1. Galois Theory

1.1. A homomorphism of fields $F \to F'$ is simply a homomorphism of rings. Such a homomorphism is always injective, because its kernel is a proper ideal (it does not contain 1), which must therefore be zero.

A field $E$ containing a field $F$ is called an extension field of $F$. We write $[E : F] = \dim_F E$ for the degree of $E$ over $F$. We say that $E$ is finite over $F$ if $[E : F] < \infty$.

For $E/F$ extension and $\alpha \in E$. Consider $F[x] \to E$, $f \mapsto f(\alpha)$.

There are two possibilities:

Case 1: ker = (0). We say that $\alpha$ is transcendental over $F$. We have an isomorphism $F(x) \to F(\alpha)$.

Case 2: ker = (f). Here $f$ is a monic irreducible polynomial. We say that $\alpha$ is algebraic over $F$ and $f$ is a minimal polynomial of $\alpha$ over $F$. We have an isomorphism $F[x]/(f) \to F(\alpha)$.

Proposition 1.1. $E/F$ is finite iff $E$ is algebraic and finitely generated (as a field) over $F$.

Let $E, E'$ be fields containing $F$. An $F$-homomorphism is a homomorphism $\varphi : E \to E'$ such that $\varphi_F = \text{id}$.

Proposition 1.2. Let $F(\alpha)$ be a simple field extension of a field $F$, and let $\varphi_0 : F \to \Omega$ be a homomorphism of fields.

(a) If $\alpha$ is transcendental over $F$, then the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence between extensions $\varphi : F(\alpha) \to \Omega$ of $\varphi_0$ and elements of $\Omega$ transcendental over $\varphi_0(F)$.

(b) If $\alpha$ is algebraic over $F$, with minimum polynomial $f \in F[x]$, then the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence between extensions $\varphi : F(\alpha) \to \Omega$ of $\varphi_0$ and the roots of $\varphi_0(f)$ over $\Omega$. In particular, the number of such maps is the number of distinct roots of $\varphi_0(f)$ in $\Omega$.

1.2. Let $f \in F[x]$. We say $E/F$ splits $f$ if $f(x) = \prod(x - \alpha_i)$ for $\alpha_i \in E$. If in addition, $E$ is generated by the roots of $f$, then we say that $E$ is a splitting field of $f$.

Proposition 1.3. Every polynomial $f \in F[x]$ has a splitting field $E_f$ and $[E_f : E] \leq (\deg f)!$.

Proposition 1.4. Let $f \in F[x]$, $E/F$ generated by roots of $f$. $\Omega/F$ splits $f$. Then

(1) There exists $F$-homomorphism $E \to \Omega$. 

1
(2) \(\sharp\{F\text{-hom}: E \to \Omega\} \leq |E:F|\) and equals \([E:F]\) if \(f\) has only simple roots in \(\Omega\).

**Corollary 1.5.** Let \(f \in \mathbb{F}[x]\). The splitting field \(E_f\) is unique up to isomorphism.

**Corollary 1.6.** Let \(E/F\) be a splitting field of \(f\). Then \(|\text{Aut}(E/F)| \leq |E:F|\) and equals \([E:F]\) if \(f\) is separable over \(F\) (i.e., none of its irreducible factor in \(F[x]\) has multiple roots) Here \(\text{Aut}(E/F)\) is the group of \(F\)-automorphism \(E \to E\).

1.3. \(E/F\) is called separable if minimal polynomial of any element of \(E\) is separable (i.e., no multiple roots). \(E/F\) is called normal if minimal polynomial of any element of \(E\) splits in \(E[x]\).

**Example 1.7.** \(\mathbb{Q}[\sqrt{2}]\) is separable, but not normal over \(\mathbb{Q}\). \(\mathbb{F}_p(T)\) is normal, but not separable over \(\mathbb{F}_p(T^p)\).

**Lemma 1.8.** (Dedekind) Let \(F\) be a field and \(G\) be a group. If \(\sigma_1, \cdots, \sigma_n\) are distinct characters from \(G\) to \(F\). Then \(\sigma_i\) are linearly independent over \(F\).

Proof. Otherwise, \(\sum a_i\sigma_i(g) = 0\) with \(\sharp\{i; a_i \neq 0\}\) as small as possible. So \(\sum a_i\sigma_i(h)\sigma_i(g) = 0\) for all \(g, h \in G\). Thus \(\sum a_i(\sigma_i(h) - \sigma_1(h))\sigma_i(g) = 0\). However, \(\sharp\{i; a_i(\sigma_i(h) - \sigma_1(h)) \neq 0\} < \sharp\{i; a_i \neq 0\}\). Contradiction.

**Theorem 1.9.** (Artin) Let \(G\) be a finite group of automorphisms of \(E\) and \(F = E^G\) the fixed field of \(G\). Then \([E:F] \leq |G|\).

Proof. Assume that \(G = \{1 = \sigma_1, \cdots, \sigma_n\}\) and \(\alpha_1, \cdots, \alpha_m \in E\), basis over \(F\). If \(m > n\), then the equations \(\sum_i \sigma_i(\alpha_j) x_j = 0\) for all \(1 \leq j \leq m\) has a nontrivial solution \((x_1, \cdots, x_m) = (a_1, \cdots, a_m)\) in \(E\). We may also assume that this is a solution with fewest possible nonzero elements. WLOG, \(x_1 \neq 0\) and \(x_1 \in F\) after rescaling. Then for any \(\sigma \in G\), \((\sigma(x_1), \cdots, \sigma(x_m))\) and \((\sigma(x_1) - x_1, \cdots, \sigma(x_m) - x_m)\) are also solutions. By minimality assumption, \(\sigma(x_i) = x_i\) for all \(i\) and \(\sigma \in G\). So \(x_i \in F\) for all \(i\). Thus \(\sum x_i a_i = 0\). Contradiction.

**Corollary 1.10.** Let \(G\) be a finite group of automorphisms of \(E\). Then \(G = \text{Aut}(E/E^G)\).

Proof. \(G \subseteq \text{Aut}(E/E^G)\). So \(|G| \leq |\text{Aut}(E/E^G)| \leq |E:E^G| \leq |G|\).

**Theorem 1.11.** For a finite extension \(E/F\), the following statements are equivalent:

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

(b) \(F = E^{\text{Aut}(E/F)}\).

(c) \(F = E^G\) for some finite group \(G\) of automorphisms of \(E\).

(d) \(E\) is normal and separable over \(F\).

In this case, we call that \(E\) is Galois over \(F\) and write \(\text{Gal}(E/F)\) for \(\text{Aut}(E/F)\).
Proof. (a) \( \Rightarrow \) (b). Let \( G = \text{Aut}(E/F) \). Then \( E^G \supset F \). \( E \) is splitting field of \( f \) over \( E^G \). So \( [E : E^G] = |\text{Aut}(E/E^G)| = |G| = |\text{Aut}(E/F)| = [E : F] \) and \( E^G = F \).

(b) \( \Rightarrow \) (c). Obvious.

(c) \( \Rightarrow \) (d). Let \( \alpha \in E \) and \( f \) minimal polynomial. Let \( \alpha_1, \cdots, \alpha_m \) be orbit of \( \alpha \) under \( G \). Set \( g(x) = \Pi(x - \alpha_i) \in F[x] \). Then \( f \mid g \) since \( g(\alpha) = 0 \). Also \( g \mid f \) since \( f(\alpha_i) = 0 \). Thus \( f = g \) splits into distinct factors in \( E \).

(d) \( \Rightarrow \) (a). \( E = F[\alpha_1, \cdots, \alpha_n] \). Let \( f_i \) be minimal polynomial of \( \alpha_i \) over \( F \). Then \( f_i \) splits in \( E \). Hence \( f = \Pi f_i \) splits in \( E \). This is also separable since \( E/F \) is separable.

**Corollary 1.12.** Every finite separable extension is contained in a finite Galois extension.

Proof. Let \( E = F[\alpha_1, \cdots, \alpha_n] \). Then the splitting field of \( f = \Pi f_i \) contains \( E \) and is Galois over \( F \).

**Corollary 1.13.** Let \( E \supset M \supset F \). If \( E \) is Galois over \( F \), then it is Galois over \( M \).

Proof. Assume that \( E = E_f \) with \( f \in F[x] \). Then \( E \) is also the splitting field of \( f \in M[x] \).

**Theorem 1.14.** (Fundamental theorem) Let \( E \) be a finite Galois extension of \( F \) and \( G = \text{Gal}(E/F) \). Then \( H \mapsto E^H \), \( M \mapsto \text{Gal}(E/M) \) gives bijection between subgroup of \( G \) and intermediate extension \( F \subset \supset M \subset E \). Moreover,

(a) \( H_1 \supset H_2 \) iff \( E^{H_1} \subset E^{H_2} \).

(b) \( (H_1 : H_2) = [E^{H_2} : E^{H_1}] \).

(c) \( G/H \sigma^{-1} = \sigma(M) \).

(d) \( H \) normal in \( G \) iff \( E^H \) normal over \( F \). In this case, \( E^H \) is Galois over \( F \) and \( \text{Gal}(E^H/F) \cong G/H \).

Proof. \( H = \text{Gal}(E/E^H) \) is proved. Also \( E \) is Galois over \( M \). So \( M = E^{\text{Gal}(E/M)} \).

(a) \( H_1 \supset H_2 \Rightarrow E^{H_1} \subset E^{H_2} \Rightarrow H_1 = \text{Gal}(E/E^{H_1}) \supset \text{Gal}(E/E^{H_2}) = H_2 \).

(b) \( |H_i| = [E : E^{H_i}] \).

(c) \( \forall \tau \in G, \alpha \in E, \tau \alpha = \alpha \iff \sigma \tau \sigma^{-1}(\sigma \alpha) = \sigma \alpha \). So \( \text{Gal}(E/\sigma M) = \sigma \text{Gal}(E/M) \sigma^{-1} \).

(d) If \( H \) normal in \( G \). Then \( \sigma E^H = E^{\sigma H \sigma^{-1}} = E^H \). Now \( \sigma \mapsto \sigma | E^H \) gives \( G \to \text{Aut}(E^H/F) \) with kernel \( H \). So induces \( G/H \to \text{Aut}(E^H/F) \). Since \( (E^H)^{G/H} = F \), \( E^H \) is Galois over \( F \) and \( G/H \cong \text{Gal}(E^H/F) \).

If \( M = F[\alpha_1, \cdots, \alpha_n] \) normal over \( F \), then \( \sigma(\alpha_i) \) is a root of the minimal polynomial of \( \alpha_i \) over \( F \), so in \( M \). Thus \( \sigma(M) = M \) for all \( \sigma \in G \). Hence \( \sigma H \sigma^{-1} = H \).
Proposition 1.15. Let $E, L$ be field extensions of $F$ contained in some common field. If $E/F$ is Galois, then $EL/L$ and $E/E \cap L$ are Galois, and the map 

$$\text{Gal}(EL/L) \to \text{Gal}(E/E \cap L), \quad \sigma \mapsto \sigma |_E$$

is an isomorphism. In this case 

$$[EL : F] = \frac{[E : F][L : F]}{[E \cap L : F]}.$$

Proof. $E$ is a splitting field of separable $f \in F[x]$. So $EL$ (resp. $E$) is splitting field of $f$ over $L$ (resp. $E \cap L$). For $\sigma \in \text{Gal}(EL/L)$, $\sigma$ maps roots of $f$ to roots of $f$. So $\sigma(E) = E$. Now $\sigma \mapsto \sigma |_E$ is defined.

If $\sigma \in \text{Gal}(EL/L)$ fixes the elements in $E$, then it also fixes the elements in $EL$. So $\sigma = 1$. Thus injective. If $\alpha \in E$ is fixed by $\text{Gal}(EL/F)$, then $\alpha \in E \cap L$. So image is $\text{Gal}(E/E \cap L)$ by fundamental theorem.

Proposition 1.16. Let $E, L$ be field extensions of $F$ contained in some common field. If $E, L$ are Galois over $F$, then $EL, E \cap L$ are Galois over $F$, and 

$$\text{Gal}(EL/F) \to \text{Gal}(E/F) \times \text{Gal}(L/F), \quad \sigma \mapsto (\sigma |_E, \sigma |_L)$$

is an isomorphism of $\text{Gal}(EL/F)$ onto the subgroup 

$$H = \{(\sigma_1, \sigma_2); \sigma_1 |_{E \cap L} = \sigma_2 |_{E \cap L}\}$$

of $\text{Gal}(E/F) \times \text{Gal}(L/F)$.

Proof. $E$ is a splitting field of separable $f \in F[x]$ and $L$ is a splitting field of separable $g \in F[x]$. Then $EL$ is a splitting field of separable $fg \in F[x]$. As in the previous Prop., $\text{Gal}(EL/F) \to \text{Gal}(E/F) \times \text{Gal}(L/F), \sigma \mapsto (\sigma |_E, \sigma |_L)$ is defined, injective with image contained in $H$.

Now for $\alpha \in E \cap L$ with minimal polynomial $h \in F[x]$. Then $h$ is separable, and has distinct $\deg(h)$ roots in $E$ (resp. $L$ and $EL$), since $E, L, EL$ are Galois over $F$. Thus all these roots are in $E \cap L$. So $E \cap L/F$ is normal and separable, hence Galois.

The remaining part follows from comparing the size of $\text{Gal}(EL/F)$ with $|H|$.

1.4. For separable $f \in F[x]$, let $E_f$ be the splitting field. Assume that $f$ has only simple roots in $E_f$, $f(x) = \Pi_{i=1}^n (x - \alpha_i) \in E_f[x]$. Set $G_f = \text{Gal}(E_f/F)$. Then $G_f \subset S_n$.

Proposition 1.17. (1) Let $\Delta(f) = \pi_{i<j}(\alpha_i - \alpha_j)$. Then $\Delta(f) \in F$ iff 

$$G_f \subset A_n.$$

(2) The discriminant $D(f) = \Delta(f)^2$ is always in $F$.

Proposition 1.18. $f$ is irreducible iff $G_f$ acts transitively on the set of roots $f$. 
Proof. $\Leftarrow$. If $g \mid f$ and $\alpha$ is a root of $g$. Then for any root $\beta$ of $f$, $\beta = \sigma \alpha$ for some $\sigma \in G_f$. Thus $g(\sigma \alpha) = \sigma g(\alpha) = 0$. So $\beta$ is a root of $g$ and $f = g$.

$\Rightarrow$. If $\alpha, \beta$ are roots of $f$. Then $F(\alpha) \cong F(\beta) \cong F[x]/(f)$. There exists $F$-homomorphism $\phi : F(\alpha) \to E_f$, $\alpha \mapsto \beta$. Since $E_f$ is splitting field, $\phi$ extends to $F$-homomorphism $\sigma : E_f \to E_f$. Now $\sigma(\alpha) = \beta$.

**Example 1.19.** If $f(x)$ irreducible and separable of degree 3. Then $G_f = A_3$ or $S_3$, according to $D(f)$ is square in $F$ or not. Fact. The discriminant of $x^3 + px + q$ is $-4p^3 - 27q^2$.

### 2. Application

#### 2.1. Finite fields.

$E/F_p$ of degree $n$. Then $E$ has $p^n$ elements. $E^\times$ is a cyclic group of $p^n - 1$ elements. Thus $x^{p^n - 1} = 1$ for all nonzero $x \in E$. So any element of $E$ is a root of $f(x) = x^{p^n} - x$. Since $f'(x) = -1$, $f$ has $p^n$ distinct roots and $E$ is the splitting field of $f$ and is Galois over $F_p$. We write it as $F_{p^n}$.

Frobenius map $Fr : x \mapsto x^p$ is injective, hence surjective on $E$ and $E^{Fr} = F_{p^n}$. So by fundamental theorem, $\text{Gal}(E/F_p) = < Fr >$ is a cyclic group of order $n$.

**Proposition 2.1.** Let $F$ be a field and $G$ a finite subgroup of $F^\times$. Then $G$ is cyclic.

Proof. $G$ is a finite abelian group. By the classification of finite abelian group, there exists $r \in \mathbb{N}$ such that $G$ contains an element of order $r$, $r \mid |G|$ and $x^r = 1$ for all $x \in G$. Thus every element of $G$ is a root of $x^r - 1$, thus $|G| \leq r$.

**Corollary 2.2.** (1) For any $d \mid n$, $F_{p^n}$ contains exactly one field with $p^d$ elements.

(2) $F_{p^m} \subset F_{p^n}$ iff $m \mid n$.

(3) $x^{p^n} - x$ is the product of all monic irreducible polynomial over $F_p$ whose degree divides $n$.

Proof. (1) Since $\text{Gal}(F_{p^n}/F_p)$ is cyclic, there is exactly one subgroup of order $n/d$.

(2) $\Rightarrow$ $\text{Gal}(F_{p^n}/F_p)$ is a quotient group of $\text{Gal}(F_{p^n}/F_p)$. So $m \mid n$.

(3) First, the factors of $x^{p^n} - x$ are distinct because it has no common factor with its derivative.

If $g$ is an irreducible factor of $x^{p^n} - x$ and $\alpha$ is a root of $g$ in $F_{p^n}$, then $F_p(\alpha) \subset F_{p^n}$ is a subfield of with $p^{\deg g}$ elements. Thus $\deg g \mid n$.

If $f$ is an irreducible monic polynomial of degree $m$ with $m \mid n$, then $f$ has a root $\alpha$ in a field of degree $m$ over $F_p$, thus in $F_{p^n}$. Hence $\alpha^{p^n} - \alpha = 0$ and $f \mid x^{p^n} - x$.

**Corollary 2.3.** The algebraic closure $\overline{F}$ of $F_p$ is $\overline{F} = \bigcup F_{p^n}$.
Theorem 2.4. (*Fundamental theorem of algebra*) \( \mathbb{C} \) is algebraically closed.

Proof. \( \mathbb{C} \) is the splitting field of \( x^2 + 1 \in \mathbb{R}[x] \). Let \( f \in \mathbb{R}[x] \) and \( E \) the splitting field of \( f(x)(x^2 + 1) \). Then \( E \) is Galois over \( \mathbb{R} \). Let \( G = \text{Gal}(E/\mathbb{R}) \) and \( H \) a Sylow 2-subgroup. Set \( M = E^H \). Then \([M : \mathbb{R}] = (G : H)\) is odd. We show that

1. \( M = \mathbb{R} \).

Let \( \alpha \in M \) and \( g \) the minimal polynomial. Then \([ \mathbb{R}(\alpha) : \mathbb{R}] \) is odd and \( \deg(g) \) is odd. Since \( g(-\infty) = -\infty \) and \( g(\infty) = \infty \), \( g \) has a root in \( \mathbb{R} \). Thus \( g \) has a root in \( \mathbb{R} \). We show that

2. \( E = \mathbb{C} \).

Set \( G' = \text{Gal}(E/\mathbb{C}) \). Then by (1), \( G' \) is a 2-group. If not 1, then there is a normal subgroup \( N \) of index 2. Thus \( E \) has degree 2 over \( \mathbb{C} \). But all the square roots of \( \mathbb{C} \) are in \( \mathbb{C} \). So impossible.

2.2. Constructible numbers. Recall that \( \alpha \in \mathbb{R} \) is constructible if it is in a subfield of the form \( \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}] \), where \( a_i \in \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}] \). Then in particular, \([\mathbb{Q}(\alpha) : \mathbb{Q}]\) is a power of 2.

Theorem 2.5. If \( E \subset \mathbb{R} \) is Galois over \( \mathbb{Q} \) of degree \( 2^s \), then \( \alpha \) is constructible for all \( \alpha \in E \).

Remark 2.6. It fails if \( E \) is not Galois over \( \mathbb{Q} \). For example, \( f(x) = x^4 - 4x + 2 \) has \( G_f = S_4 \). If all the roots of \( f \) are constructible, then so is \( E_f \). Let \( H \) be a Sylow 2-subgroup of \( S_4 \), then \([E^H : \mathbb{Q}]\) is odd and any element in \( E^H \setminus \mathbb{Q} \) is not constructible.

Proof. Let \( G = \text{Gal}(E/\mathbb{Q}) \). Recall that any 2-group has nontrivial center and hence a subgroup in the center of order 2. Now a sequence of groups

\[
\{1\} = G_0 \subset G_1 \subset \cdots \subset G_s = G
\]

with \([G_{i+1}/G_i] = 2\). By fundamental theorem, a sequence of fields

\[
E = E_0 \supset E_1 \supset \cdots \supset E_s = \mathbb{Q}
\]

with \([E_i : E_{i+1}] = 2\). Thus \( E_i = E_{i+1}[^{\sqrt{a_i}}] \) for some \( a_i \in E_{i+1} \).

Corollary 2.7. A regular \( p \)-gon with \( p \) prime is constructible iff \( p \) is a Fermat prime, i.e., \( p \) is of the form \( 2^r + 1 \).

Proof. \([\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}(\cos(2\pi/p))]\) is a power of 2. Now \( \mathbb{Q}(e^{2\pi i/p}) \) is Galois over \( \mathbb{Q} \) with Galois group \((\mathbb{Z}/p\mathbb{Z})^\times\) of order \( p - 1 \). Thus \( \cos(2\pi i/p) \) is constructible iff \( p - 1 \) is a power of 2. Easy to check that such \( p \) is of the form \( 2^r + 1 \).

2.3. Primitive element. Finite extension \( E/F \) is simple if \( E = F[\alpha] \) for some \( \alpha \in E \). Such \( \alpha \) is primitive element.
Theorem 2.8. (1) Finite extension $E/F$ is simple iff there are only finitely many intermediate extensions.

(2) If $E$ is separable over $F$, then it is a simple extension.

Proof. If $F$ is a finite field, then $E$ is also finite and $E^\times$ is cyclic. So (1) and (2) follows. Now assume that $F$ is infinite.

(1) $\Rightarrow$. Assume that $E = F[\alpha]$ and $f$ is the minimal polynomial of $\alpha$. For any intermediate field $M$, let $f_M \in M[x]$ be the minimal polynomial of $\alpha$. Then $f_M | f$ is a monic polynomial in $E[x]$. So in particular, there are only finitely many possible $f_M$. Now for $f_M$, let $M'$ be the subfield of $M$ generated by the coefficient of $f_M$. Then $E = M[\alpha] = M'[\alpha]$ and $[E : M[\alpha]] = \deg f_M = [E : M'[\alpha]]$. So $M = M'$.

(2) $\Leftarrow$. Assume that $E = F[\alpha, \beta]$. The case with more generators can be proved by induction. Since $|F|$ is infinite, there exists $c \neq c' \in F$ such that $F(\alpha + c\beta) = F(\alpha + c'\beta)$. Then $(c' - c)\beta \in F(\alpha + c\beta)$ and $\beta$, hence $\alpha$ also in $F(\alpha + c\beta)$. So $\alpha + c\beta$ is a primitive element.

(2) $E$ is contained in a Galois extension $E'$ of $F$. By fundamental theorem, there are only finitely many intermediate extension between $F$ and $E'$. Hence by (1), $E/F$ is simple.

2.4. Cyclotomic extension.

Proposition 2.9. Let $n \in \mathbb{N}$ and $F$ a field of char 0 or $p$ with $p \nmid n$. Let $E$ be the splitting field of $x^n - 1$. Then

(1) There exists a primitive $n$-th root $\xi$ of 1 in $E$, i.e., the order of $\xi$ is $n$.

(2) $E = F[\xi]$.

(3) $E$ is Galois over $F$. The map $\text{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$, $\sigma \mapsto i$, where $\sigma(\xi) = \xi^i$, is injective.

Proof. (1)&(2) $\gcd(x^n - 1, nx^{n-1}) = 1$. So only simple roots. All the $n$-th roots of 1 in $E$ form a subgroup of order $n$, so cyclic and there exists primitive element.

(3) Any primitive root is of the form $\xi^i$ for some $i \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 2.10. Let $F = \mathbb{Q}$. Then the cyclotomic polynomial $\Psi_n(x) = \prod_{\xi \text{primitive}} (x - \xi)$ is in $\mathbb{Z}[x]$ and is irreducible over $\mathbb{Q}$. The above map $\text{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

Proof. For any $n$-th root $\omega$ of unity, let $d$ be the order of $\omega$. Then $\omega$ is a primitive $d$-th root of unity. Now we have a bijection between the set of $n$-th root of unity, and the pair $(d, \omega)$, where $d | n$ and $\omega$ is a primitive $d$-th root of unity. So

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

In particular, by Gauss Lemma, $\Psi_d(x) \in \mathbb{Z}[x]$ for all $d | n$. 
Now assume that $\Psi_n(x) = f(x)g(x)$, where $f(x)$ irreducible and $f(x), g(x)$ are monic polynomials in $\mathbb{Z}[x]$. Assume that $\xi$ is a root of $f$. We'll show that for any $d \in \mathbb{Z}$ with $\gcd(d, n) = 1$, $\xi^d$ is also a root of $f$. It is suffices to prove the case where $d$ is a prime $p$.

If $\xi^d$ is not a root of $f$, then it is a root of $g$. Thus $f(x), g(x^p)$ has a common root and $g(x^p) = f(x)h(x)$. Hence $\tilde{g}(x^p) = \tilde{g}(x^p) = \tilde{f}(x)\tilde{h}(x)$ mod $p$ as elements in $\mathbb{F}_p[x]$. Thus $\tilde{f}, \tilde{g}$ has common roots. Therefore $x^n - 1 \in \mathbb{F}_p[x]$ has multiple roots, which is impossible.

Now $|\text{Gal}(E/F)| = |E : F| = \deg \Psi_n = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. So $\text{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

2.5. Cyclic and Kummer extension.

**Theorem 2.11.** (Hilbert’s 90) Let $E/F$ be cyclic extension with Galois group $G = \langle \sigma \rangle$. For $\beta \in E$, define the norm $N_{E/F}(\beta) = \Pi \sigma^i \beta$. Then $N_{E/F}(\beta) = 1$ if and only if $\beta = \alpha/\sigma\alpha$ for some $\alpha \in E^\times$.

**Proof.** $\Rightarrow N(\beta) = N(\alpha)/N(\sigma) = 1$.

$\Leftarrow$ Assume that $|G| = n$. Then by Dedekind’s theorem, $\sum_{i=0}^{n-1}(\Pi_{j=0}^{i-1}(\beta))\sigma^i$ is not identically zero on $E$. Hence there exists $a \in E$ such that $\alpha := \sum_{i=0}^{n-1}(\Pi_{j=0}^{i-1}(\beta))\sigma^i(a) \neq 0$. Now $\beta\sigma(\alpha) = \alpha$.

**Theorem 2.12.** Let $F$ be a field containing a primitive $n$-th root of 1. Then

1. For any nonzero $a \in F$, the splitting field $E$ for $x^n - a$ is a cyclic (Galois) extension.

2. If $E$ is a cyclic extension of $F$ of degree $n$, then $E$ is the splitting field of $x^n - a$ for some $a \in F$.

**Proof.** (1) $\gcd(x^n - a, nx^{n-1}) = 1$. So $x^n - a$ is separable and $E$ is a Galois extension. Let $\alpha$ be a root. Then all the roots are of the form $\xi\alpha$ for some $n$-th root $\xi$ of unity. Now $\text{Gal}(E/F) \to \mu_n, \sigma \mapsto \sigma(\alpha)/\alpha$ is injective since $E = F[\alpha]$. Here $\mu_n$ is the group of all $n$-th root of unity.

(2) $N(\xi) = \xi^n = 1$. By Hilbert’s 90, $\xi = \alpha/\sigma\alpha$ for some $\alpha \in E$. Since $G$ is cyclic, any subgroup of $G$ is normal and $F(\alpha)$ is Galois over $F$. The map $G \to \text{Gal}(F(\alpha)/F), \sigma^i \mapsto \sigma^i |_{F(\alpha)}$ is injective. Hence $E = F(\alpha)$. Moreover, $\sigma(\alpha^n) = (\xi\alpha)^n = \alpha^n$ and $\alpha^n \in E^G = F$.

**Theorem 2.13.** Let $F$ be a field containing a primitive $n$-th root of 1. Let $E/F$ be a finite extension. Then $E/F$ is a Kummer extension (i.e., with abelian Galois group) whose Galois group has an exponent dividing $n$ (i.e., any element in $G$ is of order dividing $n$) if $E$ is a splitting field of $(x^n - a_1) \cdots (x^n - a_r)$ for some $a_1, \ldots, a_r \in F$.

**Proof.** $\Leftarrow$. We have that $E = F(\alpha_1, \ldots, \alpha_r)$, where $\alpha_i$ is a root of $x^n - a_i$. Then for any $\sigma \in G = \text{Gal}(E/F)$, $\sigma(\alpha_i) = \xi^{u_i(\sigma)}\alpha_i$. Hence for $\tau \in \text{Gal}(E/F)$, we have that $u_i(\sigma) + u_i(\tau) = u_i(\tau) + u_i(\sigma)$ and $\sigma\tau = \tau\sigma$. Thus $G$ is abelian. Also for any $\sigma \in G$, $\sigma^n = 1$. 

\[ \Rightarrow. \] Since \( G \) is a finite abelian group, it is a direct product of cyclic groups \( C_1, \ldots, C_r \). Set \( C_i' = C_1 \times \cdots \times \hat{C}_i \times \cdots \times C_r \subset G \) and \( E_i = E^{C_i'} \). Then \( E_i/F \) is a cyclic extension. Hence \( E_i = F(\alpha_i) \) for some \( \alpha_i \) with \( \alpha_i^n = a_i \in F \). By fundamental theorem of Galois theory, \( E = E^{\cap C_i'} \) is the unique field extension that contains \( E_i \) for all \( i \). Hence \( E = F(\alpha_1, \ldots, \alpha_r) \).

2.6. Galois’s solvability theorem. Let \( F \) be a field of char 0. A polynomial \( f \in F[x] \) is called solvable if any root of \( f \) can be obtained by \( \pm, \times, / \) and \( \sqrt[n]{\cdot} \).

A group \( G \) is solvable if there is a sequence \( 1 = G_0 \subset G_1 \subset \cdots \subset G_s = G \), where \( G_i \) is normal in \( G_{i+1} \) and \( G_{i+1}/G_i \) is cyclic for all \( i \). Any subquotient of a solvable group is again solvable.

**Theorem 2.14.** \( f \in F[x] \) is solvable iff \( G_f \) is solvable.

**Proof.** \( \Leftarrow \) Let \( F' = F[\xi] \), where \( \xi \) is a primitive \((\deg f)!\)-th root of 1. Set \( G'_f = \text{Gal}(F'_f/F') \). Then the natural map \( G'_f \to G_f \) is well-defined and injective. Hence \( G'_f \) is solvable. Now there exists a sequence \( \{1\} = G_0 \subset G_1 \subset \cdots \subset G_s = G'_f \), where \( G_i \) is normal in \( G_{i+1} \) and \( G_{i+1}/G_i \) is cyclic. Let \( F_i = (F'_f)^{G_i} \). Then \( F \subset F' = F_s \subset \cdots \subset F_0 = F'_f \) and \( F_i/F_{i+1} \) is a cyclic extension.

\( \Rightarrow \) There exists \( F = F_0 \subset \cdots \subset F_m \), where \( F_{i+1} = F_i(\alpha_i), \alpha_i^n \in F_i \) and \( F_m \) splits \( f \). Set \( n = n_1 \cdot \cdots \cdot n_m \). Let \( \Omega' \) be a field containing \( F_m \) and a primitive \( n\)-th root of unity \( \xi \). Then \( \Omega' \) is contained in a Galois extension of \( F \). We denote this field by \( \Omega \). Set \( G = \text{Gal}(\Omega/F) \) and \( H = \text{Gal}(\Omega/F_m[\xi]) \). Set \( H' = \cap_{\sigma \in G} \sigma H \sigma^{-1} \). Then \( H' \) is normal in \( G \) and is the maximal subgroup in \( \sigma H \sigma^{-1} \) for all \( \sigma \). Thus \( \Omega^{H'} = \Pi_{\sigma \in G} \Omega^{H\sigma} = \Pi_{\sigma \in G} \sigma(F_m[\xi]) \) is Galois over \( F \) and is the minimal subfield containing \( \sigma \Omega^{H'} \) for all \( \sigma \in G \).

Now \( \Omega^{H'} \) is generated by \( \xi, \sigma(\alpha_i) \) over \( F \). Consider \( F \subset F[\xi] \subset F[\xi, \alpha_1] \subset \cdots \subset \Omega^{H'} \). Here each field is obtained from its predecessor by adding a \( n\)-th root of some element, hence cyclic extension. So \( \text{Gal}(\Omega^{H'}/F) \) is solvable. Since \( \text{Gal}(F_f/F) \) is a quotient of \( \text{Gal}(\Omega^{H'}/F) \), it is also solvable.

2.7. Symmetric polynomial. A polynomial \( f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \) is symmetric if \( f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \) for \( \sigma \in S_n \). The polynomials

\[
\begin{align*}
p_1 &= \sum_i x_i, \\
p_2 &= \sum_{i<j} x_ix_j, \\
\cdots, \\
p_n &= \Pi_i x_i
\end{align*}
\]
are called the elementary symmetric polynomials.

**Theorem 2.15.** (1) Every symmetric polynomial is a polynomial of elementary symmetric polynomials, i.e., if \( f \in F[x_1, \ldots, x_n] \) is symmetric, then \( f \in F[p_1, \ldots, p_n] \).

(2) The field \( F(x_1, \ldots, x_n) \) is the splitting field of \( F(p_1, \ldots, p_n) \) for the polynomial \( \Pi(X - x_i) = X^n - p_1X^{n-1} + \cdots + (-1)^np_n \) and the Galois group is \( S_n \).

Proof. (1) For example, \( x_1^3 + 4x_1^2x_2 + 4x_1x_2^2 + x_2^3 = p_1^3 + p_1p_2 \).

We define the multi-degree on polynomials as follows. The multi-degree for \( x_1^{k_1} \cdots x_n^{k_n} \) is \((k_1, \ldots, k_n) \in \mathbb{N}^n\). We use lexicographic order on \( \mathbb{N}^n \). For any polynomial \( f \), let \( x_1^{k_1} \cdots x_n^{k_n} \) be the highest monomial occurring in \( f \) with nonzero coefficient and we call \((k_1, \ldots, k_n) \) the multi-degree of \( f \).

Now for any symmetric polynomial \( f \), its multi-degree is of the form \((k_1, \ldots, k_n) \) for \( k_1 \geq k_2 \geq \cdots \geq k_n \). In other words, there exists \((d_1, \ldots, d_n) \in \mathbb{N}^n \) such that \( k_1 = d_1 + \cdots + d_n, k_2 = d_2 + \cdots + d_n, \ldots, k_n = d_n \). Notice that \( p_1^{d_1} \cdots p_n^{d_n} \) has multi-degree \((k_1, \ldots, k_n) \). Thus \( f - cp_1^{d_1} \cdots p_n^{d_n} \) is again symmetric and has multi-degree strictly less than \((k_1, \ldots, k_n) \), here \( c \) is the coefficient of \( x_1^{k_1} \cdots x_n^{k_n} \) in \( f \). Now part (1) follows from induction on multi-degree.

(2) Let \( f = g/h \) with \( g, h \in F[x_1, \ldots, x_n] \) be a symmetric function. Set \( H = \Pi_{\sigma \in S_n} \sigma(h) \). Then \( H \) and \( Hf \) are symmetric polynomials and hence in \( F[p_1, \ldots, p_n] \). Thus \( f = Hf/H \in F(p_1, \ldots, p_n) \). Therefore \( F(x_1, \ldots, x_n)^{S_n} = F(p_1, \ldots, p_n) \).

**Corollary 2.16.** We define the general polynomial of degree \( n \) to be

\[
    f(X) = X^n - t_1X^{n-1} + \cdots + (-1)^nt_n \in F(t_1, \ldots, t_n)[X].
\]

Then the Galois group of \( f(X) \) over \( F(t_1, \ldots, t_n) \) is \( S_n \).

Proof. The monomials \( p_1^{d_1} \cdots p_n^{d_n} \) for \((d_1, \ldots, d_n) \in \mathbb{N}^n \) are linearly independent since they have different multi-degree as polynomials of \( x_1, \ldots, x_n \). Hence \( p_1, \ldots, p_n \) are algebraically independent. Thus the map \( F[t_1, \ldots, t_n] \to F[p_1, \ldots, p_n], t_i \mapsto p_i \) is bijective. So it extends to an isomorphism \( F(t_1, \ldots, t_n) \to F(p_1, \ldots, p_n) \). Now the corollary follows from part (2) of the previous theorem.

**References**