

# 5 | Field Theory

In Section 2.6, we learn about extensions of a field. Here, we give more details on a construction of extension fields. We prepare the readers to Galois theory which yields a connection between field theory and group theory. Applications of Galois theory are provided in proving fundamental theorem of algebra, finite fields, and cyclotomic fields. We discuss some results on a transcendental extension in the final section.

## 5.1 Preliminary Results

**5.1.1 Definition.** Let  $F$  be a field. The intersection of all subfields of  $F$  is the smallest subfield of  $F$ , called the **prime field** of  $F$ .

Recall that the characteristic of a field is 0 or a prime  $p$ .

**5.1.2 Theorem.** Let  $F$  be a field with the prime subfield  $P$  and  $1_F$  denote the identity of  $F$ . Then  
 (1) If  $\text{char } F = p$ , a prime, then  $P = \{n \cdot 1_F : n = 0, 1, \dots, p-1\} \cong \mathbb{Z}_p$ .  
 (2) If  $\text{char } F = 0$ , then  $P = \{(m \cdot 1_F)(n \cdot 1_F)^{-1} : m, n \in \mathbb{Z}, n \neq 0\} \cong \mathbb{Q}$ .

*Proof.* Since  $P$  is a field,  $1_F \in P$ , so  $\{n \cdot 1_F : n \in \mathbb{Z}\} \subseteq P$ . Define  $\varphi : \mathbb{Z} \rightarrow P$  by  $\varphi(n) = n \cdot 1_F$  for all  $n \in \mathbb{Z}$ . Then  $\varphi$  is a ring homomorphism and  $\text{im } \varphi = \{n \cdot 1_F : n \in \mathbb{Z}\}$ , so  $\mathbb{Z}/\ker \varphi \cong \text{im } \varphi$ .

(1) Assume that  $\text{char } F = p$  is a prime. Then  $\text{im } \varphi = \{n \cdot 1_F : n = 0, 1, \dots, p-1\}$  and  $p$  is the smallest positive integer such that  $p \in \ker \varphi$ , so  $\ker \varphi = p\mathbb{Z}$ . Hence,  $\text{im } \varphi \cong \mathbb{Z}/p\mathbb{Z}$  which is a field, so  $P = \text{im } \varphi \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ .

(2) Assume that  $\text{char } F = 0$ . Then  $\varphi$  is a monomorphism. Since  $\{n \cdot 1_F : n \in \mathbb{Z}\} \subseteq P$  and  $P$  is a subfield of  $F$ ,  $\{(m \cdot 1_F)(n \cdot 1_F)^{-1} : m, n \in \mathbb{Z}, n \neq 0\} \subseteq P$ . Define  $\bar{\varphi} : \mathbb{Q} \rightarrow P$  by  $\bar{\varphi}(m/n) = \varphi(m)\varphi(n)^{-1}$  for all  $m, n \in \mathbb{Z}, n \neq 0$ . Then  $\bar{\varphi}$  is a monomorphism and  $\bar{\varphi}|_{\mathbb{Z}} = \varphi$ . Thus,  $\mathbb{Q} \cong \text{im } \bar{\varphi} = \{(m \cdot 1_F)(n \cdot 1_F)^{-1} : m, n \in \mathbb{Z}, n \neq 0\}$  which is a subfield of  $P$ , and hence they are equal.  $\square$

**5.1.3 Definition.** A field  $K$  is said to be an **extension** of a field  $F$  if  $F$  is a subring of  $K$ .

**5.1.4 Definition.** Let  $K$  be an extension field of  $F$ . The **degree** of  $K$  over  $F$ ,  $[K : F]$ , is the dimension of  $K$  as a vector space over  $F$ . More generally, if a field  $F$  is a subring of a ring  $R$ , then  $[R : F]$  is the dimension of  $R$  as a vector space over  $F$ .

For example,  $[\mathbb{C} : \mathbb{R}] = 2$  and  $[\mathbb{R} : \mathbb{Q}]$  is infinite (in fact  $[\mathbb{R} : \mathbb{Q}] = |\mathbb{R}|$ ).

**5.1.5 Theorem.** If  $[L : K]$  and  $[K : F]$  are finite, then  $[L : F]$  is finite and

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

In fact,  $[L : F] = [L : K][K : F]$  whenever  $F \subseteq K \subseteq L$ .

*Proof.* With  $F \subseteq K \subseteq L$ , let  $\{\beta_j\}_{j \in J}$  be a basis of  $K$  over  $F$  and  $\{\alpha_i\}_{i \in I}$  be a basis of  $L$  over  $K$ . Every element of  $L$  can be written uniquely as a linear combination of the elements of  $\{\alpha_i\}_{i \in I}$  with coefficients in  $K$ , and every such coefficient can be written uniquely as a linear combination of the elements of  $\{\beta_j\}_{j \in J}$  with coefficients in  $F$ . Hence, every element of  $L$  can be written uniquely as a linear combination of the elements of  $\{\alpha_i \beta_j\}_{i \in I, j \in J}$  with coefficients in  $F$ ,  $\{\alpha_i \beta_j\}_{i \in I, j \in J}$  is a basis of  $L$  over  $F$ , and so  $[L : F] = |I \times J| = [L : K][K : F]$ .  $\square$

Let  $K$  be an extension field of  $F$ .

(1) If  $t_1, \dots, t_n$  are indeterminates over  $F$ , then  $F(t_1, \dots, t_n)$  denotes the field of quotients of the polynomial ring  $F[t_1, \dots, t_n]$ .

(2) If  $u_1, \dots, u_n \in K$  (or  $S \subseteq K$ ), then  $F[u_1, \dots, u_n]$  (or  $F[S]$ ) denotes the subring of  $K$  generated by  $F$  and  $u_1, \dots, u_n$  (or  $S$ ), and  $F(u_1, \dots, u_n)$  (or  $F(S)$ ) denotes its field of quotients.

**5.1.6 Theorem.** Let  $K$  be a field extension of a field  $F$  and let  $u \in K$ . Then EITHER  
 (a)  $[F(u) : F]$  is infinite and  $F[u] \cong F[t]$ , so  $F(u) \cong F(t)$  where  $t$  is an indeterminate OR  
 (b)  $[F(u) : F]$  is finite and  $F[u] = F(u)$ .

*Proof.* Let  $t$  be an indeterminate and consider the ring homomorphism

$$F[t] \xrightarrow{\varphi} K$$

defined by  $\varphi(t) = u$  (or  $\varphi(f(t)) = f(u)$ ). Note that the kernel of  $\varphi$  is a prime ideal, since the image of  $\varphi$  has no zero divisors. There are two possibilities.

(1)  $\ker \varphi = 0$ . Then we have (a).

(2)  $\ker \varphi \neq 0$ . Then  $\ker \varphi = F[t]g(t)$  where  $g(t)$  is a monic prime (i.e., irreducible) polynomial. Since  $F[t]$  is a PID,  $F[t]g(t)$  is a maximal ideal. Thus,

$$F[u] \cong F[t]/F[t]g(t)$$

is a field, so  $F[u] = F(u)$ .  $\square$

**5.1.7 Remarks.** 1. If  $g(t) = g_0 + g_1 t + \dots + g_{n-1} t^{n-1} + t^n$ , then  $[F(u) : F] = n$  and  $\{1, u, \dots, u^{n-1}\}$  is a basis for  $F(u)$  over  $F$ .

2. Consider  $\mathbb{R} \subset \mathbb{C}$  and  $g(t) = g_0 + g_1 t + t^2 \in \mathbb{R}[t]$ . We distinguish three cases.

(a) If  $g_1^2 - 4g_0 > 0$ , then  $g(t) = (t - a)(t - b)$  where  $a, b \in \mathbb{R}$ ,  $a \neq b$  and  $\mathbb{R}[t]/\mathbb{R}[t]g(t)$  is a ring without nonzero nilpotent elements.

(b) If  $g_1^2 - 4g_0 = 0$ , then  $g(t) = (t - a)^2$  and  $\mathbb{R}[t]/\mathbb{R}[t]g(t)$  is a ring with nonzero nilpotent elements.

(c) If  $g_1^2 - 4g_0 < 0$ , then  $\mathbb{R}[t]/\mathbb{R}[t]g(t) \cong \mathbb{C}$ .

3. If  $p$  is a prime, then  $t^2 - p$  is irreducible over  $\mathbb{Q}$  and the fields  $\mathbb{Q}[\sqrt{p}] \cong \mathbb{Q}[t]/(t^2 - p)$  are all distinct.

**5.1.8 Definition.** Let  $K$  be an extension field of a field  $F$ . An element  $u \in K$  is **algebraic** over  $F$  in case there exists a nonzero polynomial  $f(t) \in F[t]$  such that  $f(u) = 0$  and **transcendental** over  $F$  otherwise.

For example, every complex number is algebraic over  $\mathbb{R}$ ;  $\sqrt[3]{2}$  and  $1 + \sqrt{5} \in \mathbb{R}$  are algebraic over  $\mathbb{Q}$ . It has been proved that  $e$  and  $\pi \in \mathbb{R}$  are transcendental over  $\mathbb{Q}$ ; it can be shown that most of real numbers are in fact transcendental over  $\mathbb{Q}$  (see Exercises). Theorem 5.1.6 yields characterizations of algebraic and transcendental elements:

**5.1.9 Corollary.** Let  $K$  be an extension field of a field  $F$  and  $u \in K$ . The following conditions on  $u$  are equivalent:

- (i)  $u$  is transcendental over  $F$  (if  $f(t) \in F[t]$  and  $f(u) = 0$ , then  $f = 0$ );
- (ii)  $F(u) \cong F(t)$ ;
- (iii)  $[F(u) : F]$  is infinite.

**5.1.10 Corollary.** Let  $K$  be an extension field of a field  $F$  and  $u \in K$ . The following conditions on  $u$  are equivalent:

- (i)  $u$  is algebraic over  $F$  (there exists a polynomial  $0 \neq f(t) \in F[t]$  such that  $f(u) = 0$ );
- (ii) there exists a monic irreducible polynomial  $g(t) \in F[t]$  such that  $g(u) = 0$ ;
- (iii)  $[F(u) : F]$  is finite.

Moreover, in part (ii), we have  $g(t)$  is unique;  $f(u) = 0$  if and only if  $g(t)$  divides  $f(t)$ ;  $F(u) \cong F[t]/(g(t))$ ; and  $[F(u) : F] = \deg g(t)$ .

**5.1.11 Definition.** When  $u$  is algebraic over  $F$ , the unique monic irreducible polynomial  $g(t) \in F[t]$  in part (ii) is the **minimal polynomial of  $u$** . The **degree of  $u$  over  $F$**  is  $\deg g(t)$ .

**5.1.12 Definition.** An extension field  $K$  of a field  $F$  is **algebraic** in case every element of  $K$  is algebraic over  $F$ .

For example,  $\mathbb{C}$  is an algebraic extension of  $\mathbb{R}$ , but  $\mathbb{R}$  is not algebraic over  $\mathbb{Q}$ . Note that if  $[K : F]$  is finite, then  $K$  is algebraic extension.

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

**5.1.14 Theorem.** If  $L$  is an algebraic extension of  $K$  and  $K$  is an algebraic extension of  $F$ , then  $L$  is algebraic extension over  $F$ .

*Proof.* Let  $u \in L$ . Since  $L$  is algebraic over  $K$ , there exists  $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$  such that  $f(u) = 0$ . Since  $K$  is algebraic over  $F$ ,  $a_0, a_1, \dots, a_n$  are algebraic over  $F$ , so  $[F(a_0, a_1, \dots, a_n) : F]$  is finite. For, let  $E = F(a_0, a_1, \dots, a_n)$ . Then

$$[E : F] = [F(a_0) : F] \prod_{i=1}^n [F(a_0, a_1, \dots, a_i) : F(a_0, a_1, \dots, a_{i-1})],$$

$a_0$  is algebraic over  $F$  and  $a_i$  is algebraic over  $F(a_0, \dots, a_{i-1})$  for all  $i \in \{1, \dots, n\}$ . Since  $f(x) \in E[x]$ ,  $u$  is algebraic over  $E$ , so  $[E(u) : E]$  is finite by Corollary 5.1.10. Thus,

$$[F(u) : F] \leq [E(u) : F] = [E(u) : E][E : F] < \infty.$$

Hence,  $u$  is algebraic over  $F$ . □

**5.1.15 Corollary.** For  $a, b \in K$ , if  $a$  and  $b$  are algebraic over  $F$  of degree  $m$  and  $n$ , respectively, then  $a \pm b$ ,  $ab$  and  $a/b$  (if  $b \neq 0$ ) are all algebraic over  $F$  of degree  $\leq mn$ . In other words,

$$A = \{u \in K : u \text{ is algebraic over } F\}$$

is a subfield of  $K$  and is an algebraic extension over  $F$ .

*Proof.* By Corollary 5.1.10,  $[F(a) : F] = m$  and  $[F(b) : F] = n$ . Since  $b$  is algebraic over  $F$ ,  $b$  is algebraic over  $F(a)$ , so  $[F(a)(b) : F(a)] \leq n$ . Thus, by Theorem 5.1.5,  $[F(a, b) : F] = [F(a)(b) : F] = [F(a)(b) : F(a)][F(a) : F] \leq mn$ . Since  $a \pm b, ab, ab^{-1}$  (if  $b \neq 0$ ) are in  $F(a, b)$  which is a finite extension, they are all algebraic over  $F$  of degree  $\leq mn$ .  $\square$

- 5.1 Exercises.**
1. Let  $E = \mathbb{Q}(u)$  where  $u^3 - u^2 + u + 2 = 0$ . Express  $(u^2 + u + 1)(u^2 - u)$  and  $(u - 1)^{-1}$  in the form  $au^2 + bu + c$  where  $a, b, c \in \mathbb{Q}$ .
  2. Let  $E$  be an algebraic extension of a field  $F$ . Show that any subring of  $E/F$  is a subfield. Hence, prove that any subring of a finite dimensional extension field  $E/F$  is a subfield.
  3. Let  $u$  and  $v$  be positive irrational numbers such that  $u$  is algebraic over  $\mathbb{Q}$  and  $v$  is transcendental over  $\mathbb{Q}$ .
    - (a) Show that  $v$  is transcendental over  $\mathbb{Q}[u]$ .
    - (b) Classify whether the following elements are algebraic or transcendental over  $\mathbb{Q}$ .
      - (i)  $\frac{1}{u+v}$
      - (ii)  $\sqrt{u}$
      - (iii)  $\sqrt{v}$
  4. Let  $E = F(u)$ ,  $u$  transcendental and let  $K \neq F$  a subfield of  $E/F$ . Show that  $u$  is algebraic over  $K$ .
  5. (a) Show that there are countably many irreducible polynomials in  $\mathbb{Q}[x]$ .  
 (b) Let  $A$  be the set of all real numbers that are algebraic over  $\mathbb{Q}$ . Show that  $A$  is countable, so that  $\mathbb{R} \setminus A$  is uncountable.
  6. Let  $K$  be a field. A map  $D : K \rightarrow K$  is called a **derivation** if  $D(u + v) = D(u) + D(v)$  and  $D(uv) = uD(v) + D(u)v$  for all  $u, v \in K$ .
    - (a) Show that  $D(1) = D(0) = 0$ ,  $D(x - y) = D(x) - D(y)$  and that the set of element  $x \in K$  such that  $D(x) = 0$  forms a subfield  $M$  of  $K$ .
    - (b) If  $[K : M]$  is finite, prove that  $\text{char } K = p > 0$  and for every  $u \in K$  there are  $m \in M$  and  $i \in \mathbb{N} \cup \{0\}$  such that  $u^{p^i} - m = 0$ .
  7. Let  $E_1$  and  $E_2$  be subfields of a field  $K$ . The **composite field** of  $E_1$  and  $E_2$ , denoted by  $E_1E_2$ , is the smallest subfield of  $K$  containing both  $E_1$  and  $E_2$ . Prove that if  $[K : F]$  is finite, then  $[E_1E_2 : F] \leq [E_1 : F][E_2 : F]$ .

## 5.2 Splitting Fields

Let  $F$  be a field. Given a polynomial  $f(x) \in F[x]$  we would like to have at hand an extension field  $E$  of  $F$  which in some sense contains all the roots of the equation  $f(x) = 0$ . We recall that  $f(r) = 0$  if and only if  $f(x)$  is divisible by  $x - r$ .

**5.2.1 Definition.** We say that  $f(x)$  **splits** in an extension field  $E$  if  $f(x) = \prod_{i=1}^n c(x - r_i)$ , that is, it is a product of linear factors in  $E[x]$  and  $c \in F$ .

We shall first study some facts about the roots of  $f(x) \in F[x]$  as follows.

**5.2.2 Theorem.** If  $f(x) \in F[x]$  and  $\deg f(x) = n \geq 1$ , then  $f(x)$  can have at most  $n$  roots counting multiplicities in any extension field of  $F$ .

*Proof.* We shall prove the theorem by induction on the degree of  $f(x)$ . If  $\deg f(x) = 1$ , then  $f(x) = ax + b$  for some  $a, b \in F$  and  $a \neq 0$ . Then  $-b/a$  is the unique root of  $f(x)$  and  $-b/a \in F$ , so we are done.

Let  $\deg f(x) = n > 1$  and assume that the result is true for all polynomials of degree  $< n$ . Let  $E$  be any extension field of  $F$ . If  $f(x)$  has no roots in  $E$ , then we are done. Let  $r \in E$  be a root of  $f(x)$  of multiplicity  $m \geq 1$ . Then there exists  $q(x) \in E[x]$  such that  $f(x) = (x - r)^m q(x)$  and  $q(r) \neq 0$ . Thus,  $\deg q(x) = n - m$ . By the inductive hypothesis  $q(x)$  has at most  $n - m$  roots in  $E$  counting multiplicities. Hence,  $f(x)$  has at most  $m + (n - m)$  roots in  $E$  counting multiplicities.  $\square$

**5.2.3 Theorem.** [Kronocker] *If  $p(t) \in F[t]$  is irreducible over  $F$ , then there exists an extension field  $E$  of  $F$  such that  $[E : F] = \deg p(t)$  and  $p(t)$  has a root in  $E$ .*

*Proof.* Let  $E = F[x]/(p(x))$  where  $x$  is an indeterminate. Then  $E$  is a field containing  $\{a + (p(x)) : a \in F\}$  as a subfield. But  $F \cong \{a + (p(x)) : a \in F\}$  by  $\varphi : a \mapsto a + (p(x))$ , so  $E$  can be considered as an extension field of  $F$  by considering  $a$  as  $a + (p(x))$  for all  $a \in F$ . Then  $E = F[x]/(p(x)) = F(\bar{t})$  where  $\bar{t} = x + (p(x))$  is a root of  $p(t)$ . Since  $E = F(\bar{t})$  and  $p(t)$  is irreducible over  $F$ ,  $[E : F] = [F(\bar{t}) : F] = \deg p(t)$  by Corollary 5.1.10.  $\square$

**5.2.4 Corollary.** *If  $p(t) \in F[t]$  is a nonconstant polynomial, then there exists a finite extension field  $E$  of  $F$  containing a root of  $p(t)$  and  $[E : F] \leq \deg p(t)$ .*

*Proof.* Since  $F[t]$  is a UFD,  $p(t)$  has an irreducible factor in  $F[t]$  say  $p_1(t)$ . By Theorem 5.2.3, there exists an extension field  $E$  of  $F$  such that  $E$  contains a root of  $p_1(t)$  and  $[E : F] = \deg p_1(t)$ . Hence,  $[E : F] \leq \deg p(t)$  and  $E$  contains a root of  $p(t)$ .  $\square$

**5.2.5 Definition.** Let  $F$  be a field and  $f(x)$  a monic polynomial in  $F[x]$ . An extension field  $E$  of  $F$  is a **splitting field** of  $f(x)$  over  $F$  if

$$f(x) = (x - r_1) \cdots (x - r_n)$$

in  $E[x]$  and

$$E = F(r_1, \dots, r_n),$$

that is,  $E$  is generated by the roots of  $f(x)$ .

The next results demonstrate the existence of a splitting field for a monic polynomial.

**5.2.6 Theorem.** [Existence of Splitting Fields] *Let  $f(x)$  be a monic polynomial of degree  $n \geq 1$ . Then there exists an extension field  $E$  of  $F$  such that  $[E : F] \leq n!$  and  $E$  contains  $n$  roots of  $f(x)$  counting multiplicities. Hence, in  $E[t]$ ,  $f(x) = c(x - r_1) \cdots (x - r_n)$  for some  $c \in F$  and  $r_1, \dots, r_n \in E$ , so that  $r_1, \dots, r_n$  are  $n$  roots of  $f(x)$  in  $E$ .*

*Proof.* We shall prove the theorem by induction on the degree of  $f(x)$ . If  $\deg f(x) = 1$ , then  $f(x)$  has exactly one root in  $F$  and  $[F : F] = 1 = 1!$ .

Let  $\deg f(x) = n > 1$  and assume that the theorem is true for the case of polynomials of degree  $< n$ . By Corollary 5.2.4, there exists an extension field  $E_0$  of  $F$  such that  $f(x)$  has a root, say  $r \in E_0$  and  $[E_0 : F] \leq n$ . Since  $r$  is a root of  $f(x)$ ,  $f(x) = (x - r)q(x)$  for some  $q(x) \in E_0[x]$ , so  $\deg q(x) = n - 1$ . By the inductive hypothesis, there exists an extension field  $E$  of  $E_0$  such that  $[E : E_0] \leq (n - 1)!$  and  $E$  contains  $n - 1$  roots of  $q(x)$ . Then  $E$  is an extension field of  $F$ ,  $[E : F] = [E : E_0][E_0 : F] \leq n!$  and  $E$  contains  $n$  roots of  $f(x)$  counting multiplicities.  $\square$

**5.2.7 Corollary.** *Let  $F$  be a field and  $f(x)$  a nonconstant polynomial over  $F$  of degree  $n$ . Then there exists a splitting field  $E$  of  $f(x)$  over  $F$ . Moreover,  $[E : F] \leq n!$ .*

*Proof.* We have seen from Theorem 5.2.6 that there exists an extension field  $E$  of  $F$  such that  $f(x) = c(x - r_1) \cdots (x - r_n)$ , for some  $c \in F$  and  $r_1, \dots, r_n \in E$ , is a product of linear factors in  $E[x]$  and  $[E : F] \leq n!$ . Hence,  $E = F(r_1, \dots, r_n)$  is a desired field.  $\square$

**5.2.8 Examples** (Examples of splitting fields). 1. Let  $f(x) = x^2 + ax + b$ . If  $f(x)$  is reducible in  $F[x]$  ( $F$  arbitrary) then  $F$  is a splitting field. Otherwise, put  $E = F[x]/(f(x)) = F(r_1)$  where  $r_1 = x + (f(x))$ . Then  $E$  is a splitting field since  $f(r_1) = 0$ , so  $f(x) = (x - r_1)(x - r_2)$  in  $E[x]$ . Thus,  $E = F(r_1) = F(r_1, r_2)$ . Since  $f(x)$  is the minimal polynomial of  $r_1$  over  $F$ ,  $[E : F] = 2$ .

2. Let the base field  $F$  be  $\mathbb{Z}/(2)$ , the field of two elements, and let  $f(x) = x^3 + x + 1$ . Since  $1+1+1 \neq 0$  and  $0+0+1 \neq 0$ ,  $f(x)$  has no roots in  $F$ ; hence  $f(x)$  is irreducible in  $F[x]$ . Put  $r_1 = x + (f(x))$  in  $F[x]/(f(x))$  so  $F(r_1)$  is a field and  $x^3 + x + 1 = (x + r_1)(x^2 + ax + b)$  in  $F(r_1)[x]$ . (Note that we can write  $+$  for  $-$  since characteristic is two.) Comparison of coefficients shows that  $a = r_1$ ,  $b = 1 + r_1^2$ . The elements of  $F(r_1)$  can be listed as  $c + dr_1 + er_1^2$ ,  $c, d, e \in F$ . There are eight of these:  $0, 1, r_1, 1+r_1, r_1^2, 1+r_1^2, r_1+r_1^2$  and  $1+r_1+r_1^2$ . Substituting these in  $x^2 + r_1x + 1 + r_1^2$ , we reach  $(r_1^2)^2 + r_1(r_1^2) + 1 + r_1^2 = r_1^4 + r_1^3 + 1 + r_1^2 = 0$  since  $r_1^3 = r_1 + 1$  and  $r_1^4 = r_1^2 + r_1$ . Hence,  $x^2 + ax + b$  factors into linear factors in  $F(r_1)[x]$  and  $E = F(r_1)$  is a splitting field of  $x^3 + x + 1$  over  $F$ .
3. Let  $F = \mathbb{Q}$ ,  $f(x) = (x^2 - 2)(x^2 - 3)$ . Since the rational roots of  $x^2 - 2$  and  $x^2 - 3$  must be integral, it follows that  $x^2 - 2$  and  $x^2 - 3$  are irreducible in  $\mathbb{Q}[x]$ . Form  $K = \mathbb{Q}(r_1)$ ,  $r_1 = x + (x^2 - 2)$  in  $\mathbb{Q}[x]/(x^2 - 2)$ . The elements of  $K$  have the form  $a + br_1$ ,  $a, b \in \mathbb{Q}$ . We claim that  $x^2 - 3$  is irreducible in  $K[x]$ . Otherwise, we have rational numbers  $a, b$  such that  $(a + br_1)^2 = 3$ . Then  $(a^2 + 2b^2) + 2abr_1 = 3$  so that  $ab = 0$  and  $a^2 + 2b^2 = 3$ . If  $b = 0$  we obtain  $a^2 = 3$  which is impossible since  $\sqrt{3}$  is not rational, and if  $a = 0$ ,  $b^2 = 3/2$ . Then  $(2b^2) = 6$  and since  $\sqrt{6}$  is not rational, we again obtain an impossibility. Thus,  $x^2 - 3$  is irreducible in  $K[x]$ . Now form  $E = K[x]/(x^2 - 3)$ . Then this is a splitting field over  $\mathbb{Q}$  of  $(x^2 - 2)(x^2 - 3)$  and  $[E : \mathbb{Q}] = [E : K][K : \mathbb{Q}] = 2 \cdot 2 = 4$ .
4. Let  $F = \mathbb{Q}$ ,  $f(x) = x^p - 1$ ,  $p$  a prime. We have  $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + x + 1)$  and we know that  $x^{p-1} + x^{p-2} + \dots + x + 1$  is irreducible in  $\mathbb{Q}[x]$ . Let  $E = \mathbb{Q}(z)$  where  $z = x + (x^{p-1} + x^{p-2} + \dots + x + 1)$  in  $\mathbb{Q}[x]/(x^{p-1} + x^{p-2} + \dots + x + 1)$ . We have  $1, z, \dots, z^{p-1}$  are distinct. Also  $(z^k)^p = (z^p)^k = 1$  so every  $z^k$  is a root of  $x^p - 1$ . It follows that  $x^p - 1 = \prod_{k=1}^{p-1} (x - z^k)$  in  $E[x]$ . Thus,  $E$  is a splitting field over  $\mathbb{Q}$  of  $x^p - 1$  and  $[E : \mathbb{Q}] = p - 1$ .
5. Since  $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$  where  $\omega \neq 1$  and  $\omega^3 = 1$ ,  $\mathbb{Q}(\sqrt[3]{2})$  is not a splitting field of  $f(x) = x^3 - 2$  over  $\mathbb{Q}$ . A splitting field of  $f(x)$  is  $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ . Since  $g(x) = x^2 + x + 1$  is irreducible over  $\mathbb{Q}(\sqrt[3]{2})$  and  $g(\omega) = 0$ ,  $[E : \mathbb{Q}(\sqrt[3]{2})] = 2$ , so  $[E : F] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$ .
6. A splitting field over  $\mathbb{Z}/(p)$  of  $x^{p^e} - 1$ ,  $e \in \mathbb{N}$ , is  $\mathbb{Z}/(p)$ .

**5.2.9 Theorem.** [Uniqueness of Splitting Fields] Let  $\eta : F \rightarrow F_1$  be an isomorphism of fields and let  $\eta : F[x] \rightarrow F_1[x]$  be the isomorphism which extends  $\eta$  and satisfies  $\eta(x) = x$ . Suppose  $f(x)$  is a monic polynomial in  $F[x]$ , let  $f_1(x) = \eta(f(x))$  and suppose that  $E/F$  and  $E_1/F_1$  are splitting fields of  $f(x)$  and  $f_1(x)$ , respectively. Then there exists an isomorphism  $\eta^* : E \rightarrow E_1$  which extends  $\eta$ .

*Proof.* Let  $\hat{f}(x)$  be an irreducible factor of  $f(x)$  and let  $\hat{f}_1(x) = \eta(\hat{f}(x))$ . Let  $r \in E$  be a root of  $\hat{f}(x)$  and let  $r_1 \in E_1$  be a root of  $\hat{f}_1(x)$ . Then we have a commutative diagram in which the vertical arrows are isomorphisms and the horizontal arrows are inclusion maps

$$\begin{array}{ccccc}
 F & \longrightarrow & F[r] & \longrightarrow & E \\
 \downarrow \eta & & \uparrow i & & \\
 & & F[x]/\hat{f}(x)F[x] & & \\
 & & \downarrow \hat{\eta} & & \\
 & & F_1[x]/\hat{f}_1(x)F_1[x] & & \\
 & & \downarrow j & & \\
 F_1 & \longrightarrow & F_1[r_1] & \longrightarrow & E_1.
 \end{array}$$

The map  $j\hat{\eta}i^{-1} = \bar{\eta}$  is an isomorphism of fields extending  $\eta$ . Also,  $\bar{\eta}(f(x)/(x - r)) = f_1(x)/(x - r_1)$  and  $E/F[r]$ ,  $E_1/F_1[r_1]$  are splitting fields of  $f(x)/(x - r)$  and  $f_1(x)/(x - r_1)$ , respectively.

Now, by induction on  $\deg f(x)$ ,  $\bar{\eta} : F[r] \rightarrow F_1[r_1]$  has an extension to  $\eta^* : E \rightarrow E_1$  and this is the required extension of  $\eta$ .  $\square$

**5.2.10 Theorem.** Assume  $f(x)$  has no multiple factors as an element of  $F[x]$ . Under the hypothesis of Theorem 5.2.9, the number of distinct extensions of  $\eta : F \rightarrow F_1$  to  $\eta : E \rightarrow E_1$  is at most  $[E : F]$ . Moreover, the number of distinct extensions is equal to  $[E : F]$  if and only if  $f(x)$  has distinct roots in  $E$ .

*Proof.* Proceeding as in the proof of Theorem 5.2.9, let  $\hat{f}(x)$  be an irreducible factor of  $f(x)$ , let  $d$  be the degree of  $\hat{f}(x)$ , let  $\hat{f}_1(x) = \eta(\hat{f}(x))$ , let  $r_1, \dots, r_e$  be the distinct roots of  $\hat{f}(x)$  in  $E$  and let  $r'_1, \dots, r'_e$  be the roots of  $\hat{f}_1(x)$  in  $E_1$ . (Note that  $e \leq d$  and  $e = d$  if  $\hat{f}_1(x)$  has no multiple roots, but this is not always the case.)

Next fix a root  $r = r_1$  of  $\hat{f}(x)$ . The argument of Theorem 5.2.9 shows that for each root  $r'_1, \dots, r'_e$  of  $\hat{f}_1(x)$  there is an isomorphism  $\hat{\eta}_j : F[r] \rightarrow F_1[r'_j]$  extending  $\eta$ , where  $\hat{\eta}_j(r) = r'_j$ .

$$\begin{array}{ccc} F & \longrightarrow & F[r] \\ \eta \downarrow & & \\ F_1 & \longrightarrow & F_1[r'_j] \hookrightarrow E_1 \end{array}$$

On the other hand, any isomorphism of  $F[r]$  into  $E_1$  must carry  $r$  into a root of  $\hat{f}_1(x)$ , and so must one of the  $\hat{\eta}_j$ . Furthermore, as noted above

$$\text{the number of roots of } \hat{f}(x) = e \leq d = [F[r] : F].$$

By induction, the number of ways each  $\hat{\eta}_j$  can be extended to an isomorphism  $E \rightarrow E_1$  is at most  $[E : F[r]]$ . Thus,

$$\begin{aligned} \text{the number of extensions of } \eta : F \rightarrow F_1 \text{ to } \eta^* : E \rightarrow E_1 \\ \leq e[E : F[r]] \leq [F[r] : F][E : F[r]] = [E : F]. \end{aligned}$$

Now we want to answer the question: When is there equality – that is, the number of extensions =  $[E : F]$ ?

Looking at the first step above we see that the number of roots of  $\hat{f}(x) = e = d = [F[r] : F]$  if and only if  $\hat{f}(x)$  has  $d = \deg \hat{f}(x)$  roots – that is if and only if  $\hat{f}(x)$  has distinct roots.

To continue inductively, we now have the set up

$$\begin{array}{ccc} F[r] & \longrightarrow & E \\ \hat{\eta}_j \downarrow & & \\ F_1[r'_j] & \longrightarrow & E_1 \end{array}$$

The key point is that  $E$  is the splitting field over  $F[r]$  of the polynomial  $f(x)/(x - r)$ . This polynomial has no multiple factor so inductively the number of extensions of  $\hat{\eta}_j$  to an isomorphism  $\eta^* : E \rightarrow E_1$  is equal to  $[E : F[r]]$  if and only if  $f(x)/(x - r)$  has distinct roots. Combining this with the result for  $\hat{f}(x)$  we get the number of extensions of  $\eta : F \rightarrow F_1$  to an isomorphism  $\eta : E \rightarrow E_1$  is equal to  $[E : F]$  if and only if  $f(x)$  has distinct roots in  $E$ .  $\square$

**5.2.11 Remarks.** (1) If  $f(x)$  is an irreducible polynomial over a field  $F$  and  $r$  is a root of  $f(x)$  in some extension field of  $F$ , then

$$F[x]/f(x)F[x] \cong F[r].$$

However, if  $f(x) = g(x)h(x)$  where  $g(x)$  and  $h(x)$  are irreducible polynomials, then by Chinese remainder theorem

$$F[x]/f(x)F[x] \cong F[x]/g(x)F[x] \times F[x]/h(x)F[x]$$

a direct product of fields. If  $f(x) = g(x)^2$ , then  $F[x]/f(x)F[x]$  even has nilpotent elements.

In general,  $E/F$  arises from a succession of simple extensions

$$\begin{aligned} F &\subseteq F_1 \cong F[x]/f_1(x)F[x], \\ F_1 &\subseteq F_2 \cong F_1[x]/f_2(x)F_1[x], \\ &\vdots \\ F_{r-1} &\subseteq F_r \cong F_{r-1}[x]/f_r(x)F_{r-1}[x] = E. \end{aligned}$$

We shall see that in some important cases (but not all), the splitting field  $E/F$  of the polynomial  $f(x)$  can be achieved as a simple extension  $F \subseteq F[x]/g(x)F[x] = E$ , but usually  $g(x) \neq f(x)$ .

(2) If  $f(x)$  and  $g(x)$  have the same roots in some extension field  $E$  of  $F$  ( $f(x), g(x) \in F[x]$ ), then they have the same splitting field. However, one cannot guarantee that the roots of  $f(x)$  are distinct (or simple, or one fold). The basic example is the polynomial

$$f(x) = x^p - a \in F[a]$$

where  $F$  is a field of characteristic  $p > 0$ . If  $r$  is a root of  $f(x)$  in some extension field  $E$  of  $F[a]$ , then  $r^p = a$  and the factorization of  $f(x)$  in  $E[x]$  is

$$f(x) = x^p - a = x^p - r^p = (x - r)^p.$$

- 5.2 Exercises.**
1. Construct a splitting field over  $\mathbb{Q}$  of  $x^5 - 2$ . Find its dimension over  $\mathbb{Q}$ .
  2. Let  $f(x) = x^4 + x^2 + 1$ . Find the splitting field of  $f(x)$  over  $\mathbb{Q}$  and determine its dimension.
  3. Let  $E/F$  be a splitting field of  $f(x)$  over  $F$  and let  $K$  be a subfield of  $E/F$ . Show that any monomorphism of  $K/F$  into  $E/F$  can be extended to an automorphism of  $E$ .
  4. If  $f(x) \in F[x]$  has degree  $n$  and  $K$  is a splitting field of  $f(x)$  over  $F$ , prove that  $[K : F]$  divides  $n!$ .
  5. Let  $F$  be a field of characteristic  $p > 0$  and let  $b \in F$ . Show that either  $x^p - b$  is irreducible in  $F[x]$  or  $b = a^p$  and  $x^p - b = (x - a)^p$  for some  $a \in F$ .

### 5.3 Algebraic Closure of a Field

We know about the *prime field* which is the smallest field such that every other field is an extension of it. However, we does not know if we can algebraically extend our field  $F$  forever to obtain a field that every polynomial in  $F[x]$  has a root in it. We shall assure it in this section.

A field  $F$  is called **algebraically closed** if every monic polynomial  $f(x)$  of positive degree with coefficients in  $F$  has a root in  $F$ .

**5.3.1 Theorem.** *Let  $F$  be a field. The following statements are equivalent.*

- (i)  $F$  is algebraically closed.
- (ii) An irreducible polynomial in  $F[x]$  is linear, and hence every polynomial of  $F[x]$  of positive degree is a product of linear factors.
- (iii)  $F$  has no proper algebraic extension field.

*Proof.* Since  $r$  is a root, that is  $f(r) = 0$ , if and only if  $x - r$  is a factor of  $f(x)$  in  $F[x]$ , we have (i)  $\Leftrightarrow$  (ii). Next, we show (i)  $\Leftrightarrow$  (iii). If  $E$  is an extension field of  $F$  and  $a \in E$  is algebraic over  $F$ , then  $[F(a) : F]$  is the degree of the minimal polynomial  $f(x)$  of  $a$  over  $F$ , and  $f(x)$

is monic and irreducible. Then  $a \in F$  if and only if  $\deg f(x) = 1$ . Hence,  $E$  is algebraic over  $F$  and  $E \supset F$  implies there exist irreducible monic polynomials in  $F[x]$  of degree  $\geq 2$ ; hence  $F$  is not algebraically closed. Conversely, if  $F$  is not algebraically closed, then there exists a monic irreducible  $f(x) \in F[x]$  with  $\deg f(x) \geq 2$ . Thus, the field  $F[x]/(f(x))$  is a proper algebraic extension of  $F$ .  $\square$

We recall that (Corollary 5.1.15) if  $E$  is an extension field of the field  $F$ , then the set of elements of  $E$  that are algebraic over  $F$  constitutes a subfield  $A$  of  $E/F$  (that is, a subfield of  $E$  containing  $F$ ). Evidently  $E = A$  if and only if  $E$  is algebraic over  $F$ . At the other extreme, if  $A = F$ , then  $F$  is said to be **algebraically closed in  $E$** . In any case  $A$  is algebraically closed in  $E$ , since any element of  $E$  that is algebraic over  $A$  is algebraic over  $F$  and so is contained in  $A$ . This result shows that if a field  $F$  has an algebraically closed extension field, then it has one that is algebraic over  $F$ .

**5.3.2 Definition.** We call an extension field  $E/F$  an **algebraic closure of  $F$**  if  $E$  is algebraic over  $F$  and  $E$  is algebraically closed.

For example, assuming the truth of the fundamental theorem of algebra (Theorem 5.6.10), that  $\mathbb{C}$  is algebraically closed, it follows that the field of  $A$  of algebraic numbers is an algebraic closure of  $\mathbb{Q}$ , and thus  $A$  is algebraically closed.

We proceed to prove the existence and uniqueness up to isomorphism of an algebraic closure of any field  $F$ . For a countable  $F$  a straightforward argument is available to establish these results. We begin by enumerating the monic polynomials of positive degree as  $f_1(x), f_2(x), \dots$ . Evidently this can be done. We now define inductively a sequence of extension fields beginning with  $F_0 = F$  and letting  $F_i$  be a splitting field over  $F_{i-1}$  of  $f_i(x)$ . The construction of such splitting fields was given at the end of the previous section. It is clear that every  $F_i$  is countable, so we can realize all of these constructions in some large set  $S$ . Then we can take  $E = \bigcup F_i$  in the set. Alternatively we can define  $E$  to be a direct limit of the fields  $F_i$ . It is easily seen that  $E$  is an algebraic closure of  $F$ . We showed that (Theorem 5.2.9) there exists an isomorphism of  $K_1/F$  onto  $K_2/F$ . This can be used to prove the isomorphism theorem for algebraic closures of a countable field by a simple inductive argument.

The pattern of the proof sketched above can be carried over to the general case by using “transfinite induction”. This is what was done by E. Steinitz, who first proved these results. There are several alternative proofs available that are based on Zorn’s lemma. We shall give one that makes use of the following lemma.

**5.3.3 Lemma.** *If  $E$  is an algebraic extension of a field  $F$ , then the cardinality of  $E$  cannot exceed the cardinality of  $F[x]$ .*

*Proof.* Let  $S$  be the set of all ordered pairs  $(f, \alpha)$  where  $f(x) \in F[x]$  is nonzero and  $\alpha \in E$  with  $f(\alpha) = 0$ . Since for each polynomial  $f(x)$ , the number of  $\alpha$  such that  $(f, \alpha)$  lies in  $S$  is finite, we have  $|S| \leq |F[x]| \aleph_0 = |F[x]|$ . On the other hand,  $E$  maps injectively into  $S$  via  $\alpha \mapsto (f_\alpha, \alpha)$  where  $f_\alpha$  is the minimal polynomial of  $\alpha$ , and thus  $|E| \leq |S|$ .  $\square$

Recall that  $|F[x]| = |F| \aleph_0$ . If  $F$  is infinite, then  $|F[x]| = |F|$  and it follows that  $|E| = |F|$ . When  $F$  is finite,  $F[x]$  is countable, and hence  $E$  is either finite or countably infinite.

**5.3.4 Corollary.** *There exist real numbers transcendental over  $\mathbb{Q}$ .*

*Proof.* There are only countably many polynomials in  $\mathbb{Q}[x]$ . Since  $\mathbb{R}$  is uncountable, the above lemma guarantees that  $\mathbb{R}$  is not algebraic over  $\mathbb{Q}$ .  $\square$

We can now prove the existence of algebraic closures.

**5.3.5 Theorem.** *Any field  $F$  has an algebraic closure.*

*Proof.* We first embed  $F$  in a set  $S$  in which we have a lot of elbow room. Precisely, we assume that  $|S| > |F|$  if  $F$  is infinite and that  $S$  is uncountable if  $F$  is finite. We now define a set  $\Lambda$  whose elements are  $(E, +, \cdot)$  where  $E$  is a subset of  $S$  containing  $F$  and  $+, \cdot$  are binary compositions in  $E$  such that  $(E, +, \cdot)$  is an algebraic extension field of  $F$ . We partially order  $\Lambda$  by declaring that  $(E, +, \cdot) > (E', +', \cdot')$  if  $E$  is an extension field of  $E'$ . By Zorn's lemma there exists a maximal element  $(E, +, \cdot)$ . Then  $E$  is an algebraic extension of  $F$ . We claim that  $E$  is algebraically closed. Otherwise we have a proper algebraic extension  $E' = E(a)$  of  $E$ . Then  $|E'| < |S|$ , so we can define an injective map of  $E'$  into  $S$  that is the identity on  $E$  and then we can transfer the addition and multiplication on  $E'$  to its image. This gives an element of  $\Lambda$  bigger than  $(E, +, \cdot)$ . This contradiction shows that  $E$  is an algebraic closure of  $F$ .  $\square$

Next we take up the question of uniqueness of algebraic closures. It is useful to generalize the concept of a splitting field of a polynomial to apply to sets of polynomials.

**5.3.6 Definition.** If  $\Gamma = \{f_\alpha(x)\}$  is a set of monic polynomials with coefficients in  $F$ , then an extension field  $E/F$  is called a **splitting field over  $F$  of the set  $\Gamma$**  if

1. every  $f_\alpha(x) \in \Gamma$  is a product of linear factors in  $E[x]$  and
2.  $E$  is generated over  $F$  by the roots of the  $f_\alpha(x) \in \Gamma$ .

It is clear that if  $E$  is a splitting field over  $F$  of  $\Gamma$ , then no proper subfield of  $E/F$  is a splitting field of  $\Gamma$  and if  $K$  is any intermediate field, then  $E$  is a splitting field of  $\Gamma$ . Since an algebraic closure  $E$  of  $F$  is algebraic, it is clear that  $E$  is a splitting field over  $F$  of the complete set of monic polynomials of positive degree in  $F[x]$ . The isomorphism theorem for algebraic closures will therefore be a consequence of a general result on isomorphisms of splitting fields that we shall now prove. Our starting point is the following result, which is Theorem 5.2.9.

Let  $\eta : a \mapsto \tilde{a}$  be an isomorphism of a field  $F$  onto a field  $\tilde{F}$ ,  $f(x) \in F[x]$  be monic of positive degree,  $\tilde{f}(x)$  the corresponding polynomial in  $\tilde{F}[x]$  (under the isomorphism, which is  $\eta$  on  $F$  and sends  $x \mapsto x$ ), and let  $E$  and  $\tilde{E}$  be splitting fields over  $F$  and  $\tilde{F}$  of  $f(x)$  and  $\tilde{f}(x)$ , respectively. Then  $\eta$  can be extended to an isomorphism of  $E$  onto  $\tilde{E}$ .

We shall now extend this to a set of polynomials.

**5.3.7 Theorem.** *Let  $\eta : a \mapsto \tilde{a}$  be an isomorphism of a field  $F$  onto a field  $\tilde{F}$ ,  $\Gamma$  a set of monic polynomials  $f_\alpha(x) \in F[x]$ ,  $\tilde{\Gamma}$  the corresponding set of polynomials  $\tilde{f}(x) \in \tilde{F}[x]$ ,  $E$  and  $\tilde{E}$  splitting fields over  $F$  and  $\tilde{F}$  of  $\Gamma$  and  $\tilde{\Gamma}$ , respectively. Then  $\eta$  can be extended to an isomorphism of  $E$  onto  $\tilde{E}$ .*

*Proof.* The proof is a straightforward application of Zorn's lemma. We consider the set of extensions of  $\eta$  to monomorphisms of subfields of  $E/F$  into  $\tilde{E}/\tilde{F}$  and use Zorn's lemma to obtain a maximal one. This must be defined on the whole  $E$ , since otherwise we could get a larger one by applying the result quoted to one of the polynomials  $f_\alpha(x) \in \Gamma$ . Now if  $\zeta$  is a monomorphism of  $E$  into  $\tilde{E}$  such that  $\zeta|_F = \eta$ , then it is clear that  $\zeta(E)$  is a splitting field over  $\tilde{F}$  of  $\tilde{\Gamma}$ . Hence,  $\zeta(E) = \tilde{E}$  and  $\zeta$  is an isomorphism of  $E$  onto  $\tilde{E}$ .  $\square$

As we have observed, this result applies in particular to algebraic closures. If we take  $\tilde{F} = F$  and  $\eta = \text{id}$ , we obtain

**5.3.8 Theorem.** *Any two algebraic closures of a field  $F$  are isomorphic over  $F$ .*

From now on we shall appropriate the notation  $\bar{F}$  for any determination of an algebraic closure of  $F$ . If  $A$  is any algebraic extension of  $F$ , its algebraic closure  $\bar{A}$  is an algebraic extension of  $A$ , hence of  $F$ , and so  $\bar{A}$  is an algebraic closure of  $F$ . Consequently, we have an isomorphism of  $\bar{A}/F$  into  $\bar{F}/F$ . This maps  $A/F$  into a subfield of  $\bar{F}/F$ . Thus, we see that every algebraic extension  $A/F$  can be realized as a subfield of the algebraic closure  $\bar{F}/F$ .

- 5.3 Exercises.**
1. No finite field  $F$  is algebraically closed. [Hint. If  $F = \{0, 1, a_2, \dots, a_n\}$ , consider the polynomial  $1 + x(x-1)(x-a_2)\dots(x-a_n) \in F[x]$ .]
  2. Let  $E$  be an algebraic extension of a field  $F$  and  $A$  an algebraic closure of  $F$ . Show that  $E/F$  is isomorphic to a subfield of  $A/F$ . [Hint. Consider the algebraic closure  $\bar{A}$  of  $A$  and note that this is an algebraic closure of  $F$ .]

## 5.4 Multiple Roots and Separability

Recall the following facts from Subsection 2.6.2 about the multiple roots.

**5.4.1 Definition.** Let  $R$  be an integral domain and  $f(x) \in R[x]$ . If  $\alpha$  is a root of  $f(x)$ , then there exist  $m \in \mathbb{N}$  and  $g(x) \in R[x]$  such that  $f(x) = (x - \alpha)^m g(x)$  and  $g(\alpha) \neq 0$ .  $m$  is called the **multiplicity** of the root  $\alpha$  of  $f(x)$  and if  $m > 1$ ,  $\alpha$  is called a **multiple root** of  $f(x)$ .

**5.4.2 Definition.** If  $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$ , we define  $f'(x) \in R[x]$ , the **derivative** of  $f(x)$ , to be

$$f'(x) = a_1 + a_2x + \dots + na_nx^{n-1}.$$

We record the straightforward properties of the derivative of polynomials in the next lemma.

**5.4.3 Lemma.** If  $f(x)$  and  $g(x)$  are polynomials over an integral domain  $R$  and  $c \in R$ , then

1.  $(cf(x))' = cf'(x)$ ,
2.  $(f(x) + g(x))' = f'(x) + g'(x)$ ,
3.  $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$ ,
4.  $((f(x))^n)' = n(f(x))^{n-1}f'(x)$  where  $n \in \mathbb{N}$ .

**5.4.4 Theorem.** Let  $E$  be an extension of a field  $F$  and  $f(x) \in F[x]$ .

1. For  $\alpha \in E$ ,  $\alpha$  is a multiple root of  $f(x)$  if and only if  $\alpha$  is a root of both  $f(x)$  and  $f'(x)$ .
2. If  $f(x)$  and  $f'(x)$  are relatively prime, then  $f(x)$  has no multiple root.
3. If  $f(x)$  is irreducible over  $F$  having a root in  $E$ , then  $f(x)$  has no multiple root in  $E$  if and only if  $f'(x) \neq 0$ .

*Proof.* (1) is clear.

(2) Since  $f(x)$  and  $f'(x)$  are relatively prime, there exist  $h(x)$  and  $k(x)$  in  $F[x]$  such that  $1 = f(x)h(x) + f'(x)k(x)$ . If  $\alpha \in E$  is a multiple root of  $f(x)$ , by (1),  $f(\alpha) = 0 = f'(\alpha)$ , so  $1 = 0$ , a contradiction.

(3) Since  $f(x)$  is irreducible,  $f'(x) \neq 0$  and  $\deg f'(x) < \deg f(x)$ , we have  $f(x)$  and  $f'(x)$  are relatively prime, so  $f(x)$  has no multiple roots. Conversely, if  $f'(x) = 0$ , then  $f(\alpha) = 0 = f'(\alpha)$  for some  $\alpha \in E$  since  $f(x)$  has a root in  $E$ . Hence, by (1),  $\alpha$  is a multiple root of  $f(x)$ .  $\square$

**5.4.5 Definition.** Let  $F$  be a field. A polynomial  $f(x) \in F[x]$  is **separable** if every root (in some splitting field over  $F$ ) of its irreducible factor is not a multiple root. If  $E$  is an extension of  $F$  and  $\alpha \in E$  is algebraic over  $F$ , then  $\alpha$  is **separable over  $F$**  if its minimal polynomial over  $F$  is separable.

Let  $F \subset K \subset E$  be field extensions. Note that if  $\alpha$  is separable over  $F$ , then  $\alpha$  is separable over  $K$  since  $m_{\alpha,K}(x) \mid m_{\alpha,F}(x)$ . Here  $m_{\alpha,-}(x)$  stands for the minimal polynomial of  $\alpha$  over the indicated field.

- 5.4.6 Examples.**
1. Consider  $f(x) = x^2 + 1$ . Over  $\mathbb{Q}$ , we have  $f(x)$  is irreducible and separable but over  $\mathbb{Z}/(2)$ , we have  $f(x) = x^2 + 1 = (x + 1)^2$  is not irreducible but is separable since the only irreducible factor is  $x + 1$  which is separable over  $\mathbb{Z}/(2)$ .
  2. Let  $K$  be a field of characteristic  $p$  and  $F = K(y)$  be the field of rational functions over  $K$  with indeterminate  $y$ . Since  $K[y]$  is UFD,  $y$  is irreducible element in  $K[y]$ , so the polynomial  $f(x) = x^p - y$  in  $F[x]$  is irreducible over  $F$  by Eisenstien criterion. Since  $f'(x) = 0$  and  $f(x)$  has a root, say  $\alpha$  in some splitting field  $E$  of  $F$ ,  $\alpha$  is a multiple root of  $f(x)$ , so  $f(x)$  is not separable over  $F$ . However, if we consider  $f(x) = x^p - y \in E[x]$ , we have  $f(x) = (x - \alpha)^p$  and its irreducible factor in  $E[x]$  is only  $x - \alpha$  which is separable over  $E$ , so  $f(x)$  is separable over  $E$ .

Suppose that  $F$  is a field of characteristic zero and  $f(x)$  is a monic irreducible polynomial over  $F$ , say  $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$ . Then  $f'(x) = a_1 + 2a_2x + \dots + nx^{n-1}$ . The key point is that  $n \neq 0$ , so  $f'(x) \neq 0$ . Since  $\deg f'(x) < \deg f(x)$  and  $f(x)$  is irreducible,  $f(x)$  and  $f'(x)$  are relatively prime, so all roots of  $f(x)$  are simple. Thus, we have shown:

**5.4.7 Theorem.** *Let  $F$  be a field of characteristic zero. Then every polynomial  $f(x) \in F[x]$  is separable.*

**5.4.8 Definition.** We call an algebraic extension field  $E$  of a field  $F$  a **separable extension** if the minimal polynomial of every element of  $E$  is separable. Hence, if  $F$  is of characteristic zero, then every algebraic extension is a separable extension. A field  $F$  is **perfect** if every polynomial  $f(x)$  over  $F$  is separable.

Thus, all fields of characteristic zero are perfect.

**5.4.9 Remark.** Suppose  $F$  is a field (or even a commutative ring) of characteristic  $p > 0$ . Then the identities

$$(ab)^p = a^p b^p \quad \text{and} \quad (a + b)^p = a^p + b^p$$

show that the map  $\varphi : F \rightarrow F$  defined by  $\varphi(a) = a^p$  is a ring homomorphism. Since  $F$  is a field,  $\varphi$  has to be one-to-one. But  $\varphi$  does *not* have to be onto - for example

$$\varphi : (\mathbb{Z}/p\mathbb{Z})(x) \rightarrow (\mathbb{Z}/p\mathbb{Z})(x)$$

is not onto; the image is  $(\mathbb{Z}/p\mathbb{Z})(x^p)$ . However, if  $F$  is finite of order  $p^n$ , then  $a^{p^n} = a$  for all  $a \in F$ , so  $\varphi$  is onto and  $\varphi^n$  is the identity map, called the **Frobenius' automorphism**.

**5.4.10 Theorem.** *Let  $F$  be a field of characteristic  $p > 0$ , and let  $a \in F$ .*  
 (1) *If  $a \in F^p$  and  $a = r^p$ , then  $x^p - a = (x - r)^p$ .*  
 (2) *If  $a \notin F^p$ , then  $x^p - a$  is irreducible.*

*Proof.* (1) is trivial.

(2) In a splitting field for  $F$ ,  $x^p - a = (x - r)^p$  ( $r$  may not be in  $F$ ). Any proper factor of  $x^p - a$  (after being made monic) has the form  $(x - r)^i$  where  $1 \leq i \leq p - 1$ . Thus, if  $x^p - a$  has a proper factor over  $F$ , then  $r^i \in F$  for some  $1 \leq i \leq p - 1$ . But then  $r^i$  and  $r^p = a \in F$ , so  $r \in F$  since  $(i, p) = 1$ . Hence,  $a = r^p \in F^p$ . □

**5.4.11 Theorem.** *Let  $F$  be a field of characteristic  $p > 0$ . Then  $F$  is perfect if and only if  $F = F^p$ .*

*Proof.* Suppose  $F \neq F^p$  and choose  $a \in F \setminus F^p$ . By Theorem 5.4.10,  $x^p - a$  is irreducible. But  $x^p - a$  does not have distinct roots in a splitting field of  $F$ . Hence,  $F$  is not perfect.

Conversely, assume that  $F$  is not perfect. Then there is an irreducible polynomial  $f(x)$  over  $F$  which does not have simple roots. By Theorem 5.4.4, this means that  $f(x)$  and  $f'(x)$  are not relatively prime. Since  $f(x)$  is irreducible and  $\deg f'(x) < \deg f(x)$ ,  $f'(x) = 0$ . Thus,  $f(x)$  is a polynomial in  $x^p$ , i.e.,

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots + a_{(m-1)p} x^{(m-1)p} + x^{mp}.$$

We shall claim that some  $a_{jp} \notin F^p$ . For if each  $a_{jp} \in F^p$ , say  $a_{jp} = (b_j)^p$ , then  $f(x) = g(x)^p$  where

$$g(x) = b_0 + b_1 x + \cdots + b_{m-1} x^{m-1} + x^m$$

which contradicts the irreducibility of  $f(x)$  over  $F$ . This establishes the claim. Hence,  $a_{jp} \notin F^p$  and  $F \neq F^p$ .  $\square$

#### 5.4.12 Corollary. Every finite field is perfect.

*Proof.* The characteristic of a finite field  $F$  is a prime  $p$ . The monomorphism  $a \mapsto a^p$  of  $F$  is an isomorphism since  $F$  is finite. Hence,  $F = F^p$  is perfect by Theorem 5.4.11.  $\square$

We shall end this section by proving the “primitive element theorem” which is a classic of field theory. We first recall that an extension field  $E$  of a field  $F$  is said to be a **simple extension** of  $F$  if  $E = F(\alpha)$  for some  $\alpha \in E$ . Such an element  $\alpha$  is called a **primitive element**.

#### 5.4.13 Theorem. If $F$ is a field and $G$ is a finite subgroup of the multiplicative group of nonzero elements of $F$ , then $G$ is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.

*Proof.* If  $G = \{1\}$ , then  $G$  is cyclic. Assume that  $G \neq \{1\}$ . Since  $G$  is a finite abelian group,

$$G \cong \mathbb{Z}/(m_1) \oplus \cdots \oplus \mathbb{Z}/(m_k)$$

where  $k \geq 1$ ,  $m_1 > 1$  and  $m_1 \mid \cdots \mid m_k$ . Since  $m_k \left( \sum_{i=1}^k \mathbb{Z}/(m_i) \right) = 0$ ,  $u$  is a root of the polynomial  $x^{m_k} - 1 \in F[x]$  for all  $u \in G$ . By Theorem 5.2.2, this polynomial has at most  $m_k$  distinct roots in  $F$ , we must have  $k = 1$  and  $G \cong \mathbb{Z}/(m_1)$  which is a cyclic group.  $\square$

#### 5.4.14 Theorem. [Primitive Element Theorem] Let $E$ be a finite separable extension of a field $F$ . Then there exists $\alpha \in E$ such that $E = F(\alpha)$ . That is, a finite separable extension of a field is a simple extension.

*Proof.* If  $F$  is a finite field, then  $E$  is also finite. Let  $\alpha$  be a generator for the cyclic group of all nonzero elements of  $E$  under multiplication. Clearly,  $E = F[\alpha]$ , so  $\alpha$  is a primitive element in this case.

We now assume that  $F$  is infinite and prove our theorem in the case that  $E = F(\beta, \gamma)$ . The induction argument from this to the general case is obvious. Let  $m_{\beta, F}(x)$  and  $m_{\gamma, F}(x)$  be the minimal polynomials over  $F$  of  $\beta$  and  $\gamma$ , respectively. Assume that  $m_{\beta, F}(x)$  has distinct roots  $\beta = \beta_1, \dots, \beta_n$  and  $m_{\gamma, F}(x)$  has distinct roots  $\gamma = \gamma_1, \dots, \gamma_m$  in  $\bar{F}$  where all roots are of multiplicity 1, since  $E$  is a separable extension of  $F$ . Since  $F$  is infinite, we can find  $a \in F$  such that

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

for all  $i$  and  $j$ , with  $j \neq 1$ . That is,  $a(\gamma - \gamma_j) \neq \beta_i - \beta$ . Letting  $\alpha = \beta + a\gamma$ , we have  $\alpha = \beta + a\gamma \neq \beta_i + a\gamma_j$ , so

$$\alpha - a\gamma_j \neq \beta_i$$

for all  $i$  and all  $j \neq 1$ . Consider  $h(x) = m_{\beta, F}(\alpha - ax) \in F(\alpha)[x]$ . Now,  $h(\gamma) = m_{\beta, F}(\beta) = 0$ . However,  $h(\gamma_j) \neq 0$  for  $j \neq 1$  by construction, since the  $\beta_i$  were the only roots of  $m_{\beta, F}(x)$ . Hence,  $h(x)$  and  $m_{\gamma, F}(x)$  have a common factor in  $F(\alpha)[x]$ , namely the minimal polynomial of  $\gamma$  over  $F(\alpha)$ , which must be linear, since  $\gamma$  is the only common root of  $m_{\gamma, F}(x)$  and  $h(x)$ . Thus,  $\gamma \in F(\alpha)$ , and therefore  $\beta = \alpha - a\gamma$  is in  $F(\alpha)$ . Hence,  $F(\beta, \gamma) = F(\alpha)$ .  $\square$

**5.4 Exercises.** 1. Suppose that  $F \subseteq K \subseteq E$  and that  $E$  is separable extension of  $F$ . Prove that  $E$  is separable over  $K$  and  $K$  is separable over  $F$ .

2. Let  $F$  be of characteristic  $p$  and let  $a \in F$ . Show that  $f(x) = x^p - x - a$  has no multiple roots and  $f(x)$  is irreducible in  $F[x]$  if and only if  $a \neq c^p - c$  for any  $c \in F$ .
3. Find a primitive element of  $\mathbb{Q}(i, \sqrt[3]{2})$  over  $\mathbb{Q}$ .
4. Let  $K = \mathbb{F}_{25}$  be the field with 5 elements and let  $F = \mathbb{Z}/(5)$  be the prime subfield of  $K$ . Determine the cardinalities of the following two sets.
  - (a) The set of elements of  $K$  which generate  $K$  as a field over  $F$ .
  - (b) The set of elements of  $K$  which generate the group of nonzero elements of  $K$  as an abelian group under multiplication.
5. Let  $F$  be a field and let  $\overline{F}$  be its algebraic closure. If a monic polynomial  $p(x) \in F[x]$  is irreducible over  $F$  and has distinct roots  $\alpha_1, \alpha_2, \dots, \alpha_k \in \overline{F}$ , prove that the multiplicities of  $\alpha_j$  are equal, that is,

$$p(x) = (x - \alpha_1)^m (x - \alpha_2)^m \dots (x - \alpha_k)^m$$

for some  $m \in \mathbb{N}$ .

## 5.5 Automorphisms of Fields and Galois Theory

If  $F$  is a field, the set of automorphisms of  $F$ ,  $\text{Aut } F$ , forms a group under composition of functions.

**5.5.1 Examples (Examples of automorphism groups).** 1. Any automorphism satisfies  $\varphi(1) = 1$ , so  $\varphi(n) = n$  for all  $n \in \mathbb{Z}$  and  $\varphi(n/m) = n/m$  if  $n, m \in \mathbb{Z}$  and  $m \neq 0$  in  $F$ . This implies that the fields  $\mathbb{Q}$  and  $\mathbb{F}_p = \mathbb{Z}/(p)$  have only the identity map as an automorphism. That is,  $\text{Aut}(F) = \{\text{id}_F\}$  if  $F = \mathbb{Q}$  or  $\mathbb{F}_p$ . Moreover, any field  $E$  is an extension of  $\mathbb{Q}$  or  $\mathbb{F}_p$  (so called the prime subfield) and any automorphism  $\varphi : E \rightarrow E$  leaves the prime subfield pointwise fixed.

2. The only automorphism  $\varphi : \mathbb{R} \rightarrow \mathbb{R}$  is the identity map. For, we have known that  $\varphi(q) = q$  for all  $q \in \mathbb{Q}$ . Note that  $\varphi(a) = \varphi((\sqrt{a})^2) = (\varphi(\sqrt{a}))^2 > 0$  for all  $a > 0$ . Thus, if  $a < b$ , then  $\varphi(a) < \varphi(b)$ . Let  $x \in \mathbb{R}$ . Suppose  $\varphi(x) \neq x$ . Then  $\varphi(x) < x$  or  $\varphi(x) > x$ . If  $\varphi(x) < x$ , then there exists a  $q \in \mathbb{Q}$  such that  $\varphi(x) < q < x$ . Thus,  $q = \varphi(q) < \varphi(x)$ , a contradiction. If  $x < \varphi(x)$ , then there exists a  $q \in \mathbb{Q}$  such that  $x < q < \varphi(x)$ , so  $\varphi(x) < \varphi(q) = q$ , a contradiction. Hence,  $\varphi = \text{id}_{\mathbb{R}}$ .
3. Complex conjugation:  $\varphi(z) = \bar{z}$  is an automorphism of  $\mathbb{C}$  of order two. In fact,  $\text{Aut } \mathbb{C}$  is uncountable, but the other automorphisms are “indescribable” and exist only via Zorn’s lemma. However, the group of automorphisms of  $\mathbb{C}$  which fix all elements of  $\mathbb{R}$  is a group of order two.
4. Let  $F$  be a field and let  $E = F(t)$  where  $t$  is transcendental over  $F$ . As shall be indicated in the Exercise 5.5 below,  $u \in E$  is a generator of  $E/F$  if and only if it has the form

$$u = \frac{\alpha t + \beta}{\gamma t + \delta}, \quad \alpha\delta - \beta\gamma \neq 0.$$

Since an automorphism of  $E/F$  sends generators into generators, it follows that every automorphism  $\varphi : E \rightarrow E$  is given by

$$\varphi(a) = a \text{ for all } a \in F \quad \text{and} \quad \varphi(t) = \frac{\alpha t + \beta}{\gamma t + \delta},$$

where  $\alpha, \beta, \gamma, \delta \in F$  and  $\alpha\delta - \beta\gamma \neq 0$ . Note that if  $c \in F$  and  $c \neq 0$ , then

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} c\alpha & c\beta \\ c\gamma & c\delta \end{bmatrix}$$

give rise to the same automorphism of  $F(t)$ . A computation shows composition of functions corresponds to matrix multiplication. The net result is that

$$\text{Aut } F(t) \cong \text{GL}_2(F)/F^\times = \text{PGL}_2(F),$$

where  $F^\times$  is the set of matrices  $aI$ ,  $a \neq 0$ .

5. If  $F$  is a subfield of  $K$ , let

$$\text{Aut}_F K = \{\varphi \in \text{Aut } K : \varphi(a) = a \text{ for all } a \in F\}.$$

The group structure of  $\text{Aut}_F F(x, y)$  is known, but very complicated. For  $n \geq 3$ , almost nothing is known about  $\text{Aut}_F F(x_1, \dots, x_n)$ .

The above examples show that  $\text{Aut } F$  is in general very complicated and probably impossible to describe. Galois theory proceeds in a different direction. One takes a subgroup  $H$  of  $\text{Aut } F$ —we shall be almost concerned with finite  $H$ —and looks the set

$$F^H = \{a \in F : \varphi(a) = a \text{ for all } \varphi \in H\}.$$

It is easy to see that  $F^H$  is a subfield of  $F$ . Moreover, if  $K$  is a subgroup of  $H$ , then

$$\begin{aligned} 1 &\subseteq K \subseteq H \\ F &\supseteq F^K \supseteq F^H. \end{aligned}$$

The fundamental result of Galois theory is that if  $F$  is separable over  $F^H$ , then there is a one-to-one correspondence between subgroups of  $H$  and subfields of  $F$  which contain  $F^H$ . Such correspondences are inclusion reversing and are called “Galois correspondences”.

**5.5.2 Definition.** Let  $E$  be an extension field of a field  $F$ . The **Galois group of  $E$  over  $F$**  denoted by  $\text{Gal}(E/F)$  is the group

$$\{\varphi \in \text{Aut } E : \varphi(a) = a \text{ for all } a \in F\}.$$

Let  $G$  be a subgroup of  $\text{Aut } E$  where  $E$  is a field. Then the **field of  $G$ -invariant of  $E$**  or the **fixed field of  $G$  acting on  $E$**  is the field

$$\{a \in E : \varphi(a) = a \text{ for all } \varphi \in G\}.$$

It is denoted by  $E^G$  or  $\text{Inv } G$ .

**5.5.3 Theorem.** (1) If  $\text{Aut } E \supseteq G_1 \supseteq G_2$ , then  $E^{G_1} \subseteq E^{G_2}$ .

(2) If  $E \supseteq F_1 \supseteq F_2$ , then  $\text{Gal}(E/F_1) \subseteq \text{Gal}(E/F_2)$ .

(3) If  $G = \text{Gal}(E/F)$ , then  $E^G \supseteq F$ .

(4) If  $F = E^G$ , then  $\text{Gal}(E/F) \supseteq G$ .

*Proof.* These are immediate consequences of the definitions.  $\square$

We shall now apply these ideas to splitting fields. Using the present terminology, Theorem 5.2.10 can be restated as follows. If  $E$  is a splitting field over  $F$  of a polynomial  $f(x)$ , then  $\text{Gal}(E/F)$  is finite and we have the inequality  $|\text{Gal}(E/F)| \leq [E : F]$ . Moreover,  $|\text{Gal}(E : F)| = [E : F]$  if  $f(x)$  has distinct roots. We therefore have the following important preliminary result.

**5.5.4 Lemma.** *Let  $E/F$  be a splitting field of a separable polynomial contained in  $F[x]$ . Then*

$$|\text{Gal}(E/F)| = [E : F].$$

Our next attack will be from the group side. We begin with an arbitrary field  $E$  and any finite group of automorphisms  $G$  acting in  $E$ . Then we have the following

**5.5.5 Lemma.** [Artin] *Let  $G$  be a finite subgroup of  $\text{Aut } E$  and let  $F = E^G$ . Then*

$$[E : F] \leq |G|.$$

*Proof.* Let  $|G| = n$  and write  $G = \{g_1 = 1, g_2, \dots, g_n\}$ . We have to show that  $[E : F] \leq n$ , or equivalently:

(\*) If  $x_1, \dots, x_{n+1} \in E$ , then there exist  $u_1, \dots, u_{n+1} \in F$  not all zero, such that

$$u_1x_1 + \dots + u_{n+1}x_{n+1} = 0,$$

that is,  $x_1, \dots, x_{n+1}$  are linearly dependent over  $F$ .

Consider the following  $n \times (n + 1)$  matrix with entries in  $E$

$$M = \begin{bmatrix} x_1 & x_2 & \dots & x_{n+1} \\ g_2(x_1) & g_2(x_2) & \dots & g_2(x_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ g_n(x_1) & g_n(x_2) & \dots & g_n(x_{n+1}) \end{bmatrix}.$$

This matrix has rank  $\leq n$ , so there is a nonzero  $(n + 1) \times 1$  vector  $\vec{v} = (v_1, \dots, v_{n+1})^t$  with entries in  $E$  such that  $M\vec{v} = \vec{0}_{(n+1) \times 1}$ . We wish to find such a vector where entries lie in  $F$ . Among all such vectors with entries in  $E$ , choose one in which the number of nonzero coordinates,  $r$ , is minimal. By renaming the elements  $x_1, \dots, x_{n+1}$ , we may suppose that the nonzero coordinates are the first  $r$  of them; by multiplying the vector by  $v_r^{-1}$  we may suppose that the last nonzero coordinate is equal to 1. Thus,

$$M\vec{v} = \vec{0}_{(n+1) \times 1} \quad \text{where} \quad \vec{v} = (v_1, \dots, v_{r-1}, 1, 0, \dots, 0)^t.$$

**Claim.** *If  $h \in G$  and  $h(\vec{v}) = (h(v_1), \dots, h(v_{r-1}), 1, 0, \dots, 0)^t$ , then  $Mh(\vec{v}) = \vec{0}$ .*

*Proof of Claim.* The inner product of the  $j$ -th row of  $M$  with  $h(\vec{v})$  is:

$$z = g_j(x_1)h(v_1) + \dots + g_j(x_{r-1})h(v_{r-1}) + g_j(x_r) \cdot 1.$$

Apply the automorphism  $h^{-1}$  to  $z$ ,

$$\begin{aligned} h^{-1}z &= h^{-1}g_j(x_1)h(v_1) + \dots + h^{-1}g_j(x_{r-1})h(v_{r-1}) + h^{-1}g_j(x_r) \cdot 1 \\ &= g_i(x_1)v_1 + \dots + g_i(x_{r-1})v_{r-1} + g_i(x_r) \cdot 1 = 0, \end{aligned}$$

since  $h^{-1}g_j = g_i$  for some  $i$ . This proves the claim.

Now we consider, for any  $h \in G$

$$\begin{aligned}\vec{v} - h(\vec{v}) &= (v_1, \dots, v_{r-1}, 1, 0, \dots, 0)^t - (h(v_1), \dots, h(v_{r-1}), 1, 0, \dots, 0)^t \\ &= (\overbrace{*, \dots, *}^{r-1}, 0, \dots, 0)^t.\end{aligned}$$

Since  $M(\vec{v} - h(\vec{v})) = \vec{0}$  and  $\vec{v} - h(\vec{v})$  has at most  $r - 1$  nonzero entries,  $\vec{v} - h(\vec{v}) = \vec{0}$  by the minimal choice of  $r$ . This means that for all  $h \in G$  and  $i = 1, \dots, r - 1$ , we have  $h(v_i) = v_i$ . Thus, all the  $v_i$  lie in  $E^G = F$  and  $(u_1, \dots, u_{n+1}) = (v_1, \dots, v_{r-1}, 0, \dots, 0)$  is a set of elements of  $F$  which satisfies (\*).  $\square$

Recall that an algebraic extension field  $E$  of a field  $F$  is a separable extension if the minimal polynomial of every element of  $E$  is separable.

**5.5.6 Definition.** We call an algebraic extension field  $E$  of a field  $F$  a **normal extension** if every irreducible polynomial in  $F[x]$  which has a root in  $E$  splits into linear factors in  $E$ . This is equivalent to saying that  $E$  contains a splitting field for the minimal polynomial of every element of  $E$ . Normality plus separability, called a **Galois extension**, mean that every irreducible polynomial of  $F[x]$  which has a root in  $E$  is a product of distinct linear factors in  $E[x]$ .

Also, by the results of the last section, if  $E$  is algebraic over  $F$ , then  $E$  is necessarily separable over  $F$  if the characteristic is zero or if the characteristic is  $p > 0$  and  $F^p = F$ .

We are now ready to derive our main results, the first of which gives two abstract characterizations of splitting fields of separable polynomials and some important additional information. We state this as

**5.5.7 Theorem.** Let  $E$  be an extension field of a field  $F$ . Then the following conditions on  $E/F$  are equivalent.

- (i)  $E$  is a splitting field over  $F$  of a separable polynomial  $f(x)$ .
  - (ii)  $F = E^G$  for some finite group  $G$  of automorphisms of  $E$ .
  - (iii)  $E$  is finite dimensional Galois (normal and separable) over  $F$ .
- Moreover, if  $E$  and  $F$  are as in (i) and  $G = \text{Gal}(E/F)$ , then  $F = E^G$  and if  $G$  and  $F$  are as in (ii), then  $G = \text{Gal}(E/F)$ .

*Proof.* (i)  $\Rightarrow$  (ii). Let  $G = \text{Gal}(E/F)$ . Then  $E^G$  is a subfield of  $E$  containing  $F$ . Also it is clear that  $E$  is a splitting field over  $E^G$  of  $f(x)$  as well as over  $F$  and  $G = \text{Gal}(E/E^G)$ . Hence, by Lemma 5.5.4,  $|G| = [E : F]$  and  $|G| = [E : E^G]$ . Since  $E \supseteq E^G \supseteq F$ , we have  $[E : F] = [E : E^G][E^G : F]$ . Hence,  $[E^G : F] = 1$ , and so  $E^G = F$ . We have prove also that  $F = E^G$  for  $G = \text{Gal}(E/F)$ , which is the first of the two supplementary statements.

(ii)  $\Rightarrow$  (iii). By Artin's lemma,  $[E : F] \leq |G|$ , and so  $E$  is finite dimensional over  $F$ . Let  $f(x)$  be an irreducible polynomial in  $F[x]$  having a root  $r$  in  $E$ . Let  $\{r = r_1, r_2, \dots, r_m\}$  be the orbit of  $r$  under the action of  $G$ . Thus, this is the set of distinct elements of the form  $\sigma(r)$ ,  $\sigma \in G$ . Hence, if  $\sigma \in G$ , then the set  $\{\sigma(r_1), \sigma(r_2), \dots, \sigma(r_m)\}$  is a permutation of  $\{r_1, r_2, \dots, r_m\}$ . We have  $f(r) = 0$  which implies that  $f(r_i) = 0$ . Then  $f(x)$  is divisible by  $x - r_i$ , and since the  $r_i$ ,  $1 \leq i \leq m$ , are distinct,  $f(x)$  is divisible by  $g(x) = \prod_{i=1}^m (x - r_i)$ . We now apply to  $g(x)$  the automorphism of  $E[x]$ , which sends  $x \rightarrow x$  and  $a \rightarrow \sigma(a)$  for  $a \in E$ . This gives  $\sigma g(x) = \prod_{i=1}^m (x - \sigma(r_i)) = \prod_{i=1}^m (x - r_i) = g(x)$ . Since this holds for every  $\sigma \in G$  we see that the coefficients of  $g(x)$  are  $G$ -invariant. Hence,  $g(x) \in F[x]$ . Since we assumed  $f(x)$  irreducible in  $F[x]$  we see that  $f(x) = g(x) = \prod (x - r_i)$ , a product of distinct linear factors in  $E[x]$ . Thus,  $E$  is separable and normal over  $F$  and (iii) holds.

(iii)  $\Rightarrow$  (i). Since we are given that  $[E : F] < \infty$  we can write  $E = F(r_1, r_2, \dots, r_k)$  and each  $r_i$  is algebraic over  $F$ . Let  $f_i(x)$  be the minimal polynomial of  $r_i$  over  $F$ . Then the hypothesis

implies that  $f_i(x)$  is a product of distinct linear factors in  $E[x]$ . It follows that  $f(x) = \prod_{i=1}^k f_i(x)$  is separable and  $E = F(r_1, r_2, \dots, r_k)$  is a splitting field over  $F$  of  $f(x)$ . Hence, we have (i).

It remains to prove the second supplementary statement. We have seen that under the hypothesis of (ii) we have  $[E : F] \leq |G|$ , and that since (i) holds, we have  $|\text{Gal}(E/F)| = [E : F]$ . Since  $G \subseteq \text{Gal}(E/F)$  and  $|G| \geq [E : F] = |\text{Gal}(E/F)|$ , equivalently  $G = \text{Gal}(E/F)$ .  $\square$

The above proof also yields

**5.5.8 Corollary.** *If  $E/F$  is the splitting field of  $f(x) \in F[x]$  and  $r_1, \dots, r_n$  are distinct roots of  $f(x)$  in  $E$ , then  $G = \text{Gal}(E/F)$  may be identified with a subgroup of  $S_n$ , the group of permutations of  $\{r_1, \dots, r_n\}$ . However, it is not always the case that  $\text{Gal}(E/F)$  is the full group of permutations of the roots of  $f(x)$ .*

There are two observations underlying the above corollary.

1. Each  $\sigma \in G$  permutes  $r_1, \dots, r_n$ .
2.  $\sigma \in G$  is determined by its action on  $r_1, \dots, r_n$  because  $r_1, \dots, r_n$  generate  $E$  as a field over  $F$ , i.e.,  $E = F[r_1, \dots, r_n] = F(r_1, \dots, r_n)$ .

**5.5.9 Example** (Elementary symmetric functions). If  $K$  is a field, then the polynomial ring  $K[x_1, \dots, x_n]$  is an integral domain. The quotient field of  $K[x_1, \dots, x_n]$  is denoted by  $K(x_1, \dots, x_n)$  and is called the **field of rational functions** in  $x_1, \dots, x_n$  over  $K$ . In the field extension

$$K \subset K(x_1, \dots, x_n)$$

each  $x_i$  is easily seen to be transcendental over  $K$ . In fact, every element of  $K(x_1, \dots, x_n)$  not in  $K$  itself is transcendental over  $K$  (Prove!).

Let  $S_n$  be the symmetric group on  $n$  letters. A rational function  $\varphi \in K(x_1, \dots, x_n)$  is said to be **symmetric** in  $x_1, \dots, x_n$  over  $K$  if for every  $\sigma \in S_n$ ,

$$\varphi(x_1, x_2, \dots, x_n) = \varphi(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

Trivially, every constant polynomial is a symmetric function. More generally, the **elementary symmetric functions** in  $x_1, \dots, x_n$  over  $K$  are defined to be the polynomials:

$$\begin{aligned} e_1 &= x_1 + x_2 + \dots + x_n = \sum_{i=1}^n x_i; \\ e_2 &= \sum_{1 \leq i < j \leq n} x_i x_j; \\ &\vdots \\ e_k &= \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}; \\ &\vdots \\ e_n &= x_1 x_2 \dots x_n. \end{aligned}$$

The verification that the  $e_i$  are indeed symmetric follows from the fact that they are simply the coefficients of  $t$  in the polynomial  $p(t) \in K[x_1, \dots, x_n][t]$ , where

$$p(t) = (t - x_1)(t - x_2) \dots (t - x_n) = t^n - e_1 t^{n-1} + e_2 t^{n-2} - \dots + (-1)^{n-1} e_{n-1} t + (-1)^n e_n.$$

If  $\sigma \in S_n$ , then the assignments  $x_i \mapsto x_{\sigma(i)}$ ,  $i = 1, 2, \dots, n$  and

$$f(x_1, \dots, x_n)/g(x_1, \dots, x_n) \mapsto f(x_{\sigma(1)}, \dots, x_{\sigma(n)})/g(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

define a  $K$ -automorphism of the field  $E = K(x_1, \dots, x_n)$  which will also be denoted  $\sigma$ . The map  $S_n \rightarrow \text{Gal}(E/K)$  given by  $\sigma \mapsto \sigma$  is clearly a monomorphism of groups, whence  $S_n$  may be considered as a subgroup of the Galois group  $\text{Gal}(E/K)$ . Clearly, the fixed field  $F = E^{S_n}$  consists precisely of symmetric functions; that is, the set of all symmetric functions is a subfield of  $E$  containing  $K$ . Therefore, by Theorem 5.5.7,  $E$  is a Galois extension of  $F$  with Galois group  $\text{Gal}(E/F) = S_n$  and dimension  $|S_n| = n!$ .

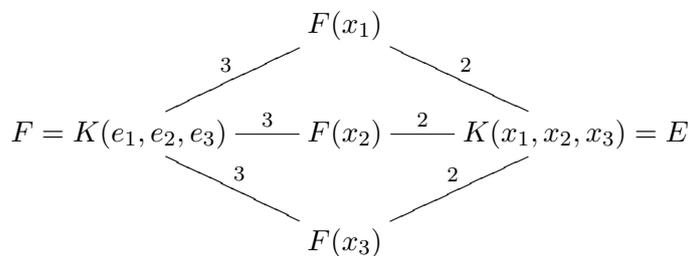
**5.5.10 Example.** Let  $K$  be a field and  $x_1, x_2, x_3$  be indeterminates over  $K$ , set

$$e_1 = x_1 + x_2 + x_3, e_2 = x_1x_2 + x_2x_3 + x_3x_1, e_3 = x_1x_2x_3$$

and consider the fields

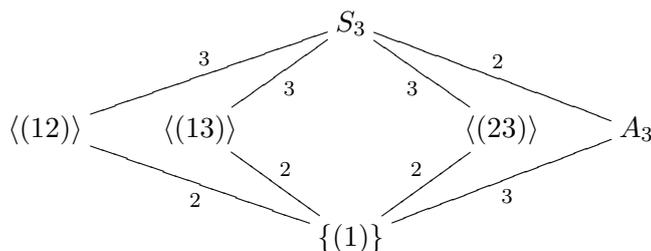
$$F = K(e_1, e_2, e_3) \subseteq K(x_1, x_2, x_3) = E.$$

The relevant subfields of  $E$  are indicated in the diagram



The fields  $F(x_1), F(x_2)$  and  $F(x_3)$  are all isomorphic (over  $F$ ), but they are distinct subfields of  $E$ . Moreover,  $E$  is a splitting field for  $f(t) = t^3 - e_1t^2 + e_2t - e_3$  but  $F(x_1), F(x_2)$  and  $F(x_3)$  are not.

We know that  $G = \text{Gal}(E/F) = S_3$  where  $S_3$  is identified with the group of permutations on 3 letters. We next calculate  $E^H$  when  $H$  is a subgroup of  $G = \text{Gal}(E/F) = S_3$ . The following is a diagram of the lattice of subgroups of  $S_3$  and their indices.



We have already calculated that  $E^{S_3} = E^G = F$  and of course  $E^{\{(1)\}} = E$ . It is not hard to verify that

$$E^{\langle(12)\rangle} = F[x_3], E^{\langle(13)\rangle} = F[x_2], E^{\langle(23)\rangle} = F[x_1].$$

It is somewhat more difficult to verify that  $E^{A_3} = F[\Delta]$  where

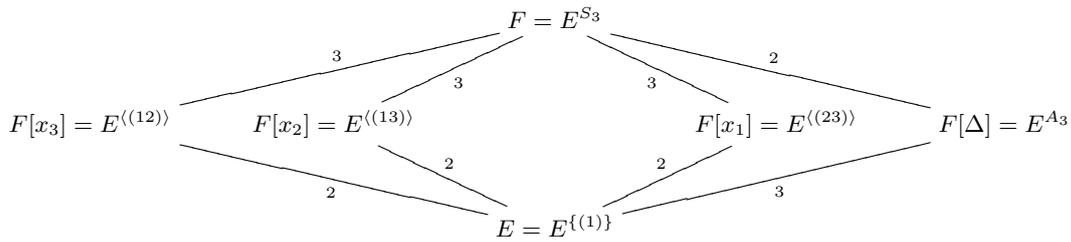
$$\Delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1).$$

Note that  $\sigma(\Delta) = \Delta$  if  $\sigma \in A_3$ , but  $\sigma(\Delta) = -\Delta$  if  $\sigma \in S_3 \setminus A_3$ .

We already know that

$$[F[x_1] : F] = [F[x_2] : F] = [F[x_3] : F] = 3$$

and one can verify that  $[F[\Delta] : F] = 2$ . Thus, we get the following diagrams of *all* (by Galois Theory) subfields of  $E$  containing  $F$



The indices are the same as in the lattice diagram for  $S_3$ , but inclusions are reversed. Recall that  $E$  is the splitting field of a separable polynomial

$$f(t) = (t - x_1)(t - x_2)(t - x_3)$$

for any field in the above diagram. More generally, it is clear that if  $M/L$  is a splitting field for  $f(t) \in L[t]$  and  $M \supseteq N \supseteq L$ , then  $M/N$  is a splitting field for  $f(t)$ , regarded as a polynomial in  $N[t]$ .

Furthermore, for each field  $L$  in the above diagram, we have  $L = E^H$  for some subgroup  $H$  of  $G = S_3$  and  $\text{Gal}(E/L) = H$ . On the other hand, things are not so nice for the extensions  $L/F$ . For example,  $\text{Gal}(F[x_i]/F) = 1$  for all  $i = 1, 2, 3$  and  $\text{Gal}(F[\Delta]/F) \cong \mathbb{Z}/(2) = \langle \varphi \rangle$  where the action of  $\varphi$  is  $\varphi(\Delta) = -\Delta$ . Here  $\Delta^2 \in F$  and  $F[\Delta]$  is the splitting field of the polynomial  $t^2 - \Delta^2$  over  $F$ , so it is Galois. However, we may conclude that the fields  $F[x_1], F[x_2]$  and  $F[x_3]$  are not the splitting fields of any polynomials over  $F$ .

The previous example illustrates the fundamental theorem of Galois theory: if  $E/F$  is the splitting field of a *separable* polynomial  $f(t) \in F[t]$ , then the map

$$H \longleftrightarrow E^H = \{a \in E : \varphi(a) = a \text{ for all } \varphi \in H\}$$

is a 1-1 correspondence between

$$\text{subgroups of } \text{Gal}(E/F) \longleftrightarrow \text{subfields of } E$$

which reverses inclusions. In addition,  $H$  is a normal subgroup of  $\text{Gal}(E/F)$  if and only if  $E^H$  is the splitting field of some separable polynomial over  $F$  (i.e.,  $E^H$  is normal over  $F$ ), and if  $H$  is *normal* in  $\text{Gal}(E/F)$ , then

$$\text{Gal}(E^H/F) \cong \text{Gal}(E/F)/H.$$

In our example, the only proper normal subgroup of  $S_3$  is  $A_3$ , and

$$\text{Gal}(E^{A_3}/F) = \text{Gal}(F[\Delta]/F) \cong \mathbb{Z}_2 \cong S_3/A_3 = \text{Gal}(E/F)/A_3.$$

We now formally establish Galois' fundamental group-field pairing as follows.

**5.5.11 Theorem.** [Fundamental Theorem of Galois Theory] *Let  $E$  be a finite dimensional Galois extension of a field  $F$  (i.e., the conditions of Theorem 5.5.7 holds) and let  $G = \text{Gal}(E/F)$ . Let  $\Gamma = \{H\}$ , the set of subgroups of  $G$ , and  $\Sigma$ , the set of intermediate fields between  $E$  and  $F$  (the subfields of  $E/F$ ). Then the map  $H \mapsto E^H$  and  $K \mapsto \text{Gal}(E/K)$ ,  $H \in \Gamma$ ,  $K \in \Sigma$ , are inverses to each other. In particular, they are one-to-one correspondences between  $\Gamma$  and  $\Sigma$ . Moreover, the pairing  $\Gamma \leftrightarrow \Sigma$  has the following properties:*

1.  $H_1 \supseteq H_2$  if and only if  $E^{H_1} \subseteq E^{H_2}$ .
2.  $|H| = [E : E^H]$  and  $[G : H] = [E^H : F] = [E^H : E^G]$ .
3.  $H$  is normal in  $G$  if and only if  $E^H$  is normal over  $F$ . In this case,

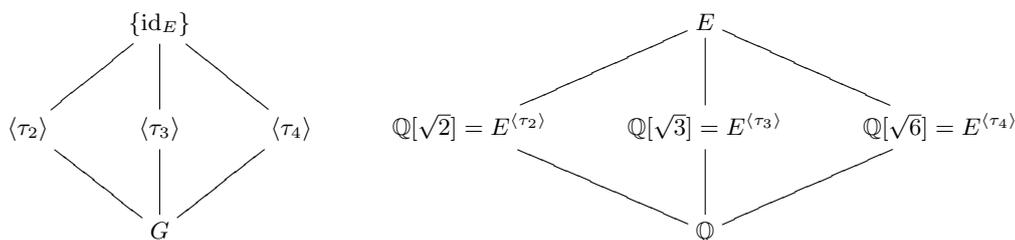
$$\text{Gal}(E^H/F) \cong G/H.$$

This is the main theorem. Most of our remaining field theory will be consequences of it.

*Proof.* Let  $H$  be a subgroup of  $G = \text{Gal}(E/F)$ . Since  $F = E^G$ ,  $F \subseteq E^H$  and  $E^H$  is thus a subfield of  $E$  containing  $F$ . Also,  $E/E^H$  is Galois. Applying the second supplementary result of Theorem 5.5.7 to  $H$  in place of  $G$  we see that  $\text{Gal}(E/E^H) = H$ . By Lemma 5.5.4,  $|H| = |\text{Gal}(E/E^H)| = [E : E^H]$ . Now let  $K$  be any subfield of  $E/F$ . Then  $\text{Gal}(E/K) \subseteq G = \text{Gal}(E/F)$ , so  $\text{Gal}(E/K)$  is a subgroup of  $G$ . It is clear also that  $E$  is a splitting field over  $K$  of a separable polynomial. Hence, the first supplementary result of Theorem 5.5.7 applied to the pair  $E$  and  $K$  shows that  $K = E^{\text{Gal}(E/K)}$ . We have now shown that the specified maps between  $\Gamma$  and  $\Sigma$  are inverses. Also, we know that if  $H_1 \supseteq H_2$ , then  $E^{H_1} \subseteq E^{H_2}$ . Moreover, if  $E^{H_1} \subseteq E^{H_2}$ , then we have also that  $H_1 = \text{Gal}(E/E^{H_1}) \supseteq \text{Gal}(E/E^{H_2}) = H_2$ . Hence, (1) holds. The first part of (2) was noted before. Since  $|G| = [E : F] = [E : E^H][E^H : F] = |H|[E^H : F]$  and  $|G| = |H|[G : H]$ , evidently  $[E^H : F] = [G : H]$ . This proves (2).

If  $H \in \Gamma$ , then  $E^{\eta H \eta^{-1}} = \eta(E^H)$  for all  $\eta \in G$ . This is clear since the condition  $\sigma(x) = x$  is equivalent to  $(\eta\sigma\eta^{-1})(\eta(x)) = \eta(x)$ . It now follows that  $H$  is normal in  $G$  if and only if  $\eta(E^H) = E^H$  for every  $\eta \in G$ . Suppose  $H$  is normal in  $G$ . Then every  $\eta \in G$  maps  $E^H$  onto itself and so its restriction  $\bar{\eta} = \eta|_{E^H}$  is an automorphism of  $E^H/F$ . Thus, we have the restriction homomorphism  $\eta \rightarrow \bar{\eta}$  of  $G = \text{Gal}(E/F)$  into  $\text{Gal}(E^H/F)$ . The image  $\bar{G}$  is a group of automorphisms in  $E^H$  and clearly  $(E^H)^{\bar{G}} = F$ . Hence,  $\bar{G} = \text{Gal}(E^H/F)$ . The kernel of the homomorphism  $\eta \rightarrow \bar{\eta}$  is the set of  $\eta \in G$  such that  $\eta|_{E^H} = \text{id}_{E^H}$ . By the pairing, this is  $\text{Gal}(E/E^H) = H$ . Hence, the kernel is  $H$  and  $\bar{G} = \text{Gal}(E^H/F) \cong G/H$ . Since  $F = (E^H)^{\bar{G}}$ ,  $E^H$  is normal over  $F$  by Theorem 5.5.7. Conversely, suppose  $E^H$  is normal over  $F$ . Let  $a \in E^H$  and let  $f(x)$  be the minimal polynomial of  $a$  over  $F$ . Then  $f(x) = (x - a_1) \dots (x - a_m)$  in  $E^H[x]$  where  $a = a_1$ . If  $\eta \in G$ , then  $f(\eta(a)) = 0$  which implies that  $\eta(a) = a_i$  for some  $i$ . Thus,  $\eta(a) \in E^H$ . We have therefore shown that  $\eta(E^H) = E^H$ . Hence,  $H$  is a normal subgroup of  $G$ . This completes the proof of (3).  $\square$

**5.5.12 Example.** Let  $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$  be a splitting field of  $f(x) = (x^2 - 2)(x^2 - 3)$ . Then  $E$  is Galois over  $\mathbb{Q}$ . Let  $G = \text{Gal}(E/\mathbb{Q})$ . Then  $|G| = [E : \mathbb{Q}] = 4$ . Since  $\mathbb{Q}(\sqrt{2})$  is a splitting field of  $x^2 - 2$ , it is Galois over  $\mathbb{Q}$  and its Galois group consists of 2 elements, namely  $\sigma_1 = \text{id}$  and  $\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$ . Each automorphism extends to an automorphism of  $E$  in two different ways;  $\sqrt{3} \mapsto \sqrt{3}$  or  $\sqrt{3} \mapsto -\sqrt{3}$ . Then the four elements of  $G$  are  $\tau_1 = \text{id}_E$ ,  $\tau_2 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$ ,  $\tau_3 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$  and  $\tau_4 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$ . Each of these elements except  $\tau_1$  has order 2. Thus,  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . Hence, the subgroup-intermediate subfield correspondence for the fundamental theorem of Galois theory is shown in the lattice diagrams



**5.5 Exercises.** 1. Let  $E = F(t)$  where  $t$  is transcendental over  $F$  and write any non-zero element of  $E$  as  $u = f(t)/g(t)$  where  $(f(t), g(t)) = 1$ . Call the maximum of degrees of  $f$  and  $g$  the *degree* of  $u$ . Show that if  $x$  and  $y$  are indeterminates then  $f(x) - yg(x)$  is irreducible in  $F[x, y]$  and hence is irreducible in  $F(y)[x]$ . Show that  $t$  is algebraic over  $F(u)$  with minimal polynomial the monic polynomial which is a multiple in  $F(u)$  of  $f(x) - ug(x)$ . Hence, conclude that  $[F(t) : F(u)] = 1$ , and  $F(u) = F(t)$  if and only if  $\deg u = 1$ . Note that this implies

$$u = \frac{at + b}{ct + d}$$

where  $ad - bc \neq 0$ . Therefore, deduce that  $\text{Gal}(E/F)$  is the set of maps  $h(t) \mapsto h(u)$  where  $u$  is of the form indicated.

2. Let  $F \subseteq K \subseteq E$  and  $E$  Galois over  $F$ . Prove that  $E$  is Galois over  $K$ .
3. Show that every element of  $K(x_1, \dots, x_n)$  which is not in  $K$  is transcendental over  $K$ .
4. Show that in the subgroup-intermediate subfield correspondence given in the fundamental theorem of Galois theory, the subfield corresponding to the intersection of two subgroups  $H_1$  and  $H_2$  is the subfield generated by the composite field  $E^{H_1}E^{H_2}$ , the smallest subfield of  $E$  generated by  $E^{H_1}$  and  $E^{H_2}$ , and the intersection of two intermediate fields  $K_1$  and  $K_2$  corresponds to the subgroup generated by  $\text{Gal}(E/K_1) \cup \text{Gal}(E/K_2)$ .
5. Use the fact that any finite group  $G$  is isomorphic to a subgroup of  $S_n$  (Cayley's theorem) to prove that given any finite group  $G$ , there exist fields  $E$  and  $E/F$  such that  $\text{Gal}(E/F) = G$ .
6. Let  $E = \mathbb{Q}(r)$  where  $r^3 + r^2 - 2r - 1 = 0$ . Verify that  $r' = r^2 - 2$  is also a root of  $x^3 + x^2 - 2x - 1 = 0$ . Determine  $\text{Gal}(E/\mathbb{Q})$ . Show that  $E$  is normal over  $\mathbb{Q}$ .
7. Let  $\alpha = \sqrt{2 + \sqrt{2}}$  in  $\mathbb{R}$ ,  $f(x)$  the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  and  $E$  is a splitting field of  $f(x)$  over  $\mathbb{Q}$ .
  - (a) Compute  $f(x)$  and  $[E : \mathbb{Q}]$ .
  - (b) Find  $G = \text{Gal}(E/\mathbb{Q})$  and draw a lattice diagram for the subgroup-intermediate subfield correspondence for the fundamental theorem of Galois theory.
8. Let  $(\mathbb{Z}/(p))(t)$  where  $t$  is transcendental over  $\mathbb{Z}/(p)$ . Let  $G$  be the group of automorphisms generated by the automorphism of  $E$  such that  $t \mapsto t + 1$ . Determine  $F = E^G$  and  $[E : F]$ .

## 5.6 Some Consequences of Galois Theory

In this section, we shall derive some consequences of Galois theory including another proof of the fundamental theorem of algebra.

**5.6.1 Theorem.** *Let  $K$  be a finite dimensional separable extension of a field  $F$ . Then there are only finitely many fields  $L$  such that  $K \supseteq L \supseteq F$ .*

*Proof.* Since  $K/F$  is finite separable, by primitive element theorem,  $K = F[\alpha]$  for some  $\alpha \in K$ . Let  $E$  be the splitting field of  $m_{\alpha, F}(x)$ . Then  $E$  is Galois over  $F$  and  $E \subseteq K \subseteq F$ . By fundamental theorem of Galois theory, the number of intermediate fields between  $E$  and  $F$  is the number of subgroups of  $\text{Gal}(E/F)$ . Hence, the number of intermediate fields between  $K$  and  $F$  is at most the number of subgroups of  $\text{Gal}(E/F)$ .  $\square$

**5.6.2 Remark.** If  $G = \text{Gal}(E/F)$ , then  $K = E^H$  for some subgroup  $H$  of  $G$  and the fields  $L$  such that  $K \supseteq L \supseteq F$  are in 1-1 correspondence with the subgroups  $J$  of  $G$  such that  $G \supseteq J \supseteq H$ .

The primitive element theorem and the previous theorem both *fail* for inseparable extensions as shown in the following example.

**5.6.3 Example.** Let  $F$  be an infinite field of prime characteristic  $p$  and let  $u$  and  $v$  be indeterminates over  $F$ . Consider

$$F(u, v) \supseteq F(u^p, v^p)$$

It is easy to see that  $[F(u, v) : F(u^p, v^p)] = p^2$ . On the other hand, if  $z \in F(u, v)$ , then  $z^p \in F(u^p, v^p)$ , so

$$[F(u^p, v^p)(z) : F(u^p, v^p)] \leq p.$$

Hence, there is no  $z$  such that  $F(u, v) = F(u^p, v^p)(z)$ , that is, no primitive element.

On the other hand, the nonexistence of a primitive element shows that the fields

$$F(u^p, v^p)(u + \alpha v),$$

for  $\alpha \in F$ , are all distinct. To see this, assume that  $F(u^p, v^p)(u + \alpha v) = F(u^p, v^p)(u + \beta v) = E$  for some  $\alpha \neq \beta$  in  $E$ . Then  $u + \alpha v$  and  $u + \beta v$  in  $E$ , so

$$\alpha(u + \beta v) - \beta(u + \alpha v) = (\alpha - \beta)u \in E.$$

Since  $\alpha - \beta \neq 0$ ,  $u$  is in  $E$  which implies that  $v$  is also in  $E$ . Thus,  $E = F(u, v)$ , a contradiction. Hence, there are infinitely many fields  $L$  such that  $F(u, v) \supset L \supset F(u^p, v^p)$ .

Let us now recall some concepts from group theory. Suppose a group  $G$  acts on a set  $S$ . The action is *transitive* if for any  $s, t \in S$  there is a  $g \in G$  such that  $gs = t$ .

**5.6.4 Remark.** The action of  $G$  being transitive simply means that the action of  $G$  on  $S$  has only one orbit. Assuming  $G$  acts transitively on  $S$ . let  $s \in S$  and let

$$H = \{g \in G : gs = s\}$$

be the stabilizer of  $s$ . Then  $S$  can be identified with the set of left cosets

$$\{gH : g \in G\},$$

with  $G$  acting by left multiplication. Note that the subgroup  $H$  depends on the choice of  $s$  and choosing a different  $s$  will give a conjugate of  $H$ . More precisely, if  $s \in S$  and  $x \in G$ , and

$$H = \text{stabilizer of } s = \{g \in G : gs = s\}$$

then

$$xHx^{-1} = \text{stabilizer of } xs = \{g \in G : g(xs) = xs\}.$$

(If  $gs = s$ , then  $(xgx^{-1})(xs) = xs$ .)

A basic example of this phenomenon is the action of  $S_n$  on  $\{1, 2, \dots, n\}$ . The stabilizer of  $i \in \{1, 2, \dots, n\}$  is  $\text{Sym}\{1, \dots, i-1, i+1, \dots, n\}$  which may be identified with  $S_{n-1}$ , but  $S_{n-1}$  has  $n$  conjugates in  $S_n$ .

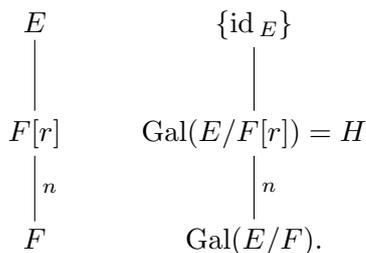
**5.6.5 Theorem.** Let  $E$  be the splitting field over  $F$  of a separable polynomial  $f(x) \in F[x]$  which is irreducible over  $F$ . Then  $\text{Gal}(E/F)$  acts transitively on the roots of  $f(x)$ . Hence,  $\text{Gal}(E/F)$  may be identified with a subgroup of  $\text{Sym}\{r_1, \dots, r_n\}$  which acts transitively on  $\{r_1, \dots, r_n\}$ , the roots of  $f(x)$  in  $E$ .

*Proof.* This is implicit in the proof of Theorem 5.2.9. For, if  $r$  and  $s$  are roots of  $f(x)$  in  $E$ , then

$$F(r) \cong F[x]/(f(x)) \cong F(s) \quad \text{with} \quad r \mapsto x + (f(x)) \mapsto s$$

by an isomorphism which fixes  $F$  pointwise. Let  $\eta : F(r) \rightarrow F(s)$  be this isomorphism. By Theorem 5.2.9,  $\eta$  extends to an isomorphism  $\hat{\eta} : E \rightarrow E$ . Then  $\hat{\eta} \in \text{Gal}(E/F)$  and  $\hat{\eta}(r) = s$ , which is what we need to prove. □

- 5.6.6 Remarks.**
1. The hypothesis that  $f(x)$  be irreducible over  $F$  is essential. For, example, if  $f(x) = f_1(x) \dots f_k(x)$  where  $f_1(x), \dots, f_k(x)$  are distinct irreducible polynomials, then all one can say is that  $\text{Gal}(E/F)$  permutes the roots of each  $f_i(x)$  among themselves. It is still true that  $\text{Gal}(E/F)$  can be identified with a subgroup of the group of permutations of the roots, but not a transitive one.
  2. Assume that  $f(x)$  is irreducible and separable over  $F$  of degree  $n$ ,  $E/F$  is a splitting field for  $f(x)$  over  $F$  and  $r$  is one root of  $f(x)$ . Then the fundamental theorem of Galois theory gives the following picture



Thus,  $F[r] = E^H$  where  $H$  is a subgroup of index  $n$  in  $G$ .

The basic Theorems 5.2.6 and 5.2.9 give the existence and uniqueness of splitting fields. That is, if  $F$  is a field and  $f(x)$  is a monic polynomial in  $F[x]$ , then

1. A splitting field  $E$  for  $f(x)$  exists.  $E$  is generated over  $F$  by the roots of  $f(x)$  and  $f(x)$  splits into linear factors in  $E[x]$ .
2. The splitting field  $E/F$  is unique up to isomorphism over  $F$ . In other words, if  $E'/F$  is another splitting field for  $f(x)$  over  $F$ , then there is an isomorphism

$$\varphi : E \rightarrow E'$$

which is identity on  $F$ .

*What does this mean if we are searching for the splitting field of some  $f(x) \in \mathbb{Q}[x]$ ?*

It means that we can realize  $E$  as a subfield of  $\mathbb{C}$ . More precisely,  $f(x)$  is a product of linear factors in  $\mathbb{C}[x]$ , say  $f(x) = (x - \alpha_1) \dots (x - \alpha_k)$  and we can take  $E$  to be the field  $\mathbb{Q}(\alpha_1, \dots, \alpha_k) \subseteq \mathbb{C}$ . This could be very helpful because it allows us to work in a concrete and explicit field.

The fundamental theorem of algebra (*every  $f(x) \in \mathbb{C}[x]$  is a product of linear factors*) is usually proved in complex analysis and there is also a topological proof. Here we present a proof based on Galois theory and the intermediate value theorem from real analysis or calculus. We shall start with some basic results.

**5.6.7 Theorem.** *Let  $f(x) \in \mathbb{R}[x]$  be a polynomial of odd degree. Then  $f(x)$  has a root in  $\mathbb{R}$ .*

*Proof.* It is enough to prove for a monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

with  $a_i \in \mathbb{R}$  and  $n$  is odd. If  $a = |a_0| + \dots + |a_{n-1}|$ , then it is easy to see that  $f(a) > 0$  and  $f(-a) < 0$ . By intermediate value theorem (because  $f(x)$  is continuous), there exists  $r \in \mathbb{R}$  such that  $f(r) = 0$ .  $\square$

Consider  $\alpha + \beta i$  with  $\alpha, \beta \in \mathbb{R}$ . If  $\gamma = \sqrt{\alpha^2 + \beta^2}$ , then

$$(\sqrt{(\gamma + \alpha)/2} + i\sqrt{(\gamma - \alpha)/2})^2 = \alpha + \beta i.$$

Hence, we have proved

**5.6.8 Theorem.** *Every complex number has a square root.*

**5.6.9 Theorem.** *If  $K$  is a field containing  $\mathbb{C}$ , then  $[K : \mathbb{C}] \neq 2$ .*

*Proof.* Suppose conversely that  $[K : \mathbb{C}] = 2$  and let  $K = \mathbb{C} + \mathbb{C}u$  for some  $u \in K$ . Then  $u$  satisfies a polynomial

$$f(x) = x^2 - bx + c$$

of degree two over  $\mathbb{C}$ , since  $1, u, u^2$  are linearly dependent over  $\mathbb{C}$ . The roots of  $f(x)$  are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2}$$

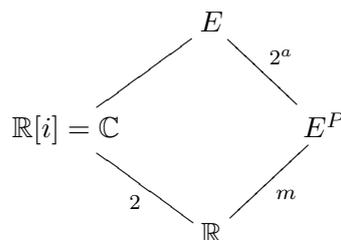
which lie in  $\mathbb{C}$ , since every element of  $\mathbb{C}$  has a square root in  $\mathbb{C}$ . Thus,  $u \in \mathbb{C}$ , a contradiction.  $\square$

Recall that a finite  $p$ -group  $G$  is nilpotent, so by Exercise 3.3, a maximal subgroup  $M$  of  $G$  is normal and  $[G : M] = p$ , i.e., if  $G$  is a nontrivial finite  $p$ -group, then  $G$  has a normal subgroup of index  $p$ .

**5.6.10 Theorem.** [Fundamental Theorem of Algebra] *Let  $f(x) \in \mathbb{C}[x]$ . Then  $f(x)$  is a product of linear factors in  $\mathbb{C}[x]$ .*

*Proof.* Let  $\bar{\phantom{x}} : \mathbb{C} \rightarrow \mathbb{C}$  denote the complex conjugation. Then  $g(x) = f(x)\overline{f(x)} \in \mathbb{R}[x]$ . Let  $E$  be a splitting field for  $g(x)(x^2 + 1)$  over  $\mathbb{R}$  and identify  $\mathbb{C}$  with the subfield of  $E$  generated by the roots of  $x^2 + 1$ . Since the characteristic is zero, all polynomials are separable, so  $E$  is the splitting field of a separable polynomial. Hence,  $E$  is Galois over  $\mathbb{R}$  by Theorem 5.5.7.

Let  $G = \text{Gal}(E/\mathbb{R})$ ,  $|G| = 2^am$ , where  $m$  is odd, and let  $P$  be a Sylow 2-subgroup of  $G$ . Consider the diagram of fields



Thus,  $E^P = \{\alpha \in E : \varphi(\alpha) = \alpha \text{ for all } \varphi \in P\}$  is an extension of  $\mathbb{R}$  of odd degree  $m$ , by the fundamental Galois correspondence. If  $u \in E^P$ , the minimal polynomial  $q(x)$  of  $u$  over  $\mathbb{R}$  is an irreducible polynomial in  $\mathbb{R}[x]$  of odd degree, so it has a root in  $\mathbb{R}$  by Theorem 5.6.7. Since  $q(x)$  is irreducible, it has degree one. Hence,  $E^P = \mathbb{R}$  and  $G = P$ , so  $|G| = 2^a$ . By the fundamental theorem of Galois theory,  $\mathbb{C} = E^H$  where  $H$  is a subgroup of  $G$  of index 2. If  $H \neq \{1\}$ , it has a subgroup  $K$  of index 2, so

$$\mathbb{R} \xrightarrow{2} \mathbb{C} = E^H \xrightarrow{2} E^K \xrightarrow{\quad} E.$$

Thus,  $[E^K : \mathbb{C}] = 2$  which contradicts Theorem 5.6.9. Hence,  $|G| = 2$ ,  $H = \{1\}$  and  $\mathbb{C} = E^H = E$ . Therefore,  $\mathbb{C}$  is a splitting field for  $g(x)(x^2 + 1) = f(x)\overline{f(x)}(x^2 + 1)$  over  $\mathbb{R}$ , so  $g(x)(x^2 + 1)$  (and hence  $f(x)$ ) splits into linear factors in  $\mathbb{C}[x]$ . □

The fundamental theorem of algebra was first rigorously proved by Gauss in 1816 (his doctoral dissertation in 1798 provides a proof using geometric considerations requiring some topological justification). There was a proof due to Laplace in 1795. However, Laplace’s proof was deemed unacceptable because he assumed the existence of a splitting field for polynomials (i.e., that the roots existed somewhere in some field), which had not been established at that time. The elegant above proof was given by Artin.

## 5.7 Finite Fields

Let  $k$  be a field of  $q$  elements. Then  $(k, +)$  is an abelian group, so  $q \cdot 1 = 0$ . Thus,  $F$  is of characteristic prime  $p > 0$  and  $p \mid q$ , so it contains  $\mathbb{Z}/p\mathbb{Z}$  as a subfield and it is a finite extension of  $\mathbb{Z}/p\mathbb{Z}$ . Its cardinality  $|k| = q = p^d$  is a power of  $p$ , with  $d = [k : \mathbb{Z}/p\mathbb{Z}]$ . This also indicates that the additive group of  $k$  is a direct sum of  $d$  copies of cyclic group of order  $p$ . We shall restate the following fact (Theorem 5.4.13).

**5.7.1 Theorem.**  $k^\times$  is cyclic of order  $q - 1$ .

Some immediate consequences of the above theorem are as follows.

**5.7.2 Corollary.** *The field  $k$  consists of the solutions to  $x^q - x = 0$  in an algebraic closure of  $\mathbb{Z}/p\mathbb{Z}$  containing  $k$ .*

**5.7.3 Corollary.** *There is an element  $\alpha \in k$  such that  $k = (\mathbb{Z}/p\mathbb{Z})[\alpha]$ , that is,  $k$  is a simple extension of the prime field  $\mathbb{Z}/p\mathbb{Z}$ .*

**5.7.4 Corollary.** *For each positive divisor  $r$  of  $q - 1 (= |k^\times|)$  there are exactly  $\phi(r)$  elements in  $k^\times$  of order  $r$ .*

**5.7.5 Corollary.** *Let  $p$  be a prime and  $d$  a positive integer. Then, up to isomorphism, there is exactly one field of order  $q = p^d$ .*

*Proof.* Let  $E$  be a splitting field of  $f(t) = t^{p^d} - t$  over  $\mathbb{Z}/p\mathbb{Z}$  in an algebraic closure of  $\mathbb{Z}/p\mathbb{Z}$ . By Theorem 5.2.9,  $E$  is unique up to isomorphism. It consists of the roots of  $t^{p^d} = t$  in the algebraic closure of  $\mathbb{Z}/p\mathbb{Z}$ . Thus,  $|E|$  is the number of roots of  $t^{p^d} - t$ . Since  $f'(t) = -1$ ,  $f(t)$  is separable, so  $|E| = p^d$ . Thus, we have constructed a field of order  $q = p^d$ , namely  $E$ , the splitting field of  $f(t)$  over  $\mathbb{Z}/p\mathbb{Z}$ .  $\square$

For  $q = p^d$ , we may write  $\mathbb{F}_q$  for the (unique up to isomorphism) field of  $q$  elements. Also, we may write  $\mathbb{F}_p$  for  $\mathbb{Z}/p\mathbb{Z}$ .

**5.7.6 Corollary.** *Given any positive integer  $d$ , there exists an irreducible polynomial of degree  $n$  over  $\mathbb{F}_p$ .*

*Proof.* By Corollary 5.7.3,  $\mathbb{F}_{p^d} = \mathbb{F}_p[\alpha]$  for some  $\alpha \in \mathbb{F}_{p^d}$ . Let  $f(t)$  be the minimal polynomial of  $\alpha$  over  $\mathbb{F}_p$ . Then  $\mathbb{F}_{p^d} = \mathbb{F}_p[\alpha] \cong \mathbb{F}_p[t]/(f(t))$  shows  $\deg f(t) = [\mathbb{F}_{p^d} : \mathbb{F}_p] = d$ .  $\square$

Next, we shall study finite extensions of a finite field. For simplicity,  $k$  stands for the finite field  $\mathbb{F}_q$ . Let  $k_n$  be a degree  $n$  field extension of  $k$ . If  $k_m$  is an intermediate field of degree  $m$  over  $k$ , then  $k_n$  is a vector space over  $k_m$ , so  $m$  divides  $n$ . Conversely, any degree  $m$  extension of  $k$  within an algebraic closure of  $k$  with  $m \mid n$  is a subfield of  $k_n$  by Corollary 5.7.2 since  $m \mid n$  implies  $(q^m - 1) \mid (q^n - 1)$ .

Consider the map  $\sigma$  on  $k_n$  which sends  $x$  to  $x^q$ . From

$$\sigma(x + y) = (x + y)^q = x^q + y^q = \sigma(x) + \sigma(y) \quad \text{and} \quad \sigma(xy) = (xy)^q = x^q y^q = \sigma(x)\sigma(y),$$

we see that  $\sigma$  is an endomorphism. Furthermore,  $\sigma(x) = x^q = 0$  implies  $x = 0$ . So  $\sigma$  is one-to-one. As  $k_n$  is finite, we have shown that  $\sigma$  is an automorphism of  $k_n$ . Finally,  $\sigma(x) = x^q = x$  for  $x \in k$ , this shows that  $\sigma \in \text{Gal}(k_n/k)$ , called the **Frobenius' automorphism**. Let  $r$  be the order of  $\sigma$ . Then

$$\sigma^r(x) = x^{q^r} = x \quad \text{for all } x \in k_n$$

implies  $r = n$  since  $k_n^\times$  is cyclic of order  $q^n - 1$ . Hence,  $\text{Gal}(k_n/k)$  contains the cyclic group  $\langle \sigma \rangle$  of order  $n$ . Since  $|\text{Gal}(k_n/k)| \leq [k_n : k] = n$ ,  $\text{Gal}(k_n/k) = \langle \sigma \rangle$  and so the field  $k_n$  is Galois over  $k$ . We record this in

**5.7.7 Theorem.** *The field  $k_n$  is Galois over  $k$  with the Galois group  $\text{Gal}(k_n/k)$  cyclic of order  $n$ , generated by the Frobenius' automorphism  $\sigma$ .*

Note that an element  $x \in k_n$  lies in  $k$  if and only if it satisfies  $x^q = x$ , in other words, if and only if it is fixed by the Frobenius' automorphism, or equivalently, by the group  $\text{Gal}(k_n/k)$ . Using

$G = \text{Gal}(k_n/k)$ , we define two important maps, called **trace** and **norm**, denoted by  $\text{Tr}_{k_n/k}$  and  $\text{N}_{k_n/k}$ , respectively, from  $k_n$  to  $k$  as follows:

$$\text{Tr}_{k_n/k} : x \mapsto \sum_{\tau \in G} \tau(x) = \sum_{i=1}^n \sigma^i(x),$$

$$\text{N}_{k_n/k} : x \mapsto \prod_{\tau \in G} \tau(x) = \prod_{i=1}^n \sigma^i(x).$$

One can check easily that the images of trace and norm maps are in  $k$ . It is clear that  $\text{Tr}_{k_n/k}$  is a homomorphism from the additive group  $k_n$  to the additive group  $k$  and  $\text{N}_{k_n/k}$  is a homomorphism from  $k_n^\times$  to  $k^\times$ . Next we investigate their images. We shall first need

**5.7.8 Lemma.** *If  $E$  is an extension field of a field  $F$ , then the automorphisms in  $\text{Gal}(E/F)$  are  $E$ -linearly independent  $F$ -linear transformations.*

*Proof.* Suppose otherwise. Let  $a_1\tau_1 + \cdots + a_r\tau_r = 0$  be a shortest nontrivial linear relation with  $a_1, \dots, a_r \in E^\times$  and  $\tau_1, \dots, \tau_r \in \text{Gal}(E/F)$ . Then  $r \geq 2$  and  $\tau_i$  are distinct. Let  $y \in E$  be such that  $\tau_1(y) \neq \tau_2(y)$ . From  $\sum_{i=1}^r a_i\tau_i = 0$  we get

$$\sum_{i=1}^r a_i\tau_i(yx) = \sum_{i=1}^r a_i\tau_i(y)\tau_i(x) = 0$$

for all  $x \in E$ , so  $\sum_{i=1}^r a_i\tau_i(y)\tau_i = 0$ . This yields another nontrivial relation

$$\sum_{i=1}^r a_i\tau_i(y)\tau_i - \tau_1(y) \sum_{i=1}^r a_i\tau_i = \sum_{i=2}^r a_i(\tau_i(y) - \tau_1(y))\tau_i = 0,$$

which is shorter than the relation we started with, a contradiction.  $\square$

**5.7.9 Theorem.** [Hilbert Theorem 90]

1. The norm map  $\text{N}_{k_n/k}$  from  $k_n^\times$  to  $k^\times$  is surjective with the kernel consisting of  $x/\sigma(x)$ ,  $x \in k_n^\times$ .
2. The trace map  $\text{Tr}_{k_n/k}$  from  $k_n$  to  $k$  is surjective with the kernel consisting of  $x - \sigma(x)$ ,  $x \in k_n$ .

*Proof.* (1) Since  $\text{N}_{k_n/k}(\sigma(x)) = \prod_{i=1}^n \sigma^{i+1}(x) = \prod_{i=1}^n \sigma^i(x) = \text{N}_{k_n/k}(x)$ , so  $x/\sigma(x)$  lies in the kernel of the norm map for all  $x \in k_n^\times$ . Further,  $x/\sigma(x) = y/\sigma(y)$  if and only if  $xy^{-1} \in k^\times$ , hence the elements  $x/\sigma(x)$  with  $x \in k_n^\times$  form a subgroup of  $k_n^\times$  of order  $(q^n - 1)/(q - 1)$ . Thus, it is equal to the whole kernel if and only if the norm map is surjective. To see  $\text{N}_{k_n/k}$  is onto, observe that

$$\text{N}_{k_n/k}(x) = \prod_{i=1}^n \sigma^i(x) = x \cdot x^q \cdot x^{q^2} \cdots x^{q^{n-1}} = x^{1+q+q^2+\cdots+q^{n-1}} = x^{(q^n-1)/(q-1)}$$

for all  $x \in k_n^\times$ . Hence, any generator  $x$  of  $k_n^\times$  has  $\text{N}_{k_n/k}(x)$  of order  $q - 1$ .

(2) Since elements in  $\text{Gal}(k_n/k)$  are  $k$ -linear maps, the image of  $\text{Tr}_{k_n/k}(k_n)$  is a vector space over  $k$ , hence  $\text{Tr}_{k_n/k}(k_n) = 0$  or  $k$ . If  $\text{Tr}_{k_n/k} = 0$ , then  $\sum_{i=1}^n \sigma_i = 0$ , which is a nontrivial linear relation among elements of  $\text{Gal}(k_n/k)$ , so impossible by Lemma 5.7.8. Therefore,  $\text{Tr}_{k_n/k}$  is surjective. Then its kernel has order  $q^{n-1}$ . Clearly,  $\text{Tr}_{k_n/k}(\sigma(x)) = \text{Tr}_{k_n/k}(x)$  so that kernel contains  $x - \sigma(x)$  for all  $x \in k_n$ . Further,  $x - \sigma(x) = y - \sigma(y)$  if and only if  $x - y \in k$ , so the group  $\{x - \sigma(x) : x \in k_n\}$  has order  $q^n/q$ , thus is equal to the kernel.  $\square$

**5.7.10 Remark.** The Hilbert Theorem 90 for norm and trace maps is usually proved using first cohomology group of the Galois group (à la Noether). When the base field is finite, we may use counting argument, as shown above.

**5.7.11 Definition.** Given  $z \in k_n$ , it defines a  $k$ -linear transformation  $L_z$  on  $k_n$  by  $x \mapsto zx$ , that is, multiplication by  $z$ . The **trace** and **determinant** of  $L_z$  are defined as the trace and determinant of any  $n \times n$  matrix representing  $L_z$ .

They are in fact given by  $\text{Tr}_{k_n/k}$  and  $N_{k_n/k}$  of  $z$ . More precisely, we have

**5.7.12 Theorem.** Let  $z \in k_n$  and define  $L_z$  as above. Then

1.  $\text{Tr } L_z = \text{Tr}_{k_n/k}(z)$  and  $\det L_z = N_{k_n/k}(z)$ .
2. Suppose  $k(z) = k_n$ . Let  $f(t) = t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n$  be the minimal polynomial of  $z$  over  $k$ . Then

$$-a_1 = -\text{Tr}_{k_n/k}(z) \quad \text{and} \quad a_n = (-1)^n N_{k_n/k}(z).$$

*Proof.* We shall prove (1) and (2) under the assumption (2) and leave (1) for the case  $k(z)$  being a proper subfield  $k_n$  as an exercise. For each  $\tau \in \text{Gal}(k_n/k)$ ,  $0 = \tau(f(z)) = f(\tau(z))$ , hence  $\tau(z)$  is also a root of  $f(x)$ . Further, if  $\tau$  and  $\tau'$  are two different elements in  $\text{Gal}(k_n/k)$ , then  $\tau(z) \neq \tau'(z)$  (otherwise they would agree on  $k(z) = k_n$ ). This shows that  $z$  has  $n$  distinct images under  $\text{Gal}(k_n/k)$  and they are the roots of  $f(t)$ . Therefore,

$$-a_1 = \text{the sum of roots of } f(t) = \text{Tr}_{k_n/k}(z)$$

and

$$(-1)^n a_n = \text{the product of roots of } f(t) = N_{k_n/k}(z).$$

This proves (2). For (1), we know that  $L_z$  satisfies  $f(t) = 0$ . As  $f(t)$  is irreducible over  $k$  and  $[k_n : k] = n$ ,  $f(t)$  is the characteristic polynomial of  $L_z$ . The companion matrix attached to  $L_z$  is

$$\begin{bmatrix} 0 & & & & -a_n \\ 1 & 0 & & & -a_{n-1} \\ & 1 & 0 & & -a_{n-2} \\ & & & \ddots & \vdots \\ & & & & 0 \\ & & & & 1 & -a_1 \end{bmatrix},$$

which has trace  $= -a_1$  and determinant  $= (-1)^n a_n$ . This proves (1). □

- 5.6 Exercises.**
1. Let  $k_6 = \mathbb{F}_{5^6}$  be the field with 15625 elements and let  $k = \mathbb{F}_5$  be its prime subfield.
    - (a) Determine the cardinality of the set of elements of  $k_6$  which generate  $k_6$  as a field over  $k$ .
    - (b) Draw a lattice diagram for the subgroup-intermediate subfield correspondence for the fundamental theorem of Galois theory of  $k_6/k$ .
  2. Let  $k$  be a finite field with finite extensions  $k_m$  and  $k_{mn}$  of degrees  $m$  and  $mn$ , respectively. Show that

$$\text{Tr}_{k_{mn}/k} = \text{Tr}_{k_m/k} \circ \text{Tr}_{k_{mn}/k_m} \quad \text{and} \quad N_{k_{mn}/k} = N_{k_m/k} \circ N_{k_{mn}/k_m}.$$

3. Let  $z \in k_n$ . Suppose  $k(z) = k_m$  is a proper subfield of  $k_n$ . Prove that

$$\text{Tr } L_z = \text{Tr}_{k_n/k}(z) = (n/m)\text{Tr}_{k_m/k}(z) \quad \text{and} \quad \det L_z = N_{k_m/k}(z)^{n/m}.$$

4. (a) (Normal Basis Theorem) There exists an element  $z \in k_n$  such that the set  $\{\tau(z) : \tau \in \text{Gal}(k_n/k)\}$  is a basis of  $k_n$  over  $k$ . [Hint: Consider the minimal polynomial of the Frobenius' automorphism  $\sigma$ .]
  - (b) For  $z$  in (a), we have  $\text{Tr}_{k_n/k}(z) \neq 0$ . [Hint: Express an element in  $k_n$  as a  $k$ -linear combination of  $\{\tau(z)\}$ . Then show  $\text{Tr}_{k_n/k}(k_n) = k\text{Tr}_{k_n/k}(z)$ .]

## 5.8 Cyclotomic Extensions

In this section, we shall study other important examples of Galois extension, called cyclotomic fields, and compute their Galois groups. Note that “Cyclotomy” is Greek for the art of dividing a circle into equal parts.

**5.8.1 Theorem.** *Let  $K$  be a field of characteristic 0 and let  $E$  be a splitting field of  $x^n - 1$  over  $K$ . Then  $\text{Gal}(E/K)$  is isomorphic to a subgroup of  $\text{Aut } \mathbb{Z}/(n) \cong (\mathbb{Z}/(n))^\times$ . In particular,  $\text{Gal}(E/K)$  is abelian.*

*Proof.* Since  $(x^n - 1)' = nx^{n-1} \neq 0$ , the roots of  $x^n - 1$  (in  $E$ ) are distinct, say

$$x^n - 1 = (x - 1)(x - \alpha_2) \dots (x - \alpha_n).$$

Then  $A = \{z \in E : z^n = 1\} = \{1, \alpha_2, \dots, \alpha_n\}$  is a finite subgroup of  $E^\times$ , so it is cyclic of order  $n$  by Theorem 5.4.13. Any automorphism of  $E$ ,  $\theta : E \rightarrow E$  induces an automorphism  $\theta : A \rightarrow A$ , so there is a group homomorphism from  $\text{Gal}(E/K)$  to  $\text{Aut } A$  defined by  $\theta \mapsto \theta|_A$ . This homomorphism is 1-1 since any automorphism of  $E/K$  is completely determined by its action on the roots of  $x^n - 1$ . Hence,  $\text{Gal}(E/K)$  is isomorphic to a subgroup of  $\text{Aut } A = \text{Aut } \mathbb{Z}/(n)$ .  $\square$

**5.8.2 Definition.** We call a Galois extension field  $E/F$  **abelian [cyclic] over  $F$**  if  $\text{Gal}(E/F)$  is abelian [cyclic].

Hence, the above theorem provides an example of abelian extension.

Our next objective is to show that if  $E$  is a splitting field of  $x^n - 1$  over  $\mathbb{Q}$ , then  $\text{Gal}(E/\mathbb{Q}) \cong \text{Aut } \mathbb{Z}/(n) \cong (\mathbb{Z}/(n))^\times$ . We first recall some properties of the cyclic group of order  $n$ . Let  $\mathbb{Z}/(n) = \langle a \rangle$ . Then

1. For each divisor  $d$  of  $n$ ,  $\mathbb{Z}/(n)$  has a unique subgroup of order  $d$ , generated by  $a^{n/d}$ .
2. All subgroups of  $\mathbb{Z}/(n)$  are as in (1). Thus, the number of subgroups of  $\mathbb{Z}/(n)$  is equal to the number of divisors of  $n$ .
3. If  $x, y \in \mathbb{Z}/(n)$ , then

$$\begin{aligned} \langle x \rangle = \langle y \rangle &\iff o(x) = o(y) \\ &\iff \theta(x) = y \text{ for some } \theta \in \text{Aut } \mathbb{Z}/(n) \\ &\iff x \text{ and } y \text{ lie in the same orbit under the action of } \text{Aut } \mathbb{Z}/(n). \end{aligned}$$

**5.8.3 Definition.** An element  $\omega$  in a field  $K$  is an  **$n$ th root of unity** if  $\omega^n = 1$ , it is a **primitive  $n$ th root of unity** if  $o(\omega) = n$  in  $K^\times$ , that is,  $\omega^n = 1$  and  $\omega^m \neq 1$  if  $1 \leq m < n$ .

In the complex numbers  $\mathbb{C}$ , the  $n$ th roots of unity are the powers of

$$\omega = e^{2\pi i/n} = \cos(2\pi/n) + i \sin(2\pi/n) \text{ and } \omega^t = e^{2\pi it/n} = \cos(2\pi t/n) + i \sin(2\pi t/n).$$

Thus,  $\mathbb{Q}[\omega]$  is the splitting field of  $x^n - 1$  over  $\mathbb{Q}$ , so  $[\mathbb{Q}[\omega] : \mathbb{Q}]$  is the degree of the minimal polynomial of  $\omega$  over  $\mathbb{Q}$ . We know that the set  $U$  of the  $n$ th roots of unity is a cyclic group of order  $n$  under multiplication. Hence, the number of primitive  $n$ th roots of 1, that is, the number of generators of  $U$ , is  $\phi(n)$ .

**5.8.4 Definition.** For a positive integer  $d$  and  $x$  an indeterminate, the  **$d$ th cyclotomic polynomial**,  $\Phi_d(x)$  is the product

$$\Phi_d(x) = \prod \{(x - \varepsilon) : \varepsilon \text{ is a primitive } d\text{th root of unity}\}.$$

If  $\eta \in \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$  and  $z$  is primitive  $n$ th root of unity, then  $\eta(z)$  is primitive. Hence,  $\eta(\Phi_n(x)) = \Phi_n(x)$  and so  $\Phi_n(x) \in \mathbb{Q}[x]$ . It is clear that  $\Phi_n(x) \mid (x^n - 1)$  and, in fact, since any  $n$ th root of unity has an order  $d \mid n$  we see that

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x). \quad (5.8.1)$$

**5.8.5 Remark.** The formula (5.8.1) provides us with an algorithm for calculating the polynomial  $\Phi_n(x)$ . To begin with we have

$$\Phi_1(x) = x - 1$$

and assuming we already know the  $\Phi_d(x)$  for proper divisors  $d$  of  $n$  then (5.8.1) gives us  $\Phi_n(x)$ . For example, for a prime  $p$ ,  $\Phi_1(x)\Phi_p(x) = x^p - 1$ , so we get

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Then  $\Phi_2(x) = x + 1$  and  $\Phi_3(x) = x^2 + x + 1$ , so

$$\Phi_4(x) = \frac{x^4 - 1}{\Phi_1(x)\Phi_2(x)} = x^2 + 1$$

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = x^2 - x + 1$$

$$\Phi_{12}(x) = \frac{x^{12} - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)} = x^4 - x^2 + 1.$$

Next, we observe that  $\Phi_n(x)$  has integer coefficients. This holds for  $n = 1$  and assuming it holds for every  $\Phi_d(x)$ ,  $d < n$ , we have  $x^n - 1 = \Phi_n(x)g(x)$  where  $g(x) = \prod_{d \mid n, d < n} \Phi_d(x)$  is a monic polynomial with integer coefficients. The division algorithm gives integral polynomials  $q(x)$  and  $r(x)$  with  $\deg r(x) < \deg g(x)$  such that  $x^n - 1 = q(x)g(x) + r(x)$ . Since  $q(x)$  and  $r(x)$  are unique in  $\mathbb{Z}[x]$  and  $x^n - 1 = \Phi_n(x)g(x)$  in  $\mathbb{Q}[x]$ , we see that  $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$ .

We shall now prove

**5.8.6 Theorem.** *The  $n$ th cyclotomic polynomial  $\Phi_n(x)$  has integer coefficients and is an irreducible polynomial in  $\mathbb{Q}[x]$ .*

*Proof.* Suppose that  $\Phi_n(x) = h(x)k(x)$ , where  $h(x), k(x) \in \mathbb{Z}[x]$  and  $h(x)$  is irreducible in  $\mathbb{Z}[x]$ , hence, in  $\mathbb{Q}[x]$  (Gauss' lemma). We may also assume that  $h(x)$  and  $k(x)$  are monic and so  $\deg h(x) \geq 1$ . Let  $p$  be a prime integer not dividing  $n$  and let  $\delta$  be a root of  $h(x)$ . Since  $(p, n) = 1$ ,  $\delta^p$  is a primitive  $n$ th root of unity. Assume that  $\delta^p$  is not a root of  $h(x)$ . Then  $\delta^p$  is a root of  $k(x)$ ; consequently  $\delta$  is a root of  $k(x^p)$ . Since  $h(x)$  is irreducible and has  $\delta$  as a root also,  $(h(x), k(x^p)) \neq 1$  and thus  $h(x) \mid k(x^p)$ . It follows (as mentioned earlier) that  $k(x^p) = h(x)l(x)$ , where  $l(x)$  is monic with integral coefficients. Since  $x^n - 1 = \Phi_n(x)g(x)$ , we have  $x^n - 1 = h(x)k(x)g(x)$ . We now pass to congruences modulo  $p$  or, which is the same thing, to equations in  $(\mathbb{Z}/(p))[x]$ . This gives

$$x^n - \bar{1} = \bar{h}(x)\bar{k}(x)\bar{g}(x) \quad (5.8.2)$$

where, in general, if  $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m \in \mathbb{Z}[x]$ , then  $\bar{f}(x) = \bar{a}_0x^m + \bar{a}_1x^{m-1} + \cdots + \bar{a}_m$ ,  $\bar{a}_i = a_i + (p)$  in  $\mathbb{Z}/(p)$ . Similarly, we have  $\bar{k}(x^p) = \bar{h}(x)\bar{l}(x)$ . Now, using  $\bar{a}^p = \bar{a}$  for any  $a \in \mathbb{Z}$ , we see that

$$\begin{aligned} \bar{f}(x)^p &= (\bar{a}_0x^m + \bar{a}_1x^{m-1} + \cdots + \bar{a}_m)^p \\ &= \bar{a}_0^p x^{pm} + \bar{a}_1^p x^{p(m-1)} + \cdots + \bar{a}_m^p \\ &= \bar{a}_0 x^{pm} + \bar{a}_1 x^{p(m-1)} + \cdots + \bar{a}_m \\ &= \bar{f}(x^p) \end{aligned}$$

for any  $f(x) \in \mathbb{Z}[x]$ . Thus,  $\bar{k}(x)^p = \bar{k}(x^p) = \bar{h}(x)\bar{l}(x)$  which implies that  $(\bar{h}(x), \bar{k}(x)) \neq 1$ . Then (5.8.2) shows that  $x^n - \bar{1}$  has multiple roots in its splitting field over  $\mathbb{Z}/(p)$ . Since the derivative  $(x^n - \bar{1})' = \bar{n}x^{n-1}$  and  $\bar{n} \neq 0$ , we have  $(x^n - \bar{1}, (x^n - \bar{1})') = \bar{1}$ , contrary to the derivative criterion for multiple roots. This contradiction shows that  $\delta^p$  is a root of  $h(x)$  for every prime  $p \nmid n$ . A repetition of this shows that  $\delta^r$  is a root of  $h(x)$  for every integer  $r$  prime to  $n$ . Since every primitive  $n$ th root of 1 has the form  $\delta^r$ ,  $(r, n) = 1$ , we see that  $h(x)$  is divisible by every  $x - \delta^r$ ,  $\delta^r$  primitive. Hence,  $h(x) = \Phi_n(x)$  and  $\Phi_n(x)$  is irreducible in  $\mathbb{Q}[x]$ .  $\square$

As an immediate consequence of Theorem 5.8.6, we get

**5.8.7 Theorem.** *Let  $\omega$  be a primitive  $n$ th root of unity. Then*

1.  $\Phi_n(x)$  is the minimal polynomial of  $\omega$  over  $\mathbb{Q}$ .
2.  $[\mathbb{Q}[\omega] : \mathbb{Q}] = \deg \Phi_n(x) = \phi(n)$ , the Euler's  $\phi$ -function.
3.  $\mathbb{Q}[\omega]$  is the splitting field of  $\Phi_n(x)$  over  $\mathbb{Q}$ .
4.  $\text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$ .

*Proof.* (1), (2) and (3) are obvious. To prove (4), recall that by Theorem 5.8.1,  $\text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$  is isomorphic to a subgroup of  $(\mathbb{Z}/(n))^\times$ . Since  $[\mathbb{Q}[\omega] : \mathbb{Q}] = \phi(n) = |(\mathbb{Z}/(n))^\times|$ , it must be isomorphic to all of  $(\mathbb{Z}/(n))^\times$ .  $\square$

Theorem 5.8.7 implies that  $\text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$  is isomorphic to the multiplicative group  $U_n$  of units of the ring  $\mathbb{Z}/(n)$ . If  $n$  is a prime then we know that this is a cyclic group of order  $p-1$ . Moreover, if  $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ ,  $p_i$  distinct primes, then  $U_n$  is isomorphic to the direct product of the groups  $U_{p_i^{e_i}}$ . In addition, we know the structures of  $U_{p^e}$  from the knowledge of primitive roots in number theory as follows.

**5.8.8 Theorem.** [Structure of  $U_{p^e}$ ]

1.  $U_2$  and  $U_4$  are cyclic and if  $e > 3$ , then  $U_{2^e}$  is a direct product of a cyclic group of order 2 and one of order  $2^{e-2}$ .
2. If  $p$  is an odd prime, the multiplicative group  $U_{p^e}$  of units of  $\mathbb{Z}/(p^e)$  is cyclic.

**5.8.9 Example.** If  $\omega = e^{2\pi i/72}$  is a primitive 72<sup>nd</sup> root of unity, then

$$\text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong U_{72} \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(6).$$

**5.8.10 Definition.** A finite-dimensional field extension of  $\mathbb{Q}$  is called a **cyclotomic field** if it is a subfield of  $\mathbb{Q}[\omega]$  for some root of unity  $\omega$ .

**5.8.11 Theorem.** *Let  $K$  be a cyclotomic field. Then  $K$  is Galois over  $\mathbb{Q}$  and  $\text{Gal}(K/\mathbb{Q})$  is abelian.*

*Proof.* Consider  $\mathbb{Q} \subset K \subset \mathbb{Q}[\omega]$  for some  $n$ th root of unity  $\omega$ . By the fundamental theorem of Galois theory  $K = \mathbb{Q}[\omega]^H$  for some subgroup  $H$  of  $G = \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$ . Since  $G$  is abelian,  $H$  is normal in  $G$ , so the fundamental theorem says that  $K$  is Galois over  $\mathbb{Q}$  with Galois group  $G/H$ , an abelian group.  $\square$

**5.8.12 Remark.** A deep theorem of Kronecker and Weber says that the converse of Theorem 5.8.11 is true, namely, "if  $K$  is Galois over  $\mathbb{Q}$  and  $\text{Gal}(K/\mathbb{Q})$  is abelian, then  $K$  is a cyclotomic field, that is,  $K \subset \mathbb{Q}[\omega]$  for some root of unity  $\omega$ ."

**5.8.13 Example.** Let  $\omega = e^{2\pi i/71}$  be a primitive 71<sup>st</sup> root of unity. Then

$$G = \text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong U_{71} \cong \mathbb{Z}/(70) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7).$$

Let  $H = \mathbb{Z}/(2) \times \mathbb{Z}/(5)$  be the subgroup of  $G$  of order 10. Then  $H$  is normal in  $G$  and consequently we have  $\mathbb{Q}[\omega]^H$  is a Galois extension over  $\mathbb{Q}$  of degree  $[\mathbb{Q}[\omega]^H : \mathbb{Q}] = [G : H] = 7$  and  $\text{Gal}(\mathbb{Q}[\omega]^H/\mathbb{Q}) \cong G/H \cong \mathbb{Z}/(7)$ .

We now have enough tools to find the Galois groups of splitting fields of irreducible separable polynomials  $x^n - a$ . Note that  $(x^n - a)' = nx^{n-1}$ , so  $x^n - a$  is separable over a field  $F$  if and only if  $\text{char } F \nmid n$ . In particular, if  $F$  contains a primitive  $n$ th root of unity, then  $\text{char } F \nmid n$ .

**5.8.14 Theorem.** *Let  $F$  be a field which contains a primitive  $n$ th root of unity  $\omega$ , i.e.,  $\text{char } F$  not divide  $n$ . Let  $a \in F$ ,  $f(x) = x^n - a$ ,  $E$  the splitting field for  $E$  over  $F$  and  $r$  a root of  $f(x)$  in  $E$ . Then*

(1) *The factorization of  $f(x)$  in  $E[x]$  is*

$$x^n - a = (x - r)(x - \omega r) \dots (x - \omega^{n-1}r)$$

*and  $E = F[r]$ .*

(2) *Let  $d$  be the least positive integer such that  $r^d = b \in F$ . Then  $d$  divides  $n$  and*

$$x^d - b = (x - r)(x - \varepsilon r) \dots (x - \varepsilon^{d-1}r)$$

*is the minimal polynomial of  $r$  over  $F$  where  $\varepsilon = \omega^{n/d}$ , a primitive  $d$ th root of unity. In addition,  $[E : F] = d$  and  $\text{Gal}(E/F) \cong \mathbb{Z}/(d)$ . The automorphism  $\alpha : E \rightarrow E$  defined by  $\alpha(r) = \varepsilon r$  generates  $\text{Gal}(E/F)$ .*

*Proof.* (1) Since  $r, \omega r, \dots, \omega^{n-1}r$  are all roots of  $x^n - a$ ,  $(x - r)(x - \omega r) \dots (x - \omega^{n-1}r)$  must divide  $x^n - a$ . Since both polynomials are monic of degree  $n$ , they must be equal. Also,  $\omega \in F$  by hypothesis, so  $F[r]$  contains all the roots of  $x^n - a$  and is generated over  $F$  by them. Hence,  $E = F[r]$  by the definition of splitting field.

(2) Since  $d$  is the generator of the group  $\{m \in \mathbb{Z} : r^m \in F\}$  and  $n$  is in this group,  $d$  divides  $n$ . Certainly,  $r$  is a root of  $x^d - b \in F[x]$ . If  $x^d - b$  had a proper factor of degree  $c$ ,  $0 < c < d$ , looking at its constant term would show that  $r^c \in F$ , contradicting the minimality of  $d$ . Thus,  $x^d - b$  is irreducible. Hence,  $[E : F] = [F[r] : F] = d$ , so  $|\text{Gal}(E/F)| = d$ . On the other hand, one sees that  $\alpha^i(r) = \varepsilon^i r$ , so  $\alpha$  is an element of  $\text{Gal}(E/F)$  of order  $d$ . Therefore,  $\text{Gal}(E/F) = \langle \alpha \rangle \cong \mathbb{Z}/(d)$ .  $\square$

For the sake of clarity, we reformulate Theorem 5.8.14 slightly to emphasize the case where  $f(x)$  is irreducible, which is the important one.

**5.8.15 Theorem.** *Let  $F$  be a field which contains a primitive  $n$ th root of unity  $\omega$  and let  $a \in F$ . Then  $x^n - a$  is irreducible if and only if no divisor  $d$  of  $n$ ,  $d \neq 1$ , such that  $a = b^d$  for some  $b \in F$ . If  $x^n - a$  is irreducible and  $E/F$  is its splitting field, then  $[E : F] = n$  and  $\text{Gal}(E/F) \cong \mathbb{Z}/(n)$ .*

**5.8.16 Example.** Let  $f(x) = x^n - p \in \mathbb{Q}[x]$  where  $p$  is prime. (The essential point is not that  $p$  is prime, but that it is not a proper power.) By Eisenstein's criterion  $f(x)$  is irreducible over  $\mathbb{Q}$ . If we let  $r = \sqrt[n]{p}$  denote the positive real  $n$ th root of  $p$  and  $\omega = e^{2\pi i/n}$ , a primitive  $n$ th root of unity, then the factorization of  $f(x)$  in  $\mathbb{C}[x]$  is

$$x^n - p = (x - r)(x - \omega r) \dots (x - \omega^{n-1}r).$$

Now let  $E = \mathbb{Q}[r, \omega r, \dots, \omega^{n-1}r]$  be a splitting field for  $f(x)$ , and let  $\varphi \in \text{Gal}(E/\mathbb{Q})$ . Then  $\varphi$  permutes  $\{r, \omega r, \dots, \omega^{n-1}r\}$  and  $\varphi$  is completely defined by its action on the set  $\{r, \omega r, \dots, \omega^{n-1}r\}$ . This gives rise to an embedding

$$\text{Gal}(E/\mathbb{Q}) \hookrightarrow S_n = \text{Sym}\{r, \omega r, \dots, \omega^{n-1}r\}.$$

Note that  $\omega = (\omega r)r^{-1}$ , so  $\omega \in E$ . This makes it clear that

$$E = \mathbb{Q}[r, \omega r, \dots, \omega^{n-1}r] = \mathbb{Q}[\omega, r] = \mathbb{Q}[\omega][r].$$

Thus,  $E$  is generated over  $\mathbb{Q}$  by two elements  $\omega$  and  $r$ . We also know that  $E$  can be generated over  $\mathbb{Q}$  by a primitive element. However, using such an element would not simplify the description of  $\text{Gal}(E/\mathbb{Q})$ .

Now consider  $\varphi \in \text{Gal}(E/\mathbb{Q})$ . Then

$$\varphi(\omega) = \omega^i \quad \text{and} \quad \varphi(r) = \omega^j r$$

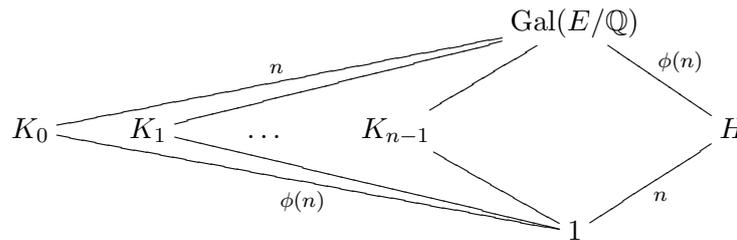
for some  $1 \leq i \leq n-1$  such that  $\text{gcd}(i, n) = 1$  and  $0 \leq j \leq n-1$ . The choice of  $i$  and  $j$  completely determines  $\varphi$  and it turns out that all of the above choices do determine automorphisms of  $E$ . Thus,

$$|\text{Gal}(E/\mathbb{Q})| = n \cdot \phi(n).$$

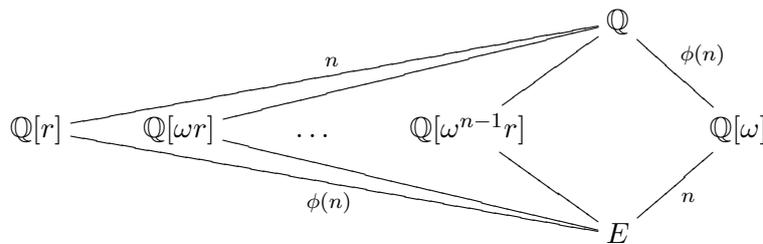
To describe  $\text{Gal}(E/\mathbb{Q})$  more precisely, let  $\mathbb{Q}[\omega] = E^H$ , and for  $0 \leq j \leq n-1$ , let  $\mathbb{Q}[\omega^j r] = E^{K_j}$ . Since  $\mathbb{Q}[\omega]$  is Galois over  $\mathbb{Q}$ ,  $H$  is normal in  $\text{Gal}(E/\mathbb{Q})$ . Moreover, by Theorem 5.8.15,  $H = \text{Gal}(E/\mathbb{Q}[\omega]) = \langle \tau \rangle \cong \mathbb{Z}/(n)$  is cyclic of order  $n$  with generator  $\tau$  defined by

$$\tau(\omega) = \omega \quad \text{and} \quad \tau(r) = \omega r.$$

The group  $K_j$  are more difficult to describe explicitly, but they are all conjugate in  $\text{Gal}(E/\mathbb{Q})$  and isomorphic as abstract groups to  $\text{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$ . We have the following diagram of subgroups of  $\text{Gal}(E/\mathbb{Q})$  which does *not* include all subgroups.



The corresponding invariant fields are



As a group,  $\text{Gal}(E/\mathbb{Q})$  is a semi-direct product  $H \rtimes K_i$  for any  $i$ .

We conclude this section with the statement of the following theorem on the Galois group of splitting fields of irreducible separable polynomials  $x^n - a$  without proof.

**5.8.17 Theorem.** *Let  $F[\omega]$  be a splitting field for  $x^n - 1$  over  $F$  where  $\omega$  is a primitive  $n$ th root of unity. Suppose that  $a \in F$  and  $f(x) = x^n - a$  is irreducible over  $F$  and let  $E$  be a splitting field for  $f(x)$  over  $F$ . Let  $d$  be the largest divisor of  $n$  such that  $b^d = a$  for some  $b \in F[\omega]$  (possibly  $d = 1$ ). Let  $G = \text{Gal}(E/F)$  and  $H = \text{Gal}(E/F[\omega])$ . Then  $H$  is cyclic of order  $d$  and normal in  $G$ ,  $\text{Gal}(F[\omega]/F) \cong G/H$  is isomorphic to a subgroup of  $(\mathbb{Z}/(n))^\times$  and  $G$  is isomorphic to a semi-direct product of  $H$  by  $G/H$ .*

Using the cyclotomic polynomials, we now present the proof of Wedderburn's theorem as follows.

**5.8.18 Theorem.** [Wedderburn, 1909] *A finite division ring is a field.*

*Proof.* Let  $D$  be a finite division ring. Then the center of  $D$ , denoted by  $F$ , is a finite field (see Exercises 2.1). Assume that  $|F| = q$ . Since  $D$  is a vector space over  $F$ ,  $|D| = q^n$  for some  $n \in \mathbb{N}$ . Also, for an element  $d \in D$ , the set  $C(d) = \{r \in D : rd = dr\}$  is a division ring containing  $F$  and  $|C(d)| = q^m$  for some  $m \leq n$ , which is strictly less than if  $d \notin F$ . Thus, the class equation (Corollary 1.4.14) for the multiplicative group  $D \setminus \{0\}$  is

$$q^n - 1 = |F \setminus \{0\}| + \sum_{i=1}^s [D \setminus \{0\} : C(d_i) \setminus \{0\}] = q - 1 + \sum_{i=1}^s \frac{q^n - 1}{q^{m_i} - 1},$$

where  $d_1, d_2, \dots, d_s$  represent the conjugacy classes of  $D \setminus \{0\}$  which contains more than one element and  $|C(d_i)| = q^{m_i}$  for some  $m_i < n$  for all  $i$ . Because each  $(q^n - 1)/(q^{m_i} - 1) = [D \setminus \{0\} : C(d_i) \setminus \{0\}]$  is an integer,  $m_i$  is a proper divisor of  $n$ . Thus, the quotient

$$\frac{x^n - 1}{\Phi_n(x)(x^{m_i} - 1)}$$

is a polynomial in  $\mathbb{Z}[x]$ . Substitute  $q$  for  $x$ , we see that  $\Phi_n(q)$  divides  $(q^n - 1)/(q^{m_i} - 1)$ . It follows from the class equation that  $\Phi_n(q)$  divides  $q - 1$  because it divides all the other terms. Then  $|\Phi_n(q)| \leq q - 1$ . On the other hand, since 1 is the closest point, on the unit circle  $\{z \in \mathbb{C} : |z| = 1\}$ , to the positive integer  $q$ , we have that for every primitive  $n$ th root of unity  $\omega^j$ ,

$$|q - \omega^j| \geq q - 1 \geq 1,$$

and the first inequality is strict unless  $\omega^j = 1$ , that is, unless 1 is a primitive  $n$ th root of unity which means  $n = 1$ . So the product  $|\Phi_n(q)|$  of the  $|q - \omega^j|$ 's is greater than or equal to  $q - 1$ , with equality only if  $n = 1$ . Because  $|\Phi_n(q)|$  is both at most  $q - 1$  and at least  $q - 1$ , we get  $|\Phi_n(q)| = q - 1$  and hence  $n = 1$ . Therefore,  $|D| = q = |C(D)|$ , so  $D = C(D)$  which implies  $D$  is commutative as desired.  $\square$

**5.8.19 Definition.** Given a field  $F$  and a polynomial  $p(x) \in F[x]$ , we say that  $p(x)$  is **solvable by radicals over  $F$**  if we can find a finite sequence of fields  $F_1 = F(\omega_1)$ ,  $F_2 = F_1(\omega_2)$ ,  $\dots$ ,  $F_k = F_{k-1}(\omega_k)$  such that  $\omega_1^{r_1} \in F$ ,  $\omega_2^{r_2} \in F_1$ ,  $\dots$ ,  $\omega_k^{r_k} \in F_{k-1}$  and all roots of  $p(x)$  lie in  $F_k$ .

If  $K$  is the splitting field of  $p(x)$  over  $F$ , then  $p(x)$  is solvable by radicals over  $F$  if we can find a finite sequence of fields as above such that  $K \subseteq F_k$ . An important remark, and one we shall use later, in the proof of Theorem 5.8.20, is that if such an  $F_k$  can be found, we can, without loss of generality, assume it to be a normal extension of  $F$ . We leave its proof as an exercise.

**5.8.20 Theorem.** [Galois] *Let  $F$  be a field which contains a primitive  $n$ th root of unity for every positive integer  $n$ . If a polynomial  $p(x) \in F[x]$  is solvable by radical over  $F$ , then the Galois group over  $F$  of  $p(x)$  is solvable.*

*Proof.* Let  $K$  be the splitting field of  $p(x)$  over  $F$ . Since  $p(x)$  is solvable by radicals, there exists a finite sequence of fields

$$F = F_0 \subset F_1 = F(\omega_1) \subset F_2 = F_1(\omega_2) \subset \dots \subset F_k = F_{k-1}(\omega_k),$$

where  $\omega_1^{r_1} \in F$ ,  $\omega_2^{r_2} \in F_1$ ,  $\dots$ ,  $\omega_k^{r_k} \in F_{k-1}$  and  $K \subseteq F_k$  such that  $F_k$  is normal over  $F$ . As a normal extension of  $F$ ,  $F_k$  is also a normal of any intermediate fields, hence  $F_k$  is a normal extension of each  $F_i$ . Theorem 5.8.14 implies that  $F_i$  is a normal extension of  $F_{i-1}$  and  $\text{Gal}(F_i/F_{i-1})$  is abelian

for all  $i$ . Thus, by the Galois correspondence,  $\text{Gal}(F_k/F_i)$  is a normal subgroup in  $\text{Gal}(F_k/F_{i-1})$ . Consider the normal series

$$\text{Gal}(F_k/F_0) \supset \text{Gal}(F_k/F_1) \supset \text{Gal}(F_k/F_2) \supset \dots \supset \text{Gal}(F_k/F_{k-1}) \supset \{1\}.$$

Since  $\text{Gal}(F_k/F_{i-1})/\text{Gal}(F_k/F_i) \cong \text{Gal}(F_i/F_{i-1})$  is abelian for all  $i$ ,  $\text{Gal}(F_k/F)$  is solvable. It follows that  $\text{Gal}(K/F) \cong \text{Gal}(F_k/F)/\text{Gal}(F_k/K)$  is solvable by Theorem 3.2.10 (2).  $\square$

We make two remarks without proof.

1. The converse of Theorem 5.8.20 is also true; that is, if the Galois group of  $p(x)$  over  $F$  is solvable, then  $p(x)$  is solvable by radicals over  $F$ .
2. Theorem 5.8.20 and its converse are true even if  $F$  does not contain roots of unity. Recall that for  $n \geq 5$ ,  $S_n$  is not solvable. Thus we have

**5.8.21 Corollary.** *The general polynomial of degree  $n \geq 5$  over  $\mathbb{Q}$  is not solvable by radical.*

- 5.7 Exercises.**
1. Prove the following statements. (a) If  $p$  is a prime number, then  $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$ .  
 (b) If  $n > 1$  is odd, then  $\Phi_{2n}(x) = \Phi_n(-x)$ .  
 (c) If  $p$  is a prime number, then  $\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p), & \text{if } p \nmid n, \\ \Phi_n(x), & \text{if } p \mid n. \end{cases}$
  2. Let  $\omega = e^{2\pi i/18}$  be a primitive 18th root of unity.
    - (a) Find the minimal polynomial of  $\omega$  over  $\mathbb{Q}$ .
    - (b) Draw a lattice diagram for the subgroup-intermediate subfield correspondence for the fundamental theorem of Galois theory of  $\mathbb{Q}[\omega]/\mathbb{Q}$ .
  3. Give an example of field  $E$  containing the field of rational numbers  $\mathbb{Q}$  such that  $E$  is Galois over  $\mathbb{Q}$  and  $\text{Gal}(E/\mathbb{Q})$  is a cyclic group of order five.
  4. Let  $K$  be a finite separable extension over  $F$  and  $E$  its normal closure (smallest normal extension over  $F$  containing  $K$ ).
    - (a) Prove that  $[E:F]$  is finite.
    - (b) If  $\text{Gal}(E/F)$  is abelian, show that  $K$  is normal over  $F$ .
  5. If  $p(x)$  is solvable by radicals over  $F$ , prove that we can find a finite sequence of fields

$$F \subset F_1 = F(\omega_1) \subset F_2 = F_1(\omega_2) \subset \dots \subset F_k = F_{k-1}(\omega_k),$$

where  $\omega_1^{r_1} \in F$ ,  $\omega_2^{r_2} \in F_1$ ,  $\dots$ ,  $\omega_k^{r_k} \in F_{k-1}$  containing all the roots of  $p(x)$  such that  $F_k$  is normal over  $F$ .

6. Assume that  $x^p - a$ ,  $a \in \mathbb{Q}$ , is irreducible in  $\mathbb{Q}[x]$ . Show that the Galois group of  $x^p - a$  over  $\mathbb{Q}$  is isomorphic to the group of transformations of  $\mathbb{Z}/(p)$  of the form  $y \mapsto ky + l$  where  $k, l \in \mathbb{Z}/(p)$  and  $k \neq 0$ .

## 5.9 Normal Bases

Let  $E$  be an extension field of a field  $F$ . We have known from Lemma 5.7.8 that the automorphism in  $\text{Gal}(E/F)$  are  $E$ -linearly independent  $F$ -linear transformations.

**5.9.1 Theorem.** *If  $E/F$  is a finite Galois extension with Galois group  $G = \{1, \sigma_2, \dots, \sigma_n\}$ . Then  $\{u_1, u_2, \dots, u_n\}$  is a basis for  $E/F$  if and only if*

$$\det \begin{bmatrix} u_1 & u_2 & \dots & u_n \\ \sigma_2(u_1) & \sigma_2(u_2) & \dots & \sigma_2(u_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \dots & \sigma_n(u_n) \end{bmatrix} \neq 0.$$

*Proof.* Call the above matrix  $M$  and suppose that  $\det M = 0$ . Since  $M \in M_n(E)$ , there are  $\alpha_1, \alpha_2, \dots, \alpha_n \in E$ , not all zero, such that

$$[\alpha_1 \ \alpha_2 \ \dots \ \alpha_n] M = \vec{0}.$$

This translates to  $\theta(u_1) = \theta(u_2) = \dots = \theta(u_n) = 0$  where

$$\theta = \alpha_1 1 + \alpha_2 \sigma_2 + \dots + \alpha_n \sigma_n : E \rightarrow E.$$

But  $\theta : E \rightarrow E$  is a  $F$ -linear map, so  $\theta$  is the zero map, since it vanishes on  $u_1, u_2, \dots, u_n$ . Since  $1, \sigma_2, \dots, \sigma_n$  are linearly independent over  $K$ , Lemma 5.7.8 says that  $\theta \neq 0$ , so we have a contradiction.

Conversely, if  $u_1, u_2, \dots, u_n$  are not a basis for  $E/F$ , then there are  $\beta_1, \beta_2, \dots, \beta_n \in F$ , not all zero, such that

$$u_1 \beta_1 + u_2 \beta_2 + \dots + u_n \beta_n = 0.$$

Then for any  $\sigma_i \in G$ ,

$$\sigma_i(u_1) \beta_1 + \sigma_i(u_2) \beta_2 + \dots + \sigma_i(u_n) \beta_n = \sigma_i(u_1 \beta_1 + u_2 \beta_2 + \dots + u_n \beta_n) = 0,$$

so  $M [\beta_1 \ \beta_2 \ \dots \ \beta_n]^T = \vec{0}$ . Hence,  $\det M = 0$ .  $\square$

Note that if  $|K| = q$ , then  $\alpha^q - \alpha = 0$  for all  $\alpha \in K$ , so  $f(x) = x^q - x$  is a nonzero polynomial but it is a zero function. The next theorem says that such a polynomial cannot exist if  $K$  is infinite.

**5.9.2 Theorem.** *Let  $F$  be an infinite field and  $F \subseteq E$ . If  $f(x_1, \dots, x_n)$  is a nonzero polynomial in  $E[x_1, \dots, x_n]$ , then there exist  $\alpha_1, \dots, \alpha_n \in F$  such that  $f(\alpha_1, \dots, \alpha_n) \neq 0$ .*

*Proof.* We shall use induction on  $n$ . For  $n = 1$ , since  $f(x_1)$  has only finitely many roots and  $F$  is infinite, there is  $\alpha_i \in F$  such that  $f(\alpha_1) \neq 0$ . Assume that the statement holds for  $n$ , and let

$$f(x_1, \dots, x_{n+1}) = f_0(x_1, \dots, x_n) + f_1(x_1, \dots, x_n)x_{n+1} + \dots + f_t(x_1, \dots, x_n)x_{n+1}^t.$$

Since  $f \neq 0$ , at least one of  $f_0(x_1, \dots, x_n), \dots, f_t(x_1, \dots, x_n)$  is nonzero, so there are  $\alpha_1, \dots, \alpha_n \in F$  such that  $f(\alpha_1, \dots, \alpha_n, x_{n+1}) \neq 0$  in  $E[x_{n+1}]$ . By the one variable case, there is  $\alpha_{n+1} \in F$  such that  $f(\alpha_1, \dots, \alpha_n, \alpha_{n+1}) \neq 0$ .  $\square$

**5.9.3 Theorem.** *Let  $F$  be an infinite field and  $E/F$  Galois with Galois group  $G = \text{Gal}(E/F) = \{1, \sigma_2, \dots, \sigma_n\}$ . Suppose that  $0 \neq f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$  where  $x_1, \dots, x_n$  are indeterminates over  $F$ . Then there exists  $u \in E$  such that  $f(u, \sigma_2(u), \dots, \sigma_n(u)) \neq 0$ .*

*Proof.* Let  $\{u_1, \dots, u_n\}$  be a basis for  $E/F$ . By Theorem 5.9.1, the matrix

$$M = \begin{bmatrix} u_1 & u_2 & \dots & u_n \\ \sigma_2(u_1) & \sigma_2(u_2) & \dots & \sigma_2(u_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \dots & \sigma_n(u_n) \end{bmatrix} \in M_n(E)$$

is invertible. This means that the map on  $E[x_1, \dots, x_n]$  defined by

$$g(x_1, \dots, x_n) \mapsto g(u_1 x_1 + \dots + u_n x_n, \dots, \sigma_n(u_1) x_1 + \dots + \sigma_n(u_n) x_n)$$

is an isomorphism. Thus,

$$h(x_1, \dots, x_n) = f(u_1 x_1 + \dots + u_n x_n, \dots, \sigma_n(u_1) x_1 + \dots + \sigma_n(u_n) x_n)$$

is a nonzero polynomial in  $E[x_1, \dots, x_n]$ . By Theorem 5.9.2, there are  $a_1, \dots, a_n$  in  $F$  such that  $h(a_1, \dots, a_n) \neq 0$ . Let  $u = u_1a_1 + \dots + u_na_n$ , this translates to

$$\begin{aligned} 0 \neq h(a_1, \dots, a_n) &= f(u_1a_1 + \dots + u_na_n, \dots, \sigma_n(u_1)a_1 + \dots + \sigma_n(u_n)a_n) \\ &= f(u, \sigma_2(u), \dots, \sigma_n(u)), \end{aligned}$$

since  $\sigma_i(u_1)a_1 + \dots + \sigma_i(u_n)a_n = \sigma_i(u_1a_1 + \dots + u_na_n) = \sigma_i(u)$ . □

Consider  $E = \mathbb{Q}[i]$  is a Galois extension over  $\mathbb{Q}$ . Its Galois group is of order two and consists of the identity map and the complex conjugation. A basis over  $\mathbb{Q}$  for it is  $\{1, i\}$ . This basis is not invariant under the Galois action, namely after acting by the complex conjugation, we obtain  $\{1, -i\}$ . We are showing the existence of a basis for a finite Galois extension which forms a single orbit under the action of the Galois group. For example, for  $\mathbb{Q}[i]$ , we may use  $\{1+i, 1-i\}$ . In the case of finite fields, this means that each of the basis elements is related to any one of them by applying the Frobenius' automorphism repeatedly.

**5.9.4 Definition.** Let  $E/F$  be Galois with Galois group  $G = \text{Gal}(E/F) = \{\sigma_1, \dots, \sigma_n\}$ . A **normal basis** for  $E/F$  is a basis of the form  $\{\sigma_1(u), \dots, \sigma_n(u)\}$  for some  $u \in E$ .

Eisenstein conjectured the existence of a normal basis in 1850 for finite extensions of finite fields and Hensel gave a proof for finite fields in 1888. Dedekind used such bases in number fields in his work on the discriminant in 1880, but he had no general proof. (See the quote by Dedekind on the bottom of page 51 of Curtis's "Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Brauer".) In 1932 Noether gave a proof for some infinite fields while Deuring gave a uniform proof for all fields (also in 1932). This basis is frequently used in cryptographic applications that are based on the discrete logarithm problem such as elliptic curve cryptography.

**5.9.5 Theorem.** [Normal Basis Theorem] Let  $E/F$  be a Galois extension with Galois group  $G = \text{Gal}(E/F) = \{\sigma_1, \dots, \sigma_n\}$ . Then  $E/F$  has a normal basis.

*Proof.* We shall assume that  $F$  is infinite and leave the finite case as an exercise (see Exercise 5.6). Let  $u \in E$ . By Theorem 5.9.1,  $\{\sigma_1(u), \sigma_2(u), \dots, \sigma_n(u)\}$  is a basis for  $E/F$  if and only if

$$\det \begin{bmatrix} \sigma_1^2(u) & \sigma_1\sigma_2(u) & \dots & \sigma_1\sigma_n(u) \\ \sigma_2\sigma_1(u) & \sigma_2^2(u) & \dots & \sigma_2\sigma_n(u) \\ \vdots & & & \\ \sigma_n\sigma_1(u) & \sigma_n\sigma_2(u) & \dots & \sigma_n^2(u) \end{bmatrix} \neq 0.$$

Note that the entries in each row or column of the above matrix, call  $M$ , are a permutation of the elements  $\sigma_1(u), \dots, \sigma_n(u)$ . In other words, each  $\sigma_i(u)$  occurs exactly once in each row and column of  $M$ . Thus,

$$M = \sigma_1(u)A_1 + \dots + \sigma_n(u)A_n$$

where each  $A_i$  is a permutation matrix (a matrix with a single entry 1 in each row and column and the remaining entries zero). Since  $\det A_i = \pm 1$ , we see by inspection that if  $x_1, \dots, x_n$  are indeterminates over  $E$

$$f(x_1, \dots, x_n) = \det(x_1A_1 + \dots + x_nA_n) = \pm x_1^n \pm \dots \pm x_n^n + \text{other terms}$$

In particular,  $f(x_1, \dots, x_n)$  is a nonzero polynomial in  $E[x]$ . By Theorem 5.9.3, there is a  $\bar{u} \in E$  such that  $f(\sigma_1(\bar{u}), \dots, \sigma_n(\bar{u})) \neq 0$ . This translates to

$$0 \neq f(\sigma_1(\bar{u}), \dots, \sigma_n(\bar{u})) = \det(\sigma_1(\bar{u})A_1 + \dots + \sigma_n(\bar{u})A_n) = \det M.$$

Hence,  $\sigma_1(\bar{u}), \dots, \sigma_n(\bar{u})$  is a desired normal basis for  $E/F$ . □

- 5.8 Exercises.**
1. Determine a normal basis for the field  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  by using the Galois group in Example 5.5.12.
  2. Determine a normal basis for the cyclotomic field  $\mathbb{Q}(e^{2\pi i/p})$  over  $\mathbb{Q}$  where  $p$  is a prime number.

## 5.10 Transcendental Extensions

Most of extension fields seen in the previous section are algebraic. In this section, we shall present some results on transcendental extension. The final theorem, namely Lüroth's theorem, has many applications in algebraic geometry and function field theory.

**5.10.1 Definition.** Let  $F$  be a subfield of a field  $E$  and let  $x_1, x_2, \dots$  be independent indeterminates over  $E$ . An element  $z \in E$  is **transcendental over  $F$**  if the homomorphism  $F[x_1] \rightarrow E$  defined by  $f(x_1) \mapsto f(z)$  is one-to-one. We call  $z \in E$  **algebraic over  $F$**  if it is not transcendental over  $F$ . A finite set  $\{z_1, \dots, z_n\} \subset E$  is **algebraically independent over  $F$**  if the homomorphism  $F[x_1, \dots, x_n] \rightarrow E$  defined by  $f(x_1, \dots, x_n) \mapsto f(z_1, \dots, z_n)$  is one-to-one. (Note that the empty set is algebraically independent since  $F \hookrightarrow E$  is one-to-one.) An arbitrary subset  $Z$  of  $E$  is **algebraically independent over  $F$**  if all of its finite subsets are algebraically independent. A subset  $Z$  of  $E$  is **algebraically dependent** if it is not algebraically independent.

- 5.10.2 Remarks.**
1. If  $z$  is transcendental over  $F$ , then  $F[z] \cong F[x_1]$ , so  $F[z]$  is not a field and  $F[z]$  is infinite dimensional over  $F$ .
  2. If  $z$  is algebraic over  $F$ , then  $F[z] \cong F[x_1]/(f(x_1))$  where  $f(x_1)$  is the minimal polynomial of  $z$  over  $F$ . Thus,  $F[z] = F(z)$  is a field and  $F[z]$  is finite dimensional over  $F$ .

**5.10.3 Example.** Let  $F \subset F(y, z) \subset E$  where  $y$  and  $z$  are independent indeterminates over  $F$ . Then  $\{y^2, z^2\}$  is an algebraically independent set but  $\{y^2, yz, z^2\}$  is not (for, if  $f(x_1, x_2, x_3) = x_1x_3 - x_2^2$ , then  $f(y^2, yz, z^2) = 0$ ).

**5.10.4 Definition.** A field extension  $E$  is **algebraic over a field  $F$**  if each element of  $E$  is algebraic over  $F$ .  $E$  is **purely transcendental over  $F$**  if it is isomorphic (by an isomorphism which is the identity on  $F$ ) to  $F(\{x_\alpha\})$  where  $\{x_\alpha\}$  is a (possibly infinite) set of independent indeterminates.

**5.10.5 Theorem.** Let  $F$  be a subfield of a field  $E$ .

1. There exists a subset  $X$  of  $E$  (possibly  $X$  is empty) such that
  - (a)  $X$  is algebraically independent over  $F$ .
  - (b)  $X$  is maximal among algebraically independent sets, in the sense: If  $X \subseteq Y \subseteq E$  and  $X \neq Y$ , then  $Y$  is not algebraically independent.
2.  $F(X)$  is purely transcendental over  $F$  and  $E$  is algebraic over  $F(X)$ .

$$\begin{array}{c}
 E \\
 \left| \text{algebraic} \right. \\
 F(X) \\
 \left| \text{purely transcendental} \right. \\
 F
 \end{array}$$

*Proof.* (1) Let  $\mathcal{S} = \{X \subseteq E : X \text{ is algebraically independent}\}$ . Since the empty set is algebraically independent,  $\mathcal{S}$  is nonempty. Let  $\{X_\alpha\}_{\alpha \in \Lambda}$  be a chain in  $\mathcal{S}$ . Let  $\{z_1, \dots, z_n\} \subseteq \bigcup_{\alpha \in \Lambda} X_\alpha$ . Then  $\forall i, \exists \alpha_i \in \Lambda, z_i \in X_{\alpha_i}$ . Since  $\{X_\alpha\}_{\alpha \in \Lambda}$  is a chain, we may rearrange  $\alpha_i$  so that there exists  $j \in \Lambda$  such that  $z_i \in X_{\alpha_j}$  for all  $i$ . Since  $X_{\alpha_j}$  is algebraically independent, so is  $\{z_1, \dots, z_n\}$ . Thus,  $\bigcup_{\alpha \in \Lambda} X_\alpha$  is an upper bound of this chain in  $\mathcal{S}$ . By Zorn's Lemma,  $\mathcal{S}$  has a maximal element, say  $X$ . Hence,  $F(X)$  is purely transcendental over  $F$ . The maximality of  $X$  implies that  $E$  must be algebraic over  $F$ .

(2) The definition of algebraically independent means that  $F(X)$  is purely transcendental over  $F$ . Consider  $z \in E$ . If  $z \in X \subset F(X)$ , then  $z$  is algebraic over  $F(X)$ . If  $z \notin X$ , the set  $X \cup \{z\}$  is algebraically dependent, so for some  $n$  there is a nonzero polynomial  $f(x_1, \dots, x_n, x_{n+1})$  ( $x_1, \dots, x_{n+1}$  are indeterminates over  $F$ ) and  $a_1, \dots, a_n \in X$  such that  $f(a_1, \dots, a_n, z) = 0$ . The polynomial  $f(x_1, \dots, x_n, x_{n+1})$  cannot be a polynomial in only  $x_1, \dots, x_n$ , since  $\{a_1, \dots, a_n\}$  is an algebraically independent set. Write

$$f(x_1, \dots, x_n, x_{n+1}) = f_0(x_1, \dots, x_n) + f(x_1, \dots, x_n)x_{n+1} + \dots + f_r(x_1, \dots, x_n)x_{n+1}^r.$$

Thus,  $f(a_1, \dots, a_n, x_{n+1}) \in F(X)[x_{n+1}]$  is a nonzero polynomial having  $z$  as a root, so  $z$  is algebraic over  $F(X)$ . Hence,  $E$  is algebraic over  $F(X)$ .  $\square$

**5.10.6 Remark.** There is no uniqueness for the field  $F(X)$ . For example, if  $E = F(t)$  where  $t$  is an indeterminate, then we can take  $X = \{p(t)/q(t)\}$  where  $p(t)/q(t)$  is any element of  $E$  which is not in  $F$ . In this case  $[E : F(p(t)/q(t))] = n$  where  $n = \max\{\deg p(t), \deg q(t)\}$  (Theorem 5.10.11). However, we shall see shortly that the number of elements in the set  $X$  is independent of particular set  $X$ .

**5.10.7 Definition.** Let  $F$  be a subfield of  $E$ . A maximal algebraically independent (over  $F$ ) subset of  $E$  is called a **transcendence basis** for  $E/F$ .

**5.10.8 Remark.** By Theorem 5.10.5, a transcendence basis for  $E/F$  exists. It may be empty, which happens precisely when  $E$  is algebraic over  $F$ . Also,  $E$  is purely transcendental over  $F$  if it has a transcendence base  $B$  such that  $E = F(B)$ .

**5.10.9 Theorem.** Let  $F$  be a subfield of  $E$ . Then any two transcendence bases for  $E/F$  have the same cardinality.

**5.10.10 Definition.** We call the number of elements of transcendence bases of  $E$  the **transcendence degree** of  $E/F$ .

For example, an algebraic extension has transcendence degree zero;  $F(x)$  has transcendence degree one over  $F$ ; in general,  $F((x_\alpha)_{\alpha \in \Lambda})$  has transcendence degree  $|\Lambda|$  over  $K$ .

The purely transcendental extension fields  $E/F$ , especially those having a finite transcendence degree, appear to be the simplest type of extension fields. It is clear that such a field is isomorphic to the field of fractions  $F(x_1, \dots, x_n)$  of the polynomial ring  $F[x_1, \dots, x_n]$  in indeterminates  $x_1, \dots, x_n$ . Even though these fields look quite innocent, there are difficult and unsolved problems particularly on the nature of the subfields of  $F(x_1, \dots, x_n)/F$ . The one case where the situation is quite simple is that in which  $E$  has transcendence degree one. We shall consider this case and close this chapter.

Let  $E = F(t)$ ,  $t$  transcendental, and let  $u \in E, u \notin F$ . We can write  $u = f(t)/g(t)$  where  $f(t), g(t) \in F[t]$  and  $(f(t), g(t)) = 1$ . If  $n$  is the larger of the degrees of  $f(t)$  and  $g(t)$ , then we can write

$$f(t) = a_0 + a_1t + \dots + a_nt^n \quad \text{and} \quad g(t) = b_0 + b_1t + \dots + b_nt^n,$$

$a_i, b_i \in F$ , and either  $a_n$  or  $b_n \neq 0$ . We have  $f(t) - ug(t) = 0$ , so

$$(a_n - ub_n)t^n + (a_{n-1} - ub_{n-1})t^{n-1} + \cdots + (a_0 - ub_0) = 0 \quad (5.10.1)$$

and  $a_n - ub_n \neq 0$  since either  $a_n \neq 0$  or  $b_n \neq 0$  and  $u \notin F$ . Thus, (5.10.1) shows that  $t$  is algebraic over  $F(u)$  and  $[F(t) : F(u)] \leq n$ . We prove the following more precise result.

**5.10.11 Theorem.** *Let  $E = F(t)$ ,  $t$  transcendental over  $F$ , and let  $u \in F(t), u \notin F$ . Write  $u = f(t)/g(t)$  where  $(f(t), g(t)) = 1$ , and let  $n = \max\{\deg f(t), \deg g(t)\}$ . Then  $u$  is transcendental over  $F$ ,  $t$  is algebraic over  $F(u)$ , and  $[F(t) : F(u)] = n$ . Moreover, the minimal polynomial of  $t$  over  $F(u)$  is a multiple in  $F(u)$  of  $f(x, u) = f(x) - ug(x)$ .*

*Proof.* Put  $f(x, y) = f(x) - yg(x) \in F[x, y]$ ,  $x, y$  indeterminates. This polynomial in  $x$  and  $y$  is of first degree in  $y$  and it has no factor  $h(x)$  of positive degree since  $(f(x), g(x)) = 1$ . Thus, it is irreducible in  $F[x, y]$ . Now  $t$  is algebraic over  $F(u)$  so if  $u$  were algebraic over  $F$ , then  $t$  would be algebraic over  $F$ , contrary to the hypothesis. Hence,  $u$  is transcendental over  $F$ . Then  $F[x, u] \cong F[x, y]$  under the isomorphism over  $F$  fixing  $x$  and mapping  $u$  into  $y$  and hence  $f(x, u)$  is irreducible in  $F[x, u]$ . It turns out that  $f(x, u)$  is irreducible in  $F(u)[x]$ . Since  $f(t, u) = f(t) - ug(t) = 0$ , it follows that  $f(x, u)$  is a multiple in  $F(u)[x]$  of the minimal polynomial of  $t$  over  $F(u)$ . Therefore,  $[F(t) : F(u)]$  is the degree in  $x$  of  $f(x, u)$ . This degree is  $n$ , so the proof is complete.  $\square$

We can determine all of the subfields  $E/F$  for  $E = F(t)$ ,  $t$  transcendental: These have the form  $F(u)$  for some  $u$ . This important result is called the Lüroth's Theorem. Lüroth proved it in case  $K = \mathbb{C}$  in 1876. It was first proved for general fields  $K$  by Steinitz in 1910, by the following argument.

**5.10.12 Theorem.** [Lüroth] *If  $E = F(t)$ ,  $t$  transcendental over  $F$ , then any subfield  $K$  of  $E/F$ ,  $K \neq F$ , has the form  $F(u)$ ,  $u$  transcendental over  $F$ .*

*Proof.* Let  $v \in K, v \notin F$ . Then we have seen that  $t$  is algebraic over  $F(v)$ . Thus,  $t$  is algebraic over  $K$ . Let  $f(x) = x^n + k_1x^{n-1} + \cdots + k_n$  be the minimal polynomial of  $t$  over  $K$ , so the  $k_i \in K$  and  $n = [F(t) : K]$ . Since  $t$  is not algebraic over  $F$ , some  $k_j \notin F$ . We shall show that  $K = F(u), u = k_j$ . We can write  $u = g(t)/h(t)$  where  $g(t), h(t) \in F[t], (g(t), h(t)) = 1$  and  $m = \max\{\deg g(t), \deg h(t)\} > 0$ . Then, by Theorem 5.10.11,  $[E : F(u)] = m$ . Since  $K \supset F(u)$  and  $[E : K] = n$ , we evidently have  $m \geq n$  and equality holds if and only if  $K = F(u)$ . Now  $t$  is a root of the polynomial  $g(x) - uh(x) \in K[x]$ . Hence, we have a  $q(x) \in K[x]$  such that

$$g(x) - uh(x) = q(x)f(x). \quad (5.10.2)$$

The coefficient  $k_i$  of  $f(x)$  is in  $F(t)$ , so there exists a nonzero polynomial  $c_0(t)$  of least degree such that  $c_0(t)k_i = c_i(t) \in F[t]$  for  $1 \leq i \leq n$ . Then  $c_0(t)f(x) = f(x, t) = c_0(t)x^n + c_1(t)x^{n-1} + \cdots + c_n(t) \in F[x, t]$ , and  $f(x, t)$  is primitive as a polynomial in  $x$ , that is, the  $c_i(t)$  are relatively prime. The  $x$ -degree of  $f(x, t)$  is  $n$ . Since  $k_j = g(t)/h(t)$  with  $(g(t), h(t)) = 1$ , the  $t$ -degree of  $f(x, t)$  is  $\geq m$ . Now replace  $u$  in (5.10.2) by  $g(t)/h(t)$  and the coefficients of  $q(x)$  by their expressions in  $t$ . There exist, therefore,  $\varphi(t)$  and  $q(x, t) \in F[x, t]$  such that

$$\varphi(t)[g(x)h(t) - g(t)h(x)] = f(x, t)q(x, t).$$

Since the coefficients  $c_0(t), c_1(t), \dots, c_n(t)$  of  $f(x, t)$  have no common factor, we know that  $\varphi(t)$  divides  $q(x, t)$ . Hence, we may assume  $\varphi(t) = 1$ . It turns out that there exists a polynomial  $q'(x, t) \in F[x, t]$  such that

$$g(x)h(t) - g(t)h(x) = f(x, t)q'(x, t).$$

Since the  $t$ -degree of the left-hand side is  $\leq m$  and that of  $f(x, t)$  is  $\geq m$ , it follows that this degree is  $m$  and  $q'(x, t) = q'(x) \in F[x]$ . Then the right-hand side is primitive as a polynomial in  $x$  and so is the left-hand side. By symmetry the left-hand side is primitive as a polynomial in  $t$  also. Hence,  $q'(x) = q' \in F$ . Thus,  $f(x, t)$  has the same  $x$ -degree and  $t$ -degree so  $m = n$ , which implies that  $K = F(u)$ .  $\square$

- 5.9 Exercises.**
1. Prove that there is no intermediate field  $K$  with  $\mathbb{Q} \subseteq K \subsetneq \mathbb{C}$  with  $\mathbb{C}$  purely transcendental over  $K$ .
  2. Prove that a purely transcendental proper extension of a field is never algebraically closed.
  3. Let  $E = F(t, v)$ , where  $t$  is transcendental over  $F$  and  $v^2 + t^2 = 1$ . Show that  $E$  is purely transcendental over  $F$ .

**20 Project** (More on Lüroth's theorem). Prove more general fact that if  $F \subseteq L \subseteq E$  and  $E$  is finitely generated over  $F$  (finite transcendence degree), then  $L$  is also finitely generated over  $F$ . We can ask more generally about minimal numbers of generators of finitely-generated extensions. For instance, suppose  $K \subsetneq L \subseteq K(x_1, \dots, x_n)$  where the  $x_i$  are algebraically independent over  $K$ . If  $L/K$  has transcendence degree 1, then  $L = K(\alpha)$ . This was proved for  $K = \mathbb{C}$  by Gordan in 1887, and for arbitrary  $K$  by Igusa in 1951. If  $\mathbb{C} \subsetneq L \subseteq \mathbb{C}(x_1, \dots, x_n)$  where  $L/\mathbb{C}$  has transcendence degree 2, then  $L = \mathbb{C}(\alpha, \beta)$ . This was proved by Castelnuovo in 1894. All known proofs are difficult. The result is not true in general for other types of fields  $K$ , such as  $\mathbb{Q}$  or  $\mathbb{R}$ . Finally, there are fields  $L$  with  $\mathbb{C} \subsetneq L \subsetneq \mathbb{C}(x_1, x_2, x_3)$  such that  $L/\mathbb{C}$  has transcendence degree 3 but cannot be generated by three elements.