Intoduction to Galois Theory

Nan An

November 16, 2022

Contents

1 Preliminaries

Remark 1.1. This section will befiefly list the preliminary definitions in fields and groups. Subgroups are often denoted by "$\leq$": $H \leq G$ means H is a subgroup of G.

Definition 1.2. Suppose G a group and $g_1, g_2 \in G$. Then $[g_1, g_2] := g_1^{-1} g_2^{-1} g_1 g_2$.

Definition 1.3 (Commutator Subgroups)**.** Suppose $H, K \leq G$. Then $[H, K] := \{[h, k] : h \in H, k \in K\}$ are called the commutator subgroup.

Definition 1.4 (Normal Series and Subnormal Series)**.** Suppose a sequence of subgroups of G:

$$G = G_1 \geq G_2 \geq \cdots \geq G_t \geq G_{t+1} = \{1\}$$

it is called a subnormal series if $G_i \triangleleft G_{i-1}$ for each i, and normal if $G_i \triangleleft G$ for each i.

Definition 1.5. Define $G^{(k)}$ via induction:

$$G^{(0)} = G, \quad G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$$

Definition 1.6 (Solvability of Groups)**.** If $\exists\, k$ such that $G^{(k)} = \{1\}$, then G is called solvable.

Proposition 1.7. Suppose an exact sequence of groups $0 \to A \to G \to B \to 0$, then G is solvable iff A and B are solvable.

Proof. Assume $A \triangleleft G$, $B = G/A$, let $\pi : G \to B$ the canonical projection. If G is solvable, since $A^{(k)} \subset G^{(k)}$, A is solvable. Obviously $\pi(G^{(k)}) = B^{(k)}$, therefore B is also solvable. Conversely, if $\exists\, k_1, k_2$ such that $A^{(k_1)} = B^{(k_2)} = \{1\}$, then $\pi(G^{(k_2)}) = 1$, therefore $G^{(k_2)} \subset A$, $G^{(k_1+k_2)} = \{1\}$. $\square$

Proposition 1.8. Suppose G is finite. Then G is a solvable group iff there exists a subnormal series of G:

$$G = G_1 \geq G_2 \geq \cdots G_s = \{1\}$$

such that G_i/G_{i+1} is an abelian group for each i.

Proof. One direction is trivial since $G^{(i)}/G^{(i+1)}$ is abelian. Conversely, G_{s-1} is abelian therefore solvable. By the exact sequence

$$0 \to G_{s-1} \to G_{s-2} \to G_{s-2}/G_{s-1} \to 0$$

G_{s-2} is solvable. By induction all G_i are solvable, therefore G is solvable. $\square$

Remark 1.9. G_i/G_{i+1} can also be assumed cyclic. Since $|G| < \infty$, $|G_i'/G_{i+1}'| \leq \infty$. Obviously $\mathbb{Z}_{p_n^{k_n-1}} \leq \mathbb{Z}_{p_n^{k_n}}$, therefore

$$G_i'/G_{i+1}' \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{k_i}} \geq \left(\bigoplus_{i=1}^{n-1} \mathbb{Z}_{p_i^{k_i}} \right) \oplus \mathbb{Z}_{p_n^{k_n-1}} = H$$

where $H \triangleleft G_i'/G_{i+1}'$, and $[G_i'/G_{i+1}' : H] = p_k$. Let $\pi : G_i' \to G_i'/G_{i+1}'$ the canonical projection and $H' = \pi^{-1}(H)$, then

$$G_i' \triangleright H' \triangleright G_{i+1}'$$

with $|G_i'/H'| = p_k$ and H'/G_{i+1}' an abelian group with smaller order. Therefore by keep adding H', such desired series can be found.

Proposition 1.10. S_n is solvable iff $n \leq 4$.

Proof. Obviously S_1, S_2 are solvable. S_3 is solvable because

$$S_3 \triangleright A_3 \triangleright \{1\}$$

S_4 is solvable because

$$S_4 \triangleright A_4 \triangleright K_4 \triangleright \{1\}$$

when $n \geq 5$, A_n is a non-abelian simple group, therefore unsolvable. Therefore S_n is unsolvable. $\square$

Remark 1.11. Suppose F is a field. The following theorem is listed without proof since it is well-known.

Proposition 1.12. If F is a finite field, then $F \backslash \{0\}$ is a cyclic group.

Theorem 1.13. $F[x]$ is an Euclid ring, therefore $F[x]$ is a PID.

Proposition 1.14. Give $f(x) \in F[x]$ and $a \in F$, $(x - a) | f(x)$ iff $f(a) = 0$.

Remark 1.15. Such a in the above proposition is called a root of $f(x) \in F$.

2 Algebraic Extensions

Definition 2.1 (Field Extensions)**.** Give a set S,

$$F[S] = \{ \sum_{i_1,\cdots,i_n \geq 0}^{<\infty} a_{i_1\cdots i_n} a_1^{i_1} \cdots a_n^{i_n}, i_1 \cdots i_n \in \mathbb{N}, a_1 \cdots a_n \in S, a_{i_1\cdots i_n} \in F\}$$

the fraction field of $F[S]$ is denoted by $F(S)$. $F(S)$ is the smallest field containing $F \cup S$.

Remark 2.2. Give an element $\alpha \in F(S)\backslash F$, if α is a root of a polynomial $f(x) \in F[x]$, then α is called an algebraic element.

Proposition 2.3. If $S = S_1 \cup S_2$, then $F(S) = F(S_1)(S_2)$

Proof. Obviously $F(S) \subset F(S_1)(S_2)$. Conversely, since $F(S_1) \subset F(S)$ and $S_2 \subset F(S)$, $F(S_1)(S_2) \subset F(S)$. $\square$

Definition 2.4 (Algebraic Extensions)**.** $F(S)$ is a algebraic extension when S is a finite collection of algebraic elements over F.

Remark 2.5. Give α an algebraic element.

Proposition 2.6. $F(\alpha) = F[\alpha] \cong F[x]/\langle p(x)\rangle$

Proof. Let $I = \{f(x) \in F[x] : f(\alpha) = 0\} = \langle p(x)\rangle$. Obviously $F[\alpha]$ is a integral domain, therefore $p(x)$ is prime, I is maximal, $F[\alpha]$ is a field. $\square$

Remark 2.7. The irreducible polynomial $p(x)$ above is unique by some unit in F. Let the coefficient of the highest degree term be 1, denote this polynomial $\mathrm{Irr}(\alpha, F)$.

Definition 2.8 (Degree)**.** $\deg(\alpha, F) = \deg(\mathrm{Irr}(\alpha, F))$.

Proposition 2.9. Suppose $\deg(\alpha, F) = n$, then $F(\alpha) = \mathrm{span}_F\{1, \alpha, \cdots, \alpha^{n-1}\}$.

Proof. $\forall\, f(x) \in F[x]$, $\exists\, q(x), r(x)$ such that

$$f(x) = q(x)\mathrm{Irr}(\alpha, F) + r(x), \quad \deg r(x) < n$$

therefore $f(\alpha) = r(\alpha)$. Also, $1, \alpha, \cdots, \alpha^{n-1}$ are linearly indepedent. $\square$

Definition 2.10. Suppose field K, $F \subset K$. Then K is a vector space over F, denote the dimension of this vector space $[K : F]$.

Proposition 2.11. $[F(\beta) : F] < \infty$ iff β is an algebraic element.

Proof. This follows immediately after writing down the basis of $F(\beta)$ as a vector space over F. $\square$

Proposition 2.12. Suppose field K, E with $F \subset E \subset K$. Then

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

Proof. This could be easily seen by directly writing down the basis of K as a vector space over F. $\square$

Proposition 2.13. Suppose K a field with $[K : F] < \infty$. Then $\exists\, \alpha_1, \cdots \alpha_n$ algebraic elements in K, and $K = F(\alpha_1, \cdots, \alpha_n)$.

Proof. Pick any element $\alpha_1 \in K\backslash F$. Then $[K : F(\alpha_1)] \leq [K : F]$. If the equality is taken, the proof is done. Otherwise repeat this process, which obviously must be done in finite steps. $\square$

3 Splitting Fields

Definition 3.1 (Splitting Fields)**.** Given $f(x) \in F[x]$, $\deg f(x) = n$. The splitting field K satisfies:
(1) $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$, where $c, \alpha_1, \cdots, \alpha_n \in K$
(2) $K = F(\alpha_1, \cdots, \alpha_n)$

Proposition 3.2. Give $f(x) \in F[x]$, the splitting field of $f(x)$ exists if $\deg f(x) > 0$

Proof. The proof will be done by induction on $\deg f(x)$. When $\deg f(x) = 1$, the splitting field of $f(x)$ is just F. Assume $\deg f(x) = n + 1$, suppose $p(x)$ is an irreducible factor of $f(x)$. Then denote $F(\alpha_1) \cong F[x]/\langle p(x)\rangle$, $p(\alpha_1) = 0$ therefore $f(\alpha_1) = 0$. Then $f(x) = (x - \alpha_1)f'(x)$, $\deg f'(x) = n$. Since the splitting field of $f'(x)$ exists, the splitting field of $f(x)$ can be found by just adding α_1. □

Proposition 3.3. Denote the splitting field of $f(x) \in F[x]$ with K. Then $[K : F] \leq (\deg f(x))!$

Proof. This is obvious by the proof of Proposition 3.2. ($[F(\alpha_1) : F] \leq n$) □

Proposition 3.4. Suppose fields $F \subset E \subset K$ and K is the splitting field of $f(x) \in F[x]$. Then K is also the splititng field of $f(x) \in E[x]$.

Proof. This is obvious since $K = F(\alpha_1, \cdots, \alpha_n) \subset E(\alpha_1, \cdots, \alpha_n) \subset K$. □

Proposition 3.5. Suppose $\sigma : F \to \overline{F}$ a field homomorphism. Then:
(1) σ can extend to an isomorphism $\sigma : F[x] \to \overline{F}[x]$, and $\sigma(p(x))$ is irreducible iff $p(x)$ is irreducible.
(2) Suppose $K, \overline{K}$ are the extensions of $F, \overline{F}$ respectively, $p(x) \in F[x]$ irreducible, and $\alpha \in K$, $\overline{\alpha} \in \overline{K}$ roots of $p(x)$ and $\sigma(p(x))$. Then σ can extend to an isomorphism $\overline{\sigma} : F(\alpha) \to \overline{F}(\overline{\alpha})$ with $\overline{\sigma}(\alpha) = \overline{\alpha}$.

Proof. For (1), just let $\sigma|_F = \sigma$, $\sigma(x) = x$. The rest is obvious. For (2), suppose $\pi : F[x] \to F[x]/\langle p(x)\rangle$, $\overline{\pi} : \overline{F}[x] \to \overline{F}[x]/\langle \sigma(p(x))\rangle$, and ν, ν' the canonical projection and isomorphism, this gives the isomorphism $\overline{\sigma}' : x + \langle p(x)\rangle \mapsto x + \langle \sigma(p(x))\rangle$. Then the $\overline{\sigma}$ can be easily found by traversing the following commutative diagram.

$$\begin{tikzcd}
F[x] \arrow[r, "\pi"] \arrow[d, hook, two heads, "\sigma"] & F[x]/\langle p(x)\rangle \arrow[r, hook, two heads, "\nu"] \arrow[d, hook, two heads, "\overline{\sigma}'"] & F(\alpha) \arrow[d, hook, two heads, "\overline{\sigma}"] \\
\overline{F}[x] \arrow[r, "\overline{\pi}"] & \overline{F}[x]/\langle \sigma(p(x))\rangle \arrow[r, hook, two heads, "\overline{\nu}"] & \overline{F}(\overline{\alpha})
\end{tikzcd}$$

□

Remark 3.6. The extension in (1) is unique.

Proposition 3.7. Give $\sigma : F \to \overline{F}$ an field isomorphism. Extend it to $\sigma : F[x] \to \overline{F}[x]$. Denote the splitting field of $f(x) \in F[x]$ and $\sigma(f(x)) \in \overline{F}[x]$ with E and $\overline{E}$ respectively. Then σ can be extend to an isomorphism $\overline{\sigma} : E \to \overline{E}$, and the number of different extensions $n_\sigma \leq [E : F]$, where the equality is taken iff every irreducible factor of $f(x)$ in E has no repeated roots.

Proof. Show the first part by induction on $\deg f(x)$. When $\deg f(x) = 1$, σ is just itself. Assume $\deg f(x) = n+1$, suppose $p(x)$ is a irreducible factor of $f(x)$. Then $\exists\, \alpha_1 \in E$ and $\overline{\alpha}_1 \in \overline{E}$, $p(\alpha_1) = \sigma(p(\overline{\alpha}_1)) = 0$. Therefore σ can be extend to $\sigma_1 : F(\alpha_1) \to \overline{F}(\overline{\alpha}_1)$ with $\sigma_1(\alpha_1) = \overline{\alpha}_1$. Then σ can be extend to $\sigma_1 : F(\alpha_1)[x] \to \overline{F}(\overline{\alpha}_1)[x]$. Then write $f(x) = (x - \alpha_1)f'(x)$, $\sigma_1(f(x)) = (x - \overline{\alpha}_1)\sigma'(f'(x))$. By previous proposition E and $\overline{E}$ are the splitting field of $f(x) \in F(\alpha_1)[x]$ and $f'(x) \in \overline{F}(\overline{\alpha}_1)[x]$ respectively. Therefore σ_1 can be extend to $\sigma_1 : E \to \overline{E}$.

For the second part, denote $\overline{\sigma} : E \to \overline{E}$ the extension of $\sigma : F \to \overline{F}$. Suppose $p(x)$ is an irreducible factor of $f(x)$ and $p(\alpha_1) = 0$ ($\alpha_1 \in E$). Then $\overline{\sigma}(\alpha_1)$ must be a root of $\sigma(p(x))$ since $\sigma(p(\overline{\sigma}(\alpha_1))) = \sigma\overline{\sigma}(p(\alpha_1)) = 0$. Denote k_1 the number of different choices of $\overline{\sigma}(\alpha_1)$, $k_1 \leq \deg p(x) = [F(\alpha_1) : F]$, where the equality is taken iff $p(x)$ has no repeated roots. Therefore there are only k_1 extensions on $F(\alpha_1)$. Since $E = F(\alpha_1, \cdots, \alpha_n)$, the number of different extensions are

$$n_\sigma = k_1 \cdots k_n \leq [F(\alpha_n) : F(\alpha_1, \cdots, \alpha_{n-1})] \cdots [F(\alpha_1) : F] = [E : F]$$

where the condition of equality can be easily verified. □

Remark 3.8. This proposition implies that the splitting field is unique under isomorphism.

Proposition 3.9. Suppose fields $F \subset E \subset K$ with E the splititng field of $f(x) \in F[x]$, then for any isomorphism $\sigma : K \to K$ such that $\sigma|_F = \mathrm{id}$, $\sigma(E) = E$.

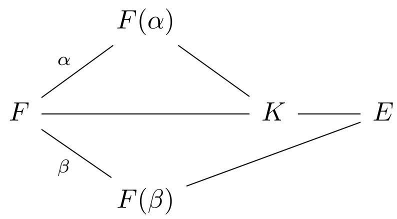
Proof. This is obvious by observing the image of σ on the roots of $f(x)$. □

4 Normal Extensions and Separable Extensions

Definition 4.1 (Normal Extensions)**.** An algebraic extension K is called a normal extension of F iff $\forall\, p(x) \in F[x]$ such that $p(x)$ is irreducible, if $p(x)$ has one root in K, then $p(x)$ splits over K.

Proposition 4.2. Give $F \subset K$ fields, K is a normal extension of F iff K is a splitting field of some polynomial in $F[x]$.

Proof. Let $K = F(\alpha_1, \cdots, \alpha_n)$ and $f(x) = \mathrm{Irr}(\alpha_1, F) \cdots \mathrm{Irr}(\alpha_n, F)$, since K is a normal extension $f(x) = (x-\beta_1)\cdots(x-\beta_t) \in K$. Therefore K is the splitting field of $f(x)$. Conversely, let K be the spliting field of $f(x)$. Then let $p(x) \in F[x]$ and $\exists\, \alpha \in K$, $p(\alpha) = 0$. Let E be the splitting field of $p(x) \in K[x]$, and $g(x) = f(x)p(x)$, then E is the splitting field of $f(x), g(x) \in F[x]$. Let $\beta \in E$ a root of $p(x)$, Then $\tau : F(\alpha) \to F(\beta), \alpha \mapsto \beta$ can be extend to an isomorphism of E with $\tau|_F = \mathrm{id}$. Then $\tau(K) = K$, therefore $\beta \in K$, the proof is done by selecting β.



□

Remark 4.3. The normal extension of a normal extension of F is not necessarily normal over F.

Definition 4.4 (Separable Polynomials)**.** $f(x) \in F[x]$ is separable iff every its irreducible factor has no repeated roots in its splitting field.

Proposition 4.5. If $\mathrm{ch}\, F = 0$, then $\forall\, f(x) \in F[x]$, $f(x)$ is separable.

Proof. For each of its irreducible factor $p(x)$, consider its derivative $p'(x)$. It is easy to see $(p'(x), p(x)) = 1$ when $p(x)$ has no repeated roots. If F is of characteristic 0, then obviously $(p'(x), p(x)) = 1$. □

Definition 4.6 (Separable Elements)**.** α is called separable over F iff $\mathrm{Irr}(\alpha, F)$ is separable.

Proposition 4.7. Every finite separable extension of F is a simple algebraic extension of F.

Proof. If F is a finite field, then its algebraic extension K is also a finite field. Since $K \backslash \{0\}$ is a cyclic group, $K = F(\alpha)$ where α is the generater of the cyclic group.

If F is an infinite field, suppose $F(\alpha_1, \cdots, \alpha_n)$. The proposition is obviously true when $n = 1$. Assume it is true for $n-1$ elements, then $F(\alpha_1, \cdots, \alpha_{n-1}) = F(\beta)$. Therefore $F(\alpha_1, \cdots, \alpha_n) = F(\alpha_n, \beta)$. Let E be the splitting field of $\mathrm{Irr}(\beta, F)\mathrm{Irr}(\alpha, F)$. Then in $E[x]$,

$$\mathrm{Irr}(\beta, F) = (x-\beta)(x-\beta_2)\cdots(x-\beta_s)$$
$$\mathrm{Irr}(\alpha_n, F) = (x-\alpha_n)(x-\alpha_n^1)\cdots(x-\alpha_n^t)$$

since α_n is separable, $(\alpha_n, \alpha_n^1, \cdots, \alpha_n^t)$ is pairwise different. Then

$$T = \left\{ \frac{\beta - \beta_k}{\alpha_n - \alpha_n^j} \right\}, \quad \text{where}\, \beta = \beta_1$$

obviously β is a finite set. Therefore take $c \in F$ such that $c \notin T$, and let $\theta = \beta - c\alpha_n$ and

$$f(x) = ((\theta - cx) - \beta)\cdots((\theta - cx) - \beta_n)$$

Then $f(\alpha_n) = 0$ and $f(\alpha_n^j) \neq 0$. Therefore

$$(f(x), \mathrm{Irr}(\alpha_n, F)) = x - \alpha_n$$

since $f(x), \mathrm{Irr}(\alpha_n, F) \in F(\theta)[x]$, $\alpha_n \in F(\theta)$. Then $\beta \in F(\theta)$, therefore $F(\theta) = F(\alpha_n, \beta)$. □

Remark 4.8. $f(x) \in F(\theta)$ since $f(x) = g(\theta - cx)$, where $g(x) = \mathrm{Irr}(\beta, F)$. And $\gcd_E(f, \mathrm{Irr}(\alpha_\mathrm{n}, \mathrm{F}))$ is equal to $\gcd_{F(\theta)}(f, \mathrm{Irr}(\alpha_\mathrm{n}, \mathrm{F}))$ since it can be computed with the Euclidean algorithm.

Remark 4.9. It is obvious that the separable extension of a separable extension of $\mathbb{Q}$ ($\mathrm{ch}\mathbb{Q} = 0$) is still separable. However, it is true for all fields. The proof is omitted since the equations of our interest are mostly over $\mathbb{Q}$,

5 Galois Groups

Definition 5.1 (Galois Group)**.** Suppose K is a finite extension over F. Then the set of all automorphism of K that is identity on F is a group, denoted by $\mathrm{Gal}(K/F)$.

Definition 5.2 (Invariant Subfield)**.** Suppose $G \leq \mathrm{Aut}(K)$. Then $\mathrm{Inv}G = \{a \in K : g(a) = a, \forall\, g \in G\}$.

Lemma 5.3. Suppose $\sigma_1, \cdots, \sigma_n$ distinct automorphisms of K, denote their invariant subfield $F := \{x \in K : \sigma_i(x) = x, \forall\, i \in \{1, \cdots, n\}\}$, then $\sigma_1, \cdots, \sigma_n$ are linearly independent as automorphism of K as vector space over F.

Proof. Assume they are linearly dependent. Then $\sigma_{s+1} = \sum_{i=1}^{s} a_i\sigma_i$ with $\sigma_1, \cdots, \sigma_s$ linearly independent, therefore the representation is unique. Suppose $a \in K$ such that $\sigma_{s+1}(a) \neq \sigma_1(a)$, then

$$\sigma_{s+1}(ax) = \sum_{i=1}^{s} a_i\sigma_i(ax), \quad \sigma_{s+1}(x) = \sum_{i=1}^{s} \frac{\sigma_i(a)}{\sigma_{s+1}(a)} a_i\sigma_i(x)$$

contradiction. □

Proposition 5.4. $[K : \mathrm{Inv}(G)] = |G|$.

Proof. Let $G = \{\sigma_1 = \mathrm{id}, \cdots, \sigma_n\}$. First take m elements from K denoted by $u_1, \cdots, u_m$. If $m > n$, Suppose a matrix A with $A_{ij} = \sigma_i(u_j)$. The linear equation $AX = 0$ must have nontrivial solutions since $m > n$. Let $(1, \cdots, b_m)$ be such solution that has most zeros. If $b_i \in \mathrm{Inv}G$ for each i, then $u_1, \cdots, u_m$ is linearly dependent since $\sum_1^m \sigma_k(b_ju_j) = \sigma_k(\sum_1^m b_ju_j) = 0$ and σ_k are isomorphisms. On the other hand, if there exists $b_i \notin G$, assume $i = 2$. Then $\exists\, \sigma \in G$ such that $\sigma(b_2) \neq b_2$. Thus

$$\sum_1^m \sigma_k(u_j)\sigma(b_j) = \sigma\left(\sum_1^m \sigma^{-1}\sigma_k(b_ju_j)\right) = 0$$

$(1, \sigma(b_2), \cdots, \sigma(b_m))$ is also a nontrivial solution. Then $(0, b_2 - \sigma(b_2), \cdots, b_m - \sigma(b_m))$ has more zero elements, contradiction. Hence every $m(m > n)$ elements in K are linearly dependent, $[K : \mathrm{Inv}G] \leq |G|$.

On the other hand, if $m < n$, let $(A)_{ij} = \sigma_j(u_i)$, then $AX = 0$ still has nontrivial solutions, denoted by $(b_1, \cdots, b_m)$. Let $a_1, \cdots, a_m$ be m arbitrary elements of F, then

$$BX = 0, \quad (B)_{ij} = \sigma_j(a_iu_i)$$

therefore

$$\sum_{i=1}^{n} \sigma_i(\sum_{j=1}^{m} a_iu_i) = 0$$

hence $\sigma_1, \cdots, \sigma_n$ linearly dependent, which contradicts lemma 5.3. □

Definition 5.5 (Galois Extension)**.** Suppose K/F with $\mathrm{Inv}(\mathrm{Gal}(K/F)) = F$, then K is called a Galois extension of F.

Proposition 5.6. Suppose K is a finite extension of F. Then the following statements are equivalent:

(1) K is the splitting field of a separable polynomial $f(x) \in F[x]$.

(2) K is a Galois extension of F and $[K : F] = |\mathrm{Gal}(K/F)|$.

(3) K is a separable normal extension of F.

Proof. (1)⇒(2). Since $f(x)$ is a separable polynomial of $F[x]$, any irreducible factor $p(x)$ of $f(x)$ has $\deg p(x)$ different roots in K. Therefore $|\mathrm{Gal}(K/F)| \leq [K : F]$ by proposition 3.7. Let $E = \mathrm{Inv}(\mathrm{Gal}(K/F))$, then obviously $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/F)$. Since K is also the splitting field of $f(x) \in E[x]$, $[K : E] = |\mathrm{Gal}(K/E)|$. Therefore $[K : E] = [K : F]$, $E = F$.

(2)⇒(3). $\forall\, \alpha \in K$, denote $G = \mathrm{Gal}(K/F)$. Let

$$\mathrm{Irr}(\alpha, F) = x^r + b_1x^{r-1} + \cdots + b_r, \quad b_i \in F$$

then $\forall\, \sigma \in G$, $\sigma(\alpha)$ is also a root of $\mathrm{Irr}(\alpha, F)$. Therefore G must be a finite group. Suppose $\{\sigma_1(\alpha), \cdots, \sigma_s(\alpha)\} = \{\sigma(\alpha) : \sigma \in G\}$ where σ_1 is the identity. Let

$$h(x) = \prod_{i=1}^{s}(x - \sigma_i(\alpha)) = x^s + p_1 x^{s-1} + \cdots + p_s$$

it is easy to verify that $\sigma(p_i) = p_i$ for any $\sigma \in G$. Therefore $p_i \in F$, $h(x) \in F[x]$. Since $s \le r$, $h(x) = \mathrm{Irr}(\alpha, F)$. Therefore $\mathrm{Irr}(\alpha, F)$ is separable, K is a separable extension. K is also a normal extension of F by the above construction, since any irreducible polynomial in $F[x]$ that has one root in K can be seen as $\mathrm{Irr}(\alpha, F)$ for some $\alpha \in K$.

(3)⇒(1) is trivial. □

Theorem 5.7 (The Fundamental Theorem)**.** Suppose K is a separable normal extension of F. Denote Γ the set of all subgroups of $G = \mathrm{Gal}(K/F)$, and Σ the set of all fields between K and F, then the map

$$\mathrm{Inv} : \Gamma \to \Sigma, H \mapsto \mathrm{Inv}H$$

is a bijection, and

(1) $\mathrm{Inv}^{-1} = \mathrm{Gal} : E \mapsto \mathrm{Gal}(K/E)$,

(2) If $H \in \Gamma$, then $|H| = [K : \mathrm{Inv}H]$, $[G : H] = [\mathrm{Inv}H : F]$.

(3) $\mathrm{Inv}H$ is a normal extension of F with $\mathrm{Gal}((\mathrm{Inv}H)/F) \cong G/H$ iff $H \triangleleft G$.

Proof. Suppose $H \in \Gamma$, $\mathrm{Inv}H = E$, then $F \subset E \subset K$. Thus $H \subset \mathrm{Gal}(K/E) \subset \mathrm{Gal}(K/F)$. Since K is a separable normal extension of F, by the last proposition, K is the splitting field of $f(x) \in F[x]$. Therefore K is the splitting field of $f(x) \in E[x]$, hence K is also a separable normal extension of F. Thus $|H| \le |\mathrm{Gal}(K/E)| = [K : E]$, and proposition 5.4 gives $|H| = [K : E]$. Therefore $H = \mathrm{Gal}(K/E)$, $\mathrm{Gal} \circ \mathrm{Inv} = \mathrm{id}_\Gamma$.

Conversely, suppose $E \in \Sigma$, then $F \subset E \subset K$. By the same argument K is a separable normal extension on E. Thus $\mathrm{Gal}(K/E) \in \Gamma$ and $E = \mathrm{Inv}(\mathrm{Gal}(K/E))$. Therefore $\mathrm{Inv} \circ \mathrm{Gal} = \mathrm{id}_\Sigma$.

For (2), in (1) it is proved that for any $H \in \Gamma$, $|H| = [K : \mathrm{Inv}H]$. Then

$$[G : H] = |G|/|H| = [K : F]/[K : \mathrm{Inv}H] = [\mathrm{Inv}H : F]$$

For (3), suppose $H \in \Gamma$ and $a \in G$. Then $aHa^{-1} \in \Gamma$. Since $\mathrm{Inv}(aHa^{-1}) = \{k \in K : aha^{-1}(k) = k\} = \{k \in K : h(a^{-1}(k)) = a^{-1}(k)\} = a(\mathrm{Inv}H)$, when $H \triangleleft G$, $a(\mathrm{Inv}H) = \mathrm{Inv}H$. Let $\overline{a}$ be the restriction of a to $\mathrm{Inv}H$, then $\overline{a} \in \mathrm{Gal}(\mathrm{Inv}H/F)$. Therefore $\pi : a \mapsto \overline{a}$ gives a homomorphism between G and $\mathrm{Gal}(\mathrm{Inv}H/F)$. Thus

$$F \subset \mathrm{Inv}(\mathrm{Gal}(\mathrm{Inv}H/F)) \subset \mathrm{Inv}\pi(G) = F \quad (*)$$

Therefore $\mathrm{Inv}H$ is a Galois extension of F, thus K/F is normal. Since $\ker \pi = H$, by (2),

$$|\pi(G)| = [G : H] = [\mathrm{Inv}H : F] = |\mathrm{Gal}(\mathrm{Inv}H/F)|$$

hence $\pi(G) = \mathrm{Gal}(\mathrm{Inv}H/F) \cong G/H$. Conversely, suppose $F \subset E \subset K$ with E a normal extension, then $\forall\, g \in G$, $g(E) = E$. Thus

$$g(E) = g(\mathrm{Inv}(\mathrm{Gal}(G/E))) = \mathrm{Inv}(g(\mathrm{Gal}(G/E))g^{-1}) = \mathrm{Inv}(\mathrm{Gal}(K/E)) = E$$

since Inv is injective, $\mathrm{Gal}(K/E) \triangleleft G$. □

Remark 5.8. Comments on $(*)$: (1) it is not obvious that $\pi(G) = \mathrm{Gal}(\mathrm{Inv}H/F)$; (2) $\mathrm{Inv}\pi(G) = F$ because π is the restriction map. If $\mathrm{Inv}\pi(G)$ is larger than F, then $\mathrm{Inv}G$ will be larger than F as well.

6 Galois Groups of Polynomials

Proposition 6.1. Suppose $f(x) \in F[x]$ is a monic polynomial with no repeated roots, K is the splitting field of $F[x]$, $f(x) = \prod_1^m (x - \alpha_i)$. Then

(1) $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup G of $S_{\alpha_1, \cdots, \alpha_m}$.

(2) $f(x) \in F[x]$ is irreducible iff G is transitive.

Proof. (1) Let $X = \{\alpha_1, \cdots, \alpha_m\}$. Suppose $\sigma \in \mathrm{Gal}(K/F)$, then $f(\sigma(\alpha_i)) = 0$, therefore $\sigma(X) \subset X$. Obviously $\sigma(\alpha_i) \neq \sigma(\alpha_j)$ when $i \neq j$. Thus $\sigma|_X \in S_X$. Since $K = F(\alpha_1, \cdots, \alpha_m)$, $\sigma = \tau \in G$ iff $\sigma(\alpha_i) = \tau(\alpha_i)$ for each i. Thus G is a subgroup of S_X.

(2) Suppose G is transitive on X, then $\forall\, \alpha_i, \alpha_j \in X$, $\exists\, \sigma \in G$, such that $\sigma(\alpha_i) = \alpha_j$. Therefore $\mathrm{Irr}(\alpha_i, F) = \mathrm{Irr}(\alpha_j, F)$. Therefore in $K[x]$, $f(x) = \prod_1^m (x - \alpha_i) | \mathrm{Irr}(\alpha_i, F)$. Therefore $f(x) = \mathrm{Irr}(\alpha_i, F)$ is irreducible.

Conversely, if $f(x)$ is irreducible, then $\mathrm{Irr}(\alpha_i, F) = \mathrm{Irr}(\alpha_j, F)$ for each i, j. Then by proposition 3.7, there is an extension σ' such that $\sigma'(\alpha_i) = \alpha_j$. □

Definition 6.2 (Galois Groups of Polynomials)**.** Given $f(x) \in F[x]$, denote its splitting field K. The galois group of this polynomial $G(f, F) := \mathrm{Gal}(K/F)$.

Proposition 6.3. Suppose $x_1, \cdots, x_n$ transcendental elements, $p_1, \cdots, p_n$ elementary symmetric polynomials of $x_1, \cdots, x_n$, $g(x) = \prod_{i=1}^n (x - x_i) \in F(p_1, \cdots, p_n)[x]$. Then $G(g, F(p_1, \cdots, p_n)) \cong S_n$.

Proof. Let $G = \mathrm{Gal}(F(x_1, \cdots, x_n)/F)$. Then $\forall\, \sigma \in S_n$, σ gives an automorphism on $F[x_1, \cdots, x_n]$ with $\sigma|_F = \mathrm{id}$. Extend it to $F(x_1, \cdots, x_n)$ with

$$\sigma(p/q) = \sigma(p)/\sigma(q), \quad p, q \in F[x_1, \cdots, x_n]$$

therefore $\sigma \in G$, $S_n \leq G$. Since $\sigma(p_i) = p_i$, $F(p_1, \cdots, p_n) \subset \mathrm{Inv} S_n$. By proposition 5.4, proposition 3.7 and the fact that $F(x_1, \cdots, x_n)$ is the splitting field of $g(x) = \prod_i (x - x_i) \in F(p_1, \cdots, p_n)$,

$$[F(x_1, \cdots, x_n) : \mathrm{Inv} S_n] = |S_n| = n! \leq [F(x_1, \cdots, x_n), F(p_1, \cdots, p_n)] \leq n!$$

therefore $\mathrm{Inv} S_n = F(p_1, \cdots, p_n)$. □

Remark 6.4. From now on, assume F is of characteristic 0.

Definition 6.5 (Roots of Unity)**.** The roots of $x^n = 1$ are called n-th root of unity. If a n-th root of unity θ satisfies

$$\theta^n = 1, \quad \theta^m \neq 1, \quad \forall\, m, 0 < m < n$$

then it is called a n-th primitive root of unity.

Proposition 6.6. Suppose θ a n-th primitive root of unity. Then θ^k is primitive iff $(k, n) = 1$.

Proof. Suppose K the splititng field of $x^n - 1 \in F[x]$. Since $(nx^{n-1}, x^n - 1) = 1$, $x^n - 1$ is separable, therefore has no repeated roots. Therefore the set of roots is $\{1, \theta, \cdots, \theta^{n-1}\} = \langle \theta \rangle$. The rest is clear since it is a cyclic group. □

Definition 6.7 (Euler Function)**.** $\varphi(n)$ denotes the number of coprimes that are less than n.

Remark 6.8. It is easy to see that $\varphi(n)$ also denotes the number of n-th primitive roots of unity.

Definition 6.9 (Cyclotomic Polynomial)**.** n-th cyclotomic polynomial is defined as

$$\phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \theta_i)$$

Remark 6.10. The following proof is omitted since lack of time.

Proposition 6.11. $\forall\, n \in \mathbb{N}$,

(1) $x^n - 1 = \prod_{d|n} \phi_d(x)$

(2) $\phi_n(x)$ is irreducible on $\mathbb{Q}[x]$.

Proposition 6.12. $G(\phi_n, \mathbb{Q})$ is abelian.

Proposition 6.13. Suppose $a \in \mathbb{Q}$, $G(x^n - a, \mathbb{Q})$ is abelian.

Proposition 6.14. If F contains n-th roots of unity, and K a Galois extension such that $\mathrm{Gal}(K/F)$ is a cyclic group of degree n, then $\exists\, \epsilon \in K$ such that $K = F(\epsilon)$ and $\epsilon^n = a \in F$.

7 Solvability: Algebraic Equations

Definition 7.1 (Radical Extensions)**.** Suppose K/F has a sequence of intermediate fields

$$F \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots F_m = K$$

where F_{i+1} is the splitting field of $x^{n_i+1} - a_{i+1} \in F_i[x]$, then K is called a radical extension of F. K is a simple radical extension of F when $m = 1$.

Definition 7.2 (Solvablility by Radicals)**.** Suppose $f(x) \in F[x]$. $f(x) = 0$ is solvable by radicals in F if there exists a radical extension K of F such that the splitting field of $f(x) \in F[x]$ is contained in F.

Remark 7.3. The definition of solvablility by radicals is consistent with its literal meaning: $f(x)$ is solvable by radicals on F if and only if the roots of $f(x) = 0$ can be expressed by finite operations of addition, subtraction, multiplication, division, and taking radicals over elements in F.

Proposition 7.4. If K is a radical extension of F, then there is a normal radical extension $\overline{K}$ of F such that $K \subset \overline{K}$.

Proof. Since K is a radical extension of F, there is a sequence of simple radical extensions from F to K, index it by m. Attempt proof by induction on m. When $m = 1$, since it is a splitting field of some polynomial, it is normal. Assume the proposition is true for $m - 1$, then $\exists \overline{E}$ such that $E = F_{m-1} \subset \overline{E}$, and $\overline{E}$ is a normal radical extension. Since $K = F_m$ is the splitting field of $x^n - \beta \in E[x]$, $K = E(\epsilon, \theta)$, where $\theta^n - \beta = 0$ and ϵ n-th primitive roots of unity. Suppose $\mathrm{Irr}(\beta, F) = \prod_{i=1}^{r}(x - \beta_i)$ with $\beta = \beta_1$, since $\overline{E}$ is a normal extension, $\beta_i \in \overline{E}$. Let α_i be the roots of $x^n - \beta_i$, $1 \le i \le r$. Let $\alpha_1 = \theta$, then

$$K = E(\epsilon, \theta) \subset \overline{E}(\epsilon, \alpha_1, \cdots, \alpha_r) = \overline{K}$$

it is easy to observe that $\overline{K}$ is a radical extension of $\overline{E}$, therefore a radical extension of $\overline{F}$. Since $\prod_1^r(x - \beta_i) = \mathrm{Irr}(\beta, F) \in F[x]$,

$$g(x) = \prod_1^r (x^n - \beta_i) \in F[x]$$

suppose $\overline{E}$ is the splitting field of $f(x) \in F[x]$. Then $\overline{K}$ is the splitting field of $f(x)g(x)$ therefore a normal extension. $\square$

Theorem 7.5. If $f(x) \in F[x]$, then $f(x)$ is solvable by radicals if $G(f, F)$ is solvable.

Proof. Suppose E the splitting field of $f(x) \in F[x]$. Since $f(x) = 0$ solvable by radicals, there exists a radical extension K such that $E \subset K$. By proposition 7.4, K can be assumed normal. Suppose the number of intermediate fields between K and F is m.

When $m = 1$, K is the splitting field of $x^{n_1} - a_1 \in F[x]$. Suppose n_1-th primitive root of unity ϵ_1 and θ_1 such that $\theta_1^{n-1} = \beta$. Then

$$F \subset F(\epsilon_1) \subset F(\epsilon_1, \theta_1) = K$$

by proposition 6.12 and proposition 6.13, $\mathrm{Gal}(F(\epsilon_1)/F)$ and $\mathrm{Gal}(F(\epsilon_1, \theta_1)/F(\epsilon_1))$ are abelian. By the fundemental theorem,

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/F(\epsilon_1)) \cong \mathrm{Gal}(F(\epsilon_1)/F)$$

therefore

$$0 \to \mathrm{Gal}(K/F(\epsilon_1)) \to \mathrm{Gal}(K/F) \to \mathrm{Gal}(F(\epsilon_1)/F) \to 0$$

$\mathrm{Gal}(K/F)$ is solvable. If $m = k - 1$, since K is a normal extension of F, K is a normal extension of F_1. Assume $\mathrm{Gal}(K/F_1)$ is solvable. Then $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/F_1) \cong \mathrm{Gal}(F_1/F)$, $\mathrm{Gal}(K/F)$ is solvable by induction on m.

Since $F \subset E \subset K$, and K, E are normal extensions of F, by the fundemental theorem,

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

therefore $\mathrm{Gal}(E/F)$ is solvable. $\square$

Remark 7.6. $g(x) = \sum_{i=1}^{n}(x - x_i) = \sum_{i=1}^{n} p_i x^i$ $(n \ge 4)$ is unsolvable on $F(p_1, \cdots, p_n)$ since $G(g, F(p_1, \cdots, p_n))$ is isomorphic to S_n. Therefore for $g(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e$, the roots cannot be expressed with a, b, c, d, e.

Theorem 7.7. If $G(f, F)$ is solvable, then $f(x)$ can be solvable by radicals.

Proof. Suppose $G_0 = G(f, F)$, E is the splitting field of $f(x) \in F[x]$. Need to show that there exists a radical extension K that contains E. Since G_0 is solvable, there is a subnormal sequence

$$G_0 \triangleright G_1 \cdots \triangleright G_s = \{1\}$$

such that G_i/G_{i+1} is cyclic. Therefore by the fundemental theorem,

$$F_0 = F \subset F_1 \subset \cdots \subset F_s = E, \quad F_i = \mathrm{Inv} G_i$$

attempt proof by induction on s. When $s = 1$, $G(f, F)$ is cyclic. Suppose its degree n, ϵ a n-th primitive root, then $F \subset E \subset E(\epsilon) = K$. Obviously K is a normal extension of K. Since $F \subset F(\epsilon) \subset K$, $\mathrm{Gal}(K/F(\epsilon))$ is a subgroup of G_0, therefore still cyclic. By proposition 6.14, K is a simple radical extension of $F(\epsilon)$. Therefore K is a radical extension of F and $E \subset K$.

Assume it is true for $s-1$. Since $G_1 \triangleleft G_0$, F_1 is normal over F and $\mathrm{Gal}(F_1/F)$ is cyclic. Thus F_1 is contained in a normal radical extension $\overline{F_1}$. Suppose it is the splitting field of $g(x) \in F[x]$, $\overline{E}$ the splitting field of $g(x)f(x)$. Then $\mathrm{Gal}(\overline{E}/\overline{F_1}) = H$ is a subgroup of $\mathrm{Gal}(E/F_1)$. Therefore there is a subnormal series

$$H = H_0 \geq \cdots H_{s-1} = \{1\}, \quad H_i = G_{i+1} \cap H$$

where H_i/H_{i+1} is cyclic. Then there is a normal radical extension K of $\overline{F_1}$. Obviously K is also a normal radical extension of F. $\square$

Remark 7.8. This showed that for $f(x) \in F[x]$, if $\deg f(x) \leq 4$, then $f(x) = 0$ is solvable by radicals.