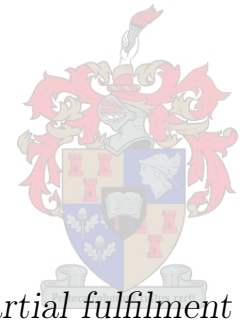
The Geometry Of The Moduli Space Of Biquadratic Field Extensions

by

Mpendulo Cele



Thesis presented in partial fulfilment of the requirements for the degree of Master of Science (Mathematics) in the Faculty of Science at Stellenbosch University

Supervisor: Dr. S. Marques

December 2020

Stellenbosch University https://scholar.sun.ac.za

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: October 2020 .....

Copyright © 2020 Stellenbosch University
All rights reserved.

Stellenbosch University https://scholar.sun.ac.za

Abstract

The Geometry Of The Moduli Space Of Biquadratic Field Extensions

M. Cele

Department of Mathematical Sciences,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Thesis: MSc (Mathematics)

December 2020

Mathematicians are always interested in understanding mathematical objects from different angles, This makes the task of classifying mathematical objects useful, as it permits one to study a mathematical object and infer the conclusions on another mathematical object that has the same underlying structure as the one studied. In this thesis we study the moduli space of non-cyclic biquadratic field extensions over any field whose characteristic if not 2.

Keywords : biquadratic, elementary abelian, Galois, radical

Stellenbosch University https://scholar.sun.ac.za

Uittreksel

Die meetkunde van die Moduli-ruimte van Bikadratiese velduitbreiding

("The Geometry Of The Moduli Space Of Biquadratic Field Extensions")

M. Cele

Departement Meganiese en Megatroniese Ingenieurswese,
Universiteit van Stellenbosch,
Privaatsak X1, Matieland 7602, Suid Afrika.

Tesis: Msc (Mathematics)

Desember 2020

Wiskundiges is altyd geïnteresseerd in die verstaan van wiskundige voorwerpe vanuit verskillende hoeke, Dit maak die taak om wiskundige voorwerpe te klassifiseer nuttig, aangesien dit een toelaat om a te bestudeer wiskundige voorwerp en lei die gevolgtrekkings oor 'n ander wiskundige voorwerp wat bestaan dieselfde onderliggende struktuur as die een wat bestudeer is. In hierdie tesis bestudeer ons die modulêre ruimte van nie-sikliese tweekadratiese velduitbreidings oor enige veld waarvan die kenmerk is so nie 2.

Keywords : bisadraties, elementere abeliaanse, Galois, radikaal

Stellenbosch University https://scholar.sun.ac.za

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Dr. Sophie Marques for guiding and assisting me in the development of this work, helping better understand mathematics and research in general. Her kindness and advices were very valuable and have helped me grow.

I would like to Prof. Francesco Baldassarri and Dr. Gareth Boxall for kindly agreeing to review the present thesis.

Throughout the writing of this dissertation I have received a great deal of support and assistance. I would like to thank University of Stellenbosch for the opportunity to do this work and the funding they provided for my studies. I would also like thank University of Padova and ALGANT for funding me for a year abroad and offering me courses that have improved my research and broaden the scope of my knowledge in Mathematics. In particular, I would like to thank Miss. Elisa Zombo, Mr. Christopher Niesen, Mrs. Lisa Muller and Mrs. Claudia Meyer for making themselves available and providing me with sound advice when I needed help.

I would like to thank my family and friends for the encouragement and support they have been giving me.

Stellenbosch University https://scholar.sun.ac.za

Dedications

To my family and Nontobeko Sibiya.

Stellenbosch University https://scholar.sun.ac.za

Contents

Stellenbosch University https://scholar.sun.ac.za

Introduction

In a previous work done by S. Marques and K. Ward in [6], [7], [8], the existence and the uniqueness of the purely cubic closure for cubics extension was identified and permitted to define purely cubic descent. These constructions have been used to classify cubic extensions as well as in computation of integral basis [9] and Riemann-Hurwitz formulae [10]. In this thesis, we start a similar approach for biquadratic extensions. The exploration of the existence of the radical closure (see Definition 3.2.8) for elementary abelian extensions revealed that radical extensions and elementary abelian extensions rarely intersect (see Theorem 4.1.4). Biquadratic extensions are quite different from cubic extensions. Fundamentally it begins with the two possible structure for groups of order 4: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ giving rise to two types of Galois extensions of degree 4: the elementary abelian extensions and the cyclic extensions. Moreover, it was possible to nicely exhibit the geometry of the moduli space of the elementary abelian extension without the use of the radical closure (see Theorem 4.1.17). Therefore, it became natural to wonder if in the quartic case, it could be that the notion of elementary abelian closure (see Definition 3.2.10) becomes of particular interest and could be used to better understand the moduli space of those extensions up to isomorphism. In this thesis we explore this idea. Some extensive work have been done on biquadratic extensions such as [1], [16], [3]. But the technics we used have not been used before on quartic extension, this work extends the work done by S. Marques and K. Ward on cubic extensions.

We begin by studying groups and field extensions in Chapter 1, revising general results that we will need later. In Chapter 2 we classify quadratic field extensions, Theorem 2.1.2 plays a key role on the classification of biquadratic extensions. This permitted us to understand the classification problem through the simplest example of field extensions.

In the Chapter 3, we start with identifying two families of polynomials with two parameters that permit to construct any quartic extension (Lemma 3.3.1 and Corollary 3.3.2). In doing so, we make explicit any change of variable that permits to pass from a general quadratic polynomial to one of those form. Among these two families, we find the biquadratic polynomials. The rest of the thesis will focus on those. We first recall a few generalities about biquadratic extensions. In section 3.4 we provide a characterization of biquadratic extensions (see Lemma 3.4.1), a criterium to determine the irreducibility of a biquadratic polynomial (see Lemma 3.4.2), a criterium to determine the biquadratic extensions that are Galois (see Lemma 3.4.4) and how to characterize the biquadratic extension according to their automorphism group (see Lemma 3.4.6).

In section 4 we studied and elementary abelian closure and radical closure, then described geometrically in group theoretic term the elementary abelian extensions and

Stellenbosch University https://scholar.sun.ac.za

non-cyclic extensions. The technics explored here are built so that they can be generalised for higher degree extensions in future.

The main goal of Section 4 is to classify elementary abelian extensions so that we can describe the geometry of the moduli space of those extensions in group theoretic term. This is obtained in one of the main theorems of this section: Theorem 4.1.17. In doing so, we found various nice characterisations of elementary abelian extension (Theorem 4.1.1), that helped with the classification of elementary abelian extensions. Along the way, we identified when elementary abelian extension are radical, that happens precisely when $F(i)$ is a quadratic subextension this extension (Theorem 4.1.4), which is a rare instance and explored a bit this path nevertheless. We discover that the radical closure may exist in other instances in the elementary abelian case but is non-unique, making it non applicable.

Understanding that the radical closure is not always of help for classification problems, In section 4.2, we identify when and how we can make use of the classification of elementary abelian extensions obtained in the previous section, using the notion of elementary abelian closure and descending along it. We realize in Lemma 4.2.2 that the existence of an elementary abelian closure is equivalent of being non-cyclic and that in this case, the elementary abelian closure happens to be unique. The next result of the section, Theorem 4.2.3 permits to understand isomorphism classes of non-cyclic biquadratic extensions using the elementary abelian closure. In other words, it proves that isomorphism classes can be descended via the elementary abelian closure. In the remaining part of the chapter, we highlight the geometry of the moduli space of those extensions. This conclude into the main result the paper Theorem 4.2.8 that brings together all the pieces constructed previously into the same universe.

The main goal of Chapter 5 is to present necessary and sufficient for existence and uniqueness of radical closure for non-elementary abelian extension. We begin by classifying radical elementary abelian extensions in Lemma 5.0.1, then present the main theorem of the section Theorem 5.0.6.

Stellenbosch University https://scholar.sun.ac.za

Chapter 1

Groups and Field Extensions

Results presented in this chapter can be found in almost any Group Theory, Field Theory, Galois Theory and Number Theory book, these are the main sources of this content [13] [14] [15]

1.1 Groups of order p^2

In this section we recall some basic properties of finite groups.

Definition 1.1.1. *Let G be a group. G is a said to be a p-group for some prime number p if any element of G has order p^k for some integer k.*

Remark 1.1.2. *Let G be a finite p-group, then the center $Z(G)$ of G is non-trivial.*

Remark 1.1.3. *Let G be a finite group and $Z(G)$ be the center of G, if $G/Z(G)$ is cyclic then G is abelian.*

Lemma 1.1.4. *Let G be a group of order p^2 where p is a prime number then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof. If G has an element of order p^2 then G is cyclic hence isomorphic to $\mathbb{Z}_{p^2}$. So we can assume G is does not have an element of order p^2, wstart by showing that G is abelian. By Lagrange theorem and Remark 1.1.2 we have that $|Z(G)| \in \{p, p^2\}$. If $|Z(G)| = p^2$ then $G = Z(G)$ hence G is abelian. Now, if $|Z(G)| = p$ then $|G/Z(G)| = p \implies G/Z(G)$ is cyclic hence G is abelian by Remark 1.1.3. Let $H :=< x >$ and $K :=< y >$ where $x \in G$ and $y \in G - H$ are non-identity elements, then $|H| = |K| = p$, since $H \cap K = \{e\}$. We claim that $H \times K \cong HK$. Let $\psi : H \times K \to HK$ be defined by $\psi(x^a, y^b) = x^a y^b$. Let $\alpha, \beta \in H \times K$ then $\alpha = (x^a, y^b)$ and $\beta = (x^c, y^d)$ for some $a, b, c, d \in \mathbb{Z}$. Then $\psi(\alpha\beta) = \psi(x^{a+c}, y^{b+d}) = x^{a+c}y^{b+d} = (x^a y^b)(x^c y^d) = \psi(\alpha)\psi(\beta)$ proving that ψ is a group homomorphism. ψ is clearly surjective so show that ψ is an isomorphism it suffices to show that ψ is injective. Suppose $\psi(\alpha) = \psi(\beta)$ i.e $x^a y^b = x^c y^d$ that is $x^{a-c} = y^{d-b} \in H \cap K$ hence $a - c = 0$ and $b - d = 0$, now $a = c$ and $b = d$ proving that $\alpha = \beta$ so indeed ψ is an isomorphism. Since $HK \subseteq G$ and $|HK| = |H \times K| = p^2$, we have that $HK = G$. Finally, $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$ as desired. □

1.2 Quotient Rings

In this section we prove that one can construct a field from a ring with a maximal ideal.

Stellenbosch University https://scholar.sun.ac.za

Definition 1.2.1. *Let R be a ring. An ideal I of R is said to be maximal in R if whenever J is an ideal of R containing I, then $J = I$ or $J = R$.*

Theorem 1.2.2 (Maximal ideal theorem)**.** *Let R be a ring with identity and M be a proper ideal in R, then M is a maximal ideal in R if and only if R/M is a field.*

Proof. $\implies$ Suppose M is a maximal ideal in R. We want to prove that any non-zero element in R/M has an inverse in R/M. Let $a \notin M$ be an element of R then $a+M \neq M$. Let $I = \{ra + m | r \in R, m \in M\}$, we will show that I is an ideal in R properly containing M. Let $i_1, i_2 \in I$ then $i_1 = r_1a + m_1$ and $i_2 = r_2a + m_2$ for some $r_1, r_2 \in R$ and $m_1, m_2 \in M$. We have $i_1 - i_2 = (r_1 - r_2)a + (m_1 - m_2) \in I$, also let $r \in R$ then $ri_1 = (rr_1)a + rm_1 \in I$ since $rr_1 \in R$ and $rm_1 \in M$, hence I is indeed an ideal in R. We now show that I properly contains M, let $m_3 \in M$ then $m_3 = 0a + m_3 \in I \implies M \subseteq I$, but $a = 1a + 0 \in I$ and $a \notin M$ therefore $M \subsetneq I$. Now M is properly contained in an ideal I then $I = R$ (since M is a maximal ideal in R), this then implies $1 \in I \implies 1 = ra + m$ for some $r \in R$ and $m \in M$ then $1 + M = (ra + m) + M = ra + M = (r + M)(a + M)$ as desired we have found an inverse of $a + M$ hence R/M is indeed a field.

$\impliedby$ Suppose R/M is a field. We want to show that M is a maximal ideal in R, that is if I is any ideal that properly contains M then $I = R$. Let I be any ideal in R properly containing M. Let $xI - M$ then $x + M \neq M$ hence there exist $y \in R$ such that $(y + M)(x + M) = yx + M = 1 + M$ which implies $1 - yx \in M \subset I$, since $x \in I$ then $yx \in I \implies (1 - xy) + yx = 1 \in I \implies I = R$ hence M is indeed a maximal ideal. □

Definition 1.2.3. *Let R be a ring and I be an ideal of R, then I is said to be a principal ideal of R if I is generated by some element $a \in R$, that is $I = <a>$.*

Definition 1.2.4. *Let R be a ring, R is said to be a principal ideal domain(PID) if every ideal of R is a principal ideal.*

Lemma 1.2.5. *Let F be a field, then the ring $F[X]$ of polynomials with coefficients from F is a principal ideal domain.*

Proof. Let I be an ideal in $F[X]$, Let $P(X)$ be a polynomial with minimal degree in I. Let $G(X) \in I$ then by the division algorithm there exists $Q(X), R(X) \in F[X]$ such that $G(X) = Q(X)P(X) + R(X)$ and the degree of $R(X)$ is less than the degree of $P(X)$ or $R(X) = 0$. We have $R(X) = G(X) - Q(X)P(X) \in I$ (since $G(X)$ and $Q(X)P(X)$ are in I), now $P(X)$ having minimal degree in I implies $R(X) = 0$ and so $G(X) = Q(X)P(X)$ as desired we have that I is principal ideal generated by $P(X)$. □

Definition 1.2.6. *Let R be a ring and I be an ideal of R, then I said to be a prime ideal of R if whenever $xy \in I$ then $x \in I$ or $y \in I$.*

Lemma 1.2.7. *Let F be a field, then every prime ideal of $F[X]$ is a maximal ideal generated by an irreducible polynomial in $F[X]$.*

Proof. Let I be a prime ideal in $F[X]$ and J be an ideal in $F[X]$ such that $I \subseteq J$. By Lemma 1.2.5 we have that $I = <P(X)>$ and $J = <Q(X)>$ for some $P(X), Q(X) \in F[X]$. $I \subseteq J \implies P(X) \in <Q(X)> \implies P(X) = C(X)Q(X)$ for some $C(X) \in R[X]$. Now I is a prime ideal hence $C(X) \in I$ or $Q(X) \in I$, if $Q(X) \in I$ then $J \subseteq I$ which implies $I = J$. If $C(X) \in I$ then $C(X) = P(X)D(X)$ for some $D(X) \in F[X]$ hence

Stellenbosch University https://scholar.sun.ac.za

$P(X) = C(X)Q(X) = P(X)D(X)Q(X)$, we now have $1 = D(X)Q(X)$, this is because $F[X]$ is an integral domain, so $1 \in J$ hence $J = R[X]$, proving that I is indeed a maximal ideal. It remains to show that $P(X)$ is irreducible over F. On the contrary $P(X)$ is reducible over F, that is there non-constant polynomials $A(X)$ and $B(X)$ such that $P(X) = A(X)B(X)$. It follows that $P(X) \in <A(X)>$ hence $I \subset <A(X)>$, by maximality of I we have that $<A(X)> = R[X]$. $1 \in <A(X)>$ implies $A(X)$ is a constant polynomial, which is a contradiction so indeed $P(X)$ is irreducible over F. □

Theorem 1.2.8. *Let F be a field then $P(X) \in F[X]$ is irreducible over F if and only if $<P(X)>$ is a maximal ideal in $F[X]$.*

Proof. $\Longleftarrow$ Let $<P(X)>$ be a maximal ideal of $F[X]$, then $<P(X)>$ is a prime ideal hence $P(X)$ is irreducible by Lemma 1.2.7.

$\Longleftarrow$ Suppose $P(X)$ is irreducible over F, Let J be an ideal in $F[X]$ such that $<P(X)> \subseteq J$, by Lemma 1.2.5 there exists $Q(X) \in F[X]$ such that $J = <Q(X)>$. It follows that from $<P(X)> \subseteq J$ that $P(X) = A(X)Q(X)$ for some $A(X) \in F[X]$, by the irreducibility of $P(X)$ over F we conclude that either $A(X)$ or $B(X)$ is a constant polynomial. So $A(X) = a$ or $Q(X) = a$ for some $a \neq 0 \in F$. If $A(X) = a$ then $Q(X) = a^{-1}P(X) \in <P(X)>$ hence $J \subseteq <P(X)>$ and so $J = <P(X)>$. If $Q(X) = a$ then $1 = a^{-1}Q(X) \in J$ hence $J = F[X]$ so indeed $<P(X)>$ is a maximal ideal. □

Remark 1.2.9. *Let F be a field and $P(X) \in F[X]$ then $P(X)$ is irreducible over F if and only if $F[X]/<P(X)>$ is a field, this follows from the previous theorem and Lemma 1.2.2.*

1.3 Field Extensions

In the previous section we constructed a field $F[X]/<P(X)>$ when $P(X) \in F[X]$ was a irreducible over F. In this section we will show that F is embedded in such a field and study some properties of field extensions.

Definition 1.3.1. *Let E be a field and F be a subfield of E, we say E is an extension of F. We will use E/F to denote that E is an extension of F.*

Remark 1.3.2. *If E/F is a field extension then E is a vector space over F.*

Definition 1.3.3. *Let E/F be a field extension, we define the degree of E/F to be the dimension of the vector space E over F. We will denote the degree of E/F as $[E : F]$.*

Definition 1.3.4. *We say that E/F is a finite field extension, when $[E : F] < \infty$.*

Lemma 1.3.5. *Let $K \subseteq F \subseteq E$ be a tower of finite field extensions then*

$$[E : F][F : K] = [E : K].$$

Proof. Let E/F and F/K be two finite dimensional extensions. Suppose $[E : F] = n$ and $[F : K] = m$. Let $\{e_1, e_2, \ldots, e_n\}$ be a basis of E over F and $\{f_1, f_2, \ldots, f_m\}$ be a basis of F over K. We claim that $B = \{e_i f_j \mid i \in [1, n] \text{ and } j \in [1, m]\}$ is a basis of E over K. Let $\lambda \in E$, then $\lambda = \sum_{i=1}^{n} a_i e_i$ where $a_i \in F$ and $a_i = \sum_{j=1}^{m} b_{ij} f_j$ where $b_{ij} \in K$, thus

Stellenbosch University https://scholar.sun.ac.za

we have $\lambda = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} b_{ij}f_j\right)e_i = \sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}f_je_i$ hence B does indeed span E over K. It now remains to show that B is linearly independent over K, on the contrary suppose $\sum_{i=1}^{n}\left(\sum_{j=1}^{m} b_{ij}f_j\right)e_i = 0$, since $\{e_1, e_2, \ldots, e_n\}$ is linearly independent over F it follows that $\sum_{j=1}^{m} b_{ij}f_j = 0$ for each $j \in [1, m]$, since $\{f_1, f_2, \ldots, f_m\}$ is linearly independent over K then $b_{ij} = 0$ for all $i,\ j$. Hence B is a basis of E over K and $[E : K] = nm = [E : F][F : K]$ as desired. □

Lemma 1.3.6. *Let F be a field and $P(X) \in F[X]$ be irreducible over F then $E = F[X]/<P(X)>$ has a subfield isomorphic to F, Moreover $P(X)$ has a root in E.*

Proof. Let $\phi : F \to F[X]/<P(X)>$ be defined by $\phi(a) = a + <P(X)>$. We claim that ϕ is an injective ring homomorphism. Let $a, b \in F$ then $\phi(a+b) = (a+b) + <P(X)> = (a + <P(X)>) + (b + <P(X)>) = \phi(a) + \phi(b)$, Also $\phi(ab) = ab + <P(X)> = (a + <P(X)>)(b + <P(X)>) = \phi(a)\phi(b)$. It remains to show that ϕ is injective. Suppose $\phi(a) = \phi(b)$ then $a + <P(X)> = b + <P(X)>$ implies $a - b \in <P(X)>$. If $a - b \neq 0$ the $1 = (a-b)^{-1}(a-b) \in <P(X)>$ which is impossible hence $a - b = 0$ so $a = b$ and ϕ is injective. It follows that $\phi : F \to \phi(F)$ is a ring isomorphism. We now show that $\alpha := X + <P(X)>$ is a root of $P(X)$ in $F[X]/<P(X)>$. Suppose $P(X) = a_0 + a_1X + \cdots + a_nX^n$, then

$$\begin{aligned} P(\alpha) &= a_0 + a_1(X + <P(X)>) + \cdots + a_n(X + <P(X)>)^n \\ &= a_0 + (a_1X + <P(X)>) + \cdots + (a_nX^n + <P(X)> \\ &= (a_0 + a_1X + \cdots + a_nX^n) + <P(X)> \\ &= P(X) + <P(X)> \\ &= <P(X)> \end{aligned}$$

which is the zero element in $F[X]/<P(X)>$ hence α is indeed a root of $P(X)$. □

Lemma 1.3.7. *Let F be a field and $P(X)$ be an irreducible polynomial of degree $n \in \mathbb{N}$ in $F[X]$, α be a root of $P(X)$ in a field extension of F. Then $S_\alpha := \{Q(X) \in F[X] | Q(\alpha) = 0\}$ is an ideal in $F[X]$, moreover S_α is a principal ideal generated by $P(X)$.*

Proof. The zero polynomial is in S_α hence $S_\alpha \neq \emptyset$. Let $Q_1(X), Q_2(X) \in S_\alpha$ then $Q_1(\alpha) - Q_2(\alpha) = 0 - 0 = 0 \implies Q_1(X) - Q_2(X) \in S_\alpha$, also if $Q(X) \in F[X]$ then $Q(\alpha)Q_1(\alpha) = Q(\alpha)0 = 0 \implies Q(X)Q_1(X) \in S_\alpha$ hence S_α is indeed ideal in $F[X]$. It follows from Lemma 1.2.5 that S_α is a principal ideal, it remains to show that $P(X)$ is a generator of S_α. Let $S_\alpha = <S(X)>$, then $P(X) = A(X)S(X)$ for some $A(X) \in F[X]$, this implies $<P(X)> \subseteq S_\alpha$. By Lemma 1.2.8 we have that $F[X]/<P(X)>$ is a field so by Lemma 1.2.2 we get that $<P(X)>$ is a maximal ideal, hence $S_\alpha = <P(X)>$ since $S_\alpha \neq F[X]$ (as $1 \notin S_\alpha$). □

Definition 1.3.8. *Let E/K be a field extension, an element $\alpha \in E/F$ is said to be algebraic over F if there exists a a non-zero polynomial $P(X) \in F[X]$ such that $P(\alpha) = 0$, otherwise α is said to be transcendental over F.*

Stellenbosch University https://scholar.sun.ac.za

Definition 1.3.9. *Let $P(X)$ be a non-zero polynomial in $F[X]$ then $P(X)$ is said to be monic if the leading coefficient of $P(X)$ is 1.*

Definition 1.3.10. *Let E/K be a field extension and $\alpha \in E$ be algebraic over F, we defined a minimal polynomial of α over F to be a monic polynomial $P(X) \in F[X]$ of minimal degree such $P(\alpha) = 0$. We will denote a minimal polynomial of α over F as $min(\alpha, F)$.*

Remark 1.3.11. *Let $K \subseteq F \subseteq E$ be a tower of fields and $\alpha \in E$ be algebraic over K, then $min(\alpha, F)$ divides $min(\alpha, K)$ in $F[X]$. To see that this is the case let S_α be the ideal generated by $min(\alpha, F)$ in $F[X]$, now $K[X] \subseteq F[X]$ and $min(\alpha, K)(\alpha) = 0$ hence $min(\alpha, K) \in S_\alpha$ so $min(\alpha, K) = A(X)min(\alpha, F)$ for some $A(X) \in F[X]$.*

Lemma 1.3.12. *Let E/F be a field extension and $\alpha \in E$ be algebraic over F, then α has a unique minimal polynomial over F.*

Proof. Let $P(X) \in F[X]$ be a minimal polynomial of α and $n \in \mathbb{N}$ be the degree of $P(X)$. Let $Q(X)$ also be a minimal polynomials of α over F. The degrees of $P(X)$ and $Q(X)$ are both minimal in S_α by the definition of a minimal polynomial, hence they are equal. Now let $A(X) = P(X) - Q(X)$, note that $S(X) = 0$ or $S(X)$ has degree strictly less than the degree of $P(X)$, this is because both $P(X)$ and $Q(X)$ are monic polynomial of same degree. $S(X) = P(\alpha) - Q(\alpha) = 0$ so $S(X) = 0$ otherwise $P(X)$ is not a minimal polynomial of α. $S(X) = 0 \implies Q(X) = P(X)$ proving that the minimal polynomial of α over F is indeed unique. □

Definition 1.3.13. *Let E/F be a field extension and $\alpha \in E$, We define $F[\alpha] = \{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 | a_i \in F, n \in \mathbb{N} \cup \{0\}\}$ to be the ring of polynomials with indeterminate α and coefficients from F.*

Theorem 1.3.14. *Let E/F be a field extension and $\alpha \in E$ be algebraic over F then $F[\alpha]$ is a field.*

Proof. Let $P(X)$ be the minimal polynomial of α over F. $F[\alpha]$ is an integral domain hence it suffices to show that any non-zero element in $F[\alpha]$ has an inverse in $F[\alpha]$. Let $G(\alpha) \in F[\alpha]$ be a non-zero element, then $P(X)$ does not divide $G(X)$ otherwise $G(X) \in S_\alpha$ and $G(\alpha) = 0$ which is a contradiction. Let $D(X) = gcd(P(X), G(X))$, then by the Euclidean algorithm there exists $A(X), B(X) \in F[X]$ such that $D(X) = A(X)P(X) + B(X)G(X)$. Since $P(X)$ being irreducible in $F[X]$ and the degree of $G(X)$ is less than the degree of $P(X)$ it follows that $D(X) = P(X)$ is not possible, hence $D(X) = 1$. $1 = A(X)P(X) + B(X)G(X) \implies 1 = A(\alpha)P(\alpha) + B(\alpha)G(\alpha) = B(\alpha)G(\alpha)$, this implies $G(\alpha)$ has an inverse in $F[\alpha]$ namely $B(\alpha)$, so $F[\alpha]$ is indeed a field.

□

Definition 1.3.15. *Let E/K be a field extension and $\alpha \in E$ be an algebraic element. Let $A(\alpha), B(\alpha) \in F[\alpha]$ with $B(\alpha) \neq 0$, we define the quotient of two polynomials $A(\alpha)/B(\alpha)$ as $A(\alpha)(B(\alpha))^{-1}$ where $B(\alpha)^{-1}$ is the inverse of $B(\alpha)$ in $F[\alpha]$.*

Definition 1.3.16. *Let E/F be a field extension and $\alpha \in E$ be an algebraic element. We define $F(\alpha)$ to be a set of quotients of polynomials in $F[\alpha]$, that is*
$F(\alpha) = \{A(\alpha)/B(\alpha) | A(\alpha), B(\alpha) \in F[\alpha], B(\alpha) \neq 0\}$.

Stellenbosch University https://scholar.sun.ac.za

Lemma 1.3.17. *Let E/F be a field extension and $\alpha \in E$ be algebraic over F, then $F(\alpha)$ is a field. Moreover $F[\alpha] = F(\alpha)$.*

Proof. We will show that $F[\alpha] = F(\alpha)$ which will then imply $F(\alpha)$ is also field. Let $A(\alpha)/B(\alpha) \in F(\alpha)$. $B(\alpha) \in F[\alpha]$ implies $B(\alpha)^{-1} \in F[\alpha]$ since $F[\alpha]$ is a field.
$A(\alpha)/B(\alpha) = A(\alpha)B(\alpha)^{-1} \in F[\alpha]$ since $F[\alpha]$ is closed under multiplication, this then implies $F(\alpha) \subseteq F[\alpha]$. Let $A(\alpha) \in F[\alpha]$ then $A(\alpha) = A(\alpha)/1 \in F(\alpha) \implies F[\alpha] \subseteq F(\alpha)$ hence $F[\alpha] = F(\alpha)$ as desired. □

Lemma 1.3.18. *Let E/F be a field extension and $\alpha \in E$ be algebraic over E, then $F[\alpha]$ is the smallest subfield of E containing F and α.*

Proof. We will show that intersection of all subfields of E containing F and α is $F[\alpha]$. Let K be the intersection of all subfields of E containing F and α, then K is not an empty intersection since $F[\alpha]$ contains both F and α. If L is any subfield of E containing F and α then L is part of the intersection hence $K \subseteq L$ hence $K \subseteq F[\alpha]$. Let $A(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 \in F[\alpha]$ then for any $i \in [0, n]$ $a_i\alpha^i \in K$ since K is closed under multiplication. Also $a_n\alpha^n + a_{n-1} + \cdots + a_1\alpha + a_0 \in K$ since K is closed under addition, hence $F[\alpha] \subseteq K$ this then implies $K = F[\alpha]$. □

Definition 1.3.19. *Let E/F and K/F be field extension, we say the extensions are isomorphism and write $E/F \cong K/F$ if there exist a ring isomorphism $\phi : E \to K$ such that $\phi(f) = f$ for all $f \in F$, such an map is called an F-isomorphism.*

Lemma 1.3.20. *Let E/F be a field extension and $\alpha \in E$ be algebraic over F, then $F(\alpha)$ and $F[X]/<P(X)>$ are F- isomorphic.*

Proof. Let $\phi : F[X] \to F[\alpha]$ be the homomorphism defined sending X to α. Let $G(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 \in F[\alpha]$ then $\phi(a_nX^n + \cdots + a_1X + a_0) = G(\alpha)$ hence ϕ is subjective. To show that $F[X]/<P(X)>$ and $F[\alpha]$ are isomorphic as rings it suffices to show that $ker(\phi) = <P(X)>$, the existence of a ring isomorphism from $F[X]/<P(X)>$ to $F[\alpha]$ follows from the first isomorphism theorem of rings. Let $Q(X) = \sum_{i=0}^{n} a_iX^i \in F[X]$, then $Q(X) \in ker(\phi)$ if and only if $\sum_{i=0}^{n} a_i\alpha^i = 0$, this is equivalent to having $G(X) \in S_\alpha = <P(X)>$. By the first isomorphism of rings we have a ring isomorphism $\overline{\phi}$: $F[X]/<P(X)>$ defined by $\overline{\phi}(Q(X) + <P(X)>) = Q(\alpha)$. It follows from Lemma 1.3.6 that $\overline{\phi}$ is an F-isomorphism. □

Lemma 1.3.21. *Let E/F be a field extension and $\alpha \in E$ be algebraic over F. If the minimal polynomial of α over F has degree n then $F(\alpha) = \{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 | b_i \in F, i \in [0, n-1]\}$, moreover $[F(\alpha) : F] = n$.*

Proof. Let $P(X)$ be the minimal polynomial of α over F. It's clear from the definition of $F[\alpha]$ that $\{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 | b_i \in F, i \in [0, n-1]\} \subseteq F[\alpha]$, so we need to show the reverse inclusion. Let $G(\alpha) \in F[\alpha]$, by the division algorithm there exists $Q(X)$ and $R(X)$ in $F[X]$ such that $G(X) = Q(X)P(X) + R(X)$ where the degree of $R(X)$ is less than the degree of $P(X)$ or $R(X) = 0$. Let $R(X) = a_rX^r + a_{r-1}X^{r-1} + \ldots a_0$ then $r < n$ and so $R(\alpha) \in \{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 | b_i \in F, i \in [0, n-1]\} \subseteq F[\alpha]$, now $G(\alpha) = Q(\alpha)P(\alpha) + R(\alpha) = R(\alpha) \in \{b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 | b_i \in F, i \in [0, n-1]\} \subseteq F[\alpha]$ as desired.

We have shown that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ spans $F(\alpha)$ so to show that $[F(\alpha) : F] = n$ it suffices to show $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly independent. We argue by contradiction,

Stellenbosch University https://scholar.sun.ac.za

suppose there exists $b_0, b_1, \ldots, b_{n-1} \in F$ not all zero such that $b_0+b_1\alpha+b_2\alpha^2+\cdots+\alpha^{n-1} = 0$ then α is a root $S(X) = b_{n-1}X^{n-1} + \cdots + b_1X + b_0$, now let i be the largest integer such that $b_i \neq 0$ then $b_i^{-1}S(X)$ is a monic polynomial of degree less than n and has α as a root, this contradicts the fact that $P(X)$ is the minimal polynomial of α over F. So indeed $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly independent hence is a basis of $F(\alpha)/F$ proving that $[F(\alpha) : F] = n$. □

Definition 1.3.22. *Let E/F be a field extension, then E/F is said to be algebraic if every $\alpha \in E$ is algebraic over F.*

Lemma 1.3.23. *Every finite field extension E/F is algebraic.*

Proof. Let $n = [E : F]$, now for any $\alpha \in E$ we have that $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is not linearly independent over F. So there exists $a_0, a_1, \ldots, a_n \in F$ not all zero such that $a_n\alpha^n+\cdots+a_2\alpha^2+a_1\alpha+a_0 = 0$, this implies α is root of $P(X) = a_nX^n+\cdots+a_1X+a_0 \in F[X]$, hence α is algebraic over F. □

1.4 Splitting Fields

Our goal in this section is to prove that for any field F and polynomial $P(X) \in F[X]$, there exist a unique field extension of E/F (up to isomorphism) such that L contains all the roots of $P(X)$. We will then use this idea to prove that all finite fields of same order are isomorphic.

Definition 1.4.1. *Let F be a field and $P(X) \in F[X]$, $P(X)$ is said to split in a field E if there exists $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ and $c \in F$ such that $P(X) = c(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$. E is said to be a splitting field of $P(X)$ over F if $P(X)$ splits in E and $P(X)$ does not split in any proper subfield of E containing F.*

Remark 1.4.2. *Let E/F be a field and $P(X)$ be a non-constant polynomial in $F[X]$, if $P(X) = (X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ then $F(\alpha_1, \ldots, \alpha_n)$ is a splitting field of $P(X)$*

Lemma 1.4.3. *Let F be a field and $P(X)$ be a non-constant polynomial in $F[X]$, then $P(X)$ has a splitting field.*

Proof. Let n be the degree of $P(X)$, if $n = 1$ then $P(X) = aX + b$ for some $a, b \in F$ with $a \neq 0$, then $\alpha := -\frac{b}{a}$ is a root of $P(X)$, i,e $P(X) = a(X - \alpha)$ so F is a splitting field of $P(X)$. We proceed by induction on n, suppose the statement holds true for all polynomials of degree less than n. Suppose $P(X)$ is irreducible of F, then by Lemma 1.3.6 we have $E := F[X]/<P(X)>$ as an extension of F having $\alpha_0 := X + <P(X)>$ as a root of $P(X)$ by Lemma 1.3.6, so $P(X) = (X - \alpha)G(X)$ for some $G(X) \in E[X]$. $G(X)$ has degree $n - 1$ hence by the inductive hypothesis $G(X)$ has a splitting field K. Let $G(X) = c(X - \alpha_1)(X - \alpha_1)\ldots(X - \alpha_{n-1})$ for some $c \in F$ and $\alpha_i \in K$ for $i \in [1, n-1]$, it follows that $P(X)$ splits in $K' := F(\alpha_0, \alpha_1, \ldots, \alpha_n)$ as $P(X) = c(X - \alpha_0)(X - \alpha_1)(X - \alpha_1)\ldots(X - \alpha_{n-1})$ and K' is a splitting field of $P(X)$. Now suppose $P(X) = A(X)B(X)$ where $A(X)$ and $B(X)$ both have degrees greater than 1, then by the inductive hypothesis $A(X) = c(X - \beta_1)(X - \beta_2)\ldots(X - \beta_m)$ in a splitting field of $A(X)$ and $B(X) = c'(X - \beta'_1)(X - \beta'_2)\ldots(X - \beta'_m)$ in a splitting field of $B(X)$, it follows that $P(X) = cc'(X - \beta_1)(X - \beta_2)\ldots(X - \beta_m)(X - \beta'_1)(X - \beta'_2)\ldots(X -$

Stellenbosch University https://scholar.sun.ac.za

$\beta'_s)$ in $F(\beta_1,\ldots,\beta_m,\beta'_1,\ldots,\beta'_s)$ and $F(\beta_1,\ldots,\beta_m,\beta'_1,\ldots,\beta'_s)$ is indeed a splitting field of $P(X)$. □

Lemma 1.4.4. *Let $\phi\colon E\to K$ be a field isomorphism, and $\phi^*: E[X]\to K[X]$ defined by $\phi^*(\sum_{i=0}^n a_iX^i)=\sum_{i=0}^n\phi(a_i)X^i$ be the corresponding isomorphism of rings. Let $P(X)$ is irreducible over F and $P^*(X):=\phi^*(P(X))$, if α is a root of $P(X)$ in a field extension of E and α' is a root of $P^*(X)$ in a field extension of K, then there exists a isomorphism $\overline{\phi}: E(\alpha)\to K(\alpha')$ extending ϕ.*

Proof. Let $\tau\colon E[X]\to K[X]/<P^*(X)>$ be a map defined by $\tau(G(X))=G(X)^*+<P^*(X)>$, where $G(X)^*=\phi^*(G(X))$. Let $H(X),G(X)\in F[X]$ then $\tau(H(X)+G(X))=(H(X)+G(X))^*+<P^*(X)>=H(X)^*+G(X)^*+<P^*(X)>=(H(X)^*+<P^*(X)>)+(G(X)^*+<P^*(X)>)=\tau(H(X))+\tau(G(X))$, also $\tau(H(X)G(X))=(H(X)G(X))^*+<P^*(X)>=H(X)^*G(X)^*+<P^*(X)>=(H(X)^*+<P^*(X)>)(G^*(X)+<P^*(X)>)=\tau(H(X))\tau(G(X))$ hence τ is ring homomorphism. $\tau(H(X))=0\iff H(X)^*+<P^*(X)>=<P^*(X)>\iff P(X)^*|H(X)^*\iff P(X)|H(X)$ so $Ker(\tau)=<P(X)>$ and by first homomorphism theorem of rings we have a ring isomorphism from $\overline{\phi}: E[X]/<P(X)>\to K[X]/<P(X)^*>$ defined by $\overline{\phi}(S(X)+<P(X)>)=S^*(X)+<P^*(X)>$. By Lemma 1.3.20 there exists a E-isomorphism $\psi_E: E(\alpha)\to E[X]/<P(X)>$ and and a K-isomorphism $\psi_K: K(\alpha')\to K[X]/<P^*(X)>$ hence we have a ring isomorphism $\psi_K^{-1}\circ\overline{\phi}\circ\psi_E$ from $E(\alpha)$ to $K(\alpha')$, moreover if $e\in E$ then $\psi_K^{-1}\circ\overline{\phi}\circ\psi_E(e)=\psi_K^{-1}\circ\overline{\phi}(e+<P(X)>)=\psi_K^{-1}(\phi(e)+<P^*(X)>)=\phi(e)$ hence the composition map extends ϕ as desired. □

Lemma 1.4.5. *Let $\phi\colon F\to F'$ be a field isomorphism, $P(X)\in F[X]$ and $P^*(X)\in F'[X]$ be the polynomial corresponding to $P(X)$ via the extension of ϕ from $F[X]$ to $F'[X]$. Let E be a splitting field of $P(X)$ over F and E' be a splitting field of $S^*(X)$ over F' then there exists a ring isomorphism $\overline{\phi}$ from E to E' extending ϕ.*

Proof. If $[E:F]=1$ then $P(X)=c(X-\alpha_1)\ldots(X-\alpha_m)$ where $c\in F$ and $\alpha_i\in F$ for each $i\in[1,m]$. It follows that $P^*(X)=\phi(c)(X-\phi(\alpha_1))\ldots(X-\phi(\alpha_m))$ hence $E'=F$ so taking $\overline{\phi}=\phi$ completes the proof. We proceed by induction on $[E:F]$. Suppose the statement holds true for all field extensions of degree less than $n:=[E:F]$. Pick $\alpha\in E$ a root of $P(X)$ such that $\alpha\notin F$, let $S(X)$ be the minimal polynomial of α over F. By Lemma 1.3.7 we have that $S(X)$ divides $P(X)$ in $F[X]$. Let $S^*(X)\in F'[X]$ be the polynomial corresponding to $S(X)$, so $S^*(X)$ divides $P^*(X)$ hence $S^*(X)$ has a root in $\alpha'\in E'$. Note that E is a splitting field of $P(X)$ over $F(\alpha)$ and E' is a splitting field of $P^*(X)$ over $F'(\alpha')$ hence by Lemma 1.4.4 there exists a ring isomorphism $\phi_1: F(\alpha)\to F'(\alpha)$ extending ϕ. Since $[F(\alpha):F]>1$ it follows that $[E:F(\alpha)]<[E:F]$ hence by the inductive hypothesis there exists a ring isomorphism $\overline{\phi}: E\to E'$ extending ϕ_1, so $\overline{\phi}$ extends ϕ as desired.

□

Lemma 1.4.6. *Let F be a finite field, then F is an extension of $\mathbb{Z}_p$ for some prime number p.*

Proof. Let $p:=char(F)$ then $p\neq 0$ since F is fnite. Also p is a prime number and $|F|=p^n$ for some $n\in\mathbb{N}$. Let $\phi\colon\mathbb{Z}\to F$ be defined by $\phi(a)=a.1=1_F+1_F+\cdots+1_F$ (a times). We will show that ϕ is a ring homomorphism. For any $a,b\in\mathbb{Z}$ we have $\phi(a+b)=(a+b).1_F=a.1_F+b.1_F=\phi(a)+\phi(b)$ and $\phi(ab)=(ab).1_F=(a.1_F)(b.1_F)=$

Stellenbosch University https://scholar.sun.ac.za

$\phi(a)\phi(b)$ so ϕ is indeed a ring homomorphism. Note that $\phi(a) = 0 \iff a.1_F = 0_F \iff p|a \iff a \in <p>$ hence $ker(\phi) = <p>$. By first ring homomorphism theorem of rings we have $\mathbb{Z}/<p> = \mathbb{Z}_p \cong Im(\phi) \subseteq F$ hence F is indeed a field extension of $\mathbb{Z}_p$ up to isomorphism. □

Definition 1.4.7. *Let F be a field and $P(X) = \sum_{i=0}^{n} a_i X^i \in F[X]$ we define the derivative of $P(X)$ as $P'(X) = \sum_{i=1}^{n} i a_i X^{i-1} \in F[X]$.*

Definition 1.4.8. *Let F be a field , $\alpha \in F$ be a root of $P(X) \in F[X]$ then α has multiplicity $m \in \mathbb{N}$ in $P(X)$ if $(X-\alpha)^m | P(X)$ and $(X-\alpha)^{m+1} \nmid P(X)$.*

Lemma 1.4.9. *Let F be a field and $P(X) \in F[X]$ then every root of $P(X)$ has multiplicity 1 in the splitting field of $P(X)$ if and only if $1 = gcd(P(X), P'(X))$.*

Proof. Let E be the splitting field of $P(X)$.

$\implies$ Suppose every root of $P(X)$ has multiplicity 1 in E. Let $\alpha \in E$ be a root of $P(X)$ then we have $P(X) = (X-\alpha)G(X)$ where α is not a root of $G(X) \in E[X]$. Hence $P'(X) = G(X) + (X-\alpha)G'(X)$, it follows that $P'(\alpha) = G(\alpha) \neq 0$. $P(X)$ and $P'(X)$ have no common root E hence have no non-trivial common divisor in $F[X]$ i.e they are co-prime so $1 = GCD(P(X), P'(X))$.

$\impliedby$ Suppose $1 = gcd(P(X), P'(X))$, we argue by contradiction that every root of $P(X)$ has multiplicity 1 in E. Suppose α is a root of $P(X)$ with multiplicity $m > 1$, then $P(X) = (X-\alpha)^2 Q(X)$ for some $Q(X) \in E[X]$ then $P'(X) = 2(X-\alpha)Q(X) + (X-\alpha)^2 Q'(X)$ and so $P'(\alpha) = 0$, this implies that the minimal polynomial of α over F divides both $P(X)$ and $P'(X)$ contradicting that $1 = gcd(P(X), P'(X))$. □

Theorem 1.4.10. *Let E and E' be finite fields of same order, then $E/\mathbb{Z}_p \cong E'/\mathbb{Z}_p$ for some prime number p.*

Proof. We have $|E| = |E'| = p^n$ for some prime number p and $n \in \mathbb{N}$. By Lemma 1.4.6 we have that E and E' are extensions of $\mathbb{Z}_p$. To show $E/\mathbb{Z}_p \cong E'/\mathbb{Z}_p$ it suffices to show that E and E' are both splitting fields of $P(X) = X^{p^n} - X \in \mathbb{Z}_p[X]$ by Lemma 1.4.5. Since E and E' are finite we have that $E^\times$ and $(E')^\times$ are cyclic groups of order $p^n - 1$. Hence for any non-zero $\alpha \in E$ we have $\alpha^{p^n-1} = 1$ so $\alpha^{p^n} - \alpha = 0$ and $0^{p^n} - 0 = 0$. It follows that $P(X)$ splits in E, to show that E is a splitting field of $P(X)$ over $\mathbb{Z}_p$ it suffices to show any any root of α of $P(X)$ in E has multiplicity 1, as this imply the splitting field of $P(X)$ must have atleast p^n elements. $P'(X) = p^n X^{p^n-1} - 1 = -1$ hence $gcd(P(X), P'(X)) = 1$ this implies any root of $P(X)$ in E has multiplicity 1, so E is indeed a splitting field of $P(X)$ over $\mathbb{Z}_p$. Similary E' is splitting field of $P(X)$ over $\mathbb{Z}_p$ hence $E/\mathbb{Z}_p \cong E'/\mathbb{Z}_p$ by Lemma 1.4.5. □

1.5 Separable Field Extensions

In this section we explore some basic properties of separable field extension.

Definition 1.5.1. *Let E/F be a field extension and $\alpha \in E$ be algebraic over F, we say α is an algebraic element of degree n if the minimal polynomial of α over F has degree n.*

Stellenbosch University https://scholar.sun.ac.za

Definition 1.5.2. *Let F be a field and $P(X) \in F[X]$ then $P(X)$ is said to be separable over F if $P(X)$ has distinct roots in the splitting field of $P(X)$ over F, that is all roots of $P(X)$ have multiplicity 1. If $P(X)$ is not separable then $P(X)$ is said to be inseparable.*

Remark 1.5.3. *A divisor of a separable polynomial is separable.*

Definition 1.5.4. *Let E/F be a field extension and $\alpha \in E$ be algebraic, then α is said to be separable if the minimal polynomial of α over F is separable.*

Definition 1.5.5. *Let E/F be an algebraic field extension, then E is said to be a separable extension of F if for any $\alpha \in E$ the minimal polynomial of α over F is separable.*

Lemma 1.5.6. *Let E/F be an algebraic field extension, if $char(F) = 0$ then E/F is separable.*

Proof. Let $\alpha \in E$ be non-zero and $P(X)$ be the minimal polynomial of α over F. Let n be the degree of $P(X)$. If $n = 1$ then $P(X)$ is separable as $P(X)$ has exactly one root in the splitting field of $P(X)$. Now suppose $n > 1$. Let $D(X) = gcd(P(X), P'(X))$, then by the irreducibility of $P(X)$ over F we have that $D(X) = 1$ or $D(X) = P(X)$. Note $P(X) \nmid P'(X)$ as $P'(X)$ is a non-zero polynomial of degree $n - 1$ hence $D(X) \neq P(X)$, it follows that $D(X) = 1$ and so $P(X)$ is separable by Lemma 1.4.9. Since α was an arbitrary algebraic element of E, it follows that E/F is separable. □

Definition 1.5.7. *A field extension E/F is said to be a simple extension if there is an element $\alpha \in E$ such that $E = F(\alpha)$. If such α exists then α is said to be a primitive element of E over K.*

Lemma 1.5.8. *Let E/F and K/F be finite isomorphic field extensions with isomorphism given by ϕ. Then if $\alpha \in E$ is primitive element over F then $\phi(\alpha)$ is also a primitive element of K over F.*

Proof. To show that $\phi(\alpha)$ is a primitive element in K we will show that any element in K can be written as a linear combination of powers of $\phi(\alpha)$ with coefficients in F. Let $k \in K$ then $k = \phi(\beta)$ for some $\beta \in E$ (ϕ is subjective). Now $k = a_{l-1}\alpha^{l-1} + a_{l-2}e^{l-2} + \cdots + a_1\alpha + a_0$ where $a_i \in F$ for each $i \in [0, l-1]$ and l is the degree of $min(\alpha, F)$. It follows that $k = \phi(\beta) = a_{l-1}\phi(\alpha)^{l-1} + a_{l-2}\phi(\alpha)^{l-2} + \cdots + a_1\phi(\alpha) + a_0 \in F(\phi(\beta))$ hence $K = F(\phi(\beta))$ as desired.

□

1.6 Galois Theory

Definition 1.6.1. *Let L/F be a field extension, Then $Aut_F(L)$ is defined to be the set of automorphism of L such that for each $\sigma \in Aut_F(L)$ we have $\sigma(f) = f$ for all $f \in F$.*

Remark 1.6.2.

1. *Let L_1, L_2 and L_3 be rings such that $\phi : L_1 \to L_2$ and $\tau : L_2 \to L_3$ are ring homomorphisms then $\tau \circ \phi$ is again a ring homomorphism from L_1 to L_3.*
2. *Let L/F be a field extension. Then $Aut_F(L)$ is a group under composition.*

Lemma 1.6.3. *Let L/F be a finite field extension and fix $\phi \in Aut_F(L)$. If $P(X) \in F[X]$ and $\beta \in L$ then $P(\phi(\beta)) = \phi(P(\beta))$*

Stellenbosch University https://scholar.sun.ac.za

Proof. Suppose $P(X) = \sum_{i=0}^{n} a_i X^i$, then

$$\phi(P(\beta)) = \phi\big(\sum_{i=0}^{n} a_i\beta^i\big) = \sum_{i=0}^{n} \phi(a_i\beta^i) = \sum_{i=0}^{n} a_i\phi(\beta)^i = P(\phi(\beta))$$

□

Lemma 1.6.4. *Let L/F be a field extension and $\phi \in Aut_F(L)$. Then*

1. *If $P(X) \in F[X]$ has $\alpha \in L$ as a root, then $\phi(\alpha)$ is a root on $P(X)$.*
2. *if $L = F(\alpha)$ then ϕ is uniquely determined by $\phi(\alpha)$.*

Proof.

1. By Lemma 1.6.3 we have that $P(\phi(\alpha)) = \phi(P(\alpha)) = \phi(0) = 0$.
2. Let $n = deg(min(\alpha, F))$ and $\beta \in L$, then there exist $a_0, a_2, \ldots, a_{n-1}$ such that $\beta = \sum_{i=0}^{n} a_i\alpha^n$, it follows that $\phi(\beta) = \sum_{i=0}^{n} \phi(\alpha)^n$. So indeed $\phi(\beta)$ is knwown as soon as $\phi(\alpha)$ is known, since is β an arbitrary element in L, the results holds true for any element in L.

□

Lemma 1.6.5. *Let L/F be a finite field extension. Then the Galois group $Aut_F(L)$ is finite.*

Proof. Let $L = F(\alpha_1, \alpha_2, \ldots \alpha_n)$. If $\phi \in Aut_F(L)$ then ϕ is uniquely determined by the values $\phi(\alpha_1), \phi(\alpha_2), \ldots, \phi(\alpha_n)$. If $f_i \in F[X]$ is the minimal polynomial of α_i then by Lemma 1.6.4, 1., $\phi(\alpha_i)$ has at most $deg(f_i)$ possible values hence $|Gal(L/F)| \leq deg(f_1) \ldots deg(f_n)$. □

Lemma 1.6.6. *Let L/F and E/F be F-isomorphic field extension, then $Aut_F(L) \cong Aut_F(E)$.*

Proof. Let $\varphi : L \to E$ be a F-isomorphism, we will show the map $\tau : Aut_F(L) \to Aut_F(E)$ defined by $\tau(\phi) = \varphi \circ \phi \circ \varphi^{-1}$ is a group isomorphism. Let $\phi_1, \phi_2 \in Aut_F(L)$ then $\tau(\phi_1 \circ \phi_2) = \varphi \circ (\phi_1 \circ \phi_2) \circ \varphi^{-1} = \varphi \circ (\phi_1 \circ (\varphi^{-1} \circ \varphi) \circ \phi_2) \circ \varphi^{-1} = (\varphi \circ \phi_1 \circ \varphi^{-1}) \circ (\varphi \circ \phi_2 \circ \varphi^{-1}) = \tau(\phi_1) \circ \tau(\phi_2)$ hence τ is a group homomorphism. It remains to show that τ is injective and surjective. Suppose $\tau(\phi_1) = \tau(\phi_2)$ that is $\tau(\phi_1)(x) = \tau(\phi_2)(x)$ for all $x \in E \implies \varphi(\phi_1(\varphi^{-1}(x))) = \varphi(\phi_2(\varphi^{-1}(x))) \implies \phi_1(\varphi^{-1}(x)) = \phi_2(\varphi^{-1}(x))$ so $\phi_2^{-1}(\phi_1(\varphi^{-1}(x))) = \varphi^{-1}(x)$ and $\phi_1^{-1}(\phi_2(\varphi^{-1}(x))) = \varphi^{-1}(x)$. Since φ is an isomorphism it follows that $\phi_2 \circ \phi_1 = Id_L$ and $\phi_1 \circ \phi_1 = Id_L$, hence $\phi_1 = \phi_2$ so τ is indeed injective. Let $\phi \in Aut_F(E)$ then $\tau(\varphi^{-1} \circ \phi \circ \varphi) = \varphi \circ (\varphi^{-1} \circ \phi \circ \varphi) \circ \varphi^{-1} = \phi$ so τ is surjective hence a group isomorphism. □

Definition 1.6.7. *Let F be a field and $P(X) \in F[X]$, the automorphism group of $P(X)$ over F is defined to be $Aut_F(L)$ where L is the splitting of $P(X)$ over F.*

Note that this definition is well defined since the splitting field is unique upt isomorphism and from the result above we have that $Aut_F(L) \cong Aut_F(E)$ if $L/F \cong E/F$.

Lemma 1.6.8. *Let F be a field and $P(X) \in F[X]$ be separable, then the automorphism group of $P(X)$ over F has order $|Aut_F(L)| = [L : F]$, where L is the splitting field of $P(X)$ over F.*

Stellenbosch University https://scholar.sun.ac.za

Proof. Let L be the splitting field of $P(X)$, if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of $P(X)$ in L then $L = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, hence L is a finite extension. Note that α_i is separable, hence by the Primitive Element Theorem there exists $\beta \in L$ such that $L = F(\beta)$. Let $H(X) \in F[X]$ be the minimal polynomial of β over F, this implies $m := deg(H(X)) = [L : F]$. We now want to show that $Aut_F(L)$ has m elements, note that by Lemma 1.6.4 has at most $deg(H(X)) = m$ as each element of $\sigma \in Aut_F(L)$ is uniquely determined by what $\sigma(\beta)$ and there are m possible values of $\sigma(m)$ by Lemma 1.6.4.

$H(X)$ being separable implies $H(X)$ has m distinct roots in L say $\beta_1, \beta_2, \ldots, \beta_m$, fix one of the roots say β_k then for each β_i where $i \neq k$ there exists a unique automorphism ϕ_i in L fixing F such that $\phi(\beta_k) = \beta_i$ by Lemma 1.4.4 , $\phi_i \in Aut_F(L)$ we now have $m-1$ elements in $Aut_M(L)$, adding the identity map in L we have $|Aut_F(L)| = [L : F] = m$ as desired. □

Lemma 1.6.9. *Let L/F be a field extension, H be a subgroup of $Aut_F(L)$ then $L_H = \{\alpha \in L | \phi(\alpha) = \alpha \ \forall \phi \in H\}$ is a subfield of L (known as a fixed field of H).*

Proof. For any $\phi \in H$ we have $\phi(1) = 1$ and $\phi(0) = 0$ hence $0, 1 \in L_H \implies L_H \neq \emptyset$. Let $\alpha, \beta \in L_H$ then $\phi(\alpha - \beta) = \phi(\alpha) - \phi(\beta) = \alpha - \beta \implies L_H$ is a subgroup of L. It suffices to show that $L_H^\times$ is a group under multiplication, this is because associativity and distributive laws follows from the fact L is a field. Suppose both $\alpha, \beta \in L_H$ are not zero, then β^{-1} exist and $\phi(\alpha\beta^{-1}) = \phi(\alpha)(\phi(\beta))^{-1} = \alpha\beta^{-1}$. Therefore $L_H^\times$ is indeed a group under multiplication, which concludes the proof. □

Definition 1.6.10. *Let L/F be a field extension, then L/F is said to be a Galois extension if F is the fixed field of $Aut_F(L)$. In this case, $Aut_F(L)$ is called the Galois group and denoted by $Gal(L/F)$.*

Theorem 1.6.11. *Let L/F be a finite field extension, then the following are equivalent:*

1. *L is a splitting field of a separable polynomial in $F[X]$.*
2. *F is a fixed field of $Aut_F(L)$.*
3. *L/F is a normal separable extension.*

Proof. (1) $\implies$ (2) Let $P(X) \in F[X]$ be such that L is the splitting field of $P(X)$. Let K be the fixed field of $Aut_F(L)$ then $F \subseteq K \subseteq L$. Note that $P(X) \in K[x]$ and L is also the splitting field of $P(X)$ over K hence $|Aut_F(L)| = [L : F]$, $|Aut_K(L)| = [L : K]$ and $Aut_K(L) \subseteq Aut_F(L)$ since every automorphism of L fixing K also F. If $\phi \in Aut_F(L)$ then ϕ is identity on K (by definition of K) hence $Aut_F(L) \subseteq Aut_K(L) \implies Aut_F(L) = Aut_K(L)$ proving that $[L : F] = [L : K]$ but $[L : F] = [L : K][K : F]$ hence $[K : F] = 1$ so $K = F$ as desired.
(2) $\implies$ (3) We start by showing that L/F is a normal extension, let $\alpha \in L$ be algebraic over F. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct elements in L obtained by applying elements of $Aut_F(L)$ on α and $H(X) = \prod_{i=1}^{n}(X - \alpha_i)$. We claim that $h(x)$ is an element of $F[X]$ and $h(x)$ is the minimal polynomial of α. For any $\phi \in Aut_F(L)$ we have that $\phi(\alpha_i) = \alpha_j$ for some $1 \leq j \leq n$ by Lemma 1.6.4, since ϕ injective we have that ϕ permutes $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Hence we have $\phi(H(X)) = \prod_{i=1}^{n}(X - \phi(\alpha_i))$, proving that coefficients of

Stellenbosch University https://scholar.sun.ac.za

$H(X)$ are fixed by ϕ, that is coefficients of $H(X)$ are fixed by any element of $Aut_F(L)$ since ϕ was chosen arbitrarily. Hence follows that $H(X) \in F[X]$ Let $G(X)$ be the minimal polynomial of α over F, then by $G(X)|H(X)$. Now $H(X)$ splits in L so $G(X)$ also splits in L, it follows that L/F is normal and separable.
(3) $\implies$ (1) Let $L = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be normal and separable, then each $min(\alpha_i, F)$ is separable. Let $Q_1(x), \ldots, Q_e(X)$ be distinct elements in $\{min(\alpha_i, F)|i \in [1, n]\}$ and $Q(X) = \prod_{i=1}^{r} Q_i(X)$. We claim that $Q(X)$ is separable and L is the splitting field of $Q(X)$. Since L/F is normal each $Q_i(X)$ splits into linear factors in $L[X]$ so does $Q(X)$. We argue by contradiction that $Q(X)$ is separable, suppose $Q(X) = (X-\alpha)^2 S(X)$ for some $\alpha \in L$ and $S(X) \in L[X]$ then either $(X-\alpha)^2|Q_i(X)$ for some $i \in [1, r]$ or there exists $i \neq j$ such that $X-\alpha|Q_i(x)$ and $X-\alpha|Q_j(X)$, the first case is impossible as each $Q_i(X)$ is separable. Assuming the second case then we have $min(\alpha, F)|Q_i(x)$ but both $min(\alpha, F)$ and $Q_i(x)$ are monic and irreducible over F hence $min(\alpha, F) = Q_i(X)$ using similar argument we conclude similarly $Q_j(X) = min(\alpha, F) = Q_i(x)$ contradicting the choice of $Q_i(X)$'s hence $Q(X)$ is separable. Let $K = F(A)$ where A is the set of all roots of $Q(X)$, note that $F, A \subseteq L$ hence $K \subseteq L$, again $\alpha_1, \ldots, \alpha_n \subset A$ hence $L = F(\alpha_1, \ldots, \alpha_n) \subseteq K$ proving that $K = L$, so L is the splitting field of $Q(X)$ as desired.

□

Lemma 1.6.12. *Let L/F be a finite field extension, then*

1. *$|Aut_F(L)|$ divides $[L : F]$.*
2. *L/F is a Galois extension if and only if $|Gal(L/F)| = [L : F]$.*

Proof. 1. Let K be a fixed field of $Aut_F(L)$. Then L/K, then $[L : K] = |Aut_F(L)|$. Note that $[L : F] = [L : K][K : F] = |Aut_F(L)|[K : F]$ so indeed $|Aut_F(L)|$ divides $[L : F]$.

2. $\implies$ If L/F is a Galois extension then L is a splitting field of a separable so $|Gal(L/F)| = [L : F]$ by Lemma 1.6.8.
$\impliedby$ Let $|Gal(L/F)| = [L : F]$ and K be the fixed field of $Gal(L/F)$. If $\phi \in Gal(L/K)$ then ϕ fixes K hence ϕ fixes $F \subseteq K \implies Gal(L/K) \subseteq Gal(L/F)$, again if $\phi \in Gal(L/F)$ then ϕ fixes all elements of K (by definition of K) hence $Gal(L/F) \subseteq Gal(L/K) \implies Gal(L/F) = Gal(L/K)$. $[L : F] = |Gal(L/F)| = |Gal(L/K)| = [L : K] \implies K = F$ so L/F is a Galois extension.

□

Theorem 1.6.13. *Let F be a field and $f(x) \in F[X]$ such that $n = deg(P(X))$ then the Galois group of $P(X)$ is isomorphic to a subgroup of S_n.*

Proof. Let $X = \{\alpha_1, \ldots, \alpha_n\}$ be the set of all roots $P(X)$ in the splitting field of $P(X)$. If $\phi \in Gal(L/F)$ by Lemma 1.6.4 we have that $\phi|_X$ is a permutation of X. Let $\tau : Gal(L/F) \to S_x$ be define by $\tau(\phi)) = \phi|_X$, to show that τ is a group homomorphism let $\phi, \sigma \in Gal(L/F)$ note that $\tau(\phi\sigma)$ and $\tau(\phi)\tau(\sigma)$ are both permutations on X hence they are equal if they agree on each $\alpha \in X$. $\tau(\phi\sigma) : \alpha \to \phi(\tau(\alpha))$ and $\tau(\phi)\tau(\sigma) : \alpha \to \phi(\sigma(\alpha))$ so τ is indeed a group homomorphism. It then remains to show that τ is injective, if $\tau(\phi) = \tau(\sigma)$ then ϕ and σ agree on every element on X and by Lemma 1.6.4 we have $\phi = \sigma$, this implies the image of τ is a subgroup of $S_X \cong S_n$ as desired. □

Stellenbosch University https://scholar.sun.ac.za

Chapter 2

Quadratic Field Extensions

In this chapter we classify quadratic field extensions up to isomorphism. The classification of quadratic field extensions is complete and well-known, we couldn't find literature containing the results we present so we provide our version of the classification of quadratic field extensions over any field.

Definition 2.0.1. *Let L/F be a field extension, then L/F is said to be a quadratic extension if there exist a primitive element $\alpha \in L$ with a minimal polynomial of degree 2.*

2.1 Quadratic Field Extension Over Characteristic Not 2

In this section we classify quadratic field extension when base field has characteristic not 2. We begin by showing that one can always find a primitive element whose minimal polynomial can be represented with one parameter.

Lemma 2.1.1. *Let E/F be a quadratic field extension such that $char(F) \neq 2$ then $E \cong F[X]/<X^2 - d>$ for some $d \in F$*

Proof. Let $\beta \in E$ be any primitive element, $min(\beta, F) = X^2 + bX + c$ for some $b, c \in F$ $\beta^2 + b\beta + c = 0 \implies (\beta + \frac{b}{2})^2 - (b/2)^2 + c = 0$, we claim that $\beta + b/2$ is such a primitive element. It's clear that $\beta + \frac{b}{2} \notin F$ otherwise we have $\beta \in F$. Note that $\beta + \frac{b}{2}$ is a root of $X^2 - d$ where $d = (b/2)^2 - c \in F$, so $\beta + \frac{b}{2}$ indeed satisfies the condition we need. □

Theorem 2.1.2. *Let F be a field such that $char(F) \neq 2$, If E/F and K/F are quadratic field extensions with $\alpha \in E$ and $\beta \in K$ such that $min(\alpha, F) = X^2 - d$ and $min(\beta, F) = X^2 - d'$ then E and K are F-isomorphic if and only if $d' = a^2 d$ for some $a \in F$.*

Proof. $\implies$
Let $\phi : E \to K$ be a F-isomorphism, then $\alpha' := \phi(\alpha) \in K$ is a primitive element of K/F with minimal polynomial $X^2 - d$. β is a primitive element in K hence there exist $a, b \in F$ such that $\alpha' = a\beta + b$. Note that $a \neq 0$ otherwise we have $\alpha' \in F$ contradicting that α' is a primitive element over F. We now have $\frac{\alpha' - b}{a} = \beta$ so $(\frac{\alpha' - b}{a})^2 - d' = 0$ hence $(\alpha')^2 - 2b\alpha' + b^2 - a^2 d' = 0$, by the uniqueness of minimal polynomial we have that $b = 0$ and $d = a^2 d'$ as desired.

$\impliedby$
We know that E and $F[X]/<X^2 - d>$ are F-isomorphic, it then suffices to show that K

Stellenbosch University https://scholar.sun.ac.za

is also F-isomorphic to $F[X]/<X^2-d>$. We will show this by showing that K has a primitive element α' such that $min(\alpha', F) = X^2 - d$. Note that $(\frac{\beta}{a})^2 - d = \frac{d'}{a^2} - \frac{d'}{a^2} = 0$ so indeed $K \cong F[X]/<X^2-d> \cong E$ and this conlcudes the proof. □

Definition 2.1.3. *Let F be a field, a non-zero element $\alpha \in F$ is said to be a quadratic residue in F if there exists $\beta \in F$ such that $\alpha = \beta^2$.*

Remark 2.1.4. *Let F be a field and $(F^\times)^2$ be a set of all quadratic residues in F, then $(F^\times)^2$ is a subgroup of $F^\times$*

Lemma 2.1.5. *Let F be a field and S be a set of all quadratic extensions of F, and $\sim_{iso}$ be a relation between elements in S define by $E_1/F \sim_{iso} E_2/F$ if and only if E_1 and E_2 are F-isomorphic then $\sim_{iso}$ is an equivalence relation.*

Proof. $E_1 \sim_{iso} E_1$ with the identity map on E_1 being a F-isomorphism, so $\sim_{iso}$ is reflexive. If $E_1 \sim_{iso} E_2$ with an F-isomorphism $\phi : E_{\to} E_2$ then $E_2 \sim_{iso} E_2$ with $\phi^{-1} : E_2 \to E_1$ being a F-isomorphism, so $\sim_{iso}$ is symmetric. Let $E_1 \sim_{iso} E_2$ with $\psi_1 : E_1 \to E_2$ and $E_2 \sim_{iso} E_3$ with $\psi_2 : E_2 \to E_3$ being an F-isomorphism then $E_1 \sim_{iso} E_3$ via $\psi_2 \circ \psi_1$ so $\sim_{iso}$ is transitive proving that $\sim_{iso}$ is an equivalence relation. □

Theorem 2.1.6. *Let F be a field such that $char(F) \neq 2$, S be a set of quadratic extensions of F. Then there exists a bijection from $\frac{F^\times}{(F^\times)^2} - \{(F^\times)^2\}$ to $S/\sim_{iso}$ where S is the set of all quadratic field extensions over F.*

Proof. Let $\phi : \frac{F^\times}{(F^\times)^2} - \{(F^\times)^2\} \to S/\sim_{iso}$ be given by $\phi([a(F^\times)^2]) = [F[X]/<X^2-a>]_{iso}$. Note that if $a \notin F^2$ then X^2-a is irreducible over F hence $F[X]/<X^2-a>$ is a quadratic field extensions of F. Suppose $[a(F^\times)^2] = [b(F^\times)^2]$ then $\frac{a}{b} \in F^2$ hence $F[X]/<X^2-a> \cong F[X]/<X^2-b>$ by Theorem 2.1.2 hence $[F[X]/<X^2-a>]_{iso} = [F[X]/<X^2-a>]_{iso}$ hence ϕ is well defined. Now suppose $\phi([a(F^\times)^2]) = \phi([b(F^\times)^2])$ then $F[X]/<X^2-a> \cong F[X]/<X^2-b>$ hence by Theorem 2.1.2 we have $\frac{a}{b} \in F^2$ so $[a(F^\times)^2] = [b(F^\times)^2]$, proving that ϕ is injective. It remains to show that ϕ is surjective, let E/F be a quadratic field extension. By Lemma 2.1.1 we have that $E \simeq F[X]/<X^2-a>$ for some $a \in F$, Therefore, we have $\phi(a(F^\times)^2) = [E]_{iso}$, concluding the proof. □

We now use apply classification we got on finite fields.

Remark 2.1.7. *Let F be a finite field of order p^n such that $char(F) \neq 2$, then there are precisely $\frac{p^n-1}{2}$ quadratic residues and $\frac{p^n-1}{2}$ quadratic non-residues in F.*

Lemma 2.1.8. *Let F be a finite field such that $char(F) \neq 2$, then up to isomorphism there exists only one quadratic extension of F.*

Proof. From Theorem 2.1.6 we have that a one to one correspondence between $\{$quadratic field extension of $F\}/\sim_{iso}$ and $\frac{F^\times}{(F^\times)^2} - (F^\times)^2$. But in this case we have $|F^\times/(F^\times)^2| = 2$ so $|\frac{F^\times}{(F^\times)^2} - (F^\times)^2| = 1$ this implies there exist only one class of quadratic extensions of F up to isomorphism, □

Stellenbosch University https://scholar.sun.ac.za

2.2 Quadratic Field Extension Over Characteristic 2

In this section we classify separable quadratic feild extensions over any field of characterstic 2.

Lemma 2.2.1. *Let E/F be a separable quadratic field extension such that $char(F) = 2$ then $E \cong F[X]/<X^2 - X - d>$ for some $d \in F$*

Proof. Let $\beta \in E$ be any primitive element then $P(X) := min(\beta, F) = X^2 + bX + c$, then $b \neq 0$ otherwise $P'(X) = 0$ contradicting that L/E is separable. It follows $\beta^2 + b\beta + c = 0 \implies (\beta/b)^2 + (\beta/b) + c/b^2 = 0$, we claim that $-\beta/b$ is a primitive element we need. Note that $-\beta/b$ is a root of $X^2 - X - d$ where $d = -c/b^2$, It therefore remain to show that β/b is a generator of E , since $b \in F$ and $\beta \notin F$ it follows that $-\frac{\beta}{b}$ is not i F hence $-\beta/b$ is indeed a primitive elememt hence $F[X]<P(X)> \cong E/F$. □

Lemma 2.2.2. *Let F be a field such that $char(F) = 2$, If E/F and K/F are separable quadratic field extensions with primitive elements $\alpha \in E$ and $\beta \in K$ such that $min(\alpha, F) = X^2 - X - d$ and $min(\beta, F) = X^2 - X - d'$ then E and K are F-isomorphic if and only if $d' - d = b^2 - b$ for some $b \in F$.*

Proof. $\implies$ Let ϕ a F-isomorphism between E and K, α being a primitive element of E implies $\phi(\beta) = a\alpha + b$ for some $a \neq 0, b \in F$, hence $\phi(\beta)^2 - d' = 0 \implies (a\alpha + b)^2 - (a\alpha + b) - d' = 0 \implies a^2\alpha^2 + b^2 - a\alpha - b - d' = 0 \implies \alpha^2 - (1/a)\alpha - (d' + b - b^2)/a^2 = 0 \implies \alpha$ is a root of $X^2 - (1/a)X - (d' + b - b^2)/a^2$ but there is only one monic degree 2 polynomial in $F[X]$ containing α as a root namely $min(\alpha, F)$ hence $X^2 - (1/a)X - (d' + b - b^2)/a^2 = X^2 - X - d \implies a = 1$ and $d' - d = b^2 - b$ as desired.
$\impliedby$
Suppose $d' - d = b^2 - b$, It suffices to show that E has an element β' such that $min(\beta', F) = X^2 - X - d'$. $(\alpha + b)^2 - (\alpha + b) - d' = \alpha^2 + b^2 - \alpha - b - (b^2 - b + d) = \alpha^2 - \alpha - d = 0 \implies \alpha + b$ is a root of $X^2 - X - d'$. Note that $\alpha + b \notin F$ hence $min(\alpha + b, F) = X^2 - X - d'$, it follows that $E/F \cong F[X]/<X^2 - X - d'> \cong K/F$ as desired. □

Lemma 2.2.3. *Let F be a field of characteristic 2 and $G = \{b^2 - b | b \in F\}$, then G is a subgroup of the additive group of F.*

Proof. $0 = 0^2 - 0$ hence $0 \in G \implies G \neq \emptyset$. Let $a, b \in G$ then $a = c^2 - c$, $b = d^2 - d$ for some $c, d \in G$ and $a - b = c^2 - c - (d^2 - d) = (c^2 - d^2) - (c - d) = (c - d)^2 - (c - d)$ hence $a - b \in G \implies G$ is indeed a subgroup of F (as an additive group). □

Theorem 2.2.4. *Let F be a field such that $char(F) = 2$, S be a set of separable quadratic extensions of F. Then there exists a bijection from $F/G - \{G\}$ to $S/\sim_{iso}$ where $\sim_{iso}$ is the equivalence relation defined in S by $E_1 \sim_{iso} E_2$ if and only E_1 and E_2 are $F-$isomorphic.*

Proof. Let $\phi : F/G - \{G\} \to S/\sim_{iso}$ be defined by $\phi(a + G) = [F[X]/<X^2 - X - a>]$. ϕ is well defined. Indeed, let $a + G = b + G \implies a - b \in G \implies a - b = c^2 - c$ for some $c \in G$. It follows that from Lemma 2.2.2 that $F[X]/<X^2 - X - a>$ and $F[X]/<X^2 - X - b>$ are F-isomorphic, hence $\phi(a + G) = \phi(b + G)$. From Lemma 2.2.1 it's clear that ϕ is surjective. It remains to show that ϕ is injective. Suppose $\phi(a + G) = \phi(b + G)$ i.e $[F[X]/<X^2 - X - a>]_{\sim_{iso}} = [F[X]/<X^2 - X - b>]_{\sim_{iso}}$ hence $a - b = c^2 - c$ for some $c \in F$ by Lemma 2.2.2, this implies $a - b \in G \implies a + G = b + G$ as desired so ϕ is injective, this concludes the proof. □

Stellenbosch University https://scholar.sun.ac.za

Lemma 2.2.5. *Let F be a finite field such that $char(F) = 2$, then up to isomorphism there exists only one quadratic field extension of F.*

Proof. We will show that there exists a group homomorphism ϕ from F to F^2-F such that $F/ker(\phi) \cong F^2$-F and $ker(\phi) = \{0, 1\}$ which will imply if F is finite $|F|/|F^2\text{-}F| = 2$ hence $F/(F^2\text{-}F) - \{F^2\text{-}F\}$ contains only 1 element then using *Theorem* 2.2.4 we conclude that F has only one quadratic extension up to isomorphism. Let $\phi : F \to F^2$-F be defined by $\phi(a) = a^2 - a$, then $\phi(a+b) = (a+b)^2 - (a+b) = a^2 - b^2 - a - b = (a^2 - a) - (b^2 - b) = \phi(a) + \phi(b)$ hence ϕ is a group homomorphism, also $ker(\phi) = \{b \in F | b^2 - b = 0\} = \{b \in F | b(b-1) = 0\} = \{b \in F | b = 0 \text{ or } b = 1\} = \{0, 1\}$ and this concludes the proof. □

2.3 Applications over $\mathbb{Q}$

Over $\mathbb{Q}$, on can give a representative for each isomorphism class of quadratic extension up to isomorphism.

Lemma 2.3.1. *Let $\mathbb{Q}(\beta)$ be a quadratic extension of $\mathbb{Q}$ generated by $P(X) = X^2 - a \in \mathbb{Q}[X]$ then there exists a square free integer $b \in \mathbb{Z}$ and $\beta \in \bar{\mathbb{Q}}$ such that $\beta^2 = b$ such that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are $\mathbb{Q}$-isomorphic.*

Proof. Let $a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ be the prime factorization of a where $a_i \neq 0$ for $i \in \{1, \cdots, k\}$. Now define $b = p_{i_1} p_{i_2} \dots p_{i_s}$ square free where $i_j \in \{1, \cdots, k\}$ and $2 \nmid a_{i_j}$. Then $a/b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ where $2 | b_i$. Therefore, $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ as in the statement are $\mathbb{Q}$-isomorphic. □

Stellenbosch University https://scholar.sun.ac.za

Chapter 3

Quartic Field Extensions

For the remaining part of the thesis F will always denote a field of characteristic not 2.

3.1 Basic context

In the following, F denotes a field of characteristic not 2. Given a quartic polynomial $P(X)$ we denote by $P'(X)$, $P''(X)$, $P'''(X)$ the first, second, third and forth derivative respectively.

Definition 3.1.1. *Let K be a function field over F and L/K be a finite extension. The extension of function fields L/K is said to be **geometric** if $L \cap \overline{F} = F$.*

Definition 3.1.2. *Let L/F and K/F be field extensions, we assume that there is a field E containing both L and K. The **compositum** of $L.K$ is defined to be $L.K = F(L \cup K)$ where there right hand side denotes the extension of F generated by L and K in E.*

3.2 Notation and terminology around quartic extensions

We will study and classify a special case of quartic extensions the non-cyclic biquadratic extensions.

Definition 3.2.1. *A field extension L/F is said to be a **quartic extensions** if there exists a primitive element in L that has a minimal polynomial of degree 4.*

Definition 3.2.2. *A quartic field extension L/F is said to be **biquadratic** if there exists a primitive element $\alpha \in L$ such that $\min(\alpha, F) = X^4 + uX^2 + w$ where $u, w \in F$. Such α is called a biquadratic generator.*

Remark 3.2.3.

1. *If L/F is a biquadratic field extension then L/F is separable. Indeed, pick a biquadratic generator $\alpha \in L$, let $P(X) := min(\alpha, F) = X^4 + uX^2 + w$ then $P'(X) = 4X^3 + 2uX \neq 0$ as $char(F) \neq 0$. It follows that $gcd(P(X), P'(X)) = 1$ as $P(X)$ is irreducible over F.*

2. *Biquadratic Galois extensions are either cyclic or elementary abelian, we provide proof in Lemma 3.4.6.*

Stellenbosch University https://scholar.sun.ac.za

Definition 3.2.4. *A quartic field extension L/F is said to be* ***cyclic*** *if L/F is Galois and Galois group is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.*

Definition 3.2.5. *A quartic field extension L/F is said to be an* ***elementary abelian extension*** *if L/F is Galois and the Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Remark 3.2.6. *In the literature, one may also define a biquadratic field extension as a Galois extensions with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. That definition is not equivalent to the definition we provided.*

Definition 3.2.7. *A finite field extension L/F of degree n is said to be* ***radical*** *if there exists a primitive element $\alpha \in L$ such that $\alpha^n \in F$. Such α is called a radical generator.*

Definition 3.2.8. *Let L/F be a field extension of degree n, a* ***radical closure*** *of L/F (when it exists) is an extension K/F of smallest degree such that LK/K is a radical extension of degree n.*

Remark 3.2.9.

1. *If L/F be a biquadratic quartic extension admitting a radical closure K then $L \cap K = F$. Indeed, pick a biquadratic generator $\alpha \in L$ with minimal polynomial $P(X) = X^4 + uX^2 + w$ over F. We argue by contradiction, suppose there exists $\theta \in L \cap K - F$, then $F(\theta) = L$ or $F(\theta)$ is a quadratic sub-extension of L/F, so $P(X)$ is reducible over $F(\theta)$ hence reducible over K. This proves that the minimal polynomial of α over K is a proper divisor of $P(X)$ in $K[X]$ and $K(\alpha)/K$ is not a quartic field extension, contradicting the definition of radical closure so $L \cap K = F$.*

2. *In Theorem 4.1.4 we prove that when an elementary abelian extensions admits non-trivial radical closure then we have precisely 3 non-isomorphic radical closures.*

Definition 3.2.10. *Let L/F be a field extension of degree n, an* ***elementary abelian closure*** *of L/F (when it exists) is an extension K/F of smallest degree such that LK/K is an elementary abelian of degree n.*

Definition 3.2.11. *Let $L/K/F$ and $L'/K/F$ be a towers of fields, we say the* ***towers are isomorphic*** *denoted as $L/K/F \cong L'/K'/F$ if there exists a ring isomorphism $\phi : L \to L'$ such that $\phi\big|_K$ is an F-isomorphism.*

3.3 Families of minimal polynomials with at most two parameters

In the following results, we are looking for a family of minimal polynomials with at most two parameters to represent all the quartic extensions. We found two of them the biquadratic polynomials and the polynomials of the form $T(X) = X^4 + X^3 + cX^2 + d$ where c and d are in the ground field.

Lemma 3.3.1. *[12, M. Cele, S. Marques] Given a quartic polynomial*

$$P(X) = X^4 + uX^3 + vX^2 + wX + z$$

where $u, v, w, z \in F$
We denote $P_0 = P\left(-\frac{u}{4}\right)$, $P_1 = P'\left(-\frac{u}{4}\right)$, $P_2 = P''\left(-\frac{u}{4}\right)$ and $P_4 = p''''(-\frac{u}{4})$

Stellenbosch University https://scholar.sun.ac.za

1. *When $z = 0$, then $P(X)$ is reducible with 0 as a root;*
2. *When $z \neq 0$, $P_0 = 0$, then $P(X)$ is reducible with $-\frac{u}{4}$ as a root;*
3. *When $z \neq 0$, $P_0 \neq 0$ and $P_1 = 0$, then $P(X)$ is irreducible if and only if $S(X) = P(X - \frac{u}{4}) = X^4 + aX^2 + b$ is irreducible where $a = \frac{1}{2}P_2$ and $b = P_0$*
4. *When $z \neq 0$, $P_0 \neq 0$ and $P_1 \neq 0$, then the following statement are equivalent:*
   a) *$P(X)$ is irreducible*
   b) *$R(X) = X^4 + aX^2 + bX + b$ is irreducible where $a = \frac{P_1^2 P_2}{2P_0^2}$ and $b = \frac{P_1^4}{P_0^3}$.*
   c) *$T(X) = X^4 + X^3 + cX^2 + d$ is irreducible where $c = \frac{P_2 P_0}{2P_1^2}$ and $b = \frac{P_0^3}{P_1^4}$.*

Proof. 1. and 2. are clear.
For 3. and 4., we set $S(X) = P(X - u/4)$. Using tailor expansion, we have

$$P(X) = P_0 + P_1(X + \frac{u}{4}) + \frac{1}{2}P_2(X + \frac{u}{4})^2 + \frac{1}{6}P_3(X + \frac{u}{4})^3 + \frac{1}{24}P_4(X + \frac{u}{4})^4$$

since $P_3 = P'''(-\frac{u}{4}) = 0$ and $P_4 = P''''(X) = 24$ we have

$$P(X) = P_0 + P_1(X + \frac{u}{4}) + \frac{1}{2}P_2(X + \frac{u}{4})^2 + (X + \frac{u}{4})^4$$

hence

$$S(X) = P(X - \frac{u}{4}) = P_0 + P_1 X + \frac{1}{2}P_2 X^2 + X^4$$

3. When $P_1 = 0$ then $S(X) = X^4 + \frac{1}{2}P_2 X^2 + P_0$, therefore the result is clear.
4. Setting $R(X) = \frac{P_1^4}{P_0^4} S(\frac{P_0}{P_1}X) = \frac{P_1^4}{P_0^4}\left((\frac{P_0}{P_1}X)^4 + \frac{1}{2}P_2(\frac{P_0}{P_1}X)^2 + P_1(\frac{P_0}{P_1}X) + P_0\right) = X^4 + \frac{P_1^2 P_2}{2P_0^2}X^2 + \frac{P_1^4}{P_0^3}X + \frac{P_1^4}{P_0^3}$ and $T(X) = \frac{X^4}{b}R(\frac{1}{X})$, there the result is clear.

□

Corollary 3.3.2. *Let L/F be a quartic field extension, $x \in L$ be a primitive element with minimal polynomial*

$$P(X) = X^4 + uX^3 + vX^2 + wX + z$$

where $u, v, w, z \in F$
We denote $P_0 = P\left(-\frac{u}{4}\right)$, $P_1 = P'\left(-\frac{u}{4}\right)$ and $P_2 = P''\left(-\frac{u}{4}\right)$.

1. *When $P_1 = 0$ then $y = x + \frac{u}{4}$ is a primitive element with minimal polynomial*

$$R(X) = X^4 + \frac{1}{2}P_2 X^2 + P_0$$

2. *When $P_1 \neq 0$ then*
   a) *$y = \frac{P_0}{P_1}(x + \frac{u}{4})$ is a primitive element with minimal polynomial*

$$S(X) = X^4 + aX^2 + bX + b$$

   where $a = \frac{P_1^2 P_2}{2P_0^2}$ and $b = \frac{P_1^4}{P_0^3}$
   b) *$z = \frac{4P_0}{P_1(4x+u)}$ is a primitive element with the minimal polynomial $T(X) = X^4 + X^3 + cX^2 + d$ where $c = \frac{P_2 P_0}{2P_1^2}$ and $d = \frac{P_0^3}{P_1^4}$*

Stellenbosch University https://scholar.sun.ac.za

3.4 Generalities about biquadratic extensions

In the rest of the thesis, we will only focus on biquadratic extensions.

The following characterisation of biquadratic extension is well-known and very useful.
t

Lemma 3.4.1. *Let L/F be a quartic field extension, then L/F is a biquadratic if and only if L/F has intermediate quadratic sub-extension.*

The following lemma give a criterium to determine when a biquadratic polynomial is irreducible.

Lemma 3.4.2. *Let F be a field and $P(X) = X^4+uX^2+w \in F[X]$ with roots $\alpha, -\alpha, \beta, -\beta$ in it's splitting field, then the following are equivalent*

1. *$P(X)$ is irreducible over F*
2. *$\alpha^2, \alpha+\beta$ and $\alpha-\beta$ are not in F*
3. *$u^2-4w, -u+2\omega$, and $-u-2\omega$ are not F^2, where $\omega^2 = w$.*

Proof. Let $\Delta = \alpha^2 - \beta^2$ then $\Delta^2 = u^2 - 4w$. Moreover, $P(X)$ is reducible if and only if $P(X)$ has a monic quadratic factor in $F[X]$. Indeed, the factor can be chosen to be monic since F is a field. Moreover, if $P(X)$ is reducible over F and does not have a monic quadratic factor, the factor would have a root, say α but then $-\alpha$ is also a root and $X^2 - \alpha^2$ divides $P(X)$. The converse is clear. We note also that over $\overline{F}$, we have

$$P(X) = (X-\alpha)(X+\alpha)(X-\beta)(X+\beta)$$

Therefore, there are 3 ways to write $P(X)$ as a product quadratic polynomials, these are

(a) $(X^2-\alpha^2)(X^2-\beta^2)$.

(b) $\big(X^2-(\alpha+\beta)X+\alpha\beta\big)\big(X^2+(\alpha+\beta)X+\alpha\beta\big)$.

(c) $\big(X^2-(\alpha-\beta)X-\alpha\beta\big)\big(X^2+(\alpha-\beta)X-\alpha\beta\big)$.

The factorisation 1. lies in $F[X]$ if and only if $\alpha^2 \in F$ if and only the discriminant Δ^2 of $P(X^2)$ is a square in F.
The factorisation 2. lies in $F[X]$ if and only if $\alpha+\beta \in F$. Indeed, $\alpha+\beta \in F$ implies that $\alpha\beta \in F$ since $\alpha\beta = -\frac{1}{2}(\alpha^2+\beta^2-(\alpha+\beta)^2)$ and $\alpha^2+\beta^2 = -u \in F$, this is true if and only if $(\alpha+\beta)^2 = \alpha^2+\beta^2+2\alpha\beta = -u+2\omega \in F^2$ where $\omega^2 = w$.

Finally, the factorisation 3. lies in $F[X]$ if and only if $\alpha-\beta \in F$. Indeed, $\alpha-\beta \in F$ implies that $\alpha\beta \in F$ since $\alpha\beta = \frac{1}{2}(\alpha^2+\beta^2-(\alpha-\beta)^2)$ and $\alpha^2+\beta^2 = -u \in F$, this is true if and only if $(\alpha-\beta)^2 = \alpha^2+\beta^2-2\alpha\beta = -u-2\omega \in F^2$. □

Remark 3.4.3. *Let F be a field and $P(X) = X^4+uX^2+w \in F[X]$. If $\alpha \in F$ is a root of $P(X)$ then $u^2-4w \in F^2$. This follows from the fact that α^2 is a root of $P(X^2) = X^2+uX+w$ in F. In the case, when $P(X)$ is irreducible over F and $L := F[X]/<P(X)>$ and α is a generator for L/F with minimal polynomial $P(X)$, we can deduce that $u^2-4w \in L^2$. We also have that $F(\alpha^2) = F(\gamma)$ is a quadratic sub-extension of L/F with $\gamma^2 = u^2-4w$.*

Stellenbosch University https://scholar.sun.ac.za

The following result characterise the Galois biquadratic extensions, proved by M. Cele and S. Marques in [12]

Lemma 3.4.4. *Let L/F be a biquadratic field extension, $\alpha \in L$ be a biquadratic generator with minimal polynomial $P(X) = X^4 + uX^2 + w$ over F. Then the following statements are equivalent,*

1. *L/F is a Galois extension;*
2. *$u^2 - 4w, u - 2\omega$ and $u + 2\omega$ are in L^2 with $\omega^2 = w$;*
3. *$w \in L^2$.*

Proof. Under the present assumptions, L/F is separable, therefore L/F Galois is equivalent to L is the splitting field of $P(X)$ over F.

1. $\implies$ 2. $\implies$ 3. In the proof of the previous Lemma, we see that any of the factorisation (a), (b) and (c) are all valid in the splitting field. Therefore $u^2 - 4w, -u + 2\omega, -u - 2\omega \in L^2$. In particular, we have $\omega \in L$. So that $w \in L^2$

3. $\implies$ 1. Let $\{\pm\alpha, \pm\beta\}$ be the roots $P(X)$ in the splitting field of $P(X)$, then $P(X)$ factors as $P(X) = (X^2 - \alpha^2)(X^2 - \beta^2) = X^4 - (\alpha^2 + \beta^2)X^2 + (\alpha\beta)^2$. Now $w = (\alpha\beta)^2 \in L^2$ implies $\alpha\beta \in L$. So that, $\beta \in L$ since $\alpha \in L$ by assumption. So $\{\pm\alpha, \pm\beta\} \subset L$ which proves L is the splitting field of $P(X)$ over F. Hence, L/F is Galois. □

Remark 3.4.5. *Let L/F be a biquadratic non-galois quartic extension, $\alpha \in L$ be a biquadratic generator with minimal polynomial $P(X) = X^4 + uX^2 + w$ over F. Then*

1. *$L^{Gal} = L(\omega)$ where $\omega \in \overline{F}$ and $\omega^2 = w$, this is because the roots of $P(X)$ in L^{Gal} are of the form $\pm\alpha, \pm\beta$ so $w = (\alpha\beta)^2 \in (L^{Gal})^2$, but $w \notin L^2$ by the previous Lemma.*
2. *$Aut(L^{Gal}/F) \cong D_8$. This is because $[L^{Gal} : F] = [L^{Gal} : L][L : F] = 8$, So $Aut(L^{Gal}/F)$ has 8 elements, but the only transitive subgroup of A_4 of order 8 is D_8. We know $Aut(L^{Gal}/F)$ is a transitive subgroup of S_4 by [2, Theorem 2.9].*

The next result is well-known. Since we could not find a reference that would prove the result in the present form, we decide to include the proof for completeness. This characterization is useful in distinguishing between elementary abelian and non-elementary abelian extension in the classification of these extensions.

Lemma 3.4.6. *Let L/F be a biquadratic field extension, $\alpha \in L$ be a primitive element with minimal polynomial $P = X^4 + uX^2 + w$, then $Aut(L/F)$ isomorphic to*

1. *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if $w \in F^2$*
2. *$\mathbb{Z}/4\mathbb{Z}$ if and only if $w \notin F^2$ and $w(u^2 - 4w) \in F^2$*
3. *$\mathbb{Z}/2\mathbb{Z}$ if and only if $w \notin F^2$ and $w(u^2 - 4w) \notin F^2$*

Proof. 1. If $Aut(L/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ then the discriminant of $P(X)$ is a square in F by [2, Theorem 4.7] since $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is a subgroup of A_4, that is $\Delta(P(X)) = 16w(u^2 - 4w)^2 \in F^2$ hence $w \in F^2$. Conversely, let $w = \omega^2$ for some $\omega \in F$. By Lemma 3.4.4 L/F is Galois i.e $|Aut(L/F)| = [L : F] = 4$, therefore L/F is isomorphic to either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. By Lemma 3.4.4 there exists $\gamma, \delta \in L$ such that $\gamma^2 = u^2 - 4w$ and $\delta^2 = -u - 2\omega$, in addition $F(\gamma)$ and $F(\delta)$ are quadratic

Stellenbosch University https://scholar.sun.ac.za

sub-extensions of L/F. Those two quadratic extensions are distinct since otherwise $\frac{u^2-2w}{-u-2\omega} = -u+2\omega \in F^2$ by Theorem 2.1.2 and this would contradict the irreducibility of $P(X)$ over F by Lemma 3.4.2. Since there is a one-to-one correspondence between quadratic sub-extensions of L/F and subgroups $Aut(L/F)$ of degree 2 it follows that $Aut(L/F)$ has at least two subgroups of order 2 hence $Aut(L/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2. We suppose $Aut(L/F) \cong \mathbb{Z}/4\mathbb{Z}$ then L/F is Galois and $w \notin F^2$ by 1.. $u^2-4w \notin F^2$ by Lemma 3.4.2 and by Lemma 3.4.4 there exists $\gamma, \delta \in L$ such that $\gamma^2 = w$ and $\delta^2 = u^2-4w$ so $F(\gamma)$ and $F(\delta)$ are quadratic sub-extensions of L/F. Since quadratic sub-extensions correspond with subgroups of $Gal(L/F)$ of degree 2 and $Aut(L/F)$ has 1 subgroup of order 2 it follows that $F(\delta) = F(\gamma)$. As a consequence, $u^2-4w = a^2w$ for some $a \in F$ by Theorem 2.1.2, this implies $w(u^2-4w) = (aw)^2 \in F^2$ as desired. Conversely, let $w(u^2-4w) \in F^2$ and $w \notin F^2$, we want to show that $w \in L^2$ which from Lemma 3.4.4 and 1. will prove the result. This follows from $u^2-4w \in L^2$ since it is the discriminant of $Q(X) = X^2+uX+w$ with $\alpha^2 \in L$ as root. Now that $w(u^2-4w), u^2-4w \in L^2$ it follows that $w \in L^2$.

3. If $Aut(L/G) \cong \mathbb{Z}/2\mathbb{Z}$, then $w \notin F^2$ by 1. and $w(u^2-4w) \notin F^2$ by 2. Conversely if $u(u^2-4w) \notin F^2$ and $w \notin F^2$ then L/F is not Galois by 1. and 2. It then follows that $Aut(L/F) \cong \mathbb{Z}/2\mathbb{Z}$ or $Aut(L/F)$ is the trivial group. The automorphism $\sigma : \alpha \to -\alpha$ fixes F and is not trivial hence $Aut(L/F)$ is not trivial. Therefore, $Aut(L/F) \cong \mathbb{Z}/2\mathbb{Z}$

□

Stellenbosch University https://scholar.sun.ac.za

Chapter 4

Non-cyclic extensions

4.1 Elementary Abelian Extensions

The following result characterize elementary abelian extensions via number of quadratic sub-extensions and description of the minimal polynomial.

Theorem 4.1.1. *[12, M. Cele, S. Marques] Let L/F be a quartic field extension, the following are equivalent*

1. *L/F is Galois and $Gal(L/F) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
2. *L/F has exactly 3 quadratic sub-extensions.*
3. *L/F has more than 1 quadratic sub-extension.*
4. *There exists $\alpha, \beta \in L$ such that $\alpha^2 \in F$, $\beta^2 \in F$, $F(\alpha)$ and $F(\beta)$ are quadratic extensions of F, $F(\alpha) \neq F(\beta)$ and $L = F(\alpha, \beta)$.*
5. *L/F has a biquadratic generator has with minimal polynomial of the $P(X) = X^4 - 2(a+b)X^2 + (a-b)^2$ over F for unique $a, b \in F$.*
6. *Any biquadratic generator of L/F has a minimal polynomial has the form*

$$P(X) = X^4 - 2(a+b)X^2 + (a-b)^2$$

over F for unique $a, b \in F$.

Note that assuming 5. or 6. guarantee that there exists $\alpha, \beta \in L$ such that $\gamma^2 = a$ and $\delta^2 = b$, moreover $F(\alpha)$, $F(\beta)$ are quadratic extensions of F, $F(\alpha) \neq F(\beta)$, that is $a/b \notin F^2$ and $L = F(\alpha, \beta)$. Also $\alpha + \beta$ is a primitive element of L/F with minimal polynomial $P(X)$.

Proof. We will prove that

$$1. \implies 2. \implies 3. \implies 4. \implies 5. \implies 1. \implies 6. \implies 1.$$

$1. \implies 2.$ L/F is Galois hence there is a one-to-one correspondence between quadratic sub-extensions of L/F and subgroups of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ of order 2, so L/F has 3 quadratic sub-extensions.
$2. \implies 3.$ is trivial

Stellenbosch University https://scholar.sun.ac.za

3. $\implies$ 4 Let $F(\alpha)$ and $F(\beta)$ be distinct quadratic sub-extensions of L/F, by Lemma 2.1.1 we can assume that $\alpha^2 \in F$ and $\beta^2 \in F$. From $[F(\alpha,\beta) : F] = 4$ we get that $L = F(\alpha,\beta)$concluding the proof.
4. $\implies$ 5 Let $F(\alpha)$ and $F(\beta)$ be distinct quadratic sub-extensions of L/F, We will prove $P(X) = X^4 - 2(a+b)X^2 + (a-b)^2$ is the minimal polynomial of $\alpha+\beta$. Indeed, firstly, by completing the square, we obtain $P(\alpha+\beta) = ((\alpha+\beta)^2 - (\alpha^2+\beta^2))^2 - (\alpha^2+\beta^2)^2 + (\alpha^2-\beta^2)^2 = 0$ and we will prove that $P(X)$ is irreducible over F. We have similarly that $\alpha-\beta$ is also a root in $P(X)$ in L. Therefore, the roots of $P(X)$ are $\pm\alpha$, $\pm\beta$ where $\alpha = \alpha+\beta$ and $\beta = \alpha-\beta$. But $\alpha^2 = a+b+2\alpha\beta \notin F$ because $\frac{\alpha}{\beta} \notin F$. Moreover, neither $\alpha+\beta = 2\alpha$, nor $\alpha-\beta = 2\beta$ are in F, since $F(\alpha)$ and $F(\beta)$ are quadratic extensions of F.
5. $\implies$ 1. Follows from Lemma 3.4.6
1. $\implies$ 6. We assume that L/F is Galois with $Gal(L/F) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $\alpha \in L$ be a biquadratic generator and $P(X)$ be the minimal polynomial of α over F, then by Lemma 3.4.6, $P(X) = X^4 + uX^2 + w$ for some $u, w \in F$ with $w = \omega^2$ for some $\omega \in F$. Let $a = \frac{1}{4}(2\omega - u)$ and $b = -\frac{1}{4}(2\omega + u)$ then $P(X) = X^4 - 2(a+b)X^2 + (a-b)^2$. Suppose a and b are not unique, that is there exist $x, y \in F$ such that $u = -2(x+y) = -2(a+b)$ and $w = (x-y)^2 = (a-b)^2$, then $x+y = a+b$ and $x-y = \pm(a-b)$, it follows that $x = a$, $y = b$ or $x = b$, $y = a$.
6. $\implies$ 1. Follows from Lemma 3.4.6

□

Remark 4.1.2. *Note that, if F is a field and $P(X) = X^4 - 2(a+b)X^2 + (a-b)^2 \in F[X]$ as in the previous theorem then $P(X)$ is irreducible over F if and only $a \notin F^2$ and $b \notin F^2$ and $ab \notin F^2$ by Lemma 3.4.2. Moreover, the roots of this polynomial are $\epsilon_1\gamma + \epsilon_2\delta$, where α (resp. γ) is such that $\gamma^2 = a$ (resp. $\delta^2 = b$) and $\epsilon_i \in \{\pm 1\}$, $i = 1, 2$. Also, the possible quadratic factorisation of of $P(X)$ are now $(X^2 - a - b - 2\gamma\delta)\,(X^2 - a - b + 2\gamma\delta)$, $\big(X^2 - 2\gamma X + a - b\big)\big(X^2 + 2\gamma X + a - b\big)$ and $\big(X^2 - 2\delta X - a + b\big)\big(X^2 + 2\delta X - a + b\big)$.*

A nice application of the previous theorem, describe radical elementary abelian extensions. Part of the following result is also part of [16, Theorem 6.1.]. We start with a remark we will use multiple times in the proof.

Remark 4.1.3. *Let L/F be an elementary abelian extension, if K is a radical closure of L/F then $L.K/K$ is an elementary abelian extension, if α is a biquadratic generator of L/F then $L.K/K = K(\alpha)$ and $min(\alpha, F) = min(\alpha, K)$ where the second equality follows because $min(\alpha, F), min(\alpha, K)$ are both degree 4 monic elements of $K[X]$ having α as a root.*

Theorem 4.1.4. *[12, M. Cele, S. Marques] Let L/F be a elementary abelian extension then L/F has*

1. *a trivial radical closure if and only if $F(i)$ is a quadratic sub-extension of L/F. In this case L/F is radical, and any radical generator is of the form $\gamma(i+1)$ where $\gamma \in L$ is a radical generator of a quadratic sub-extension of L/F and $F(\gamma) \neq F(i)$.*

2. *no radical closure if and only if $i \in F$;*

3. *exactly 3 radical closures if and only if $i \notin L$. In this case, the 3 radical closure are precisely $F(\gamma i)$ where γ is a radical generator of a quadratic subextension of L/F.*

Stellenbosch University https://scholar.sun.ac.za

Proof. 1. Let L/F be a radical extension and $\alpha \in L$ be a radical generator of L/F, then $min(\alpha, F) = P(X) = X^4 + w$ where $w = \omega^2$ for some $\omega \in F$. Moreover, $P(X)$ is irreducible over F hence $-4w = -4\omega^2 \notin F^2$ by Lemma 3.4.2 this implies $-1 \notin F^2$ hence $i \notin F$. By Remark 3.4.3, $-4w = -4\omega^2 \in L^2$ hence $i \in L$ so indeed $F(i)$ is a quadratic sub-extension of L/F.

Conversely, let $F(i)$ be a quadratic sub-extension of L/F. Pick $F(\gamma)$ a quadratic sub-extension of L/F different from $F(i)$ such that $\delta^2 = a \in F$, then $-a \notin F^2$ by Theorem 2.1.2. We claim that $\delta(1+i) \in L$ is a radical generator for L/F with minimal polynomial $Q(X) = X^4 + 4a^2$. First, $\delta(1+i) \in L$ is a root of $Q(X)$ since $Q(\delta(1+i)) = (\delta(1+i))^4 + (2a)^2 = 0$. Also, we prove that $Q(X)$ is irreducible. For this we apply Lemma 3.4.2 for $Q(X)$ so that $u = 0$ and $w = 4a^2$ and therefore $u^2 - 4w = -(4a)^2 \notin F^2$ as $-1 \notin F^2$, $-u + 2\omega = 4a \notin F^2$ as $a \notin F^2$, lastly $-u - 2\omega = -4a \notin F^2$ as $-a \notin F^2$, proving the irreducibility of $Q(X)$ and concluding the proof of the claim.

We now show that any radical generator is of the form $\gamma(i+1)$ for some γ is a radical generator of a quadratic sub-extension of L/F. Let $min(\beta, F) = X^4 + w^2$. We have $w = a - b$ and $0 = a + b$ for some $a, b \in F \setminus F^2$. So that, $w = 2a$. By Lemma 4.1.1 $a = \gamma^2$ for some $\gamma \in L$ such that $[F(\gamma) : F] = 2$. Moreover, $\gamma \notin F(i)$. Indeed, if it was then by Theorem 2.1.2 there will be $c \in F$ such that $a = -c^2$ but $-a = b$ is not a square in F leading to a contradiction. We can rewrite $\beta^4 + w^2 = 0$ as $(\beta^2 - 2ia)(\beta^2 + 2ia) = 0$. Therefore, $\beta^2 = \pm 2ia$ so that $\beta = \gamma(i \pm 1)$ or $\beta = -\gamma(i \pm 1)$. Proving the theorem since γ/i is a generator of one of the quadratic subextensions of L/F and $i(i+1) = 1 - i$.

2. We argue by contradiction. Suppose $i \in F$ and L/F has a radical closure K. By 1., $K(i)$ is quadratic extension of $L.K/K$ contradicting that $i \in F \subset K$. Hence such K does not exist, L/F does not have a radical closure.

   Conversely, we will prove that if $i \notin F$ then L/F has a radical closure. For this, we suppose $i \notin F$. If $i \in L$ then F is the trivial radical closure of L/F and we are done. We can then assume that $i \notin L$, let $F(\gamma)$ be quadratic sub-extension of L/F such that $\gamma^2 \in F$. We claim that $K := F(i\gamma)$ is a radical closure of L/F. We first show that $L.K/K$ is a quartic extension, we prove by contradiction that $K \cap L = F$. Suppose $K \subset L$ then $i\gamma, \gamma \in L$ which implies $i = \frac{i\gamma}{\gamma} \in L$, contradicting that L/F is not radical so indeed $K \cap L = F$ hence $L.K/K$ is a quartic extension. It remains to show that $L.K/K$ is a radical extension, for this it suffices to show $K(i)$ is quadratic sub-extension of $L.K/K$. Note that $i \notin K$, otherwise of $i \in K$ then $K = F(i) = F(i\gamma)$ and this implies $\gamma \in F$ by Theorem 2.1.2 contradicting that $F(\gamma)$ is quadratic sub-extension of L/F. We have $\gamma, i\gamma \in L.K$ hence $i \in L.K$ this implies $K(i)$ is indeed a quadratic sub-extension of $L.K/K$, this proves $L.K/K$ is indeed a radical extension.

3. The "only if direction" is a clear consequence of 1. and 2.. We suppose that $i \notin L$. Since $i \notin F$, from the proof of 2., we know that $F(i\gamma)$ is a radical closure of L/F whenever $F(\gamma)$ is a quadratic sub-extension of L/F. When $F(\gamma)$, $F(\delta)$ and $F(\gamma\delta)$ are distinct quadratic sub-extensions of L/F then $F(i\gamma)$, $F(i\delta)$ and $F(i\gamma\delta)$ are also distincts. We can prove the latter as usual using Theorem 2.1.2. Therefore, L/F has at least 3 radical closures. It remains to prove that given M a radical closure of L/F, M is one of the above. One can prove that $M(\gamma), M(\delta)$ and $M(\gamma\delta)$ are

Stellenbosch University https://scholar.sun.ac.za

the quadratic sub-extensions of $L.M/M$. Also, by 1., since $L.M/M$ is radical, $M(i)$ is quadratic sub-extension of $L.M/M$. Thus, $M(i) = M(\theta)$ where $\theta \in \{\gamma, \delta, \gamma\delta\}$ which implies $i\theta \in M$ by lemma 2.1.2. Hence, $M = F(i\theta)$, by definition of a radical closure. This concludes the proof of 3.

□

Remark 4.1.5. *Note when F is a function field and L/F is a function fields extension then the previous result state that if an extension is geometric and elementary abelian, then it cannot be radical.*

Corollary 4.1.6. *Let L/F and L'/F be two elementary abelian radical extensions with radical generators $\alpha \in L$ and $\alpha' \in L'$ with minimal polynomial $P(X) = X^4 + a$ and $Q(X) = X^4 + a'$ respectively. Then, the following statements are equivalent:*

1. *L/F is F-isomorphic to L'/F.*
2. *$a' = d^4a^j$ where j is 1 or 3 and $d \in F$.*
3. *$a' = c^4a$ where $c \in F$.*
4. *$c\alpha'$ is a radical generator with minimal polynomial $P(X)$ where $c \in F$.*
5. *$d\alpha'^j$ is a radical generator with minimal polynomial $P(X)$ where j is 1 or 3 and $d \in F$.*

Proof. 1. $\implies$ 2. Let ϕ be a F-isomorphism from L/F to L'/F. Let $\alpha' = \phi(\alpha) \in L$. It is then a root of $Q(X)$. By Lemma 4.1.4 there exists radical generators $\gamma, \delta \in L$ of quadratic sub-extensions of L/F different from $F(i)$ such that $\alpha = \gamma(i+1)$ and $\alpha' = \delta(i+1)$. $F(i), F(\gamma)$ and $F(i\gamma)$ are the quadratics sub-extensions of L/F hence $F(\delta)$ is one of them i.e $F(\gamma) = F(\delta)$ or $F(i\gamma) = F(\delta)$, in the former we have $\delta = d\gamma$ for some $d \in F$ by Theorem 2.1.2 hence $\alpha' = \delta(i+1) = d\gamma(i+1) = d\alpha$ so $a' = d^4a$. When $F(\gamma) = F(i\delta)$ we have $\delta = bi\gamma$ for some $b \in F$ by Theorem 2.1.2 , let $e := \gamma^2 \in F$. Then $\alpha' = \delta(i+1) = bi\gamma(i+1) = -\frac{d}{2e}(\gamma(i+1))^3 = d\alpha^3$ where $d = -\frac{c}{2e}$ hence $a' = d^4a^3$.

2. $\implies$ 3. When $j = 1$ setting $c = d$ concludes the proof. From Lemma 3.4.6 we have know that $a = \omega^2$ for some $\omega \in F$, so when $j = 3$ we have $a' = d^4a^3 = (d\omega)^4a$ then setting $c = d\omega$ concludes the proof.

3. $\implies$ 4. $P(c\alpha') = (c\alpha')^4 + a' = c^4(-a') + a = 0$, $c\alpha'$ being a primitive element of L/F follows from the fact that $P(X)$ is irreducible over F.

4. $\implies$ 5. Clear.

5. $\implies$ 1. The ring homomorphism sending $d\alpha'^j$ to α and extended by linearity is an F-isomorphism.

□

Lemma 4.1.7. *[12, M. Cele, S. Marques] Let L/F be an elementary abelian extension, $F(\gamma)$ and $F(\delta)$ be distinct quadratic sub-extensions of L/F. If L'/F is quartic extension then L/F and L'/F are F-isomorphic if and only $F(\gamma)$ and $F(\delta)$ are isomorphic to quadratic sub-extensions of L'/F.*

Proof. $\implies$ Let $\psi : L \to L'$ be a F-isomorphism, it is not hard to show that $F(\psi(\gamma))$ and $F(\psi(\delta))$ are quadratic sub-extensions of L'/F and that $F(\gamma) \cong F(\psi(\gamma))$ and $F(\delta) \cong F(\psi(\delta))$.

Stellenbosch University https://scholar.sun.ac.za

$\Longleftarrow$ Let $L_1, L_2 \subset L$ be distinct quadratic extensions and $L_1', L_2' \subset L'$ be distinct quadratic extensions such that $L_1 := F(\gamma) \cong L_1'$ and $L_2 := F(\delta) \cong L_2'$. Let $\sigma_i : L_i \to L_i'$ be F-isomorphisms. Since δ is a generator of L_2 over F, then $\sigma_2(\delta)$ is a generator of L_2' over F both with the same minimal polynomial $P(X)$. We have that $P(X)$ is irreducible over $F(\gamma)$. Indeed, $P(X)$ does not have a root in $F(\gamma)$ since $F(\gamma) \cap F(\delta) = F$. Hence, by [15, Lemma 50], there exists a F-isomorphism $\overline{\sigma_1} : L = L_1(\delta) \to L' = L_1'(\sigma_2(\delta))$ extending σ_1. This concludes the proof. □

The following theorem, permits to classify elementary abelian extensions comparing their minimal biquadratic polynomials.

Theorem 4.1.8. *[12, M. Cele, S. Marques] Let L/F be an elementary abelian field extension, $y \in L$ be a biquadratic generator with minimal polynomial*

$$P(X) = X^4 + uX^2 + w^2 \in F[X].$$

Let L'/F be a biquadratic field extension, $y' \in L'$ biquadratic generator then with minimal polynomial

$$Q(X) = X^4 + vX^2 + z^2 \in F[X]$$

following then L/F and L'/F are F-isomorphic if and only if at least one the following statements is true.

1. $\frac{-v-2z}{-u+2w}, \frac{-v+2z}{-u-2w} \in F^2$
2. $\frac{-v-2z}{-u+2w}, \frac{-v+2z}{u^2-4w^2} \in F^2$
3. $\frac{-v-2z}{-u-2w}, \frac{-v+2z}{-u+2w} \in F^2$
4. $\frac{-v-2z}{-u-2w}, \frac{-v+2z}{u^2-4w^2} \in F^2$
5. $\frac{-v-2z}{u^2-4w^2}, \frac{-v+2z}{-u-2w} \in F^2$
6. $\frac{-v-2z}{u^2-4w^2}, \frac{-v+2z}{-u+2w} \in F^2$

Proof. The quadratic sub-extensions of L/F are precisely $F(\alpha)$, $F(\beta)$ and $F(\alpha\beta)$ with $\alpha^2 = -u+2w$, and $\beta^2 = -u-2w$ so $(\alpha\beta)^2 = u^2-4w^2$, also the quadratic sub-extensions of L'/F are $F(\delta)$, $F(\gamma)$ and $F(\delta\gamma)$ where $\delta^2 = -v+2z$, $\gamma^2 = -v-2z$ and $(\delta\gamma)^2 = v^2-4z^2$. By Lemma 4.1.7, L/F and L'/F are isomorphic if and only if $F(\delta)$ and $F(\gamma)$ are isomorphic to quadratic sub-extensions of L/F since $L' = F(\delta).F(\gamma)$. There are exactly 6 ways in which this can happen, these are the possibilities.

1. $F(\gamma) \cong F(\alpha)$ and $F(\delta) \cong F(\beta) \iff \frac{\gamma^2}{\alpha^2} = \frac{-v-2z}{-u+2w}, \frac{\delta^2}{\beta^2} = \frac{-v+2z}{-u-2w}, \in F^2$.
2. $F(\gamma) \cong F(\alpha)$ and $F(\delta) \cong F(\alpha\beta) \iff \frac{\gamma^2}{\alpha^2} = \frac{-v-2z}{-u+2w}, \frac{\delta^2}{(\alpha\beta)^2} = \frac{-v+2z}{u^2-4w^2} \in F^2$.
3. $F(\gamma) \cong F(\beta)$ and $F(\delta) \cong F(\alpha) \iff \frac{\gamma^2}{\beta^2} = \frac{-v-2z}{-u-2w}, \frac{\delta^2}{\alpha^2} = \frac{-v+2z}{-u+2w} \in F^2$.
4. $F(\gamma) \cong F(\beta)$ and $F(\delta) \cong F(\alpha\beta) \iff \frac{\gamma^2}{\beta^2} = \frac{-v-2z}{-u-2w}, \frac{\delta^2}{(\alpha\beta)^2} = \frac{-v+2z}{u^2-4w^2} \in F^2$.
5. $F(\gamma) \cong F(\alpha\beta)$ and $F(\delta) \cong F(\alpha) \iff \frac{\gamma^2}{(\alpha\beta)^2} = \frac{-v-2z}{u^2-4w^2}, \frac{\delta^2}{\alpha^2} = \frac{-v+2z}{-u+2w} \in F^2$.
6. $F(\gamma) \cong F(\alpha\beta)$ and $F(\delta) \cong F(\beta) \iff \frac{\gamma^2}{(\alpha\beta)^2} = \frac{-v-2z}{u^2-4w^2}, \frac{\delta^2}{\beta^2} = \frac{-v+2z}{-u-2w} \in F^2$.

The six previous equivalences are obtained using Theorem 2.1.2 □

The next remark explicit the relationship between generator of isomorphism elementary abelian extensions.

Stellenbosch University https://scholar.sun.ac.za

Remark 4.1.9. *1. Note that for $P(X) = X^4 + uX^2 + w^2$ (resp. $Q(X) = X^4 + vX^2 + z^2$), we have $P(X) = X^4 - 2(a+b)X^2 + (a-b)^2$ where $a = -u - 2w, b = -u + 2w$ (resp. $Q(X) = X^4 - 2(a'+b')X^2 + (a'-b')^2$ where $a' = -v - 2z$ and $b' = -v + 2z$). We also note that such a, b (resp. a', b') are unique (see also Theorem 4.1.1).*

2. Let L/F be an elementary abelian extension, y a generator and $P(X) = X^4 - 2(a+b)X^2 + (a-b)^2$ be its minimal polynomial (see Theorem 4.1.1). We also know from Theorem 4.1.1, that $y := \alpha + \beta$ whith α (resp. β) such that $\alpha^2 = a$ (resp. $\beta^2 = b$). From the proof of Lemma 4.1.1 and Theorem 4.1.8, we have that the set of biquadratic generators of L/F is $X := X_a \cup X_b \cup X_{ab}$ where $X_{ab} = \{s\alpha + r\beta | s, r \in F^\times\}, X_a = \{r\beta + s\alpha\beta | r, s \in F^\times\}, X_b = \{r\alpha + s\alpha\beta | r, s \in F^\times\}$. From $y^2 = a+b+2\alpha\beta$, we get $\alpha\beta = \frac{1}{2}(y^2 - a - b)$. So $\frac{1}{2}y(y^2 - a - b) - ay = \alpha\beta y - ay = (a-b)\alpha$. Hence $\alpha = \frac{3a+b}{2(a-b)}y - \frac{1}{2(a-b)}y^3$. Similarly, $\beta = \frac{1}{2(a-b)}y^3 - \frac{(a+3b)}{2(a-b)}y$. It follows that $s\alpha + r\beta = \frac{r-s}{2(a-b)}y^3 + \frac{(3a+b)s-(a+3b)r}{2(a-b)}y$, $s\alpha + r\alpha\beta = s(\frac{3a+b}{2(a-b)}y - \frac{1}{2(a-b)}y^3) + r(\frac{1}{2}(y^2 - a - b)) = -\frac{(a+b)r}{2} + \frac{(3a+b)s}{2(a-b)}y + \frac{r}{2}y^2 - \frac{s}{2(a-b)}y^3$, and $s\beta + r\alpha\beta = s(\frac{1}{2(a-b)}y^3 - \frac{(a+3b)}{2(a-b)}y) + r(\frac{1}{2}(y^2 - a - b)) = -\frac{(a+b)r}{2} - \frac{(a+3b)s}{2(a-b)}y + \frac{r}{2}y^2 + \frac{s}{2(a-b)}y^3$. Therefore, $X = \{-\frac{(a+b)r}{2} - \frac{(a+3b)s}{2(a-b)}y + \frac{r}{2}y^2 + \frac{s}{2(a-b)}y^3 | r, s \in F^\times\} \cup \{-\frac{(a+b)r}{2} + \frac{(3a+b)s}{2(a-b)}y + \frac{r}{2}y^2 - \frac{s}{2(a-b)}y^3 | r, s \in F^\times\} \cup \{\frac{r-s}{2(a-b)}y^3 + \frac{(3a+b)s-(a+3b)r}{2(a-b)}y | r, s \in F^\times\}$. Note that $X_{ab} = \{uy + vy^3 | u, v \in F$ such that $u \neq -(a+3b)v$ or $u \neq -(3b+a)v\}$, this follows from the fact that $uy + vy^3 = \frac{r-s}{2(a-b)}y^3 + \frac{(3a+b)s-(a+3b)r}{2(a-b)}y$ where $s = u + (a+3b)v$ and $r = u + (3a+b)v$.

The goal of the remaining part of this section is to reformulate the previous theorem into a group theoretic language.

Definition 4.1.10. *We define a relation $\sim_1$ on $F^\times \times F^\times$ as follows, if $(a, a'), (b, b') \in F^\times \times F^\times$ then $(a, a') \sim_1 (b, b')$ if only if at least one of the following is true*

1. $ab, a'b' \in F^2$
2. $ab', a'b \in F^2$
3. $ab, a'bb' \in F^2$
4. $abb', a'b \in F^2$
5. $ab', a'bb' \in F^2$
6. $abb', a'b' \in F^2$

Definition 4.1.11. *Let $\sim_1$ be a relation on $F^\times \times F^\times$ defined by $(a, a') \sim_1 (b, b')$ if $ab, a'b' \in F^2$. This relation is clearly an equivalence relation. Note that $(F^\times \times F^\times)/\sim_1 \simeq F^\times/(F^\times)^2 \times F^\times/(F^\times)^2$*

Remark 4.1.12. *1. Note that $\sim$ is also the equivalence relation defined by $(a, a') \sim (b, b')$ if and only if at least one of the following is satisfied*

1. $(a, a') \sim_1 (b, b')$,
2. $(a, a') \sim_1 (b', b) \Leftrightarrow (a', a) \sim_1 (b, b')$
3. $(a, a') \sim_1 (b, bb') \Leftrightarrow (a, aa') \sim_1 (b, b')$
4. $(a, a') \sim_1 (bb', b) \Leftrightarrow (a', aa') \sim_1 (b, b')$
5. $(a, a') \sim_1 (b', bb') \Leftrightarrow (aa', a) \sim_1 (b, b')$
6. $(a, a') \sim_1 (bb', b') \Leftrightarrow (aa', a') \sim_1 (b, b')$

where each of those point are respectively equivalent to the point in the Definition 4.1.10.

Stellenbosch University https://scholar.sun.ac.za

2. $(a,a') \sim (b,b') \Leftrightarrow (a,a') \sim (b',b) \Leftrightarrow (a,a') \sim (b,bb') \Leftrightarrow (a,a') \sim (b',bb') \Leftrightarrow (a,a') \sim (bb',b) \Leftrightarrow (a,a') \sim (bb',b')$.

Lemma 4.1.13. *The relation $\sim$ is an equivalence relation.*

Proof. Let $(a,a'),(b,b'),(c,c') \in F^\times \times F^\times$

- Reflexitivity is clear
- Symmetry is not hard to prove from Remark 4.1.12 since $\sim_1$ is symmetric.
- Let $(a,a') \sim (b,b')$ and $(b,b') \sim (c,c')$. From Remark 4.1.12, $(a,a') \sim_1 (b_1,b_1')$ and $(c,c') \sim_1 (b_2,b_2')$ where $b_i \in \{b,bb',b'\}$ and $b_i' \in \{b,bb',b'\}\backslash\{b_i\}$ for $i=1,2$. Then, it is not hard to prove that $(b_1,b_1') \sim_1 (c_1,c_1')$ where $c_1 \in \{c,cc',c'\}$ and $c_1' \in \{c,cc',c'\}\backslash\{c_1\}$. This will conclude the proof of transitivity.

□

Lemma 4.1.14 (Definition)**.** *One can define an action of S_3 on $(F^\times \times F^\times)/\sim_1 \simeq F^\times/(F^\times)^2 \times F^\times/(F^\times)^2$. Given $\sigma \in S_3$ and $[(b,b')]_{\sim_1} \in (F^\times \times F^\times)/\sim_1$, we define $\sigma \cdot [(b,b')]_{\sim_1} := [(\sigma_{(b,b')}(b), \sigma_{(b,b')}(b'))]_{\sim_1}$ where $\sigma_{(b,b')}(b) = c$ and $\sigma_{(b,b')}(b') = d$ where $c,d \in \{b,b',bb'\}$ such that when b is identified with 1, b' with 2 and bb' with 3, c (resp. d) is the element of $\{b,b',bb'\}$ identified with $\sigma(1)$ (resp. $\sigma(2)$). We will denote the set of equivalence classes by $\frac{F^\times/(F^\times)^2 \times F^\times/(F^\times)^2}{S_3}$ and $O_{S_3}([(a,b)]_{\sim_1})$ the orbit of $[(a,b)]_{\sim_1}$ via this action.*

Proof. We start by showing that given $\sigma \in S_3$ and $(a,b) \in F^\times \times F^\times$, we to show that $\sigma([(a,b)]_{\sim_1})$ is well defined i.e $\sigma([(a,b)]_{\sim_1})$ does not depend on the choice of (a,b). Let $[(a,b)]_{\sim_1} = [(c,d)]_{\sim_1}$ then $ac, bd \in F^2$ hence $(ab)(cd) \in F^2$, now we want to prove that $[(a',b')]_{\sim_1} = [(c',d')]_{\sim_1}$ where $a' = \sigma_{[(a,b)]}(a)$, $b' = \sigma_{[(a,b)]}(b)$, $c' = \sigma_{[(c,d)]}(c)$ and $d' = \sigma_{[(c,d)]}(d)$, then

- if $\sigma(1) = 1$ then $a' = a$ and $c' = c$ hence $a'c' = ac \in F^2$
- if $\sigma(1) = 2$ then $a' = b$ and $c' = d$ hence $a'c' = bd \in F^2$
- if $\sigma(1) = 3$ then $a' = ab$ and $c' = cd$ hence $a'c' = (ab)(cd) \in F^2$

Similar arguments can be used to show $b'd' \in F^2$ by looking at possibilities of $\sigma(2)$, this proves $[(a',b')]_{\sim_1} = [(c',d')]_{\sim_1}$ so $\sigma([(a,b)]_{\sim_1})$ is indeed well defined. Let $\psi : S_3 \times (F^\times \times F^\times)/\sim_1 \to (F^\times \times F^\times)/\sim_1$ be defined by $\psi(\sigma, [(a,b)]_{\sim_1}) = \sigma([(a,b)]_{\sim_1})$. The fact that ψ is a group action follows from the fact that S_3 acts on $F^\times \times F^\times$.

□

Lemma 4.1.15. *We have the following natural bijection:*

$$(F^\times \times F^\times)/\sim \simeq \frac{F^\times/(F^\times)^2 \times F^\times/(F^\times)^2}{S_3}$$

Proof. Let $\phi : (F^\times \times F^\times)/\sim \to \frac{F^\times/(F^\times)^2 \times F^\times/(F^\times)^2}{S_3}$ be defined by $\phi([(a,b)]_\sim) = O_{S_3}([(a,b)]_{\sim_1})$. We start by showing that ϕ is well defined. Let $[(a,b)]_\sim = [(c,d)]_\sim$. Then, by Remark 4.1.12, there exists $c',d' \in \{c,d,cd\}$ such that $[(a,b)]_{\sim_1} = [(c',d')]_{\sim_1}$ where $c' = \sigma_{(c,d)}(c)$, $d' = \sigma_{(c,d)}(d)$ for some $\sigma \in S_3$. Hence $\phi([(a,b)]_\sim) = O_{S_3}([(a,b)]_{\sim_1}) = O_{S_3}([(c,d)]_{\sim_1}) =$

Stellenbosch University https://scholar.sun.ac.za

$\phi([(c,d)]_\sim)$ proving that ϕ is well defined. It's clear that ϕ is surjective, so it remains to show that ϕ is injective. Let $\phi([(a,b)]_\sim) = \phi([(a,b)]_\sim)$ that is $O_{S_3}([(a,b)]_{\sim_1}) = O_{S_3}([(c,d)]_{\sim_1})$, this implies there exists $\sigma \in S_3$ such that $[(a,b)]_{\sim_1} = [(\sigma_{(c,d)}(c), \sigma_{(c,d)}(d))]_{\sim_1} = [(c',d')]_{\sim_1}$ where $c', d' \in \{c, d, cd\}$ and by Remark 4.1.12 we have that $[(a,b)]_\sim = [(c,d)]_\sim$ hence ϕ injective. □

We are aiming to use the above quotient to describe a bijective correspondance between the elementary abelian extension up isomorphism and a subset of this quotient. To do this, we can consider quartic elementary abelian extensions as compositum of two distinct quadratic extensions and identify them with the pair of corresponding parameters of those quadratics extension for some choosen radical generators. Following this identification, we need to exclude the following subset

$$S = \{[(a,a')]_\sim | a \in (F^\times)^2 \text{ or } a' \in (F^\times)^2 \text{ or } aa' \in (F^\times)^2\}$$

as it leads to a compositum of degree smaller than 4.

Lemma 4.1.16. *We have that*

$$S = \{[(1,a)]_\sim | a \in F^\times\} \simeq \frac{N}{S_3} \simeq F^\times/(F^\times)^2$$

where N is a subgroup $F^\times/(F^\times)^2 \times F^\times/(F^\times)^2$ isomorphic to $F^\times/(F^\times)^2$.

Proof. Note that 1 is a representative for a square in $F/(F^\times)^2$ and therefore

$$\begin{aligned} S &= \{[1,a]_\sim | a \in F^\times\} \cup \{[a,1]_\sim | a \in F^\times\} \cup \{[a,1/a]_\sim | a \in F^\times\} \\ &= \{[1,a]_\sim | a \in F^\times\} = \{[a,1]_\sim | a \in F^\times\} = \{[a,1/a]_\sim | a \in F^\times\} \end{aligned}$$

We can take $N = \{[1,a]_{\sim_1} | a \in F^\times\}$ (Note that we could have taken also to be either $\{[a,1]_{\sim_1} | a \in F^\times\}$ or$\{[a,1/a]_{\sim_1} | a \in F^\times\}$) and $\psi : \frac{N}{S_3} \to F/(F^\times)^2$ be defined as $\psi(O_{S_3}([(1,a)])) = a(F^\times)^2$. We will show that ψ is a group isomomorphsim. It is clear that ψ is well defined. Indeed, by definition, $O_{S_3}([(1,a)]_{\sim_1}) = O_{S_3}([(1,b)]_{\sim_1})$ implies $a(F^\times)^2 = b(F^\times)^2$ so ψ is indeed well defined. The fact that ψ is surjectivite and a group homormorphism is clear. The injectivity is the result of the definition of $\sim$ and Lemma 4.1.15.

□

Theorem 4.1.17. *[12, M. Cele, S. Marques] F is fixed and using the notation above. We have the following bijective correspondance:*

$$\{L/F \text{ elementary abelian extension}\}/\sim_{iso} \simeq \frac{[(F^\times/(F^\times)^2 \times F^\times/(F^\times)^2] - N}{S_3}$$

where $\sim_{iso}$ is the equivalence relation on the quartic extensions $L/F \sim_{iso} L'/F$ if L/F is F-isomorphic to L'/F.

Proof. Let us define the map

$$\psi : \{L/F \text{ elementary abelian extension}\}/\sim_{iso} \to \frac{(F^\times/(F^\times)^2 \times F^\times/(F^\times)^2) \backslash N}{S_3}.$$

For L/F be an elementary abelian extensions and $\alpha \in L$ be a biquadratic generator, then by Lemma 4.1.1 the minimal polynomial of α over F is $P(X) = X^4 - 2(a+b)X^2 + (a-b)^2$

Stellenbosch University https://scholar.sun.ac.za

for some $a, b \in F$ moreover we have $\gamma, \delta \in L$ such that $a = \gamma^2$, $b = \delta^2$ and $F(\gamma)$, $F(\delta)$, $F(\gamma\delta)$ are the quadratic sub-extensions of L/F. We define ψ as $\psi([L/F]_{iso}) = O_{S_3}([(a, b)])$. One can prove without much difficulty that ψ is well defined injection using Theorem 4.1.8 and Lemma 4.1.15. It remains to show that ψ is surjective. For any $O_{S_3}([a, b]) \in \frac{(F^\times/(F^\times)^2 \times F^\times/(F^\times)^2) \backslash N}{S_3}$, we have $\phi(F(\alpha)) = O_{S_3}([a, b])$ where α is a root of $P(X) = X^4 - 2(a+b)X^2 + (a-b)^2$ irreducible over F by Lemma 3.4.2 since $a, b,$ and ab are not squares in F, by Lemma 4.1.16.

□

Remark 4.1.18. *1. Let F be a field such that $-1 \notin F^2$, then there exists a one to one correspondence between the isomorphism class quartic radical elementary abelian extensions and the set*

$$\begin{aligned} & \{[(-1, a)]_\sim | a \in F^\times\} - (\{-1\} \times -(F^\times)^2 \cup \{-1\} \times (F^\times)^2) \\ = \; & \{[(-1, a)]_\sim | a \in F^\times\} - \{[(-1, 1)]_\sim, (-1, -1)]_\sim\} \\ \simeq \; & F^\times/{F^\times}^2 - \{-(F^\times)^2, (F^\times)^2\}. \end{aligned}$$

We note that the pair $(-1, 1)$ correspond to an extension defined by the minimal polynomial $X^4 + 4$.

2. When F is a field and $-1 \in F^2$, we observe again that in this situation, there is no radical elementary abelian extension (see also Theorem 4.1.4).

4.2 Elementary Abelian Closure

Remark 4.2.1. *Let L/F be a biquadratic extension admitting an elementary abelian closure E, Then any biquadratic generator α of L/F is a biquadratic generator of LE/E i.e $LE = E(\alpha)$ and $min(\alpha, F) = min(\alpha, E)$ where the second equality follows because $min(\alpha, F)$ and $min(\alpha, E)$ are both degree 4 monic elements of $E[X]$ having α as a root.*

Lemma 4.2.2. *[12, M. Cele, S. Marques] Let L/F be a biquadratic field extension and $\alpha \in L$ be a biquadratic generator with minimal polynomial $P(X) = X^4 + uX^2 + w$.*

1. *L/F admits a trivial elementary abelian closure if and only if $w \in F^2$.*
2. *If L/F admits an elementary abelian closure E, then $E = F(\eta)$ for some $\eta \in \overline{F}$ such that $\eta^2 = w$.*
3. *L/F admits an elementary abelian closure if and only if L/F is not cyclic.*

Proof. It follows from Lemma 3.4.1 and Theorem 4.1.1 that L/F has a unique quadratic sub-extension $M = F(\gamma)$ for some $\gamma \in L$ such that $\gamma^2 = u^2 - 4w$.

1. Follows from Theorem 4.1.1.
2. Suppose L/F admits an elementary abelian closure E. If $w \in F^2$ then $E = F$, also by Lemma 4.1.1 we have that L/F is elementary abelian, implying L/F has trivial elementary abelian closure hence the statements is true. Let L/F be an non-elementary abelian and η be an element in $\overline{F}$ such that $\eta^2 = w$. Note α is a biquadratic generator of LE/E and $P(X)$ is the minimal polynomial by Remark 4.2.1, hence $w \in E^2$ by Lemma 3.4.6 and $F(\eta) \subseteq E$. It follows from the minimality of degree of E over F such that $E = F(\eta)$.

Stellenbosch University https://scholar.sun.ac.za

3. $\Longrightarrow$ Suppose L/F does not admit an elementary abelian closure, then L/F is not elementary abelian and $w \notin F^2$ by Lemma 3.4.6. Let $\eta \in \overline{F}$ such that $\eta^2 = w$ then $E := F(\eta)$ is a quadratic extension, $E \subset L$. Indeed, $P(X)$ is reducible over E otherwise $LE = E(\alpha)$ is quartic extension over E and elementary abelian by Lemma 3.4.6, contradicting that L/F does not admit an elementary abelian closure. From Lemma 3.4.2 we know that at least one the following statements is true

   a) $u^2 - 4w = -4(\beta^2 - \sigma(\beta)^2)^2 \in E^2$

   b) $-u + 2\sqrt{w} = 2(\beta + \sigma(\beta))^2 \in E^2$

   c) $-u - 2\sqrt{w} = -2(\beta - \sigma(\beta))^2 \in E^2$

   If $\delta \in E$ such that $\delta^2 = -u - 2\sqrt{w}$ (resp. $\delta^2 = -u + 2\sqrt{w}$) then δ is a root of $T(X) = X^4 + 2uX^2 + u^2 - 4w$. $T(X)$ is irreducible over F by Lemma 3.4.2 as $u^2 - 4w \notin F^2$ and $(2u)^2 - 4(u^2 - 4w) = 16w \notin F^2$ this implies $F(\delta)$ is a quartic extension of F contradicting that E is a quadratic extension of F. It follows that there exists $\theta \in E$ such that $\theta^2 = u^2 - 4w$, $F(\theta)$ is a quadratic extension as $u^2 - 4w \notin F^2$ by Lemma 3.4.2. Hence $F(\theta) = F(\eta)$ it follows from Theorem 2.1.2 that $\frac{u^2-4w}{w} \in F^2$ hence $w(u^2 - 4w) \in F^2$ proving that L/F is cyclic by Lemma 3.4.6.

   $\Longleftarrow$ Let L/F be cyclic. Suppose L/F admits an elementary abelian E, then $E = F(\eta)$ for some $\eta \in \overline{F}$ such that $\eta^2 = w$ by 2. Note that L/F cyclic implies $w \in L^2$ by Lemma 3.4.4, it follows that E is F-isomorphic to the quadratic sub-extension of L/F hence $P(X)$ is reducible over E and LE/E is not a quartic extension. This contradicts our assumption, hence L/F does not admit an elementary abelian.

□

Theorem 4.2.3. *[12, M. Cele, S. Marques] Let L/F and L'/F be biquadratic fields extensions admitting elementary abelian closure E and E' respectively. If α is a biquadratic generator of L/F and $\beta \in L'$ is a biquadratic generator of L'/F such that $min(\alpha, F) = P(X) = X^4 + uX^2 + w$ and $min(\beta, F) = Q(X) = X^4 + vX^2 + z$ then the following are equivalent*

1. *$L/F \cong L'/F$*
2. *$LE/E/F \cong L'E'/E'/F$*
3. *There exist $a, c \in F$ and $s, r \in \{1, -1\}$ such that $\frac{z}{w} = c^2$, $\frac{v^2-4z}{u^2-4w} = a^2$ and $\Omega = \frac{1}{2}\left(\frac{ra}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right) \in F^2$, when $\Omega = 0$, in addition, either $\frac{ra}{w} \in F^2$ or $ra \in F^2$.*

Proof. By Lemma 4.2.2, $E = F(\eta)$ for some $\eta \in E$ such that $\eta^2 = w$, similarly $E' = F(\epsilon)$ for some $\epsilon \in E'$ such that $\epsilon^2 = z$.

1. $\Longrightarrow$ 2. The isomorphism $L/F \cong L'/F$ extends to a isomorphism of $LE/E/F \cong L'E'/E'/F$, this follows from the uniqueness of the elementary abelian closure

2. $\Longrightarrow$ 1. Let $LE/E/F \cong LE'/E'/F$. This implies that $Q(X)$ is the minimal polynomial of some primitive element in LE. To show that $L/F \cong L'/F$ it suffice to prove that $Q(X)$ has a root in L. Let $\pm\alpha, \pm\delta$ be the roots of $P(X)$ in LE and $\pm\mu, \pm\kappa$ be the roots of $Q(X)$ in LE, such roots exist because LE/E is Galois. Let σ be the generator of $Gal(LE/L)$. We show that either $\sigma(\mu) = \mu$ or $\sigma(\kappa) = \kappa$. From

Stellenbosch University https://scholar.sun.ac.za

$\epsilon^2 = z = (\mu\kappa)^2$, $\eta^2 = w = (\alpha\delta)^2$, $-v = \mu^2 + \kappa^2$ and $-u = \alpha^2 + \beta^2$ we get that there exist $s_1, s_2 \in \{1, -1\}$ such that $\mu\kappa = s_1\epsilon$ and $\alpha\delta = s_2\eta$, now by Lemma 2.1.2 there exist $c \in F$ such that $\epsilon = c\eta$ so $\mu\kappa = c'\alpha\delta$ where $c' = cs_1s_2$. Up to changing the choice ϵ (resp η) of the root of $x^2 - z$ (resp. $x^2 - w$), we can assume $s_1 = s_2 = 1$. So that $\sigma((\mu-\kappa)^2) = \sigma(-v-2\epsilon) = -v+2\epsilon = (\mu+\kappa)^2$ hence $\sigma(\mu)-\sigma(\kappa) = \sigma(\mu-\kappa) = \pm(\mu+\kappa)$. Also $\sigma(\delta) = \sigma(\frac{\eta}{\alpha}) = -\frac{\eta}{\alpha} = -\delta$, hence $\sigma(\mu)\sigma(\kappa) = \sigma(\mu\kappa) = \sigma(c\alpha\delta) = -c\alpha\delta = -\mu\kappa$. If $\sigma(\mu) - \sigma(\kappa) = -(\mu+\kappa)$ then $\sigma(\mu)^2 + (\mu+\kappa)\sigma(\mu) + \mu\kappa = 0$ so $\sigma(\mu) = -\mu$ or $\sigma(\mu) = -\kappa$. Note that $\sigma(\mu) = -\kappa$ is not possible otherwise $\sigma(\kappa) = -\mu$, then $\mu\kappa = \frac{\sqrt{w}}{c} = \frac{\eta}{c}$ is fixed by σ contradicting that $w \notin L^2$. Now $\sigma(\mu) = -\mu$ implies $\sigma(\kappa) = \kappa$ from $\sigma(\mu\kappa) = -\mu\kappa$. Similarly $\sigma(\mu) - \sigma(\kappa) = \mu + \kappa$ implies $\sigma(\mu) = \mu$, so indeed either $\kappa \in L$ or $\mu \in L$ concluding the proof.

2. $\Leftrightarrow$ 3. Let $LE/E/F \cong L'E'/E'/F$. Since $E/F \cong E'/F$ is equivalent by Theorem 2.1.2 to the existence of $c \in F$ such that $\epsilon = c\eta$. By Theorem 4.1.8, $LE/E \cong L'E'/E'$ is equivalent to one of the following statements being true

(a) $\frac{-v-2c\eta}{-u-2s\eta} \in E^2$ for some $s \in \{1, -1\}$

(b) $\frac{-v-2c\eta}{u^2-4w} \in E^2$

We prove that (b) cannot be true since LE/E and $L'E'/E'$ are elementary abelian. We argue by contradiction, assuming that there exist $g, h \in F$ such that $\frac{-v-2c\eta}{u^2-4w} = (g + h\eta)^2$. Let σ be generator of $Gal(E/F)$, then $\sigma(\frac{-v-2c\eta}{u^2-4w}) = \frac{-v+2c\eta}{u^2-4w} = (g - h\eta)^2 \in E^2$ hence $E(\sqrt{-v-2c\eta}) \cong E(\sqrt{-v+2c\eta}) \cong E(\sqrt{u^2-4w})$, by Theorem 2.1.2, contradicting that $E(\sqrt{-v-2c\eta}), E(\sqrt{-v+2c\eta})$ are distinct quadratic sub-extensions of LE/E by Theorem 4.1.1. It follows that (a) is true, that is $m := \frac{-v-2c\eta}{-u-2s\eta} = (x + y\eta)^2$ for some $x, y \in E$. That is

$$\frac{(-v-2c\eta)(-u+2s\eta)}{u^2-4w} = x^2 + 4wy^2 + 2xy\eta$$

Equivalently,

$$uv - 4csw + 2\eta(cu - sv) = (x^2 + 4wy^2)(u^2 - 4w) + 2xy(u^2 - 4w)\eta$$

This is true if and only if $(x^2 + wy^2)(u^2 - 4w) = uv - 4csw$ and $cu - sv = xy(u^2 - 4w)$ $(*)$.

- when $cu = sv$, we have $\frac{v^2-4z}{u^2-4w} = c^2$, one could have
  - $x = 0$, then $wy^2(u^2 - 4w) = uv - 4csw$, that is $y^2 = \frac{uv-4csw}{w(u^2-4w)} = \frac{c}{sw}$ (In this case, $w^3y^4 = z$).
  - $y = 0$, then $x^2 = \frac{uv-4csw}{u^2-4w} = \frac{c}{s}$ $(wx^4 = z)$.

  (Note that both cannot be true simultaneously otherwise w would be a square, and L/F is not elementary abelian.)

- when $cu \neq sv$, We have $x = \frac{cu-sv}{y(u^2-4w)}$ and

$$y^4 + \frac{4wcs - vu}{w(u^2 - 4w)}y^2 + \frac{1}{w}\left(\frac{vs - uc}{4w - u^2}\right)^2 = 0,$$

Stellenbosch University https://scholar.sun.ac.za

so y is a root of $S(X) = X^4 + (\frac{4wcs-vu}{w(u^2-4w)})X^2\frac{1}{w}\left(\frac{vs-uc}{4w-u^2}\right)^2$.

Let $\Delta = \left(\frac{uv-4wcs}{w(u^2-4w)}\right)^2 - 4\left(\frac{1}{w}\left(\frac{vs-uc}{4w-u^2}\right)^2\right) = \frac{a^2}{w^2}$ then y is such that

$$y^2 = \frac{1}{2}\left(\pm\sqrt{\Delta} + \frac{uv-4wcs}{w(u^2-4w)}\right) = \frac{1}{2}\left(\pm\frac{a}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right).$$

Hence we have that either $\frac{1}{2}\left(\frac{a}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right) \in F^2$ or $\frac{1}{2}\left(-\frac{a}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right) \in F^2$.

Proving 3. (Note that given L/F as in the statement we cannot have $\frac{1}{2}\left(\frac{a}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right) \in F^2$ and $\frac{1}{2}\left(-\frac{a}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right) \in F^2$. Indeed, if that happens since

$$\frac{1}{2}\left(\frac{a}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right)\frac{1}{2}\left(-\frac{a}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right) = \frac{1}{w}\left(\frac{vs-uc}{4w-u^2}\right)^2$$

then w would be a square in F which is excluded in the assumption.)

3. $\Rightarrow$ 2. Given $a, c, d \in F$ and $s, r \in \{1, -1\}$ such that $\frac{z}{w} = c^2$, $\frac{v^2-4z}{u^2-4w} = a^2$ and $\frac{1}{2}\left(\frac{ra}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right) \in F^2$, we are looking for x and y in F satifying $(*)$. When $\Omega \neq 0$, we can take y such that $\frac{1}{2}\left(\frac{ra}{w} + \frac{uv-4wcs}{w(u^2-4w)}\right) = y^2$ and $x = \frac{cu-sv}{y(u^2-4w)}$ and when $\Omega = 0$, $\frac{ra}{w} + \frac{uv-4wcs}{w(u^2-4w)} = 0$ then $a = -\frac{uv-4wcs}{r(u^2-4w)}$ so that

$$a^2 = \frac{v^2-4z}{u^2-4w} = \left(\frac{uv-4wcs}{r(u^2-4w)}\right)^2$$

$$\begin{aligned}
&\Leftrightarrow (v^2-4z)(u^2-4w) = u^2v^2 - 8uvwcs + 16w^2c^2\\
&\Leftrightarrow u^2v^2 - 4zu^2 - 4wv^2 + 16wz = u^2v^2 - 8uvwcs + 16wz\\
&\Leftrightarrow zu^2 + wv^2 = 2uvwcs\\
&\Leftrightarrow \frac{z}{w}\left(\frac{u}{v}\right)^2 - 2\frac{u}{v}cs + 1\\
&\Leftrightarrow \left(c\frac{u}{v}\right)^2 - 2\frac{u}{v}cs + 1\\
&\Leftrightarrow (c\frac{u}{v} - s)^2 = 0 \Leftrightarrow cu = sv
\end{aligned}$$

If $cr \in F^2$, then x such that $x^2 = cr$ and $y = 0$ would be pairs of solution for $(*)$. Finally, if $\frac{cr}{w} \in F^2$, then y such that $y^2 = \frac{cr}{w}$ and $x = 0$ would be pairs of solution for $(*)$ concluding the proof of the theorem.

□

Remark 4.2.4. *Let L/F be a non-elementary abelian field extension, $y \in L$ be a biquadratic generator over F with minimal polynomial $P(X) = X^4 + uX^2 + w$. Let $E := F(\eta)$ where $\eta \in \overline{F}$ such that $\eta^2 = w$, then by Lemma 4.2.2 we have that E the elementary abelian closure of L/F, so LE/E is an elementary abelian extension and y is a biquadratic generator of LE/E. Note that $P(X) = X^4 - 2(a+b)X^2 + (a-b)$ where $a = \frac{1}{4}(-u - 2\eta)$ and $b = \frac{1}{4}(-u + 2\eta)$. Moreover by Theorem 4.1.1 there exists $\alpha, \beta \in LE$ such that $\alpha^2 = a$, $\beta^2 = b$ and $y = \alpha + \beta$. By Remark 4.1.9 we have that*

Stellenbosch University https://scholar.sun.ac.za

any biquadratic generator of LE/E is in $X := X_a \cup X_b \cap X_{ab}$ where $X_a = \{-\frac{(a+b)r}{2} - \frac{a+3b}{2(a-b)}y + \frac{r}{2}y^2 + \frac{s}{2(a-b)}y^3 | r, s \in E^\times\}$, $X_b = \{-\frac{(a+b)r}{2} + \frac{(3a+b)s}{2(a-b)}y + \frac{r}{2}y^2 - \frac{s}{2(a-b)}y^3 | r, s \in E^\times\}$ and $X_{ab} = \{\frac{r-s}{2(a-b)}y^3 + \frac{(3a+b)s-(a+3b)r}{2(a-b)}y | r, s \in E^\times\}$. We want to show that all biquadratic generators of L/F are in $X' := \{s\alpha + r\beta | r, s \in E^\times$ and $\sigma(s) = r\} \subset X_{ab}$ where σ is a generator of LE/L. Note that $\sigma(a) = b$ i.e $\sigma(\alpha)^2 = \sigma(\beta)^2$ hence $\sigma(\alpha) = \beta$ or $\sigma(\alpha) = -\beta$. Suppose $\sigma(\alpha) = -\beta$ then $\sigma(y) = \sigma(\alpha) + \sigma(\beta) = -(\alpha + \beta) = -y$ contradicting that $y \in L$ hence fixed by σ, so $\sigma(\alpha) = \beta$. Let $y' \in LE$ be a biquadratic generator of LE/E. If $y \in X_a$ then $y' = s\beta + r\alpha\beta$ for some $s, r \in E^\times$ so $\sigma(y') = \sigma(s)\alpha + \sigma(r)\alpha\beta \in X_b$ hence $\sigma(y') \neq y'$ so $y' \notin L$. Similarly if $y' \in X_b$ then $y' \notin L$. Now let $y' \in X_{ab}$ then $y' = s\alpha + r\beta$ for some $r, s \in E^\times$, so $\sigma(y') = \sigma(r)\alpha + \sigma(s)\beta$, it follows that $y' \in L$ if and only if $\sigma(s) = r$, that is if and only if $y' \in X'$ concluding the proof.

Definition 4.2.5. *Let E/F be a quadratic field extension, then $Gal(E/F) \cong S_2$. Let $\phi : S_2 \to Gal(E/F)$ be a group isomorphism, then S_2 act on $\frac{E^\times}{(E^\times)^2}$ by the group action $\tau : S_2 \times \frac{E^\times}{(E^\times)^2} \to \frac{E^\times}{(E^\times)^2}$ as $\tau(\sigma, x) = \phi(\sigma)(x)(E^\times)^2$.*

Lemma 4.2.6. *[12, M. Cele, S. Marques] Let F be field and $S \subset F^\times$ be a complete set of representatives of $\frac{F^\times}{(F^\times)^2} - \{(F^\times)^2\}$. Let $s \in S$ and $N_{F(\sqrt{s})} = \{\alpha \in (F(\sqrt{s}))^\times | \alpha\sigma(\alpha) \in (F(\sqrt{s})^\times)^2\}$ where σ is the generator of $Gal(F(\sqrt{s})/F)$. Then*

$$\{L/F \text{ non-Galois quartic extension}\}/\sim_{iso} \simeq \coprod_{s\in S} \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2}$$

Proof. Let $\psi : \coprod_{s\in S} \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2} \to \{L/F \text{ non-Galois quartic extension}\}/\sim_{iso}$ be defined as

$$\psi([(a + b\sqrt{s})(F(\sqrt{s})^\times)^2]_{S_2}) = [F(\beta)]_{iso}$$

where β is a root of $P(X) = X^4 - aX^2 + \frac{1}{4}b^2s$. Indeed, by Lemma 3.4.2, we have $F(\beta)$ is a biquadratic extension since $\alpha := a + b\sqrt{s} \notin N_{F(\sqrt{s})}$. Moreover, $s \notin F^2$ hence $F(\beta)$ is not elementary abelian by Lemma 3.4.6. In addition, $\alpha \notin N_{F(\sqrt{s})}$ implies $\frac{1}{4}b^2s(a^2 - b^2s) \notin F^2$. That is $F(\beta)$ is not a cyclic extension. As a consequence, $F(\beta)$ is non-Galois.

Now we show that ψ is well-defined. Let $[(a+b\sqrt{s})(F(\sqrt{s})^\times)^2]_{S_2}, [(a'+b'\sqrt{s'})(F(\sqrt{s'})^\times)^2]_{S_2} \in \amalg_{s\in S} \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2}$ such that $[(a + b\sqrt{s})(F(\sqrt{s}))^2]_{S_2} = [(a' + b'\sqrt{s'})(F(\sqrt{s'}))^2]_{S_2}$. We want to prove that $[F(\beta)]_{iso} = [F(\beta')]_{iso}$ where $\beta, \beta' \in \overline{F}$ are roots of $P(X) = X^4 - aX^2 + \frac{1}{4}b^2s$ and $P'(X) = X^4 - a'X^2 + \frac{1}{4}(b')^2s'$ respectively. Since $\sqrt{s} \in F(\sqrt{s'})$, by Theorem 2.1.2 and the definition of S, we have $s = s'$. In addition from $[(a + b\sqrt{s})(F(\sqrt{s}))^2]_{S_2} = [(a' + b'\sqrt{s'})(F(\sqrt{s}))^2]_{S_2}$, we also have that there exists $r \in \{1, -1\}$ such that $\frac{a+b\sqrt{s}}{a'+rb'\sqrt{s}} \in F(\sqrt{s})^2$. This implies that $\sigma(\frac{a+b\sqrt{s}}{a'+sb'\sqrt{s}}) = \frac{a-b\sqrt{s}}{a'-sb'\sqrt{s}} \in F(\sqrt{s})^2$. Therefore, it follows from Thereom 4.1.8 we have that $F(\sqrt{s})(\beta) \cong F(\sqrt{s})(\beta')$. Since by Lemma 4.2.2 we have that the elementary abelian closure of $F(\beta)$ (resp. $F(\beta')$) is $F(\sqrt{s})$ (resp. $F(\sqrt{s'})$), by Theorem 4.2.3, ψ is indeed well defined.

Suppose $\psi([(a+b\sqrt{s})(F(\sqrt{s})^\times)^2]_{S_2}) = \psi([(a'+b'\sqrt{s'})(F(\sqrt{s'})^\times)^2]_{S_2})$, that is $[F(\beta)]_{iso} = [F(\beta')]_{iso}$. Then, by Lemma 4.2.2 we have that $E = F(\sqrt{s}) \cong F(\sqrt{s'})$ is the elementary abelian closure of $F(\beta)$ and $F(\beta')$. By Lemma 4.2.3 we have that $\frac{a^2-b^2s}{(a')^2-(b')^2s'} \in F^2$ and $LE/E \cong L'E/E$. Hence, by Theorem 4.1.8, $[(a + b\sqrt{s})(F(\sqrt{s})^\times)^2]_{S_2} = [(a' + b'\sqrt{s'})(F(\sqrt{s'})^\times)^2]_{S_2}$. So ψ is injective.

Stellenbosch University https://scholar.sun.ac.za

Let L/F be a non-Galois biquadratic generator and $\beta \in L$ be a biquadratic generator with minimal polynomial $Q(X) = X^4 + uX^2 + w$. Since $w \notin F^2$ by Lemma 4.2.2, there exists a unique $s \in S$ such that $w = d^2 s$ for some $d \in F$. We have $-u - 2d\sqrt{s} \notin N_{F(\sqrt{s})}$, since $F(\sqrt{s})$ is the elementary abelian closure of L/F by Lemma 4.2.2. Now $\psi([(-u - 2d\sqrt{s})(F(\sqrt{s})^\times)^2]_{S_2}) = [F(\beta)]_{iso}$ □

Lemma 4.2.7. *Let F be a field and C be a compositum of all quadratic fields extensions of F. If G is a subgroup of $C^\times$ generated by F then relation $\sim_{Q^2}$ on $C^\times \times C^\times$ defined by $(a, a') \sim_{Q^2} (b, b')$ if*

1. *$a = b$ and $a' = b'$ or,*
2. *if $(a, a'), (b, b') \in F^\times \times F^\times$, then $\frac{a}{b} \in (F^\times)^2$ and $\frac{a'}{b'} \in (F^\times)^2$*
3. *if $a, b \in F(\delta)^\times - F^\times$ where $\delta^2 \in F^\times$, $\sigma(a) = a'$ and $\sigma(b) = b'$ where $Gal(F(\delta)/F) = <\sigma>$, then $\frac{a}{b} \in (F(\delta)^\times)^2$.*

Then $\sim_{Q^2}$ is an equivalence relation.

Proof. It follows from condition 1. that $\sim_{Q^2}$ is reflexive, so it remains to show that $\sim_{Q^2}$ is symmetric and transitive. Let $(a, a') \sim_{Q^2} (b, b')$, if 1. is satisfied then $(b, b') \sim_{Q^2} (a, a')$ by 1.. If 2. is satisfied then $\frac{b}{a} \in (F^\times)^2$ and $\frac{b'}{a'} \in (F^\times)^2$ as $a \neq 0$ and $b \neq 0$ so $(b, b') \sim_{Q^2} (a, a')$. If 3. is satisfied then $\sigma(a') = a$ and $\sigma(b') = b$ this follows from the fact that σ^2 is the identity automorphism in $Gal(F(\delta)/F)$, moreover $\frac{a}{b} \in (F(\delta)^\times)^2 \implies \frac{b}{a} \in (F(\delta)^\times)^2$. So $\sim_{Q^2}$ is indeed symmetric.

Let $(a, a') \sim_{Q^2} (b, b')$ and $(b, b') \sim_{Q^2} (c, c')$, if (a, a') and (b, b') satisfies 1. then (a, a') and (c, c') satisfies 1. as $(a, a') = (b, b')$. Similarly if (b, b') and (c, c') satisfies 1. then $(a, a') \sim_{Q^2} (c, c')$ as $(b, b') = (c, c')$.

If (a, a') and (b, b') satisfies 2. with (b, b') and (c, c') also satisfying 2. then $\frac{a}{c} = \frac{a}{b} \times \frac{b}{c} \in (F^\times)^2$ and $\frac{a'}{c'} = \frac{a'}{b'} \times \frac{b'}{c'} \in (F^\times)^2$ so $(a, a') \sim_{Q^2} (c, c')$.

If (a, a') and (b, b') satisfies 3. with (b, b') and (c, c') also satisfying 3.. Let $\delta \in C$ be a generator of the quadratic field extensions generated by a and b, then $(b, b') \sim_{Q^2} (c, c')$ implies c is a generator of $F(\delta)$. We now have $\sigma(a) = a'$, $\sigma(c) = c'$ and $\frac{a}{c} = \frac{a}{b} \times \frac{b}{c} \in (F(\delta)^\times)^2$ by so (a, a') and (c, c') satisfies 3..

Note that it's not possible to (a, a') and (b, b') satisfying 2. and also have (b, b') and (c, c') satisfying 3. (or vice vesa) as this would imply $a \in F^\times$ and $a \in C - F^\times$. It follows that $\sim_{Q^2}$ is transitive hence an equivalence relation. □

We have now classified all non-cyclic extensions, the following results allows us to see the classes of elementary abelian extensions and non-Galois extension as subset of a set.

Theorem 4.2.8. *[12, M. Cele, S. Marques] Let F be a field, C be the compositum of all quadratic field extensions over F, then*

$$\{\textit{non-cylic biquadratic extension}\}/\sim_{iso} \simeq \coprod_{s \in S} \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2} \coprod \frac{\frac{F^\times}{(F^\times)^2} \times \frac{F^\times}{(F^\times)^2} - N}{S_3}$$

where N is a subgroup of $\frac{F^\times}{(F^\times)^2} \times \frac{F^\times}{(F^\times)^2}$ isomorphic to $\frac{F^\times}{(F^\times)^2}$, Moreover, the right hand side can be naturally embedded into $\frac{\frac{C^\times \times C^\times}{\sim_{Q^2}}}{S_3}$ where $\sim_{Q^2}$ is defined in Definition 4.2.7 and S_3 act on $\frac{C^\times \times C^\times}{\sim_{Q^2}}$ similarly as defined in Lemma 4.1.14.

Stellenbosch University https://scholar.sun.ac.za

Proof. Let

$$\psi_{elem} : \{L/F \text{ elementary abelian extension of } F\}/\sim_{iso} \to \frac{\frac{F^\times}{(F^\times)^2} \times \frac{F^\times}{(F^\times)^2} - N}{S_3}$$

be the bijection defined in Theorem 4.1.17 defined in Theorem 4.1.17 and

$$\psi_{non\text{-}G} : \{\text{non-Galois biquadratic extension of } F\}/\sim_{iso} \longrightarrow \coprod_{s\in S} \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2}$$

be the bijection defined in Theorem 4.2.6. We now define

$$\psi : \{\text{non-cylic biquadratic extension of } F\}/\sim_{iso} \longrightarrow \coprod_{s\in S} \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2} \coprod \frac{\frac{F^\times}{(F^\times)^2} \times \frac{F^\times}{(F^\times)^2}}{S_3}$$

as follows, for each $[L/F]_{iso} \in \{\text{non-cylic biquadratic extension of } F\}/\sim_{iso}$ we set $\psi([L/F]_{iso}) = \psi_{elem}([L/F]_{iso})$ if L/F is elementary abelian and $\psi([L/F]_{iso}) = \psi_{non-G}([L/F]_{iso})$ if L/F is non-Galois, it's clear that ψ well-defined is a bijection since both ψ_{eleme} and ψ_{non-G} are bijections, also the right hand side has an empty intersection.

We now show $\coprod_{s\in S} \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2} \coprod \frac{\frac{F^\times}{(F^\times)^2} \times \frac{F^\times}{(F^\times)^2}}{S_3}$ can be embedded in $\frac{\frac{C^\times \times C^\times}{\sim_{Q^2}}}{S_3}$.

For each $s \in S$, let $\Delta_s : \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2} \longrightarrow \frac{\frac{F(\sqrt{s})^\times}{(F(\sqrt{s})^\times)^2} \times \frac{F(\sqrt{s})^\times}{(F(\sqrt{s})^\times)^2}}{S_3}$ defined by $\Delta_s([\alpha(F(\sqrt{s})^\times])^2]_{S_2} = [\alpha(F(\sqrt{s})^\times)^2, \sigma(\alpha)(F(\sqrt{s})^\times)^2]_{S_3}$ where σ is the generator of $Gal(F(\sqrt{s})/F)$.

To show Δ_s is well-defined, let $[\alpha(F(\sqrt{s})^\times)]_{S_2} = [\beta(F(\sqrt{s})^\times)^2]_{S_2}$, then $\alpha = \gamma^2\beta$ or $\alpha = \gamma^2\sigma(\beta)$ for some $\gamma \in F(\sqrt{s})^\times$. So if $\alpha = \gamma^2\beta$ then $\sigma(\alpha) = (\sigma(\gamma))^2\sigma(\beta) \implies \sigma(\alpha)(F(\sqrt{s})^\times)^2 = \sigma(\beta)(F(\sqrt{s})^\times)^2$ and $\alpha\sigma(\alpha) = (\gamma\sigma(\gamma))^2\beta\sigma(\beta)$ so $\alpha\sigma(\alpha)(F(\sqrt{s})^\times)^2 = \beta\sigma(\beta)(F(\sqrt{s})^\times)^2$ proving that $[(\alpha(F(\sqrt{s})^\times)^2, \sigma(\alpha)(F(\sqrt{s})^\times)^2)]_{S_3} = [(\beta(F(\sqrt{s})^\times)^2, \sigma(\beta)(F(\sqrt{s})^\times)^2)]_{S_3}$. We can prove the well definedness similarly when $\alpha = \gamma^2\sigma(\beta)$.

As for the injectivity, let $\Delta_s([\alpha(F(\sqrt{s})^\times)^2]_{S_2}) = \Delta_s([\beta(F(\sqrt{s})^\times)^2]_{S_2})$, then one of the following statements is true

(a) $\alpha(F(\sqrt{s})^\times)^2 = \beta(F(\sqrt{s})^\times)^2$

(b) $\alpha(F(\sqrt{s})^\times)^2 = \sigma(\beta)(F(\sqrt{s})^\times)^2$

(c) $\alpha(F(\sqrt{s})^\times)^2 = \beta\sigma(\beta)(F(\sqrt{s})^\times)^2$

If (a) or (b) is true then $[\alpha(F(\sqrt{s})^\times)^2]_{S_2} = [\beta(F(\sqrt{s})^\times)^2]_{S_2}$ and we are done. We will now see that (c) cannot be true. Indeed, if it was then $\alpha = \beta\sigma(\beta)\gamma^2$ for some $\gamma \in F(\sqrt{s})^\times$. Moreover, by Lemma 4.2.6 we have $Q(X) := X^4 - \frac{1}{2}(\alpha + \sigma(\alpha))X^2 + \frac{1}{16}(\alpha - \sigma(\alpha))^2$as a minimal polynomial of some biquadratic generator of over $F(\sqrt{s})$, but $(\frac{1}{2}(\alpha + \sigma(\alpha)))^2 - 4(\frac{1}{16}(\alpha - \sigma(\alpha))^2) = \alpha\sigma(\alpha) = (\beta\sigma(\beta)\gamma\sigma(\gamma))^2 \in F(\sqrt{s})^2$ contradicting the irreducibility of $Q(X)$ over $F(\sqrt{s})$ by Lemma 3.4.2. So indeed Δ_s is injective.

Those maps induce naturally an embedding

$$\Delta : \coprod_{s\in S} \frac{\frac{F(\sqrt{s})^\times - N_{F(\sqrt{s})}}{(F(\sqrt{s})^\times)^2}}{S_2} \coprod \frac{\frac{F^\times}{(F^\times)^2} \times \frac{F^\times}{(F^\times)^2}}{S_3} \longrightarrow \coprod_{s\in S} \frac{\frac{F(\sqrt{s})^\times}{(F(\sqrt{s})^\times)^2} \times \frac{F(\sqrt{s})^\times}{(F(\sqrt{s})^\times)^2}}{S_3} \coprod \frac{\frac{F^\times}{(F^\times)^2} \times \frac{F^\times}{(F^\times)^2}}{S_3}.$$

Stellenbosch University https://scholar.sun.ac.za

Finally, by definition of $\sim_{Q^2}$, we obtain a natural embedding

$$\iota : \coprod_{s\in S} \frac{\frac{F(\sqrt{s})^\times}{(F(\sqrt{s})^\times)^2} \times \frac{F(\sqrt{s})^\times}{(F(\sqrt{s})^\times)^2}}{S_3} \coprod \frac{\frac{F^\times}{(F^\times)^2} \times \frac{F^\times}{(F^\times)^2}}{S_3} \hookrightarrow \frac{\frac{C^\times \times C^\times}{\sim_{Q^2}}}{S_3}.$$

The embedding of the theorem is then the composite $\iota \circ \Delta$.

□

Stellenbosch University https://scholar.sun.ac.za

Chapter 5

Radical Closure For Non-elementary Abelian Extensions

In this section, we explore the existence of the radical closure. We start with classifying radical extensions and describe their moduli space.

The content in this section is work in progress by myself and Sophie Marques, by the time this work get published some results may have been improved. All the results presented here are new.

Lemma 5.0.1. *Let L/F and L'/F be two non elementary abelian radical extensions with radical generators $\alpha \in L$ and $\beta \in L'$ with minimal polynomial $P(X) = X^4 + a$ and $Q(X) = X^4 + b$ respectively. Then, the following statements are equivalent:*

1. *L/F is F-isomorphic to L'/F;*
2. *$b = d^4a^j$ where j is 1 or 3 and $d \in F$;*
3. *$d\beta^j$ is a radical generator with minimal polynomial $P(X)$ where j is 1 or 3 and $d \in F$.*

Proof. 1. $\Rightarrow$ 2. and 1. $\Rightarrow$ 3. Let $\phi : L \to L'$ Let $\beta' = \phi^{-1}(\beta)$, then $L = F(\beta')$ and $min(\beta', F) = Q(X)$. $F(\alpha^2)$ and $F((\beta')^2)$ are quadratic sub-extensions of L/F, by Theorem 4.1.1 and Lemma 3.4.1 we know L/F have a unique quadratic sub-extension hence $K := F(\alpha^2) = F((\beta')^2)$ so by Theorem 2.1.2 there exists $t \in F$ such that $(\beta')^2 = t\alpha^2$. Also α and β' are radical generator for the quadratic extension L/K with $min(\alpha, K) = X^2 - \alpha^2$ and $min(\beta, K) = X^2 - (\beta')^2$, by Theorem 2.1.2 $\beta' = k\alpha$ for some $k \in F(\alpha^2)$. Therefore e have $k = e\alpha^2 + f$ for some $e, f \in F$, and $(e\alpha^2 + f)^2 = t$ so that $e^2\alpha^4 + 2ef\alpha^2 + f^2 = t$ That is, $2ef\alpha^2 - e^2a + f^2 - t = 0$. That implies $e = 0$ or $f = 0$, since $\{1, \alpha^2\}$ is a basis over F.

- When $e = 0$ then $t = f^2$ and $\beta' = f\alpha$, implying that $b = f^4a$ and $f\beta$ is a generator with minimal polynomial $P(X)$
- When $f = 0$ then $\beta' = e\alpha^3$ implying that $b = e^2a^3$ and $f\beta^3$ is a generator with minimal polynomial $P(X)$.

Proving 2. and 3.

2. $\Leftrightarrow$ 3. is clear.

Stellenbosch University https://scholar.sun.ac.za

Finally, 3. $\Rightarrow$ 1. the well defined F-morphism from L to L' sending α to $d\beta^j$ is an isomorphism.

□

Definition 5.0.2. *One can defined a group action of U_4 on $F^\times/(F^\times)^4$ by as $\psi : U_4 \times F^\times/(F^\times)^4 \to F^\times/(F^\times)^4$ where $\psi(g,[a]) = [a^g]$.*

We leave to the reader to check that this map is well defined and indeed defines an action.

Lemma 5.0.3. *Let F be a field and $N = O_{U_4}([-4]) \cup \frac{(F^\times)^2/(F^\times)^4}{U_4}$, We have the following bijective correspondance:*

$$\{L/F \text{ radical quartic extension}\}/\sim_{iso} \simeq \frac{F^\times/(F^\times)^4}{U_4} - N$$

Moreover,

$$\{L/F \text{ radical elementary abelian quartic extension}\}/\sim_{iso} \simeq \frac{-(F^\times)^2/(F^\times)^4}{U_4} - \{O_{U_4}([-4])\}$$

Proof. Let $\phi : \{L/F \text{ radical quartic extension}\}/\sim_{iso} \to \frac{F^\times/(F^\times)^4}{U_4} - N$, be defined by $\phi([L/F]_{iso}) = O_{U_4}([a])$ by choosing a radical primitive element $\alpha \in L/F$ then observe that the with minimal polynomial of α over F is $P(X) = X^4 - a$ for some $a \in F$. Lemma 5.0.1 and Corollary 4.1.6 implies that $\phi([L/F]_{iso})$ does not depend on the choice of extension L/F and primitive element α, proving that L/F is well defined. By Lemma 3.4.2 we have that $P(X)$ is irreducible over F if and only if $a \notin F^2$ and $a \notin 4(F^\times)^4$. So $\phi([L/F]_{iso}) = O_{U_4}([a]) \notin N$. When $O_{U_4}([a]) \in \frac{F^\times/(F^\times)^4}{U_4} - N$ we have that $X^4 - a$ is irreducible over F hence generates a radical quartic extension L/F such that $\phi([L/F]_{iso}) = O_{U_4}([a])$ proving that ϕ is surjective. The injectivity of ϕ follows from Lemma 5.0.1 and Corollary 4.1.6, so ϕ is indeed a bijection. The remaining part of the lemma is a consequence of Lemma 3.4.6. □

Remark 5.0.4. *Note that using the notation of the previous Lemma, one can prove that*

$$N \cup \frac{-(F^\times)^2/(F^\times)^4}{U_4} = Fix_{U_4}(F^\times/(F^\times)^4)$$

In particular, $O_{U_4}([a]) = [a]$ for each $[a] \in N$.

Lemma 5.0.5. *Let L/F be a non-elementary abelian quartic extension, R be a radical closure of degree 2. Let σ be a generator of $Gal(LR/L)$ and $\beta \in LR$ a radical generator with radical polynomial $Q(X) = X^4 + a$. Then $\beta\sigma(\beta) \in F$ and $\beta + \sigma(\beta)$ is a biquadratic generator for L/F with minimal polynomial $P(X) = X^4 - 4dX^2 + (2d^2 + 2c)$ where $d = \beta\sigma(\beta)$ and $c = 1/2(a + \sigma(a))$.*

Proof. Let $\alpha = \beta + \sigma(\beta)$, we have $\sigma(\alpha) = \alpha$ so $\alpha \in L$. Note that $\alpha^2 = (\beta^2 + \sigma(\beta)^2) + 2d$ and $\alpha^4 = (-a - \sigma(a) + 2d^2) + 4d(\beta^2 + \sigma(\beta)^2) + 4d^2 = 4d(\beta^2 + \sigma(\beta)^2) + 6d^2 - 2c$ hence $\alpha^4 - 4d\alpha^2 + (2d^2 + 2c) = 0 = P(\alpha)$. To show that $P(X) \in F[X]$ it suffices to show that $d = \beta\sigma(\beta) \in F$, since $c \in F$ since it is in R and invariant by the action of σ. Note $\sigma(\beta)$ and β are both radical generators of LR/R. Hence by Lemma 5.0.1 and Corollary 4.1.6, $\sigma(\beta) = e\beta^j$ for some $e \in R$ and $j = 1$ or 3. Suppose $j = 1$ then

Stellenbosch University https://scholar.sun.ac.za

$\alpha = \beta + \sigma(\beta) = (e+1)\beta \in L$, but this is impossible since $(e+1)\beta$ is a radical generator of LR/R and L/F is not radical, so $\sigma(\beta) = e\beta^3$. Now $\beta\sigma(\beta) = e\beta^4 = -ae \in R$, so $\beta\sigma(\beta) \in L \cap R = F$, by Remark 3.2.9, so $P(X) \in F[X]$ as desired. Using the notation of Lemma 3.4.2 we have $P(X) = X^4 + uX^2 + w$ where $u = -4d = -4\beta\sigma(\beta)$ and $w = 2d^2 + 2c = (\beta^2 + \sigma(\beta)^2)^2$. We have $w \notin F^2$. Indeed, if $\beta^2 + \sigma(\beta)^2 = \beta^2(1 - ae^2) = f$ for some $f \in F$. Then β would be the root of a quadratic polynomial over R contradicting the definition of β.

By Lemma 3.4.2 we have that $P(X)$ is reducible over F if and only one of the following statement is true

1. $u^2 - 4w = -4(\beta^2 - \sigma(\beta)^2)^2 \in F^2$
2. $-u + 2\omega = 2(\beta + \sigma(\beta))^2 \in F^2$
3. $-u - 2\omega = -2(\beta - \sigma(\beta))^2 \in F^2$

where $\omega \in \bar{F}$ such that $\omega^2 = w$.

But 2. and 3. are not possible as $w \notin F^2$. Moreover, 1. cannot be true. Indeed, if it was $2i(\beta^2 - \sigma(\beta)^2) = 2i\beta^2(1 + e^2a) \in F$ where $i \in \bar{F}$ such that $i^2 = -1$. But since $1 + e^2a \neq 0$ as otherwise $-a$ is a square contradicting the irreducibility of $X^4 + a$. Now $2i\beta^2(1+e^2a) \in F \subset R$ implies that $i\beta^2 \in R$ so $-a \in R^2$, this contradicts the irreducibility of $Q(X)$ over R. We can therefore deduce the irreducibility of $P(X)$ over R.

□

Theorem 5.0.6. *Let L/F be a non-elementary abelian quartic field extension, $\alpha \in L$ be a biquadratic generator with minimal polynomial $P(X) = X^4 + uX^2 + w$ over F, R a radical closure when it exists, and $\Delta = -w(u^2-4w)$, then one of the following is satisfied:*

1. *The following statements are equivalent.*
   a) *L/F has a trivial radical closure.*
   b) *there exists $a, c, d \in F$ such that $2a(\alpha^2 + u/2) = (c + \alpha^2 d)^2\alpha^2$.*
   c) *Δ is a square in F.*
   d) *$-w \in L^2 - F^2$.*

   Any radical generators are of the form $\frac{1}{d}(\theta_i\alpha + \alpha^3)$ where $d \in F$, $i = 1, 2$ and θ_i is a root of $S(X) = uX^2 + (4w - 2u^2)X + u^3 - 3uw$.

2. *The following statement are equivalent*
   a) *L/F has no radical closure*
   b) *$\Delta \in L^2 - F^2$*
   c) *$-w \in F^2$.*

3. *L/F has a unique non-trivial radical closure $R := F(\epsilon)$ where $\epsilon^2 = \Delta$.*

In case 1. and 3., there exists a radical generator $\beta \in L$ with minimal polynomial $Q(X) = X^4 + (u^2 - 8w + 4\epsilon)$ where $\epsilon^2 = \Delta$ over R such that $\alpha = \beta - \frac{u}{4\beta}$ and $\beta = \frac{u}{2e}(\frac{u^2-2w+\epsilon}{u}\alpha + \alpha^3)$. When R is a non-trivial extension of F and σ is a generator of $Gal(LK/K)$ then $\alpha = \beta + \sigma(\beta)$. Note that $u = -4d$ and $w = 2d^2 + 2c$ where $d = \beta\sigma(\beta)$ and $d = \frac{1}{2}(\delta + \sigma(\delta))$. Moreover, $\frac{16\delta}{u^2}$ is a root of $T(X) = X^2 + \frac{2(8w-u^2)}{8u}X + 1$.

Stellenbosch University https://scholar.sun.ac.za

Proof. Note that L/F has a unique quadratic sub-extension M/F (see Theorem 4.1.1 and Lemma 3.4.1) and α^2 is a generator M with minimal polynomial X^2+uX+w, completing the square we get that $\gamma = 2\alpha^2+u$ is a radical generator for this extension with minimal polynomial X^2+4w-u^2, i.e $M = F(\gamma)$

1. $(a) \iff (b)$

   $\implies$ Let L/F be radical and $\beta \in L$ be a radical generator of L/F with minimal polynomial $Q(X) = X^4+r$ over F. So β^2 is a radical generator of a quadratic sub-extension of L/F, since there is only one such extension it follows that $M = F(\gamma) = F(\beta^2)$, hence by Theorem 2.1.2 there exists $a \in F$ such that $a^2(u^2-4w) = -r$ and $\beta^2 = 2a(\alpha^2+u/2)$. Moreover, $M(\alpha) = M(\beta)$ implies there exists $m \in M$ such that $\beta^2 = m^2\alpha^2$ by Theorem 2.1.2. From $\beta^2 = 2a(\alpha^2+u/2)$ and $\beta^2 = m^2\alpha^2$ we have $2a(\alpha^2+u/2) = m^2\alpha^2$. Since $\{1,\alpha^2\}$ is a bais of M over F, there exists $c,d \in F$ such that $m = c+d\alpha^2$, hence $a(2\alpha^2+u) = (c+d\alpha^2)^2\alpha^2$ as desired.

   $\impliedby$ Suppose there exists $a,c,d \in F$ such that $a(2\alpha^2+u) = (c+d\alpha^2)^2\alpha^2$. Let $\beta = (c+d\alpha^2)\alpha$ then L/F is radical with radical generator β with minimal polynomial $X^4-a^2(u^2-4w)$ over F.

   $(b) \iff (c)$

   Suppose there exists $a,c,d \in F$ such that $a(2\alpha^2+u) = (c+d\alpha^2)^2\alpha^2$. We know that $\alpha^4 = -w-u\alpha^2$, so that $(c+d\alpha^2)^2 = (c^2-d^2w)+(2cd-ud^2)\alpha^2$. Using those identities, we have

$$\begin{aligned}
&2a(\alpha^2+u/2) = (c^2-d^2w)\alpha^2+(2cd-ud^2)\alpha^4\\
\Leftrightarrow &2a\alpha^2+au = (c^2-d^2w)\alpha^2+(2cd-ud^2)(-w-u\alpha^2)\\
\Leftrightarrow &2a\alpha^2+au = (c^2-d^2w+u^2d^2-2cdu)\alpha^2+(d^2uw-2cdw)\\
\Leftrightarrow &0 = (c^2-d^2w+u^2d^2-2cdu-2a)\alpha^2+(d^2uw-2cdw-au)
\end{aligned}$$

   Since $\{1,\alpha^2\}$ is basis of M over F as a vector basis. Solving the equation above is equivalent to solving the system of equation

$$\begin{cases} d^2uw-2cdw-au &= 0\\ c^2-d^2w+u^2d^2-2cdu-2a &= 0 \end{cases}$$

   This becomes equivalent to $a = \frac{c^2-d^2w+u^2d^2-2cdu}{2}$ and

$$\begin{aligned}
d^2uw-2cdw-u(\frac{c^2-d^2w+u^2d^2+2cdu}{2}) &= 0\\
(\frac{3}{2}uw-\frac{1}{2}u^3)d^2+(u^2-2w)cd-(\frac{u}{2})c^2 &= 0\\
u(\frac{c}{d})^2+(4w-2u^2)(\frac{c}{d})+u^3-3uw &= 0
\end{aligned}$$

   so $\frac{c}{d}$ is a root of $S(X) = uX^2+(4w-2u^2)X^2+u^3-3uw$ in F. Indeed, $d \neq 0$, to see this suppose by contradiction that $d = 0$ we have $2a(\alpha^2+u/2) = c^2\alpha^2$ hence $(2a-c^2)\alpha^2+u/2 = 0$ but then $u/2 \neq 0$ implies $(2a-u^2) \neq 0$, hence α^2 is a root of a monic quadratic polynomial $X^2+\frac{u}{2(2a-c^2)}$, contradicting that the minimal

Stellenbosch University https://scholar.sun.ac.za

polynomial of α^2 is $X^2 + uX + w$. Now $S(X)$ has a root in F, this is true if and only if tje discriminant $-4w(u^2 - 4w)$ is a square in F, which is equivalent to Δ being a square in F.

$(c) \implies (d)$ Let $-w \in L^2 - F^2$, this implies there exists $\delta \in L$ such that $\delta^2 = -w$ and $F(\delta)$ is a quadratic sub-extension of L/F. Since L/F has a unique quadratic sub-extension we have that $F(\gamma) = F(\delta)$ so by Theorem 2.1.2 we have $\frac{u^2-4w}{-w} \in F^2$ hence $\Delta = -w(u^2 - 4w) \in F^2$.

$(d) \implies (c)$ Let $\Delta \in F^2$, then by Theorem 2.1.2 we have $F(\gamma) \cong F(\delta)$ for some $\delta \in \overline{F}$ such that $\delta^2 = -w$, proving that $-w \in L^2$.

From the above we have shown that any radical generator β is of the form $\beta = d\alpha^2 + c\alpha = d(\theta\alpha + \alpha^3)$ where $\theta = \frac{c}{d}$ is a root of $S(X) = uX^2 + (4w - 2u^2)X + u^3 - 3uw$. Hence radical generators are of the form $f(\theta_i\alpha + \alpha^3)$ where $f \in F$, $i = 1, 2$ and θ_i is a root of $S(X)$.

2. We will show that $(a) \iff (b) \iff (c)$.

   $(a) \implies (b)$ Suppose L/F does not admit a radical closure, then $\Delta \notin F^2$ by 1.. Let $\epsilon \in \overline{F}$ such that $\epsilon^2 = \Delta$ and $R := F(\epsilon)$. We argue by contradiction. Suppose $\epsilon \notin L$, then $L \cap R = F$. We claim that $P(X)$ is irreducible over R, by Lemma 3.4.2 that is all the following statements are true

   - $u^2 - 4w \notin R^2$
   - $-u - 2\omega \notin R^2$
   - $-u + 2\omega \notin R^2$

   where $\omega \in \bar{F}$ such that $\omega^2 = w$.

   If $u^2 - 4w \in R^2$ then $\gamma \in L \cap R$ contradicting that $L \cap R = F$. If $-u + 2\omega \in R^2$ then $R = F(\delta)$ for some $\delta \in \overline{F}$ such that $\delta^2 = -u + 2\omega$ so δ is a root of $Q(X) = X^4 + 2uX^2 + u^2 - 4w.Q(X)$ is irreducible by Lemma 3.4.2 as $u^2 - 4w \notin F^2$ and $(2u)^2 - 4(u^2 - 4w) = 16w \notin F^2$, similarly $-u - 2\omega \notin R^2$. Hence $P(X)$ is irreducible over F and LR/R is a radical quartic extension by 1., contradicting that L/F does not have a radical closure. So indeed Δ is a square in $L - F$. $(b) \implies (a)$ Let $\Delta \in L^2 - F^2$. Arguing by contradiction, we suppose that L/F admits a radical closure R, then by 1. we have $\Delta \in R^2$ so $L \cap R \neq F$ contradicting R is a radical closure by Remark 3.2.9. Hence L/F does not have a radical closure.

   $(b) \iff (c)$ Let $\epsilon \in \overline{F}$ such that $\epsilon^2 = \Delta$. Note that $\Delta \in L^2 - F^2$ if and only if $F(\epsilon) \cong F(\gamma)$ since $F(\gamma)$ is the unique quadratic sub-extension of L/F. It follows from Theorem 2.1.2 that $F(\epsilon) \cong F(\gamma)$ if and only if $-w \in F^2$.

3. Suppose 1 and 2 are not satisfied. Then L/F has a non-trivial radical closure R. Let $\epsilon \in \overline{F}$ such that $\epsilon^2 = \Delta$ and By 1. we have that $\epsilon \notin F$. Again by 1 we know that $\epsilon \in R$, we show claim that $F(\epsilon) = R$. It's clear that $F(\epsilon) \subseteq R$, suppose $R' := F(\epsilon) \subsetneq R$. Since $P(X)$ is irreducible over R we have that $P(X)$ is irreducible over R' and this implies $R'(\alpha)/R'$ is a quartic extension. $R'(\alpha)/R'$ is radical by 1. so K' is a radical closure of L/F, hence $R = R'$ by minimality of the degree of a radical closure.

Stellenbosch University https://scholar.sun.ac.za

Let R be the radical closure of L/F. Then $S(X) = uX^2+(4w-2u^2)X+u^3-3uw$ has a roots $\theta, \theta' \in R$. Also any radical generator of LR/R has the form $R(\theta\alpha+\alpha^3)$ or $r(\theta'\alpha+\alpha^3)$ for some $r \in R$. Consider the case when R/F is not trivial, in this case we have $\theta' = \sigma(\theta)$ where σ is a generator of $Aut(LR/L)$. To find radical generator β of LR/R we solve for $\alpha = b(\theta\alpha+\alpha^3)+\sigma(b(\theta\alpha+\alpha^3))$ which is equivalent to $(b\theta+\sigma(b\theta)-1)\alpha+(b+\sigma(b))\alpha^3 = 0$ so α is a root of $Q(X) = (b+\sigma(b))X^2+(b\theta+\sigma(b\theta)-1) \in R[X]$, but minimal polynomial of α over R has degree 4 so $Q(X) = 0$ that is $\sigma(b) = -b$ and $b(\theta-\sigma(\theta)) = 1$ which implies $b = \frac{1}{\theta-\sigma(\theta)}$. Hence $\beta := b(\theta\alpha+\alpha^3)$ is a desired radical generator. From Lemma 5.0.5 we have that $\sigma(\beta) = \frac{-u}{4\beta}$ hence $\alpha = \beta+\sigma(\beta) = \beta-\frac{u}{4\beta}$ as desired. Let $Q(X) = X^4+\delta$ be the minimal polynomial of β over K, then $\delta = -\beta^4 = b^4(\theta\alpha+\alpha^4) = -(-\frac{u^2}{4w(u^2-4w)})^2(\frac{w^2(u^2-4w)^2(4\theta-3u)}{u^3}) = -\frac{u(4\theta-3u)}{16}$ so $Q(X) = X^4-\frac{u(4\theta-3u)}{16}$.

Note that $\delta+\sigma(\delta) = \frac{8w-u^2}{8}$ and $\delta\sigma(\delta) = (\frac{u}{4})^4$, hence the minimal polynomial of δ over F is $X^2+\frac{8w-u^2}{8}X+(\frac{u}{4})^4$. It follows that $\frac{16\delta}{u^2}$ is a root of $X^2+\frac{2(8w-u^2)}{u}X+1$ as desired. □

Lemma 5.0.7. *Let L/F be a non-elementary abelian biquadratic field extension , $\alpha \in L$ be a biquadratic generator with minimal polynomial $P(X) = X^4+uX^2+w$. Let $\Delta = -w(u^2-4w)$, M be the unique quadratic sub-extension of L/F and $T(X) = X^2-\alpha X-\frac{u}{4}$ and β, β' the roots of $T(X)$ in $\bar{F}$. Then $L(\beta) = L(-w) = LR$ where $R = K(\epsilon)$ where $\epsilon^2 = -w(u^2-4w)$, then $\alpha = \beta+\beta'$ and $\beta^4 = \frac{1}{16}(u^2-8w\pm4\epsilon) \in R$.*

1. *When $\epsilon \in F$, then β radical generator of L/F*
2. *When $\epsilon \notin L$, then β radical generator of LR/R*

Proof. Note that $\gamma := 2\alpha^2+u \in L$ is a radical generator of M/F and $\gamma^2 = u^2-4w$. The roots of $T(X)$ in $\overline{L}$ are $\frac{\alpha^2\pm\eta}{2\alpha}$ where $\eta^2 = \alpha^2+u = \frac{-w}{\alpha^2}$ hence $T(X)$ has a root in L if and only if $-w \in L^2$.

1. Let $\epsilon \in F$ then by Theorem 2.1.2 we have $F(\eta) = F(\gamma)$ so $\eta = a\gamma = 2a\alpha^2+au$ for some $a \in F$ hence $-w = (a\gamma)^2 \in L^2$ proving that $\beta \in L$. The roots $\beta, \beta' = \frac{\alpha^2\pm\eta}{2\alpha}$ of $T(X)$ are in $L-M$, this follows from the fact that $\alpha^2 \pm \eta \in M$ and $2\alpha \in L-M$ so β and β' are generators of L/F. Now $\beta^2, (\beta')^2 = \frac{-(1\pm2a)(u\alpha^2+2w)}{4\alpha^2} \in M$ and $\beta^4, (\beta')^4 = \frac{(1\pm2a)^2(u^2-4w)}{16} = \frac{1}{16}(u^2-8w\pm4\epsilon)$ where $\epsilon^2 = \Delta$, so $\beta = \frac{\alpha^2+\eta}{2\alpha}$ (resp. $\beta' = \frac{\alpha^2-\eta}{2\alpha}$) has minimal polynomial $Q_1(X) = X^4-\frac{1}{16}(u^2-8w+4\epsilon)$ (resp. $Q_2(X) = X^4-\frac{1}{16}(u^2-8w-4\epsilon)$) over F.

2. Let $\epsilon \notin L$ then $\eta \notin L^2$ so $T(X)$ is irreducible over L. Then $L(\beta)$ is a quadratic extension of L and $L(\eta) = L(\beta)$. Let $\delta = \eta\gamma \in L(\beta)$ then $\delta^2 = \Delta$. We claim that $R := F(\delta)$ is a radical closure of L/F. It's clear thatr $R \not\subset L$ as $\gamma \in L$ and $\eta \notin L$ so $LR = L(\beta)$. We now show that $LR = R(\alpha)$, for this we show that $P(X)$ irreducible over R. Suppose $P(X)$ is reducible over R then by Lemma 3.4.2 at least one the following statements is true

   a) $u^2-4w \in R^2$

   b) $-u+\omega \in R^2$

   c) $-u-\omega \in R^2$

Stellenbosch University https://scholar.sun.ac.za

where $\omega \in \overline{F}$ such that $\omega^2 = w$.

If (a) is true then $F(\gamma) = R$ contradicting that $R \not\subset L$. If there exists $\theta \in R$ such that $\theta^2 = -u - 2\omega$ (resp. $\theta^2 = -u + 2\omega$) then θ is a root of $T(X) = X^4 + 2uX^2 + u^2 - 4w$. $T(X)$ is irreducible over F by Lemma 3.4.2 as $u^2 - 4w \notin F^2$ and $(2u)^2 - 4(u^2 - 4w) = 16w \notin F^2$ this implies $F(\theta)$ is a quartic extension of F contradicting that R is a quadratic extension of F. So indeed $P(X)$ is irreducible over R and $LR = R(\alpha)$. Now LR/R is quartic extension and $\delta^2 = -w(u^2-4w) \in R^2$ so LR/R is radical proving that R is a radical closure of L/F.

□

Lemma 5.0.8. *Let L/F be a cyclic biquadratic extension, then*

1. *L/F admits a trivial radical closure if and only if $-1 \in F^2$*
2. *L/F does not admit a radical closure if and only if $F(i)$ is the quadratic sub-extension of L/F where $i \in \overline{F}$ such that $i^2 = -1$.*

Proof. Let $\alpha \in L$ be a biquadratic generator with minimal polynomial $P(X) = X^4 + uX^2 + w$, and $\Delta = -w(u^2 - 4w)$. By Lemma 3.4.6, since L/F is cyclic, we have that $w(u^2 - 4w) \in F^2$.

1. By Lemma 3.4.6, we have that $w(u^2 - 4w) \in F^2$. Also by Theorem 5.0.6 L/F is radical if and only if $\Delta \in F^2$. Hence L/F is radical if and only if $-1 = \frac{\Delta}{w(u^2-4w)} \in F^2$.
2. By Theorem 5.0.6, we know L/F does not admit a radical closure if and only if $\Delta \in L^2 - F^2$, this is true if and only if $i \in L^2 - F^2$ if and only if $F(i)$ is a quadratic sub-extension of L/F.

□

Lemma 5.0.9. *Let L/F be quartic extension admitting a non-trivial radical closure R, then the following are equivalent*

1. *LR/R is an elementary abelian extension,*
2. *$R(i)$ is a quadratic sub-extension of LR/R.*
3. *L/F is an elementary abelian extension or $F(i)$ is a quadratic sub-extension of L/F. (Note that in the case L/F is not an elementary abelian extension.)*
4. *$L \cap R(i) \neq F$*

Proof. Let α be a biquadratic generator of L/F with minimal polynomial $P(X) = X^4 + uX^2 + w$, note $LR = R(\alpha)$ and $P(X)$ is the minimal polynomial of α over K.

We will prove that 1. $\iff$ 2. $\implies$ 3. $\implies$ 4. $\implies$ 1.

1. $\implies$ 2. Suppose LR/R is elementary abelian. LR/R is also radical hence $R(i)$ is quadratic sub-extension of LR/R by Theorem 4.1.4.

2. $\implies$ 3. Suppose that $R(i)$ is a quadratic sub-extension of LR/R and L/F is not elementary abelian. Then $w \notin F^2$ by Lemma 3.4.6. We can deduce that $R = F(\omega)$ where $\omega^2 = w$ since LR/R is elementary abelian. By Theorem 5.0.6, we have that $R = F(\gamma)$

Stellenbosch University https://scholar.sun.ac.za

where $\gamma^2 = -w(u^2 - 4w)$. Therefore, $F(\omega) = F(\gamma)$ hence $-(u^2 - 4w) \in F^2 \subset L^2$. We know that $u^2 - 4w \in L^2$ by Remark 3.4.3, that permits us to deduce that $i \in L$ proving that $F(i)$ is a quadratic sub-extension of L/F as $i \notin F$ as by assumption $i \notin R$.

3. $\implies$ 4. Suppose L/F is elementary abelian. Then $R = F(i\gamma)$ where $\gamma \in L$ is a radical generator of a quadratic sub-extension of L/F by Theorem 4.1.4. Hence $\gamma \in R(i)$, proving that $\gamma \in L \cap R(i)$ so $L \cap R(i) \neq F$. Now suppose $F(i)$ is a quadratic sub-extension of L/F. Then $L \cap R(i) = F(i)$.

4. $\implies$ 1. Suppose $L \cap R(i) \neq F$. If L/F is elementary abelian then $w \in F^2$ by Lemma 3.4.6, so $w \in R^2$ proving that LR/R is elementary abelian by Lemma 3.4.6. If L/F is not elementary abelian, we let $\delta \in L \cap R(i) - F$, so that $F(\delta)$ is quadratic sub-extension of L/F since L cannot be $R(i)$ as $L \cap R = F$. By Remark 3.4.3, $F(\gamma)$ is a quadratic sub-extension of L/F where $\gamma^2 = u^2 - 4w$. Hence $F(\gamma) = F(\delta)$ by Lemma 4.1.1. But then $R(\gamma) = R(i)$ and $-(u^2 - 4w) \in R^2$ by Theorem 2.1.2. Finally, as $-w(u^2 - 4w) \in R^2$ by Theorem 5.0.6, we deduce $w \in R^2$ proving that LR/R is elementary abelian by Lemma 3.4.6.

□

Stellenbosch University https://scholar.sun.ac.za

Conclusion

In this thesis, the bulk of work has been made in the pursuit of understanding the geometry of the moduli space of non-cyclic biquadratic extension through the elementary abelian closure. Even though it was very nice to be able to find two families of two parameters polynomials to describe all the quartic polynomials for future work. This taught us that the geometry roughty speaking consisted of a pair of elements in a quadratic extension of the base field together with a S_3 action. We could also identify an underlined multiplicative structure. It would be interesting to understand better how if and how this multiplicative structure translates in term of extension. The result that was essential to obtain this understand was the Theorem 4.2.3. It actually proved that we could descend our good understanding of the elementary abelian closure Theorem 4.1.8 through the elementary abelian closure. This left us with the question of the possible extension of these results to fields of higher degrees. Moreover, this work enable us to see classify uniformly all the non-cyclic extension and be able to think of them inside the same space (see Theorem 4.2.8). In the last chapter we started our work on the radical closure and also determined when it exists (see Theorem 5.0.6). It appears that there seem to be three worlds the one admitting an elementary abelian closure, the ones admitting a radical closure and the one admitting neither (very small and non existent for geometric biquadratic function fields extensions). Their intersection is also rare. So they seem to be almost complement of each others. It will be very interesting and informative to understand this better geometrically for biquadratic extensions and even general quartic. It would bring a more geometric global knowledge of the moduli space of quartic extensions.

Stellenbosch University https://scholar.sun.ac.za

Future Work

A first paper has been prepared together with this thesis and will appear very soon on the Arxiv (see [12]) In addition, this work offers a panel of different routes to follow in future works.

In particular, we intend to continue with the classification of quartic field extensions and classify all cyclic quartic field extensions, then study the moduli space of all quartic field extensions. The work can begin by investigating to see if radical descent is possible for quartic quartic field extension admitting a unique radical closure. Then study non-biquadratic field extension, investigating the existence and uniqueness of radical closure and elementary abelian closure.

The techniques explored in this thesis are generalizable to extensions of higher degree, hence may be useful in classifying field extensions of higher degree.

Stellenbosch University https://scholar.sun.ac.za

List of References

[1] H. Chu and M. Kang. Quartic fields and radical extensions. *J. Symb. Comput.*, 34:83–89, 2002.

[2] K Conrad. Galois groups as permutation groups. *Preprint*

[3] K Conrad. Galois groups of cubics and quartics. *Preprint*

[4] K Conrad. Galois groups of cubics and quartics(not in characteristic 2). *Preprint*

[5] S. Marques. Generic polynomials for cyclic function field extensions over certain finite fields. *European Journal of Mathematics*, 4(2):585–602, 2017.

[6] S. Marques and K. Ward. A complete classification of cubic function fields over any field. *Preprint*, 2017.

[7] S. Marques and K. Ward. Cubic fields: A primer. *Preprint, full version*, page 47, 2017.

[8] S. Marques and K. Ward. Cubic fields: A primer. *European Journal of Mathematics*, pages 1–20, 2018.

[9] S. Marques and K. Ward. An explicit triangular integral basis for any separable cubic extension of a function field. *European Journal of Mathematics*, pages 1–15, 2018.

[10] S. Marques and J. Ward. A complete study of the ramification for any separable cubic global function field. *Research in Number Theory volume 5, Article number: 36*, pages 1–15, 2019.

[11] V. Karemaker, S. Marques, J. Sijsling. Cubic function fields with prescribed ramification *Preprint*, 2020.

[12] S. Marques and M. Cele. The Geometry Of The Moduli Space Of non-cyclic Biquadratic Field Extensions *To appear soon on the Arxiv*

[13] M. Anderson *A First Course in Abstract Algebra. A First Course in Abstract Algebra. New York: Chapman and Hall/CRC*

[14] J. Milne. *Fields and Galois Theory. Fields and Galois Theory. London, Springer*, 2006

[15] J. Rotman. *Galois Theory. Galois Theory. Universitext. Springer, New York, NY*, 1998

Stellenbosch University https://scholar.sun.ac.za

[16] Q. Wu and R. Scheidler. An explicit treatment of biquadratic function fields. *Contributions to Discrete Mathematics [electronic only]*, 2, 01 2007.