}.$$

Finally, all dihedral extensions of $M_{13}, \cdots, M_{16}$ contain $\sqrt{-10}$, but there are some dihedral extensions in $M_1, \cdots, M_{12}$ such that they don't contain $\sqrt{-10}$. So

$$M_1, \cdots, M_{12} \notin \{M_{13}, M_{14}, M_{15}, M_{16}\}.$$

□

Theorem 3.2.3. *There is no $U_n(\mathbb{F}_2)-$extension of $\mathbb{Q}_2$ for $n \geq 5$.*

Proof. Let M be a $U_n(\mathbb{F}_2)-$extension of $\mathbb{Q}_2$. Let $ker(\varphi)$ be the kernel of the surjective map $\varphi : U_n(\mathbb{F}_2) \to \mathbb{F}_2^{n-1}$ where $\varphi([a_{ij}]) = (a_{1,2}, a_{2,3}, \cdots, a_{n-1,n})$. Also assume K to be the fixed field of $ker(\varphi)$, so $Gal(K/\mathbb{Q}_2) \cong U_n(\mathbb{F}_2)/ker(\varphi) \cong \mathbb{F}_2^{n-1}$.

To generate K, we need exactly $n-1$ $\mathbb{F}_2-$linearly independent elements of $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. But $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ has only three linearly independent elements. Therefore, for $n \geq 5$, there are not enough linearly independent elements to generate K. Hence, there is no $U_n(\mathbb{F}_2)-$extension of $\mathbb{Q}_2$ for $n \geq 5$. □

Corollary 3.2.4. *Number of $U_n(\mathbb{F}_2)-$extensions of $\mathbb{Q}_2$ is as follows:*

$$\#\{U_n(\mathbb{F}_2) - \textit{extensions of } \mathbb{Q}_2\} = \begin{cases} 7 & \textit{if } n = 2 \\ 18 & \textit{if } n = 3 \\ 16 & \textit{if } n = 4 \\ 0 & \textit{if } n \geq 5 \end{cases} \tag{3.42}$$

Proof. Chapter 2 and Theorems 3.2.2 and 3.2.3. ⊡

Summary

In this thesis we classify all $U_4(\mathbb{F}_2)-$Galois extensions L/F. Using the same method, we classify all $U_3(\mathbb{F}_2)-$Galois extensions which are isomorphic to the dihedral extensions over any fields. Also, as an example, we list all $U_n(\mathbb{F}_2)-$Galois extensions of $\mathbb{Q}_2$.

An open question is extending the results to all $U_n(\mathbb{F}_p)-$Galois extensions for all natural numbers n and prime numbers p. Another interesting problem is to replace $\mathbb{F}_p$ by any finite fields.

These problems are part of a major problem in Galois theory which is the classification of all Galois extensions over any fields.

Bibliography

[Ama14] Fumiya Amano. On a certain nilpotent extension over $\mathbb{Q}$ of degree 64 and the 4-th multiple residue symbol. *Tohoku Mathematical Journal*, 66(4):501–522, 2014.

[AMT15] Masoud Ataei, Ján Mináč, and Nguyễn Duy Tân. Description of Galois unipotent extensions. *arXiv preprint arXiv:1508.05540*, 2015.

[BD01] Daniel K Biss and Samit Dasgupta. A presentation for the unipotent group over rings with identity. *Journal of Algebra*, 237(2):691–707, 2001.

[CF67] John W.S. Cassels and Albrecht Fröhlich. *Algebraic number theory*. Academic Press, London, 1967.

[Coh08] Henri Cohen. *Number theory: Volume I: Tools and diophantine equations*, volume 239. Springer-Verlag, 2008.

[Con65] Ian G Connell. Elementary generalizations of Hilbert's Theorem 90. *Canad. Math. Bull*, 8(6), 1965.

[DGMS75] Pierre Deligne, Phillip Griffiths, John Morgan, and Dennis Sullivan. Real homotopy theory of Kähler manifolds. *Inventiones mathematicae*, 29(3):245–274, 1975.

[Dwy75] William G Dwyer. Homology, Massey products and maps between groups. *Journal of Pure and Applied Algebra*, 6(2):177–190, 1975.

[Efr14] Ido Efrat. The Zassenhaus filtration, Massey products, and representations of profinite groups. *Advances in Mathematics*, 263:389–411, 2014.

[EM11] Ido Efrat and Ján Mináč. On the descending central sequence of absolute Galois groups. *American journal of mathematics*, 133(6):1503–1532, 2011.

[EM14] Ido Efrat and Eliyahu Matzri. Triple Massey products and absolute Galois groups. *arXiv preprint arXiv:1412.7265*, 2014.

[HW15] Michael J Hopkins and Kirsten G Wickelgren. Splitting varieties for triple Massey products. *Journal of Pure and Applied Algebra*, 219(5):1304–1319, 2015.

[Jac64] Nathan Jacobson. *Lectures in abstract algebra. Vol. 3, Theory of fields and Galois theory*. Springer-Verlag, 1964.

[Jar11] Moshe Jarden. *Algebraic patching*. Springer-Verlag, 2011.

[JLY02] Christian U Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials: constructive aspects of the inverse Galois problem*, volume 45. Cambridge University Press, 2002.

[Koc02] Helmut Koch. *Galois theory of p-extensions*. Springer-Verlag, 2002.

[Lam05] Tsit-Yuen Lam. *Introduction to quadratic forms over fields*. American Mathematical Soc., 2005.

[Lan13] Serge Lang. *Algebraic number theory*, volume 110. Springer-Verlag, 2013.

[Led05] Arne Ledet. *Brauer type embedding problems*, volume 21. American Mathematical Soc., 2005.

[LMS03] David B Leep, Ján Mináč, and Tara L Smith. Galois groups over nonrigid fields. *Valuation Theory and its Applications*, 33:61–77, 2003.

[Mas58] William S Massey. Some higher order cohomology operations. In *Symposium internacional de topologıa algebraica International symposium on algebraic topology*, pages 145–154, 1958.

[Mas87] Richard Massy. Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p. *Journal of Algebra*, 109(2):508–535, 1987.

[McL08] Cam McLeman. p-Tower groups over quadratic imaginary number fields. *Ann. Sci. Math. Québec*, 32(2):199–209, 2008.

[MNQD77] Richard Massy and Thong Nguyễn -Quang-Do. Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3: étude locale-globale. *J. Reine Angew. Math.*, 291:149–161, 1977.

[MS90] Ján Mináč and Michel Spira. Formally real fields, Pythagorean fields, C-fields and W-groups. *Mathematische Zeitschrift*, 205(4):519–530, 1990.

[MS96] Ján Mináč and Michel Spira. Witt rings and Galois groups. *Annals of mathematics (2)*, 144(1):35–60, 1996.

[MT13] Ján Mináč and Nguyễn Duy Tân. Triple Massey products and Galois theory. *arXiv preprint arXiv:1307.6624 - It will appear in Journal of European Mathematical Society*, 2013.

[MT14a] Ján Mináč and Nguyễn Duy Tân. Counting Galois $\mathbb{U}_4(\mathbb{F}_p)-$extensions using Massey products. *arXiv preprint arXiv:1408.2586*, 2014.

[MT14b] Ján Mináč and Nguyễn Duy Tân. Triple Massey products vanish over all fields. *arXiv preprint arXiv:1412.7611*, 2014.

[MT15a] Ján Mináč and Nguyễn Duy Tân. The kernel unipotent conjecture and the vanishing of Massey products for odd rigid fields. *Advances in Mathematics*, 273:242–270, 2015.

[MT15b] Ján Mináč and Nguyễn Duy Tân. Construction of unipotent Galois extensions and Massey products. *arXiv preprint arXiv:1501.01346*, 2015.

[MZ11] Ivo M Michailov and Nikola P Ziapkov. On realizability of p-groups as Galois groups. *arXiv preprint arXiv:1112.1522*, 2011.

[Nai95] Hirotada Naito. Dihedral extensions of degree 8 over the rational p-adic fields. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 71(1):17–18, 1995.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Springer-Verlag, 1999.

[NSW13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323. Springer-Verlag, 2013.

[Sal82] David J Saltman. Generic Galois extensions and problems in field theory. *Advances in Mathematics*, 43(3):250–283, 1982.

[Ser78] Jean-Pierre Serre. Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local. *C. R. Acad. Sci. Paris Sér. A-B*, 286(22):A1031–A1036, 1978.

[Ser13] Jean-Pierre Serre. *Local fields*, volume 67. Springer-Verlag, 2013.

[Sha72] Stephen S Shatz. *Profinite groups, arithmetic, and geometry*. Number 67. Princeton university press, 1972.

[Vil] Fernando R. Villegas. Relations between quadratic forms and certain Galois extensions, a manuscript, Ohio State University, 1988.

[Wat74] William C Waterhouse. Profinite groups are Galois groups. *Proceedings of the American Mathematical Society*, 42(2):639–640, 1974.

[Wat94] William C Waterhouse. The normal closures of certain Kummer extensions. *Canad. Math. Bull*, 37(1):133–139, 1994.

[Wei95] André Weil. Basic number theory, reprint of the second (1973) edition, Classics in Mathematics, 1995.

[Yam95] Masakazu Yamagishi. On the number of Galois p-extensions of a local field. *Proceedings of the American Mathematical Society*, 123(8):2373–2380, 1995.

Curriculum Vitae

Name: Masoud Ataei Jaliseh

Education

University of Western Ontario
London, ON
2011 - 2015 Ph.D. in Mathematics

Institute for Advanced Studies in Basic Sciences (IASBS)
Zanjan, Iran
2009–2011 MSc in Mathematics

Related Work Experience: Teaching Assistant
The University of Western Ontario
2011 - 2015

Publications:

- Masoud Ataei, Ján Mináč and Nguyễn Duy Tân, *Description of Galois unipotent extensions* arXiv preprint arXiv:1508.05540, 2015.
- Masoud Ataei, *A new good Galois tower of function fields over finite fields* (In Progress).
- Masoud Ataei, Michael Bush, Ján Mináč and Nguyễn Duy Tân, *Constructions of Galois extensions with restricted ramification* (In Progress).