Field Theory

Theodoulos Garefalakis

May 04, 2026

---

1 Field Theory

1.1 Background

Definition 1.1 An element $p \in R$ is called **prime** if
1. $p \neq 0, p \notin R^*$,
2. $\forall a, b \in R$, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

An element $p \in R$ is called **irreducible** if
1. $p \neq 0, p \notin R^*$,
2. $\forall a, b \in R$, if $p = a \cdot b$ then $a \in R^*$ or $b \in R^*$.

Definition 1.2 An ideal P of R is called **prime** if
1. $P \neq R$,
2. $\forall a, b \in R$, if $ab \in P$ then $a \in P$ or $b \in P$.

An ideal M is called **maximal** if
1. $M \neq R$,
2. If I is an ideal of R such that $M \subsetneq I$, then $I = R$.

Theorem 1.3
1. The ideal P is prime $\iff R/P$ is a domain.
2. The ideal M is maximal $\iff R/M$ is a field.

Proof.
1. Assume that P is prime and consider $a + P, b + P \in R/P$. Assume that $(a + P)(b + P) = 0 + P$.

Then $ab \in P$. Since P is prime, $a \in P$ or $b \in P$. Therefore, $a + P = 0 + P$ or $b + P = 0 + P$. Thus, R/P is a domain.

Conversely, assume that R/P is a domain and let $ab \in P$. Then $(a + P)(b + P) = P$, so $a + P = P$ or $b + P = P$. Therefore, $a \in P$ or $b \in P$, and P is prime.

1. Assume that M is maximal and let $a + M \in R/M$ with $a \notin M$. Then

$M \subsetneq \langle M, a\rangle$, so $\langle M, a\rangle = R$. Thus, $1 = ba + m$ for some $m \in M$ and $b \in R$. It follows that $(a + M)(b + M) = 1 + M$. Therefore, R/M is a field.

Conversely, assume that R/M is a field and let I be an ideal such that $M \subsetneq I$. Then there exists $a \in I \setminus M$. Since R/M is a field, there exists $b \in R$ such that $(a + M)(b + M) = 1 + M$, so $1 = ba + m$ for some $m \in M$. Thus, $1 \in I$, so $I = R$, and M is maximal.

Theorem 1.4 Let R be a PID. Then:
1. $p \in R$ is prime $\iff (p)$ is prime.
2. $p \in R$ is irreducible $\iff (p)$ is maximal.

Theorem 1.5 Let R be a domain. Then every prime is irreducible. If R is a PID, then the converse is also true.

Theorem 1.6 (Eisenstein's Irreducibility Criterion) Let R be a domain and $f(x) = a_n x^n + \cdots + a_0 \in R[x]$. If there exists a prime $p \in R$ such that
1. $p \mid a_i$, $0 \leq i \leq n-1$,
2. $p \nmid a_n$,
3. $p^2 \nmid a_0$,

then $f(x)$ is irreducible in $R[x]$.

Proof. Assume that $f(x) = g(x)h(x)$ with

$$g(x) = g_m x^m + \cdots + g_0 \quad \text{and} \quad h(x) = h_{n-m} x^{n-m} + \cdots + h_0, \tag{1}$$

where $m \geq 1$, $n - m \geq 1$. Then $p \mid a_0 = g_0 h_0$. Assume that $p \mid g_0$ and $p \nmid h_0$ (since $p^2 \nmid a_0$). Then $p \mid a_1 = g_0 h_1 + g_1 h_0$, so $p \mid g_1 h_0$. Since $p \nmid h_0$, $p \mid g_1$. By induction, $p \mid g_0, g_1, \ldots, g_m$. It follows that $p \mid g_m h_{n-m}$, which is a contradiction to the assumption $p \nmid a_n$.

Lemma 1.7 (Gauss) Let R be a UFD and F its field of fractions. Let $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ and assume that $\gcd(a_0, \ldots, a_n) = 1$. Then $f(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.

Proof. If f is irreducible in $F[x]$ then it is irreducible in $R[x]$. Indeed, if $f(x) = g(x)h(x)$ with $\deg g, \deg h \geq 1$, this is a factorization in $F[x]$.

Conversely, assume that f is irreducible in $R[x]$, and assume that $f(x) = g(x)h(x)$ with $g, h \in F[x]$ and $\deg g, \deg h \geq 1$. Let

$$g(x) = \frac{a_n}{b_m} x^n + \cdots + \frac{a_0}{b_n} \quad \text{and} \quad h(x) = \frac{c_{n-m}}{d_{n-m}} x^{n-m} + \cdots + \frac{c_0}{d_0}. \tag{2}$$

If $b = \operatorname{lcm}(b_0, \ldots, b_m)$ and $d = \operatorname{lcm}(d_0, \ldots, d_{n-m})$, then $bd f(x) = ac g_1(x) h_1(x)$ where $g_1, h_1 \in R[x]$ with $\operatorname{cont}(g_1) = \operatorname{cont}(h_1) = 1$. Therefore, $bd \cdot \operatorname{cont}(f) = ac \cdot \operatorname{cont}(g_1 \cdot h_1)$, so $bd = ac$ and $f(x) = g_1(x)h_1(x)$, a contradiction.

Theorem 1.8 Let F be a field and G be a finite subgroup of F^*. Then G is cyclic.

1.2 Field Extensions

Definition 1.9 Let K/F be a field extension. The **characteristic** of R, $\mathrm{char}(R)$, is the smallest positive integer n such that $n \cdot 1_R = 0_R$, or 0 if no such n exists.

Proposition 1.10 If $\mathrm{char}(F) = n > 0$, then n is a prime.

Theorem 1.11 Let K be a field.
- If $\mathrm{char}(K) = 0$ then K contains an isomorphic copy of $\mathbb{Q}$.
- If $\mathrm{char}(K) = p$ then K contains a copy of $\mathbb{F}_p$.

Proof. Consider $\varphi : \mathbb{Z} \to K$, $n \mapsto n \cdot 1$. If $\mathrm{char}(K) = 0$, then φ is injective and K contains $\varphi(\mathbb{Z}) \cong \mathbb{Z}$. Since K is a field, it contains the field of fractions of $\varphi(\mathbb{Z})$, which is isomorphic to $\mathbb{Q}$. If $\mathrm{char}(K) = p$, then $\ker \varphi = (p)$ and $\mathrm{im}(\varphi) \cong \mathbb{Z}/(p) = \mathbb{F}_p$.

Definition 1.12 Let K/F be a field extension and $X \subseteq K$. Define

$$F[X] = \bigcap \{R : R \text{ subring of } K, X \subseteq R, F \subseteq R\}, \tag{3}$$

$$F(X) = \bigcap \{L : L \text{ subfield of } K, X \subseteq L, F \subseteq L\}. \tag{4}$$

Theorem 1.13 Let K/F be a field extension and $\alpha \in K$. Then

$$F[\alpha] = \{f(\alpha) : f \in F[x]\}, \tag{5}$$

$$F(\alpha) = \{f(\alpha)/g(\alpha) : f, g \in F[x], g(\alpha) \neq 0\}. \tag{6}$$

Proof. Denote $R = \{f(\alpha) : f \in F[x]\}$. Clearly R is a subring of K that contains F and α. Therefore $F[\alpha] \subseteq R$. On the other hand, if $f(x) = a_n x^n + \cdots + a_0 \in F[x]$, then every ring S that contains F and α also contains $f(\alpha)$, since it is closed under the operations. So $R \subseteq S$ and therefore R is contained in the intersection, that is, $R \subseteq F[\alpha]$.

The proof of the second statement is similar and is left as an exercise.

Theorem 1.14 Let K/F be a field extension and $\alpha_1, ..., \alpha_m \in K$. Then

$$F[\alpha_1, ..., \alpha_m] = \{f(\alpha_1, ..., \alpha_m) : f \in F[x_1, ..., x_m]\}, \tag{7}$$

$$F(\alpha_1, ..., \alpha_m) = \{f(\alpha_1, ..., \alpha_m)/g(\alpha_1, ..., \alpha_m) : f, g \in F[x_1, ..., x_m], g(\alpha_1, ..., \alpha_m) \neq 0\}. \tag{8}$$

Proof. The proof is essentially the same as that for $m = 1$ and is left as an exercise.

Theorem 1.15 Let K/F be a field extension and $X \subseteq K$. Then

$$F(X) = \bigcup_{\substack{S \subseteq X \\ |S| < \infty}} F(S). \tag{9}$$

Proof. It is clear that $F(S) \subseteq F(X)$ for every finite $S \subseteq X$, so

$$\bigcup_{\substack{S \subseteq X \\ |S| < \infty}} F(S) \subseteq F(X). \tag{10}$$

For the reverse inclusion, it suffices to show that $\bigcup\{F(S) : S \subseteq X, |S| < \infty\}$ is a field that contains F and X. For that, let $\alpha, \beta \in \bigcup\{F(S) : S \subseteq X, |S| < \infty\}$. Then $\alpha \in F(S_1)$ and $\beta \in F(S_2)$ for some finite subets, S_1, S_2, of X. Then $\alpha, \beta \in F(S_1 \cup S_2)$ so $\alpha \pm \beta, \alpha \cdot \beta^{-1} \in F(S_1 \cup S_2)$ and $S_1 \cup S_2$ is a finite subset of X. This shows that $\bigcup\{F(S) : S \subseteq X, |S| < \infty\}$ is closed under the operations and therefore it is a subfield of K, that clearly contains X and F.

Definition 1.16 Let K/F be a field extension. The element $\alpha \in K$ is called **algebraic** over F if there exists a non-zero polynomial $f \in F[x]$ such that $f(\alpha) = 0$. Otherwise, it is called **transcendental** over F.

Example 1.17
- $\sqrt{2}$ is algebraic over $\mathbb{Q}$, since it is a root of $x^2 - 2 \in \mathbb{Q}[x]$.
- $i \in \mathbb{C}$ is a root of $x^2 + 1 \in \mathbb{Q}[x]$ and therefore it is algebraic over $\mathbb{Q}$.
- Every element of F is algebraic over F, for every field F.
- π is not algebraic over $\mathbb{Q}$, but of course it is algebraic over $\mathbb{R}$.

Definition 1.18 Let α be algebraic over F. The unique monic polynomial of least degree, $f \in F[x]$, such that $f(\alpha) = 0$ is called the **minimal polynomial** of α over F, and is denoted by $\min(F, \alpha)$.

Lemma 1.19 Let F be a field and α be algebraic over F. For every $f \in F[x]$,

$$f(\alpha) = 0 \quad \Leftrightarrow \quad \min(F, \alpha) \mid f \tag{11}$$

Proof. Euclidean division in $F[x]$ gives us polynomials $q, r \in F[x]$, such that, $f = q \min(F, \alpha) + r$ and either $r = 0$ or $\deg(r) < \deg(\min(F, \alpha))$. Since $f(\alpha) = r(\alpha)$ and $\min(F, \alpha)$ is the monic polynomial of minimum degree that has α as a root, we necessarily have $f(\alpha) = 0 \Leftrightarrow r = 0$.

Lemma 1.20 Let F be a field and α be algebraic over F. Then $\min(F, \alpha)$ is irreducible in $F[x]$.

Proof. If it were reducible there would be monic polynomials $g, h \in F[x]$ each of degree at least 1 and at most $\deg(\min(F, \alpha)) - 1$ such that $f = g \cdot h$. Then $0 = f(\alpha) = g(\alpha)h(\alpha)$ and we would have either $g(\alpha) = 0$ or $h(\alpha) = 0$ (or both). This would contradict the minimality of the degree of $\min(F, \alpha)$.

Example 1.21
1. If $f \in F[x]$ is irreducible and α is a root of f, then $f = \min(F, \alpha)$.
2. Every $a \in F$ is algebraic over F, with $\min(F, a) = x - a \in F[x]$.
3. Since $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible (by Eisenstein's Criterion) and has $\sqrt{2}$ as a root, $\min\left(\mathbb{Q}, \sqrt{2}\right) = x^2 - 2$.

Consider the evaluation-at-α homomorphism

$$\mathrm{ev}_\alpha : F[x] \to K, \mathrm{ev}_\alpha(f) = f(\alpha). \tag{12}$$

Then $\ker(\mathrm{ev}_\alpha) = (P_\alpha)$ for some monic $P_\alpha \in F[x]$. Evidently, $P_\alpha = \min(F, \alpha)$.

Theorem 1.22 Let α be algebraic over F. Then
1. $F[\alpha] = F(\alpha)$
2. $[F(\alpha) : F] = \deg(\min(F, \alpha))$

Proof.
1. We know that $F[\alpha] \subseteq F(\alpha)$. If we show that $F[\alpha]$ is a field we are done. Let $P_\alpha = \min(F, \alpha)$. The evaluation at α homomorphism $\mathrm{ev}_\alpha : F[x] \to F[\alpha]$, $f \mapsto f(\alpha)$ is an epimorphism with kernel (P_α). Then $F[x]/(P_\alpha) \cong F[\alpha]$. But P_α is irreducible in $F[x]$, so $F[x]/(P_\alpha)$ is a field.
2. Let $n = \deg P_\alpha$ and let $f \in F[x]$. Then $f = g \cdot P_\alpha + r$, $r = 0$ or $\deg r < n$, and $f(\alpha) = r(\alpha)$. It follows that the set $\{1, \alpha, ..., \alpha^{n-1}\}$ generates $F(\alpha)$ as an F-space. If it were linearly dependent, α would be the root of a polynomial of degree $< n$, a contradiction.

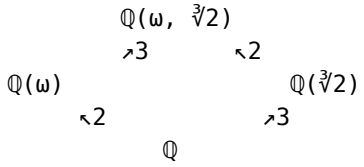
Theorem 1.23 Let $F \subseteq L \subseteq K$ be fields. Then K/F is finite if and only if K/L and L/F are finite. In this case $[K : F] = [K : L][L : F]$.

Proof. Assume that $[K : F] = n \in \mathbb{N}$, and $\{\gamma_1, ..., \gamma_n\}$ is an F-basis of K. Then L is an F-subspace of K so L/F is finite. Every element α of K is expressed as $\alpha = c_1\gamma_1 + ... + c_n\gamma_n$ with $c_i \in F \subseteq L$, so $\{\gamma_1, ..., \gamma_n\}$ generates K as an L-space. It follows that $[K : L]$ is finite.

Conversely, if $[K : L] = m$, $[L : F] = k$ we will show that $[K : F] = m \cdot k$. If $\{\alpha_1, ..., \alpha_m\}$ is a basis of K/L and $\{\beta_1, ..., \beta_k\}$ a basis of L/F, then $\{\alpha_i\beta_j : 1 \leq i \leq m, 1 \leq j \leq k\}$ is a basis of K/F.

$\alpha \in K$ can be written as $\alpha = \sum_{i=1}^{m} b_i \alpha_i$, $b_i \in L$ and $b_i = \sum_{j=1}^{k} c_{ij}\beta_j$ with $c_{ij} \in F$. So $\alpha = \sum_i \sum_j c_{ij}\alpha_i\beta_j$. Show that the set is also linearly independent over F.

Example 1.24 We will compute the degree of $\left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right) : \mathbb{Q}\right]$, where ω is a root of $x^2 + x + 1 \in \mathbb{Q}[x]$.



- $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ because $\min(\mathbb{Q}, \omega) = x^2 + x + 1$.
- $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$ because $\min\left(\mathbb{Q}, \sqrt[3]{2}\right) = x^3 - 2$.

Let $\left[Q\left(\omega, \sqrt[3]{2}\right) : Q(\omega)\right] = d$ and $\left[Q\left(\omega, \sqrt[3]{2}\right) : Q\left(\sqrt[3]{2}\right)\right] = l$. Then $2d = 3l \Longrightarrow 3 \mid d$ and $2 \mid l$. Also $\min\left(Q(\omega), \sqrt[3]{2}\right) \mid x^3 - 2$, so $d \leq 3$. Therefore $d = 3$ (and also $l = 2$), and $\left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right) : \mathbb{Q}\right] = 6$. Note, that the above argument shows that $\left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right) : \mathbb{Q}(\omega)\right] = \deg(\min\left(\mathbb{Q}(\omega), \sqrt[3]{2}\right) = 3$, and since $\min\left(\mathbb{Q}(\omega), \sqrt[3]{2}\right) \mid x^3 - 2$, it follows that $\min\left(\mathbb{Q}(\omega), \sqrt[3]{2}\right) = x^3 - 2$. In particular, $x^3 - 2$ remains irreducible in $\mathbb{Q}(\omega)[x]$.

Theorem 1.25 Let $\alpha_1, ..., \alpha_m$ be algebraic over F. Then

$$[F(\alpha_1, ..., \alpha_m) : F] \leq \prod_{i=1}^{m} [F(\alpha_i) : F]. \tag{13}$$

Proof. Induction on m. For $m = 1$ it is clear. Assume $[F(\alpha_1, ..., \alpha_{m-1}) : F] \leq \prod_{i=1}^{m-1} [F(\alpha_i) : F]$. Then

$$\begin{aligned} [F(\alpha_1, ..., \alpha_m) : F] &= [F(\alpha_1, ..., \alpha_m) : F(\alpha_1, ..., \alpha_{m-1})] \cdot [F(\alpha_1, ..., \alpha_{m-1}) : F] \\ &\leq [L(\alpha_m) : L] \prod_{i=1}^{m-1} [F(\alpha_i) : F], \end{aligned} \tag{14}$$

where $L = F(\alpha_1, ..., \alpha_{m-1})$. But $[L(\alpha_m) : L] \leq [F(\alpha_m) : F]$ since the $\min(F, \alpha_m)$ is a polynomial in $L[x]$ that is zero at α, and therefore is divisible by $\min(L, \alpha_m)$.

Theorem 1.26 Let $F \subseteq K$ be finite. Then it is algebraic.

Proof. Let $[K : F] = n$ and let $\alpha \in K$. The set $\{1, \alpha, ..., \alpha^n\}$ is linearly dependent over F, so $c_0 + c_1\alpha + ... + c_n\alpha^n = 0$ with $c_i \in F$, not all equal to 0.

Theorem 1.27 The extension K/F is finite if and only if it is algebraic and finitely generated.

Corollary 1.28 If $\alpha_1, ..., \alpha_m$ are algebraic over F, then the extension $F(\alpha_1, ..., \alpha_n)$ is algebraic.

Proof. Each of $[F(\alpha_i) : F]$ is finite, so $[F(\alpha_1, ..., \alpha_m) : F]$ is finite, thus algebraic.

Definition 1.29 Let $F \subseteq K$ and define

$$L = \{\alpha \in K : \alpha \text{ is algebraic over } F\}. \tag{15}$$

L is a field extension of F called the **algebraic closure** of F in K.

L clearly contains F. If $\alpha, \beta \in L$, then α, β are algebraic over F, so $F(\alpha, \beta)$ is algebraic over F. Since $\alpha \pm \beta, \alpha \cdot \beta^{-1} \in F(\alpha, \beta)$, they are algebraic over F and therefore are contained in L. So L is a subfield of K.

The algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, lets denote it by $\overline{\mathbb{Q}}$, is an algebraic extension of $\mathbb{Q}$, but it is not finite (and therefore not finitely generated over $\mathbb{Q}$). Indeed, the polynomial $x^n - 2 \in \mathbb{Q}[x]$ is irreducible for every $n \in \mathbb{N}$ and has $\sqrt[n]{2}$ as a root. It follows that $\sqrt[n]{2} \in \overline{\mathbb{Q}}$, so $\mathbb{Q}\left(\sqrt[n]{2}\right) \leq \overline{\mathbb{Q}}$ and $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] \geq \left[\mathbb{Q}\left(\sqrt[n]{2}\right) : \mathbb{Q}\right] = n$.

Theorem 1.30 Let $F \leq L \leq K$ be fields. K/F is algebraic if and only if K/L and L/F are algebraic.

Proof. Assume that K/F is algebraic. Then every $\alpha \in K$ is algebraic over F, so L/F is algebraic. Every $\alpha \in K$ is a root of some monic polynomial in $F[x]$. Every such polynomial may be viewed as a polynomial in $L[x]$, so K/L is algebraic.

Conversely, assume that K/L and L/F are algebraic and let $\alpha \in K$. Then $[L(\alpha) : L] = n \in \mathbb{N}$ and $\min(L, \alpha) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ for some $c_0, ..., c_{n-1} \in L$. Define $L_0 = F(c_0, ..., c_{n-1})$. Then L_0/F is algebraic and finitely generated, so finite. Also, $\min(L, \alpha) \in L_0[x]$, so $\min(L_0, \alpha) \mid \min(L, \alpha)$ (in fact $\min(L_0, \alpha) = \min(L, \alpha)$), therefore $[L_0(\alpha) : L_0] \leq [L(\alpha) : L] = n$. Note now that $[L_0(\alpha) : F] = [L_0(\alpha) : L_0] \cdot [L_0 : F] < \infty$ and that $F(\alpha) \leq L_0(\alpha)$. Therefore, $[F(\alpha) : F] < \infty$ and α is algebraic over F.

1.3 Splitting Fields

Theorem 1.31 Let F be a field, $f \in F[x]$ be an irreducible polynomial. There exists an extension of F that contains a root of f.

Proof. Since f is irreducible, $F[x]/(f)$ is a field. If $\deg f = n$, then

$$F[x]/(f) = \{g + (f) : g \in F[x]\}. \tag{16}$$

By Euclidean division, $g = h \cdot f + r$ for some $r \in F[x]$ with $r = 0$ or $\deg r < n$. Then $g + (f) = r + (f)$. Therefore,

$$F[x]/(f) = \{r + (f) : r \in F[x], r = 0 \text{ or } \deg r < n\}. \tag{17}$$

The classes in the above set are distinct. We can write

$$F[x]/(f) = \{\overline{a}_0 + \overline{a}_1\overline{x} + \cdots + \overline{a}_{n-1}\overline{x}^{n-1} : a_i \in F, 0 \leq i \leq n-1\}, \tag{18}$$

where $\overline{h}$ denotes $h + (f)$. $K = F[x]/(f)$ contains a copy of F, since $F \hookrightarrow K$, $a \mapsto \overline{a}$ is a field monomorphism. Identifying F with its image, we have

$$K = \{a_0 + a_1\overline{x} + \cdots + a_{n-1}\overline{x}^{n-1} : a_i \in F\}. \tag{19}$$

Note now that $\overline{x}$ is a root of f: if $f(x) = f_0 + f_1x + \cdots + f_nx^n$, then

$$f(\overline{x}) = f_0 + f_1\overline{x} + \cdots + f_n\overline{x}^n = \overline{f_0 + f_1x + \cdots + f_nx^n} = 0. \tag{20}$$

In particular, note that $K = F(\alpha)$ if $\alpha = \overline{x}$.

Example 1.32

1. $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's Criterion. Then $\mathbb{Q}[x]/(x^2-2)$ is a field that contains a root of $x^2 - 2$. If we denote this root by $\sqrt{2}$, then
$$\mathbb{Q}[x]/(x^2-2) = \left\{a_0 + a_1 \cdot \sqrt{2} : a_0, a_1 \in \mathbb{Q}\right\} = \mathbb{Q}\left(\sqrt{2}\right). \tag{21}$$
2. $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible, because it has no roots in $\mathbb{F}_2$ and is of degree 2. Then $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a field that contains a root α of $x^2 + x + 1$. Therefore
$$\mathbb{F}_2[x]/(x^2 + x + 1) = \mathbb{F}_2(\alpha) \text{ with } \alpha^2 + \alpha + 1 = 0. \tag{22}$$

Theorem 1.33 Let F be a field and $\{f_1, \ldots, f_m\} \subseteq F[x]$ be a set of non-constant polynomials. There exists a finite field extension K of F that contains all roots of all polynomials in the set.

Proof. Letting $f = f_1 \cdots f_m$, we see that we need to construct a field K that contains F and all roots of f. We prove it by induction on $\deg f = n$.

For $n = 1$, f has a root in F, so $K = F$. Assume that such an extension exists for every polynomial f of degree $< n$. Let now $\deg f = n$ and let P be an irreducible factor of f. There exists an extension L of F that contains some root α of P. Then $f = (x - \alpha) \cdot g$ with $g \in L[x]$ and $\deg g = n - 1$. By the induction hypothesis, there exists an extension K of L that contains all roots of g. So K contains all roots of f.

Extend the proof to show that $[K : F] \leq n!$, where $n = \deg(f_1 \cdots f_m)$

Definition 1.34 Let $f \in F[x]$ and K an extension of F. We say that f **splits** in K if there exist $c \in F$ and $\alpha_1, ..., \alpha_n \in K$ and $f(x) = c(x - \alpha_1)...(x - \alpha_n)$.

A field K is called a **splitting field** of a set of polynomials $S \subset F[x]$ if it is of the form $K = F(X)$, where X is the set of roots of every polynomial in S. It is the smallest extension of F where every polynomial in S splits.

Theorem 1.35 Let $S \subset F[x]$ be finite. There exists a splitting field of S over F.

Proof. By the previous theorem, there exists a field K that extends F and contains the set of all roots of all polynomials in S, call it X. Then $F(X)$ is a splitting field for S over F.

Example 1.36

1. $\mathbb{Q}\left(\sqrt{2}\right)$ is a splitting field of $x^2 - 2$ over $\mathbb{Q}$.
2. $\mathbb{Q}\left(\sqrt[3]{2}\right)$ is not a splitting field of $x^3 - 2$ over $\mathbb{Q}$. The roots of $x^3 - 2$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, where ω is a root of $x^2 + x + 1$ which is irreducible over $\mathbb{Q}$.
3. If $f \in F[x]$ is irreducible of degree n, and K is a splitting field of K over F, then $[K : F]$ can be as small as n or as large as $n!$. For example $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 = \deg(x^2 - 2)$. The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$ and $\left[\mathbb{Q}\left(\sqrt[3]{2}, \omega\right) : \mathbb{Q}\right] = 6 = 3!$

Example 1.37 Consider the polynomial $f = x^4 - 2x^3 + 6x^2 - 6x + 9 \in \mathbb{Q}[x]$ and note that $i\sqrt{3}$ is one of its roots. We see that $\min\left(\mathbb{Q}, i\sqrt{3}\right) = x^2 + 3$, so $x^2 + 3 \mid f$. By Euclidean division we have $f = (x^2 + 3)(x^2 - 2x + 3)$. Therefore, the roots of f are $\pm i\sqrt{3}$, $1 \pm i\sqrt{2}$, and the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}\left(i\sqrt{2}, i\sqrt{3}\right)$. Considering the tower $\mathbb{Q} \leq \mathbb{Q}\left(i\sqrt{2}\right) \leq \mathbb{Q}\left(i\sqrt{2}, i\sqrt{3}\right)$, we have

$$\left[\mathbb{Q}\left(i\sqrt{2}\right) : \mathbb{Q}\right] = \deg(x^2 + 2) = 2 \tag{23}$$

and

$$\left[\mathbb{Q}\left(i\sqrt{2}, i\sqrt{3}\right) : \mathbb{Q}\left(i\sqrt{2}\right)\right] = \deg\left(\min\left(\mathbb{Q}\left(i\sqrt{2}\right), i\sqrt{3}\right)\right). \tag{24}$$

Since $\min\left(\mathbb{Q}\left(i\sqrt{2}\right), i\sqrt{3}\right) \mid x^2 + 3$, we see that $\left[\mathbb{Q}\left(i\sqrt{2}, i\sqrt{3}\right) : \mathbb{Q}\left(i\sqrt{2}\right)\right] = 1$ or 2. If the degree were equal to 1, we would have $\mathbb{Q}\left(i\sqrt{2}, i\sqrt{3}\right) = \mathbb{Q}\left(i\sqrt{2}\right)$ and $i\sqrt{3} = a + bi\sqrt{2}$ for some $a, b \in \mathbb{Q}$. This leads to $(a^2 - 2b^2 + 3) + (2ab)i\sqrt{2} = 0$. Since $\left\{1, i\sqrt{2}\right\}$ is linearly independent over $\mathbb{Q}$ (as a basis of $\mathbb{Q}\left(i\sqrt{2}\right)/\mathbb{Q}$), we obtain the system

$$\begin{cases} a^2 - 2b^2 + 3 = 0 \\ 2ab \qquad\quad = 0 \end{cases} \Leftrightarrow \begin{cases} 2b^2 = 3 \\ a \;\; = 0 \end{cases} \quad \text{or} \quad \begin{cases} a^2 = -3 \\ b \;\; = 0 \end{cases} \tag{25}$$

which is impossible. It follows that $\left[\mathbb{Q}\left(i\sqrt{2}, i\sqrt{3}\right) : \mathbb{Q}\left(i\sqrt{2}\right)\right] = 2$ and $\left[\mathbb{Q}\left(i\sqrt{2}, i\sqrt{3}\right) : \mathbb{Q}\right] = 4$.

1.4 Algebraic Closure

Definition 1.38 A field K is called **algebraically closed** if the only algebraic extension of K is K itself.

Proposition 1.39 Let K be a field. The following are equivalent:
1. K is algebraically closed.
2. The only finite extension of K is K itself.
3. If L is an extension of K then $K = \{\alpha \in L : \alpha \text{ is algebraic over } K\}$.
4. Every irreducible polynomial in $K[x]$ splits in K.
5. Every irreducible polynomial in $K[x]$ has a root in K.
6. Every irreducible polynomial in $K[x]$ has degree 1.

Proof.
- (1) $\Rightarrow$ (2) If L/K is finite then it is algebraic, so by assumption, $L = K$.
- (2) $\Rightarrow$ (3) Clearly $K \subseteq \{\alpha \in L : \alpha \text{ is algebraic over } K\}$, since every $\alpha \in K$ is algebraic over K. If $\alpha \in L$ and α is algebraic over K, then $K(\alpha)$ is algebraic over K, so by assumption $K(\alpha) = K$. This implies $\alpha \in K$.
- (3) $\Rightarrow$ (4) Let $f \in K[x]$ be irreducible and let L be a splitting field of f over K. Then the roots of f belong to L and are algebraic over K, so by assumption they belong to K.
- (4) $\Rightarrow$ (5) Obvious.
- (5) $\Rightarrow$ (6) Let $f \in K[x]$ be irreducible. Then it has a root $\alpha \in K$, so $f = (x - \alpha) \cdot g$ with $g \in K[x]$. Since f is irreducible, g is a unit of $K[x]$, that is $g = c \in K^*$.
- (6) $\Rightarrow$ (1) Let L be an algebraic extension of K and $\alpha \in L$. Then $f = \min(K, \alpha)$ is irreducible over K, so $f = x - \alpha$ and $\alpha \in K$. Therefore $L = K$.

Definition 1.40 Let F be a field. An extension K of F is called an **algebraic closure** of F if it is algebraically closed and is algebraic over F.

Lemma 1.41 Let L be an algebraically closed extension of F. Then $K = \{\alpha \in L : \alpha \text{ is algebraic over } F\}$ is an algebraic closure of F.

Proof. We already know that K/F is algebraic. Let $f \in K[x]$ be non-constant. Then $f \in L[x]$, and since L is algebraically closed it contains a root α of f. But then $K(\alpha)/K$ and K/F are algebraic, so $K(\alpha)/F$ is algebraic, so α is algebraic over F, therefore $\alpha \in K$. It follows that every non-constant polynomial in $K[x]$ has a root in K, so K is algebraically closed.

Theorem 1.42 Every field F has an algebraically closed extension.

Proof. Omitted.

Theorem 1.43 Every field F has an algebraic closure.

Proof. Follows immediately from the previous theorem and lemma.

2 Galois Theory

Let $\sigma : K \to L$ be field homomorphism. Since $\ker(\sigma)$ is an ideal of K and K is a field, $\ker(\sigma)$ is either K or $\{0\}$. This means that σ either is the zero map, or it is injective. If both K and L are extensions of F, and if σ fixes F, that is, $\sigma(a) = a$ for every $a \in F$, then σ is injective. We say that σ is an *F-homomorphism* (*F-isomorphism*, *F-automorphism*) if σ is a homomorphism (resp. isomorphism, automorphism) and it fixes F. We denote by $\mathrm{Hom}_F(K, L)$ the set of F-homomorphisms from K to L. If $K = L$, we denote $\mathrm{End}_F(K) = \mathrm{Hom}_F(K, K)$. The set of endomorphisms $\mathrm{End}_F(K)$ equipped with pointwise addition and function composition, forms a ring. $\mathrm{Aut}_F(K) = \{\sigma \in \mathrm{End}_F(K) : \sigma \text{ is an automorphism}\}$ equipped with function compositin is a group. We denote $\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K)$ and call it the **Galois group** of the extension.

Note that every $\sigma \in \mathrm{Hom}_F(K, L)$ is F-linear map. Indeed, for $\alpha, \beta \in K$ and $c \in F$, we have

$$\sigma(c\alpha + \beta) = \sigma(c)\sigma(\alpha) + \sigma(\beta) = c\sigma(\alpha) + \sigma(\beta). \tag{26}$$

If $[K : F] < \infty$, every $\sigma \in \mathrm{End}_F(K)$ defines an injective F-linear map $\sigma : K \to K$, which must be surjective, so $\mathrm{End}_F(K) = \mathrm{Aut}_F(K)$.

Any field isomorphism $\sigma : F \to F'$ induces an ring isomorphism $\sigma^* : F[x] \to F'[x]$, defined as

$$\sigma^*\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \sigma(a_i) x^i. \tag{27}$$

Lemma 2.1 Let $\sigma : F \to F'$ be a field isomorphism. Then $f \in F[x]$ is irreducible if and only if $\sigma^*(f)$ is irreducible.

Theorem 2.2 Let $K/F, K'/F'$ be field extensions, $\sigma : F \to F'$ be an isomorphism, $f \in F[x]$, $f' = \sigma^*(f) \in F'[x]$. Assume that f is irreducible in $F[x]$ and let α be a root of f in K, and α' a root of f' in K'. Then σ can be extended to $\rho : F(\alpha) \to F'(\alpha')$ with $\rho(\alpha) = \alpha'$.

Proof.

$$F(\alpha) \xrightarrow{\sim} F[x]/(f) \xrightarrow{\overline{\sigma}} F'[x]/(f') \xrightarrow{\sim} F'(\alpha') \tag{28}$$

where $\overline{\sigma}(h + (f)) = \sigma^*(h) + (f')$. The map $\overline{\sigma}$ is well defined: if $h_1 + (f) = h_2 + (f)$, then $h_1 - h_2 = g \cdot f$ for some $g \in F[x]$, so $\sigma^*(h_1 - h_2) = \sigma^*(g) \cdot \sigma^*(f)$, hence $\sigma^*(h_1) - \sigma^*(h_2) \in (f')$.

$\overline{\sigma}$ is a field homomorphism (check it!)

$\overline{\sigma}$ is non-zero: Indeed, $\overline{\sigma}(1+(f)) = 1+(f')$. As a non-zero field homomorphism, $\overline{\sigma}$ is injective.

$\overline{\sigma}$ is surjective: Let $h'+(f') \in F'[x]/(f')$. There exists (a unique) $h \in F[x]$ such that $\sigma^*(h) = h'$. Then $\overline{\sigma}(h+(f)) = \sigma^*(h)+(f') = h'+(f')$.

ρ is the composition of isomorphisms. Further,

$$\alpha \mapsto x+(f) \mapsto x+(f') \mapsto \alpha'. \tag{29}$$

Theorem 2.3 Let $\sigma : F \to F'$ be a field isomorphism and $f \in F[x]$. Let K be a splitting field of f over F and K' be a splitting field of $f' = \sigma^*(f)$ over F'. There exists an isomorphism $\rho : K \to K'$ that extends σ. If α is a root of f, then ρ may be chosen so that $\rho(\alpha) = \alpha'$, where α' is a root of $\sigma^*(\min(F,\alpha))$.

Proof. We prove the statement by induction on $[K:F]$. If $[K:F]=1$, then f splits over F and $\rho = \sigma$. Assume the statement is true for any field extension K/F of degree $< n$ and any polynomial $f \in F[x]$. For the induction step, let K be a splitting field of $f \in F[x]$ and $[K:F] < n$. Let $P(x)$ be an irreducible factor of $f(x)$ of degree at least 2, that has α as a root. Then σ may be extended to $\tau : F(\alpha) \to F'(\alpha')$, with $\tau(\alpha) = \alpha'$ and α' is a root of $\sigma^*(P)$. Then $[K:F] = [K:F(\alpha)]\cdot[F(\alpha):F]$, and by construction $[F(\alpha):F] > 1$, so $[K:F(\alpha)] < [K:F]$. Furthermore, $f(x) = (x-\alpha)g(x)$, with $g \in F(\alpha)[x]$, $f'(x) = (x-\alpha')g'(x)$, where $g' = \tau^*(g) \in F'(\alpha')[x]$, K is a splitting field of g over $F(\alpha)$ and K' is a splitting field of g' over $F'(\alpha')$. By the induction hypothesis, τ can be exteded to $\rho : K \to K'$, and $\rho(\alpha) = \tau(\alpha) = \alpha'$.

Note that $\rho(\alpha)$ *has* to be a root of $\sigma^*(\min(F,\alpha))$. The Isomorphism Extension Theorem guaranties that ρ can be chosen so that $\rho(\alpha) = \alpha'$ for any root, α' of $\sigma^*(\min(F,\alpha))$. More generaly, for any $\beta \in K$, $\rho(\beta)$ is a root of $\sigma^*(\min(F,\beta))$. Indeed, if $P = \sum_{i=0}^m a_i x^i = \min(F,\beta)$, then

$$\sigma^*(P)(\rho(\beta)) = \sum_{i=0}^n \sigma(a_i)\rho(\beta)^i = \sum_{i=0}^n \rho(a_i)\rho(\beta^i) = \rho\left(\sum_{i=0}^n a_i\beta^i\right) = \rho(0) = 0. \tag{30}$$

A special, but important, case of Theorem 2.3 is for $F' = F$ and $\sigma = \mathrm{id} : F \to F$.

Theorem 2.4 Let $f \in F[x]$ and let K, K' be splitting fields of f over F. Then there exist an F-isomophism $\rho : K \to K'$. Moreover, if $\alpha \in K$ is a root of K, then ρ can be chosen so that $\rho(\alpha) = \alpha'$, where α' is a root of $\min(F,\alpha)$ in K'.

Example 2.5 The field $K = \mathbb{Q}\left(\omega, \sqrt[3]{2}\right)$, where ω is a root of $x^2+x+1 \in \mathbb{Q}[x]$ is the splitting field of x^3-2 over $\mathbb{Q}$. The intermediate field $\mathbb{Q} \le \mathbb{Q}(\omega) \le K$ is the splitting field of x^2+x+1 over $\mathbb{Q}$. By Theorem 2.3, $\mathrm{id} : \mathbb{Q} \to \mathbb{Q}$ can be extended to $\tau_i : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ and may be chosen so that $\tau_i(\omega) = \omega^i$ for $i = 1, 2$. Note that x^3-2 is irreducible in $\mathbb{Q}(\omega)[x]$ with roots $\omega^j\sqrt[3]{2}$, for $j = 0, 1, 2$.

One more application of Theorem 2.3, this time for the extension $K/\mathbb{Q}(\omega)$, gives the isomorphisms $\rho_{i,j} : K \to K$, such that

$$\rho_{i,j}(\omega) = \omega^i, \rho\left(\sqrt[3]{2}\right) = \omega^j \sqrt[3]{2} \quad \text{for} \quad 1 \leq i \leq 2, 0 \leq j \leq 2 \tag{31}$$

where each $\rho_{i,j}$ extends τ_i.

For a finite set of polynomials $S = \{f_1, ..., f_m\} \subset F[x]$, the set of roots of all polynomials in S is the same as the set of roots of $f = f_1 \cdots f_m$, so Theorem 2.3 can be extended to splitting fields of finite sets of polynomials. It is possible to prove a general Isomorphism Extension Theorem, for arbitraty sets of polynomials $S \subseteq F[x]$ (using Zorn's Lemma).

Theorem 2.6 (Isomorphism Extension Theorem) Let $\sigma : F \to F'$ be a field isomorphism and $S = \{f_i\} \subseteq F[x]$. Let K be a splitting field of S over F and K' be a splitting field of $S' = \{\sigma^*(f_i)\}$ over F'. There exists an isomorphism $\rho : K \to K'$ that extends σ. If α is a root of some $f \in S$, then ρ may be chosen so that $\rho(\alpha) = \alpha'$, where α' is a root of $\sigma^*(\min(F, \alpha))$.

If S is the set of all non-constant polynomials in $F[x]$, then a splitting field K of S over F is an algebraic closure of F. If we apply the Isomorphism Extension Theorem, with $F' = F$ and $\sigma = \mathrm{id} : F \to F$, we see that any two algebraic closures of a field F are isomorphic.

2.1 Normal Extensions

Definition 2.7 A field extension K/F is **normal** if K is the splitting field of a set of polynomials $S \subset F[x]$.

Theorem 2.8 Let K/F be a field extension. The following are equivalent:
1. K is normal over F.
2. If an irreducible polynomial $P \in F[x]$ has a root in K, then it splits in K.

Proof.

- (2) $\Rightarrow$ (1) Let $S = \{\min(F, \alpha) : \alpha \in K\}$. Then K is the splitting field of S over F.
- (1) $\Rightarrow$ (2) Suppose that $K = F(X)$, where X is the set of all the roots of a set of polynomials $S \subseteq F[x]$. Consider any irreducible $P \in F[x]$ and assume that $\alpha \in K$ is a root of P. Then

$$\alpha = \frac{h_1(\gamma_1, ..., \gamma_m)}{h_2(\gamma_1, ..., \gamma_m)} \quad \text{for} \quad h_1, h_2 \in F[x_1, ..., x_m] \quad \text{and} \quad \gamma_1, ..., \gamma_m \in X. \tag{32}$$

  Let M be a splitting field of $S \cup \{P\}$ over F. Let β be any root of P. Then $\beta \in M$. By the Isomorphism Extension Theorem, we get an F-isomorphism

$$\rho : M \longrightarrow M \quad \text{with} \quad \rho(\alpha) = \beta. \tag{33}$$

  Note now that $\rho(h_i(\gamma_1, ..., \gamma_m)) = h_i(\rho(\gamma_1), ..., \rho(\gamma_m))$. But ρ maps γ_i to some root of $\min(F, \gamma_i)$, which is already in X. So $\rho(\gamma_i) \in X$ and therefore

$$\beta = \rho(\alpha) = \frac{\rho(h_1(\gamma_1, ..., \gamma_m))}{\rho(h_2(\gamma_1, ..., \gamma_m))} = \frac{h_1(\rho(\gamma_1), ..., \rho(\gamma_m))}{h_2(\rho(\gamma_1), ..., \rho(\gamma_m))} \in F(X) = K. \tag{34}$$

Example 2.9 $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ is not normal, since the irreducible polynomial $x^3 - 2$ has one root in $\mathbb{Q}\left(\sqrt[3]{2}\right)$ but does not split there.

Proposition 2.10 Any field extension K/F of degree 2 is normal.

Proof. Since $[K : F] = 2$, there exists some $a \in K \setminus F$. Then $F \subsetneq F(\alpha) \subseteq K$ and

$$2 = [K : F] = [K : F(\alpha)] \cdot [F(\alpha) : F]. \tag{35}$$

It follows that $[K : F(\alpha)] = 1$, that is, $K = F(\alpha)$. The roots of $\min(F, \alpha) = x^2 + bx + c \in F[x]$ are α and $\beta = -b - \alpha$, so the splitting field of $\min(F, \alpha)$ is $F(\alpha, \beta) = F(\alpha) = K$.

Example 2.11 Note that "normality" is not transitive: If K/L and L/F, it is not true, in general, that K/F is normal. As an example, consider the fields $F = \mathbb{Q}$, $L = \mathbb{Q}\left(\sqrt{2}\right)$ and $K = \mathbb{Q}\left(\sqrt[4]{2}\right)$. Each extension K/L and L/F is of degree 2, therefore normal. However, the extension K/F is not normal, since the irreducible polynomial $x^4 - 2 \in F[x]$ has a root in K, but does not split there.

Proposition 2.12 Let K/F be a normal extension and $F \leq L \leq K$. Then K/L is normal.

Proof. If $K = F(X)$, where X is the set of roots of $S \subseteq F[x]$, then $K = F(X) \subseteq L(X) \subseteq K$, so $K = L(X)$. Since S is a set of polynomials in $L[x]$, K is the splitting field of S over L.

Alterantively, one may use Theorem 2.8: Let $P \in L[x]$ be a irreducible polynomial and $\alpha \in K$ be a root of P. We will prove that P splits in K. Indeed, if $f = \min(F, \alpha)$, then $P \mid f$ and f splits in K, since it has a root in K and K/F is normal. Therefore P splits in K.

Theorem 2.8 yields the following variation of the Isomorphism Extension Theorem.

Theorem 2.13 Let K/F be a normal extension and $\alpha \in K$ and β be any root of $\min(F, \alpha)$. There exists some $\rho \in \mathrm{Gal}(K/F)$ such that $\rho(\alpha) = \beta$.

Proof. Let $P = \min(F, \alpha)$. By Theorem 2.8 we know that P splits in K, so $\beta \in K$. Let L be the splitting field of P over F. By Theorem 2.3, there exists an F-isomorphism $\tau : L \to L$, such that $\tau(\alpha) = \beta$. Since K/L is also normal, the Isomorphism Extension Theorem allows us to extend τ to an F-isomorphism $\rho : K \to K$. Note that $\rho \in \mathrm{Gal}(K/F)$ and $\rho(\alpha) = \tau(\alpha) = \beta$.

2.2 Separable Extensions

Let $f \in F[x]$ be a polynomial of degree n and let $\alpha_1, ..., \alpha_m$ be the distinct roots of f in some splitting field K. Then $f = c(x-\alpha_1)^{e_1} \cdots (x-\alpha_m)^{e_m}$ for some $c \in F$ and $e_1, ..., e_m \in \mathbb{N}$. The root α_i is called simple if $e_i = 1$. The exponent e_i is called the multiplicity of α_i (as a root of f). Equivalently, the multiplicity of the root α_i is the largest positive integer e_i such that $(x-\alpha_i)^{e_i} \mid f$ (the divisibility is considered in $K[x]$) and it is called simple if it has multiplicity 1.

Definition 2.14

1. An irreducible polynomial $P \in F[x]$ is separable over F, if all its roots are simple.
2. A polynomial $f \in F[x]$ is separable over F, if all its irreducible factors in F[x] are separable.
3. An element α, that is algebraic over F, is separable over F, if $\min(F, \alpha)$ is separable over F.

Example 2.15

1. The polynomial $x^2 + x + 1 \in \mathbb{Q}[x]$ is separable over $\mathbb{Q}$ since it is irreducible in $\mathbb{Q}[x]$ and has two distinct roots of multiplicity 1.
2. The polynomial $x^2 - 2x + 1 \in \mathbb{Q}[x]$ is separable over $\mathbb{Q}$ since $x^2 - 2x + 1 = (x-1)^2$ and its only irreducible factor in $\mathbb{Q}[x]$ is $x - 1$ and is separable.
3. For every field F, every polynomial $f \in F[x]$ of degree 1 is separable over F. It follows that every $a \in F$ is separable over F.

For the notion of separability, the characteristic of the fields involved play a significant role. We review some basic properties of field arithmetic in characteristic p.

Lemma 2.16 For any prime p, and any $1 \leq k \leq p-1$, $p \mid \binom{p}{k}$.

Lemma 2.17 Let F be a field of characteristic p.

1. For any $a_1, ..., a_k \in F$ and any $m \in \mathbb{Z}_{\geq 0}$,
$$(a_1 + ... + a_k)^{p^m} = a_1^{p^m} + \cdots + a_k^{p^m}. \tag{36}$$
2. For any polynomial $\sum_i a_i x^i \in F[x]$,
$$\left(\sum_i a_i x^i\right)^{p^m} = \sum_i a_i^{p^m} x^{ip^m}. \tag{37}$$

Proof.

1. For $m = 0$ the statement is obvious. First consider the case $k = 1$ and $m = 1$.
$$(a_1 + a_2)^p = \sum_{i=0}^{p} \binom{p}{i} a_1^i a_2^{p-i} = a_1^p + a_2^p. \tag{38}$$
The last equality holds since $\binom{p}{i} = 0$ in F for $1 \leq i \leq p-1$. Induction on m proves the statement for $k = 2$ and any $m \geq 1$. One more induction on k this time, proves the first statement.
2. The proof of the second statement is virtually identical.

A convenient tool for checking the multiplicity of roots of polynomials is the derivative. For any field F, we define the derivative of the polynomial $f = \sum_{i=0}^{n} a_i x^i \in F[x]$ to be $f' = \sum_{i=1}^{n} i a_i x^{i-1} \in F[x]$.

Lemma 2.18 Let $f, g \in F[x]$ and $a, b \in F$. Then
1. $(af + bg)' = af' + bg'$
2. $(f \cdot g)' = f'g + fg'$.

Proof. Immediate from the definition. Left as an exercise.

Lemma 2.19
1. An element α is a root of $f \in F[x]$ of multiplicity $m \geq 2$ if and only if $f'(\alpha) = 0$.
2. A polynomial $f \in F[x]$ has no repeated roots if and only if $(f, f') = 1$.
3. An irreducible polynomial $P \in F[x]$ is separable if and only if $P' \neq 0$.

Proof. For the first statement, let α be a root of f of multiplicity m. Then $f = (x - \alpha)^m \cdot g$, with $g(\alpha) \neq 0$. Furthermore, $f' = m(x - \alpha)^{m-1} g + (x - \alpha)^m g'$. It is clear now, that if $m = 1$, then $f'(\alpha) \neq 0$ and if $m \geq 2$, then $f'(\alpha) = 0$.

For the second statement, assume first that $(f, f') = 1$. Suppose α is a root of f of multiplicity $m \geq 2$. Then α is a root of f'. If $P = \min(F, \alpha)$, then P is a common factor of f and f', therefore $P \mid (f, f')$, a contradiction. Conversely, if $(f, f') \neq 1$ and P is an irreducible factor of (f, f'), then any root α of P is a common root of f and f', and therefore a repeated root of f.

For the last statement, P is inseparable if and only if $(P, P') \neq 1$. Since P is irreducible, $(P, P') \neq 1 \Leftrightarrow (P, P') = P$, which is possible if and only if $P' = 0$ (what is $\deg(P')$ if $P' \neq 0$?)

Theorem 2.20 Let F be a field and $P \in F[x]$ be an irreducible polynomial.
1. If $\mathrm{char}(F) = 0$, then P is separable over F.
2. If $\mathrm{char}(F) = p$, then P is not separable over F if and only if $P \in F[x^p]$, that is, if $P(x) = g(x^p)$ for some $g \in F[x]$.
3. If $\mathrm{char}(F) = p$, then there exist some $m \in \mathbb{Z}_{\geq 0}$, such that $P(x) = g(x^{p^m})$ for some separable irreducible polynomial $g \in F[x]$.

Proof. We use Lemma 2.19. Let $P = a_n x^n + \cdots + a_0$, with $a_n \neq 0$, and $P' = n a_n x^{n-1} + \cdots + a_1$.
1. If $\mathrm{char}(F) = 0$, $P' \neq 0$, since $n a_n \neq 0$ in characteristic 0.
2. If $\mathrm{char}(F) = p$, $P' = 0$ if and only if $i a_i = 0$ for $1 \leq i \leq n$. This is possible if and only if either $a_i = 0$ or $p \mid i$, which is equivalent to $i = pj$ for every i such that $a_i \neq 0$. So $P' = 0$ if and only if
$$P = \sum_j a_{pj} x^{pj} = \sum_j a_{pj} (x^p)^j \in F[x^p]. \tag{39}$$
3. Let P be non-separable and consider the set $A = \left\{ j \in \mathbb{N} : P \in F\left[x^{p^j}\right] \right\}$. Then A is non-empty, since $1 \in A$. Also, A is upper bounded (a very rough upper bound is the degree of P). If $m =$

max A, then $P = g(x^{p^m})$ for some $g \in F[x]$. Any non-trivial factorization of g would imply a non-trivial factorization of P, so g is irreducible. If g were inseparable, then $g(x) = h(x^p)$ for some $h \in F[x]$ and $P = h\left(x^{p^{m+1}}\right)$, contradicting the choice of m.

Theorem 2.21 Let p be a prime. Every irreducible polynomial in $\mathbb{F}_p[x]$ is separable.

Proof. Let $P \in \mathbb{F}_p[x]$ be irreducible and assume it is inseparable. Then $P = \sum_i a_i x^{pi}$ for $a_i \in \mathbb{F}_p$. First note that $a^p = a$ for every $a \in \mathbb{F}_p$. Indeed, $a^{p-1} = 1$ for every $a \in \mathbb{F}_p^*$, by Lagrange's Theorem. Therefore $a^p = a$ for every $a \in \mathbb{F}_p^*$ and the last equality holds for $a = 0$ too. It follows that

$$P = \sum_i a_i x^{pi} = \sum_i a_i^p (x^i)^p = \left(\sum_i a_i x^i\right)^p, \tag{40}$$

which contradicts the assumption that P is irreducbile.

In light of Theorem 2.21, in order to produce an example of a field F and an irreducible polynomial $P \in F[x]$ that is inseparable over F, we need to consider fields F different from $\mathbb{F}_p$, and as we will later, different from any finite extension of $\mathbb{F}_p$.

Example 2.22 Let p be a prime, y be transcedental over $\mathbb{F}_p$, $F = \mathbb{F}_p(y)$. Clearly, F is the field of fractions of the domain $R = \mathbb{F}_p[y]$ and y is prime element of R. By Eisenstein's Irreducibility Criterion, the polynomial $P = x^p - y \in R[x]$ is irreducible in $R[x]$ and therefore irreducible in $F[x]$, since it is monic (by Gauss' Lemma). Let K be a splitting field of P over F, and $t \in K$ be a root of P. Then $t^p = y$ and

$$P = x^p - y = x^p - t^p = (x - t)^p. \tag{41}$$

So, P has a single root of multiplicity p and therefore it is inseparable.

Definition 2.23 An extension K/F is **separable** if every element of K is separable over F.

2.3 The Galois Group

For any abelian group G and field K, a homomorphism $\sigma : G \to K^*$ is called a *character* of G. Given characters $\sigma_1, ..., \sigma_n$, we may define the K-linear combination

$$\rho = c_1\sigma_1 + \cdots + c_n\sigma_n : G \to K, \quad \rho(g) = c_1\sigma_1(g) + \cdots + c_n\sigma_n(g). \tag{42}$$

An important result of Dedekind, states that distinct characters of *finite* abelian groups are linearly independent.

Lemma 2.24 (Dedekind) Let G be a finite abelian group, K a field and $\sigma_1, ..., \sigma_n$ be distinct characters from G to K^*. Then $c_1\sigma_1 + \cdots + c_n\sigma_n$ is the zero map if and only if $c_1 = \cdots = c_n = 0$.

Proof. Suppose that the set $\{\sigma_1, ..., \sigma_n\}$ is linearly dependent. Then there exists a linearly dependent subset of $\{\sigma_1, ..., \sigma_n\}$ of minimum cardinality m. Assume without loss of generality, that $\{\sigma_1, ..., \sigma_m\}$ is such a linearly dependent subset. Then there exist $c_1, ..., c_m \in K$, all non-zero, such that

$$c_1\sigma_1(g) + c_2\sigma_2(g) + ... + c_m\sigma_m(g) = 0 \quad \text{for every} \quad g \in G. \tag{43}$$

Since $\sigma_1 \neq \sigma_2$, there exists some $h \in G$, such that $\sigma_1(g) \neq \sigma_2(h)$. Subsituting hg for g in Equation 43, we have

$$c_1\sigma_1(h)\sigma_1(g) + c_2\sigma_2(h)\sigma_2(g) + ... + c_m\sigma_m(h)\sigma_m(g) = 0 \quad \text{for every} \quad g \in G. \tag{44}$$

Multiplying both sides of Equation 43 by $\sigma_1(h)$ and subtracting from Equation 44, we obtain

$$c_2(\sigma_2(h) - \sigma_1(h))\sigma_2(g) + ... + c_m(\sigma_m(h) - \sigma_1(h))\sigma_m(g) = 0 \quad \text{for every} \quad g \in G. \tag{45}$$

Since $c_2(\sigma_2(h) - \sigma_1(h)) \neq 0$, this is a linear dependence relation for $\{\sigma_2, ..., \sigma_m\}$, which contradicts the minimality of m.

Proposition 2.25 Let K/F be a finite extension. Then $|\operatorname{Gal}(K/F)| \leq [K : F]$.

Proof. Let $[K : F] = n$, let $\{\gamma_1, ..., \gamma_n\}$ be an F-basis of K, and assume $\operatorname{Gal}(K/F)$ contains $n + 1$ distinct automorphisms $\sigma_1, ..., \sigma_{n+1}$. Consider the matrix $A = \big(\sigma_i(\gamma_j)\big) \in K^{(n+1)\times n}$. Let rows of A must be linearly dependent over K, so there exist $c_1, ..., c_{n+1} \in K$, not all equal to zero, such that

$$\sum_{i=1}^{n+1} c_i(\sigma_i(\gamma_1), ..., \sigma_i(\gamma_n)) = 0. \tag{46}$$

This implies that

$$\sum_{i=0}^{n+1} c_i\sigma_i\big(\gamma_j\big) = 0 \quad \text{for every} \quad 1 \leq j \leq n. \tag{47}$$

We claim that $\sum_{i=0}^{n+1} c_i\sigma_i$ is the zero map, which would contradict Dedekind's Lemma. Indeed, any $\alpha \in K$ can be written as $\alpha = \sum_{j=1}^{n} \lambda_j\gamma_j$, for some $\lambda_1, ..., \lambda_n \in F$. Then

$$\sum_{i=1}^{n+1} c_i\sigma_i(\alpha) = \sum_{i=1}^{n+1} c_i\sigma_i\left(\sum_{j=1}^{n} \lambda_j\gamma_j\right) = \sum_{i=1}^{n+1}\sum_{j=1}^{n} c_i\lambda_j\sigma_i\big(\gamma_j\big) = \sum_{j=1}^{n} \lambda_j \sum_{i=1}^{n+1} c_i\sigma_i\big(\gamma_j\big) = 0. \tag{48}$$

Proposition 2.25 gives a bound for $|\operatorname{Gal}(K/F)|$ that turns out to be sharp. We have already seen extensions, in Theorem 4.5, that attain the bound with equality. Given a field K, the following proposition may be viewed as a construction of a subfield F such that $|\operatorname{Gal}(K/F)|$ attains the upper bound. An important notion that is introduced, is that of the fixed field of a set of automorphisms of K.

Definition 2.26 Let K be a field and $S \subseteq \operatorname{Aut}(K)$ be set of automorphisms of K. The set

$$\mathcal{F}(S) = \{a \in K : \sigma(a) = a \quad \text{for every} \quad \sigma \in S\} \tag{49}$$

is a subfield of K, called the **fixed field** of S.

Abusing notation we write $\mathcal{F}(\sigma)$ instead of $\mathcal{F}(\{\sigma\})$ and note that $\mathcal{F}(\langle\sigma\rangle) = \mathcal{F}(\sigma)$.

Proposition 2.27 Let G be a finite subgroup of $\mathrm{Aut}(K)$ and $F = \mathcal{F}(G)$. Then $|G| = [K : F]$ and $\mathrm{Gal}(K/F) = G$.

Proof. Let $|G| = n$, $G = \{\sigma_1, ..., \sigma_n\}$. Assume that $[K : F] > n$ and that $\{\gamma_1, ..., \gamma_{n+1}\}$ is a subset of K that is linearly independent over F. The matrix $A = \big(\sigma_i(\gamma_j)\big) \in K^{n\times(n+1)}$ has rank at most n, so the columns are linealy dependent over K. If m is the smallest number of linearly dependent columns of A, we may assume that the first m columns are linealy dependent (rearranging the columns if necessary). So we have a linear dependence relation

$$\sum_{j=1}^{m} c_j \cdot \begin{pmatrix} \sigma_1(\gamma_j) \\ \vdots \\ \sigma_n(\gamma_j) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \tag{50}$$

with $c_i \in K$ and all $c_j \neq 0$ (because of the minimality of m) and we may assume that $c_1 = 1$ (dividing by c_1 if necessary). Our aim is to show that $c_i \in F$, which would mean that the set $\{\gamma_1, ..., \gamma_{n+1}\}$ is linearly dependent over F, which contradicts our assuption.

Equation 50 implies that

$$\sum_{j=1}^{m} c_j \sigma_i(\gamma_j) = 0 \quad \text{for} \quad 1 \leq i \leq n. \tag{51}$$

For any $\sigma \in G$, we have

$$0 = \sigma\left(\sum_{j=1}^{m} c_j \sigma_i(\gamma_j)\right) = \sum_{j=1}^{m} \sigma(c_j)\sigma\sigma_i(\gamma_j). \tag{52}$$

As σ_i varies over G, so does $\sigma\sigma_i$ and we obtain

$$\sum_{j=1}^{m} \sigma(c_j)\sigma_i(\gamma_j) = 0 \quad \text{for} \quad 1 \leq i \leq n. \tag{53}$$

Subtracting Equation 51 from Equation 53, we obtain

$$\sum_{j=2}^{m} (\sigma(c_j) - c_j)\sigma_i(\gamma_j) = 0 \quad \text{for} \quad 1 \leq i \leq n. \tag{54}$$

This violates the minimality of m unless $\sigma(c_j) = c_j$ for every j. This holds for every $\sigma \in G$, which implies that $c_j \in \mathcal{F}(G) = F$. Then Equation 51 gives a linear dependence of $\{\gamma_1, ..., \gamma_m\}$ over F, which is a contradiction. It follows that $[K : F] \leq |G|$. Observe now, that $G \leq \mathrm{Gal}(K/F)$, so

$$[K : F] \leq |G| \leq |\,\mathrm{Gal}(K/F)| \leq [K : F], \tag{55}$$

and the statements of the proposition follow.

Example 2.28 Let $K = \mathbb{Q}\left(\sqrt{2}, i\right)$. Every automorphism of K fixes $\mathbb{Q}$, therefore $\mathrm{Aut}(K) = \mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$, where id is the identity map and

$$\begin{aligned} \sigma_1\left(\sqrt{2}\right) &= \sqrt{2}, \sigma_1(i) = -i \\ \sigma_2\left(\sqrt{2}\right) &= -\sqrt{2}, \sigma_2(i) = i \\ \sigma_3\left(\sqrt{2}\right) &= -\sqrt{2}, \sigma_3(i) = -i. \end{aligned} \tag{56}$$

Let $G = \langle\sigma_1\rangle$ be the cyclic group generated by σ_1. We will determine $\mathcal{F}(\langle\sigma_1\rangle) = \mathcal{F}(\sigma_1)$. The set $\left\{1, \sqrt{2}, i, i\sqrt{2}\right\}$ is a basis of K over $\mathbb{Q}$. Every element of $\mathcal{F}(\sigma_1)$ if of the form $a + b\sqrt{2} + ci + di\sqrt{2}$, with $a, b, c, d \in \mathbb{Q}$, with

$$\begin{aligned} \sigma_1\left(a + b\sqrt{2} + ci + di\sqrt{2}\right) &= a + b\sqrt{2} + ci + di\sqrt{2} \Leftrightarrow \\ a + b\sigma_1\left(\sqrt{2}\right) + c\sigma_1(i) + d\sigma_1(i)\sigma_1\left(\sqrt{2}\right) &= a + b\sqrt{2} + ci + di\sqrt{2} \Leftrightarrow \\ a + b\sqrt{2} - ci - di\sqrt{2} &= a + b\sqrt{2} + ci + di\sqrt{2} \Leftrightarrow \\ ci + di\sqrt{2} &= 0 \Leftrightarrow c = d = 0. \end{aligned} \tag{57}$$

Thus,

$$\mathcal{F}(\langle\sigma_1\rangle) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\} = \mathbb{Q}\left(\sqrt{2}\right). \tag{58}$$

By Proposition 2.27, $\mathrm{Gal}\left(K/\mathbb{Q}\left(\sqrt{2}\right)\right) = \langle\sigma_1\rangle$ and we can verify that $\left[K : \mathbb{Q}\left(\sqrt{2}\right)\right] = |\langle\sigma_1\rangle| = 2$.

Example 2.29 Let $\omega \in \mathbb{C}$ be a primitive 8th root of unity. Then $f(x) = x^4 + 1$ is the minimal polynomial of ω over $\mathbb{Q}$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$. The roots of $f(x)$ are ω^j for $j \in \{1, 3, 5, 7\}$ and $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \left\{\sigma_j : j = 1, 3, 5, 7\right\}$, where $\sigma_{j(\omega)} = \omega^j$. We will determine $\mathcal{F}(\sigma_3)$. A basis of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ is $\left\{1, \omega, \omega^2, \omega^3\right\}$ and the elements of $\mathcal{F}(\sigma_3)$ are of the form $a + b\omega + c\omega^2 + d\omega^3$, with $a, b, c, d \in \mathbb{Q}$ and $\sigma_3(a + b\omega + c\omega^2 + d\omega^3) = a + b\omega + c\omega^2 + d\omega^3$. We compute

$$\begin{aligned} \sigma_3(a + b\omega + c\omega^2 + d\omega^3) &= a + b\omega + c\omega^2 + d\omega^3 \Leftrightarrow \\ a + b\sigma_3(\omega) + c\sigma_3(\omega)^2 + d\sigma_3(\omega)^3 &= a + b\omega + c\omega^2 + d\omega^3 \Leftrightarrow \\ a + b\omega^3 + c\omega^6 + d\omega^9 &= a + b\omega + c\omega^2 + d\omega^3 \Leftrightarrow \\ a + b\omega^3 - c\omega^2 + d\omega &= a + b\omega + c\omega^2 + d\omega^3 \Leftrightarrow \\ c = 0 \quad \text{and} \quad b &= d, \end{aligned} \tag{59}$$

where we used the equation $\omega^4 = -1$ (ω is a root of its minimal polynomial), to substitute $\omega^6 = -\omega^2$ and $\omega^9 = \omega$. Therefore, $\mathcal{F}(\sigma_3) = \left\{a + b\left(\omega + \omega^3\right) : a, b \in \mathbb{Q}\right\}$. By Proposition 2.27, $[\mathbb{Q}(\omega) : \mathcal{F}(\sigma_3)] = |\langle\sigma_3\rangle| = 2$, and we have $[\mathcal{F}(\sigma_3) : \mathbb{Q}] = \frac{[\mathbb{Q}(\omega):\mathbb{Q}]}{[\mathbb{Q}(\omega):\mathcal{F}(\sigma_3)]} = 2$. So $\mathcal{F}(\sigma_3) = \mathbb{Q}(\omega + \omega^3)$ and $\deg(\min(\mathbb{Q}, \omega + \omega^3)) = 2$. Indeed, we can verify that $\min(\mathbb{Q}, \omega + \omega^3) = x^2 + 2$ and $\omega + \omega^3 = i\sqrt{2}$ (or $-i\sqrt{2}$ depending which primitive 8th root of unity ω is).

Theorem 2.30 Let K/F be a finite extension. The following are equivalent.

1. $F = \mathcal{F}(\mathrm{Gal}(K/F))$
2. $|\mathrm{Gal}(K/F)| = [K : F]$

Proof.

- (1) $\Rightarrow$ (2) Assume that $F = \mathcal{F}(\mathrm{Gal}(K/F))$, and apply Proposition 2.27 with $G = \mathrm{Gal}(K/F)$. We obtain

$$|\mathrm{Gal}(K/F)| = [K : \mathcal{F}(\mathrm{Gal}(K/F))] = [K : F]. \tag{60}$$

- (2) $\Rightarrow$ (1) Assume that $|\mathrm{Gal}(K/F)| = [K : F]$. For $a \in F$, $\sigma(a) = a$ for every $\sigma \in \mathrm{Gal}(K/F)$, so $a \in \mathcal{F}(\mathrm{Gal}(K/F))$. Therefore $F \leq \mathcal{F}(\mathrm{Gal}(K/F))$. Apply Proposition 2.27 with $G = \mathrm{Gal}(K/F)$ to get

$$|\mathrm{Gal}(K/F)| = [K : \mathcal{F}(\mathrm{Gal}(K/F))] \leq [K : F] = |\mathrm{Gal}(K/F)|. \tag{61}$$

  This is implies that $[K : \mathcal{F}(\mathrm{Gal}(K/F))] = [K : F]$, which in turn implies $F = \mathcal{F}(\mathrm{Gal}(K/F))$.

We can repeat the argument of Theorem 4.5 for any simple extension $F(\alpha)/F$. Let $P = \min(F, \alpha)$ be of degree n and let $\{\alpha_1, ..., \alpha_m\}$ be the distinct roots of P in $F(\alpha)$. Then there exist F-automorphisms $\tau_j : F(\alpha) \to F(\alpha)$, with $\tau_j(\alpha) = \alpha_j$ (which are clearly distinct) and any F-automorphism $\rho : F(\alpha) \to F(\alpha)$ must map α to one of the α_j, so ρ must be one of the τ_j. Therefore $\mathrm{Gal}(F(\alpha)/F) = \{\tau_j : j = 1, ..., m\}$. We can see now that $|\mathrm{Gal}(F(\alpha)/F)| = [F(\alpha) : F]$ if and only if P has n distinct roots in $F(\alpha)$, that is, if and only if $F(\alpha)/F$ is normal and α is separable over F. We will show that this is true for any finite extension K that is generated over F by a set of elements that are separable over F.

Lemma 2.31 Let K/F be a finite, $\beta \in K$ and let m be the number of distinct roots of $\min(F, \beta)$ in K. Then $|\mathrm{Gal}(K/F)| = m \cdot |\mathrm{Gal}(K/F(\beta))|$.

Proof. Denote $G = \mathrm{Gal}(K/F)$ and $H = \mathrm{Gal}(K/F(\beta))$ and note that $H \leq G$. Let $\{\beta_1, ..., \beta_m\}$ be the set of dstinct roots of $\min(F, \beta)$ in K. By Theorem 2.3, there are automorphisms $\tau_j \in G$, with $\tau_j(\beta) = \beta_j$ for $1 \leq j \leq m$. The cosets $\tau_j H$ are distinct. Indeed,

$$\tau_i H = \tau_j H \Rightarrow \tau_j^{-1}\tau_i \in H \Rightarrow \tau_i(\beta) = \tau_j(\beta) \Rightarrow \beta_i = \beta_j \Rightarrow i = j. \tag{62}$$

Therefore $(G : H) = \frac{|G|}{|H|} \geq m$.

On the other hand, for any $\rho \in G$, $\rho(\beta) = \beta_j$ for some j, so $\rho^{-1}\tau_j$ fixes $F(\beta)$ and therefore $\rho^{-1}\tau_j \in H$, which implies that $\rho H = \tau_j H$. It follows that $\frac{G}{H} = \{\tau_j H : 1 \leq j \leq m\}$ and $(G : H) = m$.

Theorem 2.32 Let K/F be a finite extension. The following statements are equivalent.

1. K/F is normal and separable,
2. K is the splitting field of a set of separable polynomials over F,
3. $|\mathrm{Gal}(K/F)| = [K : F]$,
4. $F = \mathcal{F}(\mathrm{Gal}(K/F))$.

Proof. We already know that statements (3) and (4) are equivalent. We prove the equivalence of the first three statements.

- (1) $\Rightarrow$ (2) K/F is normal by assumption. Since K/F is finite and algebraic, it is of the form $K = F(\alpha_1, ..., \alpha_r)$ for some $\alpha_1, ..., \alpha_r \in K$, which are separable over F. If $S = \{\min(F, \alpha_i) : 1 \leq i \leq r\}$, then K is the splitting field of S over F.
- (2) $\Rightarrow$ (3) By induction on $n = [K : F]$. If $n = 1$ then $K = F$ and $|\mathrm{Gal}(K/F)| = [K : F] = 1$. Assume that the statement of true for any extension of degree $< n$ (that is the splitting field of a set of separable polynomials). For the inductive step, let $K = F(\alpha_1, ..., \alpha_r)$ be normal over F and $\alpha_1, ..., \alpha_r$ be separable over F, and $[K : F] = n$. Let α be one of the α_i and $\alpha \notin F$. Denote $G = \mathrm{Gal}(K/F)$ and $H = \mathrm{Gal}(K/F(\alpha))$. The extension $K/F(\alpha)$ is normal, it is generated over $F(\alpha)$ by the same elements $\{\alpha_1, ..., \alpha_r\}$ and $[K : F(\alpha)] < [K : F] = n$. So by the induction hypothesis, $|H| = [K : F(\alpha)]$. Also $\deg(\min(F, \alpha)) = [F(\alpha) : F]$ and $\min(F, \alpha)$ is separable over F, so it has $[F(\alpha) : F]$ distinct roots in K. By Lemma 2.31,
$$|G| = [F(\alpha) : F] \cdot |H| = [F(\alpha) : F] \cdot [K : F(\alpha)] = [K : F]. \tag{63}$$
- (3) $\Rightarrow$ (1) Assume that $|\mathrm{Gal}(K/F)| = [K : F]$ and let $\beta \in K$. Let $\{\beta_1, ..., \beta_m\}$ be the set of distinct roots of $\min(F, \beta)$ in K. By Lemma 2.31, $|\mathrm{Gal}(K/F)| = m \cdot |\mathrm{Gal}(K/F(\beta))|$. Then
$$[K : F] = |\mathrm{Gal}(K/F)| = m \cdot |\mathrm{Gal}(K/F(\beta))| \leq [F(\beta) : F] \cdot [K : F(\beta)] = [K : F]. \tag{64}$$
Since $m \leq [F(\beta) : F]$ and $|\mathrm{Gal}(K/F(\beta))| \leq [K : F(\beta)]$, Equation 64 implies $m = [F(\beta) : F]$ (and $|\mathrm{Gal}(K/F(\beta))| = [K : F(\beta)]$). This means that $\min(F, \beta)$ splits in K and its roots are simple. This holds for every $\beta \in K$, so K/F is normal and separable over F.

Corollary 2.33 $K = F(\alpha_1, ..., \alpha_r)$ is separable over F if and only if $\alpha_1, ..., \alpha_r$ are separable over F.

Proof. If K/F is separable, then each α_j is separable over F. For the converse, let N be the splitting field of $\{\min(F, \alpha_j), 1 \leq j \leq r\}$ over F. Then N is the splitting field of a set of separable polynomials over F, so by Theorem 2.32, N/F is normal and separable. It follows that K/F is also separable.

Theorem 2.32 motivates the following definition.

Definition 2.34 A field extension K/F is **Galois** if it satisfies one of the equivalent conditions of Theorem 2.32

Remark 2.35
1. If $\mathrm{char}(F) = 0$, any algebraic extension K/F is separable. Therefore K/F is Galois, if and only if it is normal.
2. If K/F is Galois and L is an intermediate field of K/F, then K/L is also Galois. Indeed, K/F is normal and separable, so K/L is normal and separable.

Example 2.36 Let p be a prime, ω be a primitive p-th root of unity. Then $\min(\mathbb{Q},\omega) = x^{p-1} + \cdots + x + 1$, so $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$. Since $\operatorname{char}(\mathbb{Q}) = 0$, the extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is separable. The complete set of roots of $x^{p-1} + \cdots + x + 1$ is $\{\omega^j : j = 1, ..., p-1\}$ so, $\min(\mathbb{Q},\omega)$ splits in $\mathbb{Q}(\omega)$, so the extension is also normal and therefore it is Galois. For every $j \in \mathbb{Z}$, $p \nmid j$, ω^j is a root of $\min(\mathbb{Q},\omega)$ and the map

$$\sigma_j : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega), \quad \sigma_j(\omega) = \omega^j \tag{65}$$

is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\omega)$. The Galois group is

$$\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \left\{\sigma_j : 1 \le j \le p-1\right\}. \tag{66}$$

Note that if $i \equiv j \pmod p$, then $\sigma_i(\omega) = \omega^i = \omega^j = \sigma_j(\omega)$, so $\sigma_i = \sigma_j$ and we may index the automorphisms by the classes of $\mathbb{Z}_p^*$, that is

$$\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \left\{\sigma_{[j]} : 1 \le j \le p-1\right\}. \tag{67}$$

We claim that $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_p^*$. Indeed, the map

$$\varphi : \mathbb{Z}_p^* \to \operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}), \quad \varphi([j]) = \sigma_{[j]} \tag{68}$$

is well defined, and it is a surjective group homorphism, since

$$\sigma_{[i]}\sigma_{[j]}(\omega) = \sigma_{[i]}(\omega^j) = \sigma_{[i]}(\omega)^j = \omega^{ij} = \sigma_{[ij]}(\omega). \tag{69}$$

Furthermore,

$$[i] \in \ker(\varphi) \Leftrightarrow \sigma_{[i]} = \mathrm{id} \Leftrightarrow \omega^i = \omega \Leftrightarrow i \equiv 1 \pmod p \tag{70}$$

so $\ker\varphi = \langle[1]\rangle$, the map is injective and $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_p^*$. In particular $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is cyclic.

2.4 Galois Correspondence

Let K be a field. We define the maps

$$\begin{aligned} \mathcal{F}(\cdot) : \{\text{subsets of } \operatorname{Aut}(K)\} &\longrightarrow \{\text{subfields of } K\} \\ S &\mapsto \mathcal{F}(S) = \{a \in K : \sigma(a) = a \text{ for every } a \in L\} \end{aligned} \tag{71}$$

and

$$\begin{aligned} \mathcal{G}(\cdot) : \{\text{subfields of } K\} &\longrightarrow \{\text{subgroups of } \operatorname{Aut}(K)\} \\ L &\mapsto \mathcal{G}(L) = \operatorname{Gal}(K/L) = \{\sigma \in \operatorname{Aut}(K) : \sigma(a) = a \text{ for every } a \in L\} \end{aligned} \tag{72}$$

If K is an extension of F, a field L such that $F \le L \le K$, is an intermediate extension of K/F. The following lemma shows that the two maps are well defined.

Lemma 2.37 Let K be a field.
1. If $S \subseteq \operatorname{Aut}(K)$, then $\mathcal{F}(S)$ is a subfield of K.
2. If $F \le K$ and $S \subseteq \operatorname{Gal}(K/F)$, then $\mathcal{F}(S)$ is an itermediate extension of K/F.
3. If $L \le K$, then $\mathcal{G}(L)$ is a subgroup of $\operatorname{Aut}(K)$.
4. If $F \le L \le K$, then $\mathcal{G}(L)$ is a subgroup of $\operatorname{Gal}(K/F)$.

Proof.

1. By definition, $\mathcal{F}(S)$ is a subset of K. Let $a, b \in \mathcal{F}(S)$ and $\sigma \in S$. Then $\sigma(a+b) = \sigma(a) + \sigma(b) = a + b$, $\sigma(ab) = \sigma(a)\sigma(b) = ab$ and for $a \neq 0$, $\sigma(a^{-1}) = \sigma(a)^{-1} = a^{-1}$. So $a + b, ab, a^{-1} \in \mathcal{F}(S)$ and $\mathcal{F}(S)$ is a subfield of K.
2. If $S \subseteq \mathrm{Gal}(K/F)$, then every $a \in F$ is fixed by every $\sigma \in S$, and therefore $a \in \mathcal{F}(S)$. It follows that $F \leq L$.
3. Let $\sigma, \tau \in \mathcal{G}(L) = \mathrm{Gal}(K/L)$. Then $\sigma \circ \tau, \sigma^{-1} \in \mathrm{Gal}(K/F)$, so $\mathcal{G}(L)$ is a subgroup of $\mathrm{Aut}(K)$.
4. If $F \leq L \leq K$, then every $\sigma \in \mathcal{G}(L)$ is an automorphism of K that fixes L, so it fixes F and therefore $\sigma \in \mathrm{Gal}(K/F)$.

The following lemma lists some basic properties of the two maps.

Lemma 2.38 Let K be a field.

1. If $L_1 \leq L_2$ are subfields of K, then $\mathcal{G}(L_2) \leq \mathcal{G}(L_1)$.
2. If $L \leq K$, then $L \leq \mathcal{F}(\mathcal{G}(L))$.
3. If $S_1 \subseteq S_2$ are subsets of $\mathrm{Aut}(K)$, then $\mathcal{F}(S_2) \leq \mathcal{F}(S_1)$.
4. If $S \subseteq \mathrm{Aut}(K)$, then $S \subseteq \mathcal{G}(\mathcal{F}(S))$.
5. If $L = \mathcal{F}(S)$ for some $S \subseteq \mathrm{Aut}(K)$, then $L = \mathcal{F}(\mathcal{G}(L))$.
6. If $H = \mathcal{G}(L)$ for some $L \leq K$, then $H = \mathcal{G}(\mathcal{F}(H))$.

Proof.

1. For $\sigma \in \mathcal{G}(L_2)$, $\sigma(a) = a$ for every $a \in L_2$, therefore $\sigma(a) = a$ for every $a \in L_1$ and $\sigma \in \mathcal{G}(L_1)$.
2. Let $a \in L$. For every $\sigma \in \mathcal{G}(L)$, $\sigma(a) = a$, so $a \in \mathcal{F}(\mathcal{G}(L))$.
3. For $a \in \mathcal{F}(S_2)$, $\sigma(a) = a$ for every $\sigma \in S_2$, therefore $\sigma(a) = a$ for every $\sigma \in S_1$ and $a \in \mathcal{F}(S_1)$.
4. Let $\sigma \in S$. For every $a \in \mathcal{F}(S)$, $\sigma(a) = a$, so $\sigma \in \mathrm{Gal}(K/\mathcal{F}(S)) = \mathcal{G}(\mathcal{F}(S))$.
5. Let $S \subseteq \mathrm{Aut}(K)$ and $L = \mathcal{F}(S)$. Then by (4), $S \subseteq \mathcal{G}(\mathcal{F}(S)) = \mathcal{G}(L)$. Then (3) implies, $\mathcal{F}(\mathcal{G}(L)) \leq \mathcal{F}(S) = L$. By (2), $L \leq \mathcal{F}(\mathcal{G}(L))$ and equality follows.
6. Let $L \leq K$ and $H = \mathcal{G}(L)$. Then by (2), $L \leq \mathcal{F}(\mathcal{G}(L)) = \mathcal{F}(H)$ and by (1) we have $\mathcal{G}(\mathcal{F}(H)) \leq \mathcal{G}(L) = H$. Furthermore, by (4) we have $H \leq \mathcal{G}(\mathcal{F}(H))$ and equality follows.

The maps $\mathcal{F}$ and $\mathcal{G}$, as defined are not bijective. However, Lemma 2.38 shows that if we restrict the domain of $\mathcal{F}$ to the intermediate fields of the form $L = \mathcal{F}(H)$ for some subgroup H of $\mathrm{Gal}(K/F)$ and the codomain to the subgroups of H of $\mathrm{Gal}(K/F)$ of the form $\mathrm{Gal}(K/L)$ for some intermediate extension L of K/F, then the two maps are bijective, and in fact, by statements (5) and (6), one is the inverse of the other. Furthermore, the two maps are *inclusion reversing*, by statements (1) and (3). We record our observations in the following theorem.

Theorem 2.39 Let K/F be a field extension. Then the maps $\mathcal{F}$ and $\mathcal{G}$ define an *inclusion reversing* correspondence between the set of subgroups of $\mathrm{Gal}(K/F)$ of the form $\mathrm{Gal}(K/L)$ for some subfield of K containing F and the set of subfields of K that contain F and are of the form $\mathcal{G}(H)$ for some subgroup H of $\mathrm{Gal}(K/F)$. The maps $\mathcal{F}$ and $\mathcal{G}$ defined on these sets are inverses of each other.

A natural question to investigate, is under which conditions, the two maps define bijections between the set of *all* intermediate extensions of K/F and *all* subgroups of $\mathrm{Gal}(K/F)$. Equivalently, under which

conditions, every intermediate extension of K/F is of the form $L = \mathcal{F}(H)$ for some $H \leq \mathrm{Gal}(K/F)$ and every subgroup of $\mathrm{Gal}(K/F)$ is of the form $H = \mathcal{G}(L)$ for some intermediate field L. As it turns out, this happens if and only if the extension K/F is Galois.

Theorem 2.40 (Fundamental Theorem of Galois Theory) Let K be a finite Galois extension of F and let $G = \mathrm{Gal}(K/F)$. Then the maps $L \mapsto \mathcal{G}(L)$ and $H \mapsto \mathcal{F}(H)$ define an 1-1 inclusion reversing correspondence between intermediate fields of K/F and subgroups of G. If $L = \mathcal{F}(H)$ (and therefore $H = \mathcal{G}(L)$), we have $[K : L] = |H|$ and $[L : F] = (G : H)$. Furthermore, H is normal in G if and only if L/F is Galois. In this case, $\mathrm{Gal}(L/F) \cong G/H$.

Proof. By Theorem 2.39 we know that the maps $\mathcal{F}$ and $\mathcal{G}$ define an inclusion reversing 1-1 correspondence between the set of subgroups of $\mathrm{Gal}(K/F)$ of the form $\mathrm{Gal}(K/L)$ for some subfield of K containing F and the set of subfields of K that contain F and are of the form $\mathcal{G}(H)$ for some subgroup H of $\mathrm{Gal}(K/F)$. Let L be an intermediate field of K/F. Since K/F is Galois, K/L is also Galois. So $L = \mathcal{F}(\mathrm{Gal}(K/L))$ and L is a fixed field of a subgroup of G. For any $H \leq G$, by Proposition 2.27 we have $H = \mathrm{Gal}(K/\mathcal{F}(H))$, so H is of the form $\mathrm{Gal}(K/L)$ for some intermediate extension L of K/F. It follows the maps $\mathcal{F}$ and $\mathcal{G}$ define the stated correspondence between *all* intermediate fields of K/F and *all* subgroups of G. Since K/F and K/L are Galois, we have $[K : F] = |G|$ and $[K : L] = |\mathrm{Gal}(K/L)| = |\mathcal{G}(L)| = |H|$. Also, $[L : F] = [K : F]/[K : L] = |G|/|H|$.

For the last statement, assume first that H is normal in G and let $L = \mathcal{F}(H)$, and therefore $H = \mathcal{G}(F) = \mathrm{Gal}(K/L)$. The extension L/F is separable (since every element of L is also an element of K and the extension K/F is separable). We will show that L/F is also normal. Let $a \in L$ and let b be a root of $\min(F, a)$. Since K/F is normal, we know that $b \in K$. By the Isomorphism Extension Theorem, there exists some $\sigma \in G$, such that $b = \sigma(a)$. For any $\tau \in H$, we have

$$\tau(b) = \tau\sigma(a) = \sigma\sigma^{-1}\tau\sigma(a) = \sigma(\sigma^{-1}\tau\sigma(a)). \tag{73}$$

Since H is normal in G, we have $\sigma^{-1}\tau\sigma \in H$, so it fixes L, that is, $\sigma^{-1}\tau\sigma(a) = a$ and $\tau(b) = \sigma(a) = b$. It follows that b is fixed be H, that is, $b \in \mathcal{F}(H) = L$. So $\min(F, a)$ splits in L. Conversely, assume that L/F is Galois and let $H = \mathrm{Gal}(K/L)$. Consider the restriction map

$$\theta : G \to \mathrm{Gal}(L/F), \quad \theta(\sigma) = \sigma|_L. \tag{74}$$

Every automorphism $\tau \in \mathrm{Gal}(L/F)$ can be extended to an automorphism $\sigma \in G$, by the Isomorphism Extension Theorem, so θ is surjective. Furhtermore

$$\sigma \in \ker(\theta) \Leftrightarrow \sigma|_L = \mathrm{id} \Leftrightarrow \sigma(a) = a \quad \text{for every} \quad a \in L \Leftrightarrow \sigma \in \mathrm{Gal}(K/L) = H. \tag{75}$$

It follows that $\ker(\theta) = H$ and H is normal in G (as the kernel of a group homomorphism). In this case, the first isomorphism theorem of groups yields $\mathrm{Gal}(L/F) \cong G/H$.

Example 2.41 Let p be a prime and $\omega \in \mathbb{C}$ be a primitive p-th root of unity. We have seen that the extension $\mathbb{Q}(\omega)/\mathbb{Q}$ has degree $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$ and has Galois group $G \cong \mathbb{Z}_p^*$ is cyclic. In particular $G = \langle \sigma_{[i]} \rangle$, where $\sigma_{[i]}(\omega) = \omega^i$ and $[i]$ is a generator of $\mathbb{Z}_p^*$. For every divisor $d \mid p - 1$ there exists a unique subgroup of G of order d, $H_d = \langle \sigma_{[i]}^{\frac{p-1}{d}} \rangle = \langle \sigma_{\left[i^{\frac{p-1}{d}}\right]} \rangle$, where $\left[i^{\frac{p-1}{d}}\right]$ is the unique element of $\mathbb{Z}_p^*$ of order d. The corresponding intermediate field is $L_d = \mathcal{F}(H_d)$. By Theorem 2.40,

those are exactly the intermediate fields of $\mathbb{Q}(\omega)/\mathbb{Q}$. Since G is abelian, every subgroup H_d is normal in G. It follows that $L_d/\mathbb{Q}$ is also Galois and

$$[L_d : \mathbb{Q}] = \frac{|G|}{|H_d|} = \frac{p-1}{d}. \tag{76}$$

Furthermore,

$$\mathrm{Gal}(L_d/\mathbb{Q}) \cong G/H_d \cong \langle [i] \rangle / \langle \left[i^{\frac{p-1}{d}} \right] \rangle \cong \langle [i^d] \rangle. \tag{77}$$

Example 2.42 Let $\omega \in \mathbb{C}$ be a primitive 5-th root of unity. The extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois of degree 4 and $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_5^* = \langle [2] \rangle$. The group $\mathbb{Z}_5^*$ has three subgroups: $\langle \mathrm{id} \rangle$, $\langle \sigma_{[4]} \rangle$, $\mathbb{Z}_5^*$ (corresponding to the divisors $1, 2, 4$ of the order of $\mathbb{Z}_5^*$). For the first and third subgroups, the corresponding intermediate fields are $\mathcal{F}(\langle \mathrm{id} \rangle) = \mathbb{Q}(\omega)$, $\mathcal{F}(\mathbb{Z}_5^*) = \mathcal{F}(\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})) = \mathbb{Q}$. Let $L = \mathcal{F}\left(\langle \sigma_{[4]} \rangle\right)$. Every $a \in L$ can be written as $a = \sum_{j=0}^{3} c_j \omega^j$, with $c_j \in \mathbb{Q}$.

$$\begin{aligned} \sigma_{[4]}(a) &= \sum_{j=0}^{3} c_j \sigma_{[4]}(\omega^j) = \sum_{j=0}^{3} c_j \omega^{4j} \\ &= c_0 + c_1\omega^4 + c_2\omega^3 + c_3\omega^2 \\ &= c_0 + c_1(-1 - \omega - \omega^2 - \omega^3) + c_2\omega^3 + c_3\omega^2 \\ &= (c_0 - c_1) - c_1\omega + (c_3 - c_1)\omega^2 + (c_2 - c_1)\omega^3. \end{aligned} \tag{78}$$

Therefore $a \in L$ if and only if

$$\begin{aligned} \sigma_{[4]}(a) = a &\Leftrightarrow (c_0 - c_1) - c_1\omega + (c_3 - c_1)\omega^2 + (c_2 - c_1)\omega^3 = c_0 + c_1\omega + c_2\omega^2 + c_3\omega^3 \\ &\Leftrightarrow c_0 - c_1 = c_0, \quad -c_1 = c_1, \quad c_3 - c_1 = c_2, \quad c_2 - c_1 = c_3 \\ &\Leftrightarrow c_1 = 0, \quad c_2 = c_3. \end{aligned} \tag{79}$$

So we have $L = \{c_0 + c_2(\omega^2 + \omega^3) : c_0, c_2 \in \mathbb{Q}\} = \mathbb{Q}(\omega^2 + \omega^3) = \mathbb{Q}(\omega + \omega^4)$. Since $[L : \mathbb{Q}] = \frac{|\langle [2] \rangle|}{|\langle [4] \rangle|} = 2$, we see that $\deg \min(\mathbb{Q}, \omega + \omega^4) = 2$. Indeed,

$$(\omega + \omega^4)^2 = \omega^2 + 2\omega^5 + \omega^8 = 2 + \omega^2 + \omega^3 = 1 - \omega - \omega^4, \tag{80}$$

and it is easy to check that

$$(\omega^2 + \omega^3)^2 = 1 - \omega^2 - \omega^3. \tag{81}$$

so $\min(\mathbb{Q}, \omega + \omega^4) = \min(\mathbb{Q}, \omega^2 + \omega^3) = x^2 + x - 1$. The roots of $x^2 + x - 1$ are $\frac{-1 \pm \sqrt{5}}{2}$, so $L = \mathbb{Q}\left(\frac{-1+\sqrt{5}}{2}\right) = \mathbb{Q}\left(\sqrt{5}\right)$.

Theorem 2.43 (Primitive Element Theorem) A finite extension K/F is simple if and only if there are finitely many intermediate extensions $F \leq L \leq K$.

Proof. If F is a finite field, then K is also a finite field, and therefore K^* is a cyclic group by Theorem 1.8. If $K^* = \langle \alpha \rangle$, then $K = F(\alpha)$, so the extension is simple. It is also easy to see that there are finitely many intermediate extensions (after all, there are only finitely many subsets of K), so the statement holds in this case. Assume now that F is infinite and suppose that K/F has finitely many intermediate extensions. Since K/F is finite, $K = F(\alpha_1, ..., \alpha_n)$ for some $\alpha_1, ...\alpha_n \in K$. We will prove that K/F is simple by induction on n. For $n = 1$, $K = F(\alpha_1)$ and the statement holds. Assume now that every extension of F that is generated by at most $n-1$ elements over F is a simple extension of F. Let $L = F(\alpha_1, ..., \alpha_{n-1})$. Then the extension L/F is finite and has finitely many intermediate extensions, so by the induction hypothesis $L = F(\beta)$ for some $\beta \in L$. Thus $K = F(\alpha_n, \beta)$. For $c \in F$, define the field $K_c = F(\alpha_n + c\beta)$. Clearly, $F \leq K_c \leq K$, so there exist $b, c \in F$, $b \neq c$, such that $K_b = K_c$ (this is where the infinity of F is used). Then $\alpha_n + b\beta, \alpha_n + c\beta \in K_b$, $\beta = \frac{(\alpha_n + b\beta) - (\alpha_n + c\beta)}{b-c} \in K_b$ and $\alpha_n = (\alpha_n + b\beta) - b\beta \in K_b$. It follows that $K = K_b = F(\alpha_n + b\beta)$. Conversely, assume that $K = F(\alpha)$ for some $\alpha \in K$ and let $p(x) = \min(F, \alpha)$. We will show that every intermediate extension L of K/F is determined by the divisors of $p(x)$, which are finitely many. Let L be an intermediate extension of K/F. Then $K = L(\alpha)$. Let $q(x) = \min(L, \alpha) = a_0 + \cdots + a_{m-1}x^{m-1} + x^m \in L[x]$, and $L_0 = F(a_0, ..., a_{m-1})$. Then $F \leq L_0 \leq L$, $K = L_0(\alpha)$ and $q(x), \min(L_0, \alpha) \in L_0[x]$, both irreducible over L_0 and both have α as a root, so $\min(L_0, \alpha) = q(x)$. It follows that $[K : L] = [K : L_0]$, so $L = L_0$ and L is determined by $q(x)$ which is a divisor of $p(x)$.

Corollary 2.44 If K/F is finite and separable, then $K = F(\alpha)$ for some $\alpha \in K$.

Proof. If K/F is normal, then K/F is Galois and by the Fundamental Theorem of Galois Theory, there are only finitely many intermediate extensions. If K/F is not Galois, we can construct a extension N of K, such that N/F is finite and Galois: since K/F is finite, $K = F(\alpha_1, ..., \alpha_n)$ for some $\alpha_1, ..., \alpha_n \in K$ that are separable over F. Let N be the splitting field of $\{\min(F, \alpha_1), ..., \min(F, \alpha_n)\}$ over F. Then N is the splitting field of a set of separable polynomials over F, so it is Galois, and it is clearly finite. So by the Fundamental Theorem of Galois Theory, there are only finitely many intermediate extensions of N/F and therefore of K/F. The statement now follows from Theorem 2.43.

3 Cyclotomic Extensions

Definition 3.1 Let F be a field. An element $\omega \in F$ is an n-th root of unity of $\omega^n = 1$. It is called a *primitive* n-th root of unity, if its order in F^* is n. The extension $F(\omega)/F$ is called a cyclotomic extension.

We note that if ω is an n-th root of unity, then it is also an m-th root of unity for any m that is a multiple of n. Since n-th roots of unity are the roots of $x^n - 1 \in F[x]$, there are at most n distinct n-th roots of unity in any extension of F. Also note that primitive n-th roots of unity do not always exist, as the following lemma shows.

Lemma 3.2 Let F be a field. Then a primitive n-th root of unity exists in an extension K of F if and only if the characteristic of F does not divide n.

Proof. Assume that $\mathrm{char}(F) = p$ and $n = pm$. Then an n-th root of unity ω is a root of $x^n - 1 \in F[x]$. Since $x^n - 1 = x^{pm} - 1 = (x^m - 1)^p$, we see that ω has order that divides m. Conversely, assume that n is not a multiple of $\mathrm{char}(F)$, and consider the set G of roots of $x^n - 1$, in the splitting field K of $x^n - 1$ over F. Since the derivative of $x^n - 1$ is $nx^{n-1} \neq 0$, which is relatively prime to $x^n - 1$, the roots of $x^n - 1$ are distinct, so $|G| = n$. Furthermore, by Theorem 1.8, G is cyclic, so there exists some $\omega \in G$ of order n.

A cyclotomic exension $F(\omega)/F$ is always Galois, and its Galois group is a subgroup of the $\mathbb{Z}_n^*$.

Proposition 3.3 Let F be a field of characteristic prime to n and let ω be a primitive n-th root of unity. The extension $F(\omega)/F$ is Galois, with Galois group isomorphic to a subgroup of $\mathbb{Z}_n^*$. In particular, $\mathrm{Gal}(F(\omega)/F)$ is abelian and $[F(\omega) : F] \mid \varphi(n)$.

Proof. Since $\gcd(n, \mathrm{char}(F)) = 1$, the polynomial $x^n - 1 \in F[x]$ is separable (by the derivative test) and since ω is a primitive n-th root of unity, $F(\omega)$ is the splitting field of $x^n - 1$ over F. So $F(\omega)$ is Galois over F. The automorphisms of $G = \mathrm{Gal}(F(\omega)/F)$ are determined by their action on ω. Any $\sigma \in G$ maps ω to another n-th root of unity ζ, $\sigma(\omega) = \zeta$. If the order of ζ is $d \mid n$, then $\sigma(\omega^d) = \zeta^d = 1$, and since σ is injective, $\omega^d = 1$, so that $n \mid d$ and therefore $d = n$. It follows that every automorphism in G maps ω to another *primitive* n-th root of unity ω^t with $1 \leq t \leq n$, $\gcd(t, n) = 1$. Furthermore, for $t_1, t_2 \in \mathbb{Z}$, if $t_1 \equiv t_2 (\mathrm{mod}\, n)$ then $\omega^{t_1} = \omega^{t_2}$. So the map

$$\begin{aligned} \theta : \mathrm{Gal}(F(\omega)/F) &\longrightarrow \mathbb{Z}_n^* \\ \sigma &\mapsto \overline{t} \end{aligned} \tag{82}$$

where $\sigma(\omega) = \omega^t$ is well defined and is clearly injective. For $\overline{t} \in \mathrm{im}(\theta)$, We denote σ_t the automorphism that maps to $\overline{t}$, that is $\theta(\sigma_t) = \overline{t}$, and the indices are taken modulo n. Since

$$\sigma_{st}(\omega) = \omega^{st} = (\omega^t)^s = \sigma_s(\omega^t) = \sigma_s \sigma_t(\omega), \tag{83}$$

we have

$$\theta(\sigma_s \cdot \sigma_t) = \theta(\sigma_{st}) = \overline{st} = \overline{s} \cdot \overline{t} = \theta(\sigma_s)\theta(\sigma_t). \tag{84}$$

Therefore, θ is an injective group homomorphism and $\mathrm{Gal}(F(\omega)/F))$ is isomorphic to $\mathrm{im}(\theta)$. Finally, $[F(\omega) : F] = |\mathrm{Gal}(F(\omega)/F)| = |\mathrm{im}(\theta)|$ and $|\mathrm{im}(\theta)|$ divides $|\mathbb{Z}_n^*| = \varphi(n)$.

It may be tempting to assume that ω can be mapped to *any* other primitive n-th root of unity, by some element of $\mathrm{Gal}(F(\omega)/F)$ (which would have to be isomorphic to $\mathbb{Z}_n^*$). Of course this is not true: one example may be constructed by taking F to contain ω. In this case $F(\omega) = F$, $\min(F, \omega) = x - \omega$ and indeed $\mathrm{Gal}(F(\omega)/F) = \{\mathrm{id}\}$. Other examples can be constructed when F is a finite field, as we will see in Section 4.

Definition 3.4 Let F be a field of characteristic prime to n and ω a primitive n-th root of unity in an extension of F. The polynomial

$$\Psi_n(x) = \prod_{\substack{0 \le j < n \\ \gcd(j,n)=1}} (x - \omega^j) \tag{85}$$

is called the n-th cyclotomic polynomial.

It is clear that $\deg(\Psi_n) = \varphi(n)$ and $\min(F, \omega) \mid \Psi_n$. The following proposition list some basic facts regarding cyclotomic polynomials.

Proposition 3.5 Let F be a field and n be prime to $\mathrm{char}(F)$. Then
1. $\Psi_n(x) \in F[x]$,
2. $x^n - 1 = \prod_{d \mid n} \Psi_d$.

Proof. Recall that any $\sigma \in \mathrm{Gal}(F(\omega)/F)$, may be extended to an automorhism σ^* of $F(\omega)[x]$, by

$$\sigma^*\left(\sum_i c_i x^i\right) = \sum_i \sigma(c_i) x^i. \tag{86}$$

Then $f \in F[x] \Leftrightarrow \sigma^*(f) = f$. We proceed to show that this is true for Ψ_n. Let $\sigma = \sigma_t$ for some $1 < t < n$, $\gcd(t, n) = 1$ and compute

$$\begin{aligned} \sigma^*(\Psi_n) = \sigma^*\left(\prod_{\substack{0 \le j < n \\ \gcd(j,n)=1}} (x - \omega^j)\right) &= \prod_{\substack{0 \le j < n \\ \gcd(j,n)=1}} \sigma^*(x - \omega^j) \\ = \prod_{\substack{0 \le j < n \\ \gcd(j,n)=1}} (x - \sigma(\omega)^j) \qquad &= \prod_{\substack{0 \le j < n \\ \gcd(j,n)=1}} (x - \omega^{jt}). \end{aligned} \tag{87}$$

Note now, that the map

$$\mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*, \quad \bar{j} \mapsto \bar{t} \cdot \bar{j} \tag{88}$$

is bijective, so as j ranges over the set $\{1 < j < n : \gcd(j, n) = 1\}$ so does $jt \bmod n$. It follows that

$$\prod_{\substack{0 \le j < n \\ \gcd(j,n)=1}} (x - \omega^{jt}) = \prod_{\substack{0 \le j < n \\ \gcd(j,n)=1}} (x - \omega^j) = \Psi_n. \tag{89}$$

The second statement is a matter of grouping together primitive d-th roots of unity, for $d \mid n$. More precisely, the set $\{0 \le j < n\}$ can be partitioned as

$$\begin{aligned}\{0 \le j < n\} &= \bigcup_{d \mid n} \left\{0 \le j < n : \gcd(j,n) = \frac{n}{d}\right\} \\ &= \bigcup_{d \mid n} \left\{0 \le \frac{n}{d} j' < n : \gcd\left(\frac{n}{d} j', n\right) = \frac{n}{d}\right\} \\ &= \bigcup_{d \mid n} \left\{\frac{n}{d} j' : 0 \le j' < d, \gcd(j', d) = 1\right\}.\end{aligned} \tag{90}$$

$$\Psi_n = \prod_{\substack{0<j<n \\ \gcd(j,n)=1}} (x - \omega^j) = \prod_{d \mid n} \prod_{0 \le j' < d} \left(x - \omega^{\frac{n}{d} j'}\right) = \prod_{d \mid n} \Psi_d, \tag{91}$$

since $\omega^{\frac{n}{d}}$ is a primitive d-th root of unity.

We focus now to the case $F = \mathbb{Q}$. It is immediate from the previous proposition, that $\Psi_n \in \mathbb{Q}[x]$. We can prove by induction on n that $\Psi_n \in \mathbb{Z}[x]$. Indeed, $\Psi_1 = x - 1 \in \mathbb{Z}[x]$. Assume $\Psi_d \in \mathbb{Z}[x]$ for $1 \le d < n$. Since $x^n - 1 = \Psi_n \cdot \left(\prod_{\substack{d \mid n \\ d<n}} \Psi_d\right)$, and by assumption $\prod_{\substack{d \mid n \\ d<n}} \Psi_d \in \mathbb{Z}[x]$, we obtain $\Psi_n \in \mathbb{Z}[x]$, as the unique quotient of the Euclidean division of $x^n - 1$ by $\prod_{\substack{d \mid n \\ d<n}} \Psi_d$ in $\mathbb{Z}[x]$.

Example 3.6 If n is prime, every $0 < j < n$ is relatively prime to n, so

$$\Psi_n = \prod_{0<j<n} (x - \omega^j) = \frac{x^n - 1}{x - 1} = 1 + x + \cdots + x^{n-1}. \tag{92}$$

Example 3.7 The primitive 1-st and 2-nd roots of unity in $\mathbb{C}^*$ are 1 and -1 respectively, so $\Psi_1 = x - 1$ and $\Psi_2 = x + 1$. To compute Ψ_3, note that $x^3 - 1 = (x-1)(x^2 + x + 1) = \Psi_1 \Psi_3$, so $\Psi_3 = x^2 + x + 1$. Further, $x^4 - 1 = (x^2 - 1)(x^2 + 1) = \Psi_1 \Psi_2 \Psi_4$ and since $x^2 - 1 = \Psi_1 \Psi_2$, we have $\Psi_4 = x^2 + 1$. Having computed Ψ_d for $d \mid n$, one can compute Ψ_n as the quotient of $x^n - 1$ by $\prod_{d \mid n} \Psi_d$.

Theorem 3.8 For any $n \in \mathbb{N}$, the polynomial $\Psi_n \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

Theorem 3.9 Let $n \in \mathbb{N}$ and let $\omega \in \mathbb{C}$ be a primitive n-th root of unity. Then $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$ and $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong Z_n^*$. More precisely, $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \left\{\sigma_j : 0 < j < n, \gcd(j,n) = 1\right\}$, where $\sigma_j(\omega) = \omega^j$.

Proof. By Proposition 3.3, $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is isomorphic to a subgroup of $\mathbb{Z}_n^*$. Since $\min(\mathbb{Q}, \omega) \mid \Psi_n$ and by Theorem 3.8, Ψ_n is irreducible in $\mathbb{Q}[x]$, it follows that $\min(\mathbb{Q}, \omega) = \Psi_n$ and $|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = [\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. It follows that $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ has to be isomorphic to the full group $\mathbb{Z}_n^*$.

4 Finite Fields

Let p be a prime, $\mathbb{F}_p$ be a finite field with p elements and let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$. If $K \leq \overline{\mathbb{F}}_p$ is a finite field, then K is a finite extension of $\mathbb{F}_p$. If $\left[K : \mathbb{F}_p\right] = n$ and $\{\gamma_1, ..., \gamma_n\}$ is an $\mathbb{F}_p$-basis of K, then every element of K can be written uniquely as $c_1\gamma_1 + \cdots + c_n\gamma_n$ for some $c_1, ..., c_n \in \mathbb{F}_p$. It follows that $|K| = p^n$. The goal of this section is to prove that for every $n \in \mathbb{N}$ there exists a unique extension of $\mathbb{F}_p$ in $\overline{\mathbb{F}}_p$ with p^n elements.

Theorem 4.1 (Existence and Uniqueness of Finite Fields) Let p be a prime and $n \in \mathbb{N}$. There exist a unique extension K of $\mathbb{F}_p$ with $\left[K : \mathbb{F}_p\right] = n$ in $\overline{\mathbb{F}}_p$.

Proof. Let $f = x^{p^n} - x \in \mathbb{F}_p[x]$ and $K = \left\{\alpha \in \overline{\mathbb{F}}_p : \alpha^{p^n} = \alpha\right\}$. Since $f' = -1$, by Lemma 2.19 the polynomial f has p^n distinct roots in $\overline{\mathbb{F}}_p$. For $\alpha, \beta \in K$, we have $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$ and for $\beta \neq 0$, $\left(\alpha\beta^{-1}\right)^{p^n} = \alpha^{p^n}\left(\beta^{p^n}\right)^{-1} = \alpha\beta^{-1}$, so K is a subfield of $\overline{\mathbb{F}}_p$ with p^n elements. It is in fact the spitting field of f over $\mathbb{F}_p$. Clearly $\left[K : \mathbb{F}_p\right] = n$.

To prove the uniqueness of K, let L any extension of $\mathbb{F}_p$ inside $\overline{\mathbb{F}}_p$ with $|L| = p^n$. For any $\gamma \in L^*$, we have $\gamma^{p^n - 1} = 1$ by Lagrange's Theorem, and thus $\gamma^{p^n} = \gamma$ for every $\gamma \in L$. It follows that $L \subseteq K$ and $|L| = |K| = p^n$, so $L = K$.

We will denote the finite field with $q = p^e$ elements by $\mathbb{F}_q$ and note that

$$\mathbb{F}_q = \left\{\gamma \in \overline{\mathbb{F}}_p : \gamma^q = \gamma\right\}. \tag{93}$$

Theorem 4.2 Let p be a prime and $n \in \mathbb{N}$.
1. There exists some $\alpha \in \mathbb{F}_{p^n}$ such that $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$.
2. There exists an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree n.

Proof. By Theorem 1.8, there exists some $\alpha \in \mathbb{F}_{p^n}^*$ such that $\mathbb{F}_{p^n}^* = \left\{\alpha^j : 0 \leq j \leq p^n - 2\right\}$. It is clear that $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p(\alpha)$, and $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$, since $\alpha \in \mathbb{F}_{p^n}$. So $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. Furthermore, $\deg\left(\min\left(\mathbb{F}_p, \alpha\right)\right) = \left[\mathbb{F}_{p^n} : \mathbb{F}_p\right] = n$.

Theorem 4.3 Let q be a power of a prime p. Then $\mathbb{F}_{q^m} \leq \mathbb{F}_{q^n} \Leftrightarrow m \mid n$.

Proof. By Equation 93, any $\gamma \in \mathbb{F}_q$ satisfies $\gamma^q = \gamma$, and by induction $\gamma^{q^j} = \gamma$ for every $j \in \mathbb{N}$. Therefore $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$. Futhermore, $\left[\mathbb{F}_{q^m} : \mathbb{F}_q\right] = m$ and $\left[\mathbb{F}_{q^n} : \mathbb{F}_q\right] = n$.

If $\mathbb{F}_q \leq \mathbb{F}_{q^m} \leq \mathbb{F}_{q^n}$, then $\left[\mathbb{F}_{q^m} : \mathbb{F}_q\right] \mid \left[\mathbb{F}_{q^n} : \mathbb{F}_q\right] \Rightarrow m \mid n$.

Conversely, assume that $n = dm$. For any $\gamma \in \mathbb{F}_{q^m}$, we have

$$\gamma^{q^m} = \gamma \Rightarrow \left(\gamma^{q^m}\right)^{q^m} = \gamma^{q^m} = \gamma \Rightarrow \gamma^{q^{2m}} = \gamma. \tag{94}$$

By induction we get $\gamma^{q^{dm}} = \gamma$, which implies that $\gamma \in \mathbb{F}_{q^n}$.

Proposition 4.4 Let q be a power of a prime, let $P \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree d and α a root of P. Then
1. $\mathbb{F}(\alpha) = \mathbb{F}_{q^d}$ and $\alpha \in \mathbb{F}_{q^n} \Leftrightarrow d \mid n$.
2. P has d simple roots in $\mathbb{F}_{q^d}$, namely $\left\{\alpha^{q^j} : j = 0, 1, ..., d-1\right\}$.

Proof.

1. We know that $\left[\mathbb{F}_q(\alpha) : \mathbb{F}_q\right] = \deg\big(\min\big(\mathbb{F}_q, \alpha\big)\big) = \deg(P) = d$, so $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$. Furthermore,
$$\alpha \in \mathbb{F}_{q^n} \Leftrightarrow \mathbb{F}_q(\alpha) \leq \mathbb{F}_{q^n} \Leftrightarrow \mathbb{F}_{q^d} \leq \mathbb{F}_{q^n} \Leftrightarrow d \mid n. \tag{95}$$
2. We may assume $d > 1$. Let $P = \sum_{i=0}^{d} c_i x^i \in \mathbb{F}_q[x]$. By assumption, $P(\alpha) = \sum_{i=0}^{d} c_i \alpha^i = 0$. Then
$$P(\alpha^q) = \sum_{i=0}^{d} c_i \alpha^{qi} = \sum_{i=0}^{d} c_i^q (\alpha^i)^q = \left(\sum_{i=0}^{d} c_i \alpha^i\right)^q = 0. \tag{96}$$
Inductively, we get $P\left(\alpha^{q^j}\right) = 0$ for every $j = 0, 1, ...$ We claim that $\alpha^{q^i} \neq \alpha^{q^j}$ for $0 \leq i < j \leq d-1$. Indeed,
$$\alpha^{q^i} = \alpha^{q^j} \Rightarrow \alpha^{q^i}\left(\alpha^{q^j - q^i} - 1\right) = 0 \Rightarrow \alpha^{q^j - q^i} = 1 \Rightarrow \alpha^{q^i(q^{j-i}-1)} = 1. \tag{97}$$
Since $\operatorname{ord}(\alpha) = t \mid q^d - 1$, we have $(t, q^i) = 1$, so there exists $s \in \mathbb{Z}$ such that $sq^i \equiv 1 \pmod{t}$. Therefore,
$$\alpha^{sq^i(q^{j-i}-1)} = 1 \Rightarrow \alpha^{q^{j-i}-1} = 1 \Rightarrow \alpha^{q^{j-i}} = \alpha \Rightarrow \alpha \in \mathbb{F}_{q^{j-i}} \Rightarrow d \mid j - i, \tag{98}$$
which is impossible, since $0 < j - i < d$.

Theorem 4.5 Let q be a prime power. Then $\operatorname{Gal}\big(\mathbb{F}_{q^n}/\mathbb{F}_q\big) = \langle \sigma_q \rangle = \left\{\sigma_q^j : j = 0, 1, ..., n-1\right\}$, where $\sigma_q(\gamma) = \gamma^q$ is the Frobenius automorphism.

Proof. By Theorem 4.2, $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ for some $\alpha \in \mathbb{F}_{q^n}$ and the roots of $\min\big(\mathbb{F}_q, \alpha\big)$ are α^{q^j} for $0 \leq j \leq n-1$. By Theorem 2.3, $\mathrm{id} : \mathbb{F}_q \to \mathbb{F}_q$ can be extended to $\tau_j : \mathbb{F}_q(\alpha) \to \mathbb{F}_q(\alpha)$, with $\tau_j(\alpha) = \alpha^{q^j}$. Moreover, any $\mathbb{F}_q$-automorphism $\rho : \mathbb{F}_q(\alpha) \to \mathbb{F}_q(\alpha)$ maps α to α^{q^j} for some $0 \leq j \leq n-1$, so $\rho = \tau_j$. It follow that $\operatorname{Gal}\big(\mathbb{F}_{q^n}/\mathbb{F}_q\big) = \left\{\tau_j : 0 \leq j \leq n-1\right\}$. To finish the proof, note that $\tau_1(\alpha) = \alpha^q = \sigma_q(\alpha)$ and $\tau_j(\alpha) = \alpha^{q^j} = \sigma_q^j(\alpha)$ for $0 \leq j \leq n-1$.