CHAPTER 2

GALOIS EXTENSIONS

2.1 Field Extensions

Definition 2.1.1. Let K and F be fields such that $K \subseteq F$ is a subring. We say that K is a *subfield* of F, and that F is a *field extension* of K, denoted $F|K$. If $K \subseteq E \subseteq F$ are fields, we call E an *intermediate field* of the field extension $F|K$.

Definition 2.1.2. Let $F|K$ be a field extension and let $\mathcal{S} \subseteq F$. We denote by $K(\mathcal{S}) \subseteq F$ the intermediate field of $F|K$ generated by $\mathcal{S}$. In particular, $K(\mathcal{S})$ is the intersection of all intermediate fields $K \subseteq E \subseteq F$ such that $\mathcal{S} \subseteq E$. If $\mathcal{S} = \{\alpha\}$, then we write $K(\alpha)$ instead of $K(\mathcal{S})$.

Definition 2.1.3. Let $F|K$ be a field extension. We define the *degree of the field extension* $[F : K]$ by the dimension of the K-vector space F, i.e.

$$[F : K] = \dim_K(F).$$

We say that the field extension $F|K$ is finite if the degree $[F : K]$ is finite. Otherwise, $F|K$ is infinite.

Proposition 2.1.4 (The Tower Law)**.** *Let $K \subseteq E \subseteq F$ be field extensions. If $F|E$ and $E|K$ are finite, then $F|K$ is finite, with*

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

Moreover, $[F : K]$ is infinite if and only if $[F : E]$ or $[E : K]$ is infinite.

Proof. Assume that $F|E$ and $E|K$ are finite. Then, we can find a finite K-basis for E and a finite E-basis F respectively:

$$\{e_1, e_2, \dots, e_n\}, \qquad \{f_1, f_2, \dots, f_m\}.$$

We claim that the following is a K-basis for F:

$$\{e_1 f_1, e_1 f_2, \dots, e_n f_m\}.$$

So, let $\alpha \in F$. Using the E-basis for F, we can find $\alpha_1, \alpha_2, \dots, \alpha_m \in E$ such that

$$\alpha = \alpha_1 f_1 + \alpha_2 f_2 + \dots + \alpha_m f_m.$$

Now, using the K-basis for E, we can find $\beta_{i,j} \in K$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ such that

$$\begin{aligned}
\alpha &= \alpha_1 f_1 + \dots + \alpha_m f_m \\
&= (\beta_{1,1} e_1 + \dots + \beta_{1,n} e_n) f_1 + \dots + (\beta_{m,1} e_1 + \dots + \beta_{m,n} e_n) f_m \\
&= \beta_{1,1} e_1 f_1 + \dots + \beta_{1,n} e_n f_1 + \dots + \beta_{m,n} e_n f_m.
\end{aligned}$$

Hence, the set

$$\{e_1f_1, e_1f_2, \dots, e_nf_m\}.$$

spans F. Now, let $\alpha_{i,j} \in K$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ such that

$$\begin{aligned} 0 &= \alpha_{1,1}e_1f_1 + \dots + \alpha_{m,n}e_nf_m \\ &= (\alpha_{1,1}e_1 + \dots + \alpha_{1,n}e_n)f_1 + \dots (\alpha_{m,1}e_1 + \dots + \alpha_{m,n}f_m). \end{aligned}$$

In that case, since $\{f_1, f_2, \dots, f_m\}$ forms a basis for F, we find that

$$\alpha_{i,1}e_1 + \dots + \alpha_{i,n}e_n = 0$$

for all $1 \leq i \leq m$. Moreover, since $\{e_1, e_2, \dots, e_n\}$ forms a basis for E, we find that $\alpha_{i,j} = 0$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. Hence, the set

$$\{e_1f_1, e_1f_2, \dots, e_nf_m\}.$$

forms a basis for F. In particular,

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

□

Definition 2.1.5. Let $F|K$ be a field extension, and let $\alpha \in F$. We say that α is *algebraic* over K if there exists a non-zero polynomial $f \in K[x]$ such that $f(\alpha) = 0$. Otherwise, α is *transcendental* over K. We say that the extension $F|K$ is *algebraic* if for all $\alpha \in F$, α is algebraic over K.

Proposition 2.1.6. *Let $F|K$ be a finite extension. Then, $F|K$ is an algebraic extension.*

Proof. Let $[F : K] = n$, and let $\alpha \in F$. We know that the set

$$\{1, \alpha, \alpha^2, \dots, \alpha^n\}$$

has $n + 1$ elements, so it cannot be linearly independent in K. Hence, there exist $k_0, k_1, \dots, k_n \in K$, not all zero, such that

$$k_n\alpha^n + \dots + k_1\alpha + k_0 = 0.$$

So, define the polynomial $f \in K[x]$ by

$$f(x) = k_nx^n + \dots + k_1x + k_0.$$

Since not all of k_i's are zero for $0 \leq i \leq n$, we find that f is a non-zero polynomial. Moreover, $f(\alpha) = 0$ by construction. Hence, α is algebraic over K, meaning that $F|K$ is an algebraic extension. □

Lemma 2.1.7. *Let $F|K$ be a field extension and let $\alpha \in F$. Then, α is algebraic over K if and only if the evaluation map $ev_\alpha \colon K[x] \to K$ is not injective.*

Proof. Assume first that α is algebraic over K. In that case, there exists a non-zero polynomial $f \in K[x]$ such that $f(\alpha) = 0$. Hence, the evaluation map ev_α cannot be injective- there are 2 polynomials mapping to 0.

Now, assume that the evaluation map ev_α is not injective. In that case, the kernel $\ker ev_\alpha = (f)$ is non-zero, i.e. f is non-zero. Moreover, $f(\alpha) = 0$, meaning that α is algebraic over K. □

Proposition 2.1.8. *Let $F|K$ be a field extension and let $\alpha \in F$ be algebraic over K. Then, there exists a unique monic polynomial $m_{\alpha,K} \in K[x]$, of smallest degree, such that*

- $m_{\alpha,K} = 0$*;*
- $m_{\alpha,K}$ *divides any $g \in K[x]$ with $g(\alpha) = 0$.*

Proof. Since α is algebraic, the evaluation map $ev_\alpha \colon K[x] \to K$ is not injective. Moreover, since $K[x]$ is a principal ideal domain, we find that $\ker ev_\alpha = (f)$. Without loss of generality, assume that f is monic. In that case, we can set $m_{\alpha,K} = f$, so that it satisfies both the properties. □

Definition 2.1.9. Let $F|K$ be a field extension and let $\alpha \in F$ be algebraic over K. The unique monic polynomial of smallest degree $m_{\alpha,K} \in K[x]$ is called the *minimal polynomial* of α over K.

Lemma 2.1.10. *Let $F|K$ be a field extension and let $\alpha \in F$ be algebraic over K. The minimal polynomial $m_{\alpha,K}$ is irreducible. Moreover, it is the unique monic polynomial that is irreducible over K such that α has a root.*

Proof. Let $m_{\alpha,K} = fg$, for $f, g \in K[x]$. In that case, $f(\alpha)g(\alpha) = 0$, meaning that either $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss of generality, assume that $f(\alpha) = 0$, meaning that $f \in \ker ev_\alpha = (m_{\alpha,K})$. Hence, g is a unit in $K[x]$, so $m_{\alpha,K}$ is irreducible. □

Lemma 2.1.11. *Let $F|K$ be a field extension and let $\alpha \in F$ be algebraic over K. Then,*

$$K[x]/(m_{\alpha,K}) \cong \operatorname{Im} ev_\alpha = K(\alpha) \subseteq F.$$

Proof. By the First isomorphism theorem, we know that

$$K[x]/(m_{\alpha,K}) \cong \operatorname{Im} ev_\alpha.$$

Since $m_{\alpha,K}$ is irreducible, we know that $\operatorname{Im} ev_\alpha$ is a field. Since the image $\operatorname{Im} ev_\alpha$ is a field containing K (constant functions) and α (the image of $f(x) = x$), i.e. $K(\alpha) \subseteq \operatorname{Im} ev_\alpha$. Moreover, a field containing K and α contains expressions in α with coefficients in K, so $K(\alpha) \supseteq \operatorname{Im} ev_\alpha$. □

Lemma 2.1.12. *Let K be a field and let $f \in K[x]$. Then,* $\dim_K(K[x]/(f)) = \deg(f)$.

Proof. For any $g \in K[x]$, the division algorithm tells us that $g = fq + r$, for $q, r \in K[x]$ with $\deg r < \deg f = d$. Hence,

$$K[x] = (f) \oplus K[x]_{\leq d},$$

where $K[x]_{\leq d}$ is the space of polynomials of degree less than d. Hence, $K[x]/(f) \cong K[x]_{\leq d}$ as vector spaces, meaning that

$$\dim_K(K[x]/(f)) = \dim_K K[x]_{\leq d} = d = \deg(f).$$

□

Theorem 2.1.13. *Let $F|K$ be a field extension and let $\alpha \in F$ be algebraic over K, with monic polynomial $m_{\alpha,K} \in K[x]$. Then, there is an isomorphism of fields and K-vector spaces*

$$K[x]/(m_{\alpha,K}) \to K(\alpha)$$

given by $f + (m_{\alpha,K}) \mapsto f(\alpha)$. In particular, $[K(\alpha) : K] = \deg(m_{\alpha,K})$. In particular, $K(\alpha)|K$ is an algebraic extension.

Definition 2.1.14. Let $F|K$ be a field extension. We say that $F|K$ is *simple* if $F = K(\alpha)$ for some $\alpha \in F$.

Proposition 2.1.15. *Let $F|K$ be a field extension and let $\alpha, \beta \in F$ be algebraic over K, with $K(\alpha)|K$ and $K(\beta)|K$ simple algebraic extensions. Then, there exists a field isomorphism $\theta \colon K(\alpha) \to K(\beta)$ fixing all elements of K such that $\theta(\alpha) = \beta$ if and only if α and β have the same minimal polynomial over K.*

Proof. Assume first that there exists a field isomorphism $\theta \colon K(\alpha) \to K(\beta)$. In that case, let

$$m_{\alpha,K} = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x].$$

We know that $m_{\alpha,K}(\alpha) = 0$, meaning that

$$\begin{aligned} m_{\alpha,K}(\beta) &= \beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0 \\ &= \theta(\alpha)^n + a_{n-1}\theta(\alpha)^{n-1} + \cdots + a_1\theta(\alpha) + a_0 \\ &= \theta(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\ &= \theta(f(\alpha)) = \theta(0) = 0. \end{aligned}$$

Since $m_{\alpha,K}$ is irreducible over K, we find that $m_{\alpha,K} = m_{\beta,K}$. That is, α and β have the same minimal polynomial over K.

Now, assume that α and β have the same minimal polynomial f over K. We know that

$$K(\alpha) \cong K[x]/(f) \cong K(\beta).$$

We have isomorphisms $\varphi_\alpha \colon K[x]/(f) \to K(\alpha)$ and $\varphi_\beta \colon K[x]/(f) \to K(\beta)$. Define $\theta = \varphi_\beta \circ \varphi_\alpha^{-1}$. Then, for all $k \in K$,

$$\theta(k) = \varphi_\beta(\varphi_\alpha^{-1}(k)) = \varphi_\beta(k + (f)) = k.$$

So, θ is a field isomorphism fixing K. □

Theorem 2.1.16 (Kronecker's Theorem). *Let K be a field and let $f \in K[x]$ be a polynomial. Then, there exists a field extension $F|K$ and an $\alpha \in F$ such that $f(\alpha) = 0$.*

Proof. Without loss of generality, assume that f is irreducible. In that case, $F = K[x]/(f)$ is a field, with $F|K$ is a field extension. Now, let $\alpha \in F$ by $\alpha = x + (f)$. Then,

$$f(\alpha) = f(x) + (f) = 0.$$

□

Definition 2.1.17. Let $\overline{K}|K$ be a field extension. We say that $\overline{K}|K$ is *algebraic field extension* if $\overline{K}$ is algebraically closed.

Theorem 2.1.18. *Every field has an algebraic closure.*

Theorem 2.1.19. *Let K be a subfield of $\mathbb{C}$. Then,*

$$\overline{K} = \{\alpha \in \mathbb{C} \mid \alpha \textit{ algebraic over } K\}.$$

Proof. Let

$$L = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } K\}.$$

We first claim that L is a field. So, let $\alpha_1, \alpha_2 \in L$. Then, α_1, α_2 are algebraic over K. In that case, we know that $[K(\alpha, \beta) : K]$ is finite, and hence algebraic. In particular, we find that $\alpha - \beta \in K(\alpha, \beta)$ is algebraic over K, and $\alpha\beta^{-1} \in K(\alpha, \beta)$ is algebraic over K if β is non-zero. Hence, L is a field.

By definition, L is algebraic over K, i.e. $L \subseteq \overline{K}$. Now, we show that $\overline{K} = L$. So, let $f \in K[x]$ be a non-constant polynomial. We know that f has roots in $\mathbb{C}$- $\alpha_1, \dots, \alpha_n$. Define the field $M = L(\alpha_1, \dots, \alpha_n)$. Since $M|L$ is finite, it is algebraic. Now, since $M|L$ and $L|K$ are both algebraic, $M|K$ is algebraic. In particular, $\alpha_1, \dots, \alpha_n$ are algebraic over K, meaning that they lie in L. Hence, L is algebraically closed. Hence, $L = \overline{K}$. □

2.2 Normal and Separable Extensions

Definition 2.2.1. An *algebra* over a ring K is a ring homomorphism $\eta\colon K \to F$, for some field K. A homomorphism between two K-algebras $\eta\colon K \to F$ and $\eta'\colon K \to F'$ is a ring homomorphism $f\colon F \to F'$ such that $f \circ \eta = \eta'$.

Definition 2.2.2. Let $F|K$ be a field extension. We denote by $\mathrm{Aut}(F|K)$ the set of all K-algebra isomorphism $F \to F$, considered as a group under composition.

Definition 2.2.3. Let K be a field and let $f \in K[x]$. An extension field F of K is called a *splitting field* for f if it factorises into linear factors over F, and if there is no intermediate field $K \subseteq E \subsetneq F$ with this property.

Theorem 2.2.4. *Let K be a field. For every $f \in K[x]$, there exists a splitting field $F|K$.*

Proof. If f factorises into linear factors over K, then K is the splitting field of f. Otherwise, f has an irreducible factor g. In that case, let $F = K[x]/(g)$. Since g is irreducible, (g) is a maximal ideal, and so F a field. Now, let $\alpha = x + (g) \in F$. We have

$$g(\alpha) = g(x) + (g) = 0 + (g),$$

so g has a root in K. Hence, $g(x) = (x - \alpha)h(x)$, where $\deg h = \deg g - 1$. We can continue this process to fully factorise f- it will take at most $\deg f$ steps.

The resulting field F must be the splitting field for f- by construction, f splits into linear factors in F. Moreover, for an intermediate subfield $K \subseteq L \subsetneq F$, we know that L does not contain one of the roots of f (by construction), and so f cannot split into linear factors in L. □

This field can be taken as the algebraic closure $\overline{K}$ of K.

Theorem 2.2.5. *Let $\phi\colon K_1 \to K_2$ be a field isomorphism. Moreover, let $F_1|K_1$ be a splitting field for $f \in K_1[x]$ and let $F_2|K_2$ be a splitting field $\phi(f) \in K_2[x]$. Then, there exists an isomorphism $\Phi\colon F_1 \to F_2$ such that $\iota_1 \circ \Phi = \phi \circ \iota_2$, where $\iota_1 \circ K_1 \to F_1$ and $\iota_2\colon K_2 \to F_2$ be inclusion maps.*

Proof. □

Corollary 2.2.6. *Let K be a field and let $f \in K[x]$. If F_1 and F_2 are splitting fields for f, then there exists an isomorphism $F_1 \cong F_2$ of K-algebras.*

Proof. □

Definition 2.2.7. Let $F|K$ be a field extension. We say that the extension $F|K$ is *normal* if for all polynomial $f \in K[x]$ irreducible with a root in F, f splits into linear factors in $F[x]$.

Theorem 2.2.8. *Let $E|K$ be a field extension. Then, $E|K$ is a finite, normal extension if and only if $E|K$ is the splitting field of some $f \in K[x]$.*

Proof. First, assume that $E|K$ is a finite, normal extension. In that case, $E = K(\alpha_1, \dots, \alpha_n)$, for $\alpha_1, \dots, \alpha_n \in E$. Since α_i are algebraic over K, we can find minimal polynomial $f_i \in K[x]$ of α_i. Since $E|K$ is normal, we know that f_i split over E. Hence, $f = f_1 \dots f_n$ splits over E. Since E is generated by the roots of f, E must be the splitting field of f.

Now, assume that $E|K$ is the splitting field of $f \in K[x]$. In that case, $E = K(\alpha_1, \dots, \alpha_n)$, for $\alpha_1, \dots, \alpha_n \in \overline{K}$. So, $E|K$ is a finite extension. Now, let $g \in K[x]$ be an irreducible polynomial with a root in E. Define F to be the splitting field of fg. Since all roots of f are roots of fg, we find that $E \subseteq F$. Let $\beta_1, \beta_2 \in F$ be roots of g. We claim that

$$[E(\beta_1) : E] = [E(\beta_2) : E].$$

Consider the field towers

$$K \subseteq K(\beta_1) \subseteq E(\beta_1) \subseteq F \qquad K \subseteq K(\beta_2) \subseteq E(\beta_2) \subseteq F.$$

Hence,

$$\begin{aligned}[E(\beta_1) : K(\beta_1)] \cdot [K(\beta_1) : K] = [E(\beta_1) : K] = [E(\beta_1) : E] \cdot [E : K] \\ [E(\beta_2) : K(\beta_2)] \cdot [K(\beta_2) : K] = [E(\beta_2) : K] = [E(\beta_2) : E] \cdot [E : K].\end{aligned}$$

Since g is irreducible over K, we find that $K(\beta_1) \cong K(\beta_2)$, meaning that $[K(\beta_1) : K] = [K(\beta_2) : K]$. Moreover, since $E(\beta_j)$ is the splitting field of f over $K(\beta_j)$ for $j = 1, 2$, we have $E(\beta_1) \cong E(\beta_2)$. So,

$$[E(\beta_1) : K(\beta_1)] = [E(\beta_2) : K(\beta_2)].$$

So,

$$\begin{aligned}[E(\beta_1) : E] &= \frac{[E(\beta_1) : K(\beta_1)] \cdot [K(\beta_1) : K]}{[E : K]} \\ &\frac{[E(\beta_2) : K(\beta_2)] \cdot [K(\beta_2) : K]}{[E : K]} = [E(\beta_2) : K].\end{aligned}$$

We know that $\beta \in E$ if and only if $[E(\beta_1) : E] = 1$. Since g has a root in E, all the roots of g are contained in E. Hence, $E|K$ is normal. □

Theorem 2.2.9. *Let $F|K$ be a finite normal extension. If $K \subseteq E \subseteq F$ is an intermediate field, then any K-algebra homomorphism $\sigma \colon E \to F$ extends to a K-algebra homomorphism $F \to F$.*

Proof. Note that σ is injective, so $E \cong \sigma(E)$. We know that F is the splitting field of some polynomial $f \in K[x]$. So, $F = K(\alpha_1, \dots, \alpha_n)$, where α_i are roots of f not in K. Now, let $f_1 \in E[x]$ be the minimal polynomial of α_1. In that case, $\sigma(f_1)$ is irreducible. Moreover, f_1 divides f, meaning that $\sigma(f_1)$ divides $\sigma(f) = f$. Since α_1 and β_1 have the same minimal polynomial, we can extend σ to $E(\alpha_1) \to \sigma(E)(\beta_1)$. We can continue this inductively to extend the homomorphism to F. □

Theorem 2.2.10. *Let $E|K$ be a finite extension. Then, $E|K$ is normal if and only if there exists a finite normal extension $F|K$ such that $K \subseteq E \subseteq F$, and for every K-homomorphism $\sigma \colon E \to F$, we have $\sigma(E) = E$.*

Proof. If $E|K$ is normal, we can take $F = E$- for a K-homomorphism $\sigma\colon E \to F$, we have $\sigma(E) = F = E$. Now, assume that there exists a finite normal extension $F|K$ such that $K \subseteq E \subseteq F$, and for every K-homomorphism $\sigma\colon E \to F$, we have $\sigma(E) = E$. Let $f \in K[x]$ have a root $\alpha \in E$. Without loss of generality, assume that f is irreducible over K. In that case, since $F|K$ is normal, f splits over F. Now, let $\beta \in F$ be another root of f. We know that we can extend σ to $K(\alpha) \to K(\beta) \subseteq F$. Hence, we can further extend σ to $F \to F$. In that case, we have $\beta = \sigma(\alpha) \in E$, meaning that $E|K$ is normal. □

Proposition 2.2.11. *Let $K(\alpha)|K$ is finite, then*

$$[\mathrm{Aut}(K(\alpha)|K)] \leq [K(\alpha) : K].$$

Proof. Let $f \in K[x]$ be the minimal polynomial of α. We know that $[K(\alpha) : K] = \deg f$. Now, let $\alpha_1, \dots, \alpha_m$ be the roots of α. Since f has at most $\deg f$ distinct roots, we have $m \leq \deg f$. A K-homomorphism $K(\alpha) \to K(\alpha)$ permutes the roots of α. Moreover, it is determined by where it sends α. Hence,

$$[\mathrm{Aut}(K(\alpha)|K)] \leq m \leq [K(\alpha) : K].$$

□

Definition 2.2.12. Let K be a field, and $F|K$ an algebraic extension.

1. An irreducible polynomial $f \in K[x]$ is *separable* if every root of f is a splitting field F of f is simple (i.e. appears with multiplicity 1).

2. An element $\alpha \in F$ is called *separable* if its minimal polynomial is separable.

3. $F|K$ is called *separable* if every element of F is separable.

Proposition 2.2.13. *Let $E|K$ be a finite, normal, separable, simple extension. Then, $[E : K] = |\operatorname{Aut}(E|K)|$.*

Proof. Let $E = K(\alpha)$, for some $\alpha \in E$, and let $\alpha_1, \dots, \alpha_m$ be the roots of the minimal polynomial f of α. Without loss of generality, assume that $\alpha_1 = \alpha$. Since $E|K$ is separable, we have $m = \deg f$. We know that there exists a K-homomorphism $K(\alpha) \to K(\alpha_i)$ that maps α to α_i, for each $1 \leq i \leq m$. Hence,

$$[E : K] = [K(\alpha) : K] = [K(\alpha_i) : K].$$

Since $K(\alpha_i) \subseteq E$, this implies that $K(\alpha_i) = E$. So, there are $\deg f$ distinct K-automorphisms of E, i.e. $[E : K] = |\operatorname{Aut}(E|K)|$. □

Theorem 2.2.14 (Primitive Element Theorem)**.** *Let $E|K$ be a finite, separable extension. Then, there exists an $\alpha \in E$ such that $E = K(\alpha)$.*

Proof. First, assume that F has infinitely many elements. Since $E|K$ is finite, we know that $E = K(\alpha_1, \dots, \alpha_n)$, for $\alpha_1, \dots, \alpha_n \in E$. So, inductively, we show that $K(\beta, \gamma) = K(\alpha)$ for all $\beta, \gamma \in E$. Let f, g be the minimal polynomials of β and γ over K respectively. Next, let F be the splitting field of $fg \in E[x]$. Let $\beta_1 = \beta, \beta_2, \dots, \beta_m$ and $\gamma_1 = \gamma, \gamma_2, \dots, \gamma_n$ be the roots of f and g respectively.

Since $E|K$ is separable, $\beta_1, \ldots, \beta_m$ are distinct, and so are $\gamma_1, \ldots, \gamma_n$. Now, since K is infinite, there exists a non-zero $\alpha \in K$ such that

$$\alpha \neq \frac{\beta_i - \beta}{\gamma_j - \gamma}$$

for $1 \leq i \leq m$ and $2 \leq j \leq n$. Now, let $\alpha = \beta + a\gamma$. We find that $\alpha - a\gamma_j \neq \beta_i$ for $1 \leq i \leq m$ and $2 \leq j \leq n$. We know that f is the minimal polynomial of β, so $f(\beta) = 0$. Now, consider the polynomial $h(x) = f(\alpha - ax) \in K(\alpha)[x]$. We find that

$$h(\gamma) = f(\alpha - a\gamma) = f(\beta) = 0.$$

Moreover, $h(\gamma_j) \neq 0$ for all $2 \leq j \leq n$, meaning that γ is the only common root of h and g. That is, $m_{\gamma,K(\alpha)}$ divides both h and g, we find that $m_{\gamma,K(\alpha)}$ is linear, i.e. $m_{\gamma,K(\alpha)} = x - \gamma \in K(\alpha)[x]$. So, $\gamma \in K(\alpha)$, meaning that $\beta = \alpha - a\gamma \in K(\alpha)$. Hence, $K(\alpha) = K(\beta, \gamma)$.

Instead, if K is finite, then E is also finite. Since E is a field, this implies that E^* is cyclic, so let $E^* = \langle \alpha \rangle$. Then, $E = K(\alpha)$. □

Definition 2.2.15. Let $E|K$ be a finite, separable extension, and let $\alpha \in E$ such that $E = K(\alpha)$. We say that α is a *primitive element.*

Corollary 2.2.16. *Let $E|K$ be any finite, normal, separable extension. Then,*

$$[E : K] = [Aut(E|K)].$$

Proof. Since $E|K$ is finite and separable, we have $E = K(\alpha)$. Hence, E is simple, meaning that

$$[E : K] = [Aut(E|K)].$$

□

Proposition 2.2.17. *Let $F|E$ and $E|K$ be finite extensions. If $F|K$ is separable, then $F|E$ and $E|K$ are separable.*

Proof. Let $\alpha \in E$. Since $F|K$ is separable, we know that the minimal polynomial of $\alpha \in F$ is separable. Hence, $E|K$ is separable. Now, let $\alpha \in F$, and let $f \in E[x]$ be the minimal polynomial of α, and $g \in K[x]$ the minimal polynomial of α. Since $F|K$ is separable, g has distinct roots. We have $f \mid g$, so f also has distinct roots, meaning that f is separable. Hence, $F|E$ is separable. □

Definition 2.2.18. Let K be a field. We say that K is *perfect* if every finite extension of K is separable.

Lemma 2.2.19. *Let K be a field of characteristic zero, and let $f \in K[x]$ be non-zero. Let $\overline{K}$ be the algebraic closure of K. Then, f has multiple roots in $\overline{K}$ if and only if f and the derivative f' have a common factor of positive degree in $K[x]$.*

Proof. □

Proposition 2.2.20. *Let K be a field of characteristic zero. Then, every irreducible polynomial $f \in K[x]$ is separable. Hence, K is a perfect field.*

Proof. □

Proposition 2.2.21. *Let K be a finite field. Then, K is perfect.*

Proof. $\square$

2.3 Galois Extensions

Definition 2.3.1. Let $F|K$ is a field extension. We say that $F|K$ is *Galois* if it is finite, normal and separable.

Corollary 2.3.2. *Let $K \subseteq F \subseteq \mathbb{C}$ be fields. Then, the following are equivalent:*

1. *$F|K$ is Galois.*
2. *$F|K$ is finite and normal.*
3. *F is the splitting field of some $f \in K[x]$.*

Proof. $\square$

Definition 2.3.3. Let $F|K$ be a Galois extension. Then, the automorphism group $\mathrm{Aut}(F|K)$ is the *Galois group* of $F|K$.

Proposition 2.3.4. *Let $F|K$ be a Galois extension and let $K \subseteq E \subseteq F$ be an intermediate field. Then, $F|E$ is a Galois extension and $\mathrm{Fix}(F, \mathrm{Aut}(F|E)) = E$.*

Proof. $\square$

Theorem 2.3.5 (The Main Theorem of Galois Theory)**.** *Let $F|K$ be a Galois extension, with Galois group $G = \mathrm{Aut}(F|K)$.*

1. *Let*

   $$M = \{E \mid K \subseteq E \subseteq F \textit{ intermediate field}\}, \qquad N = \{H \mid H \subseteq G \textit{ subgroup}\}.$$

   Then, there is a map $\alpha\colon M \to N$ defined by $\alpha(E) = \mathrm{AUt}(F|E)$, with inverse $\phi\colon N \to M$ given by $\phi(H) = \mathrm{Fix}(F, H)$, which are inverse bijections.

2. *The maps α and ϕ are order reversing, i.e.*

   $$E_1 \subseteq E_2 \iff \alpha(E_1) \supseteq \alpha(E_2) \iff \mathrm{Aut}(F|E_2) \subseteq \mathrm{Aut}(F|E_1),$$

   and

   $$H_1 \subseteq H_2 \iff \phi(H_1) \supseteq \phi(H_2) \iff \mathrm{Fix}(F, H_2) \subseteq \mathrm{Fix}(F, H_1).$$

3. *If $K \subseteq E \subseteq F$ is an intermediate field, then $F|E$ is Galois, with*

   $$[F : E] = |\mathrm{Aut}(F|E)| \textit{ and } [E : K] = \frac{|G|}{|\mathrm{Aut}(F|E|)}.$$

4. *A subgroup $H \subseteq G$ is normal if and only if the corresponding field extension $\phi(H)|K$ is normal. In this case,*

   $$\mathrm{Aut}(\varphi(H)|K) \cong G/H.$$

   Alternatively, an intermediate field extension $E|K$ is normal if and only if $\mathrm{Aut}(F|E) \lhd \mathrm{Aut}(F|K)$, in which case

   $$\mathrm{Aut}(E|K) \cong \mathrm{Aut}(F|K)/\mathrm{Aut}(F|E).$$

Proof. $\square$

2.4 Solving the Quintic Equation

Definition 2.4.1. Let G be a group. We say that G is *solvable* if there is a composition series

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

such that for every $0 \leq j < n$,

- the group G_j is normal in G_{j+1} and
- the quotient group G_{j+1}/G_j is abelian.

Lemma 2.4.2. *Let G be a group and $N \lhd G$. Then, G is solvable if and only if N and G/N are solvable.*

Proof. □

Theorem 2.4.3. *Let $n \in \mathbb{Z}_{\geq 5}$. Then, A_n is not simple. In particular, S_n is not solvable.*

Proof. □

Proposition 2.4.4. *Let $G \leq S_5$ such that G has a transposition and a 5-cycle. Then, $G = S_5$.*

Proof. □

Definition 2.4.5. Let $F|K$ be a field extension and let $\alpha \in F$. We say that $\alpha \in F$ is a *radical over* K if there exists an $n \in \mathbb{Z}_{\geq 1}$ such that $\alpha^n \in K$.

Definition 2.4.6. Let $F|K$ be a field extension. We say that $F|K$ is a *radical extension* if

$$F = K(\alpha_1, \ldots, \alpha_m)$$

such that α_1 is a radical over K, and α_j is a radical over $K(\alpha_1, \ldots, \alpha_{j-1})$ for $2 \leq j \leq m$. The elements α_j are said to form a *radical sequence*.

Definition 2.4.7. Let $K \subseteq \mathbb{C}$ be a field and $f \in K[x]$. If $K \subseteq E \subseteq \mathbb{C}$ is a splitting field for f, then we say that f is *solvable by radicals* if there exists $K \subseteq E \subseteq F \subseteq \mathbb{C}$ such that $F|K$ is a radical extension.

Lemma 2.4.8. *Let $K \subseteq E \subseteq \mathbb{C}$, where $E|K$ is the splitting field of $x^n - 1 \in K[x]$ and $n \in \mathbb{Z}_{\geq 1}$. Then, $\mathrm{Aut}(E|K)$ is abelian.*

Proof. □

Lemma 2.4.9. *Let $n \in \mathbb{Z}_{\geq 1}$ and let $E \subseteq \mathbb{C}$ be a subfield in which $x^n - 1$ splits. Moreover, let $a \in E$ and $F \subseteq \mathbb{C}$ be the splitting field for $x^n - a \in E[x]$. Then, $\mathrm{Aut}(F|E)$ is abelian.*

Proof. □

Proposition 2.4.10. *Let $K \subseteq \mathbb{C}$ and $a \in K$. If F is the splitting field of $f(x) = x^n - a \in K[x]$, then $\mathrm{Aut}(F|K)$ is solvable.*

Proof. $\square$

Theorem 2.4.11. *Let $K \subseteq E \subseteq F \subseteq \mathbb{C}$ be fields such that $E|K$ is normal and $F|K$ a radical extension. Then, the group $\mathrm{Aut}(E|K)$ is solvable.*

Proof. $\square$

Corollary 2.4.12. *Let $K \subseteq \mathbb{C}$ be a field, $f \in K[x]$ and let $E|K$ be a splitting field of f. If f is solvable by radicals, then $\mathrm{Aut}(E|K)$ is solvable.*

Proof. $\square$

Definition 2.4.13. Let $F|K$ be a field extension. We say that $\mathrm{Aut}(F|K)$ is the *Galois group* of $f \in K[x]$ over K if $F|K$ is the splitting field of f.

Lemma 2.4.14. *Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5. If f has precisely three real roots in $\mathbb{C}$, then the Galois group of f over $\mathbb{Q}$ is isomorphic to the symmetric group S_5.*

Proof. $\square$

Example 2.4.15. We show that the polynomial $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ is not solvable by radicals.