

## 1 extra

**Proposition 1.** Suppose that  $K$  and  $L$  are fields and that  $\varphi : K \rightarrow L$  is a homomorphism. With  $t$  and  $y$  denoting indeterminates, extend the homomorphism  $\varphi$  to the mapping  $\psi : K[t] \rightarrow L[y]$  by defining

$$\psi(a_0 + a_1t + \cdots + a_nt^n) = \varphi(a_0) + \varphi(a_1)y + \cdots + \varphi(a_n)y^n.$$

Then  $\psi : K[t] \rightarrow L[y]$  is an injective homomorphism. Also, when  $\varphi : K \rightarrow L$  is surjective, then  $\psi : K[t] \rightarrow L[y]$  is surjective and maps irreducible polynomials in  $K[t]$  to irreducible polynomials in  $L[y]$ .

**Proposition 2.** Suppose  $L : K$  is a field extension with  $K \subseteq L$ , and  $\alpha \in L$ . Then  $E_\alpha$  is a ring homomorphism.

**Proposition 3.** Let  $L : K$  be a field extension with  $K \subseteq L$ , and suppose that  $\alpha \in L$  is algebraic over  $K$ . Then

$$I = \ker(E_\alpha) = \{f \in K[t] : f(\alpha) = 0\}$$

is a nonzero ideal of  $K[t]$ , and there is a unique monic polynomial  $\mu_\alpha^K \in K[t]$  that generates  $I$ .

**Theorem 1.1.** Suppose that  $L : K$  is a field extension, and that  $\alpha \in L$  is algebraic over  $K$ . Let  $g$  be the minimal polynomial  $\mu_\alpha^K$  of  $\alpha$  over  $K$ . Then  $g$  is irreducible over  $K$ , and  $K[t]/(g)$  is a field.

**Theorem 1.2.** Let  $K$  be a field, and suppose that  $f \in K[t]$  is irreducible. Then there exists a field extension  $L : K$ , with associated embedding  $\varphi : K[t] \rightarrow L[y]$ , having the property that  $L$  contains a root of  $\varphi(f)$ .

**Proposition 4.** Let  $L : K$  be a field extension with  $K \subseteq L$ . Let  $A \subseteq L$  and

$$\mathcal{C} = \{C \subseteq A : C \text{ is a finite set}\}.$$

Then  $K(A) = \cup_{C \in \mathcal{C}} K(C)$ . Further, when  $[K(C) : K] < \infty$  for all  $C \in \mathcal{C}$ , then  $K(A) : K$  is an algebraic extension.

**Proposition 5.** Let  $L : K$  be a field extension with  $K \subseteq L$ , and suppose that  $\alpha \in L$ . Then

$$K[\alpha] = \{c_0 + c_1\alpha + \cdots + c_d\alpha^d : d \in \mathbb{Z}_{\geq 0}, c_0, \dots, c_d \in K\}$$

and

$$K(\alpha) = \{f/g : f, g \in K[\alpha], g \neq 0\}.$$

**Proposition 6.** Let  $L : K$  be a field extension with  $K \subseteq L$ , and suppose that  $\alpha \in L$ . Then  $\alpha$  is algebraic over  $K$  if and only if  $[K(\alpha) : K] < \infty$ .

### 1.1 Review of finite fields and tests for irreducibility

**Definition 1** (Characteristic). Let  $K$  be a field with additive identity  $0_K$  and multiplicative identity  $1_K$ . When  $n \in \mathbb{N}$ , we write  $n \cdot 1_K$  to denote  $1_K + \cdots + 1_K$  (as an  $n$ -fold sum). We define the characteristic of  $K$ , denoted by  $\text{char } K$ , to be the smallest positive integer  $m$  with the property that  $m \cdot 1_K = 0_K$ ; if no such integer  $m$  exists, we define the characteristic of  $K$  to be 0.

**Proposition 7.** Let  $K$  be a field with  $\text{char } K > 0$ . Then  $\text{char } K$  is equal to a prime number  $p$ , and then for all  $x \in K$  one has  $p \cdot x = 0$ .

**Theorem 1.3** (Localisation principle). Let  $R$  be an integral domain, and let  $I$  be a prime ideal of  $R$ . Define  $\varphi : R[X] \rightarrow (R/I)[X]$  by putting

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_nX^n,$$

where  $\bar{a}_j = a_j + I$ . Then  $\varphi$  is a surjective homomorphism. Moreover, if  $f \in R[X]$  is primitive with leading coefficient not in  $I$ , then  $f$  is irreducible in  $R[X]$  whenever  $\varphi(f)$  is irreducible in  $(R/I)[X]$ .

**Note:** Proposition 3.1 tells us that when  $f \in K[t]$  and  $\sigma \in \text{Gal}(L : K)$ , the mapping  $\sigma$  permutes the roots of  $f$  that lie in  $L$ .

**Theorem 1.4.** Suppose that  $L : K$  is an algebraic extension, and  $\sigma : L \rightarrow L$  is a  $K$ -homomorphism. Then  $\sigma$  is an automorphism of  $L$ .

**Theorem 1.5.** If  $L : K$  is a finite extension, then  $|\text{Gal}(L : K)| \leq [L : K]$ .

**Corollary 1.** Suppose that  $L : F$  and  $L : F'$  are finite extensions with  $F \subseteq L$  and  $F' \subseteq L$ , and further that  $\psi : F \rightarrow F'$  is an isomorphism. Then there are at most  $[L : F]$  ways to extend  $\psi$  to a homomorphism from  $L$  into  $L$ .

**Corollary 2.** Let  $L : K$  be a finite extension with  $K \subseteq L$ . Suppose that  $\alpha_1, \dots, \alpha_n \in L$  and put  $L = K(\alpha_1, \dots, \alpha_n)$ . Let  $K_0 = K$ , and for  $1 \leq i \leq n$ , let  $K_i = K_{i-1}(\alpha_i)$ . Then every automorphism  $\tau \in \text{Gal}(L : K)$  corresponds to a sequence of homomorphisms  $\sigma_1, \dots, \sigma_n$ , having the property that  $\sigma_0 : K \rightarrow L$  is the inclusion map, one has  $\sigma_n = \tau$ , and for  $1 \leq i \leq n$ , the map  $\sigma_i : K_i \rightarrow L$  is a homomorphism extending  $\sigma_{i-1} : K_{i-1} \rightarrow L$ .

## 2 Algebraic closures

### 2.1 The definition of an algebraic closure, and Zorn's Lemma

### 2.2 The existence of an algebraic closure

**Corollary 3.** When  $K$  is a field, the field  $\overline{K}$  is a maximal algebraic extension of  $K$ .

### 2.3 Properties of algebraic closures

**Corollary 4.** Suppose that  $\overline{K}$  is an algebraic closure of  $K$ , and assume that  $K \subseteq \overline{K}$ . Take  $\alpha \in \overline{K}$  and suppose that  $\sigma : K \rightarrow \overline{K}$  is a homomorphism. Then the number of distinct roots of  $\mu_\alpha^K$  in  $\overline{K}$  is equal to the number of distinct roots of  $\sigma(\mu_\alpha^K)$  in  $\overline{K}$ .

**Proposition 8.** Suppose that  $L$  and  $M$  are fields having the property that  $L$  is algebraically closed, and  $\psi : L \rightarrow M$  is a homomorphism. Then  $\psi(L)$  is algebraically closed.

**Proposition 9.** If  $L : K$  is an algebraic extension, then  $\overline{L}$  is an algebraic closure of  $K$ , and hence  $\overline{L} \cong \overline{K}$ . If in addition  $K \subseteq L \subseteq \overline{L}$ , then we can take  $\overline{K} = \overline{L}$ .

## 3 Splitting field extensions

**Definition 2** (Splitting field, splitting field extension). Suppose that  $L : K$  is a field extension relative to the embedding  $\varphi : K \rightarrow L$ , and  $f \in K[t] \setminus K$ .

- (i) We say that  $f$  splits over  $L$  if  $\varphi(f) = \lambda(t - \alpha_1) \cdots (t - \alpha_n)$ , for some  $\lambda \in \varphi(K)$  and  $\alpha_1, \dots, \alpha_n \in L$ .
- (ii) Suppose that  $f$  splits over  $L$ , and let  $M$  be a field with  $\varphi(K) \subseteq M \subseteq L$ . We say that  $M : K$  is a splitting field extension for  $f$  if  $M$  is the smallest subfield of  $L$  containing  $\varphi(K)$  over which  $f$  splits.
- (iii) More generally, suppose that  $S \subseteq K[t] \setminus K$  has the property that every  $f \in S$  splits over  $L$ . Let  $M$  be a field with  $\varphi(K) \subseteq M \subseteq L$ . We say that  $M : K$  is a splitting field extension for  $S$  if  $M$  is the smallest subfield of  $L$  containing  $\varphi(K)$  over which every polynomial  $f \in S$  splits.

**Proposition 10.** Suppose that  $L : K$  is a splitting field extension for the polynomial  $f \in K[t] \setminus K$  with associated embedding  $\varphi : K \rightarrow L$ . Let  $\alpha_1, \dots, \alpha_n \in L$  be the roots of  $\varphi(f)$ . Then  $L = \varphi(K)(\alpha_1, \dots, \alpha_n)$ .

**Proposition 11.** Suppose that  $L : K$  is a splitting field extension for the polynomial  $f \in K[t] \setminus K$ . Then  $[L : K] \leq (\deg f)!$

**Proposition 12.** Given  $S \subseteq K[t] \setminus K$ , there exists a splitting field extension  $L : K$  for  $S$ , and  $L : K$  is an algebraic extension. More explicitly, suppose that  $\overline{K}$  is an algebraic closure of  $K$ , and that  $\overline{K} : K$  is an extension relative to the embedding  $\varphi : \overline{K} \rightarrow K$ . Let

$$A = \{\alpha \in \overline{K} : \alpha \text{ is a root of } \varphi(f), \text{ for some } f \in S\}.$$

Put  $K' = \varphi(K)$ . Then  $K'(A) : K$  is a splitting field extension for  $S$ .

**Theorem 3.1.** Let  $f \in K[t] \setminus K$ , and suppose that  $L : K$  and  $M : K$  are splitting field extensions for  $f$ . Then  $L \cong M$ , and thus  $[L : K] = [M : K]$ .

**Theorem 3.2.** Suppose that  $S \subseteq K[t] \setminus K$ , and suppose that  $L : K$  and  $M : K$  are splitting field extensions for  $S$ . Then  $L \cong M$  and  $[L : K] = [M : K]$ .

## 4 Normal extensions and composita

### 4.1 Normal extensions and splitting field extensions

**Proposition 13.** Suppose that  $L : M : K$  is a tower of field extensions and  $L : K$  is a normal extension. Then  $L : M$  is also a normal extension.

### 4.2 Normal closures

**Theorem 4.1.** Suppose that  $M : L : K$  is a tower of field extensions having the property that  $M : K$  is normal. Assume that  $K \subseteq L \subseteq M$ . Then the following are equivalent:

- (i) the field extension  $L : K$  is normal;
- (ii) any  $K$ -homomorphism of  $L$  into  $M$  is an automorphism of  $L$ ;
- (iii) whenever  $\sigma : M \rightarrow M$  is a  $K$ -automorphism, then  $\sigma(L) \subseteq L$ .

### 4.3 Composita of field extensions

**Proposition 14.** Suppose that  $E : K$  and  $F : K$  are finite extensions having the property that  $K$ ,  $E$  and  $F$  are contained in a field  $L$ . Then  $EF : K$  is a finite extension.

**Theorem 4.2.** Let  $E : K$  and  $F : K$  be finite extensions having the property that  $K$ ,  $E$  and  $F$  are contained in a field  $L$ .

- (a) When  $E : K$  is normal, then  $EF : F$  is normal.
- (b) When  $E : K$  and  $F : K$  are both normal, then  $EF : K$  and  $E \cap F : K$  are normal.

### 4.4 Normal closures (non-examinable)

## 5 Separability

**Theorem 5.1.** Suppose that  $L : M : K$  is a tower of algebraic extensions. Then  $L : K$  is separable if and only if  $L : M$  and  $M : K$  are both separable.

**Theorem 5.2.** Suppose that  $E : K$  and  $F : K$  are finite extensions with  $E \subseteq L$  and  $F \subseteq L$ , where  $L$  is a field.

- (a) When  $E : K$  is separable, then so too is  $EF : F$ ;
- (b) When  $E : K$  and  $F : K$  are both separable, then so too are  $EF : K$  and  $E \cap F : K$ .

## 6 Inseparable polynomials, differentiation, and the Frobenius map

### 6.1 Inseparable polynomials and differentiation

### 6.2 The Frobenius map

## 7 The Primitive Element Theorem

## 8 Fixed fields and Galois extensions

**Theorem 8.1.** *Suppose that  $L : K$  is an algebraic extension. Then  $L : K$  is Galois if and only if  $K = \text{Fix}_L(\text{Gal}(L : K))$ .*

**Theorem 8.2.** *Suppose that  $L$  is a field and  $G$  is a finite subgroup of  $\text{Aut}(L)$ , and put  $K = \text{Fix}_L(G)$ . Then  $L : K$  is a finite Galois extension with  $[L : K] = |\text{Gal}(L : K)|$ , and furthermore  $G = \text{Gal}(L : K)$ .*

**Theorem 8.3.** *Suppose that  $L : K$  is a finite extension. Then, if  $L : K$  is a Galois extension, one has  $|\text{Gal}(L : K)| = [L : K]$  and  $K = \text{Fix}_L(\text{Gal}(L : K))$ . If  $L : K$  is not Galois, meanwhile, one has  $|\text{Gal}(L : K)| < [L : K]$  and  $K$  is a proper subfield of  $\text{Fix}_L(\text{Gal}(L : K))$ .*

**Proposition 15.** *Suppose that  $L : K$  is a Galois extension, and further that  $L : M : K$  is a tower of field extensions. Then  $L : M$  is a Galois extension.*

## 9 The main theorems of Galois theory

### 9.1 The Fundamental Theorem

**Definition 25.** Suppose that  $L : K$  is a field extension. When  $G$  is a subgroup of  $\text{Aut}(L)$ , we write  $\phi(G)$  for  $\text{Fix}_L(G)$ , and when  $L : M : K_0$  is a tower of field extensions with  $K_0 = \phi(\text{Gal}(L : K))$ , we write  $\gamma(M)$  for  $\text{Gal}(L : M)$ .

**Theorem 9.1** (The Fundamental Theorem of Galois Theory). *Suppose that  $L : K$  is a finite extension, let  $G = \text{Gal}(L : K)$ , and put  $K_0 = \phi(G)$ . Then one has the following:*

- (a) *the map  $\phi$  is a bijection from the set of subgroups of  $G$  onto the set of fields  $M$  intermediate between  $L$  and  $K_0$ , and  $\gamma$  is the inverse map;*
- (b) *if  $H \leq G$ , then  $H \trianglelefteq G$  if and only if  $\phi(H) : K_0$  is a normal extension;*
- (c) *if  $H \leq G$ , one has  $\text{Gal}(\phi(H) : K_0) \cong G/H$ . In particular, if  $\sigma \in G$ , one has  $\sigma|_{\phi(H)} \in \text{Gal}(\phi(H) : K_0)$ , and the map  $\sigma \mapsto \sigma|_{\phi(H)}$  is a homomorphism of  $G$  onto  $\text{Gal}(\phi(H) : K_0)$  with kernel  $H$ .*

**Definition 26** (Galois group of polynomial). When  $f \in K[t]$  and  $L : K$  is a splitting field extension for  $f$ , we define the Galois group of the polynomial  $f$  over  $K$  to be  $\text{Gal}_K(f) = \text{Gal}(L : K)$ .

### 9.2 Non-examinable: consequences for composita and intersections

## 10 Finite fields

## 11 Solvability and solubility

**Definition 27** (Soluble group). A finite group  $G$  is soluble if there is a series of groups

$$\{\text{id}\} = G_0 \leq G_1 \leq \cdots \leq G_n = G,$$

with the property that  $G_i \trianglelefteq G_{i+1}$  and  $G_{i+1}/G_i$  is abelian ( $0 \leq i < n$ ).

**Theorem 11.1.** *Let  $K$  be a field of characteristic 0. Then  $f \in K[t]$  is solvable by radicals if and only if  $\text{Gal}_K(f)$  is soluble.*

**Lemma 11.2.** *Suppose  $\text{char } K = 0$  and  $L : K$  is a radical extension. Then there exists an extension  $N : L$  such that  $N : K$  is normal and radical.*

**Definition 28** (Cyclic extension). The extension  $L : K$  is cyclic if  $L : K$  is a Galois extension and  $\text{Gal}(L : K)$  is a cyclic group.

**Lemma 11.3.** *Suppose that  $\text{char } K = 0$  and let  $p$  be a prime number. Also, let  $L : K$  be a splitting field extension for  $t^p - 1$ . Then  $\text{Gal}(L : K)$  is cyclic, and hence  $L : K$  is a cyclic extension.*

**Lemma 11.4.** *Let  $\text{char } K = 0$  and suppose that  $n$  is an integer such that  $t^n - 1$  splits over  $K$ . Let  $L : K$  be a splitting field extension for  $t^n - a$ , for some  $a \in K$ . Then  $\text{Gal}(L : K)$  is abelian.*

**Theorem 11.5.** *Let  $\text{char } K = 0$  and suppose that  $L : K$  is Galois. Suppose that there is an extension  $M : L$  with the property that  $M : K$  is radical. Then  $\text{Gal}(L : K)$  is soluble.*

**Corollary 5.** *Suppose that  $\text{char } K = 0$ . Then  $\text{Gal}_K(f)$  is soluble whenever  $f \in K[t]$  is soluble by radicals.*

**Corollary 6.** *There exist quintic polynomials in  $\mathbb{Q}[t]$  with insoluble Galois groups, such as  $f(t) = t^5 - 4t + 2$ , and which are not solvable by radicals.*

**Lemma 11.6.** *Let  $\text{char } K = 0$ , and suppose that  $L : K$  is a cyclic extension of degree  $n$ . Suppose also that  $K$  contains a primitive  $n$ -th root of 1. Then there exists  $\theta \in K$  having the property that  $t^n - \theta$  is irreducible over  $K$ , and  $L : K$  is a splitting field for  $t^n - \theta$ . Further, if  $\beta$  is a root of  $t^n - \theta$  over  $L$ , then  $L = K(\beta)$ .*

**Theorem 11.7.** *Let  $\text{char } K = 0$ , and suppose that  $f \in K[t] \setminus K$ . Then  $f$  is solvable by radicals whenever  $\text{Gal}_K(f)$  is soluble.*