Galois Theory

Lectured by Yongquan Hu
Typed by Yining Chen

January 2022

Contents

1 Introduction

The theme of this mini-course is Galois theory, which starts with field extension. The prerequisites we assume are some basic group theory, ring theory and field theory, which are contained in the undergraduate course *Abstract Algebra*.

Roughly speaking, Galois theory is to study field theory using the technique of group theory. If we assume the field extension K/F is finite Galois, which means for an element $u \in K$, all roots of its minimal polynomial are different and in K, we define the Galois group

$$\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K) := \{f : K \xrightarrow{\sim} K \mid f|_F = id_F\}$$

Then the Galois correspondence (Theorem 3.9) states there is a one-to-one correspondence between subfields of K containing F and subgroups of $\mathrm{Gal}(K/F)$. Classically Galois theory comes from solvability of algebraic equations. For a polynomial $f(X) \in \mathbb{Q}[X]$ it's solvable by radicals iff the Galois group of its splitting field is solvable (Theorem 3.51). This is the theme of Section 3.4. It's famous that polynomials of degree ≤ 4 are always solvable by radicals but those of degree ≥ 5 are not solvable in general. In Section 3.5 we will construct those polynomials not solvable. In this course we also talk about applications of Galois theory to compass and straightedge construction. Actually compass and straightedge could only define a field extension of degree a power of 2. See Theorem 3.5 and Remark 3.36. This characterization will help us solve four difficult problems in ancient Greece.

Apart from finite Galois theory, we also introduce infinite Galois theory and there is a Galois correspondence as well (see Theorem 3.93). To deal with this we equip Galois groups with a special topology called Krull topology and consider closed subgroups. Such theory is compatible with finite Galois theory. Actually for a finite Galois extension, its Galois group is a discrete finite group with Krull topology. Hence all its subgroups are open as well as closed.

Finally we talk about Galois cohomology and Kummer theory. Galois cohomology is a special case of Group cohomology and the most important theorem here is Hilbert 90 which also has a classical form focusing on finite cyclic Galois extension using the technique of norm and trace. Of course we consider the Galois cohomology for infinite Galois extensions as well which is called continuous cohomology. And this infinite case can be reduced to the finite case via inverse limits and inductive limits (see Proposition 4.31 and Theorem 4.33).

In the end we study Kummer theory which is the starting point of class field theory. Classically multiplicative Kummer theory deduce a correspondence between cyclic extensions and cyclic groups of $F^\times/(F^\times)^n$ where F is assumed to contain n-th primitive root of unity 1. As a generalization there is a concept of Kummer extensions. Interestingly there is also a modern viewpoint of multiplicative Kummer theory using Galois cohomology. Moreover Artin–Schreier theory is an analogy of Kummer theory in the case of char $= p > 0$, which is of the additive form. And there is a viewpoint in Galois cohomology of it as well. All these are themes of Section 4.3.

2 Field Extension

Let F be a field. Its **characteristic** is the minimal positive integer n such that $n \cdot 1 = 0$ in F. If such integer doesn't exist, we say F has characteristic zero. It's obvious to see if $\mathrm{char}(F) \neq 0$, then $\mathrm{char}(F) = p$ where p is a prime number. If $\mathrm{char}(F) = p$, then $(a+b)^p = a^p + b^p$ for $a, b \in F$, since $p | \mathrm{C}_p^i$ where $1 < i < p$.

If K is another field and $f : F \to K$ is a ring morphism, then f is injective since in a field the only proper ideal is (0).

Definition 2.1. *The injection $F \hookrightarrow K$ is called a* ***field extension****, and it can be written as $F \subseteq K$ or K/F as well. Since F is a field, we can view K as a vector space over F, whose dimension is denoted by $\dim_F K = [K : F]$. A field extension $F \subseteq K$ is called* ***finite****, resp.* ***infinite*** *if $[K : F] < \infty$, resp. $[K : F] = \infty$.*

Proposition 2.2. *Let $F \subseteq E \subseteq K$ be field extensions. Then*

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

Proof. If $\{x_i | i \in I\}$ is a basis of E over F, and $\{y_j | j \in J\}$ is a basis of K over E. Then every element $u \in K$ can be written as $u = \sum_{k=1}^{m} a_k y_{j_k}$ where $a_k \in E$. But $a_k = \sum_{l=1}^{m'} b_{kl} x_{i_l}, b_{kl} \in F$. Then $u = \sum_{k,l} b_{kl} x_{i_l} y_{j_k}$. Therefore $\{x_i y_j\}$ generate K over F.

On the other hand, if $\sum_{k,l} c_{kl} x_{i_l} y_{j_k} = 0$, then $\sum_k \sum_l (c_{kl} x_{i_l}) y_{j_k} = 0 \Rightarrow \sum_l c_{kl} x_{i_l} = 0 \Rightarrow c_{kl} = 0$, which means $x_i y_j$'s are independent and form a basis of K over F. Hence $[K : F] = [K : E] \cdot [E : F]$. □

For a field extension $F \subseteq K$, if S is a subset of K, then the smallest subring (resp. subfield) is denoted by $F[S]$ (resp. $F(S)$).

Definition 2.3. *Given a field extension K/F, an element $u \in K$ is called* ***algebraic over*** *F is there is a polynomial $P(X) \in F[X]$ such that $P(u) = 0$ in K. The field extension $F \subseteq K$ is* ***algebraic****, if all elements of K are algebraic over F.*

Theorem 2.4. *If K/F is a finite field extension, then it's algebraic. On the other hand, if $u \in K$ is algebraic over F then $[F(u) : F] < \infty$, where $F(u)$ is the samllest subfield of K containing F and u.*

Proof. If $F \subseteq K$ is finite, for any $u \in K$, $\{1, u^2, ..., u^n, ...\}$ will be dependent. This proves the first statement.

On the other hand, we consider the F-morphism $f : F[X] \to K, X \mapsto u$. Then $F[X]/I \cong im\ f = F[u]$, which is an integral domain. Since $F[X]$ is PID, $I = (P_u)$ generated by a monic prime polynomial P_u. But in a PID, every prime ideal is maximal, thus $F[X]/(P_u) \cong F[u]$ is a field and $F[u] = F(u)$. The monic irreducible polynomial P_u is called the minimal polynomial of u. If $[F(u) : F] = deg(P_u) < \infty$. □

Remark 2.5. If $u, v \in K$ are algebraic over F, then $u \cdot v$ and $u + v$ are algebraic over F as well. It's easy to prove, just considering $F(u, v)$, since $[F(u, v) : F] < \infty$. Similarly, if E, E' are subfields of K containing F, which are algebraic over F, then $E \cdot E'$ is algebraic over F as well.

Theorem 2.6. *Given field extensions $F \subseteq E \subseteq K$, if E/F and K/E are algebraic, then K/F is algebraic as well.*

Proof. Assume $u \in K$, its minimal polynomial over E is $P_u = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, where $a_i \in E$. Since E is algebraic over F, $[F(a_i) : F] < \infty$. Then $[F(a_0, ..., a_{n-1}) : F] \leq \prod_{i=0}^{n-1}[F(a_i) : F] < \infty$. Then u is algebraic over $F(a_0, ..., a_{n-1})$, hence algebraic over F. □

Lemma 2.7. *Given a field extension K/F, $u \in K$ is algebraic over F and P_u is the minimal polynomial of u. If E/F is another field extension and there is an element $v \in E$ such that $P_u(v) = 0$ in E, then there is a unique embedding $F(u) \hookrightarrow E$ such that $u \mapsto v$.*

Proof. $F(u) \cong F[X]/(P_u)$.

$$\begin{tikzcd}
F[X] \arrow[r] \arrow[d] & E \\
F[X]/(P_u) \arrow[ur, dotted, "\exists!"'] &
\end{tikzcd} \tag{1}$$

Since $P_u(v) = 0$, there is a unique morphism $F(u) \to E$. □

2.1 Splitting Fields and Algebraic Closure

Definition 2.8. *Given a field extension K/F, $P \in F[X]$* ***splits*** *in K if P factors as*

$$P(X) = c(X - u_1) \cdot ... \cdot (X - u_n)$$

where $c \in F$, $u_i \in K$. We say K is a ***splitting field*** *of P over F if K is the smallest field in which P splits.*

This definition means that the splitting field K of P is generated by its roots.

Theorem 2.9. *For any $P \in F[X]$ there exists a splitting field K of it over F (unique up to isomorphism) and moreover $[K : F] \leq n!$ where $n := \deg(P)$.*

Proof. We prove the unique existence of splitting field by induction on the degree of P. If $n = 1$, $P = c(X - u)$. Since $c, cu \in F$, $u \in F$, then $K = F$. We assume it's true for $n - 1$, $\deg(P) = n$, and P doesn't split in F. We write P as $P = \prod_i Q_i$ where Q_i is irreducible. Choose one $Q_i = Q$, $\deg Q \leq degP$. We consider the field $F_1 = F[X]/(Q)$,$u = \bar{X}$, $[F_1 : F] = deg(Q) \leq n$. All coefficients of P are in F, thus $P(X) \in F_1[X]$. But $P(u) = 0$, $P(X) = (X - u)P_1(X)$, $deg(P_1(X)) = n - 1$. Then there is a unique splitting field K of P_1 over F_1 and $[K : F_1] \leq (n-1)!$. According to the definition of splitting fields it's obvious to see K is a splitting field of P over F and $[K : F] = [K : F_1] \cdot [F_1 : F] \leq (n - 1)! \cdot n = n!$. If K' is another splitting field of P over F, then according to the Lemma 2.7, there is an embedding $F_1 \hookrightarrow K'$. Then K' will also be a splitting field of P_1 over F_1. Since $deg(P_1) = n - 1$, $K \cong K'$.

Note though the splitting field is unique, isomorphisms between them may not be unique. □

Definition 2.10. *A field F is called* ***algebraically closed*** *if for any algebraic field extension K/F, $K = F$. K/F is called an* ***algebraic closure*** *if it's algebraic and K is algebraically closed.*

According to the definition, we know K is algebraically closed iff every polynomial $P(X) \in K[X]$ with $\deg(P) \geq 1$ decomposes in $K[X]$ into a product of linear factors $P(X) = c\prod_i(X - u_i)$ where $c \in K^\times, u_i \in K$.

Theorem 2.11. *The algebraic closure $\bar{F}$ of F always exists and is unique up to isomorphism.*

To prove the theorem above, we need to know Zorn's lemma, which is equivalent to the axiom of choice.

Lemma 2.12 (Zorn)**.** *let M be a partially ordered set such that every subset of M that is totally ordered with respect to the order induced by M admits an upper bound in M. Then there exists a maximal element in M.*

Proposition 2.13. *Every field F admits an extension field K which is algebraically closed.*

Proof. The construction process of K will be based on polynomial rings in infinitely many variables over F following E. Artin. In the first step we set up a field K_1 extending F such that every $f \in F[X]$ with $\deg(f) \geq 1$ admits a zero in K_1. To do this we consider the system of variables $\mathfrak{X} = \{X_f | f \in F[X],\ \deg(f) \geq 1\}$ and $F[\mathfrak{X}]$. We assume the ideal $I = (f(X_f))$ is generated by all polynomials of one variable $f(X_f)$ where $f \in F[X]$, $\deg(f) \geq 1$. We prove it's a proper ideal in $F[\mathfrak{X}]$ first.

If $I = F[\mathfrak{X}]$, then we have the equation

$$\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1$$

There will exist a field F' containing F such that every polynomial f_i has a root u_i in F'. We can construct F' as follows. First choose an irreducible factor h_1 of f_1 over F, and let $F_1 = F[X]/(h_1)$. Then choose an irreducible factor h_2 of f_2 over F_1, since $f_2 \in F_1[X]$, then $F_2 = F_1[X]/(h_2)$. Continuing this process, we will finally obtain such F'.

Now we consider the F-morphism $F[\mathfrak{X}] \to F'$ such that $X_{f_i} \mapsto u_i$, other $X_f \mapsto 0$. Then the equation above of left hand vanishes. A contradiction! Thus I is proper. We choose a maximal ideal $\mathfrak{m}$ of $F[\mathfrak{X}]$ containing I and let $K_1 = F[\mathfrak{X}]/\mathfrak{m}$. Then there is a canonical map

$$F \hookrightarrow F[\mathfrak{X}] \to F[\mathfrak{X}]/\mathfrak{m} = K_1$$

The residue class of X_f in K_1 is denoted by $\bar{X}_f$, and it's a root of $f(X)$. Continuing this process, we obtain the sequence

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq ...$$

Let $K = \cup_{i=0}^{\infty} K_i$. We prove it's algebraically closed. Given any polynomial $f \in K[X]$, all coefficients will lie in some K_n. Then it has a root in K_{n+1}. f will factor as $f = (X - u_1)f_1$, where $f_1 \in K_{n+1}$. Continuing this factorization process, we will finally obtain $f = c\prod_i (X - u_i)$ where $c \in K^*, u_i \in K$. □

Proof of Theorem 2.11. According to Proposition 2.13, there is an algebraically closed field K extending F. We define

$$\bar{F} := \{u \in K | u \text{ is algebraic over } F\}$$

From the Remark 2.5, we know $\bar{F}$ is actually an algebraic field extension of F. Given $f(X) = a_n X^n + \cdots + a_0 \in \bar{F}[X]$, then all roots v_i of it are in K, which means these v_i's are algebraic over $F(a_0, \ldots, a_n)$ hence algebraic over F and then $v_i \in \bar{F}$.

Next we will use the Lemma 2.7 and Zorn's lemma to prove the uniqueness of the algebraic closure, which is the corollary of the next proposition, though the isomorphism between algebraic closures are not unique nor canonical. □

Proposition 2.14. *Given a field extension L/F and a field morphism $\sigma : F \hookrightarrow K$ such that L/F is algebraic and K is algebraically closed, then σ can be extended to be an extension $\sigma' : L \hookrightarrow K$. If moreover, L is algebraically closed and K is algebraic over $\sigma(F)$, then every extension σ' of σ is an isomorphism.*

Proof. If $u \in L$ and $P_u \in F[X]$ is the minimal polynomial of u over F, then $\sigma(P_u)$ has a root v in K and according to the Lemma 2.7, there will be a unique morphism $F(u) \hookrightarrow K, u \mapsto v$. Let M be the set of pairs (E, τ) such that E is a subfield of L containing F and $\tau : E \hookrightarrow K$ extends $\sigma : F \hookrightarrow K$. $(E, \tau) \leq (E', \tau')$ if $E \subseteq E'$ and

τ' extends τ. The statement above shows M is not empty. If N is a totally ordered subset of M, it's obvious to see it has an upper bound $E' = \cup_{E \in N} E, \sigma'|E = \sigma$. By Zorn's lemma, there is an maximal element (E', σ') in M. According to the Lemma 2.7, we can conclude $E' = L$.

If moreover L is algebraically closed and K is algebraic over $\sigma(F)$ hence algebraic over $\sigma'(L)$, there is a morphism $\mu : K \hookrightarrow L$ extending $\sigma'^{-1} : \sigma'(L) \to L$. Then $\mu \circ \sigma' = id_L$, and μ is surjective. Hence μ is an isomorphism, whose converse is σ'. □

In the following, for every field F we always fix an algebraic closure $\bar{F}$, and its field extensions considered are contained in $\bar{F}$.

Example 2.15. The complex field $\mathbb{C}$ is an algebraic closure of the field $\mathbb{R}$ of real numbers. There is a generalization of this example, which is called Artin-Schreier theorem[1] that if $\bar{F}$ is the algebraic closure of F and $1 < [\bar{F}, F] < \infty$, then $[\bar{F} : F] = 2$ and -1 is not a square root in F, which means $\bar{F} = F(\sqrt{-1})$.

From the proof of the Theorem 2.11, we know if $\mathbb{Q}$ is the field of rational numbers, then

$$\bar{\mathbb{Q}} = \{u \in \mathbb{C} \mid u \text{ is algebraic over } \mathbb{Q}\}.$$

Therefore there are only countably many elements in $\bar{\mathbb{Q}}$ and then $\bar{\mathbb{Q}} \neq \mathbb{C}$.

Exercise 2.16. Let p be a prime number. Decide the splitting field (in the algebraic closure $\bar{\mathbb{Q}}$) of $X^p - 2 \in \mathbb{Q}[X]$.

2.2 Normal Extension

Definition 2.17. *A field extension $F \subseteq K \subseteq \bar{F}$ is called **normal**, if every irreducible polynomial $P(X) \in F[X]$ admitting a zero in K splits over K (which means all its roots in $\bar{F}$ are in K).*

Theorem 2.18. *The following statements are equivalent:*

(1) K/F is normal.

(2) Every F-embedding $\iota : K \hookrightarrow \bar{F}$ satisfies $\iota(K) \subseteq K$.

(3) $\mathrm{Hom}_F(K, \bar{F}) = \mathrm{Hom}_F(K, K)$.

If moreover $[K : F] < \infty$ then the above statements are equivalent to that K is a splitting field of some $P(X) \in F[X]$.

[1] See [Jac89] Theorem 11.14 or [Bos18] Section 6.3 for details.

Proof. The equivalence of (2) and (3) is obvious and we only prove the equivalence between (1) and (2).

(1) $\Rightarrow$ (2) Assume K/F is normal, $u \in K$ and P_u is the minimal polynomial of u over F. Then all roots of P_u are in K. For any F-embedding $\iota : K \hookrightarrow \bar{F}$, $\iota(u)$ is a root of P_u since $\iota(P_u(u)) = P_u(\iota(u)) = 0$. Then $\iota(u) \in K$, $\iota(K) \subseteq K$.

(2) $\Rightarrow$ (1) If the irreducible polynomial $P \in F[X]$ has a root u in K, then $P = P_u$ is the minimal polynomial of u over F. If v (may equal u) is another root of P in $\bar{F}$, then there is a morphism $F(u) \to \bar{F}, u \mapsto v$, which can be extended to be $\iota : K \to \bar{F}$ according to Proposition 2.14. Then $\iota(u) = v \in K$. Hence K/F is normal.

Now suppose $[K : F] < \infty$. First we assume $F \subseteq K$ is normal and choose $u_1 \in K - F$. Then its minimal polynomial is P_{u_1} and $[K : F(u_1)] < [K : F]$. Next we choose $u_2 \in K - F(u_1)$. Continuing this process, we conclude $K - F(u_1, ..., u_n)$. Let $P = \prod_{i=1}^{n} P_{u_i}$, and then K is the splitting field of P.

On the other hand, if K is the splitting field of $P \in F[X]$ whose roots in $\bar{F}$ are $\{u_1, ..., u_n\}$. Then $K = F(u_1, ..., u_n)$. Consider an F-embedding $\iota : F(u_1, ..., u_n) \to \bar{F}$, since $\iota(u_i)$ is a root of P as well, $\iota(u_i) \in K$. Hence $\iota(K) \subseteq K$. □

Corollary 2.19.

(1) For field extensions $F \subseteq E \subseteq K \subseteq \bar{F}$, if K/F is normal then K/E is normal. But E/F is not necessarily normal.

(2) If E/F and E'/F are normal, then $E \cdot E'/F$ is normal.

Proof. (1). Given an element $u \in K$, P_u and P'_u are its minimal polynomials over F and E respectively. Then $P'_u | P_u$. Since all roots of P_u are in K, all roots of P'_u are also in K. HenceK/E is normal.

(2). Given any embedding $\iota : E \cdot E' \to \bar{F}$, since E/F and E'/F are normal, $\iota(E) \subseteq E, \iota(E') \subseteq E'$. Then $\iota(E \cdot E') \subseteq E \cdot E'$. Then $E \cdot E'/F$ is normal. □

Remark 2.20. The property of being normal is not transitive, i.e. for field extensions $F \subseteq E \subseteq K$, if $F \subseteq E$ and $E \subseteq K$ are normal, the field extension $F \subseteq K$ need not be normal. For example $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ are normal since they are of degree 2. But $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is not normal. Indeed, the polynomial $X^4 - 2$ is irreducible over $\mathbb{Q}$ according to the Eisenstein's criterion, and $\sqrt[4]{2} \cdot i$ is also a root of $X^4 - 2$, but $i \notin \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$.

Moreover, the splitting field of $X^4 - 2$ is $\mathbb{Q}(\sqrt[4]{2}, i)$ since its roots are $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2} \cdot i, -\sqrt[4]{2} \cdot i$. Then for field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$. Though $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$ is normal, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is not normal.

2.3 Separable Extension

Definition 2.21. *Given $P(X) \in F[X]$ (may not be irreducible), it is called* ***separable*** *if it has no multiple roots in $\bar{F}$, otherwise* ***inseparable****.*

For a field extension $F \subseteq K$, an element $u \in K$ is called separable if its minimal polynomial P_u is separable. The field extension $F \subseteq K$ is called separable if all elements of K are separable.

For a polynomial $P(X) = \sum_k a_k X^k \in F[X]$, we define its derivative $P'(X) = \sum_k k a_k X^{k-1}$.

Lemma 2.22. *Given a polynomial $P(X) \in F[X]$, it has multiple roots in $\bar{F}$ iff $(P, P') \neq 1$ in $\bar{F}$. Moreover if P is irreducible, then P has multiple roots iff $P' = 0$.*

Proof. Write $P(X) = c\prod_{i=1}^{n}(X - u_i)$, then

$$P'(X) = c\sum_{i=1}^{n}(X - u_1)\cdot ... \cdot(X - u_{i-1})(X - u_{i+1})\cdot ... \cdot(X - u_n).$$

If P has multiple roots, say $u_1 = u_2$, then $P'(u_1) = 0$ and so $(X - u_1)|(P, P')$. Conversely, if $u_i \neq u_j$ for any $i \neq j$, then $P'(u_i) \neq 0$ for any $1 \leq i \leq n$, thus $(P, P') = 1$.

If moreover P is irreducible, then$(P, P') = 1$ or P. Hence P has multiple roots iff $(P, P') = P$. But deg$P' \leq n - 1$, we must have $P' = 0$. □

Remark 2.23. If char$(F) = 0$, any nonconstant polynomial P will have a non zero derivative P'. Therefore, any field extension of characteristic 0 is separable. But it's not true when char$(F) = p > 0$.

For example, let $F = \mathbb{F}_p(t) = Q(\mathbb{F}_p[t])$ the function field over the finite field $\mathbb{F}_p$. Suppose $P(X) = X^p - t \in F[X]$. According the Eisenstein's criterion t is a prime element of $\mathbb{F}_p[t]$ and $t|t, t^2 \nmid t, t \nmid 1$. Then $P(X)$ is irreducible in $\mathbb{F}_p[t][X]$ hence irreducible in $Q(\mathbb{F}_p[t])[X] = F[X]$. But $P(X)$ is inseparable since $P'(X) = pX^{p-1} = 0$. The splitting field of P is not separable.

Since all field extensions of characteristic 0 are separable, we assume char$(F) = p > 0$ in the following.

Exercise 2.24. A field F is called *perfect* if every irreducible polynomial $F[X]$ is separable. Prove the following statements.

(1) A field F with F $= p > 0$ is perfect iff $F^p = F$.

(2) Every finite field is perfect.

Remark 2.25. $P(X) \in F[X]$ is an irreducible and inseparable polynomial. Then P has multiple roots in $\bar{F}$ and $P' = 0$. If $P = \sum_k a_k X^k$, then $P' = \sum_k k a_k X^{k-1} = 0$, $p \nmid k \Rightarrow a_k = 0$. Hence $P = \sum_k a_{pk} X^{pk} = P_1(X^p)$, where $P_1 = \sum_k a_{pk} X^k \in F[X]$. Since P is irreducible, P_1 is irreducible as well. If P_1 is separable, we are done. Otherwise, we continue this process. Since $deg(P) < \infty$, finally we will obtain an irreducible and separable polynomial P_e such that $P(X) = P_e(X^{p^e})$. $n_s = deg(P_e) \Rightarrow n = n_s \cdot p^e = deg(P)$. Here n_s is called the **separable degree** and p^e is called the **inseparable degree** of P.

Lemma 2.26. *Given a field extension K/F, $u \in K$ is separable over F iff $F(u) = F(u^p)$.*

Proof. We assume u is separable first. Then $F_1 = F(u^p) \subseteq F(u)$. Consider the polynomial $X^p - u^p \in F_1[X]$ and u is a root of it. Let P be the minimal polynomial of u over $F_1 \Rightarrow P | X^p - u^p$. But $X^p - u^p = (X-u)^p$. Thus $P = (X-u)^k$ for some integer k. Since P is separable and all roots of it are different, $P = X - u$. Hence $u \in F_1$. Then $F(u) = F(u^p)$.

On the other hand, we assume $F(u) = F(u^p)$. Let P be the minimal polynomial of u over F. If P is not separable, then $P(X) = P_1(X^p)$ according to the Remark 2.25. Since P_1 is irreducible and $P(u^p) = 0$, P_1 is the minimal polynomial of u^p. Then $[F(u) : F] = [F(u^p) : F] = degP = degP_1 = p \cdot degP_1$. A contradiction! Hence P is separable and u is separable. □

Proposition 2.27.

(1) $F \subseteq E \subseteq K$ are field extensions. K/F is separable iff E/F and K/E are separable.

(2) If E/F and E'/F are separable, then $E \cdot E'/F$ is separable.

The part of $\Rightarrow$ of (1) is trivial. But the part of $\Leftarrow$ is not easy and we need more characterizations of the property of being separable.

Lemma 2.28. *Assume $[K : F] = d < \infty$. The following statements are equivalent.*

(1) $F \subseteq K$ is separable.

(2) $K = F \cdot K^p$, where $K^p = \{k^p | k \in K\}$ a subfield of K since $char(F) = char(K) = p > 0$;

(3) There is a basis $\{e_1, ..., e_d\}$ of K over F such that $\{e_1^p, ..., e_d^p\}$ is still a basis.

Proof. (1) $\Rightarrow$ (2): Since all $u \in K$ are separable over F, $F(u) = F(u^p)$ according to the Lemma 2.26. Then $u \in F(u^p) \subseteq F \cdot K^p$. Hence $K \subseteq F \cdot K^p$. $F \cdot K^p \subseteq K$ is obvious.

(2) $\Rightarrow$ (3): Assume $K = Fe_1 \oplus ... \oplus Fe_d$. Then $k = \sum_i f_i e_i \Rightarrow k^p = \sum_i f_i^p e_i^p$. Hence $K^p = F^p e_1^p + ... + F^p e_d^p$. $F \cdot K^p = Fe_1^p + ... + Fe_d^p = K$. Since $[K : F] = d$, $\{e_1^p, ..., e_d^p\}$ is still a basis. Also from $F \cdot K^p = Fe_1^p + ... + Fe_d^p = K$, it's obvious to see (3) $\Rightarrow$ (2).

(2) $\Rightarrow$ (1): We assume $u \in K$ is inseparable. Then if P is the minimal polynomial of u, then $P(X) = P_1(X^p) = \sum_{k=0}^n a_k X^{pk}$. $P(u) = 0 \Rightarrow \{1, u^p, ..., u^{np}\}$ are linearly dependent, but $\{1, u, ..., u^{np-1}\}$ are linearly independent. Accordting to the proof of (2). $\Rightarrow$ (3)., $\{1, u^p, ..., u^{p(np-1)}\}$ are linearly independent. But $n \leq 2n - 1 \leq pn - 1$, $\{1, u^p, ..., u^{np}\} \subseteq \{1, u^p, ..., u^{p(np-1)}\}$ are linearly independent. A contradiction! □

Lemma 2.29. *A simple algebraic extension $F(u)/F$ is separable iff u is separable over F.*

Proof. The part of $\Rightarrow$ is trivial and it's enough to prove the part of $\Leftarrow$. If $P(X) \in F[X]$ is the minimal polynomial of u over F, $P(X) = \sum_k a_k X^k$ with $deg(P) = n$, then $\{1, u, ..., u^{n-1}\}$ form a basis of $F(u)$ over F. We prove $\{1, u^p, ..., u^{p(n-1)}\}$ is a basis as well. If this is true, from the Lemma 2.28, $F \subseteq F(u)$ is separable. If this is not true, there will exist $\{b_k\}$ which are not all zero such that $\sum_k b_k u^{kp} = 0$. Let $P_1(X) = \sum_k b_k X^k$, with $deg(P_1) \leq n-1$. $P_1(u^p) = 0$. Then $[F(u^p) : F] \leq deg(P_1) \leq n - 1$. But since u is separable, according to the Lemma 2.26 $F(u) = F(u^p)$, $[F(u) : F] = [F(u^p) : F] = n$, a contradiction! Hence $\{1, u^p, ..., u^{p(n-1)}\}$ is a basis as well. □

Proof of Proposition 2.27. (1). We only prove the part of $\Leftarrow$. If $[K : F] < \infty$, $K = E \cdot K^p = (F \cdot E^p) \cdot K^p = F \cdot (E^p \cdot K^p) = F \cdot K^p$. Hence K/F is separable.

If $[K : F] = \infty$, $u \in K$ and $P_u \in E[X]$ is the minimal polynomial of u over E. $P_u(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$. Consider $F \subseteq F(a_0, ..., a_{n_1}) \subseteq E \subseteq E(u) \subseteq K$. Since E/F is separable, according to the part of $\Rightarrow$ of 1., we know $F(a_0, ..., a_{n-1})/F$ is separable. And since the minimal polynomial of u over $F(a_0, ..., a_{n_1})$ is just P_u, which is separable. Then from the Lemma 2.29, $F(a_0, ..., a_{n_1}, u)/F(a_0, ..., a_{n_1})$ is separable. Since $[F(a_0, ..., a_{n_1}, u) : F] < \infty$, $F(a_0, ..., a_{n_1}, u)/F$ is separable and especially u is separable.

(2). Assume $u \in E, u' \in E$ and their minimal polynomials are P_u and $P_{u'}$ respectively. Then since u is separable, $F(u)/F$ is separable. The minimal polynomial of u' over $F(u)$ divides $P_{u'}$, hence separable as well. Then $F(u, u')/F(u)$ is separable $\Rightarrow F(u, u')/F$ is separable. Hence $u \cdot u'$, $u + u'$ and $u - u'$ are all separable. This proves the part of (2). □

According to the proof of the part (2) above, we know given an algebraic extension K/F, all separable elements in K form a subfield containing F, which is denoted by K_s. Especially if $K = \bar{F}$, $\bar{F}_s$ is denoted by F_{sep} and called the **separable closure**. This motivates us to study K_s/F and K/K_s respectively, which is the task in the next subsection.

2.4 Purely Inseparable Extension

Definition 2.30. *For an algebraic extension K/F, the **separable degree** is defined to be $[K : F]_s = [K_s : F]$ and the **inseparable degree** is $[K : F]_i = [K : K_s]$.*

Definition 2.31. *A polynomial $P(X) \in F[X]$ is called **purely inseparable** if it admits only one zero $u \in \bar{F}$. Given an algebraic extension $F \subseteq K$, $u \in K$ is called purely inseparable if it's the root of a purely inseparable polynomial in $F[X]$. This algebraic extension is purely inseparable if all its elements are purely inseparable over F.*

Remark 2.32. If $P(X) \in F[X]$ is monic, irreducible and purely inseparable with $deg(P) = p^r m > 1$ where $p \nmid m$, then according the Remark 2.25 $P(X) = P_1(X^p)$, with P_1 monic and irreducible. $P_1(X) = 0 \Leftrightarrow P(X^{\frac{1}{p}}) = 0 \Leftrightarrow X^{\frac{1}{p}} = u \Leftrightarrow X = u^p$, which means P_1 is purely inseparable. Continue this process. Finally we obtain $P_e(X)$ with $deg(P_e) = m$. But P_e is also purely inseparable, if $m > 1$ then it's inseparable and hence $p|m$. A contradiction! Therefore $m = 1$ and $P(X) = X^{p^e} - c$ where $c = u^{p^e}$. In a summary, given an algebraic extension K/F, $u \in K$ is purely inseparable iff u is the root of a polynomial $X^{p^n} - c \in F[X]$ iff $u^{p^n} \in F$ for some n.

Fact 2.33.

(1) If K/F is a finite purely inseparable extension, then $[K : F]$ is a power of p.

(2) If E/F and K/E are purely inseparable, then K/F is purely inseparable as well.

(3) If E/F and E'/F are purely inseparable, then $E \cdot E'/F$ is purely inseparable.

Proof. (1). Since K/F is finite, $u \in K$ is the root of some polynomial $X^{p^n} - c \in F[X]$. Hence the degree of its minimal polynomial is the power of p. Moreover, if E is any subfield of K containing F, then the minimal polynomial of $u \in K$ over E divides that over F, hence whose degree is the power of p as well. Since $K = F(u_1, ..., u_m)$ we conclude $[K : F] = [F(u_1, ..., u_m) : F(u_1, ..., u_{m-1})] \cdot ... \cdot [F(u_1) : F]$ is a power of p.

(2). Let $u \in K$. Since K/E is purely inseparable, there is some n such that $u^{p^n} \in E$. E/F is purely inseparable as well. Then $(u^{p^n})^{p^m} = u^{p^{n+m}} \in F$. Therefore K/F is purely inseparable.

(3). For any $u \in E, v \in E'$, there are integers n and m such that $u^{p^n}, v^{p^m} \in F$. Then $(u \cdot v)^{p^{n+m}}, (u + v)^{p^{n+m}} \in F$. Hence $E \cdot E'/F$ is purely inseparable. □

Proposition 2.34. *$K_s \subseteq K$ is purely inseparable.*

Proof. Assume $u \in K$ and P is the minimal polynomial of u over K_s. According the Remark 2.25, there is an irreducible and separable polynomial P_e such that $P_e(X^{p^e}) = P(X)$. Then $P_e(u^{p^e}) = 0$, which means P_e is the minimal polynomial of

u^{p^e} over K_s and u^{p^e} is separable over K_s. Thus $u^{p^e} \in K_s$ and then $P_e(X) = X - u^{p^e}$. $P(X) = X^{p^e} - u^{p^e}$ and u is purely inseparable over K_s. □

Remark 2.35. If $F(u)/F$ is a simple algebraic extension, then we prove $[F(u) : F]_s = n_s$ where n_s comes from the Remark 2.25 and is the degree of P_e.

Proof. Since u^{p^e} is separable, $F(u^{p^e}) \subseteq F(u)_s$. If $v \in F(u)_s - F(u^{p^e})$ is separable over F and is independent from $\{1, u^{p^e}, ..., u^{p^e(n_s-1)}\}$. According to the Lemma 2.26, $F(u^{p^e}, v) = F(u^{p^e}, v^{p^e})$ and then v^{p^e} is independent from $\{1, u^{p^e}, ..., u^{p^e(n_s-1)}\}$. Since $\{1, u, ..., u^{p^e n_s - 1}\}$ form a basis of $F(u)$ over F, $v = \sum_k a_k u^k$ and $v^{p^e} = \sum_k a_k^{p^e} u^{p^e k}$. Since $u^{p^e n_s}$ is a linear sum of $u^{p^e k}$, v^{p^e} is a linear sum of $u^{p^e k}$ as well, where $0 \leq k \leq n_s - 1$. A contradiction! Hence $F(u^{p^e}) = F(u)_s$ and $n_s = [F(u^{p^e}) : F] = [F(u)_s : F]$. □

Theorem 2.36. *Given a finite algebraic extension K/F, we have the following equation*

$$[K : F]_s = |\mathrm{Hom}_F(K, \bar{F})|$$

then $|\mathrm{Hom}_F(K, \bar{F})| \leq [K : F]$ and $|\mathrm{Hom}_F(K, \bar{F})| = [K : F]$ iff $[K : F] = [K : F]_s$ iff $F \subseteq K$ is separable.[2]

Proof. Consider $F \subseteq K_s \subseteq K$. We first prove $\mathrm{Hom}_F(K, \bar{F}) = \mathrm{Hom}_F(K_s, \bar{F})$. In fact there is a map $\mathrm{Hom}_F(K, \bar{F}) \to \mathrm{Hom}_F(K_s, \bar{F}), \tau \mapsto \tau | K_s$. According to the Proposition 2.14, this map is surjective. Thus it's enough to prove it's injective.

From the Proposition 2.33 we know $K_s \subseteq K$ is purely inseparable, which means every $u \in K$ is the only root of a polynomial $X^{p^n} - c \in K_s[X]$, where $c = u^{p^n}$. In fact, given any $\tau : K \to \bar{F}$, we assume $v = \tau(u^{p^n}) = \tau(u)^{p^n}$. Then consider the polynomial $X^{p^n} - v \in \bar{F}[X]$. If v' is a root of it, then $X^{p^n} - v = (X - v')^{p^n}$. Hence the root v' is unique. But since $\tau(u)$ is the root of $X^{p^n} - \tau(c) = X^{p^n} - v$, $\tau(u) = v'$, which means τ is determined by $\tau | K_s$ and we could only consider F-morphisms $K_s \to \bar{F}$.

Given a separable element $v \in K_s$, P is its minimal polynomial over F with $deg(P) = n = [F(v) : F]$. Then P is irreducible and separable, whose roots are all different in $\bar{F}$. According to the Lemma 2.7, there are only n's different F-morphisms $F(v) \to \bar{F}$. By induction, we conclude $[K_s : F] = |\mathrm{Hom}_F(K_s, \bar{F})| = |\mathrm{Hom}_F(K, \bar{F})|$. □

2.5 Appendix on Finite Fields

In this section, we review some basic facts about finite fields. Actually all finite fields are of the form $\mathbb{F}_q$ having q elements where $q = p^n$ and p is prime. Note $\mathbb{F}_q$ is different from $\mathbb{Z}/q\mathbb{Z}$ if $n > 1$.

[2] In some textbooks such as [Bos18] and [Lan02], the equation above is the definition of the separable degree. And to prove the equation without the assumption of finite degree we may need the transfinite induction.

Remark 2.37. If $\mathbb{F}$ is a finite field, then $\mathrm{char}(F) = p > 0$, therefore $\mathbb{F}_p \subseteq \mathbb{F}$ and it's a finite algebraic extension. Viewing $\mathbb{F}$ as a vector space over $\mathbb{F}_p$, we know there must be $q = p^n$ elements in $\mathbb{F}$. Then the multiplicative group $\mathbb{F}^\times$ has order $q-1$ and all elements of $\mathbb{F}^\times$ are roots of the polynomial $X^{q-1} - 1$. Hence $\mathbb{F}$ is the splitting field of $X^q - X$ over $\mathbb{F}_p$. According to the Theorem 2.18, it's normal.

On the other hand, if $q = p^n$ then all roots of $X^q - X$ in $\bar{\mathbb{F}}_p$ form a subfield, since $(u+v)^{p^n} = u^{p^n} + v^{p^n}$.

Lemma 2.38. *Let F be a field and H is a finite subgroup of the multiplicative group $F^\times$. Then H is cyclic.*

Proof. For all elements of H there exists one $a \in H$ with the maximal order m. Let H_m be the subgroup of all elements in H whose order divides m. Then all elements of H_m are zeros of the polynomial $X^m - 1$. Hence $|H_m| \leq m$. But $< a > \subseteq H_m$ therefore $H_m =< a >$ and it's cyclic. If there is some $b \in H - H_m$ whose order n doesn't divides m, then there will be an element with order $\mathrm{lcm}(n, m) > n$. A contradiction! Hence $H_m = H$. □

Corollary 2.39. *For any finite field $\mathbb{F}_q$, its multiplicative group $\mathbb{F}_q^\times$ is cyclic.*

3 Galois Theory

We fix some notations first.

If K/F is a field extension not necessarily algebraic, we define

$$\mathrm{Aut}_F(K) := \{\tau : K \xrightarrow{\sim} K |\ \tau|F = id_F\}$$

then $\mathrm{Aut}_F(K)$ is a group. For any two $\tau, \sigma \in \mathrm{Aut}_F(K)$, we let $\sigma \cdot \tau = \sigma \circ \tau : K \xrightarrow{\tau} K \xrightarrow{\sigma} K$.

Fact 3.1. If K/F is algebraic, then $\mathrm{Aut}_F(K) = \mathrm{Hom}_F(K, K)$.

Proof. Given any F-morphism $\tau : K \to K$, we know it's injective and it' enough to prove it's surjective. We assume $u \in K$ and $P \in F[X]$ is its minimal polynomial over F. If $u_1, ..., u_n$ are its different roots in $\bar{F}$, we assume only $u_1, ..., u_r$ are in K. Then $u \in \{u_1, ..., u_r\}$. Since τ fixes F, $\tau(u_i)$ is also a root of P in K where $1 \leq i \leq r$. Then $\tau : \{u_1, ..., u_r\} \to \{u_1, .., u_r\}$. That τ is injective implies it's surjective on this subset as well, which means $\exists u_i, \tau(u_i) = u$. □

There are tow operations we should know:

1. If $H \leq \mathrm{Aut}_F(K)$, $K^H := \{u \in K | \forall \tau \in H, \tau(u) = u\}$ a subfield of K containing F.
2. If $F \subseteq E \subseteq K$, then $\mathrm{Aut}_E(K) \leq \mathrm{Aut}_F(K)$.

and it's obvious to see

1. If $H_1 \leq H_2$, then $K^{H_2} \subseteq K^{H_1}$.
2. If $E_1 \subseteq E_2$, then $\mathrm{Aut}_{E_2}(K) \leq \mathrm{Aut}_{E_1}(K)$.

Definition 3.2. *An algebraic extension K/F is called* ***Galois*** *if it's normal and separable. And the* ***Galois group*** *is defined to be* $\mathrm{Gal}(K/F) := \mathrm{Aut}_F(k)$.

Remark 3.3. If we assume K/F is Galois, then $\mathrm{Hom}_F(K, \bar{F}) = \mathrm{Hom}_F(K, K) = \mathrm{Aut}_F(K) = \mathrm{Gal}(K/F)$. In particular if K/F is finite, $|\mathrm{Gal}(K/F)| = [K : F]$ according to the Theorem 2.36.

Remark 3.4. Given an algebraic extension K/F, there exists a smallest normal extension N/F such that $K \subseteq N \subseteq \bar{F}$ and this normal extension is called the **normal closure**. If $K = F(\mathfrak{U})$ where $\mathfrak{U} = \{u_i\}$ is a family of elements in K and P_i's are their minimal polynomial over F. If M/F is any normal extension containing K, then all roots of P_i are in M. Let N be the field generated by all roots of P_i in $\bar{F}$. Then $F \subseteq K \subseteq N \subseteq M$. Consider the F-embedding $\iota : N \to \bar{F}$, which is determined by its values on roots of those P_i. But if u is a root of P, then $\iota(u)$ is a root of P as well. We see $\iota(N) \subseteq N$. According to the Theorem 2.18, N/F is normal. Hence N/F is the normal closure of F/K. And this normal closure is unique, since it's the intersection of all such M.

If K/F is finite, then the family $\mathfrak{U}$ has only finitely many elements and there are only finitely many polynomials P_i, hence $[N : F] < \infty$. Moreover if we assume K/F is separable, then $N = K(u_1, ..., u_n)$ where u_i is some root of irreducible and separable polynomial $P_i \in F[X]$. According to the Lemma 2.29, N/F is finite separable, hence finite Galois.

For any algebraic field extension K/F we define the **Galois closure** to be the smallest Galois extension E/F such that $F \subseteq K \subseteq E \subseteq \bar{F}$. If K/F is finite separable, we have seen that the Galois closure is just the normal closure of K/F which is finite as well.

Example 3.5. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. The irreducible polynomial $X^3 - 2$ has roots $\sqrt[3]{2}, \sqrt[3]{2}\xi_3, \sqrt[3]{2}\xi_3^2$, where $\xi_3 = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$ and $\xi_3^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$. Though $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$, the other roots are not in $\mathbb{Q}(\sqrt[3]{2})$. But $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is finite separable. Hence its Galois closure is just its normal closure $\mathbb{Q}(\sqrt[3]{2}, \xi_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ of degree 6 over $\mathbb{Q}$.

Now we try to introduce the most important theorem Galois correspondence between group theory and field theory. But before that we should prove a general but difficult lemma of E. Artin. The following lemma is a summary of sections 5.6 and 5.7 in [Art07].

Lemma 3.6 (E. Artin)**.** *Let K be a field and $H = \{\tau_1, ..., \tau_n\}$ is a finite subgroup of* $\mathrm{Aut}(K)$*. If $E = K^H$, then K/E is finite Galois with degree $[K : E] = |H| = n$.*

We divides three steps to prove this lemma.

1. Step 1: $[K : E] \geq n$.
2. Step 2: $[K : E] \leq n$.
3. Step 3: K/E is Galois i.e. normal and separable.

To prove the step 1, we need the following lemma:

Lemma 3.7. *Let K be a field and $H = \{\tau_1, ..., \tau_n\}$ is a finite subset (not necessarily a subgroup) of* $\mathrm{Aut}(K)$ *whose elements are all different. If there are $c_i \in K$ such that*

$$c_1\tau_1(x) + ... + c_n\tau_n(x) = 0$$

for all $x \in K$, then $c_i = 0$, $i = 1, ..., n$.

Proof. If there are non trivial relations among τ_i, we may assume

$$c_1\tau_1(x) + ... + c_r\tau_r(x) = 0$$

for all $x \in K$ such that $c_i \neq 0$ for $i = 1, .., r$ and r is the smallest one. Evidently $r \geq 2$, otherwise $r = 1$ and $c_1\tau_1(x) = 0$ for all $x \in K$. Since τ_1 is an automorphism, it's impossible. Replacing x by ax where $a \in K^*$, we have

$$c_1\tau_1(a)\tau_1(x) + ... + c_r\tau_r(a)\tau_r(x) = 0$$

This yields the following relation:

$$c_1[\tau_1(a) - \tau_r(a)]\tau_1(x) + ... + c_{r-1}[\tau_{r-1}(a) - \tau_r(a)]\tau_{r-1}(x) = 0$$

which is shorter than we have assumed. Hence $\tau_i(a) = \tau_r(a)$ where $i = 1, ..., r-1$ for all $a \in K^*$, which means $\tau_1 = \tau_r$, $r \geq 2$. A contradiction! □

Proof of Lemma 3.6. Step 1: $[K : E] \geq n$.

Assume $[K : E] = r < n$ and let $x_1, ..., x_r$ be a basis of K over E. Then for each $y \in K$ there are $c_i \in E$ such that

$$y = c_1x_1 + ... + c_rx_r$$

Consider the $r \times n$ matrix $(\tau_j(x_i))$ with rank $\leq r < n$. Hence there are $\xi_i \in K$ not all trivial such that $\xi_1\tau_1(x_i) + ... + \xi_n\tau_n(x_i) = 0$ for all $1 \leq i \leq n$.

$$\begin{cases} \xi_1\tau_1(x_1) + ... + \xi_n\tau_n(x_1) = 0 \\ \qquad\qquad\vdots \\ \xi_1\tau_1(x_r) + ... + \xi_n\tau_n(x_r) = 0 \end{cases}$$

Multiply the ith equation above by $c_i \in E$. Since $E = K^H$, $\tau_j(c_i) = c_i$. Then

$$\begin{cases} \xi_1\tau_1(c_1x_1) + ... + \xi_n\tau_n(c_1x_1) = 0 \\ \qquad\qquad\vdots \\ \xi_1\tau_1(c_rx_r) + ... + \xi_n\tau_n(c_rx_r) = 0 \end{cases}$$

hence $\xi_1\tau_1(y) + ... + \xi_n\tau_n(y) = 0$ for all $y \in K$. According to the Lemma 3.7 $\xi_i = 0$. A contradiction.

Step 2: $[K : E] \leq n$.

We prove all $n + 1$ elements of K are linearly dependent over E. Assume $v_1, ..., v_{n+1} \in K$ with $v_i \neq 0$ for all $i = 1, ..., n + 1$. Then we consider the $n \times (n + 1)$

matrix $(\tau_i(v_j))$ whose rank $\leq n < n+1$. Hence there are $c_i \in K$ not all trivial such that $c_1\tau_i(v_1) + ... + c_{n+1}\tau_i(v_{n+1}) = 0$ for all $1 \leq i \leq n$. We may just assume $c_1 \neq 0$.

$$\begin{cases} c_1\tau_1(v_1) + ... + c_{n+1}\tau_1(v_{n+1}) = 0 \\ \qquad\qquad \vdots \\ c_1\tau_n(v_1) + ... + c_{n+1}\tau_n(v_{n+1}) = 0 \end{cases}$$

Note since H is a group, $\{\tau_i\tau_1, ..., \tau_i\tau_n\}$ will still be H, which means if $a = \tau_1(x) + ... + \tau_n(x), x \in K$ then $a \in E$, because $\tau_i(a) = \sum_j \tau_i\tau_j(x) = \sum_j \tau_j(x) = a$. Moreover if $x \neq 0$, then there exists a $\lambda \in K^*$ such that $a = \tau_1(\lambda x) + ... + \tau_n(\lambda x) \neq 0$. Otherwise $\tau_1 + ... + \tau_n = 0$ on K, which is impossible according to the Lemma 3.7.

Since $\lambda c_1\tau_i(v_1) + ... + \lambda c_{n+1}\tau_i(v_{n+1}) = 0$ as well for all $1 \leq i \leq n$, after choosing λ such that $\tau_1(\lambda c_1) + ... + \tau_n(\lambda c_1) \neq 0$, we can just assume $a_1 = \tau_1(c_1) + ... + \tau_n(c_1) \neq 0$. Applying τ_j to the system above, we obtain

$$\begin{cases} \tau_j(c_1)\tau_j\tau_1(v_1) + ... + \tau_j(c_{n+1})\tau_j\tau_1(v_{n+1}) = 0 \\ \qquad\qquad \vdots \\ \tau_j(c_1)\tau_j\tau_n(v_1) + ... + \tau_j(c_{n+1})\tau_j\tau_n(v_{n+1}) = 0 \end{cases}$$

which is equivalent to the original one since $\{\tau_j\tau_1, ..., \tau_j\tau_n\} = H$. And we have

$$\tau_j(c_1)\tau_i(v_1) + ... + \tau_j(c_{n+1})\tau_i(v_{n+1}) = 0$$

for all $1 \leq i \leq n$. Then $a_i = \sum_j \tau_j(c_i) \in E$ are also the solution of such system, which means $a_1\tau_i(v_1) + ... + a_{n+1}\tau_i(v_{n+1}) = 0$. Hence $a_1v_1 + ... + a_{n+1}v_{n+1} = 0$ where $a_1 \neq 0$, which means $\{v_1, ..., v_{n+1}\}$ are dependent over E.

Step 3: K/E is Galois i.e. normal and separable.

Since $[K : E] = n$, K/E is finite. Let $u \in K$ and P is the minimal polynomial of u over E. Define $O := H$-orbit of u i.e. $\{\tau_i(u) | \tau_i \in H\}$ with $|O| \leq n$. Let $Q := \prod_{\alpha \in O}(X - \alpha)$. Since $\{\tau_j\tau_1, ..., \tau_j\tau_n\} = H$, $\{\tau_j\tau_1(u), ..., \tau_j\tau_n(u)\} = O = \tau_j(O)$. Then $\tau_j : O \to O$ is surjective. But since $|O|$ is finite, τ_j is injective as well. Hence it's a bijection. Then $Q = \prod_{\alpha \in O}(X - \tau_j(\alpha)) = \tau_j(Q)$, which means all coefficients Q are in E. H is actually a subgroup, $id_K \in H$. Therefore $u \in O$ and $Q(u) = 0$. $P|Q$. Since all roots of Q are different and in K, all roots of P are then different and in K. Thus K/E is normal and separable. □

Remark 3.8. Note if H in the lemma above is not a subgroup, then the step 2 will not be true. Assume F is a field and $F(t)$ is the field of rational functions over F. Consider the automorphism $f : F(t) \to F(t), g(t) \mapsto g(t+1)$. We suppose $g(t) = \frac{u(t)}{v(t)}$ where $u(t), v(t) \in F[t]$ and $(u(t), v(t)) = 1$. If $g(t) = g(t+1)$, then

$\frac{u(t)}{v(t)} = \frac{u(t+1)}{v(t+1)} \Rightarrow u(t)v(t+1) = u(t+1)v(t)$. Since $(u(t), v(t)) = 1$, $v(t)|v(t+1)$. But $deg(v(t)) = deg(v(t+1))$, then $v(t+1) = v(t)$. $v(t) = 0 \Leftrightarrow v(t+1) = 0$. Hence if $v(t)$ has a root α in $\bar{F}$, then $\alpha + 1$ is a root of $v(t)$ as well, which means $v(t)$ has infinitely many roots. It's impossible. Thus $v(t)$ has no roots and then $v(t) \in F$. The same argument implies $u(t) \in F$ and then $g(t) \in F$. Therefore the subfield fixed by f is just F. But $[F(t) : F] = \infty$.

Now we state the most important theorem in this section.

Theorem 3.9 (Galois Correspondence)**.** *If K/F is finite Galois, then there is a one-to-one correspondence*

$$\begin{aligned} \{\textit{subgroups } H \textit{ of } \mathrm{Gal}(K/F)\} &\longleftrightarrow \{\textit{subfields } E \textit{ of } K \textit{ containing } F\} \\ H &\longmapsto K^H \\ \mathrm{Gal}(K/E) &\longleftarrow\!\shortmid E \end{aligned} \tag{2}$$

Moreover E/F is Galois iff $\mathrm{Gal}(E/F)$ *is a normal subgroup of* $\mathrm{Gal}(K/F)$ *and we have the following one-to-one correspondence*

$$\{\textit{normal subgroups of } \mathrm{Gal}(K/F)\} \longleftrightarrow \{\textit{Galois subextensions}\}$$

where $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$*.*

For simplicity we prove the following lemma first.

Lemma 3.10. *If K/F is finite Galois, then $K^{\mathrm{Gal}(K/F)} = F$.*

Proof. Obviously $F \subseteq K^{\mathrm{Gal}(K/F)}$. Now we suppose $u \in K^{\mathrm{Gal}(K/F)}$, and P is its minimal polynomial over F. If v is a root of P in $\bar{F}$, according to the Lemma 2.7 there is a unique map $F(u) \to \bar{F}, u \mapsto v$. From the Proposition 2.14, this map can be extended to be $\tau : K \to \bar{F}, \tau(u) = v$. Since K/F is normal, $\tau(K) \subseteq K$. Then $\tau(u) = v \in K$. But $u \in K^{\mathrm{Gal}(K/F)}$ and $\tau \in \mathrm{Gal}(K/F)$, then $v = \tau(u) = u$. P is separable $\Rightarrow P = X - u$, then $u \in F$. □

Proof of Theorem 3.9. Step 1: $F \subseteq E \subseteq K$. K/E will be finite Galois. Then $K^{\mathrm{Gal}(K/E)} = E$.

Step 2: We prove $\mathrm{Gal}(K/K^H) = H$. It's obvious to see $H \subseteq \mathrm{Gal}(K/K^H)$. But according to the lemma of E. Artin and Remark 3.3, $|H| = [K : K^H] = |\mathrm{Gal}(K/K^H)|$, hence $H = \mathrm{Gal}(K/K^H)$.

Step 3: We prove E/F is Galois iff $\mathrm{Gal}(K/E)$ is normal. Let $\tau \in \mathrm{Gal}(K/F)$, $F \subseteq \tau(E) := \{\tau(x)|x \in E\}$ which is a subfield of K. Given any $\sigma \in \mathrm{Gal}(K/E)$, $\tau\sigma\tau^{-1} \in \mathrm{Gal}(K/\tau(E))$. And given any $\xi \in \mathrm{Gal}(K/\tau(E))$, $\tau^{-1}\xi\tau \in \mathrm{Gal}(K/E)$. Hence

$$\mathrm{Gal}(K/\tau(E)) = \tau \cdot \mathrm{Gal}(K/E) \cdot \tau^{-1}$$

If E/F is Galois, especially E/F is normal. $\tau|E : E \to \tau(E) \hookrightarrow \bar{F}$ is an F-embedding. Then $\tau(E) = E$, for all $\tau \in \mathrm{Gal}(K/F)$. On the other hand if $\tau(E) = E$ for all $\tau \in \mathrm{Gal}(K/F)$, since any F-morphism $\iota : E \to \bar{F}$ can be extended to be some $K \to \bar{F}$ and K/F is normal, $\iota : E \to \bar{F}$ can be extended to be an element $\tau \in \mathrm{Gal}(K/F)$. $\tau|E = \iota$ but according to the assumption $\tau(E) = E$ then $\iota(E) = E$. Hence E/F is normal.

Therefore E/F is Galois iff $\tau(E) = E$ for all $\tau \in \mathrm{Gal}(K/F)$ iff $\mathrm{Gal}(K/E) = \tau \cdot \mathrm{Gal}(K/E) \cdot \tau^{-1}$ for all $\tau \in \mathrm{Gal}(K/F)$ iff $\mathrm{Gal}(K/E)$ is a normal subgroup. The second "iff" comes from the Galois correspondence we have proved in Step 1 and Step 2. □

Corollary 3.11. *If K/F is a finite separable field extension, then there are only finitely many subfields E of K containing F.*

Proof. According to Remark 3.4, we could choose K' to be the Galois closure of K/E which is the normal closure of finite dimension. $F \subseteq K \subseteq K'$, we can only prove there are finitely many subfields between F and K'. From the Galois correspondence, the number of subfields is $|\mathrm{Gal}(K'/F)| = [K' : F] < \infty$. □

Theorem 3.12 (Primitive Element)**.** *If K/F is finite separable, then $K = F(u)$ for some $u \in K$.*

Proof. Step 1: Suppose F is a finite field. Then K is a finite field as well. According to Remark 2.37, $K = \mathbb{F}_q$ for some $q = p^m$. Corollary 2.39 tells us $\mathbb{F}_q^\times =< \xi >$ is cyclic. Hence $\mathbb{F}_q = \mathbb{F}_p(\xi) = F(\xi)$.

Step 2: Suppose F is an infinite field. Since K is finite over F, we can write $K = F(u_1, ..., u_n)$for $u_i \in K$. If $n = 1$ there is nothing to prove. By induction it suffices to prove the case $n = 2$, i.e. $K = F(u_1, u_2)$. For any $r \in F$, consider the subfield $F(u_1 + ru_2)$. Corollary 3.11 tells us that there are only finitely many intermediate subfields between F and K. and by assumption there are infinitely many elements in F, there must exist $r_1, r_2 \in F$ such that $F(u_1 + r_1u_2) = F(u_1 + r_2u_2) = F'$ with $r_1 \neq r_2$. Then $(r_1 - r_2)u_2 \in F'$, and consequently $u_1, u_2 \in F'$. □

In general, such primitive element is difficult to find.

Exercise 3.13. Let $K = \mathbb{F}_p(x, y)$ the field of rational functions in two variables. Let $F = K^p$. Prove that (1): K is not a simple extension of F; (2): There are infinitely many intermediate fields between K and F.

Proposition 3.14. (1)*. Assume E/F and K/F are finite Galois extensions. Then $E \cdot K/F$ is finite Galois and the morphism*

$$\varphi : \mathrm{Gal}(E \cdot K/K) \longrightarrow \mathrm{Gal}(E/E \cap K) \leq \mathrm{Gal}(E/F)$$

$$\tau \longmapsto \tau|E$$

is an isomorphism

$$\begin{tikzcd}
 & E \cdot K \arrow[dl, dash] \arrow[dr, dash, "\textit{finite Galois}"] & \\
E \arrow[dr, dash] \arrow[ddr, dash, "\textit{finite Galois}"'] & & K \arrow[dl, dash] \arrow[ddl, dash, "\textit{finite Galois}"] \\
 & E \cap K \arrow[d, dash] & \\
 & F &
\end{tikzcd} \tag{3}$$

(2). *The morphism*

$$\psi : \mathrm{Gal}(E \cdot K/F) \longrightarrow \mathrm{Gal}(E/F) \times \mathrm{Gal}(K/F)$$

$$\tau \longmapsto (\tau|E, \tau|K)$$

is injective. Moreover if $E \cap K = F$ then ψ is surjective hence an isomorphism.

Proof. (1). According to Corollary 2.19, we know $E \cdot K/F$ is normal. And according to the Proposition 2.27, $E \cdot K/F$ is separable. Hence $E \cdot K/F$ is Galois. Since $E \cdot K = F(E, K)$, E, K are finite over F, $E \cdot K/F$ is finite as well. Hence $E \cdot K/F$ is finite Galois.

Given any $\tau \in \mathrm{Gal}(E \cdot K/K)$, $\tau|E : E \to E \cdot K \hookrightarrow \bar{F}$. Since E/F is normal, $\tau(E) \subseteq E$. Hence $\tau|E \in \mathrm{Gal}(E/E \cap K)$ is well defined. If $\tau|E = id_E$, since $\tau|K = id_K$ it follows that $\tau = id_{E \cdot K}$. φ is injective.

On the other hand, $\mathrm{im}\varphi$ is a subgroup of $\mathrm{Gal}(E/E \cap K)$ and $E^{\mathrm{im}\varphi} = (E \cdot K)^{\mathrm{Gal}(E \cdot K/K)} \cap E = K \cap E$. Then $\mathrm{im}\varphi = \mathrm{Gal}(E/E \cap K)$.

(2). Obviously, ψ is well defined and if $\tau|E = id_E$, $\tau|K = id_K$, then $\tau = id_{E \cdot K}$. Hence φ is injective. If $E \cap K = F$, assume $(\sigma_1, \sigma_2) \in \mathrm{Gal}(E/F) \times \mathrm{Gal}(K/F)$. Since $F = E \cap K$, by (1). σ_1 and σ_2 can be extended to be $\sigma_1' \in \mathrm{Gal}(E \cdot K/K)$ and $\sigma_2' \in \mathrm{Gal}(E \cdot K/E)$ respectively. Let $\tau = \sigma_2' \circ \sigma_1' \in \mathrm{Gal}(E \cdot K/F)$. $\tau|K = \sigma_2' \circ \sigma_1'|K = \sigma_2' \circ id_K = \sigma_2'|K = \sigma_2$. $\tau|E = \sigma_2' \circ \sigma_1'|E = \sigma_2' \circ \sigma_1 = \sigma_1$. □

Definition 3.15. *A Galois extension is called **abelian** (resp. **cyclic**) if the Galois group is abelian (resp. cyclic).*

Remark 3.16. If K/F is finite abelian, since any subgroup of an abelian group is normal, for any intermediate field E between F and K, E/F is finite abelian.

Remark 3.17. If we assume $E_i; i \in I$ is a family of intermediate fields of $\bar{F}/F$ such that E_i/F is an abelian Galois extension. Then consider the morphism

$$\mathrm{Gal}(F(\cup_i E_i)/F) \to \prod_i \mathrm{Gal}(E_i/F), \tau \mapsto (\tau|E_i)_{i\in I}$$

which is injective since $F(\cup_i E_i)$ is the union of all $F(u_1, ..., u_n)$ where $u_j \in$ some E_i. Hence $\mathrm{Gal}(F(\cup_i E_i)/F)$ is abelian. Since $u_j \in$ some E_i, u_j is separable over F. Then $F(u_1, ..., u_n)/F$ is separable, $F(\cup_i E_i)/F$ is separable. And consider the F-embedding $F(\cup_i E_i) \hookrightarrow \bar{F}$, its restriction on E_i will be $E_i \to E_i$ which means $F(\cup_i E_i) \to F(\cup_i E_i)$. Hence $F(\cup_i E_i)/F$ is normal. $F(\cup_i E_i)/F$ is an abelian Galois extension.

Using Zorn's lemma, it's obvious to see there is a maximal abelian Galois extension F^{ab}/F, which is unique according to the statement above. Then if K/F is any abelian Galois extension, then $K \subseteq F^{ab}$. In general F^{ab}/F is an infinite field extension. And in the infinite Galois theory (Remark 3.94) we can prove $\mathrm{Gal}(F^{ab}/F) \cong \mathrm{Gal}(\bar{F}_s/F)^{ab}$ where $\bar{F}_s$ is the separable closure of F and the latter is the abelianlization of profinite groups.

Remark 3.18. The statement above also proves that K/F is a/an (abelian) Galois extension iff it's a union of finite (abelian) Galois extensions over F.

Remark 3.19. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is one of the most mysterious Galois groups in mathematics and note $\overline{\mathbb{Q}}/\mathbb{Q}$ is separable since it has characteristic zero. It's expected that every finite group occurs as a quotient of it. And Grothendieck's *Long March through Galois Theory* is trying to understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ via a concrete and geometric way. On the other hand, the *Kronecker-Weber theorem* states that any finite abelian extension of $\mathbb{Q}$ is contained in a *cyclotomic extension*. Extension fields of $\mathbb{Q}$ constructed by adjoining a root of unity are called *cyclotomic fields*. Then $\mathbb{Q}^{ab}$ is obtained by adjoining all roots of unity. If we assume $\mathbb{Q}^{(n)} = \mathbb{Q}(e^{2i\pi/n})$, then

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times \cong \widehat{\mathbb{Z}}^\times$$

where $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. It's the subject of class field theory.

There is a local viewpoint as well, which is the subject of local class field theory. The p-adic number field $\mathbb{Q}_p$ is defined to be the quotient field of $\mathbb{Z}_p$ which is the set of formal sums $\sum_{k=0}^{\infty} a_k p^k$. The *local Kronecker-Weber theorem* asserts that any abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension. A *local number field* F is a finite dimensional extension of $\mathbb{Q}_p$, whose ring of integers is denoted by $\mathcal{O}_F$. Then in local class field theory

$$\mathrm{Gal}(F^{ab}/F) \cong \widehat{F}^\times \cong \widehat{\mathbb{Z}} \times \mathcal{O}_F$$

We advise readers to consult the homepage of Milne for details. `https://www.jmilne.org/math/index.html`. These contents above are all contained in his notes *Algebraic Number Theory* and *Class Field Theory.*

Example 3.20. We study the Example 3.5 in details here. The Galois closure (normal closure) of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[3]{2}, \xi_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$.

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash, "\text{finite Galois of degree 3}"] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash] & & \mathbb{Q}(\xi_3) \arrow[dl, dash, "\text{finite Galois of degree 2}"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\xi_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$, $\xi_3^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$. $[\mathbb{Q}(\xi_3) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}i) : \mathbb{Q}] = 2$, which means $|\mathrm{Gal}(\mathbb{Q}(\xi_3)/\mathbb{Q})| = 2$ and then $\mathrm{Gal}(\mathbb{Q}(\xi_3)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. $|\mathrm{Gal}(K/\mathbb{Q}(\xi_3))| = 3$, then $\mathrm{Gal}(K/\mathbb{Q}(\xi_3)) \cong \mathbb{Z}/3\mathbb{Z}$. Assume $G = \mathrm{Gal}(K/\mathbb{Q})$ and then it's not abelian since $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois. We prove $G \cong S_3$.

Let $r \in \mathrm{Gal}(K/\mathbb{Q}(\xi_3))$ such that $r(\xi_3) = \xi_3$, $r(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3$.Then $r^2(\sqrt[3]{2}) = \sqrt[3]{2}\xi_3^2$, $r^3 = 1$. Suppose $a \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2}))$ such that $a(\sqrt[3]{2}) = \sqrt[3]{2}$, $a(\xi_3) = \xi_3^2$. $a^2(\xi_3) = \xi_3^4 = \xi$ then $a^2 = 1$. On the other hand

$$ara(\sqrt[3]{2}) = ar(\sqrt[3]{2}) = a(\sqrt[3]{2}\xi_3) = \sqrt[3]{2}\xi_3^2$$

$$ara(\xi_3) = ar(\xi_3^2) = a(\xi_3^2) = \xi_3^4 = \xi_3$$

then $ara = r^2$. $S_3 \cong G = \{1, a, r, r^2, ar, ar^2 | ara = r^2\}$. Then subgroups of G are

$$\{1, \langle r\rangle, \langle a\rangle, \langle ar\rangle, \langle ar^2\rangle, G\}$$

Only $< r >$ is nontrivial and normal. Using the Galois correspondence and the connection between field dimensions and the number of elements in groups, we conclude:

$$H \in \{1, \langle r\rangle, \langle a\rangle, \langle ar\rangle, \langle ar^2\rangle, G\}$$

$$K^H \in \{K, \mathbb{Q}(\xi_3), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}, \xi_3), \mathbb{Q}(\sqrt[3]{2}, \xi_3^2), \mathbb{Q}\}$$

Exercise 3.21. Let $K = \mathbb{Q}(\omega, i)$, where $\omega = \sqrt[4]{2}$ and $i^2 = -1$. Show that $K/\mathbb{Q}$ is Galois and determine $G = \mathrm{Gal}(K/\mathbb{Q})$. Write down all subgroups of G and for each subgroup H, the corresponding subfield K^H.

Exercise 3.22. Let ξ_5 be a primitive 5th root if unity and $K = \mathbb{Q}(\xi_5)$. Prove $K/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Determine K^H for each subgroup H of $\mathrm{Gal}(K/\mathbb{Q})$.

3.1 Galois Groups of Finite Fields

Recall contents of the Section 2.5 about finite fields. All finite field $\mathbb{F}$ is the splitting field of some $X^q - X$ over $\mathbb{F}_p$ where $q = p^n, p = \text{char}(\mathbb{F}) > 0$. Then

$$\mathbb{F}_q = \{\text{all roots of } X^q - X\}$$

If there is a field extension $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ and assume $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = r$, then $p^m = (p^n)^r = p^{nr}$, hence $n|m$. On the other hand if $m = n \cdot r$, since $\mathbb{F}_{p^n}^\times$ is cyclic and every root of $X^{p^n} - X$ is a roof of $X^{p^{nr}} - X$, then there exists a natural embedding $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \subseteq \overline{\mathbb{F}}_p$.

Theorem 3.23. *If q is a power of p, then $\mathbb{F}_{q^d}/\mathbb{F}_q$ is finite Galois with*

$$\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) \cong \mathbb{Z}/d\mathbb{Z}$$

cyclic, generated by the ***Frobenius morphism*** Frob : $x \mapsto x^q$ *for* $x \in \mathbb{F}_{q^d}$.

Proof. $\mathbb{F}_{q^d}/\mathbb{F}_p$ is the splitting filed of $X^{q^d} - X$ with all roots different. Hence it's finite Galois. Especially $\mathbb{F}_{q^d}/\mathbb{F}_q$ is finite Galois with $|\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)| = [\mathbb{F}_{q^d} : \mathbb{F}_q] = d$.

Next we prove Frob $\in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ has order d. Since $p|q$, $(x+y)^q = x^q + y^q$ and $(x-y)^q = x^q - y^q$. And any element of $\mathbb{F}_q$ is a root of $X^q - X$. Hence Frob is an automorphism with $\mathbb{F}_q$ fixed. If m is the order of Frob, then $\text{Frob}^m = id_{\mathbb{F}_{q^d}}, x \mapsto x^{q^m} = x$ for all $x \in \mathbb{F}_{q^d}$. There will be an embedding $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^m}$. Therefore $d|m, d \leq m$. Thenn $d = m$. □

Exercise 3.24. Write down an irrreducible polynomial of degree 2 in $\mathbb{F}_3[X]$, say $f(X)$. Write down the multiplication table for $\mathbb{F}_{3^2}^\times$, by identifying $\mathbb{F}_{3^2}$ with $\mathbb{F}_3[X]/(f)$.

3.2 Cyclotomic Extension

Let $\xi_n = e^{2i\pi/n}$ be the n-th root of unity 1. Then all $\xi_n^k, 0 \leq k \leq n-1$ are different. The **cyclotomic extension** is defined to be $\mathbb{Q}(\xi_n)/\mathbb{Q}$.

Fact 3.25.

(1) The set of roots of $X^n - 1$ is $\{\xi_n^k | 0 \leq k \leq n-1\}$ and $\mathbb{Q}(\xi_n)/\mathbb{Q}$ is finite Galois since it's a splitting field of a polynomial with all roots different.

(2) The primitive n-th root of unity 1 is defined to be a generator of the cyclic group $\{\xi_n^k | 0 \leq k \leq n-1\}$. Then ξ_n^k is primitive iff $(k, n) = 1$. Hence there are exactly $\phi(n)$'s primitive roots, where $\phi(n)$ is the Euler's function, $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$.

In the following, we want to compute $\text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ and the process will need Gauss Lemma.

Lemma 3.26 (Gauss)**.** *Let R be a unique factorization domain and $h \in R[X]$ a monic polynomial. If there is a factorization $h = f \cdot g$ such that monic polynomials f and g are in $Q(R)[X]$, then $f, g \in R[X]$.*

We assume the minimal polynomial of ξ_n over $\mathbb{Q}$ is $P(X) \in \mathbb{Q}[X]$. We define the cyclotomic polynomial of n to be $\Phi_n(X) = \prod_{\xi \text{ primitive}}(X - \xi)$. If $\tau \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$, then τ sends n-th primitive roots to n-th primitive roots. Hence $\tau(\Phi_n(X)) = \Phi_n(X)$, which means all coefficients of $\Phi_n(X)$ are in $\mathbb{Q}$. Then $\Phi_n(X) \in \mathbb{Q}[X]$ and $\Phi_n(X)|X^n - 1$ in $\mathbb{Q}[X]$, hence $\Phi_n(X)|X^n - 1$ in $\mathbb{Z}[X]$.

Example 3.27. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$.

Next we will prove $P(X) = \Phi_n(X)$.

Lemma 3.28. *Let $P(X)$ be the minimal polynomial of ξ_n over $\mathbb{Q}$. If p is a prime with $p \nmid n$ and u is a root $P(X)$, then u^p is a root of $P(X)$ as well.*

Proof. If $\mathbb{Q}[X]$, $X^n - 1$ has a factorization $X^n - 1 = P(X)Q(X)$, then $P(X), Q(X) \in \mathbb{Z}[X]$. We assume u^p is not a root pf $P(X)$. Then u^p is a root of $Q(X)$ and u is a root of $Q(X^p)$. But $P(X)$ is the minimal polynomial of u, $P(X)|Q(X^p)$ in $\mathbb{Z}[X]$. Consider this relation in $\mathbb{F}_p$. If we suppose in $\mathbb{Z}[X]$, $Q(X^p) = X^{pn} + a_{n-1}X^{p(n-1)} + ... + a_0$, since $\forall a \in \mathbb{F}_p, a^p = a$, then in $\mathbb{F}_p[X]$, $\overline{Q(X^p)} = \overline{Q(X)}^p$. Therefore $\overline{P(X)}|\overline{Q(X)}^p$ in $\mathbb{F}_p[X]$. If $\alpha \in \mathbb{F}_p$ is a root of $\overline{P(X)} \Rightarrow \alpha$ is a root of $\overline{Q(X)}$, which means α is a multiple root of $\overline{X^n - 1} \in \mathbb{F}_p[X]$. But $(\overline{X^n - 1})' = n\overline{X}^{n-1} \neq 0$ and then $\overline{X^n - 1}$ has no multiple roots. A contradiction! □

Theorem 3.29.

(1) $\Phi_n(X)$ *is irreducible hence* $\Phi_n(X) = P(X)$*.*

(2) $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$*, hence* $|\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})| = \phi(n)$*.*

Proof. (1). Since ξ_n is a root of Φ_n, $P|\Phi_n$. To prove $\Phi_n = P$, it's equivalent to prove every n-th primitive roots are roots of P as well. Assume $k = \prod_{p_i \text{ prime}} p_i^{r_i}$ with $r_i > 1$ and $(k, n) = 1$. Then $p_i \nmid n$. The lemma above implies $\xi_n^{p_i}$ is also a root of P. Using the lemma above by induction, we see ξ_n^k is a root of P.

(2). $|\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})| = deg\Phi_n = \phi(n)$. For $1 \leq k \leq n-1$ with $(k, n) = 1$, we define $\tau_k : \xi_n \mapsto \xi_n^k$. Since Φ_n is irreducible and separable with all roots different, we know

$$\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\xi_n), \mathbb{Q}(\xi_n)) = \{\tau_k | 1 \leq k \leq n-1, (k, n) = 1\}$$

hence $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. □

Fact 3.30. We recall some facts about the group $(\mathbb{Z}/n\mathbb{Z})^\times$. Assume $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ with $k_i > 0$, then

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^\times$$

For $(\mathbb{Z}/p^k\mathbb{Z})^\times$ with p prime there are two conditions:

1. If $p \geq 3$, $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z}$ is cyclic.
2. If $p = 2$, $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$, $(\mathbb{Z}/2^2\mathbb{Z})^\times = \{1,3\}$, $(\mathbb{Z}/2^3\mathbb{Z})^\times = \{1,3,5,7\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For $k \geq 3$, $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$.

3.3 Compass and Straightedge Construction

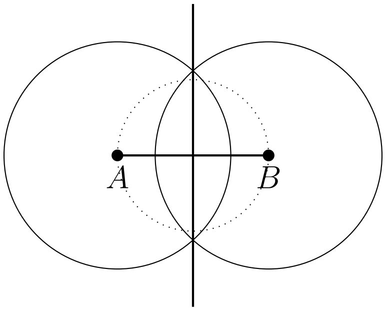
In the compass and straightedge construction, we can only use straightedge to construct the line passing through two given points and use compass to construct a circle with given center O and radius $r > 0$.

New points have only three source:

1. Intersection of two lines.
2. Intersection of a line and a circle.
3. Intersection of two circles.

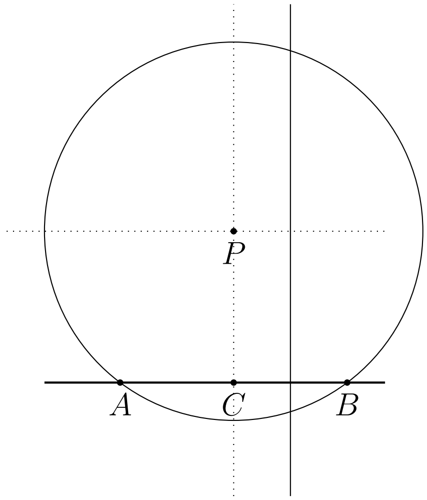
Remark 3.31 (Standard Construction)**.** In elementary plane geometry, there are two standard constructions.

(a) Given a segment AB, we can construct a circle with diameter AB.



(4)

(b) Given a line l and a point P not in l, we can construct a new line l' passing through P such that $l'//l$ or $l' \perp l$. At first draw a circle at the center P with radius big enough to intersect l with A and B. Then the process (a) will give the middle point C of AB. $PC \perp l$. Draw any other line $l'' \perp l$. We construct $l''' \perp l''$ passing through P, then $l'''//l$.



(5)

Definition 3.32. *$(a, b) \in \mathbb{R}^2$ is called* ***constructible*** *if we can construct it from the points $O = (0, , 0)$ and $(1, 0)$, using compass and straightedge. And a real number $a \in \mathbb{R}$ is constructible if $(a, 0) \in \mathbb{R}^2$ is constructible.*

It's obvious to see a point $(a, b) \in \mathbb{R}^2$ is constructible iff a and b are constructible as real numbers. If the subset of constructible numbers of $\mathbb{R}$ is denoted by $\mathcal{C}$, the subset of constructible points in $\mathbb{R}^2$ will $\mathcal{C} \times \mathcal{C}$.

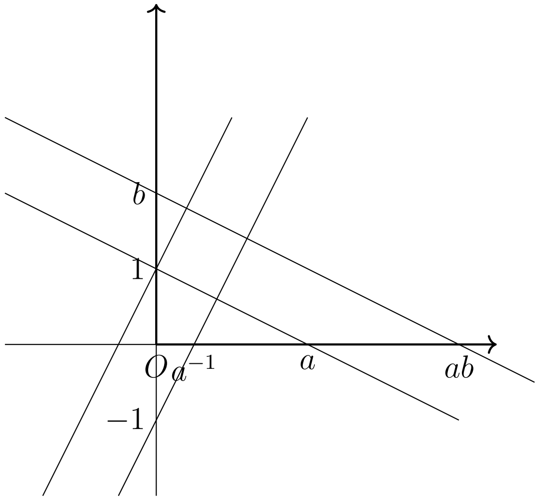
Proposition 3.33.

(1) $\mathcal{C}$ is a subfield of $\mathbb{R}$ containing $\mathbb{Q}$.

(2) If $c \in \mathcal{C}$, then $\sqrt{c} \in \mathcal{C}$.

Proof. (1). Since any field with characteristic 0 contains $\mathbb{Q}$ as a subfield, it is enough to prove $\mathcal{C}$ is a field. If $c \in \mathcal{C}$, drawing a circle at the center $O = (0, 0)$ with radius

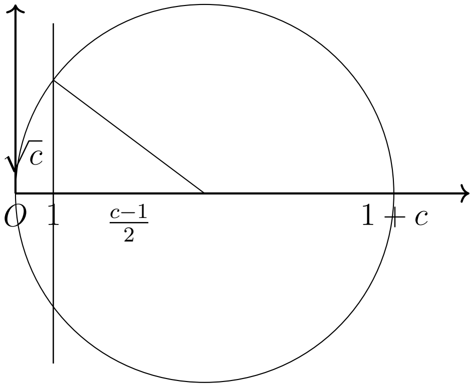
$r = c$, we see $-c \in \mathcal{C}$. If $a, b \in \mathcal{C}$, we construct ab and a^{-1} in the following picture:



(6)

hence $\mathcal{C}$ is a field.

(2). If $c \in \mathcal{C}$, $\sqrt{c}$ is constructed as follows:



(7)

□

In the following we study the connection between constructible numbers in $\mathbb{R}$ and field extensions over $\mathbb{Q}$. Finally we will use these theorems to solve four difficult problems in ancient Greece.

Let $K \subseteq \mathbb{R}$ be subfield. The plain of K means $K \times K \subseteq \mathbb{R} \times \mathbb{R}$.

- A line in K is a line in $\mathbb{R}^2$ joining two points in the plain of K.
- A circle in K is a circle in $\mathbb{R}^2$, whose center lies in $K \times K$ and radius is in K.

Lemma 3.34.

(1) The intersection of two lines in K is empty or a point in $K \times K$.

(2) The intersection of a line and a circle in K is empty, one point or two points in the plain of $K(\sqrt{u})$, where $u \in \mathbb{R}$.

(3) The intersection of two circles in K is empty, one point or two points in the plain of $K(\sqrt{u})$, where $u \in \mathbb{R}$.

Proof. (1). Given two point $(a, b), (c, d) \in K \times K$, the line passing through them are $(b - d)(x - a) - (a - c)(y - b) = 0$. All coefficients of this line equation are in K. Hence the intersection of two lines in K is empty or a point in $K \times K$.

(2) and (3). The equation of a circle in K is $(x - a)^2 + (y - b)^2 = r^2$, where $x, b, r \in K$. Hence the intersection of a line and a circle or two circles in K is to solve an equation of degree 2. □

Theorem 3.35. *A real number $c \in \mathcal{C}$ iff there is a tower of fields $\mathbb{Q} = K_0 \subseteq K_1 \subseteq ... \subseteq K_n \subseteq \mathbb{R}$ satisfying the following two conditions*

(i) $c \in K_n$.

(ii) $[K_{i+1} : K_i] = 2$, which means $K_{i+1} = K_i(\sqrt{u_{i+1}})$ with $u_{i+1} > 0$.

In particular if c is constructible, then c is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(c) : \mathbb{Q}]$ is a power of 2.

Proof. First we prove the part of ⇒. Assume $c \in \mathcal{C}$ and $(c, 0)$ is constructible in $\mathbb{R}^2$. Then $(c, 0)$ can be constructed in finitely many steps drawing a line or a circle. In every step, new points are produced as the intersection of two lines, a line and a circle or two circles, which means they will lie in the original plain of K_i or in the plain of $K_i(\sqrt{u})$ according to the lemma above. This proves the part of ⇒.

⇐: Conversely if we assume such tower of fields exist, then the minimal polynomial of c over K_{n-1} will be $X^2 + aX + b \in K_{n-1}[X]$. Then $(c, 0)$ will be the intersection point of the circle $(X + \frac{a}{2})^2 + Y^2 = \frac{a^2}{4} - b$ and the x-axis. According to the Proposition 3.33, if u, v are constructed, uv, $u + v$ or $u - v$ will be constructed then. Since a, b is a linear combination of 1 and $\sqrt{u_{n-1}}$ over K_{n-2}, the problem is reduced to construct $\sqrt{u_{n-1}}$ over K_{n-2}. But $(\sqrt{u_{n-1}}, 0)$ is the intersection of the circle $X^2 + Y^2 = u_{n-1}$ and the x-axis, where $u_{n-1} \in K_{n-2}$. The problem will then be reduced to construct $\sqrt{u_{n-2}}$. After finitely many steps we see c is constructible.

Consider $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq K_n$, then $[\mathbb{Q}(c) : \mathbb{Q}] | [K_n : \mathbb{Q}] = 2^n$ and $[\mathbb{Q}(c) : \mathbb{Q}] = 2^k$. □

Remark 3.36. The converse of the last statement of the theorem above is also true. If $K \subseteq \mathbb{R}$ is a subfield with $[K : \mathbb{Q}] = 2^n$ then $K \subseteq \mathcal{C}$.

Proof. First we replace K by its Galois closure K' over $\mathbb{Q}$. Given any $u \in K$, the degree of the minimal polynomial P of u over $\mathbb{Q}$ is a power of 2. If P has a root v not in K, then the minimal polynomial Q of v over K divides P hence whose degree is a power of 2 as well. Then we will have $[K(v) : \mathbb{Q}] = 2^{n'}$. Since the Galois closure K' of $K/\mathbb{Q}$ is just the normal closure of it, after finitely many steps of simple algebraic extension, we conclude $[K' : \mathbb{Q}]$ is a power of 2 as well.

Now we prove any group G of order 2^n, has a subgroup of index 2. Assume the order of $a \in G$ is maximal among all elements of G. If the order of a is 2^r, $r \geq 1$, we define the subgroup $H := \{x \in G | \mathrm{ord}(x) \leq 2^{r-1}\}$. It's obvious to see H is actually a proper subgroup of G. For any $g \in G, h \in H$, $(ghg^{-1})^d = g^d h^d g^{-d}$. Then $\mathrm{ord}(ghg^{-1}) \leq 2^{r-1}$, $ghg^{-1} \in H$. Thus H is normal in G, $H \trianglelefteq G$. Then consider groups H and G/H whose orders are strictly smaller than 2^n. The same process above will imply a sequence $H' \trianglelefteq H \trianglelefteq H'' \trianglelefteq G$ .And we can refine it to obtain the following series:

$$1 = H_0 \trianglelefteq H_2 \trianglelefteq ... \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

such that H_{i+1}/H_i is cyclic with order 2. Especially there is a normal subgroup H of G such that $|G/H| = 2$.

Since $|\mathrm{Gal}(K'/\mathbb{Q})| = 2^m$, there is a normal subgroup $H \subseteq \mathrm{Gal}(K'/\mathbb{Q})$ with $|\mathrm{Gal}(K'/\mathbb{Q})/H| = 2$. Then consider $\mathbb{Q} \subseteq K'^H \subseteq K'$, where $[K' : K'^H] = 2$ and $[K'^H : \mathbb{Q}]$ is a power of 2 as well. Moreover since H is normal, $K'^H/\mathbb{Q}$ is finite Galois, continuing this process we will finally obtain a sequence of fields $\mathbb{Q} = K'_0 \subseteq K'_1 \subseteq ... \subseteq K'_n = K'$, with $[K'_{i+1} : K'_i] = 2$. The Theorem 3.35 implies $K \subseteq K' \subseteq \mathcal{C}$. □

Now let us apply the Theorem 3.35 and Remark 3.36 to four problems in ancient Greece about compass and straightedge construction.

(1). The first one is about **squaring a circle**. We want to construct a square whose area is equal to the area of a given circle. This problem is equivalent to say whether $\sqrt{\pi}$ is constructible or not. The answer is negative since π is not algebraic over $\mathbb{Q}$, and thus $\sqrt{\pi}$ is not algebraic over $\mathbb{Q}$ as well.

(2). The second one is about **doubling the cube**. Given a cube, we want to construct a new cube with twice the volume. This problem is equivalent to say whether $\sqrt[3]{2}$ is constructible or not. Obviously $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^n$. Hence the answer is negative.

(3). The third problem is about **trisecting an arbitrary angle**, which means given an angle θ, we want to construct $\theta/3$. An angle θ is called constructible if there are two lines whose intersection angle is θ. This definition is equivalent to that $(\cos\theta, \sin\theta)$ is constructible. Since $\sin\theta$ is a solution of the equation $X^2 + \cos^2\theta - 1 = 0$, the definition is also equivalent to that $\cos\theta$ is constructible.

Since $\cos\theta = 4\cos^3\frac{\theta}{3} - 3\mathrm{cos}\frac{\theta}{3}$, we should consider the polynomial $4X^3 - 3X - a$. $\theta/3$ is constructible iff the polynomial $4X^3 - 3X - \cos\theta$ is not irreducible in $\mathbb{Q}(\cos\theta)$.

We give two examples here.

If $a = \cos 60^\circ = \frac{1}{2}$, then $8X^3 - 6X - 1$ is irreducible. If it's reducible, then it has a root $\frac{p}{q}$ in $\mathbb{Q}$ with $(p, q) = 1$. Hence $8p^3 - 6pq^2 = q^3$, then $p|q, q|p$. $\Rightarrow \frac{p}{q} = 1$ or -1. But $8 - 6 - 1 \neq 0, -8 + 6 - 1 \neq 0$. Thus 20° is not constructible.

The argument above is standard to prove $aX^3 + bX^2 + c$ is irreducible in $\mathbb{Q}[X]$ where $a, b, c \in \mathbb{Z}$. It's reducible iff it has a root $\frac{p}{q} \in \mathbb{Q}$ with $(p, q) = 1$, then $q|a, p|c$.

If $a = \cos 45^\circ = \frac{\sqrt{2}}{2}$, then $4X^3 - 3X - \frac{\sqrt{2}}{2}$ is not irreducible since $-\frac{\sqrt{2}}{2}$ is a root of it in $\mathbb{Q}(\sqrt{2})$, which means 45° can be trisected.

Exercise 3.37. Prove $\theta = 54^\circ$ is constructible.

(4). The final problem (**regular n-gon**) is about constructing a regular polygon with n-sides, which is equivalent to construct $\theta_n = \frac{2\pi}{n}$ or $\cos\theta_n$.

Lemma 3.38. *A regular n-gon is constructible iff θ_n is constructible iff $\cos\theta_n \in \mathcal{C}$ iff $[\mathbb{Q}(\xi_n) : \mathbb{Q}]$ is a power of 2.*

Proof. $\xi_n = \cos\theta_n + i\sin\theta_n$, $\xi_n^{-1} = \cos\theta_n - i\sin\theta_n \Rightarrow \xi_n + \xi_n^{-1} = 2\cos\theta_n \in \mathbb{Q}(\xi_n)$. And moreover ξ_n is a root of $X^2 - 2\cos\theta_n X - 1$.

$$\begin{tikzcd}
\mathbb{Q}(\xi_n) \arrow[d, dash, "\text{degree=1 or 2}"] \\
\mathbb{Q}(\cos\theta_n) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

then $[\mathbb{Q}(\cos\theta_n) : \mathbb{Q}]$ is a power of 2 iff $[\mathbb{Q}(\xi_n) : \mathbb{Q}]$ is a power of 2. According to the Remark 3.36 and Theorem 3.35 we see this lemma is true. □

A **Fermat number** has the form $\mathrm{F}_m = 1 + 2^{2^m}$. If it's a prime as well, then it's called a **Fermat prime**.

Example 3.39. $\mathrm{F}_0 = 3$, $\mathrm{F}_1 = 5$, $\mathrm{F}_2 = 17$, $\mathrm{F}_3 = 257$, $\mathrm{F}_4 = 65537$ are all Fermat primes. But $\mathrm{F}_5 = 641 \times 6700417$ and $\mathrm{F}_6 = 274177 \times 67280421310721$ are not primes. In fact until now we have not discovered any new Fermat primes different from $\mathrm{F}_i, 0 \leq i \leq 4$. Therefore there is a conjecture that $\mathrm{F}_i, 0 \leq i \leq 4$ are the only Fermat primes.

Now the following theorem solves the problem of regular n-gon.

Theorem 3.40. *A regular n-gon is constructible iff n has a prime decomposition*

$$n = 2^k p_1 ... p_s$$

such that $k, s \geq 0$, p_i's are Fermat primes.

Proof. The Lemma 3.38 tells us θ_n is constructible iff $[\mathbb{Q}(\xi_n) : \mathbb{Q}]$ is a power of 2. Assume $n = 2^k p_1^{r_1} ... p_s^{r_s}$, where $p_i \geq 3$, then

$$\phi(n) = \phi(2^k)\phi(p_1^{r_1})...\phi(p_s^{r_s}) = 2^{k-1}(p_1 - 1)p_1^{r_1 - 1}...(p_s - 1)p^{r_s - 1}$$

See the Fact 3.25 (2) for the definition of ϕ. According to the Theorem 3.29, $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ then $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})| = \phi(n)$. It's a power of 2 iff $r_i = 1$ and $p_i - 1$ is a power of 2. From the following Lemma 3.41, we know p_i will be a Fermat prime. □

Lemma 3.41. *A prime number $p \geq 3$ is a Fermat prime iff $p - 1$ is a power of 2.*

Proof. Since $\mathrm{F}_m = 1 + 2^{2^m}$, the part of ⇒ is clear. We then assume $p - 1$ is a power of 2. Suppose $p - 1 = 2^n = 2^{2^k m}$ where $2 \nmid m$, then $p = (2^{2^k})^m + 1$. Since for any odd number $r > 1$, $a^r + 1$ has the following decomposition

$$a^r + 1 = 1 - (-a)^r = [1 - (-a)][1 + (-a) + ... + (-a)^{r-1}]$$

Hence if $m > 1$, then p will not be a prime. Therefore $m = 1$ and $p = 2^{2^k} + 1 = \mathrm{F}_k$. □

3.4 Solvability of Algebraic Equations

In this section we assume all fields have characteristic 0. From the Lemma 2.22 we know all algebraic field extensions of characteristic 0 is separable. Hence here the property of being Galois is equivalent to be normal.

Definition 3.42. *A finite field extension K/F is called* ***radical*** *if there exist $u_1, .., u_n \in K, m_1, ..., m_n \in \mathbb{N}^+$ such that*

(1) $K = F(u_1, ..., u_n)$.

(2) $u_1^{m_1} \in F$, $u_i^{m_i} \in F(u_1, ..., u_{i-1})$ for all $2 \leq i \leq n$.
This is equivalent to say there is a sequence of fields

$$F \subseteq F(u_1) \subseteq F(u_1, u_2) \subseteq ... \subseteq F(u_1, ..., u_n) = K$$

such that $F(u_1, ..., u_{i-1}) \subseteq F(u_1, ..., u_i)$ is a ***simple radical extension*** *with $u_i^{m_i} \in F(u_1, ..., u_{i-1})$.*

Note a radical extension doesn't need to be Galois and the polynomial of $X^{m_i}-a \in F(u_1,...,u_{i-1})[X]$ is not necessarily to be irreducible.

Remark 3.43.

(1) $\mathbb{Q} \subseteq F$. Let ξ_n be a primitive n-th root of unity 1. Then the simple algebraic extension $F(\xi_n)/F$ is radical.

(2) Let u be a root of $X^m-a \in F[X]$. Then $F(u)/F$ is radical. But it's not necessarily to be normal. For example $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is not normal. But from the Remark 3.4 we see the normal closure N of $F(u)/F$ is generated by all roots of the minimal polynomial P of u over F which divides $X^m - a$ hence contained in $F(u, \xi_m)$ which is the splitting field of $X^m - a$ over F. Since all roots of P have the form $u\xi_m^k$ and $(u\xi_m^k)^m = a \in F$, we see the normal closure N/F is radical.

(3) More generally, if K/F is radical but not normal, let K' be the normal closure hence Galois closure of it, then K'/F will be radical.

Proof. Assume $K = F(u_1, ..., u_n)$ with $u_i^{m_i} \in F(u_1, ..., u_{i-1})$ and P_i is the minimal polynomial of u_i over F where $1 \leq i \leq n$. Then K' is generated by all roots of P_i over F. Define $G := \mathrm{Gal}(K'/F)$, $|G| = [K' : F] < \infty$. If $\tau \in G$, then $\tau(K) = F(\tau(u_1), ..., \tau(u_n))$ is radical over F as well since $\tau(u_i)^{m_i} = \tau(u_i^{m_i}) \in \tau(F(u_1, ..., u_{i-1})) = F(\tau(u_1), ..., \tau(u_{i-1}))$. If v_i is a root of P_i, then there will be an F-morphism $F(u_i) \to \bar{F}, u_i \mapsto v_i$ by the Lemma 2.7, which can be extended to be $K' \to \bar{F}$ according to the Proposition 2.14. But since K' is normal, $K' \to \bar{F}$ is actually $K' \to K'$ by the Theorem 2.18. In a summary we have

$$K' = K(\{\tau(u_i)|\tau \in G, 1 \leq i \leq n\}) = \prod_{\tau \in G} K(\tau(u_1), ..., \tau(u_n))$$

The following Fact 3.44 (3) implies K'/F is radical. □

Fact 3.44.

(1) There are field extensions $F \subseteq E \subseteq K$. If K/F is radical, then K/E is radical but E/F may not be radical.

(2) Still consider $F \subseteq E \subseteq K$. If E/F and K/E are radical, then K/F is radical.

(3) If E/F and E'/F are radical, then $E \cdot E'/F$ is radical.

These are similar to the property of being normal. See the Corollary 2.19.

Proof. (1). It's obvious since $F(u_1, .., u_n) = E(u_1, ..., u_n) = K$.

(2). $E = F(u_1, ..., u_n), K = E(u_{n+1}, ..., u_m) \Rightarrow K = F(u_1, ..., u_n, u_{n+1}, ..., u_m)$.

(3).

$$\begin{tikzcd}
& E \cdot E' \arrow[ld, dash] \arrow[rd, dash, "\text{radical}"] & \\
E \arrow[rd, dash, "\text{radical}"'] & & E' \arrow[ld, dash, "\text{radical}"] \\
& F &
\end{tikzcd}$$

$F \subseteq F(u_1) \subseteq ... \subseteq F(u_1, ..., u_n) = E$, $u_i \in E \Rightarrow u_i \in E \cdot E'$, $E' \subseteq E'(u_1) \subseteq ... \subseteq E'(u_1, ..., u_n) = E \cdot E'$ and $u_i^{m_i} \in F(u_1, ..., u_{i-1}) \subseteq E'(u_1, ..., u_{i-1})$. We see $E \cdot E'/E'$ is radical. The part of (2) implies $E \cdot E'/F$ is radical. □

Definition 3.45. *A group G is **solvable** if G has a series of subgroups*

$$\{e\} = G_0 \leq G_1 \leq ... \leq G_n = G$$

such that $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is abelian.

Example 3.46. Permutation groups S_3 and S_4 are solvable but A_5 is a non-commutative simple group hence not solvable. Note a group is called **simple** if it has no proper normal subgroups except $\{e\}$.

There are some basic facts about solvable groups in the following which we'll not prove.

Fact 3.47.

(1) If G is solvable, then for any subgroup $H \leq G$, H is solvable as well. If moreover H is normal, then G/H is also solvable.

(2) Conversely if $H \trianglelefteq G$ such that H and G/H are normal, then G is normal as well.

(3) If G has a composition series, in particular G is finite, then G is solvable iff the composition factors of G are cyclic of prime order. Especially if G is finite solvable, then G will have a normal subgroup of prime index.

The proof of second part of (3) is clear since that means there will be a maximal normal subgroup $H \trianglelefteq G$ with G/H abelian. Then G/H is a simple abelian group. Hence G/H must be a cyclic group of prime order.

Now we can state the connection between radical extensions and solvable groups.

Proposition 3.48. *If K/F is a finite Galois radical extension, then* $\mathrm{Gal}(K/F)$ *is solvable.*

Proof. $K = F(u_1, ..., u_n)$ with $u_i^{m_i} \in F(u_1, ..., u_{i-1})$. We prove this proposition by induction on n. If $n = 1$, $K = F(u_1), u_1^{m_1} \in F$. We see $K \subseteq F(u_1, \xi_{m_1})$ and it's enough to prove $\mathrm{Gal}(F(u_1, \xi_{m_1})/F)$ is solvable by the Fact 3.47 (1). Now we consider the following diagram:

$$\begin{tikzcd}
F(u_1, \xi_{m_1}) \arrow[d, dash] \\
F(\xi_{m_1}) \arrow[d, dash] \\
F
\end{tikzcd}$$

Since all roots of unity 1 are different, $F(\xi_{m_1})/F$ is normal hence Galois. From Galois Correspondence, we see $\mathrm{Gal}(F(\xi_{m_1})/F) \trianglelefteq \mathrm{Gal}(F(u_1, \xi_{m_1})/F)$ is normal. The Fact 3.47 (2) implies to prove $\mathrm{Gal}(F(u_1, \xi_{m_1})/F)$ is solvable, it's enough to prove $\mathrm{Gal}(F(\xi_{m_1})/F)$ and $\mathrm{Gal}(F(u_1, \xi_{m_1})/F(\xi_{m_1})) \cong \mathrm{Gal}(F(u_1, \xi_{m_1})/F)/\mathrm{Gal}(F(\xi_{m_1})/F)$ are solvable.

$$\begin{tikzcd}
& F(\xi_{m_1}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\xi_{m_1}) \arrow[dr, dash] & & F \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

There will be an injection $\mathrm{Gal}(F(\xi_{m_1})/F) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\xi_{m_1})/\mathbb{Q}) \cong (\mathbb{Z}/m_1\mathbb{Z})^\times$ by $\tau \mapsto \tau|\mathbb{Q}(\xi_{m_1})$. Then $\mathrm{Gal}(F(\xi_{m_1})/F)$ is abelian hence solvable. On the other hand consider an element $\tau \in \mathrm{Gal}(F(u_1, \xi_{m_1})/F(\xi_{m_1}))$. τ is determined by its value on u_1. All roots of $X^{m_1} - u_1^{m_1}$ are $u_1\xi_{m_1}^k$ with $0 \le k \le m_1 - 1$. Hence $\tau(u_1) = u_1\xi_{m_1}^k$ for some $0 \le k \le m_1 - 1$. And since $\tau(\xi_{m_1}) = \xi_{m_1}$, we see $\mathrm{Gal}(F(u_1, \xi_{m_1})/F(\xi_{m_1}))$ is an abelian group thus solvable. This proves $\mathrm{Gal}(F(u_1, \xi_{m_1})/F)$ is solvable. Therefore $\mathrm{Gal}(K/F)$ is solvable.

$$\begin{tikzcd}
K = F(u_1)(u_2, ..., u_n) \arrow[r, dash] \arrow[d, dash] & K(\xi_{m_1}) \arrow[d, dash, "\text{solvable}"] \\
F(u_1) \arrow[r, dash] \arrow[d, dash] & F(u_1, \xi_{m_1}) \\
F \arrow[ur, dash, "\text{solvable}"] &
\end{tikzcd}$$

That $\mathrm{Gal}(F(u_1, \xi_{m_1})/F)$ is solvable is proved above. Since K/F is finite Galois, then $K(\xi_{m_1})/F = K \cdot F(\xi_{m_1})/F$ is finite Galois as well according to the Corollary 2.19. Therefore $K(\xi_{m_1})/F(u_1, \xi_{m_1})$ is finite Galois and radical. By the assumption on $n-1$ we see $\mathrm{Gal}(K(\xi_{m_1})/F(u_1, \xi_{m_1}))$ is solvable. And because $F(u_1, \xi_{m_1})/F$ is Galois, then $\mathrm{Gal}(F(u_1, \xi_{m_1})/F) \trianglelefteq \mathrm{Gal}(K(\xi_{m_1})/F(u_1, \xi_{m_1}))$ is normal $\Rightarrow$ $\mathrm{Gal}(K(\xi_{m_1})/F)$ is solvable according to the Fact 3.47 (2). $\mathrm{Gal}(K/F)$ is a subgroup of $\mathrm{Gal}(K(\xi_{m_1})/F)$ hence solvable as well. □

The concept of solvable groups actually comes from the solvability of algebraic equations.

Definition 3.49. *Assume $f(X) \in F[X]$ and* Split(f) *is the splitting field of $f(X)$ over F. We say $f(X)$ is* ***solvable by radicals*** *if $f(X)$ splits in some radical extension K/F i.e.* $\mathrm{Split}(f) \subseteq K$.

Remark 3.50. Let $K = F(u_1, ..., u_n)$ with $u_i^{m_i} \in F(u_1, ..., u_{i-1})$ and all roots of $f(X)$ are in K. Then every root of $f(X)$ can be expressed as an iteration of the form $F + \sqrt[m]{-}$ such as $d + \sqrt[m_3]{c + \sqrt[m_2]{b + \sqrt[m_1]{a}}}$ where $a, b, c, d \in F$.

In the following the Galois group $\mathrm{Gal}(\mathrm{Split}(f)/F)$ is denoted by Gal_f where $f(X) \in F[X]$. Then the next theorem reveals the relation between the solvability by radicals of polynomials and the solvability of groups.

Theorem 3.51. *Let $f(X) \in F[X]$. Then $f(X)$ is solvable by radicals iff* Gal_f *is solvable.*

Proof of "⇒". The proof of the part ⇒ is clear. Actually there is a series of fields $F \subseteq \mathrm{Split}(f) \subseteq K \subseteq K'$, where K/F is radical and K' is the Galois closure of K. Then $\mathrm{Gal}_f \cong \mathrm{Gal}(K'/F)/\mathrm{Gal}(K'/\mathrm{Split}(f))$. The Remark 3.43 (3) implies K'/F is radical. Then the Proposition 3.48 tells us $\mathrm{Gal}(K'/F)$ is solvable. Since $\mathrm{Split}(f)/F$ is Galois, $\mathrm{Gal}(K'/\mathrm{Split}(f)) \trianglelefteq \mathrm{Gal}(K'/F)$ is normal. Then from the Fact 3.47 (1), Gal_f is solvable. □

To prove the part of ⇐ we need a lemma.

Lemma 3.52. *Let K/F be a Galois extension with $[K : F] = p$ prime. Assume F contains ξ_p the primitive p-th root of unity* 1*. Then K/F is a simple radical extension i.e. $\exists u \in K$ such that $u^p \in F$ and $F(u) = K$.*

Proof. In the following we construct such $u \in K$ satisfying $\tau(u) = \xi_p^{-1}u$, where $\mathrm{Gal}(K/F) = \langle\tau\rangle$ is a cyclic group of order p. Then $\tau(u) \neq u \Rightarrow u \notin F$ and $\tau(u^p) = (\xi_p^{-1}u)^p = u^p \Rightarrow u^p \in F$. Since $[K : F]$ is prime and $[K : F(u)] \cdot [F(u) : F] = [K : F]$, we will have $K = F(u)$.

Let $v \in K$ fixed, $u = \sum_{i=0}^{p-1} \xi_p^i \tau^i(v)$. Then

$$\begin{aligned}
\tau(u) &= \sum_{i=0}^{p-1} \tau(\xi_p^i)\tau^{i+1}(v) = \sum_{i=0}^{p-1} \xi_p^i \tau^{i+1}(v) \\
&= \xi_p^{-1} \sum_{i=0}^{p-1} \xi_p^{i+1}\tau^{i+1}(v) = \xi_p^{-1} \sum_{i=1}^{p} \xi_p^i \tau^i(v) \\
&= \xi_p^{-1} \sum_{i=1}^{p-1} \xi_p^i \tau^i(v) + \xi_p^{-1}\xi_p^p \tau^p(v) \\
&= \xi_p^{-1} \sum_{i=1}^{p-1} \xi_p^i \tau^i(v) + v \\
&= \xi_p^{-1} u \qquad (8)
\end{aligned}$$

□

Theorem 3.53. *Let K/F be a finite Galois extension such that* $\mathrm{Gal}(K/F)$ *is solvable. Then K is contained in a radical extension of F.*

Proof. We prove by induction on $[K : F] = n$. If $n = 2$, since any equation $X^2 + aX + b = 0$ has roots $\frac{-a+\sqrt{a^2-4b}}{2}$ and $\frac{-a-\sqrt{a^2-4b}}{2}$, then K/F is itself radical. We assume this theorem is true for $[K : F] \leq n - 1$, where $n \geq 2$. Then consider the following diagram:

$$\begin{tikzcd}
K \arrow[r, no head] \arrow[d, no head, "\text{degree}=n"'] & K(\xi_p) \arrow[r, no head] \arrow[d, no head, "\text{degree}\leq n"] & L \\
F \arrow[r, no head, "\text{radical}"'] & F(\xi_p) \arrow[ur, no head, bend right, "\text{radical}"']
\end{tikzcd}$$

Since $\mathrm{Gal}(K/F)$ is finite Galois, according to the Fact 3.47 (3), it has a normal subgroup H of index prime p. We fix such prime p and add the primitive p-th root to K. Then since $F \subseteq K$, $[K(\xi_p) : K] \leq [F(\xi_p) : F]$. But $[K(\xi_p) : K] \cdot [K : F] = [K(\xi_p) : F(\xi_p)] \cdot [F(\xi_p) : F] = [K(\xi_p) : F]$, we conclude $[K(\xi_p) : F(\xi_p)] \leq n$.

Case 1. If $[K(\xi_p) : F(\xi_p)] < n$, then by assumption $K(\xi_p)$ is contained in a field L such that $L/F(\xi_p)$ is radical. From the Fact 3.44, L/F is radical.

Case 2. $[K(\xi_p) : F(\xi_p)] = n$. We assume $E = K(\xi_p)^H$ where $H \trianglelefteq \mathrm{Gal}(K/F)$ with

$|\mathrm{Gal}(K/F)/H| = p$.

$$\begin{tikzcd}
K(\xi_p) \arrow[r, dash] \arrow[d, dash, "\text{degree}<n"'] & L \\
E \arrow[ur, dash, "\text{radical}"'] \arrow[d, dash, "\text{degree}=p"'] & \\
F(\xi_p) &
\end{tikzcd}$$

Since H is normal, $E/F(\xi_p)$ is finite Galois with degree p. The Lemma 3.52 implies $E/F(\xi_p)$ is a simple radical extension. $[K(\xi_p) : E] < n$, by assumption $K(\xi_p)/E$ will be contained in a radical extension L/E. Then $L/F(\xi_p)$ is radical. Hence L/F is radical. □

This theorem proves the part of $\Leftarrow$ of the Theorem 3.51. Since $\mathrm{Split}(f)/F$ is finite Galois with $\mathrm{Gal}_f = \mathrm{Gal}(\mathrm{Split}(f)/F)$ solvable, $\mathrm{Split}(f)$ is contained in a radical extension K/F.

In general polynomials of degree ≥ 5 are not solvable by radicals. In the following we focus on algebraic equations of degree 3 and 4 and compute their Galois groups.

Lemma 3.54. *Assume $f(X) \in \mathbb{Q}[X]$ of degree n is separable. Then* Gal_f *is isomorphic to a subgroup of* S_n. *Moreover if $f(X)$ is irreducible, then this subgroup of S_n is transitive and $n|\ |\mathrm{Gal}_f|$. A subgroup H of S_n is called transitive if $\forall i, j \in \{1, ..., n\}$, $\exists \sigma \in H$ such that $\sigma(i) = j$.*

Proof. Suppose $\{u_1, ..., u_n\}$ are distinct roots of $f(X)$ and S_n is the permutation group of them. Then since $\mathrm{Split}(f) = \mathbb{Q}(u_1, ..., u_n)$, we can define $\mathrm{Gal}_f \hookrightarrow S_n, \tau \mapsto \tau|\{u_1, ..., u_n\}$. τ is determined by its values on u_i. Hence this map is injective.

Next we assume $f(X)$ is irreducible. Then the Lemma 2.7 , Proposition 2.14 and that $\mathrm{Split}(f)/\mathbb{Q}$ is normal imply Gal_f is transitive. The minimal polynomial of u_1 over $\mathbb{Q}$ is just $f(X)$, hence $[\mathbb{Q}(u_1) : \mathbb{Q}] = n$. We see $n|\ |\mathrm{Gal}_f| = [\mathrm{Split}(f) : \mathbb{Q}]$. □

In the next section we will construct polynomials whose Galois groups are S_n. Here we recall some facts about permutation groups and details can be found in [Bos18] Section 5.3 and 5.4.

Fact 3.55.

(1) Every element of S_n can be written as the composition of transpositions (i, j). There will be a group morphism sign : $S_n \to \mathbb{Z}/2\mathbb{Z}$ such that for $\tau \in S_n$, if in a decomposition of transpositions, there are evenly many transpositions, then $\mathrm{sign}(\tau) = 0$ otherwise $\mathrm{sign}(\tau) = 1$. ker sign is denoted by A_n and it's a normal subgroup of index 2.

(2) Every permutation group S_n is solvable for $n \leq 4$, but not solvable if $n \geq 5$. To prove this we need some computations, but the proof is omitted.

$$[S_n, S_n] = A_n, \text{ for } n \geq 2$$

$$[A_n, A_n] = \begin{cases} \{1\} & \text{for } n = 2, 3 \\ V_4 & \text{for } n = 4 \\ A_n & \text{for } n \geq 5 \end{cases}$$

where $[G, G]$ denotes the commutator subgroup of G and V_4 is the **Klein four-group** $\{id, (12)(34), (13)(24), (14)(23)\} \subseteq S_4$.

(3) We then focus on describing subgroups of S_3 and S_4. In fact subgroups of S_3 have been studied in Example 3.20. We deal with S_4 here. In the following is the list of classes of subgroups of S_4.

- $S_2 \hookrightarrow S_4$: $\{id, (12)\}$, with order $= 2$, not transitive.
- $\{id, (12)(34)\}$ with order $= 2$, not transitive.
- $C_4 = \langle (1234) \rangle = \{id, (1234), (13)(24), (1432)\}$ cyclic and transitive subgroup bu not normal.
- $V_4 = \{id, (12)(34), (13)(24), (14)(23)\}$ with order $= 4$, transitive and normal.
- $\langle (12), (34) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ not transitive.
- $D_4 = \langle (1234), (13) \rangle$ with order $= 8$, transitive.
- $A_3, S_3 \hookrightarrow S_4$ (not transitive).
- A_4 transitive with order $= 12$.

and there is a subnormal series:

$$\{id\} \subseteq \{id, (12)(34)\} \subseteq V_4 \subseteq A_4 \subseteq S_4$$

we see S_4 is solvable.

Now let's consider algebraic equations of degree 3 and 4. Given a polynomial $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_0 \in F[X]$, it factors as $f(X) = \prod_{i=1}^{n}(X - x_i)$ where $x_i \in \bar{F}$. We set

$$\Delta(f) = \prod_{i<j}(x_i - x_j)$$

and let $D(f) = \Delta(f)^2$. Then $D(f)$ is called the **discriminant** of the polynomial $f(X)$. Note $D(f) \neq 0$ iff $\forall i \neq j, x_i \neq x_j$ iff $f(X)$ is separable.

We derive some special formulas for $D(f)$ of algebraic equations $f(X) = 0$ of degree ≤ 4 now and it's not necessary to assume f to be irreducible or separable.

Example 3.56.

(1) We start with a *quadratic polynomial* $f(X) \in F[X]$, say $f(X) = X^2 + aX + b$. Since

$$\begin{cases} x_1 + x_2 = -a \\ x_1 \cdot x_2 = b \end{cases}$$

we see $D(f) = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = a^2 - 4b$.

(2) Let $f(X) = X^3 + aX^2 + bX + c$. Replacing X by $X - \frac{a}{3}$, $f(X)$ has a simpler form $X^3 + pX + q$. Using Vieta theorem

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = p \\ x_1x_2x_3 = q \end{cases}$$

we have $D(f) = -4p^3 - 27q^2$.

(3) A monic polynomial $X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ has the form $f(X) = X^4 + aX^2 + bX + c$ when replacing X by $X - \frac{a_3}{4}$. Then $D(f) = 144ab^2c - 128a^2c^2 - 4a^3b^2 + 16a^4c - 27b^4 + 256c^3$.

(4) You can find more general formulas for $D(f)$ of polynomials of degree ≥ 5 in [Bos18] Section 4.4.

Next we assume $f(X) \in F[X]$ is irreducible of degree $n \Rightarrow \Delta(f) \neq 0$. Let $\sigma \in S_n$, $\sigma(\Delta(f)) = (-1)^{\text{sign}(\sigma)}\Delta(f)$, where it's enough to consider $\sigma = (ij)$, $j = i + k, k > 0$. Then $\sigma(\Delta(f)) = (-1)^{2k-1}\Delta(f) = -\Delta(f)$. Therefore $\sigma \in \mathrm{A}_n$ iff $\sigma(\Delta(f)) = \Delta(f)$. And $\sigma(D(f)) = D(f)$. Since $\text{Split}(f)/F$ is Galois and $\text{Gal}_f \subseteq S_n$, we see $D(f) \in F$. In a summary we have proved:

Lemma 3.57. *Suppose $f(X) \in F[X]$ is irreducible of degree n. Then $\text{Gal}_f \subseteq A_n$ iff $\Delta(f) \in F$ iff $\sqrt{D(f)} \in F$.*

Assume $F = \mathbb{Q}$.

- If $deg(f) = 2$, then $\text{Gal}_f \cong \mathbb{Z}/2\mathbb{Z}$.
- If $deg(f) = 3$, then $\text{Gal}_f \leq S_3$. But $3|\ |\text{Gal}_f|$. We see $|\text{Gal}_f| = 3$ or $6 \Rightarrow \text{Gal}_f = A_3$ or S_3 and $\text{Gal}_f = A_3$ iff $\Delta(f) \in \mathbb{Q}$.

Example 3.58.

(1) $f(X) = X^3 - 3X + 1$. Then f is irreducible in $\mathbb{Q}[X]$ since 1 and -1 are not its roots. $D(f) = -4 \cdot (-3)^3 - 27 = 81$, $\Delta(f) \in \mathbb{Q}$. Then $\text{Gal}_f = \mathrm{A}_3$.

(2) $f(X) = X^3 + 3X + 1$. Then $D(f) = -5 \times 3^3$. Hence $\text{Gal}_f = \mathrm{S}_3$.

Remark 3.59. Now let's consider an irreducible *quartic polynomial* $f(X) = X^4 + bX^3 + cX^2 + dX + e \in \mathbb{Q}[X]$, whose roots are x_1, x_2, x_3, x_4. Then we consider:

$$\begin{cases} \alpha = x_1x_2 + x_3x_4 \\ \beta = x_1x_3 + x_2x_4 \\ \gamma = x_1x_4 + x_2x_3 \end{cases}$$

since x_i's are all different, α, β, γ are all different as well. S_4 can act on $\{\alpha, \beta, \gamma\}$. For $\sigma \in \mathrm{S}_4$, $\sigma(\alpha) = x_{\sigma(1)}x_{\sigma(2)} + x_{\sigma(3)}x_{\sigma(4)}$. The stabilizer of α, β or γ is a Sylow 2-group. For example $\mathrm{Stab}(\beta) =< (1234), (13) >= \mathrm{D}_4$. And we could see V_4 is contained in all of stabilizers of α, β and γ. Hence V_4 fixes all of α, β, γ. In fact $V_4 = \mathrm{Stab}(\alpha) \cap \mathrm{Stab}(\beta) \cap \mathrm{Stab}(\gamma)$. Hence the Galois group $\mathrm{Gal}(\mathbb{Q}(x_1, x_2, x_3, x_4)/\mathbb{Q}(\alpha, \beta, \gamma))$ is just $\mathrm{Gal}_f \cap V_4$.

Let $g(X) = (X - \alpha)(X - \beta)(X - \gamma)$ which is called the ***cubic resolvent*** of $f(X)$. Since every element σ of S_4 which is the permutation group of $\{x_1, x_2, x_3, x_4\}$ just permutes $\{\alpha, \beta, \gamma\}$, $\sigma(g) = g$. Then $\forall \tau \in \mathrm{Gal}_f, \tau(g) = g \Rightarrow$ all coefficients of g are in $\mathbb{Q}$. $g(X) \in \mathbb{Q}[X]$, whose splitting field is $\mathbb{Q}(\alpha, \beta, \gamma)$. And $\mathbb{Q}(\alpha, \beta, \gamma)/\mathbb{Q}$ is Galois $\Rightarrow$ $\mathrm{Gal}_f \cap V_4 \trianglelefteq \mathrm{Gal}_f$ is normal, then $\mathrm{Gal}_g \cong \mathrm{Gal}_f/\mathrm{Gal}_f \cap V_4$. There is a decomposition:

$$\begin{tikzcd} \mathbb{Q}(x_1, x_2, x_3, x_4) \arrow[d, dash, "\mathrm{Gal}_f \cap \mathrm{V}_4"'] \\ \mathbb{Q}(\alpha, \beta, \gamma) \arrow[d, dash, "\mathrm{Gal}_f/\mathrm{Gal}_f \cap \mathrm{V}_4"'] \\ \mathbb{Q} \end{tikzcd} \tag{9}$$

Lemma 3.60. *If $f(X) = X^4 + bX^3 + cX^2 + dX + e$, then $g(X) = X^3 - cX^2 + (bd - 4e)X - b^2e + 4ce - d^2$ and $D(f) = D(g)$. In particular if $b = 0$, $f(X) = X^4 + cX^2 + dX + e$, $g(X) = X^3 - cX^2 - 4eX + 4ce - d^2$.*

The computation is omitted and we state the following important theorem.

Theorem 3.61. *Let $M = \mathbb{Q}(\alpha, \beta, \gamma), K = \mathbb{Q}(x_1, x_2, x_3, x_4), m = [M : \mathbb{Q}]$.*

(1) If $m = 1$, then $\mathrm{Gal}_f = V_4$.

(2) If $m = 2$, then $\mathrm{Gal}_f = C_4$ or D_4. Moreover $\mathrm{Gal}_f = D_4$ iff $\mathrm{Gal}_f \cap V_4$ acts transitively on $\{x_1, x_2, x_3, x_4\}$ iff $f(X)$ is irreducible in $M[X]$.

(3) If $m = 3$, then $\mathrm{Gal}_f = A_4$.

(4) If $m = 6$, then $\mathrm{Gal}_f = S_4$.

Proof. See Fact 3.55 (3) for subgroups of S_4.

(1). $m = 1 \Rightarrow \mathrm{Gal}_g = 1 \Rightarrow \mathrm{Gal}_f \cap V_4 = V_4 \Rightarrow \mathrm{Gal}_f \subseteq V_4$. But $\{id, (12)(34)\}$ is not transitive $\Rightarrow \mathrm{Gal}_f = V_4$.

(2). $m = 2 \Rightarrow |\mathrm{Gal}_g| = 2 \Rightarrow |\mathrm{Gal}_f/\mathrm{Gal}_f \cap V_4| = 2$. If $|\mathrm{Gal}_f \cap V_4| = 1$, then $|\mathrm{Gal}_f| = 2$. But there is no such transitive subgroup of order 2. If $|\mathrm{Gal}_f \cap V_4| = 2$, then $|\mathrm{Gal}_f| = 4 \Rightarrow \mathrm{Gal}_f = C_4$. If $|\mathrm{Gal}_f \cap V_4| = 4$, then $|\mathrm{Gal}_f| = 8 \Rightarrow \mathrm{Gal}_f = \mathrm{D}_4$. $\mathrm{Gal}_f = D_4$ iff $\mathrm{Gal}_f \cap V_4 = V_4$ iff $\mathrm{Gal}_f \cap V_4$ acts transitively on $\{x_1, x_2, x_3, x_4\}$, since no proper subgroup of V_4 satisfy it. And this is also equivalent to say $|\mathrm{Gal}_f \cap V_4| = 4$ or $[K : M] = 4$.

If $f(X)$ is not irreducible in $M[X]$, then for a root x of $f(X)$, the degree of its minimal polynomial over M is strictly smaller than 4 and it should not be 3 since $3 \nmid 4$. It must be 2. Then there will be two roots of $f(X)$ in $M(x)$ say x_1, x_2. From

$$\begin{cases} \frac{\beta}{x_1} = x_3 + \frac{x_2}{x_1} x_4 \\ \frac{\gamma}{x_1} = \frac{x_2}{x_1} x_3 + x_4 \end{cases}$$

we see $x_3, x_4 \in M(x)$ as well, which means $[K : M] = 2$. Hence when $m = 2$, $\mathrm{Gal}_f = \mathrm{D}_4$ iff $[K : M] = 4$ iff $f(X)$ is irreducible in $M[X]$.

(3). If $m = 3$, $|\mathrm{Gal}_f/\mathrm{Gal}_f \cap V_4| = 3$, $3|\ |\mathrm{Gal}_f|$. Then Gal_f should be A_4 or S_4. But $|S_4/V_4| = 6$. Then Gal_f must be A_4.

(4). If $m = 6$, $|\mathrm{Gal}_f/\mathrm{Gal}_f \cap \mathrm{V}_4| = 6$ then Gal_f should be S_4.

□

Example 3.62.

(1) $f(X) = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$. It's irreducible by Eisenstein's criterion. Its cubic resolvent is $g(X) = X^3 - 4X^2 - 8X + 32 = (X - 4)(X^2 - 8)$. Then $m = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. And $f(X) = (X^2 + 2)^2 - 2 = (X^2 + 2 + \sqrt{2})(X^2 + 2 - \sqrt{2})$. According to the Theorem 3.61 (2), $\mathrm{Gal}_f = C_4$.

(2) $f(X) = X^4 + 2X + x \in \mathbb{Q}[X]$. It's irreducible by Eisenstein's criterion. Its cubic resolvent is $g(X) = X^3 - 8X - 4$. $\{1, -1, 2, -2, 4, -4\}$ are all not its roots. Hence $g(X)$ is irreducible in $\mathbb{Q}[X]$. $D(g) = -4(-8)^3 - 27(-4)^2 = 1616$, $\sqrt{D(g)} \notin \mathbb{Q}$. Then $\mathrm{Gal}_g \cong S_3$ according to the Lemma 3.57. $m = |S_3| = 6$. Therefore $\mathrm{Gal}_f = S_4$.

Exercise 3.63. Determine Galois groups of the following polynomials over $\mathbb{Q}$:

(a) $X^3 - 2X + 3$.

(b) $X^4 + 8X + 12$.

(c) $X^4 + 3X + 3$.

Exercise 3.64. Find the Galois group of $X^6 - 3X^2 + 1$ over $\mathbb{Q}$.

Exercise 3.65. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree 5. List all (up to isomorphism) subgroups of S_5 which can be the Galois group of f.

3.5 Polynomials with Galois Group S_n over $\mathbb{Q}$

It's well known that polynomials of degree ≤ 4 are solvable by radicals but polynomials of degree ≥ 5 are not solvable by radicals in general. From the Fact 3.55 (2) we know any permutation group S_n is solvable for $n \leq 4$, but not solvable for $n \geq 5$. Hence according to the Theorem 3.51 if we construct a polynomial whose Galois group is S_n for $n \geq 5$, then we have proved the second part of the first sentence in this paragraph and this is our task in this section. We first find some criterion for subgroups of S_n to become S_n actually.

Lemma 3.66. *Let $G \leq S_n$ be a transitive subgroup of S_n. If G contains a 2-cycle and an $(n-1)$-cycle τ, then $G = S_n$.*

Proof. A d-cycle has the form $(i_1...i_d)$. We can assume $\tau = (23...n), (ij) \in G$ where $j \neq 1$. Since for any $\sigma \in S_n$, $\sigma \cdot (ij) \cdot \sigma^{-1} = (\sigma(i)\sigma(j))$, from the assumption that G is transitive, there will exist $\sigma \in G$ such that $\sigma(i) = 1$, and then $\sigma \cdot (ij) \cdot \sigma^{-1} = (1\sigma(j)) \in G$, $\sigma(j) \neq 1$. Therefore we can suppose $(1a) \in G$ where $a \in \{2, ..., n\}$.

Let τ acts on $(1a)$. $\tau^k \cdot (1a) \cdot \tau^{-k} = (\tau^k(1)\tau^k(a)) = (1\tau^k(a))$. This implies $(12), (13), ..., (1n) \in G$. And $(i1)(j1)(i1) = (ij) \in G$. We conclude $G = S_n$. □

This lemma motivates us to find a polynomial whose Galois group contains a 2-cycle and an $(n-1)$-cycle. And it can be constructed locally due to the following lemma.[3]

Lemma 3.67. *Let $f(X) \in \mathbb{Z}[X]$ be monic. We fix a prime p and consider $\bar{f} \in \mathbb{F}_p[X]$ where $deg(f) = deg(\bar{f}) = n$. If $\bar{f}$ is separable, then* $\mathrm{Gal}_{\bar{f}} \leq \mathrm{Gal}_f \leq S_n$, *where* $\mathrm{Gal}_f = \mathrm{Gal}(\mathrm{Split}(f)/\mathbb{Q})$ *and* $\mathrm{Gal}_{\bar{f}} = \mathrm{Gal}(\mathrm{Split}(\bar{f})/\mathbb{F}_p)$.

Before giving a proof here, we sketch the method, which is called *Kronecker's analysis.* If $f(X) \in \mathbb{Q}[X]$ of degree n has n's different roots $\{u_1, ..., u_n\}$, from the Lemma 3.54 we know $\mathrm{Gal}_f \subseteq S_n$. Let $E = \mathrm{Split}(f)$. We define the following polynomial

$$g(X) = \prod_{\sigma \in S_n} [X - (u_{\sigma(1)}T_1 + ... + u_{\sigma(n)}T_n)] \in E(T_1, ..., T_n)[X]$$

over the rational field $E(T_1, ..., T_n)$ and the linear factors are all different. Then $\forall \sigma \in S_n$, $\sigma(g) = g$. Especially $\forall \tau \in \mathrm{Gal}_f$, $\tau(g) = g$. Hence all coefficients of $g \in E[T_1, ..., T_n, X]$ are in $\mathbb{Q}$. Hence $g \in \mathbb{Q}[T_1, ..., T_n][X]$. Assume $g = g_1...g_k$, where $g_i \in \mathbb{Q}(T_1, ..., T_n)[X]$ is irreducible. If $X - (u_{\sigma(1)}T_1 + ... + u_{\sigma(n)}T_n) | g_i$, then

$$\forall \tau \in \mathrm{Gal}_f,\ X - (u_{\tau\sigma(1)}T_1 + ... + u_{\tau\sigma(n)}T_n) | \tau(g_i) = g_i$$

[3] This lemma comes from [Lan02] P274, or you can find details in [Jac85] Section 4.16.

which means $\prod_{\tau\in \mathrm{Gal}_f}[X-(u_{\tau\sigma(1)}T_1+...+u_{\tau\sigma(n)}T_n)]\ |g_i$. But $\prod_{\tau\in \mathrm{Gal}_f}[X-(u_{\tau\sigma(1)}T_1+ ... + u_{\tau\sigma(n)}T_n)]$ is invariant under $\tau'\in \mathrm{Gal}_f$. Hence it's in $\mathbb{Q}(T_1,...,T_n)[X]$. Then

$$\prod_{\tau\in \mathrm{Gal}_f}[X-(u_{\tau\sigma(1)}T_1+...+u_{\tau\sigma(n)}T_n)]=g_i$$

This argument implies that $g=g_1...g_k$ represents the coset decomposition of Gal_f in S_n. And we can thus assume $g_1=\prod_{\tau\in \mathrm{Gal}_f}[X-(u_{\tau(1)}T_1+...+u_{\tau(n)}T_n)]$.

Moreover we consider another action of S_n on g_i. For any $\gamma\in S_n$, $\gamma(g_i(T_1,...,T_n,X))=g_i(T_{\gamma(1)},...,T_{\gamma(n)},X)$. If $\gamma(g_i)=g_i$, then

$$\begin{aligned}&X-(u_{\sigma(1)}T_{\gamma(1)}+...+u_{\sigma(n)}T_{\gamma(n)})\\=&X-(u_{\sigma\gamma^{-1}(1)}T_1,...,u_{\sigma\gamma^{-1}}T_u)\\=&X-(u_{\tau\sigma(1)}T_1+...+u_{\tau\sigma(n)}T_n),\ \text{for some }\tau\in \mathrm{Gal}_f\end{aligned}$$

then $\sigma\gamma^{-1}=\tau\sigma\Rightarrow\gamma=\sigma^{-1}\tau^{-1}\sigma$. On the other hand for any $\sigma^{-1}\tau\sigma$ where $\tau\in \mathrm{Gal}_f$, $\mu\sigma(\sigma^{-1}\tau\sigma)^{-1}=\mu\tau^{-1}\sigma$. Hence the stabilizer of g_i in S_n is exactly $\sigma^{-1}\mathrm{Gal}_f\sigma$, which is denoted by $\mathrm{Stab}(g_i)$. Especially $\mathrm{Stab}(g_1)=\mathrm{Gal}_f$.

Proof of Lemma 3.67. $0\neq D(\bar{f})\equiv D(f)\bmod p$. Hence $D(f)\neq 0$ and $f(X)$ has n's different roots. Then we assume $\{u_1,...,u_n\}$ and $\{v_1,...,v_n\}$ are different roots of f and $\bar{f}$ in $\mathbb{C}$ and $\bar{\mathbb{F}}_p$ respectively. Consider a coefficient $h(u_1,...,u_n)$ of $g(X)$ defined above. It's invariant under S_n. Therefore $h(x_1,...,x_n)$ is a symmetric polynomial which can be expressed as a polynomial $h'(s_0,...,s_n)$ where

$$\begin{cases}s_0=1,\\ s_1=x_1+...+x_n\\ s_2=x_1x_2+x_1x_3+...+x_{n-1}x_n\\ ......\\ s_n=x_1...x_n\end{cases}$$

Since $f(X)\in\mathbb{Z}[X]$ is monic, then all $s_i\in\mathbb{Z}$. Hence $g(X)\in\mathbb{Z}[T_1,...,T_n][X]$. According to the Gauss' lemma, we see $g_i\in\mathbb{Z}[T_1,...,T_n][X]$. Suppose $\bar{g}=g(X)\bmod p\in\mathbb{F}_p(T_1,...,T_n)[X]$. Then $\bar{g}=\bar{g}_1...\bar{g}_k$.

Define

$$g'(X)=\prod_{\sigma\in S_n}[X-(v_{\sigma(1)}T_1+...+v_{\sigma(n)}T_n)]\in\mathbb{F}_p(T_1,...,T_n)[X]$$

we have $g'(X)=\bar{g}$. And $\bar{g}=\bar{g}_1...\bar{g}_k=g'_1...g'_{k'}$ where g'_i's are irreducible in $\mathbb{F}_p(T_1,...,T_n)[X]$ and represent the coset decomposition of $\mathrm{Gal}_{\bar{f}}$ in S_n. Moreover we may assume

$$g_1' = \prod_{\tau \in \mathrm{Gal}_{\bar{f}}} [X - (v_{\tau(1)}T_1 + ... + v_{\tau(n)}T_n)] \mid \bar{g}_i$$

We then prove $\mathrm{Gal}_{\bar{f}} = \mathrm{Stab}(g_1') \subseteq \mathrm{Stab}(g_i) = \sigma^{-1}\mathrm{Gal}_f\sigma$. We suppose there exists some $\gamma \in S_n$ such that $\gamma(g_1') = g_1'$ but $\gamma(g_i) \neq g_i$. Since g_i is irreducible, $\gamma(g_i)$ is irreducible as well. And $\gamma(g_i)|\gamma(g) = g$. Then $\gamma(g_i) = g_j, i \neq j$. But $\overline{\gamma(g_i)} = \gamma(\bar{g}_i)$, we see $\gamma(\bar{g}_i) = \bar{g}_j$, and $g_1' = \gamma(g_1')|\gamma(\bar{g}_i) = \bar{g}_j$, which means $g_1'^2|g'$ and g' has multiple roots. A contradiction! Hence $\sigma\mathrm{Gal}_{\bar{f}}\sigma^{-1} \subseteq \mathrm{Gal}_f$.

We know given a k-cycle $\lambda = (a_1...a_k)$, $\mu\lambda\mu^{-1} = (\mu(a_1)...\mu(a_k))$. From the Theorem 3.23, we know $\mathrm{Gal}_{\bar{f}}$ is cyclic. Decompose the generator of $\mathrm{Gal}_{\bar{f}}$as a disjoint product of n_i-cycles. We see after a rearrangement of $\{v_1, ..., v_n\}$, $\mathrm{Gal}_{\bar{f}} \subseteq \mathrm{Gal}_f$. □

Remark 3.68. In the proof above if we know the Theorem 4.38 in [Jac85], which says under the assumption of Lemma 3.67, there will exist a ring morphism $\mathbb{Z}[u_1, ..., u_n] \to \mathrm{Split}(\bar{f}) \subseteq \bar{\mathbb{F}}_p$, inducing a bicjection between the set of roots of f and the set of roots of $\bar{f} \in \mathbb{F}_p[X]$, then the proof may be simpler. Under such ring morphism, we will have $\bar{g}_1 = \prod_{\tau \in \mathrm{Gal}_f}[X - (v_{\tau(1)}T_1 + ... + v_{\tau(n)}T_n)]$.

The Lemma 3.67 is useful because it allows us to add a 2-cycle and an $(n-1)$-cycle to Gal_f, using the method of mod p reduction. To do this, it urges us studying $\mathrm{Gal}_{\bar{f}}$ further.

Theorem 3.69 (Dedekind)**.** *Under the assumption of Lemma 3.67, if*

$$\bar{f} = \bar{f}_1...\bar{f}_r, \bar{f}_i \in \mathbb{F}_p[X]$$

where $\bar{f}_i$'s are irreducible and monic. Assume $d_i = deg(\bar{f}_i)$. Then $\mathrm{Gal}_{\bar{f}}$ *is cyclic of order* $\mathrm{lcm}(d_1, d_2, ..., d_r)$*, containing a product of disjoint cycles of the form $\sigma_1...\sigma_r$, where $\sigma_i = (n_1...n_{d_i})$ is a d_i-cycle.*

Proof. Any finite field extension of $\mathbb{F}_p$ has the form $\mathbb{F}_{p^m}$.

$$\begin{aligned} \bar{f} \text{ splits completely over } \bar{F}_{p^m} &\Leftrightarrow \bar{f}_i \text{ splits completely over } \bar{F}_{p^m} \text{ for all } i \\ &\Leftrightarrow \bar{f}_i \text{ divides } X^{p^m} - X \text{ for all } i \\ &\Leftrightarrow d_i = deg(\bar{f}_i) \text{ divides } m \\ &\Leftrightarrow \mathrm{lcm}(d_1, ..., d_r) \text{ divides } m \end{aligned}$$

Choosing a root u of $\bar{f}_i$, $\mathbb{F}_p(u) = \mathbb{F}_{p^{d_i}} \subseteq \mathbb{F}_{p^m}$ iff $d_i|m$, according to the first paragraph of the Section 3.1. We see $\mathbb{F}_{p^m}$ is the splitting field of $\bar{f}$ iff $m = \mathrm{lcm}(d_1, ..., d_r)$. Then from the Theorem 3.23 $\mathrm{Gal}_{\bar{f}} = \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z}$ where $m = \mathrm{lcm}(d_1, ..., d_r)$, generated by the Frob : $x \mapsto x^p$. Especially $\mathrm{Gal}_{\bar{f_i}} \cong \mathbb{Z}/d_i\mathbb{Z}$ is generated by Frob and $\bar{f_i}$ has roots

$$u_i, u_i^p, u_i^{p^2}, ..., u_i^{p^{d_i-1}}$$

where u_i is root of $\bar{f_i}$, since $\mathrm{Split}(\bar{f_i}) = \mathbb{F}_p(u_i) = \mathbb{F}_{p^{d_i}}$. Then $\mathrm{Frob} \in \mathrm{Gal}_{\bar{f_i}}$ is a d_i-cycle. Then $\bar{f}$ has roots:

$$u_1, ..., u_1^{p^{d_1-1}}, u_2, ..., u_2^{p^{d_2-1}}, ..., u_i, ..., u_i^{p^{d_i-1}}, ..., u_r, ..., u_r^{p^{d_r-1}}$$

Therefore we can conclude the generator Frob is a product of disjoint cycles of the form $\sigma_1...\sigma_r$, where $\sigma_i = (n_1...n_{d_i})$ is a d_i-cycle. □

Now we start to construct a polynomial whose Galois group is S_n.

Theorem 3.70. *There is an irreducible polynomial of degree n over $\mathbb{Q}$ such that its Galois group is S_n for all $n \geq 1$.*

Proof. If $n = 1$ or 2, this theorem can be checked directly. If $n = 3$, then $X^3 - 2$ has Galois group S_3, see Example 3.20 or Lemma 3.57. Therefore we assume $n \geq 4$.

We first construct a monic polynomial $f_1$of degree n satisfying

- $f_1 \bmod 2 \in \mathbb{F}_2[X]$ decomposes as $X \cdot h_1$ where $h_1 \in \mathbb{F}_2[X]$ is irreducible of degree $n - 1$.

We explain why f_1 always exist. Assume $\mathbb{F}_{p^m}$ is a finite field over $\mathbb{F}_p$. From the Corollary 2.39 we know $\mathbb{F}_{p^m}^\times$ is cyclic. Hence we suppose $\mathbb{F}_{p^m}^\times$ is generated by α. Then $\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha)$. And the minimal polynomial of α over $\mathbb{F}_p$ is irreducible of degree m. And then from the Theorem 3.69, we know $\mathrm{Gal}_{\bar{f_1}}$ contains an $(n-1)$-cycle.

Next we construct a monic polynomial f_2 of degree n satisfying

- $\bar{f_2} = f_2 \bmod 3 \in \mathbb{F}_3[X]$ decomposes as $h_1' \cdot h_2'$.
- $\bar{f_2}$ is separable.
- $deg(h_1') = n - 2, deg(h_2') = 2$. h_2' is irreducible and

$$\begin{cases} \text{When } n \text{ is odd, } h_1' \text{ is irreducible} \\ \text{When } n \text{ is even, } h_1' = X \cdot h_3', \text{ where } h_3' \text{ is an irreducible of degree } n-3 \end{cases}$$

h_1' and h_2' always exist. If n is odd, then $(2, n-2) = 1$, $\mathbb{F}_{3^2} \cap \mathbb{F}_{3^{n-2}} = \mathbb{F}_3$. And if n is even, then $(2, n-3) = 1$, $\mathbb{F}_{3^2} \cap \mathbb{F}_{3^{n-3}} = \mathbb{F}_3$. We know $\mathbb{F}_{p^m}/\mathbb{F}_p$ is separable. Let h_2' is the minimal polynomial of α, where α is the generator of $\mathbb{F}_{3^{n-2}}^\times$. h_1' and h_3' is defined similarly. From the first paragraph of Section 3.1 we know h_1' and h_2' will not have a same root.

According to the Theorem 3.69 above, we know $\mathrm{Gal}_{\bar{f}_2}$ contains an element of the form:

$$\begin{cases} \text{When } n \text{ is odd, } ((n-2)\text{-cycle}) \cdot (2\text{-cycle}) = \sigma_1\sigma_2 \\ \text{When } n \text{ is even, } ((n-3)\text{-cycle}) \cdot (2\text{-cycle}) = \gamma_1\gamma_2 \end{cases}$$

Then $(\sigma_1\sigma_2)^{n-2} = \sigma_2^{n-2} = \sigma_2$ and $(\gamma_1\gamma_2)^{n-3} = \gamma_2^{n-3} = \gamma_2$. Then $\mathrm{Gal}_{\bar{f}_2}$ contains a 2-cycle.

Finally we construct a monic irreducible polynomial $f(X) \in \mathbb{Z}[X]$ of degree n as follows:

- $f_1 \equiv f \bmod 2$.
- $f_2 \equiv f \bmod 3$.

We choose a polynomial $f_3 \in \mathbb{Z}[X]$ of degree $n-1$ such that $f(X) = 3f_1 - 2f_2 + 6f_3$ is irreducible by the Eisenstein's criterion of 5. Assume $3f_1 - 2f_2 = X^n + f_4$, where $f_4 = a_{n-1}X^{n-1} + ... + a_0$. Since $6 \equiv 1 \bmod 5$, we could find b_i such that $5|a_i + 6b_i$. If $25|a_0 + 6b_0$, we replace the b_0 by $b_0 + 5$, and then $25 \nmid a_0 + 6b_0 + 30$.

From the Lemma 3.67, $\mathrm{Gal}_{\bar{f}_1}, \mathrm{Gal}_{\bar{f}_2} \leq \mathrm{Gal}_f$. Then Gal_f contains a 2-cycle and an $(n-1)$-cycle. Hence $\mathrm{Gal}_f = S_n$ from the Lemma 3.66. □

Example 3.71. Assume $n = 4$.

(1) In $\mathbb{F}_2[X]$, $X^3 + X + 1$ is irreducible since 0 and 1 are not its roots. Then we choose $f_1 = X(X^3 + X + 1) \in \mathbb{Z}[X]$.

(2) In $\mathbb{F}_3[X]$, let $h_2' = X^2 + X + 2$, which is irreducible since there is no roots in $\mathbb{F}_3$. Let $h_3' = X - 1$, then $h_1' = X(X-1)$. $f_2 = X(X-1)(X^2 + X + 2)$. Then

$$\begin{aligned} 3f_1 - 2f_2 &= (3X^4 + 3X^2 + 3X) - (2X^4 + 2X^2 - 4X) \\ &= X^4 + X^2 + 7X \end{aligned}$$

Choose $f_3 = -X^2 - 2X + 5 \Rightarrow f = 3f_1 - 2f_2 + 6f_3 = X^4 - 5X^2 - 5X + 30$. We can also use the Theorem 3.61 to prove $\mathrm{Gal}_f = S_4$.

When n is big enough, this construction will be much more complicated. But if n is prime, then it may be much more simpler thanks to the following lemma and theorem.

Lemma 3.72. *Assume $G \leq S_p$ where p is a prime. If G contains a 2-cycle and a p-cycle, then $G = S_n$.*

Proof. See the Corollary 2.10 for a proof in `https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf` □

Theorem 3.73. *Let f be an irreducible polynomial of degree p over $\mathbb{Q}$ with exactly two non-real roots in $\mathbb{C}$. Then $\mathrm{Gal}_f = S_p$.*

Proof. If $a + bi$ is a root of f where $b \neq 0$, then $a - bi$ is a root as well, since $\overline{f(a+bi)} = f(\overline{a+bi})$. We assume the conjugation function is c. Then $c \in \mathrm{Gal}_f$ and is 2-cycle.

To prove Gal_f contains a p-cycle, we need the Cauchy's theorem.

Theorem 3.74 (Cuachy)**.** *For a finite group G, if $p|\ |G|$, then G has an element of order p.*

Since f is irreducible, if u is a root of f, then $p = [\mathbb{Q}(u) : \mathbb{Q}] \mid [\mathrm{Split}(f) : \mathbb{Q}] = |\mathrm{Gal}_f|$. If $\tau = \tau_1 \cdot ... \cdot \tau_r$ is an element in Gal_f of order p, where τ_i's are disjoint d_i-cycles. Then $\tau_i^p = 1 \Rightarrow d_i|p \Rightarrow d_i = 1$ or p, which means τ is a p-cycle. Then from the lemma above $\mathrm{Gal}_f = S_p$. □

Example 3.75. Assume $p = 5$. $f(X) = X^5 - 5X + 2 \in \mathbb{Q}[X]$ is irreducible because consider $f(X+3) = (X+3)^5 - 5(X+3) + 2$, $5|3^5 - 15 + 2 = 230$ but $5^2 \nmid 230$. $f'(X) = 5X^4 - 5 = 5(X^2+1)(X-1)(X+1)$. $f(-1) = 6 > 0, f(1) = -2 < 0$. Then from the graph of $f(X)$, we conclude it has three real roots. Hence it has two non-real roots. From the Theorem 3.73, $\mathrm{Gal}_f = S_5$. Since S_5 is not solvable, then f is not solvable by radicals.

Exercise 3.76. Show that $\mathbb{Q}_{\xi_7}$ contains a unique subfield E which is of degree 3 over $\mathbb{Q}$. Show that E is not a radical extension over $\mathbb{Q}$.

Exercise 3.77. Let $\mathbb{F}_p$ be the algebraic closure of $\mathbb{F}_p$ and let $G = \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. Frob $\in G$ is the Frobenius $x \mapsto x^p$. Find an element of G which is not a power of Frob, i.e. find $\sigma \in G$ such that $\sigma \neq \mathrm{Frob}^n$ for any $n \in \mathbb{Z}$.

Note: you may need to refer to the infinite Galois theory.

3.6 Infinite Galois Theory

In the previous sections, we only consider finite Galois extensions. In this section we consider infinite Galois extension, which is a Galois extension of infinite degree. And there is a similar theorem compared with Theorem 3.9. To deal with this infinite theory, we need to equip $\mathrm{Gal}(K/F)$ with a topology. And here we talk about topological groups first.

Definition 3.78. *A group G equipped with a topology is a **topological group** if*

$$\cdot : G \times G \to G, (g,h) \mapsto gh$$

$$\iota : G \to G, g \mapsto g^{-1}$$

are continuous maps.

Example 3.79. $(\mathbb{R}, +)$, $(\mathbb{R}^\times, \times)$.

Fact 3.80. Given an element $a \in G$, the *left multiplication map* is defined to be

$$L_a : G \overset{a\times id}{\longrightarrow} G \times G \overset{\cdot}{\longrightarrow} G, g \mapsto (a, g) \mapsto a \cdot g$$

L_a is continuous and has the inverse $L_{a^{-1}}$. Hence it's a homeomorphism. Dually there is a concept of right multiplication map R_a which is a homeomorphism as well.

Note: if X is a topological space, then open subsets on $X \times X$ are those the union of the form $U \times V$, where U, V are open in X. In fact the open basis on $X \times X$ is the class of finitely intersections of the form $U \times V$ where U, V is open in X. But $\cap_i(U_i \times V_i) = (\cap_i U_i) \times (\cap_i V_i)$, hence $U \times V$ form a basis of $X \times X$.

Corollary 3.81. *If $\mathcal{N}$ is a basis of open neighborhoods of $1 \in G$, then $a\mathcal{N}$ is a basis open neighborhood of $a \in G$.*

Proof. From the Fact 3.80, L_a is a homeomorphism, hence sending open subsets to open subsets. □

From this corollary, to know a topology of a topological group G, it's enough to know its basis of open neighborhoods around $1 \in G$.

Lemma 3.82. *G is a topological groups and $H \leq G$ is a subgroup of G equipped with the topology of subspaces. Then*

(1) H is a topological space as well.

(2) The closure $\overline{H}$ of H is a subgroup of G. Moreover if H is normal, then $\overline{H}$ is normal as well.

(3) G is Hausdorff iff $\{1\}$ is closed

Proof. (1). It's trivial.

(2). $h \in \overline{H}$ iff for any open subset U containing h, $U \cap H \neq \emptyset$. Assume $h_1, h_2 \in \overline{H}$. We need to prove $h = h_1h_2 \in \overline{H}, h_1^{-1} \in \overline{H}$. Given an open subset U containing h, since $\cdot : G \to G$ is continuous, $\cdot^{-1}(U)$ is open in $G \times G$ and $(h_1, h_2) \in \cdot^{-1}(U)$, then there are open subsets V_1, V_2 such that $h_i \in V_i$ and $V_1 \times V_2 \subseteq \cdot^{-1}(U)$. Then $V_1 \cdot V_2 \subseteq U$. But since $h_i \in \overline{H}$, then $V_i \cap H \neq \emptyset$. If we assume $g_i \in V_i \cap H$, then $g_1g_2 \in V_1 \cdot V_2 \cap H$, which means $U \cap H \neq \emptyset$. Hence $h \in \overline{H}$.

Given any open subset W containing h_1^{-1}. Since $\iota : G \to G$ is continuous, $h_1 \in \iota^{-1}(W)$ is open. Then $\iota^{-1}(W) \cap H \neq \emptyset$. If we assume $g \in \iota^{-1}(W) \cap H$, then $\iota(g) = g^{-1} \in W \cap H \neq \emptyset$. Hence $h_1^{-1} \in \overline{H}$.

If moreover we assume H is normal, then $\forall g \in G, gHg^{-1} = H$. Then $H = gHg^{-1} \leq g\overline{H}g^{-1}$ where $g\overline{H}g^{-1}$ is closed. Hence $\overline{H} \subseteq g\overline{H}g^{-1}$ for all $g \in G$. Replace

g by g^{-1}. Then $\overline{H} \subseteq g^{-1}\overline{H}g \subseteq g^{-1}(g\overline{H}g^{-1})g = \overline{H}$. Therefore $\overline{H} = g\overline{H}g^{-1}$ for all $g \in G$. Then $\overline{H}$ is normal.

(3). If G is Hausdorff, then every one point set is closed especially $\{1\}$ closed. Conversely, if $\{1\}$ is closed, we consider the following function:

$$\tau : G \times G \xrightarrow{id\times\iota} G \times G \xrightarrow{\cdot} G, (g,h) \mapsto (g,h^{-1}) \mapsto gh^{-1}$$

Since $\{1\}$ is closed, $W = \{1\}^c = G - \{1\}$ is open. Given any two different elements $g, h \in G$, $1 \neq gh^{-1} \in W$. Then $(g,h) \in \tau^{-1}(W)$ is an open subset in $G \times G$. Hence there exist open subsets $U, V \subseteq G$ such that $(g,h) \in U \times V \subseteq \tau^{-1}(W)$. And obviously $U \cap V = \emptyset$, otherwise $(a,a) \in \tau^{-1}(W) \Rightarrow 1 \in W$. A contradiction! □

Lemma 3.83. *Assume G is a topological group and $H \leq G$, then*

(1) If H is open then H is closed.

(2) If H is closed of finite index, then H is open.

(3) If G is compact, then H is open iff H is closed of finite index.

Proof. (1). Let S be the set of representatives of cosets of H in G. Then there is a coset decomposition

$$G = \coprod_{\sigma \in S} \sigma \cdot H$$

where $\sigma \cdot H$ is open since H is open and L_σ is a homeomorphism. But $G - H = \coprod_{\sigma \neq id} \sigma \cdot H$ is open as well. Hence H is also closed.

(2). Since H is of finite index, $|S| < \infty$. Then $G - H$ is a finite union of closed subsets, hence closed as well $\Rightarrow$ H is open.

(3). We only need to prove if H is open then it's closed of finite index, under the assumption that G is compact. Still considering the coset decomposition above $G = \coprod_{\sigma \in S} \sigma \cdot H$, which is an open covering. Since G is compact, then S is a finite set. □

Given a Galois extension K/F, now we equip $\mathrm{Gal}(K/F)$ with a topology.

Definition 3.84. *Define*

$$\mathcal{N} := \{\mathrm{Gal}(K/E) | F \subseteq E \subseteq K \textit{ and } E/F \textit{ is a finite Galois extension.}\}$$

to be the basis of open neighborhoods of $1 \in \mathrm{Gal}(K/F)$. *The topology on* $\mathrm{Gal}(K/F)$ *induced by $\mathcal{N}$ is called **Krull topology**.*

Remark 3.85.

(1) Given any two finite Galois extensions $E/F, E'/F$ such that $E, E' \subseteq K$, $\mathrm{Gal}(K/E\cdot E') = \mathrm{Gal}(K/E) \cap \mathrm{Gal}(K/E')$, where $E \cdot E'/F$ is finite Galois as well. Hence $\mathcal{N}$ is actually a basis of open neighborhoods of id.

(3) If K/F is finite Galois, then the Krull topology is discrete, since $\mathrm{Gal}(K/K) = \{id\} \in \mathcal{N}$. Then $\{id\}$ is open and any one point set is open.

(3) With the Krull topology, $\mathrm{Gal}(K/F)$ is actually a topological group.

Proof. To prove this we need the following Lemma 3.86. Note that the proof of this lemme is independent from the fact that $\mathrm{Gal}(K/F)$ is a topological group and in the proof we only need the definition of Krull topology. Actually Krull topology can also be defined as the weakest topology of those φ's.

To prove the composition function $\circ : \mathrm{Gal}(K/F) \times \mathrm{Gal}(K/F) \to \mathrm{Gal}(K/F)$ is continuous, it's enough to prove

$$\mu : \mathrm{Gal}(K/F) \times \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F),\ (\tau, \sigma) \mapsto \tau \circ \sigma | E$$

is continuous where E/F is finite Galois and $\mathrm{Gal}(E/F)$ has discrete topology. If we assume $\lambda = \tau \circ \sigma | E$ is fixed, from the definition of Krull topology, we know $\tau \cdot \mathrm{Gal}(K/E)$ and $\mathrm{Gal}(K/E) \cdot \sigma$ is open around τ and σ respectively. But $\mu(\tau \cdot \mathrm{Gal}(K/E), \mathrm{Gal}(K/E) \cdot \sigma) = \tau \circ \sigma | E = \lambda$. Then μ is continuous.

Similarly, to prove $\iota : \mathrm{Gal}(K/F) \to \mathrm{Gal}(K/F)$, $\iota(\tau) = \tau^{-1}$ is continuous, we only need to prove $\iota' : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$, $\iota'(\tau) = \tau^{-1}|E$ is continuous. But consider the open neighborhood $\tau \cdot \mathrm{Gal}(K/E)$ of τ, we see $\iota'(\tau \cdot \mathrm{Gal}(K/E)) = \tau^{-1}|E$. Then ι' is continuous. Therefore $\mathrm{Gal}(K/F)$ is a topological group with Krull topology. □

(4) If we define

$$\mathcal{N}' := \{\mathrm{Gal}(K/E) | F \subseteq E \subseteq K \text{ and } E/F \text{ is a finite field extension.}\}$$

then this also defines the Krull topology.

Proof. Obviously, $\mathcal{N} \preceq \mathcal{N}'$. On the other hand for any finite field extension E/F contained in K, since K/F is Galois$\Rightarrow$ E/F is finite separable, then the normal closure $\overline{E}/F$ is finite Galois according to Remark 3.4 and $\mathrm{Gal}(K/\overline{E}) \subseteq \mathrm{Gal}(K/E)$. Then $\mathcal{N}' \preceq \mathcal{N}$, which implies $\mathcal{N}$ and $\mathcal{N}'$ induce the same topology. Or further we consider $H' \leq H \leq G$, where H' is open and G is a topological group. Then from the coset decomposition of H' in H, we conclude H is open as well. Then $\mathrm{Gal}(K/E)$ is open in the topology induced by $\mathcal{N}$. □

(5) If E/F is a field extension contained in K which is not necessarily finite, then $\mathrm{Gal}(K/E)$ is closed.

Proof. In fact E is the composition of all finite field extensions contained in E. Hence

$$\mathrm{Gal}(K/E) = \bigcap_{L/F \text{ finite}, \ L\subseteq E} \mathrm{Gal}(K/L)$$

But $\mathrm{Gal}(K/L)$ is open from (4) above, hence closed as well according to the Lemma 3.83. □

Lemma 3.86. *For any finite Galois extension E/F contained in a Galois extension K/F, the following map*

$$\varphi : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F), \tau \mapsto \tau|E$$

is continuous and surjective.

Proof. Since E/F is normal, from the Theorem 2.18, we see this map φ is well defined. And according to the Proposition 2.14 and the fact that K/F is normal, any may $E \to E \hookrightarrow \bar{F}$ can be embedded into $K \to K$ and then φ is surjective.

Since E/F is finite Galois, $\mathrm{Gal}(E/F)$ is a finite set with discrete topology. Then it's enough to prove $\ker\, \varphi$ is open in $\mathrm{Gal}(K/E)$. $\tau \in \ker\, \varphi$ iff $\tau|E = id$ iff $\tau \in \mathrm{Gal}(K/E)$ which is open by definition of Krull topology. In fact Krull topology is the weakest topology induced by all such φ. □

Then we could consider the map

$$\iota = \prod \varphi : \mathrm{Gal}(K/F) \longrightarrow \prod_{E/F \text{ is finite Galois}} \mathrm{Gal}(E/F)$$

which is an injective group homomorphism. If we assume $\iota(\tau) = \iota(\sigma)$, then given $u \in K$, $F(u)/F$ is the simple extension of u over F and E/F is the normal closure of $F(u)/F$, hence finite Galois. Then $\tau|E = \sigma|E$, $\tau(u) = \sigma(u) \Rightarrow \tau = \sigma$. Then ι is a group isomorphism to its image. To study im ι further, we introduce the concept of inverse limits.

If $\{G_i|i \in I\}$ is a family of groups where I is a partially ordered set and there are group homomorphisms

$$p_{ij} : G_j \to G_i, \ \forall i, j \in I, \ i \leq j$$

the ***inverse limit*** $\varprojlim G_i$ is defined to be a group G with group homomorphisms $p_i : G \to G_i$ such that $p_{ij} \circ p_j = p_i, \ \forall i, j \in I, \ i \leq j$, satisfying the universal property that if (H, f_i) is another solution such that $p_{ij} f_j = f_i, \ i \leq j$, then there is a unique homomorphism $\theta : H \to G$ such that $p_i \circ \theta = f_i$.

$$\begin{tikzcd}
G \arrow[dr, "p_j"] \arrow[ddr, "p_i"'] & & H \arrow[ll, dotted, "\exists!\ \theta"'] \arrow[dl, "f_j"'] \arrow[ddl, "f_i"] \\
& G_j \arrow[d, "p_{ij}"] & \\
& G_i &
\end{tikzcd} \tag{10}$$

For simplicity such G is denoted by $\varprojlim G_i$ as well and it's unique up to isomorphism. In the category of groups, the inverse limit has another explicit form

$$\varprojlim G_i := \{(g_i) \in \prod_{i \in I} G_i \mid p_{ij}(g_j) = g_i\}$$

Dually there is a concept of ***inductive limits*** with all arrows in the diagram (10) reversed, which is denoted by $\varinjlim G_i$.

Example 3.87. Assume $I = \mathbb{N}$ and maps $G_i = \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^{i-1}\mathbb{Z} = G_{i-1},\ x \mapsto x \bmod p$. Then

$$\begin{aligned}
\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^i\mathbb{Z} &= \{(x_i)_{i \geq 1} | x_{i-1} \equiv x_i \bmod p^{i-1}\} \\
&= \{(a_0, a_1, ...) | 0 \leq a_i \leq p-1\} \\
&= \{\sum_{i \geq 0} a_i p^i | 0 \leq a_i \leq p-1\} \qquad (11)
\end{aligned}$$

The equations are derived from the fact that every element of $\mathbb{Z}$ has the unique form $\sum_{i=0}^{n} a_i p^i$ where $0 \leq a_i \leq p-1$. $\mathbb{Z}_p$ is called *the p-adic integers.*

If we consider inverse limits in the category of topological groups, such group $\varprojlim G_i$ will have the subspace topology of $\prod_{i \in I} G_i$, hence being a topological group as well. Especially there is a special type of inverse limits of topological groups.

Definition 3.88. *An inverse limit of finite (discrete) topological groups is called a* ***profinite group****.*

Lemma 3.89. *A profinite group is compact, Hausdorff and totally disconnected.*

Proof. According to Tcychonoff's theorem which states if topological spaces X_i's are compat then $\prod_i X_i$ is compact as well, $\prod_i G_i$ is compact since G_i's are finite discrete hence compact. $\varprojlim G_i \subseteq \prod_i G_i$. It's enough to prove $\varprojlim G_i$ is closed. Given $(g)_i \notin \varprojlim G_i$, then there will exist p_{ij} such that $p_{ij}(g_j) \neq g_i$. Define

$$U = \{g_1\} \times \{g_j\} \times \prod_{k \neq i,j} G_k$$

which is open in $\prod_i G_i$ since G_i's are discrete. Then $(g_i) \in U$, but $U \cap \varprojlim G_i = \emptyset$, which means $\prod_i G_i - \varprojlim G_i$ is open.

Given any two elements $(g_i)_i$ and $(h_i)_i$ in $\prod_i G_i$ such that $(g_i)_i \neq (h_i)_i$, then there will exist some j, $g_j \neq h_j$. Define open subsets $U_j = \{g_j\} \times \prod\limits_{i \neq j} G_i$ and $V_j = (G_j - \{g_j\}) \times \prod\limits_{i \neq j} G_i$. Then $(g_i)_i \in U_j$ and $(h_i)_i \in V_j$ but $U_j \cap V_j = \emptyset$. Hence $\prod_i G_i$ is Hausdorff, and then $\varprojlim G_i$ is Hausdorff as well.

Recall that a space X is called *totally disconnected* if for every $x \in X$ the component containing x is $\{x\}$ itself, which is also equivalent to say any subspace containing more than one element of X is not connected. We assume A is a subspace of $\prod_i G_i$ containing at least two different elements $(g_i)_i, (h_i)_i$. U_j and V_j are defined as before. Note $U_j \cup V_j = \prod_i G_i$ and $U_j \cap V_j = \emptyset$. Then A is the disjoint union of proper non-empty open subsets $U_j \cap A$ and $V_j \cap A$ of A, hence not connected, □

Given a Galois extension K/F, all finite Galois extensions E_i/F contained in K are indexed by the set I. $i \leq j$ iff $E_i \subseteq E_j$. Then I is a partially order set. Especially I is *directed* which means $\forall i, j \in I$, $\exists k \in I$ such that $i, j \leq k$. Then there will exist an inverse limit $\varprojlim \mathrm{Gal}(E_i/F) \subseteq \prod_i \mathrm{Gal}(E_i/F)$.

Theorem 3.90. *Induced from the injection $\iota : \mathrm{Gal}(K/F) \hookrightarrow \prod_i \mathrm{Gal}(E_i/F)$, there is an isomorphism $\iota' : \mathrm{Gal}(K/F) \xrightarrow{\sim} \varprojlim \mathrm{Gal}(E_i/F)$ in the sense of topological groups.*

Proof. We prove im ι is $\varprojlim \mathrm{Gal}(E_i/F)$ first. im $\iota \subseteq \varprojlim \mathrm{Gal}(E_i/F)$ is obvious and we prove the converse. Given an element $(\tau_i)_i \in \varprojlim \mathrm{Gal}(E_i/F)$, $\tau_j|E_i = \tau_i$ if $E_i \subseteq E_j$. For any element $u \in K$, its simple extension $F(u)$ is contained in some E_i such as its normal closure. We define $\tau : K \to K, u \mapsto \tau_i(u)$. If $u \in E_i \cap E_j$, since $E_k = E_i \cdot E_j$ is finite Galois as well from the Corollary 2.19 (2) and Proposition 2.27 (2), $i, j \leq k$, $\tau_i = \tau_k|E_i$ and $\tau_j = \tau_k|E_j$. Then $\tau_i(u) = \tau_j(u) = \tau_k(u)$. τ is well defined and $\tau|E_i = \tau_i$. This proves $\iota' : \mathrm{Gal}(K/F) \xrightarrow{\sim} \varprojlim \mathrm{Gal}(E_i/F)$ is a group isomorphism.

We prove ι' is a homeomorphism as well. First ι is continuous and then ι' is also continuous. Next we prove ι' is open and it's enough to prove $\iota'(\mathrm{Gal}(K/E_j))$ is open.

$$\iota'(\mathrm{Gal}(K/E_j)) = (\{1\} \times \prod_{E_i \neq E_j} \mathrm{Gal}(E_i/F)) \cap \varprojlim \mathrm{Gal}(E_i/F)$$

The right part of the equation above is open in $\varprojlim \mathrm{Gal}(E_i/F)$. Hence ι' is open. □

Corollary 3.91. $\mathrm{Gal}(K/F)$ *with Krull topology is a profinite group hence compact, Hausdorff and totally disconnected.*

There is a Galois correspondence for infinite Galois extensions as well.

Proposition 3.92. *Let K/F be a Galois extension. Then:*

(1) $K^{\mathrm{Gal}(K/F)} = F$.

(2) If $H \leq \mathrm{Gal}(K/F)$, *then* $\mathrm{Gal}(K/K^H)$ *is the closure of* H.

Proof. (1). If $x \in K^{\mathrm{Gal}(K/F)}$ is contained in some finite Galois extension E_i/F, since $\mathrm{Gal}(K/F) \to \mathrm{Gal}(E_i/F), \tau \mapsto \tau|E_i$ is surjective (Lemma 3.86), we see $x \in E_i^{\mathrm{Gal}(E_i/F)} = F$.

(2). At first from the Remark 3.85 (5), $\mathrm{Gal}(K/K^H)$ is closed containing H. Then $\overline{H} \subseteq \mathrm{Gal}(K/K^H)$. Conversely, assume $\sigma \notin \overline{H}$. Then there is an open subgroup $\mathrm{Gal}(K/E)$ where E/F is finite Galois such that $\sigma \cdot \mathrm{Gal}(K/E) \cap \overline{H} = \emptyset$. Consider the following exact sequence

$$1 \to \mathrm{Gal}(K/E) \to \mathrm{Gal}(K/F) \xrightarrow{\varphi} \mathrm{Gal}(E/F) \to 1$$

We have $\varphi(\sigma \cdot \mathrm{Gal}(K/E)) = \varphi(\sigma) \notin \varphi(H)$. $\varphi(H)$ is a subgroup of $\mathrm{Gal}(E/F)$. Then the Galois correspondence for finite Galois extensions tells us $\varphi(\sigma) \notin \varphi(H) = \mathrm{Gal}(E/E^{\varphi(H)})$. And there is some $x \in E^{\varphi(H)}$ such that $\varphi(\sigma)(x) = (\sigma|E)(x) \neq x$. But $E^{\varphi(H)} = K^H \cap E$. Hence $\sigma \notin \mathrm{Gal}(K/K^H \cap E) \supseteq \mathrm{Gal}(K/K^H)$. □

Theorem 3.93 (Galois Correspondence)**.** *Given a Galois extension K/F, there is a one-to-one correspondence*

$$\begin{aligned} \{\textit{closed subgroups } H \textit{ of } \mathrm{Gal}(K/F)\} &\longleftrightarrow \{\textit{subfields } E \textit{ of } K \textit{ containing } F\} \\ H &\longmapsto K^H \\ \mathrm{Gal}(K/E) &\longleftarrow\!\shortmid E \end{aligned} \tag{12}$$

- *H is open iff K^H is finite over F.*
- *H is normal iff K^H is Galois over F and*

$$\mathrm{Gal}(K^H/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/K^H)$$

Proof. Step 1: The one-to-one correspondence is easily derived from the Proposition 3.92.

Step 2: Since Gal(K/F) is compact, from the Lemma 3.83 the subgroup $H \leq$ Gal(K/F) is open iff it's closed of finite index. Now we only assume H is closed and the corresponding subfield is K^H.

Since K/F is separable, K^H/F is separable a well. From the Theorem 2.36 we know $[K^H : F] = |\text{Hom}_F(K^H, \bar{F})|$. Suppose cosets of Gal$(K/K^H) = H$ in Gal(K/F) are $\{H, \tau_1 H, \tau_2 H, ...\}$. We define a function:

$$\psi : \{H, \tau_1 H, \tau_2 H, ...\} \to \text{Hom}_F(K^H, \bar{F}), \tau_i H \mapsto \tau_i|K^H$$

Obviously we know ψ is well defined since $H = \text{Gal}(K/K^H)$. If $\psi(\tau_i H) = \psi(\tau_j H)$, then $\tau_i|K^H = \tau_j|K^H$ and $\tau_i \cdot \tau_j^{-1}|K^H = id$, which means $\tau_i \cdot \tau_j \in H \Rightarrow \tau_i H = \tau_j H$. Hence ψ is injective. Conversely given any $\sigma : K^H \to \bar{F}$, which can be extended to be $\sigma' : K \to K$ since K/F is normal. Then we see ψ is surjective. Therefore the index of H is just $|\text{Hom}_F(K^H, \bar{F})|$. This proves H is cloed of finie index iff $[K^H : F] < \infty$.

Step 3: The Step 3 of the proof of Theorem 3.9 is also valid here. □

Remark 3.94. Here we prove the theorem that Gal$(F^{ab}/F) = $ Gal$(\bar{F}_s/F)^{ab}$ in Remark 3.17.

Proof. Assume $G = \text{Gal}(\bar{F}_s/F)$. Since by definition $G^{ab} = G/\overline{[G,G]}$ for the profinite group G, from the Theorem 3.93 above we only need to prove Gal$(\bar{F}_s/F^{ab}) = \overline{[G,G]}$ which is the closure of the subgroup $[G,G]$ generated by all commutators in G. From Lemma 3.82 (2) $[G,G] \trianglelefteq G \Rightarrow \overline{[G,G]} \trianglelefteq G$. Suppose $L = \bar{F}_s^{\overline{[G,G]}}$. Then L/F is Galois with Gal$(L/F) \cong G/\overline{[G,G]}$ abelian. Therefore $L \subseteq F^{ab} \Rightarrow$ Gal$(\bar{F}_s/F^{ab}) \subseteq$ Gal$(\bar{F}_s/L) = \overline{[G,G]}$.

On the other hand, Gal$(\bar{F}_s/F^{ab}) \trianglelefteq G$ with $G/\text{Gal}(\bar{F}_s/F^{ab}) \cong \text{Gal}(F^{ab}/F)$ abelian, and then $[G,G] \subseteq \text{Gal}(\bar{F}_s/F^{ab}) \Rightarrow \overline{[G,G]} \subseteq \text{Gal}(\bar{F}_s/F^{ab})$ since Gal$(\bar{F}_s/F^{ab})$ is closed. □

Example 3.95.

(1) Fix the prime p and assume ξ_{p^n} is the p^n-th primitive root of unity 1. Let $K := \underset{n\geq 1}{\cup} \mathbb{Q}(\xi_{p^n})$. Since $K/\mathbb{Q}$ is the union of finite Galois extensions $\mathbb{Q}(\xi_{p^n})/\mathbb{Q}$, from the Remark 3.18 and Theorem 3.90 $K/\mathbb{Q}$ is Galois such that

$$\text{Gal}(K/\mathbb{Q}) \cong \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times = \{(a_0, a_1, ...)|a_0 \neq 0,\ 0 \leq a_i \leq p-1\}$$

(2) $\mathbb{F}_p$ is the finite field. From Theorem 3.23 we know Gal$(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$. For any algebraic field extension K/F, K is the union of all finite extensions E/F. Hence $\overline{\mathbb{F}}_p = \cup \mathbb{F}_{p^n}$. Then the *absolute Galois group* is

$$\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$$

Note $\overline{\mathbb{F}}_p$ is not the only infinite field extension between $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$. The following tower defines a proper subfield of $\overline{\mathbb{F}}_p$.

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^q} \subseteq \mathbb{F}_{p^{q^2}} \subseteq \ldots$$

Exercise 3.96. Prove that every open subgroup of a profinite group contains an open normal subgroup.

4 Galois Cohomology and Kummer Theory

4.1 Norm and Trace

Definition 4.1. *Given a finite extension K/F, for any $\alpha \in K$, we could define $\mathrm{N}_{K/F}(\alpha), \mathrm{Tr}_{K/F}(\alpha) \in F$ as follows:*

$$\mathrm{N}_{K/F}(\alpha) := \det(m_\alpha) \tag{13}$$

$$\mathrm{Tr}_{K/F}(\alpha) := \mathrm{trace}(m_\alpha) \tag{14}$$

where $m_\alpha : K \to K, x \mapsto \alpha \cdot x$ is an F-linear map.

Fact 4.2.

(1) $\mathrm{N}_{K/F}(\alpha)$ and $\mathrm{Tr}_{K/F}(\alpha)$ are independent from the choice of basis.

Proof. The matrix A and B are the matrices of the map m_α corresponding with two different bases. Then there is an inverse matrix T such that $B = TAT^{-1}$. Then $\mathrm{N}_{K/F}(\alpha) = \det(B) = \det(T)\det(A)\det(T)^{-1} = \det(A)$.

Given any two $n \times n$ matrices $U = (u_{ij})$ and $V = (v_{ij})$. Then $\mathrm{trace}(UV) = \sum_i \sum_k u_{ik}v_{ki} = \sum_i \sum_k v_{ik}u_{ki} = \mathrm{trace}(VU)$. Then $\mathrm{Tr}_{K/F}(\alpha) = \mathrm{trace}(B) = \mathrm{trace}(TAT^{-1}) = \mathrm{trace}(TT^{-1}A) = \mathrm{trace}(A)$. □

(2) $\mathrm{N}_{K/F}(-)$ is multiplicative, which means $\mathrm{N}_{K/F}(\alpha \cdot \beta) = \mathrm{N}_{K/F}(\alpha) \cdot \mathrm{N}_{K/F}(\beta)$. Especially if $a \in F$, $\mathrm{N}_{K/F}(a) = a^{[K:F]}$ and $\mathrm{N}_{K/F}(a \cdot \alpha) = a^{[K:F]}\mathrm{N}_{K/F}(\alpha)$.

(3) $\mathrm{Tr}_{K/F}(-)$ is additive, which means $\mathrm{Tr}_{K/F}(\alpha + \beta) = \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta)$. And if $a \in F$, $\mathrm{Tr}_{K/F}(a\alpha) = a\mathrm{Tr}_{K/F}(\alpha)$. Note $\mathrm{Tr}_{K/F}(a) = [K : F]a$.

(4) $\mathrm{Tr}_{K/F} : K \to F$ is an F-linear map. Hence it's surjective or 0.

Lemma 4.3. *If there is a tower $F \subseteq E \subseteq K$ where K/E is finite, then $\mathrm{N}_{K/F}(\alpha) = \mathrm{N}_{E/F}(\alpha)^{[K:E]}$ and $\mathrm{Tr}_{K/F}(\alpha) = [K : E] \cdot \mathrm{Tr}_{E/F}(\alpha)$ for all $\alpha \in E$.*

Proof. Assume $\{x_1, ..., x_n\}$ is a basis of E/F and $\{y_1, ..., y_m\}$ is a basis of K/E. From Proposition 2.2 $\{x_iy_j\}$ is a basis of K/F. If $A \in M_{n\times n}(F)$ is the corresponding matrix of m_α on E/F, which means

$$\alpha \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Then

$$\alpha \cdot \begin{pmatrix} x_1y_1 \\ x_2y_1 \\ \vdots \\ x_ny_1 \\ x_1y_2 \\ \vdots \\ x_ny_2 \\ \vdots \\ x_ny_m \end{pmatrix} = \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix} \cdot \begin{pmatrix} x_1y_1 \\ x_2y_1 \\ \vdots \\ x_ny_1 \\ x_1y_2 \\ \vdots \\ x_ny_2 \\ \vdots \\ x_ny_m \end{pmatrix}$$

$\mathrm{N}_{K/F}(\alpha) = \det(A)^m = \mathrm{N}_{E/F}(\alpha)^{[K:E]}$ and $\mathrm{Tr}_{K/F}(\alpha) = m \cdot \mathrm{Tr}_{E/F}(\alpha) = [K : E] \cdot \mathrm{Tr}_{E/F}(\alpha)$. □

Remark 4.4 (Transitivity)**.** The Lemma 4.3 above is a special case of following formulas

$$\mathrm{N}_{K/F} = \mathrm{N}_{E/F} \circ \mathrm{N}_{K/E} \tag{15}$$

$$\mathrm{Tr}_{K/F} = \mathrm{Tr}_{E/F} \circ \mathrm{Tr}_{K/E} \tag{16}$$

We will prove them later.

Lemma 4.5. *Let $K = F(\alpha)$ be a simple extension of F and $P \in F[X]$ is the minimal polynomial of α over F. Assume $P(X) = x^n + a_{n-1}X^{n-1} + ... + a_0$. Then*

$$\mathrm{N}_{K/F}(\alpha) = (-1)^n a_0$$

$$\mathrm{Tr}_{K/F}(\alpha) = -a_{n-1}$$

Proof. Choose $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ as the basis. Then the matrix of m_α is

$$\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ -a_0 & -a_1 & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$

Hence the trace is $-a_{n-1}$ and the determinant is $(-1)^{n+1}(-a_0) = (-1)^n a_0$. □

Proposition 4.6. *Let K/F be a finite field extension of $[K : F] = qr$ where $r = [K : F]_s$ is the separable degree and $q = [K : F]_i$ is the inseparable degree. See Definition*

2.30. From Theorem 2.36 we assume $\mathrm{Hom}_F(K, \bar{F}) = \{\sigma_1, ..., \sigma_r\}$*. Then we have the following formulas*

$$\mathrm{Tr}_{K/F}(\alpha) = q \sum_i \sigma_i(\alpha) \tag{17}$$

$$\mathrm{N}_{K/F}(\alpha) = \prod_i \sigma_i(\alpha)^q \tag{18}$$

Furthermore if K/F *is not separable for* $p = \mathrm{char}(F) > 0$*, then* q *is a nontrivial power of* p*, and we have* $\mathrm{Tr}_{K/F}(\alpha) = 0$*.*

Proof. We assume

$$\mathrm{tr}_{K/F}(\alpha) = q \sum_i \sigma_i(\alpha)$$
$$\mathrm{n}_{K/F}(\alpha) = \prod_i \sigma_i(\alpha)^q$$

and show that $\mathrm{tr}_{K/F} = \mathrm{Tr}_{K/F}, \mathrm{n}_{K/F} = \mathrm{N}_{K/F}$. First suppose $\alpha \in F$. Then $\sigma_i(\alpha) = \alpha$. From Fact 4.2 (2) and (3)

$$\mathrm{Tr}_{K/F}(\alpha) = [K : F] \cdot a = q(ra) = q \sum_i \sigma_i(\alpha) = \mathrm{tr}_{K/F}(\alpha)$$
$$\mathrm{N}_{K/F}(\alpha) = \alpha^{[K:F]} = (\alpha^q)^r = \prod_i \sigma_i(\alpha)^q = \mathrm{n}_{K/F}(\alpha)$$

Now consider the special case of $K = F(\alpha)$. Let the minimal polynomial of α over F be

$$X^n + a_{n-1}X^{n-1} + ... + a_0$$

where $n = qr$. No matter $\mathrm{char}(F)$ is 0 or not, from Remark 2.25, Remark 2.35, Lemma 2.7 and Theorem 2.36, the polynomial has factorization

$$\prod_{i=1}^{r} (X - \sigma_i(\alpha))^q$$

in $\bar{F}[X]$. Then from Lemma 4.5

$$\mathrm{Tr}_{K/F}(\alpha) = -a_{n-1} = q \sum_i \sigma_i(\alpha) = \mathrm{tr}_{K/F}(\alpha)$$
$$\mathrm{N}_{K/F}(\alpha) = (-1)^n a_0 = \prod_i \sigma_i(\alpha)^q = \mathrm{n}_{K/F}(\alpha)$$

Now if $\alpha \in K$ is arbitrary, consider the chain of fields $F \subseteq F(\alpha) \subseteq K$. Then from Lemma 4.3

$$\begin{aligned}\mathrm{Tr}_{K/F}(\alpha) &= [K : F(\alpha)] \cdot \mathrm{Tr}_{F(\alpha)/F}(\alpha)\\ \mathrm{N}_{K/F}(\alpha) &= (\mathrm{N}_{F(\alpha)/F}(\alpha))^{[K:F(\alpha)]}\end{aligned}$$

Consider the following surjective map

$$\mathrm{Hom}_F(K, \bar{F}) \to \mathrm{Hom}_F(F(\alpha), \bar{F}), \sigma_i \mapsto \sigma_i | F(\alpha)$$

From the proof of Theorem 2.36 for any F-map $\tau : F(\alpha) \to \bar{F}$ there are exactly $[K_s : F(\alpha)_s]$ many extensions $\sigma_i : K \to \bar{F}$ such that $\sigma_i | F(\alpha) = \tau$. Hence

$$\begin{aligned}\mathrm{tr}_{K/F}(\alpha) &= [K : K_s] \sum_i \sigma_i(\alpha)\\ &= [K : K_s] \cdot [K_s : F(\alpha)_s] \sum_{\tau \in \mathrm{Hom}_F(F(\alpha), \bar{F})} \tau(\alpha)\\ &= [K : K_s] \cdot [K_s : F(\alpha)_s] \mathrm{tr}_{F(\alpha)/F}(\alpha) \cdot \frac{1}{[F(\alpha) : F(\alpha)_s]}\\ &= \frac{[K : K_s] \cdot [K_s : F(\alpha)_s] \mathrm{Tr}_{F(\alpha)/F}(\alpha)}{[F(\alpha) : F(\alpha)_s]}\\ &= [K : F(\alpha)] \mathrm{Tr}_{F(\alpha)/F}(\alpha) = \mathrm{Tr}_{K/F}(\alpha) \qquad (19)\end{aligned}$$

and

$$\begin{aligned}\mathrm{n}_{K/F}(\alpha) &= \prod_i \sigma_i(\alpha)^{[K:K_s]}\\ &= \prod_{\tau \in \mathrm{Hom}_F(F(\alpha), \bar{F})} \tau(\alpha)^{[K:K_s] \cdot [K_s : F(\alpha)_s]}\\ &= \mathrm{n}_{F(\alpha)/F}(\alpha)^{\frac{[K:K_s] \cdot [K_s : F(\alpha)_s]}{[F(\alpha) : F(\alpha)_s]}}\\ &= \mathrm{N}_{F(\alpha)/F}(\alpha)^{[K:F(\alpha)]} = \mathrm{N}_{K/F}(\alpha) \qquad (20)\end{aligned}$$

□

We now use the Proposition 4.6 to prove the transitive formulas in Remark 4.4.

Proof of Remark 4.4. Assume there is a chain of finite extensions $F \subseteq E \subseteq K$ with

$$[E : F] = q_1 [E : F]_s, \ [K : E] = q_2 [K : E]_s$$

Suppose

$$\mathrm{Hom}_F(E, \bar{F}) = \{\sigma_1, ..., \sigma_r\}, \ \mathrm{Hom}_E(K, \bar{F}) = \{\tau_1, ..., \tau_s\}$$

We extend σ_i to be $\sigma_i' : \bar{F} \to \bar{F}$. Then we have

$$\mathrm{Hom}_F(K, \bar{F}) = \{\sigma_i' \circ \tau_j | 0 \leq i \leq r,\ 0 \leq j \leq s\}$$

It follows from the Proposition 4.6 that

$$\begin{aligned}\mathrm{tr}_{K/F}(\alpha) &= q_1 q_2 \sum_{i,j} \sigma_i' \tau_j(\alpha) \\ &= q_1 \sum_i \sigma_i'(q_2 \sum_j \tau_j(\alpha)) \\ &= q_1 \sum_i \sigma_i(q_2 \sum_j \tau_j(\alpha)) \\ &= \mathrm{tr}_{E/F}(\mathrm{tr}_{K/E}(\alpha)) \end{aligned} \tag{21}$$

There are similar equalities for $\mathrm{n}_{K/F}$. □

Corollary 4.7. *Assume K/F is a finite extension. Then K/F is separable iff $\mathrm{Tr}_{K/F} : K \to F$ is surjective iff $\mathrm{Tr}_{K/F}$ is non-zero.*

Proof. That $\mathrm{Tr}_{K/F}$ is surjective iff $\mathrm{Tr}_{K/F}$ is non-zero is clear.

First we consider the case of $\mathrm{char}(F) = 0$. Then K/F must be separable. Since $1 \neq 0$, from the Lemma 3.7 we see it's impossible for all $\alpha \in K$, $\mathrm{Tr}_{K/F}(\alpha) = \sum_i \sigma_i(\alpha) = 0$, where the symbols come from the Proposition 4.6.

Now we suppose $\mathrm{char}(F) = p > 0$. Then from the Lemma 3.7, $\mathrm{Tr}_{K/F}(\alpha) = q \sum_i \sigma_i(\alpha) = 0$ for all $\alpha \in K$ iff $q = 0$ in F which means $p|q$. Since $q \geq 1$, it's enough to prove $p|q \Leftrightarrow q > 1$. The part of $\Rightarrow$ is clear because $q \geq p > 1$. We assume $q > 1$ which means K/F is not separable. Since $[K : K_s]$ is purely inseparable according to Proposition 2.34, then $q = [K : K_s] = p^m$ where $m > 1$ from the Fact 2.33. Hence $p|q$. □

Corollary 4.8. *Let K/F be a finite Galois extension. Then $\mathrm{Tr}_{K/F}$ and $\mathrm{N}_{K/F}$ are compatible with $\tau \in \mathrm{Gal}(K/F)$ which means*

$$\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}_{K/F}(\tau(\alpha)), \quad \mathrm{N}_{K/F}\alpha) = \mathrm{N}_{K/F}(\tau(\alpha))$$

Proof. It's immediate from the Proposition 4.6. □

Example 4.9. For $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ and $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ are surjective.

Proof. Any finite extension of finite fields is separable $\Rightarrow \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is surjective.

$\mathbb{F}_{q^n}^\times$ is a cyclic group and we suppose x is the generator. Then x has order q^n-1. Then from the formula of Proposition 4.6

$$\begin{aligned} \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) &= \prod_{\sigma\in \mathrm{Gal}((\mathbb{F}_{q^n}/\mathbb{F}_q)} \sigma(x) \\ &= x\cdot x^q \cdot x^{q^2}\cdot \ldots \cdot x^{q^{n-1}} \\ &= x^{\frac{q^n-1}{q-1}} = a \in \mathbb{F}_q^\times \end{aligned} \tag{22}$$

where $\mathrm{Frob} : u \mapsto u^q$ is the generator of $\mathrm{Gal}((\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. a has order $q-1$ hence generating the cyclic group $\mathbb{F}_q^\times$. Then since $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is multiplicative, $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is surjective. □

Remark 4.10. The Theorem of Hilbert 90 is that if K/F is a finite cyclic Galois extension and $\sigma \in \mathrm{Gal}(K/F)$ is the generator then the following conditions are equivalent

(1) $\mathrm{N}_{K/F}(\alpha) = 1$.

(2) There is some $\beta \in K^\times$ such that $\alpha = \frac{\sigma(\beta)}{\beta}$.

In the Example 4.9, we assume $\alpha = x^k$ for some integer k. $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)^k = a^k = 1$. Then $q-1|k$ Let $k=(q-1)r \Rightarrow \alpha = x^{(q-1)r} = \frac{(x^r)^q}{x^r} = \frac{\mathrm{Frob}(x^r)}{x^r}$.

Exercise 4.11. Let $F = \mathbb{Q}(\xi)$ where $\xi = \xi_9$ is the primitive 9-th root of unity 1 in $\mathbb{C}$. Compute $\mathrm{N}_{F/\mathbb{Q}}(x$ and $\mathrm{Tr}_{F/\mathbb{Q}}(x)$ for the following x.

- $x = \xi^2 + \xi^6$.
- $x = \xi + \xi^4 + \xi^7$.

4.2 Galois Cohomology

In this section we first sketch some motivations for group cohomology with partial proofs omitted and all details can be found in [Rot09] Chapter 9. But this will not affect reading since proofs of theorems concerning Galois cohomology are complete.

Assume R is a ring with unit 1 not necessarily being commutative. Given a short exact sequence of left R-modules (If not specified, all modules are left modules.)

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

which is called an **extension** of A by C, another extension of A by C is isomorphic to it if there is a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, equal] & B \arrow[r] \arrow[d, dotted] & C \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & A \arrow[r] & E \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

According to the five lemma, $B \to E$ is forced to be an isomorphism. In homological algebra, the set of isomorphism classes of extensions of A by C is computed as $\mathrm{Ext}^1_R(C, A)$, where Ext_R is the derived functor of Hom_R. If we consider extensions of groups or give a short exact sequence of groups

$$1 \longrightarrow A \xrightarrow{i} H \xrightarrow{p} G \longrightarrow 1$$

there are similar theorems. For simplicity we always assume A is an abelian group. We explain why we make this assumption. For any $h \in H$, h defines an inner automorphism on H by $x \mapsto hxh^{-1}$ for $x \in H$. But $A \trianglelefteq H$ is a normal subgroup. Hence the restriction of this inner automorphism on A is still an automorphism. Then there is a map $H \to \mathrm{Inn}(H) \to \mathrm{Aut}(A)$. This deduces the following diagram

$$\begin{tikzcd}
1 & & 1 \\
G \arrow[u] \arrow[rr, dotted, "\exists!"] & & \mathrm{Out}(A) \arrow[u] \\
H \arrow[u, "p"] \arrow[r] & \mathrm{Inn}(H) \arrow[r] & \mathrm{Aut}(A) \arrow[u] \\
A \arrow[u, "i"] \arrow[rr] & & \mathrm{Inn}(A) \arrow[u] \\
1 \arrow[u] & & 1 \arrow[u]
\end{tikzcd} \tag{23}$$

If A is abelian, then $\mathrm{Inn}(A) = id, \mathrm{Out}(A) = \mathrm{Aut}(A)$ and any element $g \in G$ defines an automorphism of A such that $a \mapsto hah^{-1}$ where $g = p(h)$.

Definition 4.12. *For any group G, $\mathbb{Z}[G]$ is the free abelian group generated by the underlying set of G which is called the* ***group ring*** *of G.*

$$\mathbb{Z}[G] := \{\sum_{g \in G} n_g \cdot g | n_g \in \mathbb{Z},\ n_g\text{'s are almost all zero}\}$$

$\mathbb{Z}[G]$ is actually a ring whose multiplication is defined to be

$$(\sum_{g \in G} n_g \cdot g)(\sum_{h \in G} m_h \cdot h) = \sum_{k \in G} l_k \cdot k, \quad \text{where } l_k = \sum_{gh=k} n_g m_h$$

Fact 4.13.

(1) The group ring $\mathbb{Z}[G]$ is characterized by the universal property such that given any ring R

$$\mathrm{Hom}_{\mathrm{Rings}}(\mathbb{Z}[G], R) \cong \mathrm{Hom}_{\mathrm{Groups}}(G, R^{\times})$$

The funtor $\mathbb{Z}[-]$ is left adjoint to the unit functor Rings → Groups, $R \mapsto R^{\times}$.

(2) An abelian group A is a $\mathbb{Z}[G]$-module iff there is a ring morphism $\mathbb{Z}[G] \to \mathrm{End}(A)$ iff there is a group morphism $G \to \mathrm{End}(A)^{\times} = \mathrm{Aut}(A)$. Such module structure is trivial if $G \to \mathrm{Aut}(A)$ is trivial. Therefore for any short exact sequence

$$0 \longrightarrow A \xrightarrow{i} H \xrightarrow{p} G \longrightarrow 1$$

A has a natural $\mathbb{Z}[G]$-module structure. We say such sequence *realizes* (A, θ) where $\theta : G \to \mathrm{Aut}(A)$.

The set of isomorphism classes of short exact sequences realizing (A, θ) is denoted by $\mathcal{E}_{\theta}(G, A)$ which can be computed by Group cohomology. In the short exact sequence above, since p is surjective, there will exist a *lifting* $\iota : G \to H$ such that $p \circ \iota = id_G$ where ι may not be a group morphism. We can define a function

$$f : G \times G \to H,\ (x, y) \mapsto \iota(x)\iota(y)\iota(xy)^{-1}$$

Since $p(\iota(x)\iota(y)\iota(xy)^{-1}) = xy(xy)^{-1}$, $\mathrm{im} f \subseteq A$. Therefore we write $f(x, y)$ as $\iota(x) + \iota(y) - \iota(xy)$. Such function is called a **cocycle** and it satisfies the following **cocycle identity**

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0$$

with the $\mathbb{Z}[G]$-module structure $\theta : G \to \mathrm{Aut}(A)$ such that $x \cdot a = \iota(x) + a - \iota(x)$. Conversely given (A, θ) and a function $f : G \times G \to A$ satisfying cocycle identity we could construct a short exact sequence realizing (A, θ) and f has the form $f(x, y) = \iota(x) + \iota(y) - \iota(xy)$. Moreover f and f' correspond with isomorphic sequences iff there is a function $h : G \to A$ such that

$$f(x, y) - f'(x, y) = xh(y) - h(xy) + h(x)$$

A function $g : G \times G \to A$ is called a **coboundary** if there is some function $h : G \to A$ such that

$$g(x, y) = xh(y) - h(xy) + h(x)$$

Definition 4.14. *For a $\mathbb{Z}[G]$-module A the set of cocycles and coboundaries are denoted by $Z^2(G, A)$ and $B^2(G, A)$ respectively.*

Remark 4.15. $Z^2(G, A)$ is an abelian group with addition pointwise and $B^2(G, A)$ is a subgroup of $Z^2(G, A)$.

Proof. The cocyle condition of $f+f'$ can be easily checked. We assume g is coboundary. Then

$$\begin{aligned}
&xg(y,z)-g(xy,z)+g(x,yz)-g(x,y)\\
=&x\big(yh(z)-h(yz)+h(y)\big)-\big(xyh(z)-h(xyz)+h(xy)\big)\\
&+\big(xh(yz)-h(xyz)+h(x)\big)-\big(xh(y)-h(xy)+h(x)\big)\\
=&0
\end{aligned}$$

Hence $B^2(G,A)\subseteq Z^2(G,A)$. □

The **second cohomology group** is defined to be $H^2(G,A)=Z^2(G,A)/B^2(G,A)$. Then we will have $\mathcal{E}_\theta(G,A)\cong H^2(G,A)$. This is the concrete interpretation of second group cohomology. In general there is a complex

$$0\longrightarrow C^0(G,A)\xrightarrow{d^0}C^1(G,A)\longrightarrow ...\longrightarrow C^n(G,A)\xrightarrow{d^n}C^{n+1}(G,A)\longrightarrow ... \tag{24}$$

where $C^n(G,A)=\mathrm{Map}(G^n,A)$ all maps from G^n to A in the sense of sets and $G^n=G\times ...\times G$ is the n's products of G. Moreover

$$\begin{aligned}
d^n(f)(x_1,...,x_{n+1})=&x_1f(x_2,...,x_{n+1})\\
&+\sum_{i=1}^{n}(-1)^if(x_1,...,x_ix_{i+1},...,x_{n+1})\\
&+(-1)^{n+1}f(x_1,...,x_n)
\end{aligned}\tag{25}$$

Note $G^0=\{*\}$ is the one point set and then $C^0(G,A)=A$. Viewing A as Map($\{*\}$, A), we see $d^0(f_a)(x)=xf_a(*)-f_a(*)=xa-a$. Then $d^0(a):x\mapsto xa-a$.

Fact 4.16. $d^n\circ d^{n-1}=0$

Proof.

$$
\begin{aligned}
&d^n(d^{n-1}(f))(x_1, ..., x_{n+1})\\
=&x_1 d^{n-1}(f)(x_2, ..., x_{n+1}) + \sum_{i=1}^{n}(-1)^i d^{n-1}(f)(x_1, ..., x_i x_{i+1}, ..., x_{n+1}) + (-1)^{n+1} d^{n-1}(f)(x_1, ..., x_n)\\
=&\Big(x_1 x_2 f(x_3, ..., x_{n+1}) + x_1 \sum_{i=2}^{n}(-1)^{i-1} f(x_2, ..., x_i x_{i+1}, ..., x_{n+1}) + x_1(-1)^n f(x_2, ..., x_n)\Big)\\
&+ \Big(- x_1 x_2 f(x_3, ..., x_{n+1}) + f(x_1 x_2 x_3, ..., x_{n+1}) + \sum_{i=3}^{n}(-1)^i f(x_1 x_2, ..., x_i x_{i+1}, ..., x_{n+1})\\
&+ (-1)^{n+1} f(x_1 x_2, ..., x_n)\Big) + \Big(\sum_{i=2}^{n}(-1)^i x_1 f(x_2, ..., x_i x_{i+1}, ..., x_{n+1})\\
&+ \sum_{i=3}^{n}(-1)^i \sum_{j=1}^{i-2}(-1)^j f(..., x_j x_{j+1}, ..., x_i x_{i+1}, ..., x_{n+1})\\
&+ \sum_{i=2}^{n}(-1)^i \sum_{j=i+2}^{n}(-1)^{j-1} f(..., x_i x_{i+1}, ..., x_j x_{j+1}, ..., x_{n+1})\\
&+ \sum_{i=2}^{n}(-1)^i(-1)^{i-1} f(..., x_{i-1} x_i x_{i+1}, ...) + \sum_{i=2}^{n-1}(-1)^i(-1)^i f(..., x_i x_{i+1} x_{i+2}, ...)\\
&+ \sum_{i=2}^{n-1}(-1)^i(-1)^n f(x_1, ..., x_i x_{i+1}, ..., x_n) + (-1)^n(-1)^n f(x_1, ..., x_{n-1})\Big)\\
&+ \Big((-1)^{n+1} x_1 f(x_2, .., x_n) + (-1)^{n+1} \sum_{i=1}^{n-1}(-1)^i f(x_1, ..., x_i x_{i+1}, ..., x_n)\\
&+ (-1)^{n+1}(-1)^n f(x_1, ..., x_{n-1})\Big)\\
=&0
\end{aligned}
$$

□

The n-th cohomology group is defined to be $H^n(G, A) = \mathrm{ker} d^n / \mathrm{im} d^{n-1}$. Especially $H^0 = \mathrm{ker} d^0$. For $a \in A$

$$
\begin{aligned}
d^0(a) = 0 &\Leftrightarrow d^0(f_a)(x) = 0, \forall x \in G\\
&\Leftrightarrow xa = a,\ \forall x \in G\\
&\Leftrightarrow a \in A^G
\end{aligned}
\tag{26}
$$

Then $H^0(G, A) = A^G := \{a \in A | x \cdot a = a, \ \forall x \in G\}$.

For $n = 1$, $f \in \text{ker} d^1$ iff $d^1(f)(x, y) = 0$ for all $x, y \in G$.

$$xf(y) - f(xy) + f(x) = 0 \Leftrightarrow f(xy) = f(x) + xf(y)$$

Such map (1-cocyle) $f : G \to A$ is called a *crossed homomorphism*. Especially when (A, θ) is trivial, $f(xy) = f(x) + f(y)$.

There is also another definition of group cohomology using the concept of derived functors, which is equivalent to that we talk about above. We consider the left exact functor $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ where $\mathbb{Z}$ has the trivial $\mathbb{Z}[G]$-module structure. Then any $\mathbb{Z}[G]$-morphism $f : \mathbb{Z} \to A$ is totally determined by $a = f(1)$. But

$$f \in \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \Leftrightarrow \forall x \in G, \ a = f(1) = f(x \cdot 1) = x \cdot f(1) = x \cdot a$$

Hence

$$\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \cong A^G$$

This motivates us to define the group cohomology as

$$H^n(G, A) := \text{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

Dually there is a concept of group homology as well.

$$H_n(G, A) := \text{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

In fact the two definitions of group cohomology are equivalent. Consider a special free resolution of $\mathbb{Z}$, which is called the **bar resolution**

$$... \xrightarrow{\partial_n} B_n \xrightarrow{\partial_{n-1}} ... \xrightarrow{\partial_0} B_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

where B_n is the free $\mathbb{Z}[G]$-module with basis the underlying set G^n. The single generator of B_0 is denoted by $[\ ]$ and B_n with $n \geq 1$ has basis $[x_1|x_2|...|x_n]$ where $x_i \in G$. Note $x[x_1|x_2|...|x_n] \neq [xx_1|xx_2|...|xx_n]$. Then we can describe ∂_n concretely.

$$\begin{aligned}\partial_{n+1}([x_1|...|x_{n+1}]) =& x_1[x_2|...|x_{n+1}] \\ &+ \sum_{i=1}^{n} (-1)^i [x_1|...|x_i x_{i+1}|...|x_{n+1}] \\ &+ (-1)^{n+1}[x_1|...|x_n]\end{aligned}$$

Especially if $n = 0$, $\partial_0([x]) = x[\ ] - [\ ]$ and $\epsilon([\ ]) = 1$. Take the left exact functor $\text{Hom}_{\mathbb{Z}}[G](-, A)$ to the bar resolution. We obtain the following complex

$$0 \longrightarrow \text{Hom}_{\mathbb{Z}[G]}(B_0, A) \xrightarrow{\partial_0^*} ... \xrightarrow{\partial_{n-1}^*} \text{Hom}_{\mathbb{Z}[G]}(B_n, A) \xrightarrow{\partial_n^*} ...$$

Since B_n is a free $\mathbb{Z}[G]$-module with basis described above

$$\mathrm{Hom}_{\mathbb{Z}[G]}(B_n, A) \cong \mathrm{Map}(G^n, A)$$

and such complex is equivalent to that we have defined before in equation (24).

Fact 4.17. Note that it's tedious to prove the bar resolution is actually a free resolution of $\mathbb{Z}$. Of course the most tedious part is to check $\partial_{n-1}\partial_n = 0$ which is the same as the Fact 4.16. Hence in the following we just prove the complex (bar resolution) has trivial homology groups.

Proof. We reduce the bar resolution to a complex of abelian groups and prove the identity map of this complex is chain homotopic to the zero map. Note reducing $\mathbb{Z}[G]$-modules to abelian groups will not affect homology groups.

$$\begin{aligned} s_{-1} &: \mathbb{Z} \to B_0,\ 1 \mapsto [\ ] \\ s_n &: B_n \to B_{n+1},\ x \cdot [x_1|...|x_n] \mapsto [x|x_1|...|x_n] \end{aligned}$$

Then we see $\epsilon \circ s_{-1} = id_{\mathbb{Z}}$. $(\partial_0 s_0 + s_{-1}\epsilon)(x \cdot [\ ]) = \partial_0([x]) + s_{-1}(1) = x[\ ] - [\ ] + [\ ] = x[\ ]$. Hence $\partial_0 s_0 + s_{-1}\epsilon = id_{B_0}$.

$$\begin{aligned} &(\partial_n s_n + s_{n-1}\partial_{n-1})(x \cdot [x_1|...|x_n]) \\ =&\partial_n([x|x_1|...|x_n]) + s_{n-1}\Big(x \cdot \big(x_1[x_2|...|x_n] + \sum_{i=1}^{n-1}(-1)^i[x_1|...|x_i x_{i+1}|...|x_n] + (-1)^n[x_1|...|x_{n-1}]\big)\Big) \\ =&\Big(x[x_1|...|x_n] + \sum_{i=1}^{n}(-1)^i[x|...|x_{i-1}x_i|...|x_n] + (-1)^{n+1}[x|x_1|...|x_{n-1}]\Big) \\ &+ \Big([xx_1|x_2|...|x_n] + \sum_{i=1}^{n-1}(-1)^i[x|x_1|...|x_i x_{i+1}|...|x_n] + (-1)^n[x|x_1|...|x_{n-1}]\Big) \\ =&x[x_1|...|x_n] \end{aligned}$$

Therefore $\partial_n s_n + s_{n-1}\partial_{n-1} = id_{B_n}$. □

Now let's talk about Galois cohomology which is just the group cohomology of Galois group. The most important theorem in this section is Hilbert 90 that we have introduced before in Remark 4.10. We now state it from the viewpoint of Galois cohomology.

Theorem 4.18 (Hilbert 90)**.** *If (K/F) is a finite Galois extension, then*

$$\begin{aligned} &H^1(\mathrm{Gal}(K/F), K^\times) = 0, \quad \textit{(multiplicative form)} \\ &H^1(\mathrm{Gal}(K/F), K) = 0, \quad \textit{(additive form)} \end{aligned}$$

Proof. Note there is a natural embedding $G = \mathrm{Gal}(K/F) \hookrightarrow \mathrm{Aut}(K)$. Then K is a $\mathbb{Z}[G]$-module. So is $K^\times$. We prove the multiplicative form first.

Let $f : G \to K^\times$ be a 1-cocycle, which means $f(\sigma\tau) = f(\sigma) \cdot (\sigma f(\tau))$. For any $\tau \in G$, $f(\tau) \neq 0$. From the Lemma 3.7, we see $\sum_{\tau\in G} f(\tau)\tau$ is not all zero. Then there is a element $a \in K^\times$ such that

$$\beta = \sum_{\tau\in G} f(\tau)\tau(a) \neq 0$$

therefore

$$\begin{aligned}\sigma(\beta) &= \sum_{\tau\in G} \sigma\big(f(\tau)\tau(a)\big)\\ &= \sum_{\tau\in G} \sigma\big(f(\tau)\big)\sigma\tau(a)\\ &= \sum_{\tau\in G} f(\sigma\tau)f(\sigma)^{-1}\sigma\tau(a)\\ &= \beta f(\sigma)^{-1} \qquad (27)\end{aligned}$$

Then $\forall\sigma \in G,\ f(\sigma) = \beta\sigma(\beta)^{-1}$. Let $x = \beta^{-1}$. It follows that $f(\sigma) = \sigma(x)x^{-1}$. Then f is a 1-coboundary.

Next we consider the additive form. Assume $f : G \to K$ is a 1-cocycle, which means $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$. If f is always zero, it's obvious to see it's a 1-coboundary. We suppose there is some $\gamma \in G$ such that $f(\gamma) \neq 0$. Then the β defined above is still non-zero. We choose another element $b \in K^\times$ with $\mathrm{Tr}_{K/F}(b) \neq 0$. Such element exists since K/F is Galois hence separable and from the Corollary 4.7 $\mathrm{Tr}_{K/F}$ is non-zero.

Then consider the element $c = a + b$. Let $\mu = \sum_{\tau\in G} f(\tau)\tau$. If $\mu(a + b) = 0$ then $\mu(b) = -\mu(a) \neq 0$. Then we replace β by $\mu(b)$. If $\mathrm{Tr}_{K/F}(a + b) = 0$ then $\mathrm{Tr}_{K/F}(a) \neq 0$. If $\mu(a + b) \neq 0$ and $\mathrm{Tr}_{K/F}(a + b) \neq$, we replace β by $\mu(a + b)$. The analysis above implies there is some $a \in K^\times$, $\mu(a) \neq 0$ and $\mathrm{Tr}_{K/F}(a) \neq 0$. We let

$\beta = \mu(a)$. Hence

$$\begin{aligned}\sigma(\beta) &= \sum_{\tau \in G} \sigma\big(f(\tau)\tau(a)\big) \\ &= \sum_{\tau \in G} \sigma\big(f(\tau)\big)\sigma\tau(a) \\ &= \sum_{\tau \in G} \big(f(\sigma\tau) - f(\sigma)\big)\sigma\tau(a) \\ &= \beta - f(\sigma)\sum_{\tau \in G} \sigma\tau(a) \\ &= \beta - f(\sigma)\mathrm{Tr}_{K/F}(a) \qquad (28)\end{aligned}$$

Then $f(\sigma) = \big(\beta - \sigma(\beta)\big)\mathrm{Tr}_{K/F}(a)^{-1}$. Suppose $x = -\frac{\beta}{\mathrm{Tr}_{K/F}(a)}$. $f(\sigma) = \sigma(x) - x$, which means f is a 1-coboundary.

□

The Hilbert 90 in Remark 4.10 is classical and next we apply the Hilbert 90 above to obtain classical one. But before that let's consider the 1-cocycle of cyclic group of order n. Assume G is a cyclic group of order n and $f : G \to A$ is a 1-cocyle. Then $f(xy) = f(x) + xf(y)$. If $x = y = 1$ then $f(1) = f(1) + f(1) \Rightarrow f(1) = 0$. If $x = y$, then $f(x^2) = (1 + x)f(x)$. $f(x^3) = (1 + x + x^2)f(x)$. In general

$$f(x^k) = (1 + x + ... + x^{k-1})f(x)$$

If $G = \langle x \rangle$, then f is totally determined by its value on x and

$$0 = f(1) = f(x^n) = (1 + x + ... + x^{n-1})f(x)$$

Conversely assume $a \in A$ such that $(1+x+...+x^{n-1})\cdot a = 0$. Then $f : G \to A$, $x \mapsto a$ defines a 1-cocycle.

Theorem 4.19 (Hilbert 90)**.** *Let K/F be a finite cyclic Galois extension of dimension n. $G = \mathrm{Gal}(K/F) = \langle \sigma \rangle$.*

(1) If $\alpha \in K^\times$ with $\mathrm{N}_{K/F}(\alpha) = 1$, then there is some $\beta \in K^\times$ such that $\alpha = \frac{\sigma(\beta)}{\beta}$.

(2) If $\alpha \in K$ with $\mathrm{Tr}_{K/F}(\alpha) = 0$, then there is some $\beta \in K$ such that $\alpha = \sigma(\beta) - \beta$.

Proof. (1).We can prove this via the same process of (2) only replacing addition by multiplication. But here we give a more intuitive proof.

We want to find $\beta \in K^\times$ such that $\alpha = \frac{\sigma(\beta)}{\beta} \Leftrightarrow \beta = \alpha^{-1}\sigma(\beta)$. Assume $L = \alpha^{-1}\sigma : K \to K$. Then it's equivalent to find an eigenvector with eigenvalue 1. The construction is the same as in Lemma 3.52. $L \circ ... \circ L = L^n = id$, since

$$L^k(x) = \alpha^{-1}\sigma(\alpha^{-1})...\sigma^{k-1}(\alpha^{-1})\sigma^k(x)$$

$L^n(x) = \mathrm{N}_{K/F}(\alpha^{-1})x = x$. For any $x \in K$, $\beta = x + Lx + ... + L^{n-1}x \Rightarrow L\beta = Lx + L^2x + ... + L^nx = \beta$. On the other hand $1 + L + ... + L^{n-1} = 1 + \alpha^{-1}\sigma + ... + \alpha^{-n+1}\sigma^{n-1}$. From the Lemma 3.7 it's not always zero. Hence there exists some $x \in K^\times$ such that $\beta \neq 0$.

(2). $0 = \mathrm{Tr}_{K/F}(\alpha) = \sum_{\tau \in G}(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\alpha) = (1 + \sigma + ... + \sigma^{n-1})\alpha$. Then

$$f : G \to K,\ \sigma^k \mapsto (1 + \sigma + ... + \sigma^{k-1})\alpha$$

defines a 1-cocyle. Since $H^1(G, K) = 0$, f is a 1-coboundary as well and there is an element $\beta \in K$, $f(\sigma^k) = \sigma^k(\beta) - \beta$. Especially $\alpha = f(\sigma) = \sigma(\beta) - \beta$.

□

Remark 4.20. There is an application of Hilbert 90. Let $a, b \in \mathbb{Q}$ satisfying $a^2 + b^2 = 1$. Then $\exists\ c, d \in \mathbb{Q}$ shch that

$$(a, b) = (\frac{c^2 - d^2}{c^2 + d^2}, \frac{-2cd}{c^2 + d^2})$$

Proof. Consider $\mathbb{Q}(i)/\mathbb{Q}$ where $i^2 = -1$. This is a finite cyclic Galois extension and the generator of Galois group is the conjugate map. Since $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = a^2+b^2 = 1$. Then there is some $c + di \in \mathbb{Q}(i)^\times$ such that

$$a + bi = \frac{c - di}{c + di} = \frac{(c - di)^2}{c^2 + d^2}$$

□

There are two generalizations of Hilbert 90. What's the higher Galois cohomology? What's the Galois cohomology for infinite Galois extensions? We will focus on the two themes in the following.

First we still assume K/F is a finite Galois extension and we want to compute $H^n(\mathrm{Gal}(K/F), K)$ and $H^n(\mathrm{Gal}(K/F), K^\times)$ for higher n. But the two cases are different.

Theorem 4.21. *For a finite Galois extension K/F, $H^n(\mathrm{Gal}(K/F), K) = 0$, $\forall n \geq 1$.*

To prove this we need more techniques. For arbitrary group G we consider its subgroup $H \leq G$. Then $\mathbb{Z}[H] \hookrightarrow \mathbb{Z}[G]$. Given a $\mathbb{Z}[G]$-module A, the **induced module** is defined to be $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$ and the **coinduced module** is defined to be $\mathrm{Hom}_{\mathbb{Z}[H]}(Z[G], A)$. They are denoted by $\mathrm{Ind}_H^G A$ and $\mathrm{Coind}_H^G A$ respectively.

For a ring R, a left module is denoted by ${}_RA$ and right module is denoted by A_R. Then we have the following obvious fact.

Fact 4.22. Let R and S be rings. Then

(1) Given ${}_RA_S$ and ${}_RB$, $\mathrm{Hom}_R(A,B)$ is a left S-module where $(a)(sf)=(as)f$.

(2) Given ${}_RA_S$ and B_S, $\mathrm{Hom}_S(A,B)$ is a right R-module where $(fr)(a)=f(ra)$.

(3) Given A_R and ${}_SB_R$, $\mathrm{Hom}_R(A,B)$ is a left S-module where $(sf)(a)=s(f(a))$.

(4) Given ${}_SA$ and ${}_SB_R$, $\mathrm{Hom}_S(A,B)$ is a right R-module where $(a)(fr)=((a)f)r$.

Given a ring morphism $R\to S$. Then any S-module A has a natural R-module structure. For ${}_RS_S$ and ${}_RA$, $\mathrm{Hom}_R(S,A)$ is a left S-module. Hence the coinduced module $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A)$ is a left $\mathbb{Z}[G]$-module as well.

Moreover there is an adjoint isomorphism for modules $A_R, {}_RB_S, C_S$

$$\mathrm{Hom}_S(A\otimes_R B, C)\cong \mathrm{Hom}_R(A,\mathrm{Hom}_S(B,C))$$

And it's also interesting to see for a group ring $\mathbb{Z}[G]$ on it left modules are equivalent to right modules, since for any left module A we could define $a\cdot g=g^{-1}a$, and then it will have a right module structure.

Proposition 4.23 (Shapiro)**.** *Let G be a group and $H\le G$ is a subgroup. Assume A is a $\mathbb{Z}[G]$-module. Then*

(1) $H^n(H,A)\cong H^n(G,\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A))$

(2) $H_n(H,A)\cong H_n(G,\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} A)$

Proof. There are two proofs. We give a proof in the sense of homological algebra here.

(1). Given a free resolution of trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$ (such as bar resolution)

$$\longrightarrow P_1\longrightarrow P_0\longrightarrow \mathbb{Z}\longrightarrow 0$$

take the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(-,\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A))$ to it. Then

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}[G]}(P_n,\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A)) &\cong \mathrm{Hom}_{\mathbb{Z}[H]}(P_n\otimes_{\mathbb{Z}[G]}\mathbb{Z}[G],A)\\ &\cong \mathrm{Hom}_{\mathbb{Z}[H]}(P_n,A) \qquad (29)\end{aligned}$$

Next we should prove the restriction of P_n on $\mathbb{Z}[H]$ also forms a free resolution of the trivial $\mathbb{Z}[H]$-module $\mathbb{Z}$. It's not difficult. From the coset decomposition of H in G, we see $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module. Then it's obvious that every free $\mathbb{Z}[G]$-module is a free $\mathbb{Z}[H]$-module as well. Hence

$$\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z},\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A))\cong \mathrm{Ext}^n_{\mathbb{Z}[H]}(\mathbb{Z},A)$$

(2). It's similar to the proof of (1).

$$P_n\otimes_{\mathbb{Z}[G]}\big(\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]}A\big)\cong P_n\otimes_{\mathbb{Z}[H]}A$$

Then

$$\mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z},\mathbb{Z}[G]\otimes_{\mathbb{Z}[H]}A)\cong \mathrm{Tor}_n^{\mathbb{Z}[H]}(\mathbb{Z},A)$$

□

Remark 4.24. We can also prove $H^n(H,A) \cong H^n(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A))$ directly but it's much more complicated. We construct a map

$$\varphi : H^n(G, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A)) \to H^n(H,A)$$

For any n-cycle $f : G^n \to \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A)$,

$$\varphi(f) : H^n \longrightarrow G^n \xrightarrow{f} \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A) \xrightarrow{\pi} A$$

where $\pi(u) = u(1)$. There are many things should be checked. $\varphi(f)$ is an n-cycle. If f is an n-coboundary then $\varphi(f)$ is an n-coboundary as well. This proves φ is well defined. Then you should prove φ is an isomorphism. To prove this you should construct its inverse and prove it's well defined. Note the inverse is difficult to construct.

Exercise 4.25. Using the Remark 4.24 to prove the case of $n = 1$. Prove φ is well defined and construct its inverse.

Theorem 4.26 (Normal Basis)**.** *Let K/F be a finite Galois extension. Then there is a nomal basis over K/F i.e. an element $\alpha \in K^\times$ such that $\{\tau(\alpha)|\tau \in \mathrm{Gal}(K/F)$ form a basis of K/F.*

Proof. See [Lan02] Chapter VI Section 13 or `https://en.wikipedia.iwiki.eu.org/wiki/Normal_basis`. □

Corollary 4.27. *Assume K/F is a finite Galois extension. Then there is an isomorphism of $\mathbb{Z}[G]$-modules where $G = \mathrm{Gal}(K/F)$*

$$(K,+) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],F)$$

Note F is a trivial $\mathbb{Z}[G]$-module and $\mathbb{Z} \cong \mathbb{Z}[\{1\}]$.

Proof. Assume $\{G = \{\tau_1, ..., \tau_n\}$. From the Normal Baiss Theorem there is an element $\alpha \in K^\times$ such that $\{\tau_i(\alpha)|\tau_i \in G\}$ form a basis of K/F. Since $\mathbb{Z}[G]$ is the free abelian group with basis the underlying set of G, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],F) \cong F^n$ is an F-space of dimension n. We define

$$u_{\tau_i} : \mathbb{Z}[G] \to F,\ u_{\tau_i}(\tau_i) = \alpha,\ u_{\tau_i}(\tau_j) = 0, \text{ if } \ i \neq j$$

Then u_{τ_i}'s form a basis of the F-vector space $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],F)$. The left $\mathbb{Z}[G]$-module structure on it is that $(\tau \cdot u_{\tau_i})(\tau_j) = u_{\tau_i}(\tau_j \cdot \tau)$. Define the F-linear isomorphism

$$\tau_i(\alpha) \longmapsto u_{\tau_i^{-1}}$$

To prove it's an isomorphism of $\mathbb{Z}[G]$-modules, it's enough to prove $\tau \cdot (\tau_i(\alpha)) \mapsto \tau \cdot u_{\tau_i^{-1}}$, which is equivalent to say $u_{(\tau\tau_i)^{-1}} = \tau \cdot u_{\tau_i^{-1}}$. But $u_{(\tau\tau_i)^{-1}}(\tau_j) = 1$ iff

$\tau_j = (\tau\tau_i)^{-1}$ iff $\tau_j = \tau_i^{-1}\tau^{-1}$ iff $\tau_j\tau = \tau_i^{-1}$ and $\big(\tau \cdot u_{\tau_i^{-1}}\big)(\tau_j) = u_{\tau_i^{-1}}(\tau_j \cdot \tau) = 1$ iff $\tau_j\tau = \tau_i^{-1}$.

Next we prove τ respects the product of scalar $a \in F$ and that's why such map above defines a $\mathbb{Z}[G]$-module isomorphism.

$$\begin{aligned}\tau \cdot (a\tau_i(\alpha)) &= \tau(a)\tau\tau_i(\alpha) = a\tau\tau_i(\alpha)\\ \tau(au_{\tau_i})(\tau_j) &= au_{\tau_i}(\tau_j\tau) = a(\tau \cdot u_{\tau_i})(\tau_j)\end{aligned}$$

□

Proof of Theorem 4.21.

$$\begin{aligned}H^n(G,K) &\cong H^n(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],F)),\ \text{(Corollary 4.27)}\\ &\cong H^n(\{1\},F),\ \text{(Proposition 4.23)}\\ &\cong \mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z},F)\\ &\cong 0,\ \text{for } n \geq 1, \text{ since } \mathbb{Z} \text{ is free}\end{aligned}$$

□

Remark 4.28. In general $H^2(\mathrm{Gal}(K/F), K^\times) \neq 0$. For any field F the **Brauer group** of it is defined to be $H^2(\mathrm{Gal}(F_{sep}/F), F_{sep}^\times)$ where F_{sep} is the separable closure of F. The Brauer group is denoted by $\mathrm{Br}(F)$. There is another interpretation of Brauer groups.

A *central simple algebra* (CSA) over F is a finite-dimensional associative F-algebra A with center F having no non-trivial two-sided ideals. And any CSA over F is isomorphic to some matrix ring $M_n(D)$ where D is a division F-algebra with center F. And we can define an equivalence relation on CSAs over F. Given any two CSAs, $A \cong M_n(S)$ and $B \cong M_m(T)$, we say A and B are *similar* or *Brauer equivalent* if division rings $S \cong T$. Then there is a bijection

$$\mathrm{Br}(F) \longleftrightarrow \text{the set of equivalence classes of CSAs over } F$$

Now we suppose $F = \mathbb{R}$ and $K = \mathbb{C}$. Then K is the separable closure of F. We want to prove $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \neq 0$, which is equivalent to find a nontrivial CSA over $\mathbb{R}$. A trivial one is $M_2(\mathbb{R})$ whose center actaully consists of

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$$

where $r \in \mathbb{R}$. A nontrivial CSA over $\mathbb{R}$ is the *Hamilton quaternions* $\mathbb{H}$, which is defined to be

$$\mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

where

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j$$

$\mathbb{H}$ is itself a division ring which means $\mathbb{H} \cong M_1(\mathbb{H})$. A theorem of Frobenius states that the only finite dimensional division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$. But $\mathbb{C}$ is not central. Hence in $\mathrm{Br}(\mathbb{R})$ there are only two elements. Then $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$

Finally we consider Galois cohomology for infinite extensions, which is also called *continuous cohomology*. In the following we always assume G is a profinite group and let A be a discrete abelian group.

Definition 4.29. *A discrete $\mathbb{Z}[G]$-module is a discrete abelian group A with the action*

$$G \times A \to A,\ (g, a) \mapsto g \cdot g \cdot a$$

continuous, which is equivalent to that for any fixed $a \in A$ its stabilizer in G is open.

Example 4.30. Assume K/F is a Galois extension not necessarily finite. Then $\mathrm{Gal}(K/F)$ acts continuously on K and $K^\times$. For $\tau \in \mathrm{Gal}(K/F)$ and $u \in K$, $\tau(u) = u$ iff $\tau \in \mathrm{Gal}(K/F(u))$. Since $F(u)/F$ is a finite field extension, from the Remark 3.85 (4), $\mathrm{Gal}(K/F(u))$ is open.

To define continuous cohomology, we define a new complex first.

$$0 \longrightarrow C^0_{cont}(G, A) \xrightarrow{d^0} C^1_{cont}(G, A) \longrightarrow ... \longrightarrow C^n_{cont}(G, A) \xrightarrow{d^n} C^{n+1}_{cont}(G, A) \longrightarrow ... \tag{30}$$

where $C^n_{cont}(G, A) = \mathrm{Map}_{\mathrm{Top}}(G^n, A)$ consists of continuous maps from G^n to A and d^n is defined as before. Since A is discrete, continuous maps from G^n to A are locally constant. The n-th continuous cohomology is defined to be $H^n_{cont}(G, A) = \mathrm{ker} d^n / \mathrm{im} d^n$.

Proposition 4.31. *Assume $G = \varprojlim G_i$ is a profinite group where I is a directed set and $A = \varinjlim A_i$ where A_i's are discrete G_i-modules. Then*

$$C^n_{cont}(G, A) \cong \varinjlim C^n(G_i, A_i)$$

Proof. There is an obvious G-module structure on A. For $(g_i)_i \in G$ and $a \in A$, there is some $j \in I$ such that $a_j \in A_j$ which is the preimage of a. Then define $(g_i)_i \cdot a = g_j a_j$. More precisely it's the image of $g_j a_j$ in A. It's easy to prove it's well defined since I is a directed set.

Since G_i's and A_i's are discrete $C^n_{cont}(G_i, A_i) = C^n(G_i, A_i)$. For any $i \leq j$, $f_{ij} : G^n_j \to G^n_i$, $f'_{ji} : A_i \to A_j$ then $g_{ji} : C^n(G_i, A_i) \to C^n(G_j, A_j)$ is defined by composition. And for $p_i : \varprojlim G^n_i \to G^n_i, p'_i : A_i \to \varinjlim A_i$, there will also exist maps

$q_i : C^n(G_i, A_i) \to C^n_{cont}(\underleftarrow{\lim} G_i, \underrightarrow{\lim} A_i)$ defined by composition. Note inverse limits commute with inverse limits. Therefore we don't distinguish $\underleftarrow{\lim}(G_i^n)$ and $(\underleftarrow{\lim} G_i)^n$.

$$\begin{tikzcd}
\underrightarrow{\lim} C^n(G_i, A_i) \arrow[rr, dotted, "\exists!\ \theta_n"] & & C^n_{cont}(\underleftarrow{\lim} G_i, \underrightarrow{\lim} A_i) \\
& C^n(G_i, A_i) \arrow[ul, "\mu_i"'] \arrow[ur, "q_i"] \arrow[d, "g_{ji}"] & \\
& C^n(G_j, A_j) \arrow[uul, "\mu_j"] \arrow[uur, "q_j"'] &
\end{tikzcd} \tag{31}$$

The θ_n is induced by the universal property of inductive limits. Moreover θ_n's are actually a morphism between chains and the commutativity also comes from the universal property of inductive limits. We now prove θ_n is an isomorphism.

Note given an element $h \in \underrightarrow{\lim} C^n(G_i, A_i)$ there exists $h_i \in C^n(G_i, A_i)$ such that $h = \mu_i(h_i)$. $\theta_n(h)$ is defined to be $q_i(h_i)$. These information can be obtained from the diagram directly.

Given an element $u \in \underrightarrow{\lim} C^n(G_i, A_i)$ such that $\mu_i(u_i) = u$, $\theta_n(u) = q_i(u_i) = 0$. For $u_i p_i : \underleftarrow{\lim} G_i^n \to G_i^n \to A_i$, since G_i^n has only finitely many elements, there will exist $j \geq i$ such that $u_j p_j = f'_{ji} u_i p_i : \underleftarrow{\lim} G_i^n \to A_j$ is zero.

$$\begin{tikzcd}
\underleftarrow{\lim} G_i^n \arrow[dr, "p_j"'] \arrow[drr, bend left, "0"] \arrow[ddr, bend right, "p_k"'] & & \\
& G_j^n \arrow[r, "u_j"] & A_j \arrow[d, "f'_{kj}"] \\
& G_k^n \arrow[u, "f_{jk}"] \arrow[r, "u_k"'] & A_k
\end{tikzcd}$$

Assume

$$E_k := \{x \in G_k^n | u_k(x) \neq 0\}$$

for $k \geq j$. Then if $j \leq k \leq k'$, $f_{kk'}(E_{k'}) \subseteq E_k$. If some E_k is empty, then $u_k = 0$ which means $u = \mu_k(u_k) = 0$ and then θ_n is injective. We assume E_k are all non-empty. To deduce a contradiction we need the following lemma

Lemma 4.32. *The inverse limit of non-empty finite sets is non-empty where the index set I is directed.*

If the lemma above is true, then the inverse system $\{E_k | k \geq j\}$ has non-empty inverse limit. Say $(x_k)_k \in \varprojlim E_k$. It can be extended to be an element of $\varprojlim G_i^n$. For any $i \in I$, there is some $k \in I$, $i, j \leq k$. Hence the value in the position i is determined be all k. But this will deduce an contradiction, because $u_k p_k = f'_{kj} 0 = 0$. Hence some E_k must be empty. We prove Lemma 4.32 after proving θ_n is surjective.

Given a continuous map $w : \varprojlim G_i^n \to \varinjlim A_i = A$, since A is discrete, $w^{-1}(a)$ is open in $\varprojlim G_i^n$. But $\varprojlim G_i^n$ is profinite hence compact, w has only finitely many values, say$\{a_1, ..., a_m\}$. Note $w^{-1}(a)$ is closed as well. Hence $w^{-1}(a)$ is compact. Since every open subset of $\prod_i G_i^n$ has an open neighborhood $\prod_{i \in S} U_i \times \prod_{j \neq S} G_j^n$ where U_i is open in G_i^n and S is a finite set. Every $w^{-1}(a)$ is an intersection of finite unions of such open neighborhoods with $\varprojlim G_i^n$. Assume k is larger than any element in S for all $\{a_1, ..., a_m\}$. Then if we assume there are two elements u, v in $\varprojlim G_i^n$ satisfying $p_k(u) = p_k(v) \Rightarrow p_i(u) = p_i(v) = f_{ik} p_k(u)$ for any $i \in S$. Then u, v belong to the same $\prod_{i \in S} U_i \times \prod_{j \neq S} G_j^n$ hence to the same $w^{-1}(a)$. In G_k^n, $p_k(w^{-1}(a_l))$ where $1 \leq l \leq m$ are disjoint with each other. Therefore there will be a factorization of w

$$\begin{tikzcd}
\varprojlim G_i^n \arrow[r, "w"] \arrow[d, "p_k"] \arrow[dd, bend right, swap, "p_{k'}"] & A \\
G_k^n \arrow[r] \arrow[ur, dotted, "w'"] & A_{k'} \arrow[u] \\
G_{k'}^n \arrow[u] \arrow[ur, dotted, "w''"] &
\end{tikzcd}$$

But there are only finitely many elements in G_k^m, w' factors as $G_k^m \to A_{k'} \to A$. Then $w'' : G_{k'}^n \to G_k^n \to A_{k'}$ belongs to $C^n(G_{k'}, A_{k'})$ whose image under $q_{k'}$ is just w. Hence θ_n is surjective. □

Proof of Lemma 4.32. Assume $\{f_{ij} : X_j \to X_i | i \leq j\}$ is an inverse system of finite sets. Then we only need to prove $S = \cap_{j \leq k} R_{jk}$ is non-empty where $R_{jk} = \{(x_i)_i \in \prod_i X_i | f_{jk}(x_k) = x_j\}$. Equip finite set X_i with discrete topology $\Rightarrow \prod_i X_i$ is compact by Tychonoff's theorem. Since the set $T = \{(x_j, x_k) \in X_j \times X_k | f_{jk}(x_k) = x_j\}$ is closed and projection $\prod_i X_i \to X_j \times X_k$ is continuous, R_{jk} is closed. Hence we only need to prove the intersection of finitely many R_{jk} is non-empty. Choose k' large enough. $x_j = f_{jk'}(x_{k'})$ and $x_k = f_{kk'}(x_{k'})$. Other x_i's are arbitrary. Then we see such finite intersection is non-empty.

□

Theorem 4.33. *Under the assumption of Proposition 4.31,*

$$H^n_{cont}(G, A) \cong \varinjlim H^n(G_i, A_i)$$

Proof. It's a standard exercise in homological algebra that the n-th homology functor $H^n : \text{Ch.}(R) \to \text{Ab}$ commutes with inductive limits when the index set I is directed. It's not difficult just tedious and you should check many things. We leave as an exercise. □

Remark 4.34. If K/F is a Galois extension not necessarily finite and I is the index set such that E_i/F is finite Galois contained in K, then from Theorem 3.90 $\text{Gal}(K/F) \cong \varprojlim \text{Gal}(E_i/F)$ and $K = \varinjlim E_i$. Then for $n \geq 1$

$$H^n_{cont}(\text{Gal}(K/F), K) \cong \varinjlim H^n(\text{Gal}(E_i/F), E_i) = 0$$

and

$$H^1_{cont}(\text{Gal}(K/F), K^\times) \cong \varinjlim H^1(\text{Gal}(E_i/F), E_i^\times) = 0$$

4.3 Kummer Theory

In this section, the field F is special and it should contain a primitive n-th root of unity 1 with n fixed. Then F will contain all n-th roots of unity 1. Moreover we assume the polynomial $X^n - 1$ has n's different roots. We talk about Kummer theory in such special field. Actually there is also a Kummer theory for fields not satisfying this condition. But that's much more complicated and we don't consider it.

Note if F has characteristic zero, we have been familiar with it in the Section 3.2 since $\mathbb{Q} \subseteq F$. But if $\text{char}(F) = p > 0$, there will be some requirements on n. p must not divide n, $p \nmid n$. And since all roots of $X^n - 1$ form a group, from Lemma 2.38 we see such group will be cyclic and the primitive n-th root exist. The group is denoted by

$$\mu_n := \{n\text{-th roots of unity } 1\} \subseteq \bar{F}$$

and we require $\mu_n \subseteq F$.

Lemma 4.35. *Let $a \in F^\times$ and m is the order of a in the multiplicative quotient group $F^\times/(F^\times)^n$. Then every irreducible factor of $X^n - a \in F[X]$ has the form*

$$X^m - b$$

for some $b \in F$.

Proof. Assume α is a root of $P(X) = X^n - a$ in $\bar{F}$. It suffices to prove the minimal polynomial Q of α over F has the form $X^m - b$.

Step 1. We first prove $Q|X^m - b$, which is equivalent to say $\alpha^m \in F$. By definition of m, $a^m \in (F^\times)^n$ and there exist some $b \in F^\times$ such that $a^m = b^n$. Since $\alpha^n = a$, $\alpha^{nm} = b^n \Rightarrow (\alpha^m/b)^n = 1$. Then $\alpha^m/b \in \mu_n \subseteq F$. Hence $\alpha^m \in F^\times$.

Step 2. Now we only need to prove $deg(Q) = m$.

$$P = X^n - a = \prod_{i=0}^{n-1}(X - \alpha \cdot \xi_n^i) \Rightarrow Q = \prod_{i \in S}(X - \alpha\xi_n^i)$$

where $S \subseteq \{0, ..., n-1\}$ and $|S| = deg(Q)$. Expand $Q \Rightarrow \alpha^{deg(Q)}\xi_n^k \in F^\times \Rightarrow \alpha^{deg(Q)} \in F^\times$ where $k = \sum_{i \in S} i$. Then

$$a^{deg(Q)} = (\alpha^n)^{deg(Q)} = (\alpha^{deg(Q)})^n \in (F^\times)^n$$

hence $m|deg(Q) \Rightarrow m = deg(Q)$. □

Corollary 4.36. *Under the assumption of Lemma 4.35, $[F(\alpha) : F] = m$ where α is a root of $X^n - a$.*

Proposition 4.37. *Under the assumption of Lemma 4.35, if α is a root of $X^n - a$ then $F(\alpha)/F$ is a cyclic Galois extension of degree m.*

Proof. Having degree m has been proved above. Since roots of $X^n - a$ are $\{\alpha\xi_n^i | i = 0, 1..., n-1\}$ hence all different and the minimal polynomial of α divides $X^n - a$ then having different roots, $F(\alpha)/F$ is separable by Lemma 2.29. And since $\mu_n \subseteq F$, $F(\alpha)$ is the splitting field of $X^n - a$. Then $F(\alpha)/F$ is normal by Theorem 2.18. Next we define a map

$$\varphi : \mathrm{Gal}(F(\alpha)/F) \to \mu_n,\ \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$$

$\left(\frac{\sigma(\alpha)}{\alpha}\right)^n = \frac{\sigma(\alpha^n)}{\alpha^n} = \frac{\sigma(a)}{a} = 1 \Rightarrow \frac{\sigma(\alpha)}{\alpha} \in \mu_n$. We prove it's a group morphism.

$$\begin{aligned}\varphi(\sigma)\varphi(\tau) &= \frac{\sigma(\alpha)}{\alpha} \cdot \frac{\tau(\alpha)}{\alpha} \\ &= \frac{1}{\alpha}\sigma(\alpha \cdot \frac{\tau(\alpha)}{\alpha}), \quad \text{since } \frac{\tau(\alpha)}{\alpha} \subseteq \mu_n \subseteq F \\ &= \frac{(\sigma\tau)(\alpha)}{\alpha} \\ &= \varphi(\sigma\tau)\end{aligned}$$

Next we prove it's injective. If $\alpha(\sigma) = 1$, $\sigma(\alpha) = \alpha$. Then σ fixes $F(\alpha)$ hence being the identity map. Then $\mathrm{Gal}(F(\alpha)/F)$ is isomorphic to a subgroup of a cyclic group thus cyclic as well. □

Kummer theory is the converse of the proposition above.

Theorem 4.38 (Kummer)**.** *Let K/F be a Galois extension whose Galois group is $\mathbb{Z}/m\mathbb{Z} = \langle\sigma\rangle$ where $m|n$. Then $K = F(\alpha)$ with $\alpha^m \in F^\times$.*

Proof. Assume ξ_m is a primitive m-th root of unity 1 obtained from μ_n. Then $\mathrm{N}_{K/F}(\xi_m) = \xi_m^{[K:F]} = \xi_m^m = 1$. Hence according to Theorem 4.19 (multiplicative form of Hilbert 90), there exists some $\alpha \neq 0$ satisfying $\xi_m = \frac{\sigma(\alpha)}{\alpha} \Rightarrow \sigma(\alpha) = \alpha \cdot \xi_m$. Since $\sigma(\alpha^m) = (\alpha\xi_m)^m = \alpha^m$, $\alpha^m \in F^\times$. And we can see m is the minimal integer satisfying $a^m \in F\times$. Next we consider extensions $F \subseteq F(\alpha) \subseteq K$ and prove $\mathrm{Gal}(K/F(\alpha))$ is trivial. Otherwise there is $\tau \in \mathrm{Gal}(K/F(\alpha)) \subseteq \mathrm{Gal}(K/F) = \langle\sigma\rangle$ such that $\tau = \sigma^i, 1 \leq i \leq m-1$. But $\tau(\alpha) = \sigma^i(\alpha) = \alpha\xi_m^i \neq \alpha$. A contradiction! □

Note if we let $a = \alpha^n$ where α is defined above, then the order of a in $F^\times/(F^\times)^n$ is the minimal integer satisfying $\alpha^{\mathrm{ord}(a)} \in F^\times$ according to Lemma 4.35. Hence $\mathrm{ord}(a) = m$. In the following for simplicity given a group G, a *G-extension* of F means a Galois extension K/F whose Galois group is isomorphic to G. Then we have the corollary

Corollary 4.39. *There is a bijections between*

$$\{\mathbb{Z}/m\mathbb{Z}\text{-extensions of } F \text{ where } m|n\} \longleftrightarrow \{\langle a\rangle \subseteq F^\times/(F^\times)^n | \mathrm{ord}(a) = m\} \qquad (32)$$

Proof. We first prove it's well defined. Consider the morphism of part "←" and α is a root of $X^n - a$. Since $\mu \subseteq F$, the splitting field $F(\alpha)$ is independent from the choice of the root α. And if $\langle a\rangle = \langle b\rangle$ then there is an integer k with $(k, m) = 1$ such that $a = b^k$. Assume β is a root of $X^n - b$. Then $\alpha = \beta^k$ is a root of $X^n - a$. Then $F(\alpha) \subseteq F(\alpha)$. The converse is also true since as we have proved $F(\alpha)$ and $F(\beta)$ are splitting fields independent from the choice of α and β respectively.

From Theorem 4.38, we see such morphism of part "←" is suejective and we only need to prove it's injective. If there are two elements a, b haveing the same order m in $F^\times/(F^\times)^n$ and assume $\alpha^n = a, \beta^n = b$ satisfying $K = F(\alpha) = F(\beta)$, there is a morphism $\varphi : \mathrm{Gal}(K/F) = \langle\sigma\rangle \to \mu_n$ in Proposition 4.37. Then we could define $\varphi_\alpha(\sigma) = \frac{\sigma(\alpha)}{\alpha}$ and $\varphi_\beta(\sigma) = \frac{\sigma(\beta)}{\beta}$. Note $\mathrm{im}\varphi = \mu_m \Rightarrow \frac{\sigma(\alpha)}{\alpha}$ and $\frac{\sigma(\beta)}{\beta}$ are both m-th primitive roots of unity 1. Hence there exists some integer k with $(k, m) = 1$ such that $\frac{\sigma(\alpha)}{\alpha} = \left(\frac{\sigma(\beta)}{\beta}\right)^k \Rightarrow \sigma(\alpha\beta^{-k}) = \alpha\beta^{-k}$, which means $\alpha\beta^{-k} \in F^\times$. And then $(\alpha\beta^{-k})^n = ab^{-k} \in (F^\times)^n$. Hence in $F^\times/(F^\times)^n$, $a = b^k$ with $(k, m) = 1$ and $\langle a\rangle = \langle b\rangle$. □

Note the cyclic group $\mathbb{Z}/m\mathbb{Z}$ has the beautiful property with exponent dividing n which means the order of any element in $\mathbb{Z}/m\mathbb{Z}$ divides n. And this can be generalized as

Definition 4.40. *A* ***Kummer extension*** *of F is an abelian extension K/F such that the order of any element $\tau \in \mathrm{Gal}(K/F)$ divides n.*

K/F may not be cyclic nor finite. For example groups $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $\prod_{i=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$ will have the property stated above but are not cyclic and finite respectively. There is a characterization of finite Kummer extensions.

Theorem 4.41. *K/F is a finite Kummer extension iff K has the form*

$$K = F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$$

for some elements $a_i \in F^\times$.

Proof. "⇐": Every $F(\sqrt[n]{a_i})/F$ is finite Galois by Proposition 4.37 whose Galois group is cyclic of order dividing n. Consider the following injection

$$\mathrm{Gal}(K/F) \hookrightarrow \prod_{i=1}^{r} \mathrm{Gal}(F(\sqrt[n]{a_i})/F)$$

We see $\mathrm{Gal}(K/F)$ is abelian and every element in it has order dividing n.

"⇒": Since $\mathrm{Gal}(K/F)$ is finite abelian, the fundamental theorem for finitely generated modules over a PID tells us

$$\mathrm{Gal}(K/F) \cong G_1 \times ... \times G_r$$

where G_i's are cyclic of order dividing n. Assume $K_j = K^{H_j}$ and $H_j = \prod_{i \neq j} G_i \times \underset{\text{at } j}{\{1\}}$. Since $H_j \trianglelefteq G$ is normal, $\mathrm{Gal}(K_j/F) = \mathrm{Gal}(K/F)/H_j = G_j$. Then from the Theorem 4.38, $K_j = F(\sqrt[n]{a_j})$ for some $a_j \in F^\times$ and $K = K_1 \cdot ... \cdot K_r = F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$ follows from the following Lemma 4.42.

□

Lemma 4.42. *Let K/F be finite Galois extension with Galois grooup*

$$G = \mathrm{Gal}(K/F) = G_1 \times ... \times G_r$$

Then $K = K_1 \cdot ... \cdot K_r$ where $K_j = K^{H_j}$ and $H_j = \prod_{i \neq j} G_i \times \underset{at\ j}{\{1\}}$.

Proof. We prove by induction on r. If $r = 1$ then it's obvious. If $r = 2$, we need to prove $[K_1 \cdot K_2 : F] = [K : F]$. Given an element $x \in K_1 \cap K_2$, it's fixed by H_1 and H_2. Then x is fixed by $H_1 \cdot H_2 = G \Rightarrow K_1 \cap K_2 = F$. And since $H_i \trianglelefteq G$ is normal, K_i/F is finite Galois. According to the Proposition 3.14

$$\mathrm{Gal}(K_1 \cdot K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

then $[K_1 \cdot K_2 : F] = [K_1 : F] \cdot [K_2 : F] = |H_1| \cdot |H_2| = |G| = [K : F]$.

We assume the lemma is true for $\leq r$ and consider the condition on $r+1$. Suppose $H_j = \prod\limits_{i \neq j} G_i \times \underset{\text{at } j}{\{1\}}$ and $H'_r = \prod\limits_{i \neq r,\ r+1} G_i \times \underset{\text{at } r}{\{1\}} \times \underset{\text{at } r+1}{\{1\}}$. Then by assumption $K = K_1 \cdot ... \cdot K_{r-1} \cdot K'_r$ where $K_j = K^{H_j}$ and $K'_r = K^{H'_r}$. Since $H'_r \leq H_r, H_{r+1}$, $K_r, K_{r+1} \subseteq K'_r$. Moreover $\mathrm{Gal}(K'_r/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/K'_r) = G_r \times G_{r+1}$. We see from the condition $r = 2$ we have proved, $K'_r = K_r \cdot K_{r+1}$. Then $K = K_1 \cdot ... \cdot K_{r+1}$. This proves the lemma. □

Topics talked above are classical Kummer theory and actually there is a viewpoint of Galois cohomology. We assume $K_s = F_{sep}$ is the separable closure of F. K_s/F is Galois since for any element in K_s, its minimal polynomial over F is separable and then all roots of this polynomial will lie in K_s. Hence K_s/F is normal as well. And we can see K_s/F is the maximal Galois extension contained in $\bar{F}$. Therefore $K_s = \varinjlim E_i$ where E_i/F is finite Galois. For any finite Galois extension E_i/F, we have the following short exact sequence of $G_i = \mathrm{Gal}(E_i/F)$-modules

$$\begin{array}{c} 0 \longrightarrow \mu_n \longrightarrow E_i^\times \longrightarrow (E_i^\times)^n \longrightarrow 0 \\ x \longmapsto x^n \end{array} \tag{33}$$

Note for any $a \in K_s^\times$, the polynomial $X^n - a$ is separable hence all roots lying in $K_s^\times$. Then we see $(K_s^\times)^n = K_s^\times$. Hence $K_s = \varinjlim (E_i)^n$ as well. Consider the left exact functor $\mathrm{Hom}_{\mathbb{Z}[G_i]}(\mathbb{Z}, -) \cong (-)^{G_i}$ and there will exist a long exact sequence.

$$0 \longrightarrow \mu_n^{G_i} \longrightarrow (E_i^\times)^{G_i} \longrightarrow \big((E_i^\times)^n\big)^{G_i} \xrightarrow{\partial} H^1(G_i, \mu_n) \longrightarrow H^1(G_i, E_i^\times) = 0 \tag{34}$$

where $H^1(G_i, E_i^\times) = 0$ follows from the Theorem 4.18 (multiplicative form of Hilbert 90) and G_i acts trivially on μ_n. Then $\mu_n^{G_i} = \mu_n$, $(E_i^\times)^{G_i} = F^\times$ and $\big((E_i^\times)^n\big)^{G_i} = (E_i^\times)^n \cap F^\times$. Moreover for group cohomology if G acts trivially on A, then $B^1(G, A) = 0$. Then $H^1(G, A) = Z^1(G, A)$. Assume $f : G \to A$ is a 1-cocycle. We have $xf(y) - f(xy) + f(x) = 0 \Rightarrow f(xy) = f(x) + f(y)$ which is actually a group homorphism. Hence $H^1(G, A) = \mathrm{Hom}_{\mathrm{Groups}}(G, A)$. Here $H^1(G_i, \mu_i) = \mathrm{Hom}_{\mathrm{Groups}}(G_i, \mu_n)$. The long exact sequence implies

$$\big((E_i^\times)^n \cap F^\times\big)/(F^\times)^n \cong \mathrm{Hom}_{\mathrm{Groups}}(G_i, \mu_n)$$

Also notice that $\varinjlim \big((E_i)^n \cap F\big) = K_s \cap F = F$. Since inductive limits of directed index set is exact, take inductive limits to the long exact sequence above and finally we obtain

$$0 \longrightarrow \mu_n \longrightarrow F^\times \longrightarrow F^\times \xrightarrow{\partial} H^1_{cont}(G, \mu_n) \longrightarrow 0 \tag{35}$$

where $G = \mathrm{Gal}(K_s/F)$ and $H^1_{cont}(G, \mu_n) = \mathrm{Hom}_{\mathrm{ToGroups}}(G, \mu_n)$ consists of all continuous group morphisms where μ_n is equipped with discrete topology and G is with Krull topology. Then

$$F^\times/(F^\times)^n \cong \mathrm{Hom}_{\mathrm{ToGroups}}(G, \mu_n)$$

Next we study the connected morphism ∂ further and we focus on finite Galois case first. Looking at the following commutative diagram from which the long exact sequence of finite Galois case come.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathrm{Map}(G_i^0, \mu_n) \arrow[r] \arrow[d] & \mathrm{Map}(G_i^0, E_i^\times) \arrow[r, shift right] \arrow[d, shift left] \arrow[d, dotted, shift right] & \mathrm{Map}(G_i^0, (E_i^\times)^n) \arrow[l, dotted, shift right] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Map}(G_i^1, \mu_n) \arrow[r, shift right] \arrow[d] & \mathrm{Map}(G_i^1, E_i^\times) \arrow[l, dotted, shift right] \arrow[r] \arrow[d] & \mathrm{Map}(G_i^1, (E_i^\times)^n) \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

The connected morphism ∂ is just the dotted arrows. Gievn an element $a \in (E_i^\times)^n$, choose a root α of $X^n - a$ in $E_i^\times$ first. $d^1(\alpha) : \sigma \mapsto (\sigma \cdot \alpha)\alpha^{-1} = \frac{\sigma(\alpha)}{\alpha}$ which also belongs to $\mathrm{Map}(G_i^1, \mu_n)$. This is clear in snake lemma. Hence in general case

$$F^\times/(F^\times)^n \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{ToGroups}}(G, \mu_n), \quad a \longmapsto (\mathcal{X}_a : \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}) \tag{36}$$

where α is a root of $X^n - a$. This isomorphism is similar to that in Corollary 4.39. And we can check $\mathcal{X}_a$ is continuous since $\sigma \in \ker(\mathcal{X}_a)$ iff $\sigma(\alpha) = \alpha$ iff $\sigma \in \mathrm{Gal}(K_s/F(\alpha))$ where $F(\alpha)/F$ is finite. Hence $\mathrm{Gal}(K_s/F(\alpha))$ is open from Remark 3.85 (4) by definition of Krull topology. But note it's in fact not necessary to check $\mathcal{X}_a$ is whether well defined and continuous or not because all our results above come from the Section 4.2 and homological algebra with nothing new. Then $\mathcal{X}_a$ satisfies all these properties automatically.

From the checking process we see $\ker\mathcal{X}_a = \mathrm{Gal}(K_s/F(\sqrt[n]{a})) \trianglelefteq G$ is normal. Then $F(\sqrt[n]{a})/F$ is finite Galois. Moreover given distinct $\mathcal{X}_{a_1}, ..., \mathcal{X}_{a_r}$, we will have

$$\ker\mathcal{X}_{a_1} \cap ... \cap \ker\mathcal{X}_{a_r} = \mathrm{Gal}(K_s/F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r}))$$

Now we still start from the long exact sequence of finite Galois case. Assume K/F is a Kummer extension. Passing to inductive limits, we have

$$\big((K^\times)^n \cap F^\times\big)/(F^\times)^n \cong \mathrm{Hom}_{\mathrm{ToGroups}}(G, \mu_n)$$

where $G = \mathrm{Gal}(K/F)$. The *Kummer group* of K/F is defined to be

$$\mathrm{Kum}(K/F) := \big((K^\times)^n \cap F^\times\big)/(F^\times)^n$$

Especially if K/F is finite then $\mathrm{Kum}(K/F) \cong \mathrm{Hom}_{\mathrm{Groups}}(G, \mu_n)$ and there will be a *perfect bimultiplicative paring*:

$$\langle\ ,\ \rangle : \mathrm{Gal}(K/F) \times \mathrm{Kum}(K/F) \to \mu_n, \quad \langle \sigma, a\rangle = \mathcal{X}_a(\sigma) = \frac{\sigma(\alpha)}{\alpha}$$

by choosing a $\alpha = \sqrt[n]{a}$ in $K^\times$. It satisfies following properties:

- (Bimultiplicative)

$$\langle \sigma_1\sigma_2, a\rangle = \langle \sigma_1, a\rangle \cdot \langle \sigma_2, a\rangle$$
$$\langle \sigma, a_1a_2\rangle = \langle \sigma, a_1\rangle \cdot \langle \sigma, a_2\rangle$$

- (Perfect) If $\sigma \in \mathrm{Gal}(K/F)$ satisfies for all $a \in \mathrm{Kum}(K/F)$, $\langle \sigma, a\rangle = 1$ then $\sigma = id$. If $a \in \mathrm{Kum}(K/F)$ satisfies for all $\sigma \in \mathrm{Gal}(K/F)$, $\langle \sigma, a\rangle = 1$ then $a = 1$ which is equivalent to $a \in (F^\times)^n$.

Only the first part of perfect properties need some words. Since K/F is finite Kummer, according to the Theorem 4.41 $K = F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$ where $a_i \in (K^\times)^n \cap F^\times$. And then $\ker\mathcal{X}_{a_1} \cap ... \cap \ker\mathcal{X}_{a_r} = \mathrm{Gal}(K/F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})) = 1$. Hence we see if $\langle \sigma, a\rangle = 1$ for all $a \in \mathrm{Kum}(K/F)$, then $\sigma \in \cap_a \ker\mathcal{X}_a = 1$. This perfect bimultiplicative paring is called *Kummer duality.*

Moreover the inductive limits of all finite Kummer extensions form a maximal Kummer extension and it contains all roots of $X^n - a$ where $a \in F$. If the maximal Kummer extension is denoted by $\mathcal{K}/F$, then $F \subseteq \mathcal{K}^n$ and $\mathrm{Kum}(\mathcal{K}/F) = F^\times/(F^\times)^n$.

$$\langle\ ,\ \rangle : \mathrm{Gal}(\mathcal{K}/F) \times F^\times/(F^\times)^n \to \mu_n$$

The paring is still perfect bimultiplicative, since $\mathcal{K} = F(\cup_i \sqrt[n]{a_i})$ where $a_i \in F^\times$ and then $\cap_a \ker\mathcal{X}_a = \mathrm{Gal}(\mathcal{K}/F(\cup_i \sqrt[n]{a_i})) = 1$.

Until now we only consider about multiplicative forms of Kummer theory. In the following we talk about *Artin–Schreier* theory which is an analogy of Kummer theory in the case of char $= p > 0$. In Kummer theory we consider the polynomial $X^n - a$, but here we consider the Artin Schreier polynomial $X^p - X - a \in F[X]$.

Theorem 4.43. *Let F be a field of* char $= p > 0$. *Then*

(1) Given $a \in F$, polynomials $X^p - X - a$ are either irreducible or completely reducible.

(2) If K/F is a cyclic extension of degree p, then $K = F(\alpha)$ where α is a root of $X^p - X - a$ for some $a \in F$.

Proof. (1). Assume $\alpha \in \bar{F}$ is a root of $f(X) = X^n - X - a$. Then $\alpha + j$ where $0 \leq j \leq p-1$ is also a root of it since $(\alpha+j)^p - (\alpha+j) - a = (\alpha^p + j^p) - (\alpha+j) - a = 0$. Note $\mathbb{F}_p$ consists of all roots of $X^p - X$. Hence if $f(X)$ has a root in F then all its roots in F.

Now we suppose $f(X)$ has no roots in F. If $f(X)$ is not irreducible then $f = gh$ where $g, h \in F[X]$ and $0 \leq deg(g), deg(h) \leq p$. Since $f(X) = \prod_{j=0}^{p-1}(X - \alpha - j)$, $g(X) = \prod_{j \in S}(X - \alpha - j)$ where $S \subseteq \{0, 1, ..., p-1\}$. Let $d = deg(g) = |S|$. Expand $g(X) \Rightarrow g(X) = X^d + a_{d-1}X^{d-1} + ...$ and $a_{d-1} = -\sum_{j \in S}(\alpha + j) = -d\alpha - \sum_{j \in S} j \in F$. Then $d\alpha \in F \Rightarrow \alpha \in F$ since $0 < d < p$. A contradiction.

We see for any irreducible polynomial $X^n - X - a$ with a root α, its splitting field is $F(\alpha)$ of degree p with Galois group $\mathbb{Z}/p\mathbb{Z}$.

(2). Let K/F be a cyclic extension of degree p and $G = \mathrm{Gal}(K/F) = \langle \sigma \rangle$. Since $\mathrm{Tr}_{K/F}(1) = [K : F] \cdot 1 = 0$, from the Theorem 4.19 (additive form of Hilbert 90), there is some $\alpha \in K$ satisfying $1 = \sigma(\alpha) - \alpha \Rightarrow \sigma(\alpha) = 1 + \alpha$. Then $\alpha^j(\alpha) = j + \alpha$ where $0 \leq j \leq p-1$ are p's distinct conjugates of α. Then $K = F(\alpha)$. Moreover to prove the minimal polynomial of α is $X^p - X - a$, it's enough to prove $\alpha^p - \alpha \in F$. But $\sigma(\alpha^p - \alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$ Hence $\alpha^p - \alpha \in F$. □

This theorem can be generalized to p^r-groups.

Theorem 4.44. *If K/F is a Galois extension whose Galois group*

$$\mathrm{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z} \times ... \times \mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/p\mathbb{Z})^r$$

Then there are $a_1, ..., a_r \in F^\times$ such that $K = F(\alpha_1, ..., \alpha_r)$ where α_i is a root of $X^p - X - a_j$.

Proof. Use Lemma 4.42 and Theorem 4.43. □

We can also use Galois cohomology to reformulate the Artin–Schreier theory. Assume again K_s is the separable closure of F and $G = \mathrm{Gal}(K_s/F)$. There is a short exact sequence

$$\begin{aligned} 0 \longrightarrow \mathbb{F}_p \longrightarrow K_s &\xrightarrow{\varphi} K_s \longrightarrow 0 \\ x &\longmapsto x^p - x \end{aligned} \tag{37}$$

Note φ is additive $\varphi(x+y) = (x+y)^p - (x+y) = x^p - x + y^p - y = \varphi(x) + \varphi(y)$. And φ is surjective. Given any element $a \in K_s$ consider the polynomial $X^p - X - a$ which is separable since its derivative is $-1 \neq 0$. Then its roots are in K_s. There will exist some $x \in K_s$ satisfying $x^p - x = a$. And obviously $\mathrm{ker}\varphi = \mathbb{F}_p$. Take the continuous cohomology to this short exact sequence we obtained the following long exact sequence

$$0 \longrightarrow \mathbb{F}_p^G \longrightarrow K_s^G \longrightarrow K_s^G \xrightarrow{\partial} H^1_{cont}(G, \mathbb{F}_p) \longrightarrow H^1_{cont}(G, K_s)$$

where $K_s^G = F$ and $H^1_{cont}(G, K_s) = 0$ follows from Remark 4.34. And since G acts trivially on $\mathbb{F}_p$, then $H^1_{cont}(G, \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{ToGroups}}(G, \mathbb{F}_p)$. Then

$$0 \longrightarrow \mathbb{F}_p \longrightarrow F \longrightarrow F \xrightarrow{\partial} H^1_{cont}(G, \mathbb{F}_p) \longrightarrow 0 \tag{38}$$

Explicitly

$$\begin{aligned} F/\{x^p - x | x \in F\} &\cong H^1_{cont}(G, \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{ToGroups}}(G, \mathbb{F}_p) \\ a &\longmapsto (\theta_a : \sigma \mapsto \sigma(\alpha) - \alpha) \end{aligned} \tag{39}$$

where α is a root of the polynomial $X^p - X - a$. Though it's not necessary and there is no distinguished difference between this case and the multiplicative case considered before, you can check it's well defined and θ_a is actually a group morphism by yourselves.

$\sigma \in \ker\theta_a$ iff $\sigma(\alpha) = \alpha$ iff $\sigma \in \mathrm{Gal}(K_s/F(\alpha))$. Then $\ker\theta_a = \mathrm{Gal}(K_s/F(\alpha)) \trianglelefteq G$ is normal. This implies $\mathrm{Gal}(K_s^{\ker\theta_a}/F) \cong G/\ker\theta_a \cong \mathbb{Z}/p\mathbb{Z}$ since non trivial θ_a is suejective and $K_s^{\ker\theta_a} = F(\alpha)$.

Exercise 4.45. Let K/F be a $\mathbb{Z}/p^n\mathbb{Z}$-extension where p is a prime and $n \geq 1$. Let $F \subseteq E \subseteq K$ be a subfield such that $[K : E] = p$. Prove the following statement: if $K = E(\alpha)$ then we also have $K = F(\alpha)$.

Exercise 4.46. Let F be a field, $n \in \mathbb{N}$ which is coprime to $\mathrm{char}(F)$, but F is not assumed to contain μ_n. Let $K = F(\alpha)$ where $\alpha \in \bar{F}$ is a root of $X^n - a$ for some $a \in F^\times$. Prove that $[K : F]$ divides n. (Hint: reduce to the case $\mu_n \subseteq F$.)

References

[Art07] Emil Artin *Algebra with Galois Theory*, American Mathematical Society, Courant Institute of Mathematical Sciences, 2007

[Bos18] Siegfried Bosch, *Algebra: From the Viewpoint of Galois Theory*, Springer Nature Switzerland AG 2013, 2018

[Jac85] Nathan Jacobson, *Basic Algebra I*, W. H. Freeman and Company, 1985

[Jac89] Nathan Jacobson, *Basic Algebra II*, W. H. Freeman and Company, 1989

[Lan02] Serge Lang, *Algebra*, Springer-Verlag New York. Inc, 2002

[Rot09] Rotman, *An Introduction to Homological Algebra*, Springer Science+Business Media, LLC 2009

[Ser79] Jean-Pierre Serre, *Local Fields*, Springer-Verlag New York. Inc, 1979