Galois theory

Jiaheng Zhao

November 15, 2021

Contents

1 Extension of fields

1.1 Fields and field extensions

Definition 1.1. A **field** is a commutative ring such that $F^\times = F - \{0\}$ form an abelian group under the multiplication operation.

Lemma 1.2. *For any ring R, there is a unique ring homomorphism $i_R : \mathbb{Z} \to R$. If R is a field, then $\mathrm{Ker}(i_R)$ is either 0 or $p\mathbb{Z}$ for p a prime.*

Proof. The image of i_R must be an integral domain and as a result $\mathrm{Ker}(i_R)$ must be a prime ideal. □

Definition 1.3. We say that a field F is **of characteristic** 0 if $\mathrm{Ker}(i_F) = 0$. We say that F is **of characteristic** p if $\mathrm{Ker}(i_F) = p\mathbb{Z}$.

From now on we use $\mathrm{char}(F)$ to denote the characteristic of a field.

Theorem 1.4. *Let F, E be fields and $f : F \to E$ be a ring homomorphism, then F is injective. In this case we say that E is an **extension** of F, denoted by E/F.*

Proof. $\mathrm{Ker}(f)$ is an ideal of F and F has no non-trivial ideals. Thus $\mathrm{Ker}(f) = 0$. □

Definition 1.5. Let E/F and K/F be two extensions of F. We use $\hom_F(E, K)$ to denote the set of field embeddings from E to K which preserves F, and call it **the set of F-embeddings from E to K**.

Let E/F be a field extension, then we can view E as an F-algebra and in particular an F-vector space. If E is finite dimensional over F, we say that E/F is a **finite extension**. We use $[E : F]$ to denote the dimension and call it the **degree** of the field extension.

Lemma 1.6 (Tower property)**.** *Let L/E and E/F be finite extensions, then*

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

Proof. Let $\{\alpha_i\}_{i \in I}$ be a basis of E/F and $\{\beta_j\}_{j \in J}$ be a basis of L/E. Then $\{\alpha_i\beta_j\}$ form a basis of L/F. To see this, first note that the set $\{\alpha_i\beta_j\}$ generates F with coefficients in F. Then we show linear independency. Take a family of coefficients $\{c_{i,j} \in F\}$ such that

$$\sum_{i,j} c_{i,j}\alpha_i\beta_j = 0.$$

Let $d_j = \sum_i c_{i,j}\alpha_i \in E$, then $\sum_j d_j\beta_j = 0$. We conclude that $d_j = 0$ for all j, so that $c_{i,j} = 0$ for all i, j. □

Definition 1.7. Let E/F be an extension and $S \subset E$ be a set. The **field generated by** S is the minimal subextension K/F such that $S \subset K$, which is denoted by $F(S)$. If S is finite we say that $F(S)$ is **finitely generated** over F.

Definition 1.8. An extension E/F is called **simple** if $E = F(\alpha)$ for some $\alpha \in E$.

1.2 Algebraicity

Definition 1.9 (Algebraic and transcendental elements)**.** Let E/F be a field extension. An element $\alpha \in E$ is called **algebraic over** F if there exists some $R \in F[X]$ such that $R(\alpha) = 0$. Otherwise we say that α is **transcendental over** F.

Definition 1.10. E/F is called an **algebraic extension** if every $\alpha \in E$ is algebraic over F.

Theorem 1.11. *Let E/F be an extension and $\alpha \in E$ algebraic over F. Then there exists a unique monic irreducible polynomial P_α such that $P_\alpha(\alpha) = 0$. We call P_α the* ***minimal polynomial*** *of α.*

Proof. Let $Z_\alpha = \{R \in F[X] : R(\alpha) = 0\}$. Choose a monic polynomial P_α in Z_α such that P_α has minimal degree. Then P_α must be unique and irreducible. □

Proposition 1.12. *Let $P \in F[X]$ be a irreducible polynomial of degree n, define the F-algebra $E := F[X]/(P)$. Then E/F is a field extension such that $[E : F] = n$.*

Proof. $(P) \subset F[X]$ is a maximal ideal since $F[X]$ is a PID. Let $\pi : F[X] \to F[X]/(P)$, $a \mapsto \overline{a} = a + (P)$ be the quotient map, then $1, \overline{X}, \overline{X^2}, ..., \overline{X^{n-1}}$ form a basis of the extension. □

Theorem 1.13. *Let $F(\alpha)/F$ be a simple extension with α algebraic over F. Then there is a canonical isomorphism of fields $F[X]/P_\alpha \to F(\alpha)$ by sending $\overline{X}$ to α.*

Proof. The embedding $F[X]/P_\alpha \to F(\alpha)$ is induced by the universal property. We see that it is an isomorphism by counting dimension. □

Corollary 1.14. *Let α and β be distinct roots of P_α, then there is a canonical isomorphism $F(\alpha) \to F(\beta)$ sending α to β.*

Theorem 1.15. *An extension E/F is finite if and only if it is a finitely generated algebraic extension.*

1.3 Algebraic closure

Definition 1.16. We say a field E is **algebraic closed** if any algebraic extension of E is trivial. Equivalently, E is algebraically closed if any non-constant $P \in E[X]$ has a root.

Definition 1.17. Let $\overline{F}/F$ be an algebraic extension. We call $\overline{F}$ the **algebraic closure** of F if $\overline{F}$ is algebraically closed.

Theorem 1.18 (E.Steinitz)**.** *For any field F, its algebraic closure $\overline{F}$ exists and is unique up to F-isomorphisms.*

Lemma 1.19. *Consider a finite extension $F(\alpha)$ generated by a single element α (whose minimal polynomial is denoted by P_α) and fix an algebraic closure $\overline{F}/F$ of F. Then there is a bijection*

$$\hom_F(F(\alpha), \overline{F}) \Leftrightarrow \{\beta \in \overline{F} : P_\alpha(\beta) = 0\}$$

Proof. View $F(\alpha)$ as the quotient algebra $F[X]/P_\alpha$ and apply its universal property. □

Remark 1.20. From the lemma we can see that

$$|\hom_F(F(u), \overline{F})| \leq \deg P_\alpha = [F(\alpha) : F] \tag{1}$$

The equality holds iff P_α has no multiple roots.

Theorem 1.21. *Let $\overline{F}/F$ be an algebraic closure and E/F be arbitrary algebraic extension. Then there exists F-embeddings $\iota \in \hom_F(E, \overline{F})$. When E/F is finite we have $|\hom_F(E, \overline{F})| \leq [E : F]$.*

Proof. Let $E = F(x_1, ..., x_n)$. By repeated use of inequality (1) we have

$$|\hom_F(F(x_1, ..., x_n), \overline{F})| \leq \prod_{i=1}^{n} [F(x_1, ..., x_i) : F(x_1, ...x_{i-1})] = [E : F],$$

□

1.4 Normal extensions

Definition 1.22. Let $\mathcal{P} \subset F[X]$ be a family of non-constant polynomials. If E/F satisfies

1. Every $P \in \mathcal{P}$ factors into linear factors over E. That is $P = c_P \prod_{j=1}^{n_P}(X - \alpha_{P,j})$ where $c_P \in F^\times, \alpha_{P,j} \in E$.
2. All roots $\{\alpha_{P,j} : P \in \mathcal{P}, 1 \leq j \leq n_P\}$ generate E over F.

then we call E the **splitting fields** of $\mathcal{P}$ over F.

Theorem 1.23. *Let $\mathcal{P} \subset F[X]$ be a family of non-constant polynomials. Then the spitting field of $\mathcal{P}$ exists. If $P \in F[X]$ is a non-constant polynomial of degree n and E is the splitting field of P, then $[E : F] \leq n!$.*

Lemma 1.24. *For an algebraic extension L/F, any F-embeddings $\iota : L \to L$ is an isomorphism of fields. That is $\mathrm{End}_F(L) = \mathrm{Aut}_F(L)$.*

Proof. If suffices to show that ι is surjective. Take $y \in L$ and $P_y \in F[X]$ be its minimal polynomial. Let $\{y = y_1, ..., y_n\} \subset L$ be the set of roots of P_y in L. Since ι induces a permutation over $\{y_1, ..., y_n\}$, thus $y \in \mathrm{im}(\iota)$. □

Definition 1.25. A field extension E/F is called **normal** if it is a splitting field of some $\mathcal{P} \subset F[X]$ consisting of non-constant polynomials.

Theorem 1.26. *TFAE:*

1. *E/F is a normal extension,*
2. *If an irreducible polynomial $P \in F[X]$ has a root in E, then it splits into a product of linear factors over E,*
3. *Fix an algebraic closure $\overline{F}/E$ and view E as a subfield of $\overline{F}$. Then any $\iota \in \hom_F(E, \overline{F})$ satisfies $\iota(E) = E$.*

Proposition 1.27. *Let L/F be a normal extension, E/F its sub-extension, then any $\iota \in \hom_F(E, L)$ can be extended to some $\tilde{\iota} \in \mathrm{Aut}_F(L)$*

Proof. Fix an algebraic closure $\overline{F}$ of F and view L as a subfield of $\overline{F}$. Then we can always extend a $\iota \in \hom_F(E, L) \subset \hom_F(E, \overline{F})$ to some $\tilde{\iota} \in \hom_F(L, \overline{F})$ by Theorem 1.21. Normality guarantees that $\hom_F(L, \overline{F}) = \mathrm{End}_F(L)$ and Theorem 1.24 guarantees that $\mathrm{End}_F(L) = \mathrm{Aut}_F(E)$. $\square$

1.5 Separable extensions

Definition 1.28. An irreducible polynomial $P \in F[X]$ is called **separable** if it has no multiple roots in its splitting field. An algebraic element $\alpha \in E$ in an extension E/F is **separable** if its minimal polynomial is separable.

Definition 1.29. We say that an algebraic extension E/F is **separable** if for all $x \in E$ the minimal polynomial P_x of x is separable.

Lemma 1.30. *A non-zero polynomial $P \in F[X]$ has multiple roots (over its splitting field L) if and only if $(P, P') \neq 1$.*

Proposition 1.31. *If E/F is finite separable, then $|\hom_F(E, \overline{F})| = [E : F]$.*

Proof. Similar to the proof of Theorem 1.21. But separability guarantees that the equality holds. $\square$

Definition 1.32. Let E/F be an algebraic extension, then its **separable degree** is defined as $[E : F]_s := |\hom_F(E, \overline{F})|$.

Lemma 1.33. *Let $F(x)/F$ be a finite extension and let P_x be the minimal polynomial of x. Then $[F(x) : F]_s$ equals the number of roots of P_x (without counting multiplicity) in $\overline{F}$.*

Proof. This is direct from 1.19. $\square$

Theorem 1.34. *For irreducible $P \in F[X]$, the following statements are equivalent*

1. *P has multiple roots in the algebraic closure $\overline{F}$,*
2. *P has multiple roots in its splitting field,*
3. *$P' = 0$,*

4. $\mathrm{char}(F) = p > 0$, *and* P *has the form* $\sum_{k\geq 0}^{n} X^{pk}$.

Corollary 1.35. *Let* F *be a field with characteristic* $p > 0$. *Then an inseparable irreducible polynomial in* $P \in F[X]$ *has the form*

$$P(X) = P^{\natural}(X^{p^m})$$

where $P^{\natural}$ *is separable and of course irreducible.*

Theorem 1.36. *Let* E/F *be a finite extension, then* $[E:F]_s | [E:F]$

Proof. It suffices to prove this for simple extensions. Let $F(x)/F$ be a finite simple extension and we write P_x as

$$P_x(X) = P_x^{\natural}(X^{p^m})$$

Then by Lemma 1.33 $[E:F]_s = \deg P_x^{\natural}(X)$. So obviously $\deg P_x^{\natural} | \deg P_x$ and the latter is $[E:F]$. □

Definition 1.37. The number $\frac{[E:F]}{[E:F]_s}$ is called the **inseparable degree** and is denoted by $[E:F]_i$.

Definition 1.38. We say that a field F is **perfect** if any algebraic extension of F is separable.

Proposition 1.39. *The following fields are perfect:*

1. *Fields of characteristic* 0,
2. *Finite fields.*

Proof. Fields of characteristic 0 are obviously perfect. For finite fields see Theorem 4.2. □

Definition 1.40. We say that a field L is **separably closed** if any separable irreducible polynomial in $L[X]$ has a root in L. If E/F is algebraic and E is separably closed then E is called a **separable closure** of F, which we denote by F^{sep}.

Proposition 1.41. *The separable closure* F^{sep}/F *is a normal extension.*

Proof. F^{sep} can be identified with the splitting field of all separable polynomials over F. □

1.6 Trace and norm

Let E/F be a finite extension.

Definition 1.42. For $\alpha \in E$, we define the map $m_\alpha : E \to E$, $\beta \mapsto \alpha\beta$ which is F-linear. The **trace** of α is defined to be $\mathrm{tr}_{E/F}(\alpha) = \mathrm{tr}(m_\alpha) \in F$. The **norm** of α is defined to be $N_{E/F}(\alpha) = \det(m_\alpha) \in F$.

Lemma 1.43. *Let $E = F(\alpha)$ with α algebraic such that $P_\alpha(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$ to be the minimal polynomial of α. Then $\mathrm{tr}_{E/F}(\alpha) = -a_{n-1}$ and $N_{E/F}(\alpha) = (-1)^n a_0$.*

Theorem 1.44. *For finite extension E/F and $x \in E$, fix an algebraic closure $\overline{F}|F$, then we have*

$$N_{E/F}(x) = \prod_{\sigma \in \hom_F(E, \overline{F})} \sigma(x)^{[E:F]_i}$$

$$\mathrm{tr}_{E/F}(x) = [E : F]_i \sum_{\sigma \in \hom_F(E, \overline{F})} \sigma(x)$$

where $[E : F]_i$ is the inseparable degree.

Corollary 1.45. *Let E/F be a finite separable extension. Then we have*

$$N_{E/F}(x) = \prod_{\sigma \in \hom_F(E, \overline{F})} \sigma(x)$$

$$\mathrm{tr}_{E/F}(x) = \sum_{\sigma \in \hom_F(E, \overline{F})} \sigma(x)$$

These formulas are quite useful in algebraic number theory. We will demonstrate a few applications. First recall Dedekind's theorem on characters:

Theorem 1.46 (Dedekind-Artin)**.** *Let Γ be a monoid and R be a commutative domain. Then $\hom(\Gamma, (R, \times))$ is R-linearly independent. That is to say, if $\chi_1, ..., \chi_n : \Gamma \to (R, \times)$ are distinct homomorphism and $r_1, ...r_n \in R$ such that $\sum_{i=1}^n r_i\chi_i(g) = 0$ for all $g \in \Gamma$, then $r_i = 0$ for all i.*

Proof. By induction on n. For $n = 1$, it suffices to take $g = 1$. For $n \geq 2$ it suffices to show that $r_n = 0$. Choose $h \in \Gamma$ such that $\chi_1(h) \neq \chi_n(h)$. Then

$$\sum_{i=2}^n r_i(\chi_i(h) - \chi_1(h))\chi_i(g) = \sum_{i=1}^n r_i\chi_i(hg) - \chi_1(h)\sum_{i=1}^n r_i\chi_i(g) = 0.$$

By induction hypothesis, $r_n(\chi_n(h) - \chi_1(h)) = 0$ which implies $r_n = 0$. □

Theorem 1.47. *If L/K is finite separable, then the bilinear form $\mathrm{Tr} : L \times L \to K$, sending (x, y) to $\mathrm{tr}_{L/K}(x, y)$ is non-degenerate.*

Proof. If $\forall y \in L$ we have $\mathrm{Tr}_{L/K}(xy) = 0$, then

$$\sum_{i=1}^{n} \sigma_i(xy) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y) = 0, \quad \forall y \in L.$$

Apply Theorem 1.46 to $\Gamma = L^\times$, we obtain $\sigma_i(x) = 0$ for all i. Hence $x = 0$. ☐

1.7 Purely inseparable extensions

Definition 1.48. Let E/F be an extension and $x \in E$ be algebraic over F. If the minimal polynomial of x has the form $P_x = X^{p^m} - a \in F[X]$, then we say that x is **purely inseparable** over F.

Definition 1.49. An algebraic extension is **purely inseparable** if it is generated by a family of purely inseparable elements.

Corollary 1.50. *A purely inseparable extension is normal.*

Lemma 1.51. *If an algebraic extension E/F is both separable and purely inseparable, then $[E : F] = 1$.*

Example 1.52. If K/F be an extension and $\alpha \in K$ is separable over F, $b \in K$ is purely inseparable over F, then $F(\alpha, \beta) = F(\alpha + \beta)$. This is because the extension $F(\alpha, \beta) = F(\alpha + \beta)(\alpha) = F(\alpha + \beta)(\beta)$ is both separable and purely inseparable over $F(\alpha + \beta)$.

1.8 Transcendental extension

Definition 1.53. Let Ω/F be an extension. A subset $\chi \subset \Omega$ is called **algebraically independent** over F if the following condition is satisfied: for all $n \geq 1$ and distinct n elements $x_1, ..., x_n \in \chi$ and polynomial $P \in F[X_1, ..., X_n]$, we have

$$P(x_1, ..., x_n) = 0 \Leftrightarrow P = 0.$$

Lemma 1.54. *Any extension Ω/F has maximal algebraically independent subset.*

Proof. Any chain of algebraically independent subsets of Ω has an upper bound by taking the union. We conclude by Zorn's lemma. ☐

Definition 1.55. A maximal algebraically independent subset of Ω over F is a transcendental basis of the extension Ω/F.

Let $\mathcal{B}$ be a transcendental basis of Ω/F. From the definition of transcendental basis we see that

- The subextension $F(\mathcal{B})/F$ can be identified with the field of rational functions ober the set $\mathcal{B}$.
- $\Omega/F(\mathcal{B})$ is an algebraic extension.

- Conversely, any subset of Ω satisfying the above two properties is a transcendental basis.

Lemma 1.56. *Let $\mathcal{B}, \mathcal{B}'$ are transcendental basis of Ω/F. If $\mathcal{B}$ is infinite then $|\mathcal{B}'| \geq |\mathcal{B}|$.*

Lemma 1.57 (Exchange property)**.** *Let $\mathcal{B}, \mathcal{B}'$ be two finite transcendental basis of Ω/F, $b' \in \mathcal{B}' \setminus \mathcal{B}$, then there exists $b \in \mathcal{B} \setminus \mathcal{B}'$ such that $(\mathcal{B}' \setminus \{b'\}) \cup \{b\}$ is still a transcendental basis.*

Theorem 1.58. *Let $\mathcal{B}, \mathcal{B}'$ be two transcendental basis of Ω/F, then we have $|\mathcal{B}| = |\mathcal{B}'|$.*

Definition 1.59. The cardinality of a transcendental basis of Ω/F is called the **transcendental degree** of Ω/F, which is denoted by $\mathrm{tr.deg}(\Omega/F)$.

Corollary 1.60. *Let Ω_1, Ω_2 are extensions of F and are algebraically closed. Then there is an isomorphism of F-algebras $\Omega_1 \cong \Omega_2$ if and only if $\mathrm{tr.deg}(\Omega_1/F) = \mathrm{tr.deg}(\Omega_2/F)$.*

Example 1.61. Contrary to $\mathbb{R}$, whose only endomorphism is Id, $\mathbb{C}$ is isomorphic to infinitely many subfields of itself. Let $\mathcal{B}$ be a transcendental basis of $\mathbb{C}$ over $\mathbb{Q}$, which must be infinite. Then there is a bijection $\alpha : \mathcal{B} \to \mathcal{B}'$ with $\mathcal{B}'$ is a proper subset of $\mathcal{B}$. Let $\mathbb{C}'$ be the algebraic closure of $\mathbb{Q}(\mathcal{B}')$ then $\mathbb{C} \cong \mathbb{C}'$.

2 Galois theory

2.1 Finite Galois correspondence

Definition 2.1. An extension E/F is called **Galois** if it is normal and separable. The group $\mathrm{Aut}_F(E)$ is called the **Galois group** of E over F, which is denoted by $\mathrm{Gal}(E/F)$.

Lemma 2.2. *Let E/F be a finite Galois extension. Then $|\mathrm{Gal}(E/F)| = [E : F]$.*

Proof. Separability implies $|\hom_F(E, \overline{F})| = [E : F]$. Normality implies $\hom_F(E, \overline{F}) = \mathrm{Aut}_F(E)$. □

For a given extension E/F we introduce a pair of basic operations:

- To each subgroup H of $\mathrm{Aut}_F(E)$ we attach the corresponding **fixed field** E^H:
$$E^H := \{\alpha \in E : \forall \tau \in H, \tau(\alpha) = \alpha\}.$$
- To any subextension K/F of E we attach the subgroup $\mathrm{Aut}_K(E)$ of $\mathrm{Aut}_F(E)$.

Obviously we have the relation relation:

$$H_1 \subset H_2 \Rightarrow E^{H_2} \subset E^{H_1}$$

$$K_1 \subset K_2 \Rightarrow \mathrm{Aut}_{K_2}(E) \subset \mathrm{Aut}_{K_1}(E).$$

Lemma 2.3. *Let $E/K/F$ be a tower a field extension, then for $\sigma \in \mathrm{Aut}_F(E)$ we have*

$$\mathrm{Aut}_{\sigma(K)}(E) = \sigma \mathrm{Aut}_K(E)\sigma^{-1}$$

Lemma 2.4. *For a Galois extension E/F we have $E^{\mathrm{Gal}(E/F)} = F$, and the map $K \mapsto \mathrm{Aut}_K(E) = \mathrm{Gal}(E/K)$ is injective.*

Proof. Obviously $F \subset E^{\mathrm{Gal}(E/F)}$. Take $x \in E^{\mathrm{Gal}(E/F)}$, and denote its minimal polynomial by P_x. Then P_x has no multiple roots and splits into linear factors. Choose a root y of P_x then there is a canonical isomorphism $\iota : F(x) \to F(y)$. We can extend it to some $\sigma \in \mathrm{Gal}(E/F)$ which sends x to y. We immediately conclude that $y = x$ and so P_x is linear. □

Lemma 2.5 (E.Artin)**.** *Let E be a field, H a finite subgroup of $\mathrm{Aut}(E)$, then E/E^H is Galois and $\mathrm{Gal}(E/E^H) = H$.*

Proof. Take $x \in E$ and let $\mathcal{O} = \{\tau(x) : \tau \in H\}$, i.e. the orbit of x under H. Let $Q_x(X) = \prod_{y \in \mathcal{O}}(X - y)$, then $Q_x \in E^H(X)$ and $Q_x(x) = 0$. Since Q_x splits over E and has no multiple roots, we know that E/E^H is Galois. Moreover $\deg Q_x = |\mathcal{O}| \leq |H|$.

Obviously $H \leq \mathrm{Gal}(E/E^H)$. It suffices to show that $[E : E^H] \leq |H|$. We know that for any $x \in E$, $[E^H(x) : E^H] \leq |H|$. Take that $x \in E$ such that $[E^H(x) : E^H]$ is maximal, then we must have $E = E^H(x)$. Otherwise take $y \in E - E^H(x)$ then we have

$$E^H(x, y) \supsetneq E^H(x) \supset E(H)$$

However, since $E^H(x, y)$ is finite separable we can write it as the form $E^H(z)$ which contradicts with the choice of x. □

Theorem 2.6 (Finite Galois correspondence)**.** *Let E/F be a finite Galois extension.*

1. *There are mutually inverse bijections:*

$$\begin{aligned} \{\textit{intermediate fields}\} &\xleftrightarrow{\sim} \{\textit{subgroups of}\,\mathrm{Gal}(E/F)\} \\ E/K/F &\longmapsto \mathrm{Gal}(E/K) \\ E^H &\longleftarrow\!\shortmid\, H \leq \mathrm{Gal}(E/F) \end{aligned}$$

   which are order-reversing,

2. *For any intermediate field K and $\sigma \in \mathrm{Gal}(E/F)$, we have*

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

   the extension K/F is Galois if and only if $\mathrm{Gal}(E/K) \triangleleft \mathrm{Gal}(E/F)$,

3. *Furthermore, we have a bijection*

$$\Phi : \mathrm{Gal}(E/F)/Gal(E/K) \xrightarrow{\sim} \hom_F(K, E)$$
$$\sigma \cdot \mathrm{Gal}(E/K) \longmapsto \sigma|_K$$

between pointed sets. It induces a group isomorphism $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \xrightarrow{\sim} \mathrm{Gal}(K/F)$ *when* K/F *is Galois.*

Proof. The first two statements are simple translations of Lemma 2.4, 2.5 and 2.3. For third statement, σ, σ' satisfies $\sigma|_K = \sigma'|_K$ if and only if $\sigma^{-1}\sigma'|_K = \mathrm{Id}_K$ so Φ is injective. Surjectivity follows from Proposition 1.27. $\square$

Theorem 2.7. *Let* $E_1, E_2 \subset \overline{F}$ *be subfields and* $E_1/F, E_2/F$ *be Galois extensions. Then the canonical embedding* $\iota : \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$ *is an isomorphism if and only if* $E_1 \cap E_2 = F$.

Proof. $\Leftarrow$: when $E_1 \cap E_2 = F$, we can construct a reverse map $\chi : \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F) \to \mathrm{Gal}(E_1E_2/F)$ by sending (σ, τ) to $\tilde{\sigma}\tilde{\tau}$. Here $\tilde{\tau}$ is the unique field automorphism such that $\tilde{\tau}|_{E_2} = \tau$ and $\tilde{\tau}|_{E_1} = \mathrm{Id}$. Such an extension is possible only when $E_1 \cap E_2$ is trivial. $\tilde{\sigma}$ is defined by a similar extension. Obviously $\tilde{\tau}$ and $\tilde{\sigma}$ commute with each other so χ is really a group homomorphism. It is direct to see that χ and ι are reverse to each other.

$\Rightarrow$: If (σ, τ) lies in the image of ι, then $\sigma|_{E_1 \cap E_2} = \tau|_{E_1 \cap E_2}$. Since ι is an isomorphism, for all $(\sigma, \tau) \in \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$ we have $\sigma|_{E_1 \cap E_2} = \tau|_{E_1 \cap E_2}$ and thus $\sigma|_{E_1 \cap E_2} = \tau|_{E_1 \cap E_2} = \mathrm{Id}$. So $\mathrm{Gal}(E_1E_2/F)|_{E_1 \cap E_2} = \mathrm{Id}$. Therefore $E_1 \cap E_2 = F$. $\square$

The converse of the above theorem is also true:

Theorem 2.8. *Let* E/F *be an Galois extension with Galois group* G*. Suppose that there are subgroups* $H_1, H_2 \leq G$ *such that* $G = H_1 \times H_2$*. Let* $E_1 = E^{H_1}$, $E_2 = E^{H_2}$ *then we have*

1. E_1/F *and* E_2/F *are Galois extensions such that* $\mathrm{Gal}(E_1/F) = H_2$, $\mathrm{Gal}(E_2/F) = H_1$;

2. $E_1E_2 = E$;

3. $E_1 \cap E_2 = F$.

Proof. The first statement is obvious since H_1 and H_2 are normal subgroups of G and $G/H_1 \cong H_2$, $G/H_2 \cong H_1$. The second statement follows from the fact that $H_1 \cap H_2 = 1$. The third statement follows from the fact $H_1H_2 = G$. $\square$

2.2 Infinite Galois correspondence

Definition 2.9 (Krull topology)**.** For a Galois extension E/F, we can equip $\mathrm{Gal}(E/F)$ with a topology structure such that the neighbourhood basis at an arbitrary element σ has the following form:

$$\sigma\mathrm{Gal}(E/K), \quad K/F : \text{finite Galois subextension}$$

This topology structure is called the **Krull topology** over $\mathrm{Gal}(E/F)$.

Lemma 2.10. *For any Galois extension E/F, the topological group $\mathrm{Gal}(E/F)$ is a profinite group in the sense of Definition A.7. More explicitly, there is an isomorphism of topological groups*

$$\mathrm{Gal}(E/F) \xrightarrow{\sim} \varprojlim_{K/F} \mathrm{Gal}(K/F)$$

Here the limit is taken over all finite Galois subextensions K/F.

Lemma 2.11. *For any finite subextension K/F with $K \subset E$, the subgroup $\mathrm{Gal}(E/K)$ is open.*

Proof. Firstly we notice that for every $\alpha \in E$, the stabilizer $\mathrm{Stab}(\alpha)$ is open. Indeed, α lies in some finite Galois extension L/F. For example we may take L to be the normal closure of $F(\alpha)$. So $\mathrm{Stab}(\alpha) \supset \mathrm{Gal}(E/L)$ and $\mathrm{Gal}(E/L)$ is open in $\mathrm{Gal}(E/F)$. So $\mathrm{Stab}(\alpha)$ is still open by Lemma A.5. Since K/F is finite we may write $K = F(x_1, ..., x_n)$ and so $\mathrm{Gal}(E/K) = \bigcap_{i=1}^n \mathrm{Stab}(x_i)$ and so $\mathrm{Gal}(E/K)$ is open. $\square$

Lemma 2.12. *For any subextension K/F, the subgroup $\mathrm{Gal}(E/K)$ is closed.*

Proof. Similar to Lemma 2.11. Note that $\mathrm{Stab}(\alpha)$ is also closed by Lemma A.5. Then $\mathrm{Gal}(E/K) = \bigcap_{x \in K} \mathrm{Stab}(x)$. $\square$

Lemma 2.13. *The topological group $G := \mathrm{Gal}(E/F)$ satisfies the following property*

1. *G is a compact Hausdorff space. When E/F is finite then it is equipped with discrete topology,*
2. *Any open subgroup H is also closed such that $(G : H) < \infty$,*
3. *If we equip E with discrete topology, then the action map $\mathrm{Gal}(E/F) \times E \to E$ is continuous.*

Lemma 2.14. *Let H be a subgroup of G. Then $\mathrm{Gal}(E/E^H) = \overline{H}$ is the closure of H.*

Proof. The direction $\overline{H} \subset \mathrm{Gal}(E/E^H)$ is easy. Let $\sigma \in \mathrm{Gal}(E/E^H)$, by the definition of Krull topology it suffices to show that for every intermediate field K of E/F such that K/F is finite Galois, $\sigma\mathrm{Gal}(E/K) \cap H \neq \emptyset$. Let $\phi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$ be the restriction map. Since $\phi(\sigma)$ fixes $K^{\phi(H)} = K \cap E^H$, we know that $\phi(\sigma) \in \phi(H)$. $\square$

Corollary 2.15. *Let H be a closed subgroup of G, then* $\mathrm{Gal}(E/E^H) = H$.

Theorem 2.16 (Infinite Galois correspondence)**.** *Let E/F be Galois. Then*

1. *There are mutually inverse bijections:*

$$\begin{aligned} \{\textit{intermediate fields}\} &\overset{\sim}{\longleftrightarrow} \{\textit{closed subgroups of}\, \mathrm{Gal}(E/F)\} \\ E/K/F &\longmapsto \mathrm{Gal}(E/K) \\ E^H &\longleftarrow H \leq \mathrm{Gal}(E/F) \end{aligned}$$

   which are order-reversing, and G-equivariant. As a result normal closed subgroups correspond to Galois subextensions.

2. *For any intermediate fields K there is a bijection*

$$\begin{aligned} \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) &\xrightarrow{\sim} \hom_F(K, E) \\ \sigma \cdot \mathrm{Gal}(E/K) &\longmapsto \sigma|_K \end{aligned}$$

   Moreover when K/F is Galois, there is an isomorphism of topological groups

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \xrightarrow{\sim} \mathrm{Gal}(K/F)$$

   where the LHS is equipped the quotient topology.

3. *Open subgroups correspond to finite subextensions.*

3 Computation of Galois group

3.1 Galois group of polynomials

Let $f \in F[X]$ be a separable polynomial and E/F be the splitting field of F. Then E/F is Galois. We use G_f to denote its Galois group. Since G permute all roots of f, it can be viewed as a subgroup of S_n where $n = \mathrm{deg} f$.

Theorem 3.1. *G_f acts transitively on the set of roots of f if and only if $f(X)$ is irreducible.*

Proof. Two elements are in the same orbit if and only if they have the same minimal polynomial. □

Definition 3.2. Consider a monic polynomial $f(X) = X^n + a_{n-1}X^{n-1} + ... + a_0$ and $f(X) = \prod_{i=1}^n (X - \alpha_i)$ in some splitting field. Set

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j), \qquad D(f) = (\Delta(f))^2 = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

$D(f)$ is called the **discriminant** of f.

$D(f)$ is nonzero if and only if f is separable.

Lemma 3.3. *Let $f \in f[X]$ be a separable polynomial and let $\sigma \in G_f$. Then:*

1. $\sigma\Delta(f) = \mathrm{sign}(\sigma)\Delta(f)$, *where* $\mathrm{sign}(\sigma)$ *is the signature of* σ.
2. $\sigma D(f) = D(f)$.

Theorem 3.4. *Let $f(X) \in F[X]$ be separable of degree n. Let E be a splitting field of F and let G_f be the Galois group. Then*

1. $D(f) \in F$.
2. *The subfield of E corresponding to $A_n \cap G_f$ is $F[\Delta(f)]$. Hence by finite Galois correspondence (Theorem 2.6) we have $G_f \subset A_n \Leftrightarrow \Delta(f) \in F \Leftrightarrow D(f) \in F^{\times 2}$.*

Proof. Obvious from the above lemma. □

3.2 Quartic polynomials

Galois group of quadratic and cubic polynomials are easy to compute. We consider quartic polynomials here. In this section we use V to denote the following normal subgroup of S_4:

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

Let $f(X)$ be a separable quartic polynomial and E be a splitting field of $f(X)$ such that $f(X) = \prod(X - \alpha_i)$ in E. Consider the partially symmetric elements

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4$$
$$\beta = \alpha_1\alpha_3 + \alpha_2\alpha_4$$
$$\gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

The group S_4 permute $\{\alpha, \beta, \gamma\}$ transitively. The stabilizer of each of α, β, γ must therefore be a subgroup of index 3 in S_4, and hence has order 8.

Lemma 3.5. *The fixed field of $G_f \cap V$ is $F[\alpha, \beta, \gamma]$. Hence $F[\alpha, \beta, \gamma]$ is Galois over F with Galois group $G_f/G_f \cap V$.*

Let $M = F[\alpha, \beta, \gamma]$, and let $g(X) = (X - \alpha)(X - \beta)(X - \gamma) \in M[X]$, which is called the **resolvent cubic** of f. Obviously $g(X)$ is fixed by G_f and thus it has coefficients in F.

Theorem 3.6. *Let $f \in F[X]$ be an irreducible separable quartic polynomial and $M = F[\alpha, \beta, \gamma]$. Then*

- *If $[M : F] = 1$, then $G_f = V$;*
- *If $[M : F] = 2$, then G_f is conjugate to C_4 or D_4; moreover, in this case, G is conjugate to D_4 if and only if f remains irreducible in M.*
- *If $[M : F] = 3$, then $G = A_4$;*

- *If* $[M : F] = 6$, *then* $G = S_4$.

Example 3.7. Assume that $\mathrm{char}(F) \neq 2$. Let $P(X) = X^4 + cX^2 + e \in F[X]$ be an irreducible polynomial. Then,

1. If e is a square in F, then $G_P = V$.
2. If $e(c^2 - 4e)$ is a square in F, then G is conjugate to C_4.
3. If neither e nor $e(c^2 - 4e)$ is a square in F, then G is conjugate to D_4.

Example 3.8. Let $P(X) = X^4 + pX + p$ over $\mathbb{Q}$ with p a prime. By Eisenstein's criterion we see that $P(X)$ is irreducible. The resolvent cubic is $Q(X) = X^3 - 4pX - p^2$. When $p \neq 3, 5$, $Q(X)$ is irreducible over $\mathbb{Z}$, and hence is irreducible over $\mathbb{Q}$. $\Delta(Q) = p^3(256 - 27p) \notin (\mathbb{Q}^\times)^2$, thus $G_P = S_4$. When $p = 3$, $Q(X) = X^3 - 12X - 9 = (X + 3)(X^2 - 3X - 3)$. Then $M = \mathbb{Q}(\sqrt{21})$ and $[M : \mathbb{Q}] = 2$. In this case $P(X)$ is irreducible over M and so G_P is conjugate to D_4. When $p = 5$, $P(X) = X^4 + 5X + 5$ and $Q(X) = (X - 5)(X^2 + 5X + 5)$. We have $[M : \mathbb{Q}] = 2$ but this time $P(X) = (X^2 + \sqrt{5}X + \frac{5-\sqrt{5}}{2})(X^2 - \sqrt{5}X + \frac{5+\sqrt{5}}{2})$ is reducible over M. Hence G_P is conjugate to C_4.

4 Applications of Galois theory

4.1 Finite fields

Every finite field must have positive characteristic, otherwise it would contain a copy of $\mathbb{Q}$. Let us fix a primes number p in what follows.

Theorem 4.1. *Every finite fields of characteristic p has cardinality $q = p^m$ for some $m \geq 1$. Moreover, there exits a finite field with q elements for every p-power q, which is unique up to isomorphism.*

Proof. As a matter of fact, for a p-power q and $|E| = q$, E can be identified with the splitting field of $X^q - X$ over $\mathbb{F}_p$. □

We denote a finite field of cardinality q by $\mathbb{F}_q$. The automorphism $\mathrm{Fr}_q : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^q$ is called the **Frobenius automorphism**.

Theorem 4.2. *Let $E/\mathbb{F}_q$ be an extension of finite fields with characteristic p. Then E/F is Galois and* $\mathrm{Gal}(E/F)$ *is the cyclic group generated by* Fr_q.

Proof. Let $[E : F] = n$. It suffices to show that $\mathrm{Fr}_q \in \mathrm{Gal}(E/\mathbb{F}_q)$ is an element of order n. We know that any element in E satisfies $x^{q^n} = x$ so $\mathrm{Fr}_q^n = \mathrm{Id}_E$. If there is some $d|n$ such that $x^{q^d} = x$. However there are at most q^d elements satisfying this equation so $d = n$. □

Proposition 4.3. *Let F be a finite field and $|F| = q$. Let l be a prime number. Then there are $\frac{q^l - q}{l}$ distinct monic irreducible polynomials of degree l in $F[X]$.*

Proof. View F as a subfield of E with $|E| = q^l$. Introduce the following equivalence relation over $E \setminus F$: $a \sim b$ if and only if a and b share the same minimal polynomial. Then we have

1. Each equivalence class has exactly l distinct elements;
2. There is a canonical bijection between the quotient set $(E \setminus F)/\sim$ and the set of monic irreducible polynomials in $F[X]$.

$\square$

Proposition 4.4. *Let E/F be an extension of finite fields, then the norm map $N_{E/F} : E^\times \to F^\times$ is surjective.*

Proof. Let $|F| = q$ and $[E : F] = l$. Then

$$N_{E/F}(a) = \prod_{i=0}^{l-1} a^{q^i} = a^{\frac{q^l-1}{q-1}}.$$

The kernel of $N_{E/F}$ can be identified with the set of roots of the equation $x^{\frac{q^l-1}{q-1}} = 1$, and so $|\mathrm{Ker}(N_{E/F})| \leq \frac{q^l-1}{q-1}$. So $|\mathrm{Im}(N_{E/F})| \geq (q^l-1)/\frac{q^l-1}{q-1} = q-1$. $\square$

4.2 Cyclotomic extension

Definition 4.5. Fix an algebraic closure $\overline{F}/F$ and $n \in \mathbb{Z}_{\geq 1}$. An element ζ satisfying $\zeta^n = 1$ is called an **n-th root of unity**. Let $\mu_n(F) \subset F^\times$ denote the group of n-th roots of unity in F. We say $\zeta \in F^\times$ is a **primitive n-th root of unity** if it has order n.

If ζ is a primitive n-th root of unity of F, then $\mathrm{char}(F) \nmid n$.

Proposition 4.6. *Let $F(\zeta_n)/F$ be a field extension with ζ_n a primitive n-th root of unity. Then $F(\zeta_n)/F$ is the splitting field of the separable polynomial $P(X) = X^n - 1$ over F, and thus $F(\zeta_n)/F$ is Galois. Moreover we have a group embedding $G = \mathrm{Gal}(F(\zeta_n)/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. $\forall \sigma \in G$, $\sigma(\zeta_n)$ is still a generator of $\mu_n(F)$, so that $\sigma(\zeta_n) = \zeta_n^a$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. $\square$

Definition 4.7. The n-th **cyclotomic polynomial** is defined as $\Phi_n(X) = \prod_\zeta (X - \zeta)$ where ζ runs over the set of n-th primitive root of unity. It is obvious that $\deg(\Phi_n) = \varphi(n)$.

Lemma 4.8. *The following equality holds:*

$$\prod_{d|n} \Phi_d = X^n - 1.$$

Proof. It follows from the formula $X^n - 1 = \prod_{\zeta \in \mu_n}(X - \zeta)$. $\square$

Definition 4.9. We have the following:

$$\Phi_n = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$$

where μ is the Möbius function, see Theorem B.4.

Proof. By applying Möbius inversion formula. $\square$

Lemma 4.10. *Let F be a field of characteristic 0 or p not dividing n, and let ζ be a primitive n-th root of unity in some extension of F. TFAE*

1. *The n-th cyclotomic polynomial Φ_n is irreducible,*
2. *The degree $[F[\zeta] : F] = \varphi(n)$,*
3. *The injective homomorphism*

$$\mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

   is an isomorphism.

Theorem 4.11. *Φ_n is irreducible over $\mathbb{Q}[X]$.*

Corollary 4.12. $\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Example 4.13. Let $E = \mathbb{Q}(\zeta_p)$ with $p \neq 2$ a prime. Then $N_{E/\mathbb{Q}}(1 - \zeta_p) = \prod_{i=1}^{p-1}(1 - \zeta_p^i) = \Phi_p(1) = p$.

Given $m, n \in \mathbb{Z}_+$, let (m, n) denote their greatest common divisor and $[m, n]$ denote their least common multiple.

Proposition 4.14. *We have $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{[m,n]})$.*

Proof. Let ζ_{mn} be a primitive mn-th root of unity, then we choose $\zeta_m = (\zeta_{mn})^n$ and $\zeta_n = (\zeta_{mn})^m$. Therefore,

$$\zeta_m^{\mathbb{Z}}\zeta_n^{\mathbb{Z}} = \zeta_{mn}^{(m,n)\mathbb{Z}} = \zeta_{mn/(m,n)}^{\mathbb{Z}} = \zeta_{[m,n]}^{\mathbb{Z}}.$$

$\square$

Proposition 4.15. *If $(m, n) = 1$, then $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.*

Proof. Define $G_N := \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Then there is a canonical map $\iota : G_{mn} \cong (\mathbb{Z}/mn\mathbb{Z})^\times \to G_m \times G_n \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Since $(m, n) = 1$ by Chinese remainder theorem ι is an isomorphism. We conclude by Theorem 2.7. $\square$

Lemma 4.16. *Let F be a field containing a primitive n-th root of unity. Then*

$$\sum_{\zeta\in\mu_n^{\text{prim}}}\zeta=\mu(n),\qquad \prod_{\zeta\in\mu_n^{\text{prim}}}\zeta=\begin{cases}1 & n\neq 2,\\ -1 & n=2.\end{cases}$$

where μ_n^{prim} denotes the set of primitive n-th root of unity in F and $\mu(n)$ is the Möbius function.

Proof. Let $f(n)=\sum_{\zeta\in\mu_n^{\text{prim}}}\zeta$. Then

$$\sum_{d|n}f(d)=\sum_{\zeta\in\mu_n}\zeta=\iota(n)$$

for the definition of ι, see Theorem B.4. We see that $f(n)=\mu(n)$ by the definition of Möbius function. $\square$

Theorem 4.17. *Let F be a field and $E=F(\zeta_n)$, where ζ_n is a primitive n-th root of unity, satisfying $[E:F]=\varphi(n)$. Then $\mu_n^{\text{prim}}(E)$ is F-linearly independent if and only if n is square-free.*

Proof. $\Rightarrow$: Assume that n is not square-free then $\mu(n)=0$. By above lemma we see that $\sum_{\zeta\in\mu_n^{\text{prim}}(E)}\zeta=\mu(n)=0$, thus $\mu_n^{\text{prim}}(E)$ is not F-linearly independent.

$\Leftarrow$: Since n is square-free, decompose n as $n=p_1p_2...p_k$ with $p_i\neq p_j$, $i\neq j$. We make induction on k. For $k=1$, that is, $n=p$ is a prime, we know that $[F(\zeta_p):F]=\varphi(p)=p-1$. Since $(1,\zeta_p,\zeta_p^2,...,\zeta_p^{p-2})$ is linearly independent, $(\zeta_p,\zeta_p^2,...,\zeta_p^{p-2},\zeta_p^{p-1})$ must also be linearly independent. Now our conclusion follows from the fact the $\mu_m^{\text{prim}}\mu_n^{\text{prim}}=\mu_{mn}^{\text{prim}}$ if $(m,n)=1$. $\square$

4.3 Hilbert's theorem 90

Lemma 4.18. *Let E/F be a finite Galois extension and let $G=\mathrm{Gal}(E/F)$. For any $\beta\in E$, $\mathrm{tr}_{E/F}(\sigma(\beta)-\beta)=0$. For any $\beta\in E^\times$, $N_{E/F}(\sigma(\beta)/\beta)=1$.*

Proof. Direct from Corollary 1.45. $\square$

A natural question is to ask whether the reverse direction of the lemma is true.

Definition 4.19. Let E/F be a Galois extension. We say that E/F is

- **abelian**, if $\mathrm{Gal}(E/F)$ is an abelian group,
- **cyclic**, if $\mathrm{Gal}(E/F)$ is a cyclic group.

An abelian extension E/F is called of **exponent** n if $\mathrm{Gal}(E/F)$ is a group of exponent n.

Theorem 4.20 (Hilbert's Theorem 90)**.** *Let E/F be a finite cyclic extension and let $\sigma\in\mathrm{Gal}(E/F)$ be a generator.*

1. *If* $\alpha \in E$ *satisfies* $\mathrm{tr}_{E/F}(\alpha) = 0$*, then* $\alpha = \sigma(\beta) - \beta$ *for some* $\beta \in E^\times$*.*

2. *If* $\alpha \in E^\times$ *satisfies* $N_{E/F}(\alpha) = 1$*, then* $\alpha = \sigma(\beta)/\beta$ *for some* $\beta \in E^\times$*.*

We will use some terminology from group cohomology, see Appendix C.

Lemma 4.21. *Let* $G = \langle\sigma\rangle$ *be a cyclic group of order* n*. Then we have an isomorphism* $Z^1(G, M) \xrightarrow{\sim} \mathrm{Ker}(N)$*, where* $N : M \to M$ *is defined by* $N(m) = \sum_{g \in G} gm$*. The isomorphism moreover induces an isomorphism* $H^1(G, M) \cong \mathrm{Ker}(N)/\mathrm{Im}(\sigma - \mathrm{Id})$*.*

For $M = E$ where E/F is a cyclic Galois extension, then we have $N = \mathrm{tr}_{E/F}$. For $M = E^\times$ we have $N = N_{E/F}$. So we have reduced Hilbert's Theorem 90 to the following theorem.

Theorem 4.22. *Let* E/F *be a finite Galois extension and let* $G = \mathrm{Gal}(E/F)$*. Then* $H^1(G, E) = 0$ *and* $H^1(G, E^\times) = 1$*.*

Proof. Let $f : G \to E^\times$ be a crossed homomorphism. Note that this means $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$ for all $\sigma, \tau \in G$. Apply Theorem 1.46 to $\Gamma = E^\times$, $\sum_{\tau \in G} f(\tau)\tau : E^\times \to E$ is not the zero map. There exists $x \in E^\times$ such that $y := \sum_{\tau \in G} f(\tau)\tau(x) \neq 0$. Then, for every $\sigma \in G$,

$$\sigma(y) = \sum_{\tau \in G} \sigma(f(\tau))\sigma\tau(x) = \sum_{\tau \in G} f(\sigma\tau)f(\sigma)^{-1}\sigma\tau(x) = f(\sigma)^{-1}y.$$

In other words, $f(\sigma) = \sigma(y^{-1})/y^{-1}$. □

4.4 Cyclic extensions

Let F be a field containing a primitive n-th root of unity with $n \geq 2$, and write μ_n for the group of n-th roots of unity in F. Then μ_n is a cyclic subgroup of $F^\times$ of order n with generator, say, ζ. In this section we classify the cyclic extensions of degree n of F.

Consider a field $E = F(\alpha)$ generated by an element α whose n-th power (but no smaller power) is in F. Then α is a root of $X^n - a$ with $a \notin F^{\times n}$.

Lemma 4.23. *The extension* $F(\alpha)/F$ *is Galois. The Galois group is cyclic and is isomorphic to* μ_n*.*

Proof. The remaining roots are the elements $\zeta^i\alpha$, $1 \leq i \leq n-1$. Since these all lie in E, E is a Galois extension. For every $\sigma \in G = \mathrm{Gal}(E/F)$, $\sigma(\alpha)$ is also a root of $X^n - a$, and so $\sigma(\alpha) = \zeta^i\alpha$ for some i. Hence $\sigma(\alpha)/\alpha \in \mu_n$. The map

$$G \to \mu_n, \quad \sigma \mapsto \sigma(\alpha)/\alpha$$

is a homomorphism. It is injective because α generates E over F. If it is not surjective then $\alpha^d \in F$ for some $d | n, d < n$ which leads to a contradiction. □

The converse of the above lemma is also true, thus we have a complete understanding of cyclic extensions:

Proposition 4.24. *Let F be a field containing a primitive n-th root of unity with $n \geq 2$. Let E be a Galois extension of F with cyclic Galois group of order n, then $E = F(\alpha)$ for some α with $\alpha^n \in F$ and no smaller powers of α lies in F.*

Proof. Let σ generate G and let ζ generate μ_n. As $1, \sigma, ..., \sigma^{n-1}$ are distinct homomorphisms $F^\times \to F^\times$, Theorem 1.46 shows that $\sum_{i=0}^{n-1} \zeta^i \sigma^i$ are distinct homomorphisms is not the zero function, and so there is a γ such that $\alpha := \sum \zeta^i \sigma^i \gamma \neq 0$. Now $\sigma\alpha = \zeta^{-1}\alpha$.

□

4.5 Kummer theory and Artin-Schreier theory

Let F be a field containing a primitive n-th root of unity and E/F be a finite Galois extension with Galois group G. From the exact sequence

$$1 \to \mu_n \longrightarrow E^\times \longrightarrow E^{\times n} \to 1$$

we obtain a cohomology sequence

$$1 \to \mu_n \longrightarrow F^\times \longrightarrow F^\times \cap E^{\times n} \to H^1(G, \mu_n) \to 1$$

Thus we obtain an isomorphism

$$F^\times \cap E^{\times n}/F^{\times n} \to \hom(G, \mu_n).$$

Theorem 4.25 (Classical Kummer theory)**.** *The map*

$$E \mapsto F^\times \cap E^{\times n}$$

defines a one-to-one correspondence between the sets of

1. *finite abelian extensions of F of exponent n contained in some fixed algebraic closure Ω of F, and*

2. *subgroups B of $F^\times$ containing $F^{\times n}$ as a subgroup of finite index.*

The extension corresponding to B is $F[B^{1/n}]$, the smallest subfield of Ω containing F and an n-th root of each element of B.

Let F be a field of characteristic $p > 1$. Let E/F be a finite Galois extension with Galois group G. Let $P(X) = X^p - X$. We have a short exact sequence of G-modules

$$0 \to \mathbb{F}_p \to E \xrightarrow{P} P(E) \to 0$$

which induces the long exact sequence

$$0 \to \mathbb{F}_p \to F \xrightarrow{P} P(E) \cap F \to H^1(G, \mathbb{F}_p) \to H^1(G, E) = 0.$$

Theorem 4.26 (Artin-Schreier theory)**.** *Let F^{sep} be a separable closure of F. Then the map $E \mapsto P(E) \cap F$ induces a bijective correspondence between*

1. *E/F finite separable abelian extension of exponent p*
2. *Subgroups B of F containing $P(F)$.*

The other direction of this correspondence is given by

$$B \mapsto F(P^{-1}(\Delta)).$$

Example 4.27. For any $a \in \mathbb{F}_p^\times$, $P(X) = X^p - X - a$ is irreducible in $\mathbb{F}_p(X)$. If α is a root of P, then $\alpha, \alpha+1, ..., \alpha+p-1$ are p distinct roots of $P(X)$, and so $\mathbb{F}_p(\alpha)$ is the splitting field of $P(X)$. The Galois group $\text{Gal}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ is cyclic which is generated by $\sigma : \alpha \mapsto \alpha + 1$.

4.6 Solvablity by radicals

Recall that a group G is **solvable** if there exists a composition series $G = G_0 > G_1 > ... > G_m = 1$ such that $G_{i+1} \lhd G_i$ has abelian quotient.

Definition 4.28. Let E/F be a finite separable extension.

1. We say that E/F is a **radical** extension if there exists a tower of extensions $F = E_0 \subset E_1 \subset ... \subset E_m$ such that $E \subset E_m$ and that for each $0 \leq i \leq m-1$, $E_{i+1} = E_i(\alpha)$, where one of the following holds
   (a.) α is a root of $X^n - a$, $a \in E_i^\times$ and $\text{char}(F) \nmid n$;
   (b.) α is a root of $X^p - X - a$, $a \in E_i$ and $p = \text{char}(F) > 0$.
2. We say that E/F is a **solvable** extension if $\text{Gal}(K/F)$ is a solvable group, where K/F denote the Galois closure of E/F.

Theorem 4.29 (É.Galois)**.** *A finite separable extension E/F is solvable if and only if it is radical.*

A Profinite groups

A.1 Topological groups

Definition A.1. A **topological group** G is a group G equipped with a topological structure such that the multiplication map $m : G \times G \to G$ and the inverse map $i : G \to G$ are both continuous.

Definition A.2. Let TopGrp be the category of topological groups and continuous group homomorphisms.

Lemma A.3. *The left translation $l_g : h \mapsto gh$ and the right translation map $r_g : h \mapsto hg$ are both auto-homeomorphisms of G for each $g \in G$.*

By the lemma, the topology structure of G is completely determined by a neighbourhood basis of the neutral element 1.

Lemma A.4. *Let G be a topological group, TFAE*

1. *G is Hausdorff,*
2. *$\{1\} \subset G$ is a closed subset,*
3. *$\bigcap_{1 \in U, U \text{ open}} U = \{1\}$.*

Lemma A.5. *Let G be a topological group. Then*

1. *If $H \leq G$ is a topological subgroup and $U \subset H$ with U open, then H is open.*
2. *Any open subgroup of G is closed and any closed subgroup of G of finite index is open.*
3. *Any open subgroup H of a compact topological group G has finite index.*

Let I be a category and $I^{\mathrm{op}} \to \mathrm{TopGrp}$ be a functor. Denote the limit of the functor by $\varprojlim_i G_i$. Since any limit is an equalizer of a product, we can view $\varprojlim_i G_i$ as a sub-topological group of the product $\prod_{i \in I} G_i$. We denote the projections $\varprojlim_i G_i \to G_k$ by p_k.

Lemma A.6. *The topological group $\varprojlim_i G_i$ has a neighbourhood basis at 1 of the following form:*

$$\mathcal{U}_{I_0} = \bigcap_{i \in I_0} p_i^{-1}(U_i)$$

where $I_0 \subset I$ is a finite subset and $1 \in U_i$ is open in G_i. If I is filtered, it suffices to take the upper bound j of I_0.

Proof. This is simply the definition of product topology. □

A.2 Profinite groups

Definition A.7. A topological group is called **profinite** if it has the form $\varprojlim_{i \in I} G_i$ such that I is a filtered category and G_i is a finite group equipped with the discrete topology.

Proposition A.8. *A group is profinite if and only if it is compact Hausdorff and totally disconnected.*

Proof. "$\Rightarrow$" is easy. Each G_i is compact, Hausdorff, and totally disconnected. Thus so is $\prod_{i \in I} G_i$ and its closed subset $\varprojlim_{i \in I} G_i$.

"$\Leftarrow$" is much more difficult. Since G is totally disconnected and locally compact, the open subgroups of G form a base of neighbourhoods of 1. Such a subgroup U has finite index in G since G is compact; hence its conjugates gUg^{-1} are finite in number and their intersection V is both normal and open in G. Such V's are thus a base of neighbourhoods of 1; the map $G \to \varprojlim G/V$ is injective, continuous and its image is dense; a compactness argument then shows that it is an isomorphism. □

B Möbius inversion formula

Definition B.1. An **arithmetic function** is a function $f : \mathbb{N} \to \mathbb{C}$.

Definition B.2. Let f, g be arithmetic functions. Their **convolution** $f * g$ is defined as

$$(f * g)(n) := \sum_{ij=n} f(i)g(j)$$

Theorem B.3. *The set of arithmetic functions form an commutative monoid with convolution being the multiplication map.*

Proof. Commutativity and associativity are direct to check. The unit is defined as

$$\iota(n) := \begin{cases} 0, & \text{if } n \neq 1 \\ 1, & \text{if } n = 1 \end{cases}$$

□

Now let u be the constant arithmetic function valued at 1, i.e. $u(n) = 1$ for all $n \in \mathbb{N}$.

Theorem B.4. *u is an invertible arithmetic function. Its inverse is called the **Möbius function**, which is denoted by μ.*

Proof. Let $n = p_1^{k_1} ... p_m^{k_m}$ be the prime decomposition of n. Define μ as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^m & \text{if } k_i = 1 \ \forall i, \\ 0 & \text{otherwise.} \end{cases}$$

Now we show that $u * \mu = \iota$. That is $\sum_{d|n} \mu(d) = \iota(n)$. When $n = 1$ this is obvious. When $n > 1$ we write n as $n = p_1^{k_1} ... p_m^{k_m}$ then we have

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + (\mu(p_1) + ... \mu(p_m)) + \sum_{i<j} \mu(p_i p_j) + ... + \mu(p_1 ... p_m) \\ &= C_m^0 + (-1)C_m^1 + ... + C_m^m(-1)^m \\ &= (1-1)^m = 0. \end{aligned}$$

□

Corollary B.5 (Möbius inversion formula)**.** *Let f, g be arithmetic functions then $f = g * u \Leftrightarrow g = f * \mu$. More explicitly we have $f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\mu(n/d)$.*

Proof. It is a simple translation of the above theorem. □

C Group cohomology

Let G be a group, and A a left G-module. Let $C^n(G, A)$ be the abelian group of set maps $\hom_{\mathrm{Set}}(G^n, A)$ and $C^0(G, A) = A$, with coface maps $d^n : C^n(G, A) \to C^{n+1}(G, A)$ defined by

$$(d^n f)(g_1, ..., g_{n+1}) = g_1 f(g_2, ..., g_{n+1}) + \sum_{i=1}^{n} (-1)^{i+1} f(g_1, ..., g_i g_{i+1}, ..., g_{n+1}) + (-1)^{n+1} f(g_1, ..., g_n)$$

It can be easily checked that $d^{i+1} \circ d^i = 0$. Thus we can talk about its cohomology group. For our purpose we only consider $H^1(G, A)$. Let $Z^1(C, A) = \mathrm{Ker}(d^1)$ and $B^1(C, A) = \mathrm{Im}(d^0)$. Elements of $Z^1(C, A)$ are called **crossed homomorphisms**. They satisfy

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$$

for all $\sigma, \tau \in G$. A crossed homomorphism f is called **principal** if it lies in $B^1(C, A)$, i.e. it has the form $f(\tau) = \tau m - m$ for some $m \in A$. The first cohomology group $H^1(G, A)$ is simply $Z^1(C, A)/B^1(C, A)$.