Distribution Agreement

Yining Cheng April 10, 2017

The Artin-Schreier Theorem in Galois Theory

By

Yining Cheng

Suresh Venapally, Ph.D.
Advisor

Department of Mathematics and Computer Science

Suresh Venapally, Ph.D.
Advisor

Raman Parimala, Ph.D.
Committee Member

Ruixuan Liu, Ph.D.
Committee Member

2017

The Artin-Schreier Theorem in Galois Theory

By

Yining Cheng

Suresh Venapally, Ph.D.
Advisor

An abstract of
a thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2017

Abstract

The Artin-Schreier Theorem in Galois Theory

By Yining Cheng

We first list and state some basic definitions and theorems of the Galois theory of finite extensions, as well as state and prove the Kummer theory and the Artin-Schreier extensions as prerequisites. The main part of this thesis is the proof of the Artin-Schreier Theorem, which states that an algebraic closed field having finite extension with its subfield F has degree at most two and F must have characteristic 0. After the proof, we will discuss the applications for the Artin-Schreier Theorem.

The Artin-Schreier Theorem in Galois Theory

By

Yining Cheng

Suresh Venapally, Ph.D.
Advisor

A thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Sciences with Honors

Department of Mathematics and Computer Science

2017

Acknowledgements

I would like to thank Dr. Venapally for his supports and guidance as well as his time and patience on helping me write this paper. I also appreciate the help of Dr. Parimala and Dr. Liu for attending my thesis defense. Lastly, I want to thank my parents for supporting my college study that assists me to the completion of this thesis.

Contents

1 Introduction

Since elementary schools we start to solve quadratic polynomials, and as we approach high school and college, the polynomials become more and more complex and the roots of a polynomial change from simple integers to complex numbers. In field theory, we say that a field C is an algebraic closure of a field F if C is algebraic over F and every polynomial $f(x) \in F[x]$ splits over C. Simply, it can be seen as that C contains all roots of every polynomial whose coefficients are in field F. If we look at the fields $\mathbb{R}$ and $\mathbb{C}$, $\mathbb{R}$ is not algebraic closed since there are polynomials which do not have any root in $\mathbb{R}$; whereas $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, for that every polynomial $f(x) \in \mathbb{R}$ has all its roots in $\mathbb{C}$. Moreover, the characteristics of $\mathbb{R}$ and $\mathbb{C}$ are 0, meaning that none of their elements have multiples equal to 0 (i.e.,$nx \neq 0$, for all $x \in \mathbb{R}$). The degree of $[\mathbb{C} : \mathbb{R}] = 2$ because we can write $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$. In general, is there any other example of such relationship between a non-algebraic closed field and its algebraic closure that is a finite extension? The Artin-Schreier Theorem will answer this question, demonstrating that if F is not algebraic closed, and C is its algebraic closure which is its finite extension, then F must have characteristic 0 and C is of the form $F(i)$.

In section 2, we will recall basic definitions, state and prove important theorems in field theory and Galois theory following [2] and [1] as well as some significant lemmas toward the proof of the Artin Schreier theorem. In section 3 and 4, we will state and prove the Artin Schreier extension theorem and Kummer theory. In section 5, we will reproduce the Artin-Schreier Theorem following the proof of Keith Conrad in [3] by adding more detailed explanations from section 2, 3 and 4. In section 6, we will state and prove three simple corollaries as consequences of the Artin-Schreier Theorem.

2 Basic Definitions, Theorems, And Some Lemmas

2.1 Field Theory

Definition 2.1. *The characteristic of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char R.*

Theorem 2.2. *The characteristic of a field is 0 or a prime.*

Proof. Let F be a field with identity 1. If 1 has infinite order, then by definition there is no positive integer n such that $n \cdot 1 = 0$. Otherwise, suppose 1 has additive order n, then $n \cdot 1 = 0$, and n is the least positive integer with such property. So for any $x \in R$

$$\begin{aligned} n \cdot x &= (1 + 1 + \cdots + 1) \cdot x \quad (n \text{ summands}) \\ &= (n \cdot 1) \cdot x \\ &= 0x \\ &= 0 \end{aligned}$$

Thus, to show char F is a prime, it suffices to show that the additive order of 1 is finite and is a prime. Suppose 1 has additive order n and write $n = s \cdot t$. Then

$$0 = n \cdot 1 = (s \cdot t) \cdot 1 = (s \cdot 1) \cdot (t \cdot 1)$$

So either $s \cdot 1 = 0$ or $t \cdot 1 = 0$. But by assumption n is the least positive integer with $n \cdot 1 = 0$, so we must have either $s = n$ or $t = n$. Thus, n is a prime. □

Definition 2.3. *If K is a field containing a subfield F, then K is said to be an extension field (or simply an extension) of F, denoted as $K|F$.*

Definition 2.4. *A principal ideal domain is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some $a \in R$.*

Definition 2.5. *An integral domain D is a unique factorization domain if*

1. every nonzero element of D that is not a unit can be written as a product of irreducibles of D; and

2. the factorization into irreducibles is unique up to associates and the order in which the factors appear.

Theorem 2.6. *Let F be a field. Then F[x] is a principal ideal domain.*

Theorem 2.7. *Let F be a field and $p(x)$ be an irreducible polynomial. Then $\frac{F[x]}{<p(x)>}$ is a field.*

Theorem 2.8 (PID implies UFD)**.** *Every principal ideal domain is a unique factorization domain.*

Lemma 2.9. *Let p be a prime, then $x^{p^n} - y^{p^n} = (x-y)^{p^n}$.*

Proof. Proof by induction on n.

Base step: show $x^p - y^p = (x-y)^p$. Consider the following two cases:

Case 1: $p = 2$.

$$\begin{aligned}(x-y)^2 &= x^2 - 2xy + y^2 \\ &= x^2 + y^2 \\ &= x^2 - y^2 \ \ (\text{ since y}^2 = -\text{y}^2 \text{ in a field of characteristic 2})\end{aligned}$$

Case 2: $p \neq 2$ implies p is odd.

$$(x-y)^p = \sum_{k=1}^{p} \binom{p}{k} x^k y^{p-k} (-1)^k,$$

where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Therefore, for $k \neq 1$ *or* p, the coefficient of each term is a multiple of p and thus 0 in a characteristic p field. Hence, $(x-y)^p = x^p - y^p$.

Induction step: Suppose the induction hypothesis is true for $n-1$. Then

$$(x-y)^{p^{n-1}} = x^{p^{n-1}} - y^{p^{n-1}}.$$

So

$$(x-y)^{p^n} = [(x-y)^{p^{n-1}}]^p = (x^{p^{n-1}} - y^{p^{n-1}})^p = x^{p^n} - y^{p^n}.$$

Therefore, by induction, we have shown that $x^{p^n} - y^{p^n} = (x-y)^{p^n}$.

□

Lemma 2.10. *Let F be a field of char $p > 0$ and $a \in F$. If $a \notin F^p$, then $x^{p^n} - a$ is irreducible in F[x] for every $n \geq 1$.*

Proof. Proof by contrapositive.

Suppose $x^{p^n} - a$ is reducible in F[x] for some $n \geq 1$, show that $a \in F^p$.

First, note that by 2.1, since F is a field and p is positive, then p must be a prime.

Let $p(x) = x^{p^n} - a = f(x)g(x)$ for some monic polynomials $f(x), g(x) \in F[x]$. Let E be an extension field of F containing a root α in $p(x)$. So $\alpha^{p^n} = a$. By 2.9, we have $x^{p^n} - a = x^{p^n} - \alpha^{p^n} = (x-\alpha)^{p^n}$. Since E is a field, by 2.6, we know that E[x] is a PID, and by 2.8, we have E[x] a UFD. Since $f(x)$ *and* $g(x)$ are monic, and by 2.5, we can write $f(x) = (x-\alpha)^r$, where $0 < r < p^n$.

Let $r = p^t s$, where s is a non-zero integer, $p \nmid s$ *and* $t < n$.

Thus, $f(x) = (x^{p^t} - \alpha^{p^t})^s = x^{p^t s} - s\alpha^{p^t} x^{p^t s - 1} +$ lower order terms. Since $f(x) \in F[x]$, so $-s\alpha^{p^t} \in F$. Hence, $\alpha^{p^t} \in F$, which implies $a = (\alpha^{p^t})^{p^{n-t}} \in F^{p^{n-t}} \subseteq F^p$. □

Lemma 2.11. *Let F be a field in which -1 is not a square, and every element of F(i) is a square in F(i), where $i^2 = -1$. Then any finite sum of squares in F is again a square* *in F and F has characteristic 0.*

Proof. This is enough to prove that the sum of two squares is a square. Let $a, b \in F$. Since every element in F(i) is a square, there exists $c, d \in F$ such that $a+bi = (c+di)^2$. Then $a + bi = c^2 - d^2 + 2cdi$. This implies that $a = c^2 - d^2, d = 2cd$. So

$$\begin{aligned} a^2 + b^2 &= (c^2 - d^2)^2 + 4c^2d^2 \\ &= c^4 - 2c^2d^2 + d^4 + 4c^2d^2 \\ &= c^4 + 2c^2d^2 + d^4 \\ &= (c^2 + d^2)^2 \end{aligned}$$

Therefore, we have shown that the sum of two square is again a square.
If $char\ F = p > 0$, then $-1 = \sum_{i=1}^{n} 1$, if $1 + 1 + 1 + \cdots + 1 = 0$ (p summands), then $1 + 1 + 1 + \cdots + 1 = -1$ ($p - 1$ summands). Since 1 is a square in F, then the sum -1 is a square in F, which is a contradiction. Therefore, $char\ F = 0$. □

Definition 2.12. *The degree(or relative degree or index) of a field extension $K|F$, denoted [K:F], is the dimension of K as a vector space of F. The extension is said to be finite if [K:F] is finite and is said to be infinite otherwise.*

Theorem 2.13. *Let $F \subset K \subset E$ be fields, then*

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

Proof. First, note that extension degrees are multiplicative, so if one side of the equation is infinite, then the other side is also infinite. Suppose $[E : F] < \infty$, then [F : K] $<$ ∞ and [E : K] $< \infty$.

Now, we can assume $[E:K]=m<\infty,[K:F]=n<\infty$. Since $[E:K]=m$, then E is a vector space of K with dimension m. So $\exists\ \{\beta_1,\beta_2,\cdots,\beta_m\}\subset E$ a basis of $E|K$. Similarly, $\exists\ \{\alpha_1,\alpha_2,\cdots,\alpha_n\}\subset K$ a basis of $K|F$. We claim that

$$\{\alpha_i\beta_j\ |1\leq i\leq n, 1\leq j\leq m\}\ \text{ is a basis of E|F.}$$

Suppose

$$\sum_{i,j}a_{ij}\alpha_i\beta_j=0 \text{ for some } a_{ij}\in F.$$

Then

$$\sum_{j=1}^{m}(\sum_{i=1}^{n}a_{ij}\alpha_i)\beta_j=0,\ \text{ and }\ \sum_{i=1}^{n}a_{ij}\alpha_i\in K.$$

Therefore, because $\{\beta_1,\beta_2,\cdots,\beta_m\}$ is a basis of $E|K$ and thus linearly independent, we have that

$$\sum_{i=1}^{n}a_{ij}\alpha_i=0,\forall j=1,2,\cdots,m.$$

Since $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ is a basis of $K|F$, and so is linearly independent. Also, since $a_{ij}\in F$, we have that

$$a_{ij}=0,\forall i,j.$$

Therefore, $\{\alpha_i\beta_j\}$ is linearly independent over F.

Let $x\in E$. Since $\{\beta_1,\beta_2,\cdots,\beta_m\}$ is a basis of $E|K$, we can write $x=\sum_{j=1}^{n}\lambda_j\beta_j$ for some $\lambda_j\in K$. Since $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ is a basis of $K|F$, $\lambda_j=\sum_{i=1}^{n}a_{ij}\alpha_i$ for some $a_{ij}\in F$. Thus, we can write

$$x=\sum_{j=1}^{m}(\sum_{i=1}^{n}a_{ij}\alpha_i)\beta_j=\sum_{i,j}a_{ij}\alpha_i\beta_j.$$

Hence,$\{\alpha_i\beta_j\}$ spans E. Therefore, $\{\alpha_i\beta_j\ |1\leq i\leq n,1\leq j\leq m\}$ is a basis of $E|F$. Thus, $[E:F]=mn=[E:K][K:F]$. □

Definition 2.14. *If a field K is generated by a single element α over F, $K = F(\alpha)$, then K is said to be a simple extension of F and the element α is called a primitive element for the extension.*

Definition 2.15. *The element $\alpha \in K$ is said to be algebraic over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F (i.e., is not the root of any nonzero polynomial with coefficients in F) then α is said to be transcendental over F. The extension $K|F$ is said to be algebraic if every element of K is algebraic over F.*

Proposition 2.16. *If $K|F$ is a finite extension, then $K|F$ is algebraic.*

Proof. Suppose $[K : F] = n$, Let $\alpha \in K$, then $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ are linearly dependent (since the dimension is n, but the set has n+1 elements). Therefore,

$$b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0,$$

with $b_i's \in F$ not all 0. Thus, α is a root of the polynomial $b_0 + b_1x + \cdots + b_nx^n$. So α is algebraic over F. □

Definition 2.17. *Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root, and this polynomial is called the minimal polynomial for α over F.*

Definition 2.18. *The extension field K of F is called a splitting field for the polynomial $f(x) \in F[x]$ factors completely into linear factors (or splits completely) in K[x] and f(x) does not factor completely into linear factors over any proper subfield of K containing F.*

Theorem 2.19. *Let $\phi : F \simeq F'$ be isomorphisms of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying ϕ to the coefficients* *of $f(x)$. Let E be the splitting field for $f(x)$ over F and E' be the splitting field of $f'(x)$ over F'. Then there exists an extension of ϕ isomorphism $\sigma : E \longrightarrow E'$. In diagram*

$$\begin{array}{ccc} E & \xrightarrow{\exists\ \sigma} & E' \\ \Big| & & \Big| \\ F & \xrightarrow{\phi} & F' \end{array}$$

Proof. We will proceed the proof by induction on the degree n of $f(x)$.

Base step: n=1. Then $E = F, E' = F'$, so $\sigma = \phi$.

Induction step: Suppose the induction hypothesis is true for degree n-1. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$ of degree at least 2, and $p'(x)$ be the corresponding irreducible factor of $f'(x)$ in $F'[x]$ of degree at least 2.

If $\alpha \in E$ is a root to $p(x)$, and $\beta \in E'$ is a root to $p'(x)$, then we claim that $F(\alpha) \simeq \frac{F[x]}{<p(x)>}$ and $F(\beta) \simeq \frac{F'[x]}{<p'(x)>}$. Without loss of Generality, we will show $F(\alpha) \simeq \frac{F[x]}{<p(x)>}$.

First, note that $\frac{F[x]}{<p(x)>}$ is a field since $p(x)$ is irreducible, by 2.7. Let $\gamma : F[x] \longrightarrow F(\alpha)$. Since $p(\alpha) = 0$, then $p(x) \in ker(\gamma)$. Then by the First Theorem of Isomorphism, $\exists\ \psi : \frac{F[x]}{<p(x)>} \longrightarrow F(\alpha)$ a homomorphism. Furthermore, we know that $\frac{F[x]}{<p(x)>}$ is a field and $\psi \neq 0$, then ψ is an isomorphism since $F(\alpha)$ contains α and F implies that ψ is also surjective. Therefore, ψ is an isomorphism and $F(\alpha) \simeq \frac{F[x]}{<p(x)>}$.

Once we have $F(\alpha) \simeq \frac{F[x]}{<p(x)>}$ and $F(\beta) \simeq \frac{F'[x]}{<p'(x)>}$, since ϕ induces a natural isomorphism from $F[x]$ to $F'[x]$ which maps $< p(x) > \longrightarrow < p'(x) >$. Then we have the following diagram

$$\begin{array}{ccc} \frac{F[x]}{<p(x)>} & \xrightarrow{\phi} & \frac{F'[x]}{<p'(x)>} \\ \downarrow & & \downarrow \\ F(\alpha) & \xrightarrow{\exists\ \sigma'} & F(\beta) \end{array}$$

Therefore, $\exists$ an isomorphism σ' such that $\sigma' : F(\alpha) \simeq F(\beta)$.

Let $F_1 = F(\alpha)$ and $F_1' = F(\beta)$, so that we have the isomorphism $\sigma' : F_1 \longrightarrow F_1'$. By factoring, we have that $f(x) = (x - \alpha)f_1(x)$ over F_1 and similarly $f'(x) = (x - \beta)f_1'(x)$ over F_1', where $f_1(x), f_1'(x)$ have degree $n - 1$. Then E is a splitting field of $f_1(x)$ and similarly E' is also the splitting field of $f_1'(x)$. By induction hypothesis, there exists a map $\sigma : E \longrightarrow E'$ extending the isomorphism $\sigma' : F_1 \longrightarrow F_1'$. This gives the following diagram

$$\begin{array}{ccc} E & \xrightarrow{\ \sigma\ } & E' \\ | & & | \\ F_1 & \xrightarrow{\ \sigma'\ } & F_1' \\ | & & | \\ F & \xrightarrow{\ \phi\ } & F' \end{array}$$

□

Theorem 2.20 (Uniqueness of Splitting Fields). *Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.*

Proof. By previous theorem, let F maps to itself and E, E' be two splitting fields of $f(x) \in F[x]$ will do the proof. □

Definition 2.21. *An algebraic extension $K|F$ is called a normal extension if an irreducible polynomial $f(x) \in F[x]$ has a root in K and f(x) splits completely over K.*

Lemma 2.22. *Let F be a field of characteristic not equal to 2. Let $K|F$ be a quadratic extension (i.e. $[K : F] = 2$). Then $K = F(\sqrt{a})$ for some $a \in F$, which is not a square in F.*

Proof. Since $[K : F] = 2$, by 2.16, the field extension $K|F$ is algebraic. So we can let $\alpha \in K \backslash F$. By 2.17, $\exists$ a minimal polynomial $m_\alpha(x) = x^2 + bx + c$. Using quadratic formula, we obtain the roots $\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$. Note that $b^2 - 4c$ is not a square in F since $\alpha \notin F$. Then $\alpha \in F(\sqrt{b^2-4c})$ implies that $F(\alpha) \subseteq F(\sqrt{b^2-4c})$. Also, since $\sqrt{b^2-4c} = \mp(b+2\alpha)$, we have that $F(\sqrt{b^2-4c}) \subseteq F(\alpha)$. Therefore, $F(\alpha) = F(\sqrt{b^2-4c})$. Choose $a = b^2 - 4c$, we reach the conclusion. □

Definition 2.23. *A field K is called algebraically closed if every non-constant polynomial with coefficients in K has a root in K.*

Definition 2.24. *A polynomial over F is called separable if it does not have multiple roots (i.e. all its roots are distinct). A polynomial which is not separable is called inseparable.*

Definition 2.25. *A root α of $f(x) \in K$ is called a simple root if $(x-\alpha)^2 \nmid f(x)$.*

Lemma 2.26. *Let K be a field and let $f(x) \in K[x], \alpha \in K$, then α is a simple root of f(x) if and only if $f(\alpha) = 0$, $f'(\alpha) \neq 0$.*

Proof. Let $\alpha \in K$ *and* $f(\alpha) = 0$.
Suppose α is not a simple root of f(x), then $(x-\alpha)^2 | f(x)$, so we can write

$$f(x) = (x-\alpha)^2 g(x),$$

for some $g(x) \in F[x]$, Thus, $f'(x) = (x-\alpha)^2 g'(x) + 2(x-\alpha)g(x)$. so $f'(\alpha) = 0$.
Conversely, suppose α is a root of both $f(x)$ and $f'(x)$. Then we can write

$$f(x) = (x-\alpha)h(x),$$

for some $h(x) \in F[x]$. Take the derivative of f(x):

$$f'(x) = h(x) + (x-\alpha)h'(x).$$

Since α is a root to $f'(x)$, the equation above implies that $h(\alpha) = 0$, so we can write

$$h(x) = (x - \alpha)k(x),$$

for some $k(x) \in F[x]$. Thus,

$$f(x) = (x - \alpha)^2 k(x).$$

Therefore, α is not a simple root of f(x). □

Definition 2.27. *A field K of characteristic p is called perfect if every element of K is a p^{th} power in K, i.e. $K = K^p$. Any field of characteristic 0 is also called perfect.*

Proposition 2.28. *Every finite extension of a perfect field is separable.*

Proof. Let F be a finite field of *char* $p > 0$, and E be a finite extension of F with $[E : F] = n$. Then $|E| = p^n$. Therefore, $|E^*| = p^n - 1$, which implies that E is cyclic. Thus, for any nonzero element $\alpha \in E$, we have

$$\alpha^{p^n-1} = 1, \longrightarrow \alpha^{p^n} = \alpha, \longrightarrow \alpha^{p^n} - \alpha = 0.$$

Hence, any element in E is a root of the polynomial $f(x) = x^{p^n} - x$. Finally, to show f(x) is separable, note that $f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$ (i.e. By 2.26 $f'(x)$ has no roots at all so it has no multiple roots). Therefore, $E|F$ is separable. □

2.2 Galois Theory

Definition 2.29. *Let K/F be a field extension. Let Aut(K/F) denote the set of all F-automorphisms of K, that is, $Aut(K|F) = \{\phi \in Aut(K) : \phi_{|F} = id_F\}$. Then $Aut(K|F)$ is called the automorphism group of $K|F$ or the Galois group of $K|F$.*

Definition 2.30. *A finite extension $K|F$ is called Galois if it is normal and separable.*

Definition 2.31. *If H is a subgroup of the automorphism group of K, the subfield of K fixed by all elements of H is called the fixed field of H, and is denoted as K^H (i.e. $K^H = \{\alpha \in K | \sigma(\alpha) = \alpha\}$).*

Proposition 2.32. *Let $K|F$ be a finite extension, then there exists a finite normal extension $N|F$ such that $K \subset N$.*

Proof. Since $K|F$ is finite, we can write $K = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ for some $\alpha_i \in K$. Let $f_i(x) \in F[x]$ be the minimal polynomial of α_i over F. Let $f(x) = \prod_{i=1}^{n} f_i(x) \in F[x]$ and let $N|F$ be the splitting field of this $f(x)$ over F. Then $\alpha_1, \cdots, \alpha_n \in N$ implies that $K = F(\alpha_1, \cdots, \alpha_n) \subset N$, and $N|F$ is the normal extension. □

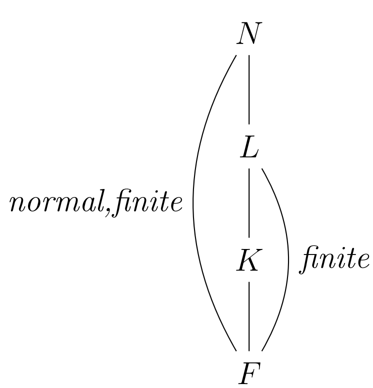
Theorem 2.33. *Let $N|F$ be a finite and normal extension, and let $L|F$ be a finite extension, then*

$$|\{\tau : K \longrightarrow N \mid \tau_F = id\}| * |\{\sigma : L \longrightarrow N \mid \sigma_K = id\}| = |\{\psi : L \longrightarrow N \mid \psi_F = id\}|,$$

denoted as the following:

$$|Hom_F(K, N)| * |Hom_K(L, N)| = |Hom_F(L, N)|.$$

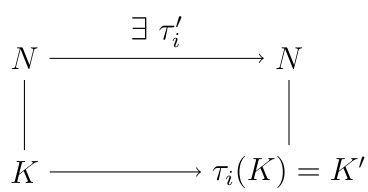
We can see more clearly by a diagram:



Proof. Since $N|F$ is finite, we have that $N|L$ and $N|K$ both finite. Then we suppose $Hom_F(K,N) = \{\tau_1, \cdots, \tau_m\}$ for some $m \in \mathbb{N}$, and $Hom_K(L,N) = \{\sigma_1, \cdots, \sigma_n\}$ for some $n \in \mathbb{N}$. We divide the proof into two parts.

Part (1): We show that $\forall\ \tau_i : K \longrightarrow N$ an F-isomorphism, $\exists\ \tau_i' : N \longrightarrow N$ such that $\tau_i'|_K = \tau_i$.

Since $N|F$ is normal and finite, then by 2.21, $N|F$ is a splitting field of some $f(x) \in F[x]$. Since $F \subset K \subset N$, the same polynomial $f(x)$ is also in $K[x]$, which implies that $N|K$ is a splitting field of $f(x)$. Then we denote $K' = \tau_i(K)$. Since $\tau_i(f(x)) = f(x)$ (note that τ_i is an F-isomorphism), then $N|K'$ is also a splitting field of $f(x)$. By uniqueness of splitting fields, $\exists\ \tau_i' : N \longrightarrow N$ an isomorphism such that $\tau_i'|_K = \tau_i$.



Part (2): Let $\phi : Hom_F(K,N) * Hom_K(L,N) \longrightarrow Hom_F(L,N)$ be a map such that $\phi(\tau_i, \sigma_j) = \tau_i' \circ \sigma_j$ for some $\tau_i \in Hom_F(K,N)$ and some $\sigma_j \in Hom_K(L,N)$. We claim that ϕ is a bijection.

First, we show that ϕ is one to one. Suppose $\phi(\tau_i, \sigma_j) = \phi(\tau_s, \sigma_k)$ for some $\tau_i, \tau_s \in Hom_F(K,N)$ and some $\sigma_j, \sigma_k \in Hom_K(L,N)$, then $\tau_i' \circ \sigma_j = \tau_s' \circ \sigma_k$. Let $\alpha \in K$, then since $\sigma_j|_K = \sigma_k|_K = id$, we have that $\sigma_j(\alpha) = \sigma_k(\alpha) = \alpha$. Then

$$\begin{aligned}
&\Rightarrow \quad (\tau'_i \circ \sigma_j)(\alpha) = (\tau'_s \circ \sigma_k)(\alpha) && (1)\\
&\Rightarrow \quad \tau'_i(\alpha) = \tau'_s(\alpha) && (2)\\
&\Rightarrow \quad \tau_i(\alpha) = \tau_s(\alpha) \text{ (since } \tau'_i|_K = \tau_i) && (3)\\
&\Rightarrow \quad \tau_i = \tau_s && (4)\\
&\Rightarrow \quad \tau'_i = \tau'_s && (5)\\
&\Rightarrow \quad \sigma_j = \sigma_k && (6)
\end{aligned}$$

Therefore, ϕ is one to one.

Now we will show that ϕ is surjective. Let $\theta \in Hom_F(L, N)$, then $\theta|_K \in Hom_F(K, N)$. This implies that $\theta|_K = \tau_i$ for some i. Consider the element $\tau_i'^{-1} \circ \theta$, then we will show that this element is in $Hom_K(L, N)$. Let $\alpha \in K$, then

$$(\tau_i'^{-1} \circ \theta)(\alpha) = \tau_i'^{-1}(\theta(\alpha)) = \tau_i'^{-1}(\tau_i(\alpha)) = \alpha.$$

Therefore, $\tau_i'^{-1} \circ \theta$ fixes any element in K, and thus $\tau_i'^{-1} \circ \theta \in Hom_K(L, N)$. So

$$\tau_i'^{-1} \circ \theta = \sigma_j \text{ for some } \sigma_j \in Hom_K(L, N).$$

Hence, ϕ is bijective and therefore

$$|Hom_F(K, N)| * |Hom_K(L, N)| = |Hom_F(L, N)|.$$

□

Theorem 2.34. *Let $\phi : F \simeq F'$ be isomorphisms of fields. Let E be a splitting field of $f(x)$ over F and E' be a splitting field of $f'(x) = \phi(f(x))$. Then the number of* *extensions satisfying that there exists an isomorphism between E and E' is at most* $[E : F]$*, with equality if* $f(x)$ *is separable over* F*.*

Proof. By 2.19, we know that $\exists$ an isomorphism $\sigma : E \longrightarrow E'$. So we will proceed by induction on $n = [E : F]$.

Base step: $n = 1$. Then $E = F, E' = F', \sigma = \phi$ and the number of such extension is 1.

Induction step: Suppose $n > 1$, then $f(x)$ has at least an irreducible factor $p(x)$ with degree at least 1 with corresponding irreducible factor $p'(x) \in F'[x]$ with degree at least 1. Then, by the proof of 2.19, if α is a root to $p(x)$, then $\exists\ \tau : F(\alpha) \simeq F'(\beta)$ with $\tau(\alpha) = \beta$. Then we have a diagram

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ | & & | \\ F(\alpha) & \xrightarrow{\tau} & F'(\beta) \\ | & & | \\ F & \xrightarrow{\phi} & F' \end{array}$$

Then we need only to count the number of such diagrams. The number of ϕ to τ is equal to the number of distinct roots of $p(x)$. Thus, since $deg(p(x)) = deg(p'(x)) = [F(\alpha) : F]$, we see that the number of such extensions is at most $[F(\alpha) : F]$, with equality if $p(x)$ is separable.

Since E is a splitting field of $f(x)$ over $F(\alpha)$ and E' is also a splitting field of $f'(x)$ over $F'(\beta)$. Then $[E : F(\alpha)] < [E : F]$ and by induction hypothesis, the number of such extensions is $\leq [E : F(\alpha)]$, with equality if $f(x)$ has distinct roots. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, the number of such extensions is $\leq [E : F]$, with equality if $f(x)$ has distinct roots. $\square$

Theorem 2.35. *Let* $K|F$ *be a finite extension and* $N|F$ *be a normal finite extension with* $K \subset N$*, then* $|Hom_F(K, N)| = [K : F]$ *if and only if* $K|F$ *is separable.*

Proof. $\Longleftarrow$ Suppose $K|F$ is separable. We will proceed by induction on the degree $[K : F] = n$.

Base step: n=1. Then $K = F$ and $|Hom_F(F, N)| = 1 = [F : F]$.

Induction step: Suppose the hypothesis is true for $n - 1$, where $n \geq 2$. Let $\alpha \in K \backslash F$. Let $m_\alpha(x)$ be the minimal polynomial of α over F. Since $N|F$ is normal and finite, by 2.16, $N|F$ is also algebraic. Thus, since $\alpha \in K \subset N$, $m_\alpha(x) \in F[x]$ is irreducible and $m_\alpha(\alpha) = 0$, we have that $m_\alpha(x)$ splits completely in N. Therefore, by 2.34,

$$|Hom_F(F(\alpha), N)| = \text{ number of distinct roots in } m_\alpha(x)$$

Since α is separable over F, then

$$\text{number of distinct roots in } m_\alpha(x) = deg(m_\alpha(x)) = [F(\alpha) : F].$$

Therefore, $|Hom_F(F(\alpha), N)| = [F(\alpha) : F]$. Since $[K : F(\alpha)] \leq [K : F]$, by induction hypothesis,

$$|Hom_{F(\alpha)}(K, N)| = [K : F(\alpha)].$$

By 2.33,

$$|Hom_F(F(\alpha), N)| * |Hom_{F(\alpha)}(K, N)| = |Hom_F(K, N)|.$$

Since $|Hom_F(F(\alpha), N)| = [F(\alpha) : F]$, and $|Hom_{F(\alpha)}(K, N)| = [K : F(\alpha)]$. then

$$[F(\alpha) : F] * [K : F(\alpha)] = |Hom_F(K, N)| = [K : F].$$

$\Longrightarrow$ Now suppose $|Hom_F(K,N)| = [K:F]$. Let $\alpha \in K \backslash F$. By 2.33,

$$|Hom_F(F(\alpha),N)| * |Hom_{F(\alpha)}(K,N)| = |Hom_F(K,N)| = [K:F].$$

Then

$$[K:F] = |Hom_F(F(\alpha),N)| * |Hom_{F(\alpha)}(K,N)| \leq [F(\alpha):F][K:F(\alpha)] = [K:F].$$

Therefore, α is separable over F. $\square$

Theorem 2.36 (Existence of Primitive Element). *Let $K|F$ be a finite separable extension. Then $K = F(\alpha)$ for some $\alpha \in K$.*

Proof. Let $N|K$ be an extension such that $N|F$ is normal (We know such extension exists from 2.32). Since $K|F$ is separable, by 2.35, we have that $|Hom_F(K,N) = [K:F]$.

Let $[K:F] = n$ and $Hom_F(K,N) = \{\sigma_1, \cdots, \sigma_n\}$ such that $\sigma_i \neq \sigma_j$ for $i \neq j$. Let $V_{ij} = \{\alpha \in K \ |\sigma_i(\alpha) = \sigma_j(\alpha)\}$. Since $\sigma_i \neq \sigma_j$, then V_{ij} is a proper subset of K. Since F is infinite,

$$\cup_{i \neq j} V_{ij} \subset K.$$

Let $\alpha \in K \backslash \cup_{i \neq j} V_{ij}$. We claim that $K = F(\alpha)$.

Let $m_\alpha(x)$ be the minimal polynomial of α over F, then $m_\alpha(\sigma_i(\alpha)) = 0, \forall\, i \in \{1, 2, \cdots, n\}$ (since σ_i only permutes the roots of $m_\alpha(x)$). Since $\alpha \notin \cup_{i \neq j} V_{ij}$, then $\forall i \neq j,\ \sigma_i(\alpha) \neq \sigma_j(\alpha)$. Therefore, $m_\alpha(x)$ has distinct roots, this implies that $deg(m_\alpha(x)) \geq n$. But $[K:F] = n$ and $\alpha \in K$ implies that $deg(m_\alpha(x)) \leq n$. Hence, $deg(m_\alpha(x)) = n$. So $[K:F] = [F(\alpha):F]$, and thus $K = F(\alpha)$.

$\square$

Theorem 2.37. *If $G \subseteq Aut(K)$ is a finite subgroup, then $K|K^G$ is a Galois extension with $Gal(K|K^G) = G$*

Proof. First note that by 2.31, $K^G = \{\alpha \in K \ |\sigma(\alpha) = \alpha \ , \ \forall \sigma \in G\}$. Let $G = \{\sigma_1 = id, \sigma_2, \cdots, \sigma_n\}$ and denote $F = K^G \subseteq K$. Let $\alpha \in K$. We can write

$$\{\sigma_i(\alpha) \ |\sigma_i \in G\} = \{\beta_1 = \alpha, \cdots, \beta_d\},$$

where $\beta_i \neq \beta_j, \ \forall i \neq j$. Let $f(x) = \prod_{i=1}^{d}(x - \beta_j) \in K[x]$. We claim that $f(x) \in F[x]$ and is irreducible.

Let $\tau \in G$, then the elements $\{\tau, \tau\sigma, \cdots, \tau\sigma_n\}$ are the same elements of $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$. Then it follows that applying τ to $\{\beta_1, \cdots, \beta_d\}$ simply permutes them. Therefore, $f(x)$ has coefficients which are fixed by all elements in G, so they are all in $K^G = F$. Hence, $f(x) \in F[x]$. Since $f(\alpha) = 0$, then α is algebraic over F. So we can let $m_\alpha(x)$ be the minimal polynomial of α over F. Therefore, $m_\alpha(\alpha) = m_\alpha(\sigma(\alpha)) = m_\alpha(\beta_i) = 0, \ \forall \ 1 \leq i \leq d$. Thus, $deg(m_\alpha(x)) \geq d$, implying that $m_\alpha(x) = f(x)$. Therefore, $f(x)$ is irreducible in $F[x]$. Since $f(x) = \prod_{i=1}^{d}(x - \beta_j)$ where $\beta_i \neq \beta_j, \ \forall \ i \neq j$. Hence, α is separable over F.

Now let $g(x) \in F[x]$ be an irreducible polynomial, and suppose $\exists \ \alpha \in K$ such that $g(\alpha) = 0$, then $g(x) = \lambda f(x) = \lambda \prod_{i=1}^{d}(x - \beta_j)$. Therefore, $f(x)$ splits completely in $K[x]$. By 2.21, $K|F$ is normal.

We know that for all $\beta \in K$, $deg_F\beta \leq |G|$. Let $\alpha \in K$ be such that $deg_F\alpha$ is maximal among all $deg_F\beta, \ \forall \ \beta \in K$. We claim that $K = F(\alpha)$.

Suppose in contrary that $K \neq F(\alpha)$, then $\exists \ \beta \in K \backslash F(\alpha)$. Hence, $F(\alpha, \beta)$ is a finite separable extension. By 2.36,

$$F(\alpha, \beta) = F(\gamma)$$

for some $\gamma \in K$. By 2.13,

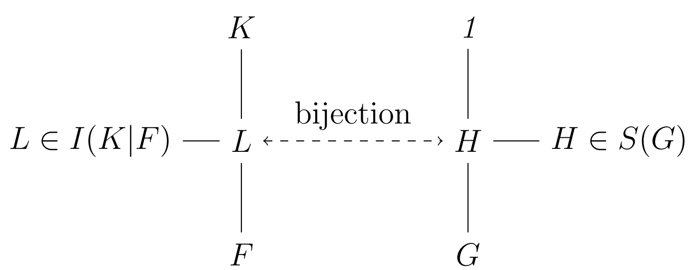
$$deg_F\gamma = [F(\gamma) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F].$$

Since $\beta \notin F(\alpha)$, we have that $[F(\alpha, \beta) : F(\alpha)] \geq 2$. Therefore, $deg_F\gamma \geq 2[F(\alpha) : F] = 2deg_F(\alpha) > deg_F(\alpha)$, which is a contradiction to $deg_F\alpha$ being maximal. So $K = F(\alpha)$. Hence, we have that $K|F$ is finite, separable and normal, so is Galois. Moreover, $[K : F] = [F(\alpha) : F] = deg_F\alpha \leq |G|$. Since $G \subseteq Gal(K|F)$, we have that

$$|G| \leq |Gal(K|F)| = [K : F] \leq |G|.$$

Therefore, $|G| = |Gal(K|F)|$, then $G = Gal(K|F)$. □

Theorem 2.38 (Fundamental Theorem of Galois Theory)**.** *Let $K|F$ be a Galois extension, and let $G = Gal(K|F)$. Define $S(G) =$ set of subgroups of G, and $I(K|F) =$ set of intermediate fields (i.e. $I(K|F) = \{L \mid F \subset L \subset K\}$). Then there is a bijection*



given by the correspondence

$$L \Longrightarrow \{\textit{the elements of } G \textit{ fixing } L\}$$

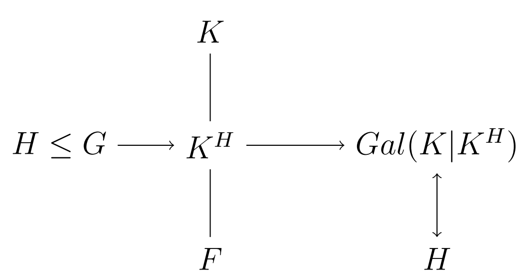
$$K^H \Longleftarrow H$$

which are inverses of each other. Under this correspondence:

(1) (inclusion reversing) If L_1, L_2 corresponds to H_1, H_2, respectively, then $L_1 \subset L_2$ if and only if $H_2 \leq H_1$.
(2)Let $H \in S(G)$, then H is a normal group in G if and only if $K^H|F$ is Galois (normal).
(3) If $F \subset L \subset K$ and $L|F$ is normal, then the natural map $Gal(K|F) \longrightarrow Gal(L|F)$ is onto with kernel $Gal(K|L)$.

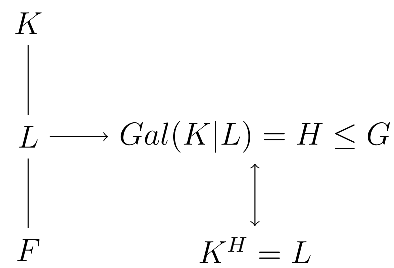
$$\frac{Gal(K|F)}{Gal(K|L)} \cong Gal(L|F).$$

Proof. For the purpose of this thesis, we will only prove that there is a bijection between the subfields L of K containing F and the subgroups H of G.
Define the map $\phi : S(G) \longrightarrow I(K|F)$ and $\psi : I(K|F) \longrightarrow S(G)$. To show there is a bijection, it is enough to show that $\phi \circ \psi = id_{I(K|F)}$ and $\psi \circ \phi = \mathrm{id}_{\mathrm{S(G)}}$. Since $H \leq G$, we have that $H \leq G = Gal(K|F) \subset Aut(K)$. Therefore, by 2.37, we have that $K|K^H$ is Galois with $H = Gal(K|K^H)$. Displaying an explicit diagram below,



hence, $\psi(\phi(H)) = H \Rightarrow \psi \circ \phi = id_{S(G)}$.
Now let $L \in I(K|F)$, then $F \subset L \subset K$. By 2.30, K is a splitting field of the separable polynomial $f(x) \in F[x]$, then we may also view $f(x)$ as an element of $L(x)$. Then K is also a splitting field of $f(x)$ over L, and thus the extension $K|L$ is also Galois. Let $H = Gal(K|L)$, then $L \subset K^H \subset K$ and $[K : L] = |H|$. Thus, $K|K^H$

is Galois with $Gal(K|K^H) = H$. So $[K : K^H] = |H| = [K : L]$, which implies $[K^H : L] = 1$, and thus $K^H = L$. Displaying an explicit diagram below,



therefore, $\phi \circ \psi = id_{I(K|F)}$.

□

Definition 2.39. *The extension $K|F$ is said to be cyclic if it is Galois with a cyclic Galois group.*

3 The Artin-Schreier Extension

Definition 3.1. *Let $K|F$ be a Galois extension and let $\alpha \in K$, define the trace of α from K to F to be $Tr_{K|F}(\alpha) = \sum_{\sigma \in Gal(K|F)} \sigma(\alpha)$.*

Lemma 3.2. *$Tr : K \longrightarrow F$ is an F-linear map.*

Proof. To show $Tr : K \longrightarrow F$ is an F-linear map, we need to show its additive and scalar multiplicative properties hold.

Let $\alpha, \beta \in K$, then we need to show that $Tr_{K|F}(\alpha+\beta) = Tr_{K|F}(\alpha) + Tr_{K|F}(\beta)$

$$\begin{aligned} Tr_{K|F}(\alpha+\beta) &= \sum_{\sigma \in Gal(K|F)} \sigma(\alpha+\beta) \\ &= \sum_{\sigma \in Gal(K|F)} (\sigma(\alpha)+\sigma(\beta)) \\ &= \sum_{\sigma \in Gal(K|F)} \sigma(\alpha) + \sum_{\sigma \in Gal(K|F)} \sigma(\beta) \\ &= Tr_{K|F}(\alpha) + Tr_{K|F}(\beta) \end{aligned}$$

Let $a \in F$, then

$$\begin{aligned} Tr_{K|F}(a\alpha) &= \sum_{\sigma \in Gal(K|F)} \sigma(a\alpha) \\ &= a \sum_{\sigma \in Gal(K|F)} \sigma(\alpha) \\ &= aTr_{K|F}(\alpha) \end{aligned}$$

□

Definition 3.3. *A character χ of a group G with values in a field L is a homomorphism from G to the multiplicative group of L:*

$$\chi : G \to L^x$$

i.e., $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$ and $\chi(g)$ is a nonzero element of L for all $g \in G$.

Theorem 3.4 (Dedekind Theorem)**.** *Let $\chi_1, \chi_2, \cdots, \chi_n$ be distinct characters of a group G with values in a field L. If $a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$, where $a_1, a_2, \cdots a_n \in L$, then $a_i = 0$ for all i.*

Proof. We will prove by induction on n.

Base step: $n = 1$, then $a_1 = 0$. The statement is true.

Induction step: Suppose the theorem is true for $n-1$, $n \geq 2$. Suppose $a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$, Since $\chi_i's$ are all distinct. So $\exists\, g_0 \in G$ such that $\chi_1(g_0) \neq \chi_n(g_0)$. Then

$$a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) = 0 \tag{7}$$

Multiply g by g_0, we have:

$$a_1\chi_1(gg_0) + a_2\chi_2(gg_0) + \cdots + a_n\chi_n(gg_0) = 0 \tag{8}$$

Since χ_i is a homomorphism, we have:

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \cdots + a_n\chi_n(g_0)\chi_n(g) = 0 \tag{9}$$

Multiply equation (7) by $\chi_1(g_0)$ on the left, we have:

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_1(g_0)\chi_2(g) + \cdots + a_n\chi_1(g_0)\chi_n(g) = 0 \tag{10}$$

Then equation (9) - equation (10), we have:

$$a_2\chi_2(g)(\chi_2(g_0) - \chi_1(g_0)) + \cdots + a_n\chi_n(g)(\chi_n(g_0) - \chi_1(g_0)) = 0 \tag{11}$$

By induction hypothesis, $a_2(\chi_2(g_0) - \chi_1(g_0)), \cdots, a_n(\chi_n(g_0) - \chi_1(g_0)) = 0$. Since $\chi_1(g_0) - \chi_n(g_0) \neq 0$, then $a_n = 0$. Therefore,

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_{n-1}\chi_{n-1} = 0$$

By induction hypothesis, $a_1 = a_2 = \cdots = a_{n-1} = a_n = 0$. □

Theorem 3.5 (Additive Hilbert's Theorem 90)**.** *Let $K|F$ be a cyclic extension of degree n with Galois group $G = Gal(K|F) =< \sigma >$. Then for $\beta \in K$*

$$Tr(\beta) = 0 \ if \ and \ only \ if \ \beta = \alpha - \sigma(\alpha) \ for \ some \ \alpha \in K.$$

Proof. $\Longleftarrow$ Let $\beta = \alpha - \sigma(\alpha)$, then

$$\begin{aligned} Tr(\beta) &= Tr(\alpha - \sigma(\alpha)) \\ &= Tr(\alpha) - Tr(\sigma(\alpha)) \\ &= \sum_{\sigma} \sigma(\alpha) - \sum_{\sigma} \sigma(\sigma(\alpha)) \\ &= 0 \end{aligned}$$

$\Longrightarrow$ Let $Tr(\beta) = 0$. By Dedekind Theorem, $Tr : K \longrightarrow F$ is a nonzero map, since $Tr = id + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$ is nonzero (with coefficients of each term being 1). Therefore, $\exists \ \theta \in K^*$ such that $Tr(\theta) \neq 0$.

Consider the function

$$\chi = \beta + (\beta + \sigma(\beta))\sigma + \cdots + (\sum_{i=0}^{n-2} \sigma^i(\beta))\sigma^{n-2}$$

Let $\alpha = \frac{\chi(\theta)}{Tr(\theta)}$, then

$$\alpha = \frac{1}{Tr(\theta)}(\beta\theta + (\beta + \sigma(\beta))\sigma(\theta) + \cdots + (\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta))\sigma^{n-2}(\theta) \qquad (12)$$

$$\sigma(\alpha) = \frac{1}{\sigma(Tr(\theta))}(\sigma(\beta)\sigma(\theta) + (\sigma(\beta) + \sigma^2(\beta))\sigma^2(\theta) + \cdots + (\sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{n-1}(\beta))\sigma^{n-1}(\theta) \qquad (13)$$

Note that $\frac{1}{\sigma(Tr(\theta))} = \frac{1}{Tr(\theta)}$. Then equation (12) - equation (13), we have

$$\begin{aligned}
\alpha - \sigma(\alpha) &= \frac{1}{Tr(\theta)}[\beta\theta + \beta\sigma(\theta) + \cdots + \beta\sigma^{n-2}(\theta) - (\beta + \cdots + \sigma^{n-1}(\beta))\sigma^{n-1}(\theta) + \beta\sigma^{n-1}(\theta)] \\
&= \frac{1}{Tr(\theta)}(\beta\theta + \beta\sigma(\theta) + \cdots + \beta\sigma^{n-1}(\theta) - Tr(\beta)\sigma^{n-1}(\theta)) \\
&= \frac{1}{Tr(\theta)}\beta Tr(\theta) \text{ (since Tr}(\beta) = 0 \text{ by assumption)} \\
&= \beta
\end{aligned}$$

□

Lemma 3.6. *Let $K|F$ be a cyclic extension of degree n. Let $\alpha \in K$, and $m_\alpha(x) = x^d + \alpha_{d-1}x^{d-1} + \cdots + \alpha_1 x + \alpha_0$ be the minimal polynomial of α over F, then $Tr_{K|F}(\alpha) = -\frac{n}{d}a_{d-1}$.*

Proof. Let $G = Gal(K|F) =< \sigma >$, consider:

$$\begin{aligned}
\prod_{\sigma \in G}(x - \sigma(\alpha)) &= x^n - (\sum_{\sigma \in G}\sigma(\alpha))x^{n-1} + \cdots \\
&= x^n - Tr_{K|F}(\alpha) + \cdots
\end{aligned}$$

Also,

$$\begin{aligned}
m_\alpha(x)^{\frac{n}{d}} &= (x^d + \alpha_{d-1}x^{d-1} + \cdots + \alpha_1 x + \alpha_0)^{\frac{n}{d}} \\
&= x^n + \frac{n}{d}a_{d-1}x^{n-1} + \cdots
\end{aligned}$$

Since we know that $\prod_{\sigma \in G}(x - \sigma(\alpha)) = m_\alpha(x)^{\frac{n}{d}}$, by equating the coefficients of x^{n-1}, we have that $Tr_{K|F}(\alpha) = -\frac{n}{d}a_{d-1}$. □

Theorem 3.7 (Artin-Schreier Extension)**.** *Let F be a field with characteristic $p > 0$ and let K be a cyclic extension of F of degree p. Then $K = F(\alpha)$, where α is a root of the polynomial $x^p - x - a$ for some $a \in F$.*

Proof. Let $K|F$ be a cyclic extension of degree p, and let $G = Gal(K|F) =< \sigma >$ for some $\sigma \in G^*$. Then by 3.6, $Tr(-1) = -p(1) = 0$ since $char\ F = p$. From Additive Hilbert's Theorem 90, we have that $-1 = \alpha - \sigma(\alpha)$, so $\sigma(\alpha) = \alpha + 1$. Moreover, $\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\alpha + 1) = \alpha + 2$. Hence, generally we have that $\sigma^i = \alpha + i$, for $i = 1, 2, \cdots, p$. Since $char\ F = p$, the elements $\alpha, \alpha + 1, \cdots, \alpha + p - 1$ are all distinct conjugates. Hence, $[F(\alpha) : F] = p = [K : F]$. So $K = F(\alpha)$. Furthermore, consider the element $\alpha^p - \alpha \in K$,

$$\sigma(\alpha^p - \alpha) = \sigma^p(\alpha) - \sigma(\alpha) = (\alpha + 1)^p - \alpha - 1 = \alpha^p + 1 - \alpha - 1 = \alpha^p - \alpha.$$

Thus, the element $\alpha^p - \alpha$ is fixed by σ, which implies that $\alpha^p - \alpha \in F$. Hence, let $a = \alpha^p - \alpha \in F$, then α is a root to the polynomial $x^p - x - a$.

□

4 Kummer Theory

Theorem 4.1 (Kummer)**.** *Let $K|F$ be a cyclic field extension of degree n, where char F does not divide n and F contains the n^{th} roots of unity, then $K = F(\sqrt[n]{a})$, for some $a \in F$.*

Proof. Let $K|F$ be a cyclic field extension of degree n and let $\rho \in F$ be the n^{th} root of unity. Since $(n, char(F)) = 1$, the elements $1, \rho, \rho^2, \cdots, \rho^{n-1}$ are all distinct. Suppose $G = Gal(K|F) =< \sigma >$, for some $\sigma \in G$, then $|G| = n$. Then for any $\sigma^i \in G,\ i \in \{1, 2, \cdots, n\}$, $\sigma^i : K^* \longrightarrow K^*$ is a homomorphism since $\sigma^i : K \longrightarrow K$ is a field automorphism. Therefore, σ^i is a characteristic of K^* with values in K. Hence, $\{id, \sigma, \cdots, \sigma^{n-1}\}$ are distinct characters of K^* with values in K. By Dedekind Theorem,

$$1 \cdot id + \rho\sigma + \cdots + \rho^{n-1}\sigma^{n-1} \neq 0.$$

Hence, $\exists\, \theta \in K^*$ such that $\theta + \rho\sigma(\theta) + \cdots + \rho^{n-1}\sigma^{n-1}(\theta) \neq 0$. Let $\beta = \theta + \rho\sigma(\theta) + \cdots + \rho^{n-1}\sigma^{n-1}(\theta)$. Then,

$$\sigma(\beta) = \sigma(\theta) + \rho\sigma^2(\theta) + \cdots + \rho^{n-1}\sigma^{n-1}(\theta). \tag{14}$$

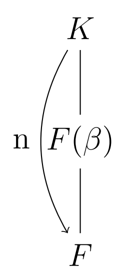
Multiply equation(14) by ρ, we have:

$$\rho\sigma(\beta) = \rho\sigma(\beta) + \rho^2\sigma^2(\theta) + \cdots + \rho^{n-1}\sigma^{n-1}(\theta) + \rho^n\sigma^n(\theta). \tag{15}$$

Since $\rho^n = 1$, and $\sigma^n = id$, then $\rho^n\sigma^n(\theta) = \theta$. Therefore, we have that $\rho\sigma(\beta) = \beta$. Hence, $\sigma(\beta) = \rho^{-1}\beta$. Then

$$\sigma(\beta^n) = \sigma^n(\beta) = \rho^{-n}\beta^n = \beta^n.$$

Therefore, $\sigma^i(\beta^n) = \beta^n$, for all $i \in \{1, 2, \cdots, n\}$, which implies that β^n is fixed by all elements of G. So $\beta^n \in F^*$. Write $a = \beta^n \in F^*$. We claim that $K = F(\sqrt[n]{a}) = F(\beta)$. Consider the diagram below:



We know that $[K : F] = n$, we need to show that $[F(\beta) : F] = n$. Since $\sigma(\beta) = \rho^{-i}(\beta)$, and ρ^{-i} are distinct for $i = 1, 2, \cdots, n$, then $\beta, \sigma(\beta), ..., \sigma^{n-1}(\beta)$ are all conjugates of β and are distinct. Therefore,

$$[F(\beta) : F] \geq n = [K : F] \geq [F(\beta) : F],$$

$$\Longrightarrow [F(\beta) : F] = n = [K : F].$$

Hence, $K = F(\beta) = F(\sqrt[n]{a})$. $\square$

5 The Artin-Schreier Theorem

Theorem 5.1 (The Artin-Schreier Theorem)**.** *Let C be algebraically closed with F a subfield such that $1 < [C : F] < \infty$. Then $C = F(i)$ where $i^2 = -1$, and F has characteristic 0. Moreover, for $a \in F$, exactly one of a or $-a$ is a square in F, and any finite sum of nonzero squares in F is again a nonzero square in F.*

Proof. We will divide the proof of the theorem to three steps.

Step I: Show that $C|F$ is Galois.

By 2.29, since we already have $[C : F] < \infty$, it is enough to show that $C|F$ is normal and separable. Since C is algebraic closed, by 2.21, we know that every nonconstant polynomial in C[x] has a root in C. Since every polynomial can be factored into irreducible factors and each factor has a root in C, this implies that every polynomial in C[x] has all roots in C. Therefore, every polynomial in C[x] splits completely in C and is normal.

To show that $C|F$ is separable, suppose $char\ F = p > 0$. It is suffices to show that F is perfect (i.e., $F = F^p$). If so, by 2.28, $C|F$ is separable. Suppose in contrary that $F \neq F^p$, then $\exists\ \alpha \in F \backslash F^p$. By 2.10, we know that $f(x) = x^{p^n} - \alpha$ is irreducible in F[x] for any $n \geq 1$, this implies that f(x) has a very large degree and thus has a very large algebraic extension, call it F_n such that $F_n \subseteq C$, which contradicts to that $[C : F] < \infty$.

Step II: Show [C:F]=2

Let $G = Gal(C|F)$, then $|G| = [C : F]$. Suppose in contrary that $|G| > 2$, then $|G|$

is divisible by 4 or by an odd prime. If $|G|$ is divisible by an odd prime, by Cauchy's theorem, G has a subgroup whose size is an odd prime; otherwise, if $|G|$ is not divisible by an odd prime, then $G = 2^r$ where $r \geq 2$, and thus is a p-group which has a subgroup of size 4. By Fundamental Theorem of Galois Theory, C has a subfield K containing F such that [C:K] is equal to 4 or an odd prime. Now replace K with F, we will show that [C:F] cannot be equal to 4 or an odd prime. Let's consider the following 2 cases:

Case 1: Suppose [C:F]=p, then $C|F$ is cyclic and so G is cyclic of order p. Let $G =< \sigma >$ for some $\sigma \in G^*$. So for any $a \in F$, $\sigma(a) = a$. Our goal is to show that p=2.

First, we will show that $char\ F \neq p$. Suppose in contrary that $char\ F = p$. By assumption $C|F$ is cyclic of order p and F has characteristic equal to p. Thus, by Artin-Schreier extension, $C = F(\alpha)$, where α is a root to the polynomial $x^p - x - a \in F[x]$. Since C is a simple extension of F, C has an F-basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{p-1}\}$. Therefore, for any element $b \in C$, we can write

$$b = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{p-1}\alpha^{p-1},$$

where $b_i's \in F$. Then

$$\begin{aligned} b^p - b &= \sum_{i=0}^{p-1}(b_i\alpha^i)^p - \sum_{i=0}^{p-1} b_i\alpha^i \\ &= \sum_{i=0}^{p-1} b_i^p(\alpha + a)^i - b_i\alpha^i \ (Since\ \alpha\ is\ a\ root\ to\ x^p - x - a, \alpha^p = \alpha + a) \\ &= (b_{p-1}^p - b_{p-1})\alpha^{p-1} + \text{ lower degree terms} \end{aligned}$$

Since C is algebraically closed, every nonconstant polynomial has a root in C. Consider the polynomial $x^p - x - a\alpha^{p-1}$, then it has a root b so that $b^p - b = a\alpha^{p-1}$.

Compare the right side of this equation to the equation above, the coefficients of α^{p-1} implies that

$$b_{p-1}^p - b_{p-1} = a, \Rightarrow b_{p-1}^p - b_{p-1} - a = 0, \Rightarrow b_{p-1} \text{ is a root of } x^p - x - a.$$

But $b_{p-1} \in F$ and $x^p - x - a$ is the minimal polynomial of α, and thus irreducible. So this is a contradiction. Therefore, $char\ F \neq p$.

Since $char\ F \neq p$, and C is an extension of F, $char\ C \neq p$. And since C is algebraically closed, C contains a primitive p^{th} root of unity, call it ρ. We will show that $[F(\rho) : F] \leq p - 1$. First, note that we have the factorization

$$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1).$$

Since $\rho \neq 1$, it follows that ρ is a root of the polynomial:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$$

So

$$[F(\rho) : F] \leq p - 1.$$

Since $[C : F] = p$, and $[C : F] = [C : F(\rho)][F(\rho) : F]$, so $p \leq [C : F(\rho)](p-1)$. Since p is a prime so either $[C : F(\rho)] = p$ or $p - 1 = p$, and the latter is clearly impossible. So $[C : F(\rho)] = p$ and $[F(\rho) : F] = 1$. Therefore, $\rho \in F$. Thus, we have that $C|F$ a cyclic extension of degree p and F contains a primitive p^{th} root of unity. By Kummer theory, we can write $C = F(\gamma)$, where $\gamma^p \in F$.

Let $\eta \in C$ be such that $\eta^p = \gamma$. So $\eta^{p^2} = \gamma^p \in F$. Therefore, $\sigma(\eta^{p^2}) = \sigma(\eta)^{p^2} = \eta^{p^2}$, which implies $\sigma(\eta) = \theta\eta$, where $\theta^{p^2} = 1$. Then, θ^p is either a primitive p^{th} root of unity or $\theta^p = 1$. First, let's consider the case when $\theta^p = 1$. Then

$$\sigma(\eta)^p = \eta^p, \Rightarrow \sigma(\eta^p) = \eta^p, \Rightarrow \eta^p = \gamma \in F$$

However, by assumption we have $\gamma \notin F$, which is a contradiction. Therefore, $\theta^p \neq 1$. Hence, θ^p has to be the primitive p^{th} root of unity and we have that $\theta^p \in F$. Therefore, $\sigma(\theta^p) = \theta^p = (\sigma(\theta))^p$. Since $\theta \in C$ and $char\ C \neq p$, we have

$$(\sigma(\theta))^p = \theta^p,$$

$$\sigma(\theta) = (\theta^p)^k \cdot \theta = \theta^{1+pk}$$

for some $k \in \mathbb{Z}$. Since $G =< \sigma >$, we have that $\sigma^p = id$. Then

$$\begin{aligned}
\eta &= \sigma^p(\eta) \\
&= \sigma^{p-1}(\sigma(\eta)) \\
&= \sigma^{p-1}(\theta\eta) \\
&= \sigma^{p-1}(\theta)\sigma^{p-1}(\eta) \\
&= \sigma^{p-1}\sigma^{p-2}(\sigma(\eta)) \\
&= \sigma^{p-1}\sigma^{p-2}(\theta)\cdots\sigma(\theta)\sigma(\eta) \\
&= \sigma^{p-1}\sigma^{p-2}(\theta)\cdots\sigma(\theta)\theta\eta \\
&= \theta\sigma(\theta)\cdots\sigma^{p-1}(\theta)\eta \\
&= \theta^{1+(1+pk)+\cdots+(1+pk)^{p-1}}\eta \text{ (since } \sigma(\theta) = \theta^{pk+1})
\end{aligned}$$

Since $\theta^{p^2} = 1$, we have the following sequence of congruence:

$$\begin{aligned}
1+(1+pk)+\cdots+(1+pk)^{p-1} &\equiv 0 \bmod p^2\\
\sum_{j=0}^{p-1}(1+pk)^j &\equiv 0 \bmod p^2\\
p+\sum_{j=0}^{p-1} jpk + (\text{ terms divisible by } p^2) &\equiv 0 \bmod p^2\\
p+\sum_{j=0}^{p-1} jpk &\equiv 0 \bmod p^2\\
p+pk\frac{(p-1)p}{2} &\equiv 0 \bmod p^2\\
1+k\frac{(p-1)p}{2} &\equiv 0 \bmod p.
\end{aligned}$$

Now we discuss the parity of p. Suppose p is odd, then $1+pkn \equiv 0 \ mod \ p$, for some $n \in \mathbb{N}$, which is impossible. Therefore, p is even (i.e., $p=2$), and k is odd.
Hence, the order of θ is $2^2 = 4$. So $\theta^4 = 1$ and $\sigma(\theta) = \theta^{1+2k} \neq \theta$. Thus, $\theta \notin F$, and we can write $\theta = i$. We then reach a conclusion that if $[C:F] = p$, then $[C:F] = 2$, $char\ F \neq 2, char\ C \neq 2$, and $C = F(i)$.

Case 2: Suppose $[C:F] = 4$, then $|G| = 4$. By Cauchy's Theorem, G has a subgroup of order 2. From the Fundamental Theorem of Galois Theory, there exists a subfield K of C such that $[C:K] = 2$. From above arguments we know that $i \notin K$. However, $F(i)$ is a subfield of C with $[C:F(i)] = 2$, and $i \in F(i)$, which is a contradiction to i not belong to a subfield of C. Therefore, $[C:F] \neq 4$.

Therefore, the above two cases have reached the following conclusion: If C is an algebraic closed field with F a subfield such that the extension degree is finite, then

$[C : F] = 2$, F and C do not have characteristic 2 and $i \notin F$. Hence, $C = F(i)$. By 2.11, we have that $char\ F = 0$.

Step III: Show that for $a \in F$, exactly one of a or $-a$ is a square in F, and any finite sum of nonzero squares in F is again a nonzero square in F.

We will prove by contradiction. Suppose that neither a nor $-a$ is a square in F, then $C|F(\sqrt{a})$ and $C|F(\sqrt{-a})$ are quadratic extensions by 2.22. Therefore, $C = F(\sqrt{a}) = F(\sqrt{-a})$. Hence, the ratio $\frac{a}{-a} = -1$ must be a square, otherwise $F(\sqrt{a}) \neq F(\sqrt{-a})$. As a consequence, $i \in F$, which contradicts to the previous conclusion in Step II. Therefore, exactly one of a or $-a$ is a square in F.

Let $b_1, b_2, \cdots, b_n$ be nonzero elements in F. Then by 2.11, $b_1^2 + b_2^2 + \cdots + b_n^2$ is again a square in F. Suppose in contrary that the sum is zero. Then

$$b_1^2 + b_2^2 + \cdots + b_n^2 = 0.$$

Divide each side by b_1^2 and rearrange the terms, we have

$$-1 = \frac{b_2^2}{b_1^2} + \cdots + \frac{b_n^2}{b_1^2}$$

This implies that -1 is the sum of squares and thus again is a square in F, which is a contradiction. So the sum of finite nonzero squares in F is a nonzero square. □

6 Applications

The Artin-Schreier theorem tells us that for an algebraic closed field C with a proper subfield F whose field extension is finite, the degree of such finite extension must be 2 and C is of the form $F(i)$ and F must have characteristic 0. We have seen a very common example of $\mathbb{C}|\mathbb{R}$, where we write $\mathbb{C} = \{a + bi \ |a, b \in \mathbb{R}, i^2 = -1\}$. For this example, $[\mathbb{C} : \mathbb{R}] = 2$ and $char\ \mathbb{R} = 0$, satisfying the main part of the Artin-Schreier theorem. Is there another example other than $\mathbb{C}|\mathbb{R}$? Yes, and in order to show another example, we will first state and prove two simple corollaries of the Artin-Schreier Theorem.

Corollary 6.1. *Let C be an algebraically closed field, and let $G \subseteq Aut(C)$ be a finite subgroup, then $|G| = 1$ or 2.*

Proof. Let $F = C^G$, then by theorem 2.37, $C|F$ is Galois and $G = Gal(C|F)$. By Artin-Schreier theorem, $|G| = [C : F] = 2$. □

Corollary 6.2. *Let C be an algebraically closed field, and let $\sigma \in Aut(C)$ and σ has finite order. Then $o(\sigma) = 1$ or 2.*

Proof. Let $G =< \sigma >$, then the result follows from Corollary 1. □

Now we can consider the following example. Consider the field $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \ |\alpha \text{ algebraic over } \mathbb{Q}\}$. Then $\bar{\mathbb{Q}}$ is algebraically closed. Consider the automorphism $\sigma : \bar{\mathbb{Q}} \longrightarrow \bar{\mathbb{Q}}$ givien by $\sigma(a + ib) = a - ib$. Then $o(\sigma) = 2$, by Corollary 2. Now we let $C = \bar{\mathbb{Q}}$ and $F = \bar{\mathbb{Q}}^{<\sigma>}$. Then $[C : F] = 2$.

Let's consider the last application of the Artin-Schreier Theorem.

Corollary 6.3. *Let C be an algebraically closed field. Let $\sigma_1, \sigma_2 \in Aut(C)$ be finite order elements such that $\sigma_1, \sigma_2 \neq id$ and $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$. Then $o(\sigma_1\sigma_2) = \infty$.*

Proof. Since $\sigma_1, \sigma_2 \neq id$ and has finite order, by Corollary 2, we know that $o(\sigma_1) = o(\sigma_2) = 2$. Suppose in contrary that $o(\sigma_1\sigma_2) < \infty$, then $o(\sigma_1\sigma_2) \leq 2$. Let's consider the following two cases:

Case 1: $o(\sigma_1\sigma_2) = 1$.

Then $\sigma_1 = \sigma_2^{-1}$. But since $o(\sigma_1) = o(\sigma_2) = 2$,

$$\sigma_1 = \sigma_1^{-1}, \sigma_2 = \sigma_2^{-1}.$$

Hence, $\sigma_1 = \sigma_2$, which implies $\sigma_1\sigma_2 = \sigma_2\sigma_1$, contradicting to the assumption.

Case 2: $o(\sigma_1\sigma_2) = 2$. Then

$$\sigma_1\sigma_2 = (\sigma_1\sigma_2)^{-1} \Longrightarrow \sigma_1\sigma_2 = \sigma_2^{-1}\sigma_1^{-1} \Longrightarrow \sigma_1\sigma_2 = \sigma_2\sigma_1.$$

Thus, both cases imply that $\sigma_1\sigma_2 = \sigma_2\sigma_1$, which is a contradiction. So $o(\sigma_1\sigma_2) = \infty$. $\square$

References

[1] David S. Dummit and Richard M. Foote *Abstract Algebra*. 3^{rd} ed., Laurie Rosarone, John Wiley and Sons, Inc, 2004.

[2] Joseph A. Gallian. *Comtemporary Abstract Algebra*. 8^{th} ed., Richard Stratton, Boston, Massachusetts, 2013.

[3] Keith Conrad: The Artin-Schreier Theorem, `http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/artinschreier.pdf`