Modern Algebra

September 15, 2023

Contents

Chapter 1

Extension Fields

1.1 Commutative Rings

Definition 1.1. Let R be a commutative ring and $a, b \in R$ with $b \neq 0$.

(a) a is said to be a *multiple* of b if there exists $x \in R$ such that $a = bx$. In this case, b is said to *divide* a or be a *divisor* of a, written $b \mid a$.

(b) A *greatest common divisor* of a and b is $0 \neq d \in R$ such that

(1) $d \mid a$ and $d \mid b$,

(2) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

A greatest common divisor of a and b will be denoted by $\gcd(a, b)$.

Remark. In a commutative ring R, $b \mid a$ if and only if $a \in (b)$ if and only if $(a) \subseteq (b)$. Then $d = \gcd(a, b)$ with $a, b \in R$ if and only if

(a) $(a, b) \subseteq (d)$,

(b) if $(a, b) \subseteq (d')$, then $(d) \subseteq (d')$.

Thus, $d = \gcd(a, b)$ is a generator for the unique smallest principal ideal containing a and b.

Proposition 1.2. Let R be a commutative ring. If $0 \neq a, b \in R$ such that $(a, b) = (d)$, then $d = \gcd(a, b)$. In particular, d can be written as an R-linear combination of a and b.

Proof. Since $(a, b) \subseteq (d)$, $d \mid a$ and $d \mid b$. Let $d' \mid a$ and $d' \mid b$. Then $(d) = (a, b) \subseteq (d')$. So $d' \mid d$. □

Remark. Note the the condition in previous proposition is not a necessary condition. For example, since in $R = \mathbb{Z}[x]$, $(2, x)$ is maximal not principal, we have $R = (1)$ is the unique principal ideal containing both 2 and x. Thus, $1 = \gcd(2, x)$ up to units.

Proposition 1.3. Let $a, b \in R$. The followings are equivalent.

(a) $\langle a \rangle = \langle b \rangle$.

(b) $a \mid b$ and $b \mid a$.

(c) There exists $u \in R^{\times}$ such that $b = ua$.

In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some $u \in R^{\times}$.

Proof. (a),(b) and (c) follow from R is an integral domain.
Since $d \mid d'$ and $d' \mid d$, $(d) \subseteq (d')$ and $(d') \subseteq (d)$. □

Theorem 1.4. *Let F be a field $\phi : F \to R$ be a ring homomorphism with F field, then $\phi = 0$ or ϕ is 1-1.*

Proof. If ϕ is 1-1, it is trivial. Otherwise, there exist $x, y \in F$ with $x \neq y$ such that $0 = \phi(x) - \phi(y) = \phi(x - y)$. Since $x \neq y$, $0 = \phi(1/(x - y))\phi(x - y) = \phi(1)$. So $\phi(z) = \phi(1_F \cdot z) = z \cdot \phi(1_F) = 0$ for any $z \in F$, i.e., $\phi = 0$. □

1.2 Maximal and Prime Ideals

Definition 1.5. A *maximal ideal* of a ring R is a proper ideal M of R such that there is no proper ideal N of R such that $M \subsetneq M$.

Example 1.6. $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

Theorem 1.7. *Let R be a commutative ring with identity. Then M is a maximal ideal of R if and only if R/M is a field.*

Proof. By the fourth isomorphism theorem for rings,

$$\{\text{ideals of } R/I\} \rightleftarrows \{\text{ideals } J \leqslant R \mid I \subseteq J\}$$
$$J/I \leftarrow\!\shortmid J.$$

So R/I is a field if and only if $\{\text{ideals of } R/I\} = \{0, R/I\}$ if and only if $\{J \leqslant R \mid I \subseteq J\} = \{I, R\}$ if and only if I is maximal. □

Definition 1.8. A proper ideal N of a commutative ring R is a *prime ideal* if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$.

Theorem 1.9. *Let R be a commutative ring with identity and N a proper ideal of R. Then N is a prime ideal of R if and only if R/N is an integral domain.*

Proof. Note that $N \leqslant R$ is prime if and only if $ab \notin N$ for any $a, b \in R \smallsetminus N$ if and only if $(a+N)(b+N) \neq N$ for any $a+N, b+N \neq N$ in R/N if and only if R/N is an integral domain. □

Example 1.10. (a) $\{0\}$ is a prime ideal in $\mathbb{Z}$ since $\mathbb{Z}/\{0\} \cong \mathbb{Z}$.

(b) $\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ since $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\}) \cong \mathbb{Z}$.

Corollary 1.11. Every maximal ideal in a commutative ring R with ideal is a prime ideal.

Proof. If M is a maximal ideal in R, then R/M is a field, hence an integral domain, and therefore M is a prime ideal. □

Theorem 1.12. *If R is a ring with unity 1, then the map*

$$\begin{aligned}\phi : \mathbb{Z} &\longrightarrow R\\ n &\mapsto n \cdot 1\end{aligned}$$

is a ring homomorphism.

Corollary 1.13. If R a ring with unity and $\text{char}(R) = n > 1$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If R has characteristic 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Theorem 1.14. *A field F is either of prime characteristic p and contain a subfield isomorphic to Z_p or of characteristic 0 and contains a subfield isomorphic to $\mathbb{Q}$.*

Definition 1.15. Let F be a field. A *prime subfield* K_F of F is the subfield of F generated by 1_F: If $\text{char}(F) = 0$, then

$$K_F = \left\{ \frac{m \cdot 1_F}{n \cdot 1_F} \;\middle|\; m, n \in \mathbb{Z} \text{ and } n \neq 0 \right\} \cong \mathbb{Q}.$$

If $\text{char}(F) = p$ is prime, then

$$K_F = \{m \cdot 1_F \mid m \in Z_p\} \cong \mathbb{F}_p.$$

1.3 P.I.D.

Definition 1.16. Let R be a commutative ring with identity. An ideal N of R is a *principal ideal (P.I.D.)* if $N = \langle a \rangle$ for some $a \in R$.

Definition 1.17. A *Principal Ideal Domain* (P.I.D.) is an integral domain in which every ideal is principal.

Proposition 1.18. Let R be a P.I.D.. Let $0 \neq a, b \in R$. Then $(a, b) = (d)$, where $d = \gcd(a, b)$ and d is unique up to units. In particular, d can be written as an R-linear combination of a and b.

Proposition 1.19. Every nonzero prime ideal in a P.I.D. is a maximal ideal.

Proof. Let $0 \neq (p) \leqslant R$ be prime and $m \in R$ such that $(p) \subseteq (m)$. Then $p = rm$ for some $r \in R$, i.e., $(p) = (rm)$. Since (p) is prime and $rm \in (p)$, $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $(p) = (m)$. If $r \in (p)$, then $r = ps$ for some $s \in R$ and so $p = rm = psm$; since $p \neq 0$ and R is an integral domain, $sm = 1$, i.e., $m \in R^\times$, thus, $(m) = R$. □

Corollary 1.20. If R is any commuative ring such that $R[x]$ is a PID, then R is a field.

Proof. Since $R[x]$ is an integral domain, R is also an integral domain. Also, since $R[x]/(x) \cong R$, $(x) \leqslant R[x]$ is a nonzero prime ideal. Thus, $0 \neq (x)$ is maximal ideal. □

Theorem 1.21. *If F is a field, then $F[x]$ is a P.I.D..*

Definition 1.22. Let R be a ring.

(a) Let $r \in R \setminus \{R^\times \cup 0\}$. Then r is called *irreducible* in R if whenever $r = ab$ with $a, b \in R$, $a \in R^\times$ or $b \in R^\times$. Otherwise, r is said to be *reducible.*

(b) $0 \neq p \in R$ is called a *prime* in R if $(p) \leqslant R$ is prime. In other words, p is a prime if $p \in R \setminus \{R^\times \cup 0\}$ and whenever $p \mid ab$ for any $a, b \in R$, either $p \mid a$ or $p \mid b$.

Proposition 1.23. In an integer domain R, $p \in R$ prime is always irreducible.

Proof. Since p is prime, $(p) \neq 0$. Let $p = ab$. Then $ab = p \in (p)$. Then $a \in (p)$ or $b \in (p)$. Without loss of generality, assume $a \in (p)$. Then $a = pr$ for some $r \in R$. So $p = ab = prb$. Since $p \neq 0$ and R is an integral domain, $rb = 1$, i.e., $b \in R^\times$. Thus, p is irreducible. ☐

Proposition 1.24. In a P.I.D. R, $p \in R$ is a prime if and only if it is irreducible.

Proof. Let p be irreducible. Assume $(p) \subseteq (m)$ for some $m \in M$. Then $p = rm$ for some $r \in R$. Since p is irreducible, $r \in R^\times$ or $m \in R^\times$, i.e., $(p) = (m)$ or $(m) = 1$. So (p) is a maximal ideal and hence a prime ideal. ☐

Corollary 1.25. In a P.I.D. R, an ideal $\langle p \rangle$ of R is maximal if and only if p is irreducible.

1.4 Euclidean Domain

Definition 1.26. Any function $N : R \to \mathbb{Z}_{\geqslant 0}$ with $N(0) = 0$ is called a *norm* on R. If $N(a) > 0$ for $a \neq 0$, N is called a *positive norm.*

Definition 1.27. R is said to be a *Euclidean Domain* (or *posses a Division Algorithm*) if there is a norm N on R such that for $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with $r = 0$ or $N(r) < N(b)$ such that $a = qb + r$, where q is called the *quotient* and r is called the *remainder.*

Example 1.28. (a) $\mathbb{Z}$ is a Euclidean Domain with norm given by $N(a) = |a|$, the usual absolute value. The existence of a Division Algorithm in $\mathbb{Z}$ (the familiar "long division" of elementary arithmetic) is verified as follows. Let $a, b \in \mathbb{Z} \setminus \{0\}$. Suppose first that $b > 0$. The half open intervals $[nb, (n+1)b), n \in \mathbb{Z}$ partition the real line and so $a \in [kb, (k+1)b)$ for some $k \in \mathbb{Z}$. Let $q = k$, then $a - qb =: r \in [0, b)$ and so $N(r) < N(b)$. If $b < 0$, then there exists $q \in \mathbb{Z}$ such that $a = q(-b) + r$ with $r < 0$ and $|r| \in [0, |b|)$ and so $a = (-q)b + r$ satisfies the requirement of the Division Algorithm for a and b.

Moreover, note if $b \nmid a$, there are always two possibilities for the pair q, r. For example for $b > 0$ and q, r are as above with $r > 0$, then $a = q'b + r'$ with $q' = q + 1$ and $r' = r - b$ also satisfy the conditions of the Division Algorithm applied to a, b. Thus, $5 = 2 \cdot 2 + 1 = 3 \cdot 2 - 1$ are the two ways of applying the division Algorithm in $\mathbb{Z}$ to $a = 5$ and $b = 2$. The quotient and remainder are unique if we require the remainder to be nonnegative.

(b) If F is a field, then $F[x]$ is a Euclidean Domain with $N(p) = \deg(p)$ for $0 \neq p \in F[x]$. In order for a polynomial ring to be a Euclidean Domain, the coefficients must come from a field since the division algorithm ultimately rests on being able to divide arbitrary nonzero coefficients. For example, in $\mathbb{Z}[x]$, $x = q \cdot 2 + r$ for $\deg(q) > 0$, then $r = 0$, $q = x/2 \notin \mathbb{Z}[x]$.

Proposition 1.29. Every ideal in a Euclidean Domain is principal. More precisely, if I is any nonzero ideal in the Euclidean Domain R, then $I = (d)$, where d is any nonzero element of I of minimum norm.

Proof. If $I = 0$, it is trivial. Assume now $I \neq 0$. Let $d = \arg\min\{N(a) \mid 0 \neq a \in I\}$, d is well-defined by the Well ordering of $(\mathbb{Z}^+, \leqslant)$ and d exists since $I \neq 0$. Then $(d) \subseteq I$. Let $a \in I$. Since $f \neq 0$, by Division Algorithm to write $a = qd + r$ with $r = 0$ or $N(r) < N(d)$. Then $r = a - qd \in I$. By the minimality of d, we have $r = 0$, i.e., $a = qd \in (d)$. So $I = (d)$. □

Example 1.30. Since $(2, x) \leqslant \mathbb{Z}[x]$ is not principal (but maximal), $\mathbb{Z}[x]$ is not a Euclidean Domain.

Theorem 1.31. *Let R be a Euclidean domain and $0 \neq a, b \in R$. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b. Then*

(a) $d = \gcd(a, b)$,

(b) $(d) = (a, b)$.

Proof. Since R is a PID, $(a, b) = (d)$ for some $d \in R$, by previous proposition, $d = \gcd(a, b)$.
Sicne $r_{n-1} = q_{n+1} r_n$, $r_n \mid r_{n-1}$. Clearly, $r_n \mid r_n$. By induction from index n downwards to index 0, assume $r_n \mid r_{k+1}$ and $r_n \mid r_k$ for some $0 \leqslant k \leqslant r - 1$. Since $r_{k-1} = q_{k+1} r_k + r_{k+1}$, we have $r_k \mid r_{k-1}$. So $r_n \mid b$ and $r_n \mid a$. Hence $(a, b) \subseteq (d)$. Note $r_0 = a - q_0 b \in (a, b)$ and $r_1 = b - q_1 r_0 \in (b, r_0) \subseteq (a, b)$. By induction, $d = r_n \in (a, b)$. □

1.5 Factorization of Polynomials over a Field

Theorem 1.32 (Division algorithm for polynomial rings)**.** *Let $f, g \in F[x]$. Then there are unique polynomials $q, r \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) = 0$ or $\deg(r) < \deg(g)$.*

Theorem 1.33 (Factor Theorem)**.** *An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.*

Proof. $\Longrightarrow$ Suppose that for $a \in F$ we have $f(a) = 0$. By the division algorithm, there exist $q, r \in F[x]$ such that

$$f(x) = (x - a)q(x) + r(x),$$

where either $r(x) = 0$ or $\deg(r) < 1$. Then we must have $r(x) = c$ for some $c \in F$, and so

$$f(x) = (x - a)q(x) + c.$$

Since $f(a) = 0$, we have that $c = 0$. Then $f(x) = (x - a)q(x)$, so $x - a$ is a factor of $f(x)$.
$\Longleftarrow$ If $x - a$ is a factor of $f(x)$ in $F[x]$, then $f(x) = (x - a)q(x)$ for some $q \in F[x]$, thus $f(a) = 0$. □

Corollary 1.34. A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F.

Proof. The factor theorem shows that if $a_1 \in F$ is a zero of $f(x)$, then

$$f(x) = (x - a_1)q_1(x),$$

where $\deg(q_1) = n - 1$. A zero $a_2 \in F$ of $q_1(x)$ then results in a factorization

$$f(x) = (x - a_1)(x - a_2)q_1(x).$$

Continuing this process, we arrive at

$$f(x) = (x - a_1) \cdots (x - a_r) q_r(x),$$

where q_r has no further zeros in F. Since $\deg(f) = n$, at most n factors $(x - a_i)$ can appear on the right-hand side of the preceding equation, so $r \leqslant n$. Also, if $b \in F$ and $b \neq a_i$ for $i = 1, \ldots, r$, then

$$f(b) = (b - a_1) \cdots (b - a_r) q_r(b) \neq 0,$$

since F has no divisors of 0 and none of $b - a_i$ or $q_r(b)$ are 0 by construction. Hence $a_1, \ldots, a_r$ are all the zeros in F of $f(x)$. $\square$

Corollary 1.35. Let F be a finite field. Then the group $\langle F^\times, \cdot \rangle$ is cyclic.

Proof. Since $F^\times$ is finite and abelian, $G \cong Z_{d_1} \times \cdots \times Z_{d_n}$ for some $n \in \mathbb{N}$ and d_i is a power of a prime. Let $m := \operatorname{lcm}(d_1, \ldots, d_n) \leqslant d_1 \cdots d_n$. Then $\alpha^m = 1$ for all $\alpha \in F^\times$, and so every element of G is a zero if $x^m - 1$. But $|F^\times| = d_1 \times \cdots \times d_r$ while $x^m - 1$ can have at most m zeros in the field F, so $m \geqslant d_1 \cdots d_r$. Hence $m = d_1 \cdots d_r$, so the primes involved in the prime powers $d_1, \ldots, d_r$ are distinct, and the group $G \cong Z_m$. $\square$

Definition 1.36. A polynomial $f \in F[x] \setminus F$ is *irreducible over F* or is an *irreducible polynomial in $F[x]$* if whenever $f = gh$ with $g, h \in F[x]$, $g \in F$ or $h \in F$. Otherwise $f(x)$ is *reducible over F*.

Remark. The units in $F[x]$ are $(F[x])^\times = F^\times = F \setminus \{0\}$.

Theorem 1.37. *Let $f \in F[x]$ and $\deg(f) = 2$ or 3. Then $f(x)$ is reducible over F if and only if it has a zero in F.*

Proof. $\Longrightarrow$ If $f(x)$ is reducible so that $f(x) = g(x)h(x)$, where $\deg(g), \deg(h) < \deg(f)$, then since $\deg(f) \leqslant 3$, either $\deg(g) = 1$ or $\deg(h) = 1$. If, say, $\deg(g) = 1$, then except for a possible factor in F, g is of the form $x - a$. Then $f(a) = g(a)h(a) = 0$, so $f(x)$ has a zero in F.

$\Longleftarrow$ The factor theorem shows that if $f(a) = 0$ for $a \in F$, then $x - a$ is a factor of $f(x)$, so $f(x)$ is reducible. $\square$

Theorem 1.38. *If $f \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$.*

Corollary 1.39. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is in $\mathbb{Z}[x]$ with $a_0 \neq 0$, and if $f(x)$ has a zero in $\mathbb{Q}$, then it has a zero m in $\mathbb{Z}$, and $m \mid a_0$.

Proof. If $f(x)$ has a zero a in $\mathbb{Q}$, then $f(x)$ has a linear factor $x - a$ in $\mathbb{Q}[x]$. But then by Theorem 1.38, $f(x)$ has a factorization with a linear factor in $\mathbb{Z}[x]$, so for some $m \in \mathbb{Z}$ we must have

$$f(x) = (x - m)(x^{n-1} + \cdots + a_0/m)$$

Thus $a_0/m \in \mathbb{Z}$, so $m \mid a_0$. $\square$

Theorem 1.40 (Eisenstein Criterion)**.** *Let $p \in \mathbb{Z}$ be prime. Suppose that $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and $a_0 \not\equiv 0 \pmod{p}$ but $a_i \equiv 0 \pmod{p}$ for all $i < n$, with $a_0 \not\equiv 0 \pmod{p^2}$. Then $f(x)$ is irreducible over $\mathbb{Q}$*

1.6 Introduction to Extension Fields

Notation 1.41. Let E be a field. We use $F \leqslant E$ to denote that F is a subfield of E.

Definition 1.42. A field E is an *extension field* of a field F if $F \leqslant E$.

Theorem 1.43 (Kronecker's Theorem)**.** *Let F be a field and $f \in F[x]$ with $d := \deg(f) > 0$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Proof. Let $K := F[x]/\langle f \rangle$. Without loss of generality, assume that f is irreducible. Since $F[x]$ is a P.I.D., f is prime in $F[x]$. Since $\deg(f) > 0$ and $F[x]$ is P.I.D., $0 \neq \langle f \rangle \leqslant F[x]$ is maximal and so K is a field. The canonical projection $\pi : F[x] \to K$ restricted to F gives a homomorphism $\varphi = \pi|_F : F \to K$. Since F is a field and $\varphi(1) = \bar{1}$, φ is 1-1 and then $F \cong \varphi(F)$. We identify F with its isomorphic image in K and view F as a subfield of K. (Idenftiying $a \in F$ with $a + \langle f \rangle$ in K.) Let $f = \sum_{i=0}^{d-1} a_i x^i$ with $a_0, \ldots, a_{d-1} \in F$ and $\theta := x + \langle f \rangle \in K$, then

$$\begin{aligned} f(\theta) &= \sum_{i=0}^{d} a_i \theta^i = \sum_{i=0}^{d} a_i (x + \langle f \rangle)^i = \sum_{i=0}^{d} (a_i + \langle f \rangle)(x + \langle f \rangle)^i \\ &= \left(\sum_{i=0}^{d} a_i x^i \right) + \langle f \rangle = f + \langle f \rangle = \langle f \rangle = 0. \end{aligned}$$

□

Example 1.44. Let $F = \mathbb{R}$ and $f(x) = x^2 + 1$, which is irreducible over $\mathbb{R}$. Then $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a field. Identifying $r \in \mathbb{R}$ with $r + \langle x^2 + 1 \rangle$ in $\mathbb{R}[x]/\langle x^2 + 1 \rangle$, we can view $\mathbb{R}$ as a subfield of $E = \mathbb{R}[x]/\langle x^2 + 1 \rangle$. Let $\alpha = x + \langle x^2 + 1 \rangle$. Computing in $\mathbb{R}[x]/\langle x^2 + 1 \rangle$, we find

$$\alpha^2 + 1 = (x + \langle x^2 + 1 \rangle)^2 + (1 + \langle x^2 + 1 \rangle) = (x^2 + \langle x^2 + 1 \rangle) + (1 + \langle x^2 + 1 \rangle) = (x^2 + 1) + \langle x^2 + 1 \rangle = 0.$$

Thus, α is a zero of $x^2 + 1$.

Example 1.45. Let $F = \mathbb{Q}$, and consider $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$, where $x^2 - 2$ and $x^2 - 3$ are both irreducible over $\mathbb{Q}$. We can start with $x^2 - 2$ and construct an extension field E of $\mathbb{Q}$ containing α such that $\alpha^2 - 2 = 0$, or we can start with $x^2 - 3$ and construct an extension field E of $\mathbb{Q}$ containing β such that $\beta^2 - 3 = 0$.

Definition 1.46. An element α of an extension field E of a field is *algebraic over* F if $f(\alpha) = 0$ for some nonzero $f(x) \in F[x]$. If α is not algebraic over F, then α is *transcendental* over F.

Example 1.47. We have that $\mathbb{Q} \leqslant \mathbb{R}$.

(a) $\sqrt{2}$ is an algebraic element over $\mathbb{Q}$ since $\sqrt{2}$ is a zero of $x^2 - 2$. Also, i is an algebraic element over $\mathbb{Q}$, being a zero of $x^2 + 1$.

(b) It is well known that π and e are transcendental over $\mathbb{Q}$.

Example 1.48. We have that $\mathbb{R} \leqslant \mathbb{C}$. π is algebraic over $\mathbb{R}$, for it is a zero of $(x - \pi) \in \mathbb{R}[x]$.

Example 1.49. $\sqrt{1 + \sqrt{3}}$ is algebraic over $\mathbb{Q}$. For $\alpha^2 = 1 + \sqrt{3}$, then $\alpha^2 - 1 = \sqrt{3}$ and $(\alpha^2 - 1)^2 = 3$. Therefore, $\alpha^4 - 2\alpha^2 - 2 = 0$, so α is a zero of $x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$.

To connect these ideas with those of number theory, we give the following definition.

Definition 1.50. An element of $\mathbb{C}$ is algebraic over $\mathbb{Q}$ is an *algebraic number*. A *transcendental* number is an element of $\mathbb{C}$ that is transcendental over $\mathbb{Q}$.

Theorem 1.51. *Let $E \supseteq F$ be a field extension and $\alpha \in E$. Let $\phi_\alpha : F[x] \to E$ be the evaluation of $F[x]$ into E. Then ϕ_α is a ring homomorphism such that $\phi_\alpha(a) = a$ for $a \in F$ and $\phi_\alpha(x) = \alpha$. Then α is transcendental over F if and only if ϕ_α is 1-1.*

Proof. α is transcendental over F if and only if $f(\alpha) \neq 0$ for all nonzero $f(x) \in F[x]$, if and only if $\phi_\alpha(f(x)) \neq 0$ for all nonzero $f(x) \in F[x]$ if and only if

$$\mathrm{Ker}(\phi_\alpha) = \{g \in F[x] \mid \phi_\alpha(g) = 0\} = \{g \in F[x] \mid g(\alpha) = 0\} = \{0\},$$

if and only if ϕ_α is 1-1. □

Theorem 1.52. *Let $E \supseteq F$ be a field extension and $\alpha \in E$ algebraic over F. Then*

(a) There exists a unique monic irreducible $m_\alpha \in F[x]$ such that $m_\alpha(\alpha) = 0$.

(b) Let $f \in F[x]$, then $f(\alpha) = 0$ if and only if $m_\alpha \mid f$.

Proof. (a) Let m_α be monic with minimal degree such that $m_\alpha(\alpha) = 0$. We claim that m_α is irreducible. Suppose $m_\alpha = g \cdot h$ and $g, h \in F[x]$ have smaller degree. Then $0 = m_\alpha(\alpha) = g(\alpha)h(\alpha)$. Since F is a field, $g(\alpha) = 0$ or $h(\alpha) = 0$, contradicting the minimality of the degree of m_α. The uniqueness follows from (b).

(b) $\Longrightarrow$ Let $g \in F[x]$ such that $g(\alpha) = 0$. By the Euclidean Algorithm in the Euclidean domain $F[x]$, there exist $q, r \in F[x]$ such that $g = qm_\alpha + r$ with $\deg(r) < \deg(m_\alpha(x))$. Then $g(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) \in E$. Since $m_\alpha(\alpha) = 0 = g(\alpha)$, we have $r(\alpha) = 0$. Then by the minimality of $m_\alpha(x)$, $r = 0$. Hence m_α divides any polynomial g in $F[x]$ having α as a root.

$\Longleftarrow$ is straightforward. □

Definition 1.53. Let $E \subseteq F$ be a field extension and $\alpha \in E$ algebraic over F. The unique monic polynomial m_α having the property described in Theorem 1.52 is the *irreducible polynomial for α over F* and will be denoted by $\mathrm{irr}(\alpha, F)$. The degree of $\mathrm{irr}(\alpha, F)$ is the *degree of α over F*, denoted by $\deg(\alpha, F)$.

Example 1.54. (a) $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$.

(b) $\mathrm{irr}(\sqrt{1+\sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2$.

(c) $\mathrm{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$.

Discussion 1.55. Le and $\alpha \in E$. Let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism of $F[x]$ into E.

Case I Suppose that α is algebraic over F. Then

$$\mathrm{Ker}(\phi_\alpha) = \{g \in F[x] \mid \phi_\alpha(g) = 0\} = \{g \in F[x] \mid g(\alpha) = 0\} = \{g \in F[x] : \mathrm{irr}(\alpha, F) \mid g\} = \langle \mathrm{irr}(\alpha, F)\rangle$$

where the last to the second equality follows from Theorem 1.52(b). By Corollary 1.25, $\langle \mathrm{irr}(\alpha, F)\rangle$ is a maximal ideal of $F[x]$. Therefore, $F[x]/\langle \mathrm{irr}(\alpha, F)\rangle$ is a field and

$$\begin{aligned} F[x]/\langle \mathrm{irr}(\alpha, F)\rangle &\xrightarrow{\cong} \phi_\alpha(F[x]) \\ f(x) + \langle \mathrm{irr}(\alpha, F)\rangle &\longmapsto f(\alpha) \\ \sum_{i=1}^{n} c_i(x + \langle \mathrm{irr}(\alpha, F)\rangle)^i &\longmapsto \sum_{i=1}^{n} c_i\alpha^i \end{aligned}$$

by the first isomorphism theorem. This subfield $\phi_\alpha(F[x])$ of E is then the smallest subfield of E containing F and α. We will denote this field by $F(\alpha)$.

Case II Suppose that α is transcendental over F. Then by Theorem 1.51 $\phi_\alpha(F[x])$ is an integral domain but not a field. We will denote this domain by $F[\alpha]$. E contains a field of quotients of $F[\alpha]$, which is thus the smallest subfield of E containing F and α. As in Case I, we denote this field by $F(\alpha)$.

Example 1.56. Since π is transcendental over $\mathbb{Q}$, the field $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$. Thus from a structural viewpoint, an element that is transcendental over a field F behaves as though it were an indeterminate over F.

Definition 1.57. An extension field E of a field F is a *simple extension* of F if $E = F(\alpha)$ for some $\alpha \in E$.

Theorem 1.58. *Let E be a simple extension of $F(\alpha)$ of a field F and α algebraic over F. Let $n := \deg(\alpha, F) \geqslant 1$. Then $F(\alpha)$ is an n-dimensional F-vector space with a basis $\{1, \alpha, \dots, \alpha^{n-1}\}$.*

Proof. It suffices to show that $\beta \in E = F(\alpha)$ can be uniquely expressed in the form

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

where the b_i's are in F. For the usual evaluation homomorphism ϕ_α, every element of $F(\alpha) = \phi_\alpha(F(x))$ is of the form $\phi_\alpha(f(x)) = f(\alpha)$, a formal polynomial in α with coefficients in F. Let

$$p(x) := \mathrm{irr}(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Then $p(\alpha) = 0$, so

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

This equation in $F(\alpha)$ can be used to express every monomial α^m for $m \geqslant n$ in terms of powers of α that are less than n. Thus, if $\beta \in F(\alpha)$, $\beta = h(\alpha)$ for some $h \in F[x]$, and so β can be expressed in the required form

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$

For uniqueness, if

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = b_0' + b_1'\alpha + \cdots + b_{n-1}'\alpha^{n-1}$$

for $b_i' \in F$, then

$$(b_0 - b_0') + (b_1 - b_1')x + \cdots + (b_{n-1} - b_{n-1}')x^{n-1} =: g(x) \in F(x),$$

and $g(\alpha) = 0$. Then $\mathrm{irr}(\alpha, F) \mid g$. By the degree argument, we have that $g = 0$. Therefore, $b_i = b_i'$. ∎

Remark.

$$F(\alpha) = \phi_\alpha(F[x]) = \{f(\alpha) \mid f \in F[x]\} = \{f(\alpha) \mid f \in F[x] \text{ and } \deg(f) \leqslant n-1\}.$$

Example 1.59. The polynomial $p(x) = x^2 + x + 1$ in $Z_2[x]$ is irreducible over Z_2, since neither 0 nor 1 of Z_2 is a zero of $p(x)$. Then there is an extension field E of Z_2 containing a zero α of $x^2 + x + 1$. By Theorem 1.58, $Z_2(\alpha)$ has as elements $0 + 0\alpha$, $1 + 0\alpha$, $0 + 1\alpha$, and $1 + 1\alpha$, that is, 0, 1, α, and $1 + \alpha$. This gives us a new finite field, of four elements. To compute $(1 + \alpha)(1 + \alpha)$ in $Z_2(\alpha)$, we observe that since $p(\alpha) = \alpha^2 + \alpha + 1 = 0$, then $\alpha^2 = -\alpha - 1 = \alpha + 1$. Therefore,

$$(1 + \alpha)(1 + \alpha) = 1 + \alpha + \alpha + \alpha^2 = 1 + \alpha^2 = 1 + \alpha + 1 = \alpha.$$

Example 1.60. We saw in Example 1.44 that we can view $\mathbb{R}[x]/\langle x^2 + 1\rangle$ as an extension field of $\mathbb{R}$. Let

$$\alpha = x + \langle x^2 + 1\rangle.$$

Since $\operatorname{irr}(\alpha, F) = x^2 + 1$, we have that $\mathbb{R}(\alpha) = \phi_\alpha(F[x]) \cong \mathbb{R}[x]/\langle x^2 + 1\rangle$ by Discussion 1.55 Case I. By Theorem 1.58, $\mathbb{R}(\alpha)$ consists of all elements of the form $a + b\alpha$ for $a, b \in \mathbb{R}$. But since $\alpha^2 + 1 = 0$, we see that α plays the role of $i \in \mathbb{C}$, and $a + b\alpha$ plays the role of $(a + bi) \in \mathbb{C}$. Thus, $\mathbb{R}(\alpha) \cong \mathbb{C}$.

Theorem 1.61. *Let $F \subseteq F$ and $\alpha \in E$ algebraic over F. Then every element β of $F(\alpha)$ is algebraic over F, and $\deg(\beta, F) \leqslant \deg(\alpha, F)$.*

Proof. Let $n := \deg(\alpha, F)$. Consider the elements

$$1, \beta, \beta^2, \ldots, \beta^n.$$

Since $F(\alpha)$ is an n-dimensional F-vector space, the elements are linearly dependent over F. So there exists $b_i \in F$ not all 0 such that

$$b_0 + b_1\beta + b_2\beta^2 + \cdots + b_n\beta^n = 0.$$

Hence $f(x) := b_n x^n + \cdots + b_1 x + b_0$ is a nonzero element of $F[x]$ such that $f(\beta) = 0$. Therefore, β is algebraic over F and $\deg(\beta, F) \leqslant n$. ☐

1.7 Algebraic Extensions

Fact 1.62. Let $E \supseteq F$ be a field extension, then the multiplication defined in E makes E into a vector space over F. For example, the scalar product $c \cdot v$ with $c \in F$ and $v \in E$ is the usual multiplication in E.

Definition 1.63. The *degree* (or *index*) of a field extension $E \supseteq F$, denoted $[E : F]$, is the dimension of E as a vector space over F. The extension is said to be *finite* if $[K : F]$ is finite and is said to be *infinite* otherwise.

Remark. $[E : F] = 1$ if and only if $E = F$ if and only if $E = F(1)$ because $\deg(1, F) = \deg(x-1) = 1$.

Remark. Let E be a simple extension of $F(\alpha)$ of a field F and α algebraic over F. Then

$$[F[\alpha] : F] = \deg(\alpha, F).$$

Definition 1.64. An extension field E of a field F is an *algebraic extension of* F if every element in E is algebraic over F.

Theorem 1.65. *A finite extension field E of a field F is an algebraic extension of F.*

Proof. Let $\alpha \in E$. Assume that $[E : F] = n$. Then $1, \alpha, \dots, \alpha^n$ are linearly dependent, and so there exists $a_i \in F$ not all 0 such that

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0.$$

Then $0 \neq f(x) = a_nx^n + \cdots + a_1x + a_0 \in F[x]$ and $f(\alpha) = 0$. Therefore, α is algebraic over F. □

Theorem 1.66 (Tower law)**.** *Let $K \supseteq E \supseteq F$ be field extensions. Then $[K : F] = [K : E][E : F]$. In particular, $[K : F] < \infty$ if and only if $[K : E] < \infty$ and $[E : F] < \infty$.*

Proof. (a) Assume $[K : E] =: m < \infty$ and $[K : F] =: n < \infty$. Let $\{\alpha_1, \dots, \alpha_m\}$ be basis for K/E and $\{\beta_1, \dots, \beta_n\}$ be basis for E/F. We claim that $\{\alpha_i\beta_j \mid i = 1, \dots, m,\ j = 1, \dots, n\}$ is a basis of K/F. Let $\gamma \in K$. Then there exists $a_1, \dots, a_m \in E$ such that $\gamma = \sum_{i=1}^m a_i\alpha_i$. For $i = 1, \dots, m$, there exists $b_{i,1}, \dots, b_{i,n} \in F$ such that $a_i = \sum_{j=1}^n b_{i,j}\beta_j$. Hence $\gamma = \sum_{i=1}^m \sum_{j=1}^n b_{ij}\alpha_i\beta_j$. Thus, $\{\alpha_i\beta_j \mid i = 1, \dots, m,\ j = 1, \dots, n\}$ spans K as a vector space over F.

Suppose $\gamma = \sum_{i=1}^m \sum_{j=1}^n c_{i,j}\alpha_i\beta_j = 0$ with $c_{i,j} \in F$. For $i = 1, \dots, m$, set $d_i = \sum_{j=1}^n c_{i,j}\beta_j \in E$. Then $\sum_{i=1}^m d_i\alpha_i = 0$. For $i = 1, \dots, m$, since $\{\alpha_1, \dots, \alpha_m\}$ is a basis for K over E, we have that $d_i = 0$, so $\sum_{j=1}^n c_{i,j}\beta_j = 0$, and thus $c_{i,j} = 0$ for $j = 1, \dots, n$ since $\{\beta_1, \dots, \beta_n\}$ is a basis for E over F. Therefore, it is a basis and has size mn.

(b) Assume $[K : E] = \infty$. Then there exist $\alpha_1, \alpha_2, \dots \in K$ such that they are linearly independent over E. So $\alpha_1, \alpha_2, \cdots$ are linearly independent over F and then $[K : F] = \infty$.

(c) Assume $[E : F] = \infty$. Then there exist $\alpha_1, \alpha_2, \dots \in E \subseteq K$ such that they are linearly independent over F and so $[K : F] = \infty$.

(d) If $[K : F] = \infty$, then $[K : E] = \infty$ or $[E : F] = \infty$ by Case (a). □

Corollary 1.67. If F_i is a field for $i = 1, \dots, r$ and F_{i+1} is an extension of F_i, then

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

Corollary 1.68. If $[E : F] < \infty$ and $\alpha \in E$, then $\deg(\alpha, F) \mid [E : F]$.

Proof. By Theorem 1.58, $\deg(\alpha, F) = [F(\alpha) : F]$. Then it follows from $[E : F] = [E : F(\alpha)][F(\alpha) : F] = [E : F(\alpha)] \deg(\alpha, F)$. □

Corollary 1.69. If E is an extension field of F, $\alpha \in E$ is algebraic over F, and $\beta \in F(\alpha)$, then $\deg(\beta, F) \mid \deg(\alpha, F)$.

Proof. By Theorem 1.58, $\deg(\alpha, F) = [F(\alpha) : F]$ and $\deg(\beta, F) = [F(\beta) : F]$. Since $F \subseteq F(\beta) \subseteq F(\alpha)$, we have that $[F(\beta) : F] \mid [F(\alpha) : F]$ by Theorem 1.66. □

Example 1.70. Suppose there is an element β of $\mathbb{Q}(\sqrt{2})$ that is a zero β of $x^3 - 2$. Then $\deg(\beta, \mathbb{Q}) \mid \deg(\sqrt{2}, \mathbb{Q})$. Since $\operatorname{irr}(\beta, \mathbb{Q}) = x^3 - 2$ and $\operatorname{irr}(\alpha, \mathbb{Q}) = x^2 - 2$, we have that $\deg(\beta, \mathbb{Q}) = 3$ and $\deg(\alpha, \mathbb{Q}) = 2$, contradicting $\deg(\beta, \mathbb{Q}) \mid \deg(\sqrt{2}, \mathbb{Q})$.

Remark. Let $E \supseteq F$ be a field extension and $\alpha_1, \alpha_2 \in E$, not necessarily algebraic over F. We consider the case that α_1 and α_2 are algebraic over F. By definition,

$$\begin{aligned} F(\alpha_1) &= \{f(\alpha_1) \mid f \in F[x]\} \\ &= \{f(\alpha_1) \mid f \in F[x] \text{ and } \deg(f) \leqslant \deg(\alpha_1, F) - 1\} \end{aligned}$$

is the smallest subfield of E that contains F and α_1. Note that

$$\begin{aligned} F(\alpha_1)(\alpha_2) &= \{g(\alpha_2) \mid g \in F(\alpha_1)[y]\} \\ &= \{f(\alpha_1, \alpha_2) \mid f \in F[x, y]\} \\ &= \{g(\alpha_1) \mid g \in F(\alpha_2)[x]\} \\ &= F(\alpha_2)(\alpha_1). \end{aligned}$$

We denote this field by $F(\alpha_1, \alpha_2)$, which can be characterized as the smallest subfield of E containing F, α_1 and α_2. Similarly, for $\alpha_i \in E$, $F(\alpha_1, \dots, \alpha_n)$ is the smallest extension field of F in E containing all the α_i for $i = 1, \dots, n$. We claim that

$$F(\alpha, \dots, \alpha_n) = \bigcap \{G \mid F \subseteq G \subseteq E \text{ are field extensions and } \alpha_i \in G, \forall i = 1, \dots, n\}.$$

Proof. $\subseteq$ Let G be a field such that $F \subseteq G \subseteq E$ and $\alpha_i \in G$ for $i = 1, \dots, n$. Since $F(\alpha, \dots, \alpha_n)$ is the smallest subfield of E containing F and all the α_i for $i = 1, \dots, n$, we have that $F(\alpha, \dots, \alpha_n) \subseteq G$.

$\supseteq$ follows from that $F(\alpha_1, \dots, \alpha_n)$ is in the intersection since $F \subseteq F(\alpha, \dots, \alpha_n) \subseteq E$ are field extensions and $\alpha_i \in G$ for $i = 1, \dots, n$. $\square$

Example 1.71. Consider $\mathbb{Q}(\sqrt{2})$. Then $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Note that $\operatorname{irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1$, then $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, and so $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Consequently, $\deg(\sqrt{3}, \mathbb{Q}(\sqrt{2})) \geqslant 2$, so $\operatorname{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3$, and thus $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. The proof of Theorem 1.66 shows that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

Example 1.72. Consider $\mathbb{Q}(2^{1/3})$. Then $\{1, 2^{1/3}, 2^{2/3}\}$ is a basis for $\mathbb{Q}(2^{1/3})$ over $\mathbb{Q}$ We have that $2^{1/2} \notin \mathbb{Q}(2^{1/3})$ because $\deg(2^{1/2}, \mathbb{Q}) = 2$ and $2 \nmid 3 = \deg(2^{1/3}, \mathbb{Q})$. Hence $\operatorname{irr}(2^{1/2}, \mathbb{Q}(2^{1/3})) = x^2 - 2$, and so $\{1, 2^{1/2}\}$ is a basis for $\mathbb{Q}(2^{1/3})(2^{1/2}) = \mathbb{Q}(2^{1/2}, 2^{1/3})$ over $\mathbb{Q}(2^{1/3})$. The proof of Theorem 1.66 shows that $\{1, 2^{1/3}, 2^{1/2}, 2^{2/3}, 2^{5/6}, 2^{7/6}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

Because $2^{7/6} = 2(2^{1/6})$, we have that $2^{1/6} \in \mathbb{Q}(2^{1/2}, 2^{1/3})$. By Eisenstein's criterion with $p = 2$, $x^6 - 2$ is irreducible over $\mathbb{Q}$. Thus, $\operatorname{irr}(2^{1/6}, \mathbb{Q}) = x^6 - 2$. By the tower law,

$$6 = [\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/6})][\mathbb{Q}(2^{1/16}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/6})]6.$$

Therefore, $[\mathbb{Q}(2^{1/2}, 2^{1/3}) : \mathbb{Q}(2^{1/6})] = 1$, and so $\mathbb{Q}(2^{1/2}, 2^{1/3}) = \mathbb{Q}(2^{1/6})$.

Theorem 1.73. *Let $E \supseteq F$ be an algebraic extension. Then there exists a finite number of elements $\alpha_1, \dots, \alpha_n$ in E such that $E = F(\alpha, \dots, \alpha_n)$ if and only if $[E : F] < \infty$.*

Proof. $\Longrightarrow$ Suppose that $E = F(\alpha_1, \dots, \alpha_n)$. Since E is an algebraic extension of F, each α_i is algebraic over F, so each α_i is algebraic over every extension field of F in E. Thus, $F(\alpha_1)$ is algebraic over F, and in general, $F(\alpha_1, \dots, \alpha_j) = F(\alpha_1, \dots, \alpha_{j-1})(\alpha_j)$ is algebraic over $F(\alpha_1, \dots, \alpha_{j-1})$ for $j = 2, \dots, n$. Hence

$$[F(\alpha_1, \dots, \alpha_{j-1}, \alpha_j) : F(\alpha_1, \dots, \alpha_{j-1})] = \deg(\alpha_j, F(\alpha_1, \dots, \alpha_{j-1})) < \infty, \forall j = 1, \dots, n,$$

where $\alpha_0 := 1$. Therefore, by the tower law and $E = F(\alpha_1, \dots, \alpha_n)$,

$$[E : F] = \prod_{j=1}^{n} [F(\alpha_1, \dots, \alpha_{j-1}, \alpha_j) : F(\alpha_1, \dots, \alpha_{j-1})] < \infty.$$

$\Longleftarrow$ Suppose that $[E : F] < \infty$. If $[E : F] = 1$, then $E = F(1) = F$, and we are done. If $E \neq F$, let $\alpha_1 \in E \smallsetminus F$. Then $[F(\alpha_1) : F] > 1$. If $F(\alpha_1) = E$, we are done; if not, let $\alpha_2 \in E$, where $\alpha_2 \notin F(\alpha_1)$. Continuing this process, we see from the tower law that since $[E : F]$ is finite, we must arrive at α_n such that $F(\alpha_1, \dots, \alpha_n) = E$. $\square$

Theorem 1.74. *Let $E \supseteq F$ be a field extension. Then*

$$\overline{F}_E = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$

is a subfield of E, the algebraic closure of F in E*.*

Proof. Let $\alpha, \beta \in \overline{F}_E$. Then $[F(\alpha) : F] < \infty$ and $[F(\alpha, \beta) : F(\alpha)] < \infty$, and so $[F(\alpha, \beta) : F] < \infty$ by the tower law. Hence $F \subseteq F(\alpha, \beta)$ is an algebraic extension by Theorem 1.65. Since $\alpha, \beta \in E$, $F(\alpha, \beta) \subseteq E$, so $F(\alpha, \beta) \subseteq \overline{F}_E$. Thus, $\overline{F}_E$ contains $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$, and also contains α/β for $\beta \neq 0$, so $\overline{F}_E$ is a subfield of E. $\square$

Corollary 1.75. The set of all algebraic numbers forms a field.

Proof. It follows immediately from Theorem 1.74, because

$$\text{The set of algebraic numbers} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\} = \overline{\mathbb{Q}}_{\mathbb{C}}. \qquad \square$$

Definition 1.76. A field F is *algebraically closed* if every nonconstant polynomial in $F[x]$ has a zero in F.

Remark. Note that it is possible that $F = \overline{F}_E$ for some field extension $E \supseteq F$, without F being algebraically closed. For example, $\mathbb{Q} = \overline{\mathbb{Q}}_{\mathbb{Q}}$, but $\mathbb{Q}$ is not algebraically closed because $x^2 + 1$ has no zero in $\mathbb{Q}$.

Theorem 1.77. *A field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ factors in $F[x]$ into linear factors.*

Proof. $\Longrightarrow$ Let F be algebraically closed and $f(x)$ a nonconstant polynomial in $F[x]$. Then $f(x)$ has a zero $a \in F$. By Theorem 1.33, $x - a$ is a factor of $f(x)$, so $f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$. Then if $g(x)$ is nonconstant, it has a zero $b \in F$, and we have $f(x) = (x-a)(x-b)h(x)$ for some $h(x) \in F[x]$. Continuing, we get a factorization of $f(x)$ in $F[x]$ into linear factors.

$\Longleftarrow$ Suppose that every nonconstant polynomial of $F[x]$ has a factorization into linear factors. If $ax - b$ is a linear factor of $f(x)$, then b/a is a zero of $f(x)$. Thus, F is algebraically closed. $\square$

Corollary 1.78. An algebraically closed field F has no proper algebraic extensions, that is, no algebraic extension E with $F \subsetneq E$.

Proof. Le be an algebraic extension. Let $\alpha \in E$. Since F is algebraically closed, $\operatorname{irr}(\alpha, F) = x - \alpha$ by Theorem 1.77. Thus, $\alpha \in F$, and so $F = E$. $\square$

Definition 1.79. An *algebraic closure* $\overline{F}$ of F is an algebraic field extension $F \subseteq \overline{F}$ such that $\overline{F}$ is algebraic closed.

Proposition 1.80. An algebraic closure $\overline{F}$ of F contains all the algebraic elements over F.

Proof. Let a be algebraic over F, then $f(a) = 0$ for some nonconstant $f \in F[x]$. By Theorem 1.33, $x - a$ is a factor of $f(x)$. But f factors into linear factors in $\overline{F}[x]$ by Theorem 1.77, thus $a \in \overline{F}$. □

Theorem 1.81. *Every field F has an algebraic closure.*

Proof. Refer to the textbook. □

Remark. An algebraic closure of F is unique up to isomorphism.

We will prove later using Galois theory the following result.

Theorem 1.82 (Fundamental Theorem of Algebra)**.** $\mathbb{C}$ *is algebraically closed.*

1.8 Finite Fields

We shall show that for every prime p and positive integer n, there is exactly one finite field (up to isomorphic) of order p^n.

Theorem 1.83. *Let $F \supseteq E$ be a finite extension of $[E : F] = n < \infty$. If $|F| = q$, then $|E| = q^n$.*

Proof. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for E as a vector space over F. Then every $\beta \in E$ can be uniquely written in the form

$$\beta = b_1\alpha_1 + \cdots + b_n\alpha_n$$

for $b_i \in F$. Since each b_i may be any of the q elements of F, the total number of such distinct linear combinations of the α_i is q^n. □

Corollary 1.84. If E is a finite field of characteristic p, then E contains exactly p^n elements for some $n \in \mathbb{N}$.

Proof. Let F be a finite field. Define a function φ by

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow E \\ m &\longmapsto m \cdot 1 \end{aligned}$$

Then φ is a ring homomorphism with $\mathrm{Ker}(\varphi) = m\mathbb{Z}$, where $m = \mathrm{char}(E)$. Then $\mathbb{Z}/m\mathbb{Z} \cong \varphi(\mathbb{Z})$ embeds as a subring of E, and so m has to be a prime number, say p. Viewing E as a vector space over $\mathbb{Z}/p\mathbb{Z}$ and let $n := \dim_{\mathbb{Z}/p\mathbb{Z}}(E)$. By theorem 1.83, $|E| = p^n$. □

Theorem 1.85. *Let E be a field of $|E| = p^n$ (p prime and $n \in \mathbb{N}$) contained in an algebraic closure $\overline{Z}_p$ of Z_p. Then the elements of E are precisely the zeros in $\overline{Z}_p$ of the polynomial $x^{p^n} - x$ in $Z_p[x]$.*

Proof. The set $E^\times$ of nonzero elements of E forms a multiplicative group of order $p^n - 1$ under the field multiplication. Then for $\alpha \in E^\times$, $\alpha^{p^n-1} = 1$, i.e., $\alpha^{p^n} = \alpha$. Therefore, every element in E is a zero of $x^{p^n} - x$. Since $x^{p^n} - x$ can have at most p^n zeros, we see that E contains precisely the zeros of $x^{p^n} - x$ in $\overline{Z}_p$. □

Definition 1.86. Let $n \in \mathbb{N}$. An element α of a field is an *n^{th} root of unity* if $\alpha^n = 1$. It is a *primitive n^{th} root of unity* if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.

Remark. Let E be a field of $|E| = p^n$. Then the elements of $E^\times$ are all $(p^n - 1)^{\text{th}}$ roots of unity.

Theorem 1.87. *$\langle F^\times, \cdot \rangle$ of nonzero elements of a finite field F is cyclic.*

Proof. It follows from Corollary 1.35. □

Corollary 1.88. A finite extension E of a finite field F is a simple extension of F.

Proof. Assume that $[E : F] = d < \infty$ and $E = F(\alpha_1, \ldots, \alpha_d)$ for some $\alpha_1, \ldots, \alpha_d \in E^\times$. Since $|F| < \infty$ and $[E : F] < \infty$, $|E| < \infty$. Then there exists $\alpha \in E$ such that $\langle E^\times, \cdot \rangle = \langle \alpha \rangle$ by Theorem 1.87. Then for $i = 1, \ldots, d$, $\alpha_i = \alpha^{n_i}$ for some $n_i \in \mathbb{Z}$, so $F(\alpha) \subseteq E = F(\alpha^{n_1}, \ldots, \alpha^{n_d}) \subseteq F(\alpha)$, and thus $E = F(\alpha)$. □

Example 1.89. Consider the finite field Z_{11}. Then $\langle Z_{11}^\times, \cdot \rangle$ is cyclic. Let us try to find a generator of $Z_{11}^\times$ by brute force and ignorance. We start by trying 2. Since $\left|Z_{11}^\times\right| = 10$ and $|2| \,\Big|\, \left|Z_{11}^\times\right|$, $|2|$ is either 2, 5 or 10. Now $2^2 = 4 \neq 1$, $2^4 = 4^2 = 5 \neq 1$, and $2^5 = (2)(5) = 10 = -1 \neq 1$. Thus, $|2| = 10$, and so 2 is a primitive 10^{th} root of unity in Z_{11}. All the generators of $Z_{11}^\times$ are of the form 2^n, where $\gcd(n, 10) = 1$. These elements are

$$2^1 = 2, \quad 2^3 = 8, \quad 2^7 = 7, \quad 2^9 = 6.$$

The primitive 5^{th} roots of unity in Z_{11} are of the form 2^m with $|2^m| = \frac{|2|}{\gcd(m,10)} = 5$, i.e., $\gcd(m, 10) = 2$, that is,

$$2^2 = 4, \quad 2^4 = 5, \quad 2^6 = 9, \quad 2^8 = 3.$$

The primitive square roots of unity in Z_{11} are of the form 2^m with $\gcd(m, 10) = 5$, that is $2^5 = 10 = -1$.

Proposition 1.90. Let F be a field with algebraic closure $\overline{F}$. Let $\alpha \in \overline{F}$ be a root of f. The followings are equivalent.

(i) α is a multiple root of f.

(ii) α is a root of the derivative of f'

(iii) $\operatorname{irr}(\alpha, F) \mid f'$.

Proof. (ii)$\Longrightarrow$(iii) follows from the definition of $\operatorname{irr}(\alpha, F)$.

(iii)$\Longrightarrow$(i) Assume $\operatorname{irr}(\alpha, F) \mid f'$. Write $f = (x - \alpha)^2 q(x) + r(x)$ for some $q, r \in F[x]$ with $r = 0$ or $\deg(r) < 2$. Then $f' = 2(x - \alpha)q(x) + (x - \alpha)^2 q'(x) + r'(x)$. Since $\operatorname{irr}(\alpha, F) \mid f'(x)$, $f'(\alpha) = 0$ and then $r'(\alpha) = 0$. Since $r = 0$ or $\deg(r) < 2$, there exist $a, b \in F$ such that $r = ax + b$. Since $a = r'(\alpha) = 0$, we have $r = b$ and then $f = (x - \alpha)^2 q(x) + b(x)$. Since $0 = f(\alpha) = b$, we have $f = (x - \alpha)^2$. So f has a multiple root.

(i)$\Longrightarrow$(ii) Write $f = (x - \alpha)^2 g(x)$ for some $g \in F[x]$. Then $f' = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$ and so α is a root of f'. □

Lemma 1.91. If F is a field of prime characteristic p with algebraic closure $\overline{F}$, then $x^{p^n} - x$ has p^n distinct zeros in $\overline{F}$.

Proof. Because $\overline{F}$ is algebraically closed, $x^{p^n} - x$ factors $\overline{F}$ into a product of linear factors $x - \alpha$, so it suffices to show that f has multiple roots over $\overline{F}$. Since $\mathrm{char}(F) = p$, $f' = p^n x^{p^n-1} - 1 = -1$, and so f has no multiple roots over $\overline{F}$ by Proposition 1.90. □

Lemma 1.92. If F is a field of prime characteristic p, then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ for all $\alpha, \beta \in F$ and all possible $n \in \mathbb{Z}_{\geqslant 0}$.

Proof. Let $\alpha, \beta \in F$ and $n \in \mathbb{Z}_{\geqslant 0}$. Then

$$\begin{aligned}(\alpha+\beta)^{p^n} &= \sum_{i=0}^{p^n} \binom{p^n}{i} \alpha^{p^n-i}\beta^i \\ &= \binom{p^n}{0}\alpha^{p^n}\beta^0 + \sum_{i=1}^{p^n-1} 0\alpha^{p^n-i}\beta^i + \binom{p^n}{p^n}\alpha^0\beta^{p^n} \\ &= \alpha^{p^n} + \beta^{p^n}.\end{aligned}$$ □

Theorem 1.93. *A finite field* $\mathrm{GF}(p^n)$ *of* p^n *elements exists for every prime power* p^n.

Proof. Let $\overline{Z}_p$ be an algebraic closure of Z_p, and

$$K = \{\text{zeros of } x^{p^n} - x \text{ in } \overline{Z}_p\} \subseteq \overline{Z}_p.$$

Let $\alpha, \beta \in K$. Then by Lemma 1.92,

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

implying that $\alpha+\beta \in K$. The equation $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ shows that $\alpha\beta \in K$. From $\alpha^{p^n} = \alpha$, we obtain $(-\alpha)^{p^n} = (-1)^{p^n}\alpha$. If p is odd, then $(-1)^{p^n} = -1$, if $p = 2$, then $(-1)^{p^n} = 1 = -1$. Thus, $(-\alpha)^{p^n} = -\alpha$. Now $0, 1 \in K$. For $\alpha \neq 0$, $\alpha^{p^n} = \alpha$ implies that $(1/\alpha)^{p^n} = 1/\alpha$. Any other laws inherit from the ones of the field $\overline{Z}_p$ since $K \subseteq \overline{Z}_p$. Thus, K is a subfield of $\overline{Z}_p$. Therefore, K is the desired field of p^n elements, since Theorem 1.85 showed that $x^{p^n} - x$ has p^n distinct zeros in $\overline{Z}_p$. □

Remark. For $\alpha \in Z_p^\times$, since $\langle Z_p^\times, \cdot\rangle$ is a group, $\alpha^p = \alpha$. Therefore, every element in Z_p is a zero of $x^p - x$. For $\alpha \in Z_p$,

$$\alpha^{p^n} = (\alpha^{p^{n-1}})^p = ((\alpha^{p^{n-2}})^p)^p = \cdots = (\cdots(\alpha^p)^p \cdots)^p = \alpha.$$

Thus, $Z_p \subseteq K$.

Corollary 1.94. If F is any finite field, then for every positive integer n, there is an irreducible polynomial in $F[x]$ of degree n.

Proof. By Corollary 1.84, we can let F have $q = p^r$ elements, where $p = \mathrm{char}(F)$. By Theorem 1.93, there is a subfield K of $\overline{F}$ consisting precisely of the zeros of $x^{p^{rn}} - x$ and $K = |p^{rn}|$. Every element of F is a zero of $x^{p^r} - x$ by Theorem 1.85. Using the fact that for $\alpha \in F$ we have $\alpha^{p^r} = \alpha$, we see that for $\alpha \in F$,

$$\alpha^{p^{rn}} = (\alpha^{p^{r(n-1)}})^{p^r} = ((\alpha^{p^{r(n-2)}})^{p^r})^{p^r} = \cdots = (\cdots(\alpha^{p^r})^{p^r} \cdots)^{p^r} = \alpha.$$

Thus, $F \leqslant K$. Since $|F| = p^r$, $|K| = p^{rn}$ and $[K : F] \in \mathbb{N}$, the proof of Theorem 1.83 show that $[K : F] = n$. By Corollary 1.88, $K = F(\beta)$ for some $\beta \in K$. Therefore $\deg(\mathrm{irr}(\beta, F)) = \deg(\beta, F) = n$. □

Theorem 1.95. *Let p be a prime and $n \in \mathbb{N}$. If E and E' are fields of order p^n, then $E \cong E'$.*

Proof. Both E and E' have Z_p as prime field, up to isomorphism. By Corollary 1.88, E is a simple extension of Z_p of degree n, so there exists an irreducible polynomial $f(x)$ of degree n in $Z_p[x]$ such that $E \cong Z_p[x]/\langle f(x)\rangle$. Let $\alpha \in \overline{Z}_p$ be such that $f(\alpha) = 0$. Since $\mathrm{irr}(\alpha, F) = f/a_n$, where a_n is the leading coefficient of $f(x)$, by Discussion 1.55 Case I, we have that

$$F(\alpha) \cong Z_p[x]/\langle \mathrm{irr}(\alpha, F)\rangle = Z_p[x]/\langle f/a_n\rangle = Z_p[x]/\langle f(x)\rangle \cong E,$$

and so $\alpha \in E$. Because the elements of E are zeros of $x^{p^n} - x$ by Theorem 1.85 and all zeros of f are in E, we see that $f(x)$ is a factor of $x^{p^n} - x$ in $Z_p[x]$. Because E' also consists of zeros of $x^{p^n} - x$ and $f \mid x^{p^n} - x$, we see that E' also contains zeros of irreducible $f(x)$ in $Z_p[x]$. Let $\alpha \in \overline{Z}_p$ be a zero of $f(x)$, then $Z_p[x]/\langle f(x)\rangle \cong F(\alpha) \subseteq E'$. Because E' also contains exactly p^n elements, $E' \cong Z_p[x]/\langle f(x)\rangle$. $\square$

Chapter 2

Automorphisms and Galois Theory

2.1 Automorphisms and fields

From now on in our work, we shall assume that all algebraic extensions and all elements algebraic over a field F under consideration are contained in one fixed algebraic closure $\overline{F}$ of F.

Definition 2.1. Let E be an algebraic extension of a field F. Two elements $\alpha, \beta \in E$ are *conjugate over* F if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$, that is, if α and β are zeros of the same irreducible polynomial over F.

Remark. If we understand that by *conjugate complex numbers* we mean complex numbers that are conjugate over $\mathbb{R}$.

Example 2.2. If $a, b \in \mathbb{R}$ and $b \neq 0$, the conjugate complex numbers $a + bi$ and $a - bi$ are both zeros of $x^2 - 2ax + a^2 + b^2$, which is irreducible in $\mathbb{R}[x]$.

Theorem 2.3 (The Conjugation Isomorphisms)**.** *Let F be a field, and α, β algebraic over F with $\deg(\alpha, F) = n$. The map*

$$\begin{aligned} \psi_{\alpha,\beta} : F(\alpha) &\longrightarrow F(\beta) \\ \sum_{i=0}^{n-1} c_i \alpha^i &\longmapsto \sum_{i=0}^{n-1} c_i \beta^i \end{aligned}$$

is an field isomorphism if and only if α and β are conjugate over F.

Proof. $\Longrightarrow$ Assume that $\psi_{\alpha,\beta}$ is an field isomorphism. Let $\operatorname{irr}(\alpha, F) = \sum_{i=0}^{n} a_i x^i$ for $a_i \in F$. Then $\sum_{i=0}^{n} a_i \alpha^i = 0$, and so

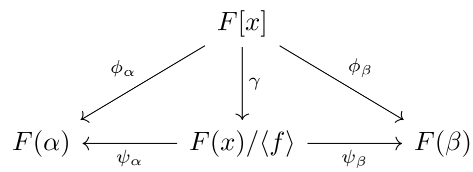
$$0 = \psi_{\alpha,\beta}(0) = \psi_{\alpha,\beta}\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} a_i \beta^i.$$

Then β is zero of $\operatorname{irr}(\alpha, F) \in F[x]$, and so $\operatorname{irr}(\beta, F) \mid \operatorname{irr}(\alpha, F)$ by Theorem 1.52(b). A similar argument using the isomorphism $(\psi_{\alpha,\beta})^{-1} = \psi_{\beta,\alpha}$ shows that $\operatorname{irr}(\alpha, F) \mid \operatorname{irr}(\beta, F)$. Therefore, since both polynomials are monic, $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$, so α and β are conjugate over F.

$\Longleftarrow$ Assume that $\operatorname{irr}(\alpha, F) = f(x) = \operatorname{irr}(\beta, F)$. Then

$$\begin{array}{ccccc} F(\alpha) & \cong & F[x]/\langle f \rangle & \cong & F(\beta) \\ \sum_{i=0}^{n-1} c_i \alpha^i & \overset{\psi_\alpha}{\longleftarrow\!\shortmid} & \sum_{i=0}^{n-1} c_i \left(x + \langle f \rangle\right)^i & \overset{\psi_\beta}{\longmapsto} & \sum_{i=0}^{n-1} c_i \beta^i. \end{array}$$

Also, with evaluation maps $\phi_\alpha : F[x] \to F(\alpha)$ and $\phi_\beta : F[x] \to F(\beta)$, we have a commutative diagram:



Let $\psi_{\alpha,\beta} = \psi_\beta \circ \psi_\alpha^{-1}$. Then for $\sum_{i=0}^{n-1} c_i \alpha^i \in F(\alpha)$,

$$\psi_{\alpha,\beta}\left(\sum_{i=0}^{n-1} c_i \alpha^i\right) = \psi_\beta \circ \psi_\alpha^{-1}\left(\sum_{i=0}^{n-1} c_i \alpha^i\right) = \psi_\beta\left(\sum_{i=0}^{n-1} c_i \left(x + \langle f \rangle\right)^i\right) = \sum_{i=0}^{n-1} c_i \beta^i.$$

Thus, $\psi_{\alpha,\beta}$ is the map defined in the statement of the theorem. □

The following corollary is the cornerstone of our proof of the important Isomorphism Extension Theorem of next section and of most of the rest of our work.

Corollary 2.4. Let α be algebraic over a field F. Every isomorphism ψ mapping $F(\alpha)$ onto a subfield of $\overline{F}$ such that $\psi|_F = \mathrm{id}$ maps α onto a conjugate β of α over F. Conversely, for each conjugate β of α over F, there exists exactly one isomorphism ψ of $F(\alpha)$ onto a subfield of $\overline{F}$ such that $\psi(\alpha) = \beta$ and $\psi|_F = \mathrm{id}$.

Proof. $\Longrightarrow$ Let ψ be an isomorphism of $F(\alpha)$ onto a subfield of $\overline{F}$ such that $\psi|_F = \mathrm{id}$ for $a \in F$. Let $\operatorname{irr}(\alpha, F) = \sum_{i=0}^{n} a_i x^i$ for $a_i \in F$. Then $\sum_{i=0}^{n} a_i \alpha^i = 0$, and so

$$0 = \psi(0) = \psi\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sum_{i=0}^{n} \psi(a_i)\psi(\alpha^i) = \sum_{i=0}^{n} a_i \psi(\alpha)^i.$$

Thus, $\operatorname{irr}(\psi(\alpha), F) = \operatorname{irr}(\alpha, F)$, and so $\beta = \psi(\alpha)$ is a conjugate of α.

$\Longleftarrow$ Existence: For each conjugate β over F, the conjugation isomorphism $\psi_{\alpha,\beta}$ of Theorem 2.3 is an isomorphism with the desired properties.

Uniqueness: Method 1: Since $F(\alpha)$ is an F-vector space with a basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, an isomorphism φ of $F(\alpha)$ is completely determined by its values on $1 \in F$ and its value on α because $\varphi(\alpha^i) = \varphi(\alpha)^i$. Thus, $\psi_{\alpha,\beta}$ is the only such isomorphism.

Method 2: Let $\varphi : F(\alpha) \to E \subseteq \overline{F}$ be an field isomorphism such that $\varphi(\alpha) = \beta$ and $\varphi(a) = a$ for $a \in F$. Then for $\gamma = \sum_{i=0}^{n-1} c_i \alpha^i \in F(\alpha)$,

$$\varphi(\gamma) = \varphi\left(\sum_{i=0}^{n-1} c_i \alpha^i\right) = \sum_{i=0}^{n-1} \varphi(c_i)\varphi(\alpha)^i = \sum_{i=0}^{n-1} c_i \beta^i = \psi_{\alpha,\beta}\left(\sum_{i=0}^{n-1} c_i \alpha^i\right) = \psi_{\alpha,\beta}(\gamma).$$

This implies that $E = \varphi(F(\alpha)) = \psi_{\alpha,\beta}(F(\alpha)) = F(\beta)$. Thus, $\varphi = \psi_{\alpha,\beta}$. □

Corollary 2.5. Let $f \in \mathbb{R}[x]$. If $f(a+bi) = 0$ for $(a+bi) \in \mathbb{C}$, where $a, b \in \mathbb{R}$, then $f(a-bi) = 0$ also. Loosely, complex zeros of polynomials with real coefficients occur in conjugate pairs.

Proof. We have seen that $\mathbb{C} = \mathbb{R}(i)$. Now $\operatorname{irr}(i, \mathbb{R}) = x^2 + 1 = \operatorname{irr}(-i, \mathbb{R})$. so i and $-i$ are conjugate over $\mathbb{R}$. By Theorem 2.3, the conjugation map

$$\begin{aligned} \psi_{i,-i} : \mathbb{C} &\longrightarrow \mathbb{C} \\ a + bi &\longmapsto a - bi \end{aligned}$$

is an isomorphism. Assume that $f(x) = \sum_{i=1}^{n} c_i x^i$ for $c_i \in F$. Then, if $f(a+bi) = 0$, then

$$\begin{aligned} 0 = \psi_{i,-i}(0) = \psi_{i,-i}(f(a+bi)) &= \psi_{i,-i}\left(\sum_{i=0}^{n} c_i (a+bi)^i\right) \\ &= \sum_{i=0}^{n} \psi_{i,-i}(c_i)\psi_{i,-i}(a+bi)^i = \sum_{i=1}^{n} c_i (a-bi)^i = f(a-bi). \end{aligned}$$ □

Example 2.6. Consider $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. The zeros of $\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ are $\sqrt{2}$ and $-\sqrt{2}$, so $\sqrt{2}$ and $-\sqrt{2}$ are conjugate over $\mathbb{Q}$. According to Theorem 2.3 the map

$$\begin{aligned} \psi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{2}) &\longrightarrow \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} &\longmapsto a - b\sqrt{2},\ a, b \in \mathbb{Q} \end{aligned}$$

is an isomorphism of $\mathbb{Q}(\sqrt{2})$ onto itself.

Definition 2.7. An isomorphism of a field onto itself is an *automorphism of the field.*

Definition 2.8. Let E be a field. Define the set $\operatorname{Aut}(E)$ by

$$\operatorname{Aut}(E) = \{\sigma : E \to E \mid \sigma \text{ is an automorphism}\}.$$

Definition 2.9. If σ is an isomorphism of a field E onto some field, then an element a of E is *left fixed by* σ if $\sigma(a) = a$. A collection S of isomorphisms of E *leaves on a subfield* F *of* E *fixed* if each $a \in F$ is left fixed by every $\sigma \in S$. If $\{\sigma\}$ leaves F fixed, then σ *leaves* F *fixed.*

Example 2.10. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The map

$$\begin{aligned} \sigma : E &\longrightarrow E \\ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} &\longmapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6},\ a, b \in \mathbb{Q} \\ (a + b\sqrt{2}) + \sqrt{3}(c + d\sqrt{2}) &\longmapsto a + b\sqrt{2} - \sqrt{3}(c + d\sqrt{2}),\ a, b \in \mathbb{Q} \end{aligned}$$

is an automorphism of E; it is the conjugation isomorphism $\psi_{\sqrt{3},-\sqrt{3}}$ of E onto itself if we view E as $\mathbb{Q}(\sqrt{2})(\sqrt{3})$. We see that σ leaves $\mathbb{Q}(\sqrt{2})$ fixed.

It is our purpose to study the structure of an algebraic extension E of a field F by studying the automorphisms of E that leave fixed each element of F.

Definition 2.11. Let E be a field. Let $S := \{\sigma_i \mid i \in I\} \subseteq \mathrm{Aut}(E)$. Define the set E_S by all $a \in E$ by

$$E_S = \{a \in E \mid \sigma_i(a) = a, \forall i \in I\}.$$

The field E_S is the *fixed field of* S. For a single automorphism σ, we shall refer to E_σ as the *fixed field of* σ.

Example 2.12. Consider the automorphism $\psi_{\sqrt{2},-\sqrt{2}}$ of $\mathbb{Q}(\sqrt{2})$ given in Example 2.6. Then

$$\begin{aligned}
\mathbb{Q}(\sqrt{2})_{\psi_{\sqrt{2},-\sqrt{2}}} &= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q} \text{ and } \psi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a + b\sqrt{2}\} \\
&= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q} \text{ and } a - b\sqrt{2} = a + b\sqrt{2}\} \\
&= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q} \text{ and } b = 0\} \\
&= \{a \mid a \in \mathbb{Q}\} \\
&= \mathbb{Q}.
\end{aligned}$$

Theorem 2.13. *Let E be a field and $S := \{\sigma_i \mid i \in I\} \subseteq \mathrm{Aut}(E)$. Then $E_S \leqslant E$.*

Proof. Let $a, b \in E_S$. Then $\sigma_i(a) = a$ and $\sigma_i(b) = b$ for all $i \in I$. Then for all $i \in I$, since σ_i is a field homomorphism, $\sigma_i(a - b) = \sigma_i(a) - \sigma_i(b) = a - b$, so $a - b \in E_S$. Since the σ_i are field homomorphism, we have that $\sigma_i(0) = 0$. Hence $E_S \neq \emptyset$. By subgroup test, $\langle E_S, +\rangle \leqslant \langle E, +\rangle$.

Let $a, b \in E_S \smallsetminus \{0\}$. Then for all $i \in I$, $\sigma_i(a/b) = \sigma_i(a)/\sigma_i(b) = a/b$, so $a/b \in E_S$. Since the σ_i are field homomorphism, we have that $\sigma_i(1) = 1$. Hence $E_S \smallsetminus \{0\} \neq \emptyset$. By subgroup test, $\langle E_S \smallsetminus \{0\}, \cdot\rangle \leqslant \langle E \smallsetminus \{0\}, \cdot\rangle$.

The distributive laws of E_S inherit from the ones in E. Thus, $E_S \leqslant E$. □

Theorem 2.14. *Let E be a field. Then* $\mathrm{Aut}(E)$ *is a group under function composition.*

Proof. Note that $\mathrm{Aut}(E) \subseteq S_E$, where S_E is the permutation group of E. The identity permutation $\mathrm{id} : E \to E$ is in $\mathrm{Aut}(E)$. Also, for $\sigma, \tau \in \mathrm{Aut}(E)$, $\sigma\tau^{-1} \in \mathrm{Aut}(E)$. Thus, by subgroup test, $\mathrm{Aut}(E) \leqslant S_E$. □

Definition 2.15. Let $E \supseteq F$ be a field extension. Define $\mathrm{G}(E/F)$ by

$$\mathrm{G}(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_F = \mathrm{id}\}.$$

The group $\mathrm{G}(E/F)$ is the *group of automorphism of E leaving F fixed*, or more briefly, the *group of E over F*.

Example 2.16. Consider the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since $\mathrm{irr}(\sqrt{2}, \mathbb{Q}(\sqrt{3})) = x^2 - 2 = \mathrm{irr}(-\sqrt{2}, \mathbb{Q}(\sqrt{3}))$, we have an automorphism

$$\begin{aligned}
\psi_{\sqrt{2},-\sqrt{2}} : \mathbb{Q}(\sqrt{3})(\sqrt{2}) &\longrightarrow \mathbb{Q}(\sqrt{3})(\sqrt{2}) \\
a + b\sqrt{2} &\longmapsto a - b\sqrt{2},\ a, b \in \mathbb{Q}(\sqrt{3}),
\end{aligned}$$

and $\mathbb{Q}(\sqrt{3})_{\psi_{\sqrt{2},-\sqrt{2}}} = \mathbb{Q}(\sqrt{3})$. Since $\mathrm{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3 = \mathrm{irr}(-\sqrt{3}, \mathbb{Q}(\sqrt{2}))$, we have an automorphism

$$\begin{aligned}
\psi_{\sqrt{3},-\sqrt{3}} : \mathbb{Q}(\sqrt{2})(\sqrt{3}) &\longrightarrow \mathbb{Q}(\sqrt{2})(\sqrt{3}) \\
a + b\sqrt{3} &\longmapsto a - b\sqrt{3},\ a, b \in \mathbb{Q}(\sqrt{2}),
\end{aligned}$$

and $\mathbb{Q}(\sqrt{2})_{\psi_{\sqrt{3},-\sqrt{3}}} = \mathbb{Q}(\sqrt{2})$. Then $\psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}} \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3}))$.

Let $\mathrm{id} : \mathbb{Q}(\sqrt{2},\sqrt{3}) \to \mathbb{Q}(\sqrt{2},\sqrt{3})$ be the identity automorphism, $\sigma_1 = \psi_{\sqrt{2},-\sqrt{2}}$, $\sigma_2 = \psi_{\sqrt{3},-\sqrt{3}}$, and $\sigma_3 = \psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}}$. One can check that $\sigma_1\sigma_2 = \sigma_2\sigma_1$. Let $G = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$. Then G is a Klein 4-group and $G \leqslant \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3}))$. For example,

$$\sigma_3\sigma_1 = \sigma_1\sigma_2\sigma_1 = \sigma_1^2\sigma_2 = \mathrm{id}\,\sigma_2 = \sigma_2.$$

Thus, $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt{2},\sqrt{3})_G \leqslant \mathbb{Q}(\sqrt{2},\sqrt{3})$ by Theorem 2.13. Since $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\sigma_1(\sqrt{2}) = -\sqrt{2}$, $\sigma_1(\sqrt{6}) = -\sqrt{6}$, and $\sigma_2(\sqrt{3}) = -\sqrt{3}$, we have that

$$\begin{aligned}\mathbb{Q}(\sqrt{2},\sqrt{3})_G &= \{\alpha := a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}, \text{ and } \sigma(\alpha) = \alpha, \forall g \in G\}\\ &= \{a \mid a \in \mathbb{Q}\}\\ &= \mathbb{Q}.\end{aligned}$$

Thus, $G \leqslant \mathrm{G}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$. Let $\sigma \in \mathrm{G}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$. Then $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3}))$, and so $\sigma(\sqrt{2}) \in \{\pm\sqrt{2}\}$ by Corollary 2.4 and by considering $\sigma : \mathbb{Q}(\sqrt{3})(\sqrt{2}) \xrightarrow{\cong} \mathbb{Q}(\sqrt{3})(\sqrt{2}) \subseteq \overline{\mathbb{Q}(\sqrt{3})}$, and $\sigma(\sqrt{3}) \in \{\pm\sqrt{3}\}$ similarly. Since $\{1,\sqrt{2},\sqrt{3},\sqrt{2}\sqrt{3}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is a $\mathbb{Q}$-algebra, we have that σ is determined by its values on $\sqrt{2}$ and $\sqrt{3}$,

$$\begin{cases}\sqrt{2} & \mapsto \sqrt{2}\\ \sqrt{3} & \mapsto \sqrt{3}\end{cases} \qquad \begin{cases}\sqrt{2} & \mapsto -\sqrt{2}\\ \sqrt{3} & \mapsto \sqrt{3}\end{cases} \qquad \begin{cases}\sqrt{2} & \mapsto \sqrt{2}\\ \sqrt{3} & \mapsto -\sqrt{3}\end{cases} \qquad \begin{cases}\sqrt{2} & \mapsto -\sqrt{2}\\ \sqrt{3} & \mapsto -\sqrt{3}\end{cases}$$

Now G gives all possible combinations of values on $\sqrt{2}$ and $\sqrt{3}$. Hence $\sigma \in G$. Thus, $G \leqslant \mathrm{G}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \subseteq G$, and so $\mathrm{G}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = G$.

Theorem 2.17. *Let $E \supseteq F$ be a field extension. Then $\mathrm{G}(E/F) \leqslant \mathrm{Aut}(E)$. Furthermore, $F \leqslant E_{\mathrm{G}(E/F)}$.*

Proof. Note that $\mathrm{id} \in \mathrm{G}(E/F)$. Let $\sigma, \tau \in \mathrm{G}(E/F)$. Then $\sigma, \tau \in \mathrm{Aut}(E)$, and so $\sigma\tau^{-1} \in \mathrm{Aut}(E)$. Also, $\sigma(a) = a$ and $\tau(a) = a$ for $a \in F$, and so $\sigma\tau^{-1}(a) = \sigma(a) = a$ for $a \in F$. Hence $\sigma\tau^{-1} \in \mathrm{G}(E/F)$. Thus, by subgroup test, $\mathrm{G}(E/F) \leqslant \mathrm{Aut}(E)$.

Note that $E_{\mathrm{G}(E/F)} = \{a \in E \mid \sigma(a) = a, \forall \sigma \in \mathrm{G}(E/F)\}$. Let $b \in F$. Then $\sigma(b) = b$ for any $\sigma \in \mathrm{G}(E/F)$. Hence $b \in E_{\mathrm{G}(E/F)}$, and so $F \subseteq E_{\mathrm{G}(E/F)}$. ☐

Theorem 2.18. *Let F be a finite field of $\mathrm{char}(F) = p$. Then*

$$\begin{aligned}\sigma_p : F &\longrightarrow F\\ a &\longmapsto a^p\end{aligned}$$

is an automorphism, the Frobenius automorphism, of F. Also, $F_{\{\sigma_p\}} \cong Z_p$.

Proof. Let $a, b \in F$. Taking $n = 1$ in Lemma 1.92, we see that $(a+b)^p = a^p + b^p$. Thus, we have

$$\sigma_p(a+b) = (a+b)^p = a^p + b^p = \sigma_p(a) + \sigma_p(b).$$

Of course,

$$\sigma_p(ab) = (ab)^p = a^p b^p = \sigma_p(a)\sigma_p(b),$$

so σ_p is a field homomorphism. Note that

$$\operatorname{Ker}(\sigma_p) = \{a \in F \mid \sigma_p(a) = 0\} = \{a \in F \mid a^p = 0\} = \{0\},$$

since F has no nonzero zero divisors. Hence σ_p is 1-1. Finally, since F is finite, σ_p is onto. Thus, σ_p is a field automorphism.

By the proof of Corollary 1.84, Z_p is contained (up to isomorphism) in F, since $\operatorname{char}(F) = p$. For $c \in Z_p$, we have $\sigma_p(c) = c^p = c$, by Little Theorem of Fermat. Since the polynomial $x^p - x$ has at most p zeros in F, the elements of Z_p are the zeros of $x^p - x$. Therefore,

$$F_{\{\sigma_p\}} = \{a \in F \mid \sigma_p(a) = a\} = \{a \in F \mid a^p = a\} = Z_p. \qquad \square$$

2.2 The isomorphism extension theorem

Theorem 2.19. *Let E be an algebraic extension of a field F. Let σ be an isomorphism of F onto a field F'. Then σ can be extened to an isomorphism $\tau : E \to \tau(E) \subseteq \overline{F'}$ such that $\tau(a) = \sigma(a)$ for all $a \in F$.*

$$\begin{array}{ccc} & & \overline{F'} \\ & & \big|\subseteq \\ E & \xrightarrow[\cong]{\ \tau\ } & \tau(E) \\ \big|\subseteq & & \big|\subseteq \\ F & \xrightarrow{\ \sigma\ } & F' \end{array}$$

Corollary 2.20. If $E \supseteq F$ is an algebraic extension and $\alpha, \beta \in E$ are conjugatione over F, then the conjugation isomorphism $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ can be extended to an isomorphism of E onto a subfield of $\overline{F}$.

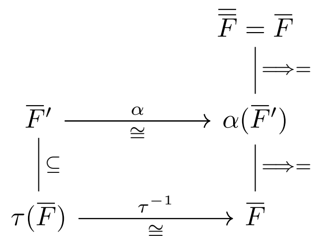
Proof. Since $F \subseteq \overline{F}$ and $\beta \in E \subseteq \overline{F}$, we have that $F(\beta) \subseteq \overline{F}$. Hence $\overline{F} \subseteq \overline{F(\beta)} \subseteq \overline{F}$, so $\overline{F(\beta)} = \overline{F}$. The remaining follows from Theorem 2.19. $\square$

Corollary 2.21. Let $\overline{F}$ and $\overline{F'}$ be two algebraic closures of F. Then there exists a field isomorphism $\tau : \overline{F} \to \overline{F'}$ such that $\tau(a) = a$ for $a \in F$.

Proof. By Theorem 2.19, the identity isomorphism of $\mathrm{id} : F \to F \subseteq \overline{F'}$ can be extended to an isomorphism $\tau : \overline{F} \to \tau(\overline{F}) \subseteq \overline{\overline{F'}} = \overline{F'}$ such that $\tau|_F = \mathrm{id}$.

$$\begin{array}{ccc} & & \overline{F'} \\ & & \big|\subseteq \\ \overline{F} & \xrightarrow[\cong]{\ \tau\ } & \tau(\overline{F}) \\ \big|\subseteq & & \big|\subseteq \\ F & \xrightarrow{\ \mathrm{id}\ } & F \end{array}$$

We need only show that τ is onto $\overline{F}'$. By Theorem 2.19, the map $\tau^{-1} : \tau(\overline{F}) \to \overline{F}$ can be extended to an isomorphism $\alpha : \overline{F}' \to \alpha(\overline{F}') \subseteq \overline{F}$.

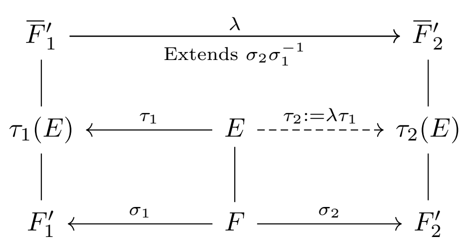


Using proof by contradiction and diagram chase, $\tau(\overline{F}) = \overline{F}'$. □

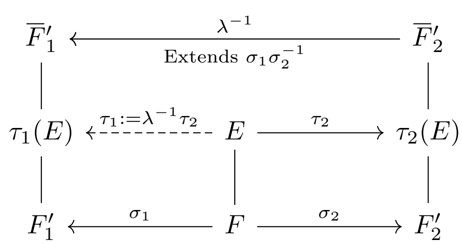
Theorem 2.22. *Let E be a finite extension of a field F. Let σ be an isomorphism of F onto a field $\overline{F}'$. Then the number of extensions of σ to an isomorphism τ of E onto a subfield of $\overline{F}'$ satisfying $\tau(a) = \sigma(a)$ for any $a \in F$, is finite, and independent of F', $\overline{F}'$, and σ, completely determined by E and F.*

Proof. Consider two field isomorphisms $\sigma_1 : F \to F_1'$ and $\sigma_2 : F \to F_2'$. Note that $\sigma_2\sigma_1^{-1} : F_1' \to F_2'$ is an field isomorphism. By Corollary 2.21, there is an field isomorphism $\lambda : \overline{F}_1' \to \overline{F}_2'$ such that $\lambda|_{F_1'} = \sigma_2\sigma_1^{-1}$. Note that $\lambda^{-1} : \overline{F}_2' \to \overline{F}_1'$ is an field homomorphism such that $\lambda^{-1}|_{F_2'} = (\lambda|_{F_1'})^{-1} = (\sigma_2\sigma_1^{-1})^{-1} = \sigma_1\sigma_2^{-1}$.

By Theorem 2.19, there is an field isomorphism $\tau_1 : E \to \tau_1(E)$ such that $\tau_1|_F = \sigma_1$. Let $\tau_2 := \lambda\tau_1$. Then $\tau_2(E) = \lambda\tau_1(E)$. Since τ_1, λ are field homomorphisms and 1-1, τ_2 is 1-1 and an field homomorphism onto $\tau_2(E) = \lambda\tau_1(E)$. Hence τ_1 is a field isomorphism. Also, $\tau_2|_F = \lambda\tau_1|_F = \lambda\sigma_1 = \sigma_2\sigma_1^{-1}\sigma_1 = \sigma_2$, where the second to last equality follows from that $\lambda|_{F_1'} = \sigma_2\sigma_1^{-1}$ and $\mathrm{Im}(\sigma_1) \subseteq F_1'$.



By Theorem 2.19, there is an field isomorphism $\tau_2 : E \to \tau_2(E)$ such that $\tau_2|_F = \sigma_2$. Let $\tau_1 := \lambda^{-1}\tau_2$. Since τ_2, λ^{-1} are field homomorphisms and 1-1, τ_1 is 1-1 and an field homomorphism onto $\tau_1(E) = \lambda^{-1}\tau_2(E)$. Hence τ_2 is a field isomorphism. Also, $\tau_1|_F = \lambda^{-1}\tau_2|_F = \lambda^{-1}\sigma_2 = \sigma_1\sigma_2^{-1}\sigma_2 = \sigma_1$, where the second to last equality follows from that $\lambda^{-1}|_{F_2'} = \sigma_1\sigma_2^{-1}$ and $\mathrm{Im}(\sigma_2) \subseteq F_2'$.



Thus, we have a 1-1 correspondence between $\tau_1 : E \to \overline{F}'_1$ and $\tau_2 : E \to \overline{F}'_2$. In view of this 1-1 correspondence, the number of τ extending σ is independent of F', $\overline{F}'$, and σ.

Since $[E : F] < \infty$, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$ by Theorem 1.73. Assume that

$$\operatorname{irr}(\alpha_i, F) = x^{m_i} + \cdots + a_{i1}x + a_{i0},\ a_{ik} \in F.$$

Then $\alpha_i^{m_i} + \cdots + a_{i1}\alpha_i + a_{i0} = 0$, so $\tau(\alpha_i)^{m_i} + \cdots + \sigma(a_{i1})\tau(\alpha_i) + \sigma(a_{i0}) = 0$, hence $\tau(\alpha_i)$ must be one of the zeros in $\overline{F}'$ of

$$x^{m_i} + \cdots + \sigma(a_{i1})x + \sigma(a_{i0}) \in F'[x].$$

Thus, there are at most m_i possible candidates for the images $\tau(\alpha_i)$ in F'. (Since $\overline{F}$ is algebraically closed, $\operatorname{irr}(\alpha_i, F)$ factors in $\overline{F}[x]$ into linear factors, but $\operatorname{irr}(\alpha_i, F)$ may have multiple roots in $\overline{F}$.) By a similar proof to the tower law and by inductive argument, there exists an F-basis $\mathcal{B}$ of the F-vector space E such that each element in $\mathcal{B}$ is of the form $\alpha_1^{i_1} \ldots \alpha_n^{i_n}$. Also, E is an F-algebra, hence the linear transformation $\tau : E \to \tau(E)$ is determined by $\tau(\alpha_1), \ldots, \tau(\alpha_n)$. Therefore, the number of mappings extending σ is finite. □

Definition 2.23. Let E be a finite extension of a field F. The number of isomorphisms τ of E onto a subfield of $\overline{F}$ leaving F fixed is the *index* $\{E : F\}$, i.e.,

$$\{E : F\} = \sharp \left\{\tau \;\middle|\; \tau : E \xrightarrow{\cong} \tau(E) \subseteq \overline{F} \text{ and } \tau|_F = \mathrm{id}\right\}.$$

Remark. By Theorem 2.22, $\{E : F\}$ is also the number of isomorphisms of E onto a subfield of $\overline{F}$ satisfying $\tau|_F = \sigma$ where $\sigma : F \to F'$ is a given field isomorphism.

Corollary 2.24. If $F \leqslant E \leqslant K$ and $[K : F] < \infty$, then $\{K : F\} = \{K : E\}\{E : F\}$.

Proof. It follows from Theorem 2.22, that each of the $\{E : F\}$ isomorphisms τ_i of E onto a subfild of $\overline{F}$ leaving F fixed has the same number of extensions to an isomorphism λ of K onto a subfield of $\overline{F}$. When condering the identity field isomorphism $\tau_i = \mathrm{id} : E \to E$, the number of extensions to an isomorphism of K is $\{K : E\}$. □

Example 2.25. Consider $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. Assume $\tau : E \to \tau(E) \subseteq \overline{\mathbb{Q}}$ is an field isomorphism leaving $\mathbb{Q}(\sqrt{2})$ fixed. Since $E = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ and $\operatorname{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3$, $\tau(\sqrt{3})$ is a root of $x^2 - 3$, by the proof of Theorem 2.22. Hence $\tau(\sqrt{3})$ have two choices: $\sqrt{3}$ and $-\sqrt{3}$, hence $\{E : \mathbb{Q}(\sqrt{2})\} = 2$. Similarly, $\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = 2$. Thus, $\{E : \mathbb{Q}\} = \{E : \mathbb{Q}(\sqrt{2})\}\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = 2(2) = 4$ by Corollary 2.24.

2.3 Splitting fields

Theorem 2.26. *If an algebraic extension E of a field F is such that*

$$\{\tau \mid \tau : E \xrightarrow{\cong} \tau(E) \subseteq \overline{F} \text{ and } \tau|_F = \mathrm{id}\} \subseteq \operatorname{Aut}(E),$$

then for every $\alpha \in E$, all conjugates of α over F must be in E also.

Proof. Proof by contrapositive argument. Suppose that $\beta \in \overline{F}$ is a conjugate of α over F and $\beta \notin E$. By Theorem 2.3, there is a conjugation isomorphism $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ such that $\psi_{\alpha,\beta}|_F = \mathrm{id}$. By Corollary 2.20, $\psi_{\alpha,\beta}$ can be extended to an field isomorphism $\tau : E \to \tau(E) \subseteq \overline{F}$ such that $\tau|_{F(\alpha)} = \psi(\alpha, \beta)$. Then $\tau|_F = \psi(\alpha, \beta)|_F = \mathrm{id}$. Since

$$F(\beta) = \psi_{\alpha,\beta}(F(\alpha)) = \tau|_{F(\alpha)}(F(\alpha)) = \tau(F(\alpha)) \subseteq \tau(E).$$

we have that $\beta \in \tau(E)$. Since $\beta \notin E$, we have that $\tau(E) \neq E$. Thus, $\tau \notin \mathrm{Aut}(E)$. □

Definition 2.27. Let F be a field. Let $\{f_i(x) \mid i \in I\} \subseteq F[x]$. A field $E \leqslant \overline{F}$ is the *splitting field of* $\{f_i(x) \mid i \in I\}$ over F if E is the smallest subfield of $\overline{F}$ containing F such that each f_i factors in $E[x]$ into linear factors.

A field $K \leqslant \overline{F}$ is a *splitting field over* F if it is the splitting field of some set of polynomials in $F[x]$.

Proposition 2.28. If $E \leqslant \overline{F}$ is the *splitting field of* $\{f_i(x) \mid i \in I\}$ over F, and $\alpha_1, \ldots, \alpha_m$ are all the zeros of $\{f_i(x) \mid i \in I\}$ over $\overline{F}$ (or over $\overline{E}$). Then $E = F(\alpha_1, \ldots, \alpha_m)$.

Proof. $\supseteq$ follows from $F \subseteq E$ and $\alpha_1, \ldots, \alpha_m \in E$.

$\subseteq$ Note that $F(\alpha_1, \ldots, \alpha_m) \subseteq \overline{F}$ contains F and each f_i factors in $F(\alpha_1, \ldots, \alpha_m)[x]$ into linear factors. Since E is the smallest subfield of $\overline{F}$ satisfying these conditions, we have that $E \subseteq K$. □

Proposition 2.29. Let F be a field and $\alpha_1, \ldots, \alpha_m \in \overline{F}$. Then

$$\begin{aligned} F(\alpha_1, \ldots, \alpha_n) &= \left\{ \frac{f(\alpha_1, \ldots, \alpha_m)}{g(\alpha_1, \ldots, \alpha_m)} \;\middle|\; f, g \in F[x_1, \ldots, x_m] \text{ and } g(\alpha_1, \ldots, \alpha_m) \neq 0 \right\} \\ &= \{ f(\alpha_1, \ldots, \alpha_m) \mid f \in F[x_1, \ldots, x_m] \}, \end{aligned}$$

Proof. Tehe first equality follows from that $F(\alpha_1, \ldots, \alpha_n)$ is a field. Now we prove the second equality. By the finite-case proof of the tower law, we get a F-basis for the F-vector space $F(\alpha_1, \ldots, \alpha_m)$:

$$\{\alpha_1^{i_1} \cdots \alpha_m^{i_m} \mid i_k = 0, \ldots, \deg(\alpha_k, F(\alpha_1, \ldots, \alpha_{k-1})), \forall k = 1, \ldots, m\},$$

where α_0 can be chosen to be any element in F, then $F(\alpha_0) = F$. Thus, an element of $F(\alpha_1, \ldots, \alpha_n)$ is of the form $f(\alpha_1, \ldots, \alpha_m)$ with $f \in F[x_1, \ldots, x_m]$. □

Example 2.30. We see that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of $\{x^2 - 2, x^2 - 3\}$ over $\mathbb{Q}$, and also of $\{x^4 - 5x^2 + 6\}$ over $\mathbb{Q}$.

Theorem 2.31. *Let $F \leqslant E \leqslant \overline{F}$. Then E is a splitting field over F if and only if for each $\sigma \in \mathrm{G}(\overline{F}/F)$, we have that $\sigma|_E \in \mathrm{G}(E/F)$.*

Proof. $\Longrightarrow$ Let E be a splitting field over F of $\{f_i(x) \mid i \in I\}$. Let $\sigma \in \mathrm{G}(\overline{F}/F)$. Let $\{\alpha_1, \ldots, \alpha_m\}$ be all the zeros of $\{f_i(x) \mid i \in I\}$ in $\overline{F}$. Then $E = F(\alpha_1, \ldots, \alpha_m)$ by Proposition 2.28. Since $(\sigma|_E)|_F = \sigma|_F = \mathrm{id}$, the field isomorphism $\sigma|_E : E \to \sigma|_E(E)$ is a linear transformation. Hence by Proposition 2.29, $\sigma|_E$ is determined by its action on the F-basis

$$\{\alpha_1^{i_1} \cdots \alpha_m^{i_m} \mid i_k = 0, \ldots, \deg(\alpha_k, F(\alpha_1, \ldots, \alpha_{k-1})), \forall k = 1, \ldots, m\}.$$

Since $\sigma|_E$ is a field homomorphism, $\sigma|_E$ is completely determined by $\alpha|_E(1_F), \sigma|_E(\alpha_1), \ldots, \sigma|_E(\alpha_m)$. But by Corollary 2.4, $\sigma|_E(\alpha_j)$ is a zero of $\mathrm{irr}(\alpha, F)$. Assume that α_j is a zero of $f_i(x)$ over $\overline{F}$. Then by

Theorem 1.52, $\operatorname{irr}(\alpha_j, F) \mid f_i(x)$. Hence over $\sigma|_E(\alpha_j)$ is a zero of $f_i(x)$ in $\overline{F}[x]$, and so $\sigma|_E(\alpha_j) \in E$. Also, $\sigma|_E(1_F) = 1_F \in E$. Thus, $\sigma|_E(E) \subseteq E$. Since $\sigma \in \mathrm{G}(E/F)$ is arbitrary, $\sigma^{-1}|_E(E) \subseteq E$. Then for $a \in E$, we have that

$$a = \sigma(\sigma^{-1}(a)) = \sigma|_E(\sigma^{-1}|_E(a)) \in \sigma|_E(E).$$

Therefore, $E \subseteq \sigma|_E(E)$, and so $\sigma|_E(E) = E$. Thus, $\sigma|_E \in \mathrm{Aut}(E)$, and so $\sigma|_E \in \mathrm{G}(E/F)$.

$\Longleftarrow$ Let $g \in F[x]$ be irreducibles with $\alpha \in E$ a zero. Let β be any zero of $g(x)$ over $\overline{F}$. Then there is a conjugation isomorphism $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ with $\psi_{\alpha,\beta}|_F = \mathrm{id}$. Note that $\psi_{\alpha,\beta}$ can be extended to an field isomorphism $\tau : \overline{F} \to \tau(\overline{F}) \subseteq \overline{F}$ such that $\tau|_{F(\alpha)} = \psi_{\alpha,\beta}$. Then $\tau|_F = \psi_{\alpha,\beta}|_F = \mathrm{id}$.

$$\begin{array}{ccc}
 & & \overline{F(\beta)} = \overline{F} \\
 & & \big| \subseteq \\
\overline{F} = \overline{F(\alpha)} & \xrightarrow[\cong]{\tau} & \tau(\overline{F}) \\
\big| \subseteq & & \big| \subseteq \\
F(\alpha) & \xrightarrow[\cong]{\psi_{\alpha,\beta}} & F(\beta)
\end{array}$$

Then $\tau^{-1} : \tau(\overline{F}) \to \overline{F}$ can be extended to an isomorphism $\lambda : \overline{F} \to \lambda(\overline{F}) \subseteq \overline{\overline{F}}$.

$$\begin{array}{ccc}
 & & \overline{\overline{F}} = \overline{F} \\
 & & \big| \Longrightarrow = \\
\overline{F} & \xrightarrow[\cong]{\lambda} & \lambda(\overline{F}) \\
\big| \subseteq & & \big| \Longrightarrow = \\
\tau(\overline{F}) & \xrightarrow[\cong]{\tau^{-1}} & \overline{F}
\end{array}$$

By diagram chase, $\tau(\overline{F}) = \overline{F}$. Thus, $\tau \in \mathrm{G}(\overline{F}/F)$. Then by assumption, $\tau|_E \in \mathrm{G}(E/F)$. Then

$$\beta = \psi_{\alpha,\beta}(\alpha) = \tau|_{F(\alpha)}(\alpha) = \tau(\alpha) = \tau|_E(\alpha) \in E.$$

Hence all zeros of $g(x)$ in $\overline{F}$ are in E. Thus, if $\{g_k(x)\}$ is the set of all irreducible polynomials in $F[x]$ having a zero in E, then E is the splitting field of $\{g_k(x)\}$ by Proposition 2.28. □

Definition 2.32. Let $E \geqslant F$ be a field extension. A polynomial $f \in F[x]$ *splits* in E if it factors into a product of linear factors in $E[x]$.

Example 2.33. The polynomial $x^4 - 5x^2 + 6$ in $\mathbb{Q}[x]$ splits in the field $\mathbb{Q}[\sqrt{2}]$ into $(x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$.

Corollary 2.34. If $E \leqslant \overline{F}$ is a splitting field over F, then every irreducible polynomial in $F[x]$ having a zero in E splits in E.

Proof. If E is a splitting field over F in $\overline{F}$, then for each $\sigma \in \mathrm{Aut}(\overline{F})$ with $\sigma|_F = \mathrm{id}$, we have that $\sigma|_E \in \mathrm{Aut}(E)$, where $(\sigma|_E)|_F = \sigma|_F = \mathrm{id}$. T he second half proof of Thereom 2.31 showed precisely that E is also the splitting field over F of the set $\{g_k(x)\}$ of all irreducible polynomials in $F[x]$

having a zero in E. Thus an irreducible polynomial $f \in F[x]$ having a zero in E has all its zeros in $\overline{F}$ in E. Therefore, its factorization into linear factors in $\overline{F}[x]$ actually takes place in $E[x]$, so $f(x)$ splits in E. $\square$

Corollary 2.35. $E \leqslant \overline{F}$ is a splitting field over F if and only if for every field isomorphism $\sigma : E \to \sigma(E) \subseteq \overline{F}$ with $\sigma|_F = \mathrm{id}$, we have that $\sigma \in \mathrm{G}(E/F)$. In particular, if E is a splitting field over F and $[E : F] < \infty$, then

$$\{E : F\} = |\mathrm{G}(E/F)|.$$

Proof. $\Longrightarrow$ Let $\sigma : E \to \sigma(E) \subseteq \overline{F}$ be with $\sigma|_F = \mathrm{id}$. By Theorem 2.19 and the second half of the proof of Theorem 2.31, we can extend σ to an $\tau \in \mathrm{G}(\overline{F}/F)$ with $\tau|_E = \sigma$. Since E is a splitting field over F, $\sigma = \tau|_E \in \mathrm{G}(E/F)$ by Theorem 2.31. Hence

$$\left\{\sigma \;\middle|\; \sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F} \text{ and } \sigma|_F = \mathrm{id}\right\} \subseteq \mathrm{G}(E/F).$$

It is clear that

$$\left\{\sigma \;\middle|\; \sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F} \text{ and } \sigma|_F = \mathrm{id}\right\} \supseteq \mathrm{G}(E/F).$$

Since $[E : F] < \infty$,

$$\{E : F\} = \sharp \left\{\sigma \;\middle|\; \sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F} \text{ and } \sigma|_F = \mathrm{id}\right\} = |\mathrm{G}(E/F)|.$$

$\Longleftarrow$ Let $\sigma : \overline{F} \xrightarrow{\cong} \sigma(\overline{F}) \subseteq \overline{F}$ be with $\sigma|_F = \mathrm{id}$. Then $\sigma|_E : E \to \sigma(E) \subseteq \overline{F}$ with $(\sigma|_E)|_F = \sigma|_F = \mathrm{id}$. Hence $\sigma|_E \in \mathrm{G}(E/F)$ by assumption. Thus, E is a splitting field over F by Theorem 2.31. $\square$

Example 2.36. We know that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $\{x^2 - 2, x^2 - 3\}$ over $\mathbb{Q}$. Example 2.16 showed that $\mathrm{G}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$. Then

$$\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\} = \left|\mathrm{G}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})\right| = 4.$$

In fact, if $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$, then $\sigma|_{\mathbb{Q}} = \mathrm{id}$ since $\mathbb{Q}$ is the prime subfiel of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hence $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$.

Example 2.37. Note that $x^3 - 2$ doesn't split in $\mathbb{Q}(\sqrt[3]{2})$. By the factor theorem, $x^3 - 2 = (x - \sqrt[3]{2})f$, where $f \in \mathbb{Q}(\sqrt[3]{2})[x]$ is irreducible of $\deg(f) = 2$ Let E be a splitting field of $x^3 - 2$ over $\mathbb{Q}$. (Then E is also a splitting field of f over $\mathbb{Q}(\sqrt[3]{2})$). Let $\alpha := a + bi$ be a root of f over $\overline{\mathbb{Q}(\sqrt[3]{2})} = \overline{\mathbb{Q}}$. Then $\overline{\alpha} = a - bi = \alpha + 2a \in \mathbb{Q}(\sqrt[3]{2}, \alpha)$ since $a \in \mathbb{Q}(\sqrt[3]{2})$ and $b \in \overline{\mathbb{Q}}$. Hence $E = \mathbb{Q}(\sqrt[3]{2}, \alpha, \overline{\alpha}) = \mathbb{Q}(\sqrt[3]{2}, \alpha)$. Since $\mathrm{irr}(\alpha, \mathbb{Q}(\sqrt[3]{2})) = f$, we have that

$$[E : \mathbb{Q}(\sqrt[3]{2})] = [\mathbb{Q}(\sqrt[3]{2})(\alpha) : \mathbb{Q}(\sqrt[3]{2})] = \deg(\alpha, \mathbb{Q}(\sqrt[3]{2})) = \deg(\mathrm{irr}(\alpha, \mathbb{Q}(\sqrt[3]{2}))) = \deg(f) = 2.$$

Then

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2(3) = 6.$$

Note that the zeros of $x^3 - 2$ in $\overline{\mathbb{Q}}$ is

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\tfrac{-1+i\sqrt{3}}{2}, \quad \sqrt[3]{2}\tfrac{-1-i\sqrt{3}}{2}.$$

Thus the splitting field E of $x^3 - 2$ over $\mathbb{Q}$ is

$$\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\frac{-1+i\sqrt{3}}{2}, \sqrt[3]{2}\frac{-1-i\sqrt{3}}{2}\right) = \mathbb{Q}\left(\sqrt[3]{2}, \frac{-1+i\sqrt{3}}{2}\right) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}).$$

2.4 Separable extensions

Definition 2.38. Let $f \in F[x]$. A zero $\alpha \in \overline{F}$ of f is *of multiplicity* ν if

$$\nu = \max \left\{ m \in \mathbb{N} \;\middle|\; (x-\alpha)^m \mid f \text{ in } \overline{F}[x] \right\}.$$

Theorem 2.39. *Let $f \in F[x]$ be irreducible. Then all zeros of $f(x)$ in $\overline{F}$ have the same multiplicity.*

Proof. Let α, β be zeros of $f(x)$ in $\overline{F}$. Then by Theorem 2.3, there is a conjugation isomorphism $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ with $\psi_{\alpha,\beta}|_F = \mathrm{id}$. By Corollary 2.20, $\psi_{\alpha,\beta}$ can be extended to an isomorphism $\tau : \overline{F} \to \overline{F}$. Define the natural map τ_x by

$$\begin{aligned} \tau_x : \overline{F}[x] &\longrightarrow \overline{F}[x] \\ \sum_{i=0}^{m} a_i x^i &\longmapsto \sum_{i=0}^{m} \tau(a_i) x^i. \end{aligned}$$

We will show that τ_x is a field homomorphism.

Let $\sum_{i=0}^{m} a_i x^i, \sum_{j=0}^{n} b_j x^j \in \overline{F}[x]$. By adding some corresponding zero terms, we can assume that $m = n$. Then it is straightforward to show that τ_x is an additive group homomorphism.

Let $\sum_{i=0}^{m} a_i x^i, \sum_{j=0}^{n} b_j x^j \in \overline{F}[x]$. Assume that $a_i = 0$ when $m+1 \leqslant i \leqslant m+n$ and $b_j = 0$ when $n+1 \leqslant j \leqslant m+n$. Then

$$\begin{aligned} \tau_x\left(\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right)\right) &= \tau_x\left(\sum_{k=0}^{m+n}\sum_{\ell=0}^{k} a_\ell b_{k-\ell} x^k\right) \\ &= \sum_{k=0}^{m+n}\sum_{\ell=0}^{k} \tau(a_\ell b_{k-\ell} x^k) \\ &= \sum_{k=0}^{m+n}\sum_{\ell=0}^{k} \tau(a_\ell b_{k-\ell}) x^k \\ &= \sum_{k=0}^{m+n}\sum_{\ell=0}^{k} \tau(a_\ell)\tau(b_{k-\ell}) x^k \\ &= \left(\sum_{i=0}^{m} \tau(a_i) x^i\right)\left(\sum_{j=0}^{n} \tau(b_j) x^j\right) \\ &= \tau_x\left(\sum_{i=0}^{m} a_i x^i\right)\tau_x\left(\sum_{j=0}^{n} b_j x^j\right). \end{aligned}$$

Hence τ_x is a multiplicative group homomorphism.

Note that for $i \in \mathbb{N}$ $\tau((-\alpha)^i) = \psi_{\alpha,\beta}((-\alpha)^i) = (\psi_{\alpha,\beta}(-\alpha))^i = (-\psi_{\alpha,\beta}(\alpha))^i = (-\beta)^i$. Let ν be the multiplicity of α in f. Since τ_x is an additive group homomorphism,

$$\begin{aligned}\tau_x((x-\alpha)^\nu) &= \tau_x\left(\sum_{i=0}^{\nu}\binom{\nu}{i}x^i(-\alpha)^{\nu-i}\right)\\ &= \sum_{i=0}^{\nu}\binom{\nu}{i}\tau_x((-\alpha)^{\nu-i}x^i)\\ &= \sum_{i=0}^{\nu}\binom{\nu}{i}\tau((-\alpha)^{\nu-i})x^i\\ &= \sum_{i=0}^{\nu}\binom{\nu}{i}x^i(-\beta)^{\nu-i}\\ &= (x-\beta)^\nu.\end{aligned}$$

Since $\tau|_F = (\tau|_{F(\alpha)})|_F = \psi_{\alpha,\beta}|_F = \mathrm{id}$, we have that $\tau_x(f(x)) = f(x)$. Write $f = (x-\alpha)^\nu g(x)$ with $g \in F[x]$. Then since τ_x is a multiplicative group homomorphism,

$$f(x) = \tau_x(f(x)) = \tau_x((x-\alpha)^\nu g(x)) = \tau_x((x-\alpha)^\nu)\tau_x(g(x)) = (x-\beta)^\nu\tau_x(g(x)).$$

Thus, the multiplicity of β in $f(x)$ is greater than or equal to the multiplicity of α. A symmetric argument gives the reverse inequality, so the multiplicity of α equals that of β. □

Corollary 2.40. If $f \in F[x]$ is irreducible, then $f(x)$ has a factorization in $\overline{F}[x]$ of the form

$$a\prod_i (x-\alpha_i)^\nu,$$

where the α_i are the distinct zeros of $f(x)$ in $\overline{F}$ and $a \in F$.

Proof. It is immediate from Theorem 2.39. □

Example 2.41. Let $E = \mathbb{F}_p(y)$, where y is an indeterminate. Let $t = y^p$ and $F = \mathbb{F}_p(t) \leqslant E$. Now $E = F(y)$ is algebraic over F, for y is a zero of $(x^p - t) \in \mathbb{F}_p(t)[x] = F[x]$. Since $y \notin F$, $\mathrm{irr}(y,F) \geqslant 2$. Since $\mathrm{char}(E) = p$, we have that in E,

$$x^p - t = x^p - y^p = (x-y)^p.$$

By Theorem 1.52(b), $\mathrm{irr}(y,F) \mid x^p - t$ in $F[x]$, and so $\mathrm{irr}(y,F) \mid (x-y)^p$ in $E[x]$. Thus, $\mathrm{irr}(y,F) = (x-y)^q$ in E for some $2 \leqslant q \leqslant p$, so y is a zero of $\mathrm{irr}(y,F)$ of multiplicity > 1.

Remark. Show that $\mathrm{irr}(y,F) = x^p - t$.

Theorem 2.42. *Let $\alpha \in \overline{F}$ be algebraic over F. Then*

$$\{F(\alpha) : F\} = \sharp\{\textit{distinct zeros of } \mathrm{irr}(\alpha,F) \textit{ in } \overline{F}\}.$$

Proof. Note that

$$\{F(\alpha) : F\} = \sharp\left\{\tau \;\middle|\; \tau : F(\alpha) \xrightarrow{\cong} \tau(F(\alpha)) \subseteq \overline{F} \text{ and } \tau|_F = \mathrm{id}\right\}.$$

Let $\alpha := \alpha_1, \ldots, \alpha_n$ be distinct zeros of $\mathrm{irr}(\alpha, F)$ in $\overline{F}$. By Theorem 2.3, we have n distinct field isomorphisms: $\psi_{\alpha,\alpha_i} : F(\alpha) \xrightarrow{\cong} F(\alpha_i) \subseteq \overline{F}$ and $\tau|_F = \mathrm{id}$. Hence $\{F(\alpha) : F\} \geqslant n$. Corollary 2.4 shows that for each τ such that $\tau : F(\alpha) \xrightarrow{\cong} \tau(F(\alpha)) \subseteq \overline{F}$ and $\tau|_F = \mathrm{id}$, we have that $\tau(\alpha) = \alpha_i$ for some i. Then $\tau = \psi_{\alpha,\alpha_i}$. Thus, $\{F(\alpha) : F\} = n$. □

Recall 2.43. A finite field extension is an algebraic extension.

Theorem 2.44. *If $E \geqslant F$ is a finite field extension, then $\{E : F\} \mid [E : F]$.*

Proof. By Theorem 1.73, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in \overline{F}$. Set $\alpha_0 \in F$. For $i = 1, \ldots, n$, we assume that $\mathrm{irr}(\alpha_i, F(\alpha_1, \ldots, \alpha_{i-1}))$ has n_i distinct zeros, each of which is of multiplicity ν_i by Theorem 2.39. Then by Theorem 1.66,

$$\begin{aligned}[E : F] &= \prod_{i=1}^{n} [F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})] \\ &= \prod_{i=1}^{n} \deg(\alpha_i, F(\alpha_1, \ldots, \alpha_{i-1})) \\ &= \prod_{i=1}^{n} n_i \nu_i.\end{aligned}$$

By Corollary 2.24,

$$\begin{aligned}\{E : F\} &= \prod_{i=1}^{n} \{F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})\} \\ &= \prod_{i=1}^{n} n_i.\end{aligned}$$

Thus, $\{E : F\} \mid [E : F]$. □

Definition 2.45. A finite field extension E of F is a *separable extension of* F if $\{E : F\} = [E : F]$. An element $\alpha \in \overline{F}$ is *separable over* F if $F(\alpha)$ is a separable extension of F.

Example 2.46. The field $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is separable over $\mathbb{Q}$ since we saw in Example 2.36 that $\{E : \mathbb{Q}\} = 4 = [E : \mathbb{Q}]$.

Definition 2.47. An irreducible polynomial $f \in F[x]$ is *separable over* F if every zero of $f(x)$ in $\overline{F}[x]$ is of multiplicity 1.

Theorem 2.48. *$\alpha \in \overline{F}$ is separable over F if and only if $\mathrm{irr}(\alpha, F)$ is separable over F.*

Proof. $\alpha \in \overline{F}$ is separable if and only if $F(\alpha)$ is a separable extension of F if and only if $\{F(\alpha) : F\} = [F(\alpha) : F]$ if and only if

$$\sharp\{\text{distinct zeros of } \mathrm{irr}(\alpha, F) \text{ in } \overline{F}\} = \{F(\alpha) : F\} = [F(\alpha) : F] = \deg(\mathrm{irr}(\alpha, F))$$

if and only if each zero of $\mathrm{irr}(\alpha, F)$ is of multiplicity 1 if and only if $\mathrm{irr}(\alpha, F)$ is separable over F. □

Theorem 2.49. *If $K \geqslant E \geqslant F$ are finite field extensions, then K is separable over F if and only if K is separable over E and E is separable over F.*

Proof. Note that $[K : F] = [K : E][E : F]$ and $\{K : F\} = \{K : E\}\{E : F\}$.

$\Longrightarrow$ Assume that K is separable over F. Then $[K : F] = \{K : F\}$, and so $[K : E][E : F] = \{K : F\} = \{K : E\}\{E : F\}$. Since $\{K : E\} \mid [K : E]$ and $\{E : F\} \mid [E : F]$ by Theorem 2.44, we have that $\{K : E\} = [K : E]$ and $\{E : F\} = [E : F]$. Hence K is separable over E and E is separable over F.

$\Longleftarrow$ Assume that K is separable over E and E is separable over F. Then $\{K : E\} = [K : E]$ and $\{E : F\} = [E : F]$. Hence

$$[K : F] = [K : E][E : F] = \{K : E\}\{E : F\} = \{K : F\}.$$

Thus, K is separable over F. □

Corollary 2.50. If $E \geqslant F$ is a finite field extension, then E is separable over F if and only if each $\alpha \in E$ is separable over F.

Proof. $\Longrightarrow$ Let $\alpha \in E$. Then $F \leqslant F(\alpha) \leqslant E$. Hence $F(\alpha)$ is separable over F by Theorem 2.49, and so α separable over F.

$\Longleftarrow$ Since $[E : F] < \infty$, there exist $\alpha_1, \ldots, \alpha_n$ such that

$$F < F(\alpha_1) < F(\alpha_1, \alpha_2) < \cdots < E = F(\alpha_1, \ldots, \alpha_n).$$

Since α_i is a zero of $\operatorname{irr}(\alpha_i, F) \in F(\alpha_1, \ldots, \alpha_{i-1})[x]$, we have that $\operatorname{irr}(\alpha_i, F(\alpha_1, \ldots, \alpha_{i-1})) \mid \operatorname{irr}(\alpha_i, F)$ by Theorem 1.52. Now since α_i is separable over F, α_i is separable over $F(\alpha_i, \ldots, \alpha_{i-1})$. Thus, $F(\alpha_1, \ldots, \alpha_i)$ is separable over $F(\alpha_1, \ldots, \alpha_{i-1})$. Therefore E is separable over F by Theorem 2.49, extended by induction. □

Lemma 2.51. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \overline{F}[x]$$

If there exists $m \in \mathbb{N}$ with $m \cdot 1_F \neq 0_F$ such that $(f(x))^m \in F[x]$, then $f(x) \in F[x]$.

Proof. It is equivalent to show that $a_{n-r} \in F$ for $r = 1, \ldots, n$. We proceed by induction on r, to show that $a_{n-r} \in F$.

Base case: When $r = 1$, we have that

$$\begin{aligned} F[x] \ni (f(x))^m &= x^{mn} + \sum_{i=1}^{m} (a_{n-1}x^{mn-1}) + \cdots + a_0^m \\ &= x^{mn} + (m \cdot 1_F)a_{n-1}x^{mn-1} + \cdots + a_0^m, \end{aligned}$$

because

$$\begin{aligned} \sum_{i=1}^{m} (a_{n-1}x^{mn-1}) = \left(\sum_{i=1}^{m} a_{n-1} \right) x^{mn-1} &= \left[\sum_{i=1}^{m} (1_F \cdot a_{n-1}) \right] x^{mn-1} \\ = \left[\left(\sum_{i=1}^{m} 1_F \right) \cdot a_{n-1} \right] x^{mn-1} &= (m \cdot 1_F)a_{n-1}x^{mn-1}. \end{aligned}$$

Then $(m \cdot 1_F)a_{n-1} \in F$. Since $m \cdot 1_F \neq 0_F$, we have that $\frac{1}{m \cdot 1_F} \in F$, hence

$$a_{n-1} = 1_F a_{n-1} = \left[\frac{1}{m \cdot 1_F}(m \cdot 1_F)\right] a_{n-1} = \frac{1}{m \cdot 1_F}\left[(m \cdot 1_F)a_{n-1}\right] \in F.$$

Induction step: Suppose that $a_{n-r} \in F$ for $r = 1, \ldots, k$. Then the coefficient of $x^{mn-(k+1)}$ in $(f(x))^m$ is of the form

$$(m \cdot 1_F)a_{n-(k+1)} + g_{k+1}(a_{n-1}, a_{n-2}, \ldots, a_{n-k}),$$

where $g_{k+1}(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$ is a formal polynomial expression in $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$. By the induction hypothesis that we just stated, $g_{k+1}(a_{n-1}, a_{n-2}, \ldots, a_{n-k}) \in F$, so $a_{n-(k+1)} \in F$, since $m \cdot 1_F \neq 0_F$. □

Definition 2.52. A field is *perfect* if every finite field extension is a separable extension.

Theorem 2.53. *Every field of characteristic zero is perfect.*

Proof. Let F be a field of $\operatorname{char}(F) = 0$. Let $E \geqslant F$ be a finite field extension. Let $\alpha \in E$. Then by Corollary 2.40 in $\overline{F}[x]$

$$\operatorname{irr}(\alpha, F) = \prod_i (x - \alpha_i)^\nu = \left(\prod_i (x - \alpha_i)\right)^\nu.$$

where α_i are the distinct zeros of $\operatorname{irr}(\alpha, F)$, and, say, $\alpha = \alpha_1$. Since $\operatorname{char}(F) = 0$, we have that $\nu \cdot 1_F \neq 0_F$, so $\prod_i (x - \alpha_i) \in F[x]$ by Lemma 2.51. Since $\alpha = \alpha_1$ is a zero of $\prod_i (x - \alpha_i) \in F[x]$, we have that

$$\left(\prod_i (x - \alpha_i)\right)^\nu = \operatorname{irr}(\alpha, F) \,\Big|\, \prod_i (x - \alpha_i)$$

by Theorem 1.52(b). Hence $\nu = 1$. Thus, α is separable over F. Therefore, E is separable over F by Corollary 2.50. □

Theorem 2.54. *Every finite field is perfect.*

Proof. Let F be a finite field of $\operatorname{char}(F) = p$, where p is prime. Let $E \geqslant F$ be a finite extension. Let $\alpha \in E$. We need to show that α is separable over F. Now we assume that $\operatorname{irr}(\alpha, F) = \prod_i (x - \alpha_i)^\nu$, where the α_i are the distinct zeros of $f(x)$, and, say, $\alpha = \alpha_1$. Write $\nu = p^t e$, where $p \nmid e$. Then

$$F[x] \ni \operatorname{irr}(\alpha, F) = \prod_i (x - \alpha_i)^\nu = \left(\prod_i (x - \alpha_i)^{p^t}\right)^e.$$

Since $e \cdot 1_F \neq 0_F$, $\prod_i (x - \alpha_i)^{p^t} \in F[x]$ by Lemma 2.51. (Since $\operatorname{irr}(\alpha, F)$ is of minimal degree over F having α as a zero, we must have $e = 1$.) Note that

$$F[x] \ni \prod_i (x - \alpha_i)^{p^t} = \prod_i (x^{p^t} - \alpha_i^{p^t})$$

by Lemma 1.92 since $\operatorname{char}(F) = p$. Let $g(x) := \prod_i (x - \alpha_i^{p^t})$. Then $g(x) \in F[x]$ since $g(x)$ can be obtained from $\prod_i (x^{p^t} - \alpha_i^{p^t})$ by lowering the degree of the corresponding terms of $\operatorname{irr}(\alpha, F)$ while keeping the coefficients. Since $x^{p^t} - \alpha^{p^t} = (x-\alpha)^{p^t}$, we see that α is the only zero of $x^{p^t} - \alpha^{p^t}$ in $\overline{F}$. Now $g(x)$ is separable over F with distinct zeros $\alpha_i^{p^t}$. Then $\operatorname{irr}(\alpha^{p^t}, F) = \operatorname{irr}(\alpha_1^{p^t}, F) \mid g(x)$, and so $\operatorname{irr}(\alpha^{p^t}, F)$ is separable. Hence α^{p^t} is separable over F by Theorem 2.48. Then $F(\alpha^{p^t})$ is separable over F.

Since $[E:F] < \infty$, $\alpha \in E$ is algebraic over F. Then $[F(\alpha):F] < \infty$, so $F(\alpha)$ is algebraic over F, hence α^{p^t} is algebraic over F. Thus, $F(\alpha^{p^t})$ is a finite-dimensional vector space over the finite field F, so $F(\alpha^{p^t})$ must be a finite field of cardinality p^n for some $n \in \mathbb{N}$. Then $\operatorname{char}(F(\alpha^{p^t})) = p$ by Corollary 1.84. Hence by Theorem 2.18, $\sigma_p \in \operatorname{Aut}(F(\alpha^{p^t}))$, where

$$\begin{aligned}\sigma_p : F(\alpha^{p^t}) &\longrightarrow F(\alpha^{p^t})\\ a &\longmapsto a^p.\end{aligned}$$

Consequently, $(\sigma_p)^t \in \operatorname{Aut}(F(\alpha^{p^t}))$ by Theorem 2.14, where

$$\begin{aligned}(\sigma_p)^t : F(\alpha^{p^t}) &\longrightarrow F(\alpha^{p^t})\\ b &\longmapsto b^{p^t}.\end{aligned}$$

Since $(\sigma_p)^t$ is onto and $\alpha^{p^t} \in F(\alpha^{p^t})$, there exists $\beta \in F(\alpha^{p^t})$ such that $\alpha^{p^t} = (\sigma_p)^t(\beta) = \beta^{p^t}$. Thus, $\beta = \alpha$. Since $\beta \in F(\alpha^{p^t})$, we have $F(\beta) \subseteq F(\alpha^{p^t}) \subseteq F(\alpha) = F(\beta)$. Hence $F(\alpha) = F(\alpha^{p^t})$. Since $F(\alpha^{p^t})$ was separable over F, we now see that $F(\alpha)$ is separable over F. Therefore α is separable over F. (Lemma 1.92 implies $t = 0$.) Thus, α is a separable extension of F by Corollary 2.50. □

Theorem 2.55 (Primitive element theorem)**.** *If $E \supseteq F$ is a finite and separable extension, then $E = F(\theta)$ for some $\alpha \in E$. (Such an element α is a* primitive element*.)*

Proof. Assuem that $|F| < \infty$. Then $|E| < \infty$, and so $E^\times = \langle \alpha \rangle$ for some $\alpha \in E$ by Corollary 1.35. Clearly, $E = F(\alpha)$.

Assume that $|F| = \infty$. It is enough to show that for $\alpha, \beta \in E$, $F(\alpha, \beta) = F(\theta)$ for some $\theta \in E$. Let $\beta = \alpha_1, \ldots, \alpha_r$ be the roots of $\operatorname{irr}(\alpha, F)$ and $\beta_1, \ldots, \beta_s$ be the roots of $\operatorname{irr}(\beta, F)$ over $\overline{F}$. Since F is infinite, we can choose $c \in F$ such that $\frac{\alpha_i - \alpha}{\beta_j - \beta} \neq -c$ for $i = 1, \ldots, r$ and $j = 2, \ldots, s$. Hence $\alpha + c(\beta - \beta_j) \neq \alpha_i$ for $i = 1, \ldots, r$ and $j = 2, \ldots, s$. Let $\theta := \alpha + c\beta$ and $f(x) := \operatorname{irr}(\alpha, F)(\theta - cx) \in F(\theta)[x]$. Then

$$f(\beta) = \operatorname{irr}(\alpha, F)(\theta - c\beta) = \operatorname{irr}(\alpha, F)(\alpha) = 0.$$

Since $\alpha + c(\beta - \beta_j) \neq \alpha_i$ for $i = 1, \ldots, r$ and $j = 2, \ldots, s$, we have that

$$f(\beta_j) = \operatorname{irr}(\alpha, F)(\theta - c\beta_j) = \operatorname{irr}(\alpha, F)(\alpha + c(\beta - \beta_j)) \neq 0, \forall j = 2, \ldots, s.$$

This implies f and $\operatorname{irr}(\beta, F)$ only have one root β in common. Since $f(\beta) = 0$ and $f \in F(\theta)[x]$, $\operatorname{irr}(\beta, F(\theta)) \mid f$. Since $\operatorname{irr}(\beta, F)(\beta) = 0$ and $\operatorname{irr}(\beta, F) \in F(\theta)[x]$, we have that $\operatorname{irr}(\beta, F(\theta)) \mid \operatorname{irr}(\beta, F)$. Since $E \supseteq F$ is separable, we have that $F(\beta)$ is separable over F, and so $\operatorname{irr}(\beta, F)$ is separable over F. Then $F(\theta)[x] \ni \operatorname{irr}(\beta, F(\theta)) = u(x - \beta)$ for some $u \in F(\theta)^\times$. Hence $u^{-1} \in F(\theta)$ and $u\beta \in F(\theta)$, so $\beta = u^{-1}(u\beta) \in F(\theta)$. Then $\alpha = \theta - c\beta \in F(\theta)$, and so $F(\alpha, \beta) \subseteq F(\theta)$. Also, since $\theta = \alpha + c\beta \in F(\alpha, \beta)$, $F(\theta) \subseteq F(\alpha, \beta)$. Therefore, $F(\theta) = F(\alpha, \theta)$. □

Corollary 2.56. A finite extension of a field of characteristic 0 is a simple extension.

Proof. It follows from at once from Theorem 2.53 and 2.55. □

Example 2.57. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Proof. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a simple extension of $\mathbb{Q}$. Indeed,

$$\sqrt{3} = \frac{(\sqrt{2}+\sqrt{3}) + (\sqrt{3}-\sqrt{2})}{2} = \frac{\sqrt{2}+\sqrt{3}}{2} + \frac{1}{2(\sqrt{2}+\sqrt{3})} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}),$$
$$\sqrt{2} = \frac{(\sqrt{2}+\sqrt{3}) + (\sqrt{2}-\sqrt{3})}{2} = \frac{\sqrt{2}+\sqrt{3}}{2} - \frac{1}{2(\sqrt{2}+\sqrt{3})} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$ □

2.5 Galois Theorem

Recall 2.58. (a) If $F \leqslant E$, then

$$\mathrm{G}(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_F = \mathrm{id}\}.$$

(b) Let $F \leqslant E \leqslant \overline{F}$ and $\sigma \in \mathrm{G}(E/F)$. Then for any $\alpha \in E$, $\sigma(\alpha) = \beta$ for some conjugate β of α over F.

(c) Let $F \leqslant E$. For any $S \subseteq \mathrm{G}(E/F)$,

$$E_S = \{e \in E \mid \sigma(e) = e, \forall \sigma \in S\}.$$

Also, $F \leqslant E_{\mathrm{G}(E/F)} \leqslant E_S$ for any $S \subseteq \mathrm{G}(E/F)$.

(d) E is a splitting field over F if and only if for each $\sigma \in \mathrm{G}(\overline{F}/F)$, we have that $\sigma|_E \in \mathrm{G}(E/F)$ if and only if for each $\sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F}$ with $\sigma|_F = \mathrm{id}$, we have that $\sigma \in \mathrm{G}(E/F)$. If $[E : F] < \infty$ and E is a splitting field over F, then $|G(E/F)| = \{E : F\}$.

(e) Let $[E : F] < \infty$. Then E is separable over F if and only if $\{E : F\} = [E : F]$. Also, E is separable over F if and only if $\mathrm{irr}(\alpha, F)$ has all zeros of multiplicity 1 for every $\alpha \in E$.

(f) If $[E : F] < \infty$, then E is a separable spliting splitting field over F if and only if $|\mathrm{G}(E/F)| = \{E : F\} = [E : F]$.

We are going to be interesed in finite extensions K of F such that for every $\sigma : K \xrightarrow{\cong} \sigma(K) \subseteq \overline{F}$ with $\sigma|_F = \mathrm{id}$, we have that $\sigma \in \mathrm{G}(E/F)$, and such that $[K : F] = \{K : F\}$. In view of results (d) and (e), these are the finite extensions of F that are separable splitting fields over F.

Definition 2.59. A finite extension K of F is a *finite normal extension of* F if K is a separable splitting field over F.

Theorem 2.60. *Let K be a finite normal extension of F and $F \leqslant E \leqslant K \leqslant \overline{F}$. Then K is finite normal extension of E and $\mathrm{G}(K/E) \leqslant \mathrm{G}(K/F)$. Moreover, for $\sigma, \tau \in \mathrm{G}(K/F)$, we have that $\sigma|_E = \tau|_E$ if and only if $\sigma\,\mathrm{G}(K/E) = \tau\,\mathrm{G}(K/E)$ in $\mathrm{G}(K/F) /\!/ \mathrm{G}(K/E)$.*

Proof. Assume that K is the splitting field of a set $\{f_i(x) \mid i \in I\} \subseteq F[x]$. Then K is the splitting field of $\{f_i(x) \mid i \in I\} \subseteq E[x]$, so K is a splitting field over E. Since $[K : F] < \infty$ and K is separable over F, K is separable over E by Theorem 2.49. Thus, K is a finite normal extension of E.

Let $\sigma \in \mathrm{G}(K/E)$. Then $\sigma \in \mathrm{Aut}(K)$ and $\sigma|_E = \mathrm{id}$. Hence $\sigma|_F = (\sigma|_E)|_F = (\mathrm{id}|_{\mathrm{E}})|_F = \mathrm{id}|_F$, and so $\sigma \in \mathrm{G}(K/F)$. Thus, $\mathrm{G}(K/E) \subseteq \mathrm{G}(K/F)$. Since $\mathrm{G}(K/E)$ is a group, $\mathrm{G}(K/E) \leqslant \mathrm{G}(K/F)$.

Note that $\sigma\,\mathrm{G}(K/E) = \tau\,\mathrm{G}(K/E)$ if and only if $\tau^{-1}\sigma \in \mathrm{G}(K/E)$ if and only if $\sigma = \tau\mu$ for some $\mu \in \mathrm{G}(K/E)$.

$\Longrightarrow$ Assume that $\sigma = \tau\mu$ for some $\mu \in \mathrm{G}(K/E)$. Then

$$\sigma|_E = (\tau\mu)|_E = \tau_{\mathrm{Im}(\mu|_E)}\mu|_E = \tau|_E\,\mathrm{id} = \tau|_E.$$

$\Longleftarrow$ Assume that $\sigma|_E = \tau|_E$. Then $\tau^{-1}\sigma \in \mathrm{Aut}(K)$ and

$$(\tau^{-1}\sigma)|_E = \tau^{-1}|_{\mathrm{Im}(\sigma|_E)}\sigma|_E = \tau^{-1}|_{\mathrm{Im}(\tau|_E)}\tau|_E = \mathrm{id}_E\,.$$

Thus, $\tau^{-1}\sigma \in \mathrm{G}(K/E)$. □

Corollary 2.61. Let K be a finite normal extension of F and $F \leqslant E \leqslant K \leqslant \overline{F}$. Then we have a bijection

$$\begin{aligned} \varphi : \mathrm{G}(K/F)/\!/\,\mathrm{G}(K/E) &\longrightarrow \left\{\sigma \;\middle|\; \sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F} \text{ and } \sigma|_F = \mathrm{id}\right\} \\ \overline{\sigma} := \sigma\,\mathrm{G}(K/E) &\longmapsto \sigma|_E. \end{aligned}$$

If E is also a splitting field over F, then we have a bijection

$$\begin{aligned} \varphi : \mathrm{G}(K/F)/\!/\,\mathrm{G}(K/E) &\longrightarrow \mathrm{G}(E/F) \\ \overline{\sigma} := \sigma\,\mathrm{G}(K/E) &\longmapsto \sigma|_E. \end{aligned}$$

Proof. Theorem 2.60 shows that φ is a well-defined 1-1 map. Let $\sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F}$ be with $\sigma|_F =$ id. Since $K \supseteq E$ is an algebraic extension, by Theorem 2.19 we can extend σ to $\tau : K \xrightarrow{\cong} \tau(K) \subseteq \overline{F}$ such that $\tau|_E = \sigma$. Note that $\tau|_F = (\tau|_E)|_F = \sigma|_F = \mathrm{id}$. Then by Corollary 2.35, $\tau \in \mathrm{G}(K/F)$. Since $\varphi(\overline{\tau}) = \tau|_R = \sigma$, we have that φ is onto.

If E is a splitting field over F, then by the proof of Corollary 2.35,

$$\left\{\sigma \;\middle|\; \sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F} \text{ and } \sigma|_F = \mathrm{id}\right\} = \mathrm{G}(E/F).$$ □

Remark. E is a finite normal extension of F if and only if $\mathrm{G}(K/E) \trianglelefteq \mathrm{G}(K/F)$. In this case, we have a group isomorphism

$$\begin{aligned} \varphi : \mathrm{G}(K/F)/\,\mathrm{G}(K/E) &\longrightarrow \mathrm{G}(E/F) \\ \overline{\sigma} := \sigma\,\mathrm{G}(K/E) &\longmapsto \sigma|_E. \end{aligned}$$

Example 2.62.

Definition 2.63. If K is a finite normal extensionf of a field F, then $\mathrm{G}(K/F)$ is the *Galois group of K over F.*

Theorem 2.64 (Main Theorem 1 of Galois Theory)**.** *Let K be a finite normal extension of a field F. Then we have a 1-1 correspondence:*

$$\{E \mid F \leqslant E \leqslant K\} \rightleftharpoons \{H \mid H \leqslant \mathrm{G}(K/F)\}$$
$$E \overset{\lambda}{\longmapsto} \mathrm{G}(K/E)$$
$$K_H \overset{\gamma}{\longleftarrow\!\!\!\shortmid} H$$

Proof. It is straightforward to show that φ is well-defined.

We then show that for E with $F \leqslant E \leqslant K$, $\gamma \circ \lambda(E) = E$, i.e., $K_{\mathrm{G}(K/E)} = E$.

$\supseteq$ follows from Theorem 2.17.

$\subseteq$ It is equivalent to show that $K \smallsetminus E \subseteq K \smallsetminus K_{\mathrm{G}(K/E)}$. Let $\alpha \in K \smallsetminus E$. Since $K \supseteq F$ is a finite normal extension, we have that $K \supseteq E$ is a finite normal extension by Theorem 2.60. Hence $\mathrm{irr}(\alpha, E)$ is separable, so there is a zero $\beta \in \mathrm{irr}(\alpha, E)$ with $\beta \neq \alpha$. Let $\psi_{\alpha,\beta} : E(\alpha) \to E(\beta)$ be the conjugation isomorphism. By isomorphism extension theorem, $\psi_{\alpha,\beta}$ can be extended to an isomorphism $\tau : K \to \tau(K) \subseteq \overline{E}$ such that $\tau|_{E(\alpha)} = \psi_{\alpha,\beta}$. Since $K \supseteq E$ is a finite normal extension, $\tau \in \mathrm{G}(K/E)$ by Corollary 2.35. However, $\tau(\alpha) = \psi_{\alpha,\beta}(\alpha) = \beta \neq \alpha$, so

$$\alpha \notin \{a \in K \mid \sigma(a) = a, \forall \sigma \in \mathrm{G}(K/E)\} = K_{\mathrm{G}(K/E)}.$$

Finally, we show that for H with $H \leqslant \mathrm{G}(K/F)$, $\lambda \circ \gamma(H) = H$, i.e., $\mathrm{G}(K/K_H) = H$.

$\supseteq$ Let $\tau \in H \leqslant \mathrm{G}(K/F)$. Then $\tau \in \mathrm{Aut}(K)$. Since $K_H = \{a \in K \mid \sigma(a) = a, \forall \sigma \in H\}$, we have that $\tau|_{K_H} = \mathrm{id}$. Thus, $\tau \in \mathrm{G}(K/K_H)$.

$\subseteq$ Suppose that $H < \mathrm{G}(K/K_H)$. Since $K \supseteq F$ is a finite normal extension and $F \leqslant K_H \leqslant K$, we have that $K \supseteq K_H$ is a finite normal extension by Theorem 2.60. Then

$$|H| < |\mathrm{G}(K/K_H)| = \{K : K_H\} = [K : K_H].$$

Also, $K = K_H(\alpha)$ for some $\alpha \in K$ by Theorem 2.55. Assume that $H = \{\sigma_1, \dots, \sigma_{|H|}\}$ and consider the polynomial

$$f(x) = \prod_{i=1}^{|H|}(x - \sigma_i(\alpha)) \in K[x].$$

Now the coefficients of each power of x in $f(x)$ are symmetric expressions in the $\sigma_i(\alpha)$. Let $\sigma \in H$. Then we can replace each σ_i with $\sigma\sigma_i$ for each occuring σ_i in the coefficients of all terms in f, resulting in

$$\prod_{i=1}^{|H|}(x - (\sigma\sigma_i)(\alpha)) = \prod_{i=1}^{|H|}(x - \sigma_i(\alpha)) = f(x).$$

Since σ is a field homomorphism, each coefficient in the term of $\prod_{i=1}^{|H|}(x - (\sigma\sigma_i)(\alpha))$ can be written $\sigma(a)$, where a is the coefficient of the corresponding term in $\prod_{i=1}^{|H|}(x - \sigma_i(\alpha))$. Hence these coefficients are invariant under each $\sigma_i \in H$, so $f \in K_H[x]$. Since $H \leqslant \mathrm{G}(K/F)$, we have that $\sigma_i = \mathrm{id}$ for some $i \in \{1, \dots, |H|\}$. Hence $\sigma_i(\alpha) = \alpha$, and so $f(\alpha) = 0$. Therefore we would have

$$\deg(\alpha, K_H) \leqslant \deg(f) = |H| < [K : K_H] = [K_H(\alpha) : K_H] = \deg(\alpha, K_H),$$

which is impossible. □

Theorem 2.65 (Main Theorem 2 of Galois Theory)**.** *Let K be a finite normal extension of a field F. Then*

(a) $[K:E] = |\mathrm{G}(K/E)|$ *and* $[E:F] = |\mathrm{G}(K/F)//\,\mathrm{G}(K/E)|$.

(b) E *is a finite normal extension of* F *if and only if* $\mathrm{G}(K/E) \trianglelefteq \mathrm{G}(K/F)$*. In this case,*

$$\mathrm{G}(E/F) \cong \mathrm{G}(K/F)/\,\mathrm{G}(K/E).$$

(c) The diagram of subgroups of $\mathrm{G}(K/F)$ *is the inverted diagram of intermediate fields of* K *over* F.

Proof. (a) Since K is a finite normal extension of E, $[K:E] = \{K:E\} = |\mathrm{G}(E/F)|$ by Deffinition 2.45 and Corollary 2.35. Since K is a separable extension over F, E is a separable extension over F by Corollary 2.50. Then

$$[E:F] = \{E:F\} = \left\{\sigma \;\middle|\; \sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F} \text{ and } \sigma|_F = \mathrm{id}\right\}.$$

Since K is a finite normal extension of F and $F \leqslant E \leqslant K \leqslant \overline{F}$, by Corollary 2.61

$$\left\{\sigma \;\middle|\; \sigma : E \xrightarrow{\cong} \sigma(E) \subseteq \overline{F} \text{ and } \sigma|_F = \mathrm{id}\right\} = |\mathrm{G}(K/F)//\,\mathrm{G}(K/E)|.$$

Thus, $[E:F] = |\mathrm{G}(K/F)//\,\mathrm{G}(K/E)|$.

(b) We showed that E is a finite separable extension of F. So it is equivalent to show that E is a splitting field over F if and only if $\mathrm{G}(K/E) \trianglelefteq \mathrm{G}(K/F)$. Since K is normal over F, every isomorphism $\sigma : E \to \sigma(E) \subseteq \overline{F}$ can be extended to $\tau \in \mathrm{G}(K/F)$ with $\tau|_E = \sigma$. Hence $\mathrm{G}(K/F)$ induces all possible isomorphisms of E onto a subfield of $\overline{F}$ leaving F fixed. Thus, by Theorem 2.31 E is a splitting field over F if and only if for all $\sigma \in \mathrm{G}(K/F)$, $\sigma|_E \in \mathrm{G}(E/F)$. Since $E = E_{\mathrm{G}(K/E)}$ by Theorem 2.64,

$$\begin{aligned}
&\forall \sigma \in \mathrm{G}(K/F), \sigma|_E \in \mathrm{G}(E/F)\\
\Longleftrightarrow\; &\forall \sigma \in \mathrm{G}(K/F), \tau \circ \sigma|_E = \sigma|_E, \forall \tau \in \mathrm{G}(K/E)\\
\Longleftrightarrow\; &\sigma^{-1}\tau\sigma|_E = \mathrm{id}, \forall \sigma \in \mathrm{G}(K/F) \text{ and } \forall \tau \in \mathrm{G}(K/E)\\
\Longleftrightarrow\; &\sigma^{-1} \circ \tau \circ \sigma \in \mathrm{G}(K/E), \forall \sigma \in \mathrm{G}(K/F) \text{ and } \forall \tau \in \mathrm{G}(K/E)\\
\Longleftrightarrow\; &\mathrm{G}(K/E) \trianglelefteq \mathrm{G}(K/F).
\end{aligned}$$

Assume that E is a finite normal extension of F. Then for $\sigma \in \mathrm{G}(K/F)$, $\sigma|_E \in \mathrm{G}(E/F)$. We have a group homomorphism

$$\begin{aligned}
\phi : \mathrm{G}(K/F) &\longrightarrow \mathrm{G}(E/F)\\
\sigma &\longmapsto \sigma|_E.
\end{aligned}$$

Let $\tau \in \mathrm{G}(E/F)$. Then τ can be extend to $\tau' \in \mathrm{G}(K/F)$ with $\tau'|_E = \tau$ since $K \supseteq F$ is a splitting extension. So ϕ is onto. Note that

$$\mathrm{Ker}(\phi) = \left\{\sigma \in \mathrm{G}(K/F) \;\middle|\; \sigma|_E = \mathrm{id}\right\} = \mathrm{G}(K/E).$$

Therefore, by the Fundamental Isomorphism Theorem,

$$\mathrm{G}(E/F) \cong \mathrm{G}(K/F)/\,\mathrm{G}(K/E).$$

□