GALOIS GROUPS AND P-CLOSURE OF A FIELD

TING GONG

Contents

1. Abstract

In abstract algebra, Galois theory has been a useful tool to connect field theory and group theory. With Galois theory, a lot of important theorems and applications could be proved, such as the Fundamental Theorem of Algebra, the proof to no formula for a polynomial equation higher than fifth power. This paper is going to present Galois Theory from scratch, and the goal of this paper is to venture into Infinite Galois Theory and explore the p-closure of a field.

2. Galois Theory from Scratch

This section introduces Galois Theory from scratch. Some knowledge in field theory and group theory are assumed.

Date: Started October 23, 2018. Last revision January 1, 2019.

2.1. **Splitting Field.**

Definition 2.1. The *field extension* of a field F is a field E that contains the field F.

Definition 2.2. Let E and F be fields, and $F \subseteq E$. The *degree* of E over F is the dimension of E of F-vector field, written as $[E : F]$.

Definition 2.3. We say a field extension being *finite* if $[E : F] < \infty$.

Remark 2.4. We call a field E being a field extension of F generated over F by α, and it is written as $F(\alpha)$. And we call α as the *adjunction* of F.

Proposition 2.5. *(Tower Rule) Let $F \subseteq E \subseteq K$ be fields. Then*

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

Proof. Assume $[K : E] = n$, and $[E : F] = m$. It suffices to prove $[K : F] = mn$. Pick $\{\alpha_1, \alpha_2 ... \alpha_n\}$ be a basis over E, and $\{\beta_1, \beta_2 ... \beta_m\}$ be a basis over F. Take $a \in K$, $\exists x_i$, such that $a = x_1\alpha_1 + x_2\alpha_2 + ... + x_n\alpha_n$. As $x_i \in E$, we have $\forall i, x_i = y_{i1}\beta_1 + y_{i2}\beta_2 ... + y_{im}\beta_m$. Thus, we have $a = \sum_{i=1}^{n}\sum_{j=1}^{m} y_{ij}\beta_j\alpha_i$. Now we want to prove linear independency. We notice that the set of β's are linearly independent. Thus, we have $\sum_{i=1}^{n}\sum_{j=1}^{m} y_{ij}\alpha_i = 0$. And we notice that the set of α's are linearly independent. Therefore, we proved $[K : F] = mn$. □

Definition 2.6. An element α is *algebraic* over a field F, if there exists a polynomial $f(\alpha) = 0$ over field F. Otherwise, α is said to be *trancendental.*

Definition 2.7. A field extension E over F is called an *algebraic extension* if all elements on E are algebraic over F, otherwise E is said to be a *trancendental extension.*

Definition 2.8. A polynomial over F is called a *minimal polynomial* of an algebraic element α if $f(\alpha)$ has the smallest degree among all the possible polynomials that have α as a root.

Definition 2.9. A field extension E over F is called a *simple extension* if $\exists \alpha \in E$, such that $E = F(\alpha)$

Proposition 2.10. *The following statements are equivalent:*
(i)A field extension E/F is finite
(ii)E is algebraic and finitely generated over F

Proof. $(i) \Rightarrow (ii)$ Assume that field extension E/F is finite. We could assume that $[E : F] = n$. Thus, we could pick a basis over F being $\{\alpha_1, \alpha_2 ... \alpha_n\}$ such that this basis generates field E. Thus, it is clear that E is finitely generated. Now, assume $a \in E$. As we know that $[E : F] = n$, we know that the set $\{1, a, a^2, a^3 ... a^n\}$ is linearly dependent. Therefore, we have the polynomial $f(x) = \sum_{i=0}^{n} x_i a^i$. And it is easy to verify that when $f(a) = 0$, due to linear dependency, we have a nonzero x, which gives us the polynomial.

$(i) \Leftarrow (ii)$ As E is finitely generated and algebraic over F, we could let $E = F(\alpha_1, \alpha_2..., \alpha_n)$. By the tower rule, we have $[E : F] = [F(\alpha_1) : F]...[F(\alpha_1, \alpha_2..., \alpha_n) : F(\alpha_1, \alpha_2..., \alpha_{n-1})]$. It is clear that the degree of E/F is finite as all the α's are algebraic. □

Definition 2.11. Let E/F be a field extension, and p be a polynomial that $p \in F[X]$. The polynomial p *splits* the field E, if

$$p = a(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$$

where $a \in F$, and $\alpha_1, \alpha_2, ...\alpha_n \in E$.

Definition 2.12. We call the field E, split by a polynomial p, and is generated by roots of p, a *splitting field* of p, a.k.a

$$E = F(\alpha_1, \alpha_2, ..\alpha_n)$$

Now, we are going to look at some properties of splitting fields.

Theorem 2.13. *(The existence of splitting fields) Let F be a field, and $p \in F[X]$. There is a splitting field E for all p. Moreover, if deg(p) = n, then $[E : F] \leq n!$.*

Proof. We will do this proof by using induction. Base case, $deg(p) = 1$. This case is trivial, let $p = X - \alpha$, we have $\alpha \in F$, thus we take $E = F$, and indeed, $[E : F] = 1 \leq 1$. Assume that this theorem holds for all $n \geq 1$. Consider case $deg(p) = n + 1$. We let f be a degree n polynomial, and $p = (X - \alpha_1)f$. Assume K is the splitting field of f. Then, it is obvious to us that we could simply pick $E = K(\alpha_1)$ as our splitting field over p. Indeed, all the roots are in this field. Also, $[E : F] = [E : K][K : F]$, and therefore, we have $[E : K] = [E : K][K : F] \leq n * (n - 1)! = n!$. □

Definition 2.14. Assume E and K are field extensions of F. Then we call the mapping $\varphi : E \to K$, such that $\varphi(a) = a$, $\forall a \in F$, an *F-homomorphism.* If the mapping is bijective, then we call it *F-isomorphism.*

Theorem 2.15. *(Uniqueness of Splitting field) Let $p \in F[X]$ be a polynomial, and E, K be the splitting field of p. Then $E \cong K$.*

Proof. Since E is a splitting field of p, then the roots of p, $\alpha_1, ...\alpha_n \in E$. Therefore, assume $E = F(\alpha_1, \alpha_2, ..\alpha_n)$. We know that p_1, being the minimal polynomial of α_1, splits K, as p splits K. Therefore, we could find $\varphi_1 : F[\alpha_1] \to K$. Now, consider the minimal polynomial p_2 α_2 over $F[\alpha_1]$. This yields a homomorphism $\varphi_2 : F[\alpha_1, \alpha_2] \to K$. Repeating this process until we get the map from E to K. Also, it is clear that the number of mappings are at most $[E : F]$, as f has only $[E : F]$ distinct roots. Therefore, $E \cong K$. □

Definition 2.16. Let $p \in E[X]$ be an arbitrary polynomial, the field E is *algebraically closed* if E contains all the roots of p.

Definition 2.17. Let E/F be a field extension, E is algebraically closed and E is algebraic over F. Then E is the *algebraic closure* of F.

We hope that $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, which we shall prove in the later sections as the Fundamental Theorem of Algebra.

2.2. **Galois Extension.**

Definition 2.18. Assume F is a field, let $p \in F[x]$, E is the splitting field of p over F. If p does not have repeated roots, then p is said to be *separable* over F.

Definition 2.19. Let F be a field, the *formal differentiation* is a F-linear map, $D : F[X] \to F[X]$, such that $X^n \mapsto nX^{n-1}$.

Notice that such F-linear map works on any field.

Definition 2.20. Let E/F be a field extension. If $\alpha \in E$, and the minimal polynomial of α is separable over F, then α is *separable* over F.

Definition 2.21. Let E/F be a field extension, and $\forall \alpha \in E$, α is separable over F, then E is separable over F.

Proposition 2.22. *Let F be a field, $l \in F[X]$ is irreducible, then*
(i) If characteristics of F is 0, then l is separable,
(ii) If the characteristics of F is prime, say p, then l is not separable iff $l \in F[X^p]$

Proof. (i) Assume F is a field with characteristic 0, and $l \in F[X]$. Assume l is not separable, then there is a repeated root, thus $gcd(l, l') \neq 1$. As l is irreducible, we have $gcd(l, l') = l$. However, we know that $deg(l') = deg(l) - 1$. Thus $l \nmid l'$. Contradiction. Thus l is separable.

(ii) Let F be a field with characteristic p this time, and by the same reason, $gcd(l, l') = l$ iff $l' = 0$, which is equivalent to $l \in F[X^p]$. □

Definition 2.23. Let E/F be a field extension, E is a *normal extension* over F if $\forall \alpha \in F$, α splits E.

Definition 2.24. Let G be a group of automorphisms of E,

$$Inv(G) = \{\alpha \in E | \sigma(\alpha) = \alpha\}$$

Then, $Inv(G)$ is called a *fixed field* of G

Definition 2.25. Let E/F be a field extension, $Gal(E/F)$ is the *Galois group* if $Gal(E/F)$ is the set of all F-automorphism of E.

Definition 2.26. Let E/F be a field extension, If $F = Inv(Gal(E/F))$, then we say E is a *Galois extension* of F.

Proposition 2.27. *If E is a splitting field of a separable polynomial $f \in F[X]$, then $Gal(E/F)$ has order $[E : F]$*

Proof. Let $f = (x-a_1)(x-a_2)...(x-a_n)$. We know this is legal because E is the splitting field of f, and f is separable. Therefore, we find f has $deg(f) = n$ distinct roots in E. Now, we examine the number of F-automorphisms. We write $E = F[a_1, a_2...a_n]$. Then consider the minimal polynomial of a_1 divides f, and $deg(f_1) = [F[a_1] : F]$. Establish $\sigma : E \to E$. It is clear that there are $deg(f_1) = [F[a_1] : F]$ F-automorphisms. And then consider the minimal polynomial of a_2 over $F[a_1]$. And clearly, by the same procedure above, we have $deg(f_2) = [F[a_2, a_1] : F[a_1]]$ F-automorphisms. By doing the same procedure, and by the tower rule, we get exactly n F-automorphisms. □

Lemma 2.28. *Let $\sigma : E \to K$ be an F-homomorphism, let $\alpha \in E$ be algebraic over F. Let $f \in F[X]$, and $f(\alpha) = 0$, then $f(\sigma(\alpha)) = 0$.*

Proof. Let $f(x) = a_0 + a_1 x + ... + a_n x^n$. Then we have

$$\begin{aligned} f(\sigma(\alpha)) &= a_0 + a_1\sigma(\alpha) + ... + a_n\sigma(a^n) \\ &= a_0 + a_1\sigma(\alpha) + ... + a_n\sigma(a)^n \\ &= \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + ... + \sigma(a_n)\sigma(a)^n \\ &= \sigma(f(\alpha)) = \sigma(0) \\ &= 0 \end{aligned}$$

□

Remark 2.29. From the above lemma, we notice that σ in fact permutates the roots in the polynomial; and it is not hard to observe the isomorphism between the minimal polynomial of α and $\sigma(\alpha)$. Thus, we call the homomorphism σ *embedding*, and the permutated roots *conjugates* of α.

Theorem 2.30. *Let E/F be a field extension, the following statements are equivalent:*

(i) E/F is a Galois extension

(ii) E/F is separable and normal

(iii) Assume $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$, p be the minimal polynomial of α_i over F ($\forall i$), then p is separable and splits E.

Proof. (i) ⇒ (ii) Assume E/F is Galois, then we assume $F = inv(Gal(E/F))$, $a \in E$, $a_1, a_2...a_n$ be conjugates of a, and $\{\sigma(a) : \sigma \in Gal(E/F)\}$ be the embeddings. By the lemma above, we find and each $\sigma(a)$ is a root of a polynomial of a, say $f(a) = (x-a)(x-a_1)...(x-a_n)$. And it is clear that the coefficients of f are in F (as σ also permutates f). Thus the minimal polynomial of a divides $f(x)$. Thus, the minimal polynomial splits over E, and it does not have repeated roots. Thus E is separable and normal.

(ii) ⇒ (iii) Assume E/F is separable and normal, then we could pick that $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$. As E is normal, we know that p splits E, and as E is separable, we know that p is separable.

(iii) $\Rightarrow$ (i) Since $E = F(\alpha_1, \alpha_2, ..., \alpha_n)$, and p is separable, we have some extension K being a Galois extension of F, such that we define $\phi : E \to K$, and the number of such F-homomorphism to be $[E : F]$. We know it is legal, by (i)$\to$(ii). Assume $E \subseteq K$. We want to show $\tau : \sigma_E \to \phi$ is an isomorphism. We already know the injection, as we claimed the homomorphism ϕ. Thus we want to show the surjection. And by the lemma above, we find that if α is a root, $\phi(\alpha)$ is also a root of p. Therefore, we know $\phi(\alpha) \in E$. And E is generated by α, we know $\phi(E) \in E$. Thus, we have the surjection. Thus, we know that E is bijective to K, meaning E is Galois over F. □

2.3. **Fundamental Theorem of Galois Theory.**

Theorem 2.31. *(Fundamental Theorem of Galois Theory) Let E/F be a finite Galois extension. Let $G = Gal(E/F)$, and let H be a subgroup of G*

(i) There is a one-to-one and onto relation between intermediate fields of E/F, say K, and subgroups of G, with $K \mapsto Gal(E/K)$ and $H \mapsto inv(H)$

(ii) If $K \mapsto H$, then $[E : K] = |H|$ and $[K : F] = [G : H]$.

(iii) H is a normal subgroup of G, iff K is Galois over F. And in this case, $Gal(K/F) \cong G/H$

Proof. (i) Assume K is a subfield of E but containing F. As E is Galois over F, we know E is normal and separable over F, and thus we know that E is normal and separable over K. So E is Galois over K. Therefore, $K = inv(Gal(E/K)$. Assume H to be a subgroup of G, then $H = Gal(K/inv(H))$.

(ii)As E/F is Galois, we know that $[E : F] = |G|$. Also, if $K \mapsto H$, we know that E/K is Galois, thus $[E : K] = |H|$. Therefore, by the tower rule, we have $[K : F] = |G|/|H| = [G : H]$

(iii)($\Rightarrow$) Assume that H is a normal group of G, and let $K = inv(H)$. Take $a \in K$, let b be a conjugate of a in E. Thus, we could find an embedding σ such that $\sigma(a) = b$. Next, we define $\tau \in H$ such that $\tau(b) = b$. Indeed, we have $\tau(b) = \sigma(\sigma^{-1}\tau\sigma(a))$, and we know that H is normal, thus $\tau(b) = \sigma(a) = b$. As E/F is Galois, we know that a splits E, and furthermore, $b \in inv(H) = K$, we know that a actually splits K. Thus, K is normal over F by former proposition. And thus, with E/F being separable, K is a subfield of E, thus K/F is separable, meaning K/F is Galois.

($\Leftarrow$) Let K be Galois over F. Thus, K/F is normal. Let $\phi : G \to Gal(K/F)$. Thus, we could find $ker\phi = \{\sigma \in K | \sigma_L = i\} = \text{Gal(K/F)} = \text{H}$. Thus, H is normal in G, as kernels are normal subgroups. And by the first isomorphism theorem, we get $Gal(K/F) \cong G/H$. □

3. Applications for finite Galois Theory

In this section, we are going to talk about the applications of Galois Theory. The examples we are going to discuss include: Fundamental Theorem of Algebra, and solubility of quintic equations.

3.1. **Fundamental Theorem of Algebra.**

Definition 3.1. Let E be a field extension of F, then the *normal closure* of E/F, L, is the minimal field extension over E that is also a normal extension over F

Remark 3.2. In order to prove the next theorem, let us state some facts first:

(i) If $f(x)$ has odd degree, then f has a root in $\mathbb{R}$. And this implies that $\mathbb{R}$ doesn't have odd degree extension.

(ii) Every positive real number has a real square root.

(iii) Every complex number has a complex square root. This implies that there is no field extension E over $\mathbb{C}$, such that $[E : \mathbb{C}] = 2$

Besides, we assume the knowledge of Sylow Theorems for the next theorem.

Theorem 3.3. *(Fundamental Theorem of Algebra) The field $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$*

Proof. Let $F/\mathbb{C}$ to be a field extension. Let N be a normal closure of $F/\mathbb{R}$. Then, it suffices to show that $\mathbb{C} = N$ to prove the statement. By main theorem, we know that if $G = Gal(N/\mathbb{R})$, then

$$|G| = [N : \mathbb{R}] = [N : \mathbb{C}][\mathbb{C} : \mathbb{R}] = 2[N : \mathbb{C}]$$

. Therefore, we know the order of G is even. Thus, we let H to be a 2-Sylow subgroup of G, and let K to be the fixed field of H. Then, $[G : H] = [K : \mathbb{R}]$ are odd. But by the fact (i) stated above, we realize that $K = \mathbb{R}$. And now we realize that $[F : \mathbb{R}] = 2[F : \mathbb{C}]$ are powers of 2. Thus, assume $[F : \mathbb{C}] > 1$, we could find a field extension, L, such that $[L : \mathbb{C}] = 2$, which is a contradiction to fact (iii). Thus, we know that $N = \mathbb{C}$. □

3.2. **Solubility of Equations.**

Definition 3.4. Let $\zeta \in F$, $\zeta^n = 1$, then we call ζ to be an *nth roots of unity.*

Remark 3.5. If ζ is a nth root of unity, and all the ζ's form a group with respect to multiplication, then we call ζ a *primitive* nth roots of unity. And we could observe an isomorphism between the multiplication group and the $\mathbb{Z}/n\mathbb{Z}^\times$ groups.

Definition 3.6. If ζ is a root of unity, then we call the field extension, $F(\zeta)/F$ to be a *cyclotomic extension*

Definition 3.7. The *nth cyclotomic polynomial* is defined as

$$\Phi_n(x) = \prod_{i \in \mathbb{Z}/n\mathbb{Z}^\times} (x - \zeta_i)$$

Theorem 3.8. *Let $n > 0$, $\Phi_n(x)$ is irreducible in $\mathbb{Q}[X]$. Prove the isomophism: $Gal(\mathbb{Q}[\zeta]/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where ζ is mth root of unity.*

Proof. Consider the function $\Phi_n(x)$. Given that it is irreducible, we have the roots of $\Phi_n(x)$ forms the primitive roots of unity. Therefore, we could observe that these roots of unity forms one orbit on the Galois group. By the order of this polynomial, we know that there are the same number of elements as in $(\mathbb{Z}/n\mathbb{Z})^\times$. Therefore, we could assign injection, and clearly it is also surjection. □

Definition 3.9. Let E/F be a Galois extension. E/F is *cyclic* if $Gal(E/F)$ is cyclic.

Theorem 3.10. *Let F be a field, and $\alpha \neq 0$. Let $n \in \mathbb{N}$, and let E be a splitting field over $x^n - \alpha$. Then the followings are true:*

(a) E contains a nth root of unity, say ζ

(b) $E/F(\zeta)$ is cyclic.

(c) $[E : F(\zeta)]|n$

(d) $[E : F(\zeta)] = n$ iff $x^n - \alpha$ is irreducible in $F(\zeta)[X]$.

Proof. (a) Firstly, we check if $x^n - \alpha$ has distinct roots by taking a derivative. We get nt^{n-1}. Then we notice there is no common roots. Thus, $x^n - \alpha$ has distinct roots. Next, we notice that the roots $x_1x_1^{-1}, x_2x_1^{-1}...x_nx_1^{-1}$ is the roots of unity. Thus, we know that ζ must be one of them.

(b) By the line of thought in (a), WLOG, we could write the roots as a set $\{x_1, x_1\zeta, x_1\zeta^2...x_1\zeta^{n-1}\}$, and also, we know that E is a splitting field over $x^n - \alpha$. Therefore, we have $E = F(x_1, ..., x_n) = F(\zeta, x_1)$. Consider $Gal(F(\zeta, x_1)/F(\zeta))$. The automorphisms will map x_1 to one of the other root, $\zeta^k x_1$. Therefore, define injective $\phi : Gal(F(\zeta, x_1)/F(\zeta)) \to \mathbb{Z}/n\mathbb{Z}$. It is clear that it is a homomorphism corresponding to k's. Thus, we could conclude that $Gal(F(\zeta, x_1)/F(\zeta))$ is a cyclic group.

(c) Since $\phi : Gal(F(\zeta, x_1)/F(\zeta)) \to \mathbb{Z}/n\mathbb{Z}$ is a homomorphism, we know that it has order as a factor of n. Thus we get the statement.

(d) ($\Rightarrow$) Assume that $[E : F(\zeta)] = n$, then $\phi : Gal(F(\zeta, x_1)/F(\zeta)) \to \mathbb{Z}/n\mathbb{Z}$ is in fact a isomorphism, since it is one-to-one with the same order. Therefore, we know that the roots are primitive and thus the equation are irreducible.

($\Leftarrow$) By a statement we showed, we know that if $x^n - \alpha$ is irriducible, then it has distinct roots in E. Therefore, it will be a primitive roots of unity, which we could deduce that $[E : F(\zeta)] = n$ □

Definition 3.11. Let F be a field contains a primitive nth roots of unity, and E/F is a Galois extension, if E is the splitting field of $x^n - \alpha$ and $[E : F] = n$, then we call E/F a *Kummer extension.*

Proposition 3.12. *Let F be a field contains a primitive nth roots of unity, and E/F is a cyclic extension with $[E : F] = n$, then E/F is a Kummer extension.*

Proof. Firstly, pick a generator ϕ. Therefore, we could write an element $\beta \in E$ to be written as a linear combination of $\zeta\phi(\alpha)$, such that

$$\beta = \alpha + \zeta\phi(a) + ... + \zeta^{n-1}\phi^{n-1}(\alpha)$$

Next, notice that

$$\phi(\beta) = \phi(\alpha) + \zeta\phi^2(a) + ... + \zeta^{n-1}\phi^n(\alpha)$$

Thus, with $\phi^{n-1}(\alpha) = \alpha$ being the identity map, we have $\zeta\beta = \phi(\beta)$. Therefore, we could find β^n to be fixed, meaning that $\beta^n \in F$. Therefore, we know that $K(\beta)$ is the splitting field of $x^n - k$. And we also have the n power of ϕ to be distinct in automorphism of $F(\beta)$. Therefore, we know that $n = [E : F] \geq F(\beta)/F = n$. Therefore, by Artin's Lemma, we have $E = F(\beta)$. Therefore, we know that E is a splitting field of $x^n - k$, thus E/F is Kummer. □

Definition 3.13. A field extension E/F is *radical* if there is an field extension K/E, such that

$$F \subseteq K_n \subseteq K_{n-1} ... \subseteq K_1 \subseteq K$$

where $\forall i, E_{i+1}/E_i$ is either a cyclotomic extension or Kummer extension.

Definition 3.14. If $f(X) \in F[X]$, then f is *solvable by radicals* if there is a radical extension E/F such that f splits over E

Definition 3.15. A finite group G is *soluble* if $\exists$ a sequence of normal subgroups,

$$1 = G_k \trianglelefteq G_{k-1} \trianglelefteq ... \trianglelefteq G_1 \trianglelefteq G_0 = G$$

With G_i/G_{i+1} abelian

Definition 3.16. A finite field extension E/F is *soluble* if there is a field extension K/E such that K/F is Galois and $Gal(K/F)$ is soluble.

Remark 3.17. We could observe from the above definitions, that if E/F be a Galois extension, then E/F is solvable iff $Gal(E/F)$ is soluble. This proof is basically by definition, and to prove the left to right direction, one only need the fundamental theorem of Galois Theory, since $Gal(E/F)$ is a intermediate field extension.

Definition 3.18. The *derived series* $\{G^m\}$ of G is defined as

$$G^0 = G$$
$$G^{i+1} = (G^i)'$$

Where we have

$$...G^{k-1} \trianglelefteq ... \trianglelefteq G^1 \trianglelefteq G^0 = G$$

With G_i/G_{i+1} abelian

Remark 3.19. Notice several properties of the derived series.

(i) G is soluble iff $\exists k$ such that $G^k = 1$

(ii)If H is a subgroup of G, then G is soluble if H is soluble.

Lemma 3.20. *Let H be a subgroup of G. Then G is soluble iff H and G/H are soluble.*

Proof. ($\Rightarrow$)Let $H \trianglelefteq G$. It is clear that if G is soluble, then H is soluble. Now, consider G/H.

$$(G/H)' = G'H/H \subseteq G/H$$

Repeat this process m times, we will find a subset being 1, meaning that G/H is soluble.

($\Leftarrow$)Let H and G/H be soluble, we have $H^k = 1$, and $(G/H)^s = G^s H/H = 1$. Therefore, we have $G^s \subseteq H$. Therefore, we have $G^{k+s} = 1$, thus G is soluble. □

Proposition 3.21. *Let F be a field whose characteristics is 0. Then, E/F is a radical extension iff it is soluble.*

Proof. ($\Rightarrow$) Let E/F be a radical extension. Then there is an field extension K/E, such that $F \subseteq K_n \subseteq K_{n-1}... \subseteq K_1 \subseteq K$ where $\forall i, E_{i+1}/E_i$ is either a cyclotomic extension or Kummer extension. Therefore, $\forall i, E_{i+1}/E_i$ is Galois. Thus, K/F is Galois. Moreover, we could set $G_i = Gal(K_i/F)$. With E_i/F being cyclotomic or Kummer, we know that it is also abelian. Therefore, E/F is soluble.

($\Leftarrow$) Assume E/F is soluble. Then, we know there is a field extension K/E so that K/F is Galois, and $Gal(K/F)$ is soluble. Therefore, we let $G_i = Gal(K_i/F)$. Thus, we find that in order for the quotient group G_i/G_{i+1} to be abelian, G_i/G_{i+1} has to be cyclic, therefore, it needs to be either cyclotomic or Kummer. □

Corollary 3.22. *$S_n (n \geq 5)$ is not soluble, which implies quintic equation is not solvable.*

4. Infinite Galois Theory

In this section, we let K be an infinite degree field extension over F, a.k.a. $[K : F] = \infty$

4.1. **Topological Groups.**

Definition 4.1. A set G is a *topological group* if it satisfies the following conditions:

(i) G is a group
(ii) G is a topological space
(iii) the map $\rho : G \times G \to G$, with $a, b \in G$, $(a, b) \mapsto ab$ is continuous.
(iv) the map $\rho : G \to G$, with $a \in G$, $a \mapsto a^{-1}$ is continuous.

Definition 4.2. Let G be a topological group, G is *homogeneous* if $\forall a, b \in G$, $\exists f$, being homeomorphism, such that $f(a) = b$

Lemma 4.3. *Let G be a topological group, let $a \in G$. $f(x) = xa$, $g(x) = ax$, $\rho(x) = x^{-1}$ are homeomorphisms of G*

Proof. These properties follows from the definition of topological groups, since these maps are clearly bijective and also they are continous. □

Proposition 4.4. *Every topological group are homogeneous.*

Proof. Consider function $f : x \mapsto ba^{-1}x$. It is clear that it maps from a to b, moreover, by the last lemma, it is homogeneous. □

Proposition 4.5. *Let G be a topological group, V be a neighbourhood of a, then there exists a neighbourhood of U of e, such that $V = aU$*

Proof. Define $U := a^{-1}V$, then consider the map $\phi : x \mapsto ax$. Therefore, we could map U to V. □

Definition 4.6. Let U be a topological group, we say U be symmetric if $U = U^{-1}$. Where U^{-1} is the set of inverse elements of U

Proposition 4.7. *Let G be a topological group. Then for all neighbourhood U of $a \in G$, there is an open symmetric group $V \subset U$ such that $V^2 \subset U$*

Proof. Define $f : x \mapsto x^2$. This, as a polynomial is continuous. Then define $V = f^{-1}(U)$, where V is a neighbourhood of e. Therefore, $V^2 = f(v) = f(f^{-1}(U)) \subseteq U$. □

Remark 4.8. At this point, we should look at some group properties of the topological groups which could help us dealt with Krull Topology in the later sections.

Proposition 4.9. *Let G be a topological group, and H be a subgroup of G. Then H is also a topological group.*

Proof. Since H is a subgroup of G, it already has group structure. Now, we need to prove the continuity requirements.

Since H has group structure, we see that it also contains all the inverses in the group. But note that these elements are also in G, thus the function is also continuous. □

Definition 4.10. Let G be a topological group, the topological closure of a subset U in G is the smallest closed set in G that contains U, we denote it as $\bar{U}$

Proposition 4.11. *Let G be a topological group. If H is a subgroup of G, then $\bar{H}$ is also a subgroup of G; If H is a normal subgroup of G, then $\bar{H}$ is also a normal subgroup of G.*

Proof. It suffices to show that $\bar{H}$ satisfies a group structure.

Consider $a, b \in H$, we could easily show that if W is a neighbourhood of ab^{-1}, then there are U, V containing a, b, such that $UV^{-1} \subset W$. Thus, we could find $x \in U \cap H$ and $y \in V \cap H$, such that $xy^{-1} \in UV^{-1} \cap H$. Therefore, we know that $xy^{-1} \in \bar{H}$

Now assume H is normal. We do the same trick, let V be a neighbourhood of $g^{-1}ag$, where $a \in G$. Then we could find U containing a such that $g^{-1}Ug \subseteq V$. Thus, we know that $U \cap H \neq \emptyset$. Thus, there is an $h \in U \cap H$ such that $g^{-1}hg \in V$ □

Definition 4.12. A topological space is *totally disconnected* if its only connected subspace is one point sets.

Proposition 4.13. *Let G be a topological group, then G is Hausdorff iff $\{e\}$ is closed in G*

Proof. ($\Rightarrow$) Assume G is Hausdorff, then we know that all singleton sets are closed. Thus, $\{e\}$ is closed.

($\Leftarrow$) Assume $\{e\}$ is closed in G. Then, we define a map $f : (x, y) \mapsto xy{-}1$. Therefore, we know this mapping is continuous. Assume e maps to $\{ab^{-1}\}$, then $\{ab^{-1}\}$ is closed. Thus $G \setminus \{ab^{-1}\}$ is open. Thus, $\exists U$ containing e, such that $U \subseteq G \setminus \{ab^{-1}\}$. Therefore, by property of continuity, we have $V, W \subseteq U$ containing e being open, with $VW^{-1} \subseteq U$. Therefore, we know that $ab^{-1} \notin VW^{-1}$, therefore, $aV \cap bW = \emptyset$. Thus it is Hausdorff. □

Proposition 4.14. *Let G be a compact topological group, then every subgroups of G has finite order.*

Proof. Assume the subgroup, say, H is open. Then the cosets are open. Thus, the cosets form a open cover of G. Now that G is compact, we know that H has finite order. □

Proposition 4.15. *Let G be a totally disconnected topological group, then G is Hausdorff a.k.a $\{x\}$ is closed in G*

Proof. Let G be totally disconnected, then only singleton sets are connected subspace, meaning singleton sets are closed. □

4.2. **Profinite Groups and Krull Topology.**

Remark 4.16. The notion of profinite groups natually arises from infinite Galois theory, and is alaos important in group cohomology. Thus, we are going to discuss some properites of them.

Definition 4.17. A *direct set* is a set with a binary relation $\leq$, such that it is reflexive, transitive and there is a upper bound for all pairs.

Definition 4.18. Assume S is a direct set. $(X_i, \phi_{ij})_S$ where $\{X_i | i \in S\}$ is a set of topological spaces, and $\{\phi : X_i \to X_j | i, j \in S, j \leq i\}$ is a set of continuous functions, is a *projective system* if it satisfies the following:

(i) ϕ_{ii} is the identity on X_i.

(ii)$\forall k \leq j \leq i, \phi_{ik} = \phi_{jk} \circ \phi_{ij}$

Definition 4.19. Let (X_i, ϕ_{ij}) be a projective system. Let $X = \prod X_i$ be the product topology. Let $\varphi_i : X \to X_i$ be a map. The projective limit is $\varprojlim X_i = \{a \in X | \varphi_j(a) = \phi_{ij}\varphi_j(a); j \leq i\}$

Proposition 4.20. *Let (X_i, ϕ_{ij}) be a projective system. Then the followings are true:*

(i) If X_i is Hausdorff, then $\varprojlim X_i$ is also Hausdorff.

(ii) If X_i is totally disconnected, then $\varprojlim X_i$ is also totally disconnected

(iii) If X_i is Hausdorff, then $\varprojlim X_i$ is closed in X.

(iv) If X_i is compact, then $\varprojlim X_i$ is also compact.

Proof. (i) Since X is a product space of X_i, and we know that $\varprojlim X_i$ is a subspace of X. Therefore, if X_i are Hausdorff, then X is Hausdorff, and this implies $\varprojlim X_i$ being Hausdorff.

(ii) Since X is a product space of X_i, and we know that $\varprojlim X_i$ is a subspace of X. Therefore, if X_i are totally disconnected, then X is totally disconnected, and this implies $\varprojlim X_i$ being totally disconnected.

(iii) Since X_i is Hausdorff, we know that all single point sets are closed. Also, we know that φ, ϕ are continuous functions, thus, we let $\pi = \varphi_j - \phi_{ij}\varphi_j$. Thus, π is also continuous, and the set $\{a \in X | \varphi_j(a) = \phi_{ij}\varphi_j(a); j \leq i\}$ is the preimage of $\{0\}$. Therefore, the set is closed. With $\varprojlim X_i$ being the intersection of closed set, the set is also closed.

(iv) Since X_i is compact, the product space, X is also compact. Also, by (iii), we know that $\varprojlim X_i$ is closed. Thus, closed subspace of a compact set is compact. Thus $\varprojlim X_i$ is compact. □

Proposition 4.21. *The projective limit $\varprojlim X_i$ is a topological group if X_i is a topological group.*

Proof. Since X_i is a topological group, the product space X is also a topological group. Now, it suffices to prove that $\varprojlim X_i$ is a subgroup.

Firstly, we check non-empty. Indeed, we know that $e \in X$ is an element in $\varprojlim X_i$ as the identity. Next, we check closure. Note that φ, ϕ are homomorphisms, we know that if $a, b \in \varprojlim X_i$, then $\varphi_j(ab) = \phi_{ij}\varphi_j(a)\varphi_j(b) = \phi_{ij}\varphi(ab)$. Therefore, it is closed. And by the same reasoning, inverse is also in the group, and for $a \in \varprojlim X_i$, the inverse is a^{-1}. □

Definition 4.22. Let G be a topological group, we say that it is a *profinite group* if it is isomorphic to $\varprojlim G_i$, with respect to a projective system (G_i, ϕ_{ij}), where G_i are finite discrete topological groups.

Theorem 4.23. *G is a profinite group iff it is totally disconnected, Hausdorff, and compact.*

Proof. ($\Rightarrow$) Assume G is a profinite group. Since it has the discrete topology, we know that discrete topology is Hausdorff, compact and totally disconnected. Therefore, we know that G as a topological group is also Hausdorff, compact and totally disconnected.

($\Leftarrow$) Assume G is compact, Hausdorff and totally connected. Assume $H = \varprojlim H_i$, where H_i are quotient open normal subgroups of G. Therefore, we want to show that $G \cong H$. We define a map $\rho : G \to H$. Since H is the inverse limit of subgroups in G, we know H is also compact, Hausdorff, and totally disconnected. Therefore, we need to show bijection and continuity.

Continuity: it is clear, since the image and the corresponding preimage are both open, we could see directly that the map is continuous.

Injective: Since G is totally connected, $\forall g \in G$ we could find a closed and open set $U \subset G$ that contains the identity but not g. We want to construct H in U. Now, assume $V = (G \setminus U) \cap U^2$. Since U is compact, it is easy to conclude that V is also compact. Assume $h \in U$, $W, X \subset U$ containing h, e, and it is easy to check that $W, X \subset V$. Therefore, all the W's form an open cover of U, and thus there is a finite subcover, say W_i. We let $Y = X \cap X^{-1}$, therefore, we have $UY = \cup W_i Y \subset W_i X \subset U$. Therefore, we could set H' to be the intersection of all such Y, say Y', and the H we want to construct is $\cap_{g \in G} g H' g^{-1}$. Since H' is open, we know that H is also open, and it is normal subgroup of G and also contained in U

Surjective: Assume $h_i H_i \in H$, where $h_i \in G$. We know that H_i is non-empty, therefore, with G being compact, we know that $\cap h_i H_i$ is non-empty. Therefore, we know that the mapping is surjective. □

Definition 4.24. Assume E/F is an infinite Galois extension, the *Krull Topology* on $Gal(E/F)$ is the topology having basis as all the cosets $\sigma Gal(E/K)$, $\sigma \in Gal(E/F), K$ is an intermediate finite Galois extension over F

Theorem 4.25. *Let E be a Galois extension of F, the group $Gal(E/F)$ with the Krull topology is*

(i) Hausdorff
(ii) Compact
(iii) totally disconnected
Thus it is a profinite group.

Proof. (i) Let $\sigma, \tau \in Gal(E/F)$, with $\sigma \neq \tau$, therefore, we have $\sigma^{-1}\tau \neq e$. Now, notice that if U is a neighbourhood around σ, $\cap U_\sigma = \cap Gal(K/F) = e$. Thus, $\exists U_0$, such that $\sigma^{-1}\tau \notin U_0$. Thus $\tau \notin \sigma U_0$, implying $\tau U_0 \cap \sigma U_0 = \emptyset$. Therefore Hausdorff.

(ii) We define a map $\phi : Gal(E/F) \to \prod Gal(K/F), \forall K$ being finite intermediate field extension over F. Therefore, we have $\prod Gal(K/F)$ having discrete topology, therefore, it is compact. Now, we want to prove that ϕ is a hemeomorphism, and thus we could get compact.

Bijective: Surjectivity is natural, since $\prod Gal(K/F)$ is the image of ϕ. And consider the kernel, $\phi(e) \mapsto e$, over F. Therefore, only the identity maps to the identity in the image. We know that this implies injective.

Continuous: We have discussed that $\varphi : \prod Gal(K/F) \to Gal(K/F)$ is continuous. And we know that $Gal(K/F)$ is a topological group, it is homogeneous. Since e is open in the image, we check the preimage of the mapping $\varphi \circ \phi$, we know that if σ fixes K, then $\sigma \in Gal(E/K)$. Since $Gal(E/K)$ is a basis element of Krull topology, we know that it is open. Thus, ϕ is continuous.

Therefore, we know that the Krull topology is compact.

(iii) Let K be a finite field extension over F, H be a connected component containing e. Let $U_H = U \cap H$. Therefore, $e \in U_H$, and U_H is open in H. Then, define $V_H = \bigcup_{x \in H \setminus U_H} xU_H$. Thus, V_H is open. We assumed that H is connected, and $H = V_H \cap U_H$. Therefore, we know that V_H must be empty, or $U_H | V_H$ is a separation of H. Therefore, $H = U_H$. Thus, $H \in \cap U = e$. Therefore, it is totally disconnected. □

4.3. **Fundamental Theorem of Infinite Galois Theory.**

Lemma 4.26. *Let E/F be a Galois extension, if H is a subgroup of $Gal(E/F)$, then $Gal(E/inv(H)) = \bar{H}$*

Proof. We know that $Gal(E/inv(H))$ is closed, H is a subgroup of $Gal(E/inv(H))$, we know that $\bar{H} \subseteq Gal(E/inv(H))$. Let $\sigma \in Gal(E/F) \setminus \bar{H}$, we can find a intermediate field extension K, such that $\sigma Gal(E/K) \cap H = \emptyset$, meaning that $\sigma \notin HGal(E/K)$. Therefore, we can find $\alpha \in K$, such that H fixes α but $\sigma(\alpha) \neq \alpha$. Thus, $\sigma \notin Gal(E/inv(H))$. Therefore, $Gal(E/inv(H)) \subseteq \bar{H}$ □

Theorem 4.27. *(Fundamental Theorem of Infinite Galois Theory) Let E/F be a finite Galois extension. Let $G = Gal(E/F)$, and let H be a subgroup of G*

(i) There is a one-to-one and onto relation between intermediate fields of E/F, say K, and subgroups of G, with $K \mapsto Gal(E/K)$ and $H \mapsto inv(H)$

(ii) Let H_1, H_2 be closed subgroups of G, then $H_2 \subset H_1$ iff $inv(H_1) \subset inv(H_2)$

(iii) A closed subgroup H is open in G, iff $inv(H)$ has finite degree over F.

(iv) H is a closed normal subgroup of G, iff $inv(H)$ is Galois over F. And in this case, $Gal(inv(H)/F) \cong G/H$

Proof. (i) has mostly the same proof as the finite one. Only that considering lemma 5.1, we could deduce that in order for the bijection to work, we have to have the group to be closed.

(ii) Since H_1, H_2 are both closed, and $H_2 \subset H_1$, then we know that the elements that fixes H_1 must also fix H_2. Therefore, we have $inv(H_1) \subset inv(H_2)$. The converse have the same proof.

(iii) We know the subgroup is closed, and by a former proposition, we know that in a topological group, every open group is closed iff they have finite index.

(iv) ($\Rightarrow$) Assume $H = Gal(E/K)$ is a closed and normal subgroup of G, where K is an intermediate field. And assume $f(X) \in F[X]$ be the minimal polynomial of a, and a, b be conjugates. Thus, define $\sigma(a) = b$. if $\tau \in H$, then $\tau(b) = \tau(\sigma^{-1}(a)) = \sigma^{-1}\sigma\tau\sigma^{-1}(a)$. We know that $\sigma\tau\sigma^{-1} \in H$, and a fixes H, thus $\sigma^{-1}\sigma\tau\sigma^{-1}(a) = \sigma^{-1}(a) = b$. Thus b also fixes H, meaning that K/F is normal, and this implies that $inv(H)$ is Galois over F.

($\Leftarrow$) If K/F is Galois, then we define $\phi : G \to Gal(K/F)$ having kernel being H. Thus, H is normal in G □

5. Exploration of the p-adics

Remark 5.1. Consider the mapping $\phi_{nm} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$. Define a projective system: $(\mathbb{Z}/p^n\mathbb{Z}, \phi_{nm})$. Then, we define $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. We call the additive group of $\mathbb{Z}_p$ the group of *p-adic integers.* Notice that this can form a profinite group.

Theorem 5.2. *The algebraic closure of $\mathbb{Q}_p$ has infinite degree over $\mathbb{Q}_p$*

Proof. We know that $x^n - p$ is irreducible over $\mathbb{Q}_p$. Therefore, we could have $x^n - p$ be in $\mathbb{Q}_p(\sqrt[n]{p})$, and thus $[\mathbb{Q}_p(\sqrt[n]{p}) : \mathbb{Q}_p] = n$. However, we know that $\mathbb{Q}_p(\sqrt[n]{p}) \subset \bar{\mathbb{Q}}_p$. Therefore, we have $[\bar{\mathbb{Q}}_p : \mathbb{Q}_p] \geq [\mathbb{Q}_p(\sqrt[n]{p}) : \mathbb{Q}_p] = n$. Then if $n \to \infty$, we have $\mathbb{Q}_p$ have infinite degree over $\mathbb{Q}_p$ □

Remark 5.3. For more properties about p-adic algebraic closure, we need more knowledge about algebraic number theory, including the concept of ramification, and Hensel's lemma. Therefore, our discussion will stop here.

Acknowledgements. I would like to thank my advisor, Professor Michael Gekhtman, for his encouragement in starting this project and his mentoring during the process of making the paper.

References

[1] Weintraub, Steven H. *Galois Theory*, New York, NY: Springer, 2000.
[2] Morandi, Patrick *Field and Galois Theory*, New York, NY: Springer, 1996.
[3] Milne, J.S. *Field and Galois Theory*, v. 4.30, www.jmilne.org/math/, 2012.
[4] Chevalley, Rosalie *Profinite groups and Galois cohomology*, Vienna: University of Vienna, 2010

Department of Mathematics, University of Notre Dame, Notre Dame, IN 46556-4618.
Email address: tgong@nd.edu