1 Field extensions and algebraic elements

Definition 1 (Field extension)**.** *When K and L are fields, we say that L is an extension of K if there is a homomorphism $\varphi : K \to L$. We then talk about the field extension (φ, K, L).*

Definition 2 (Degree, finite extension)**.** *Suppose that $L : K$ is a field extension. We define the degree of $L : K$ to be the dimension of L as a vector space over K. We use the notation $[L : K]$ to denote the degree of $L : K$. Further, we say that $L : K$ is a finite extension if $[L : K] < \infty$.*

Definition 3 (Tower, intermediate field)**.** *We say that $M : L : K$ is a tower of field extensions if $M : L$ and $L : K$ are field extensions, and in this case we say that L is an intermediate field (relative to the extension $M : K$)*

Proposition 1.1. *Suppose that L is a field extension of K with associated embedding $\varphi : K \to L$. Then L forms a vector space over K, under the operations*

$$\begin{aligned} \text{(vector addition) } \psi : L \times L \to L \quad &\textit{given by} \quad (v_1, v_2) \mapsto v_1 + v_2 \\ \text{(scalar multiplication) } \tau : K \times L \to L \quad &\textit{given by} \quad (k, v) \mapsto \varphi(k)v. \end{aligned}$$

Theorem 1.2 (The Tower Law)**.** *Suppose that $M : L : K$ is a tower of field extensions. Then $M : K$ is a field extension, and $[M : K] = [M : L][L : K]$.*

Corollary 1.3. *Suppose that $L : K$ is a field extension for which $[L : K]$ is a prime number. Then whenever $L : M : K$ is a tower of field extensions with $K \subseteq M \subseteq L$, one has either $M = L$ or $M = K$.*

Proposition 1.4. *Suppose that K and L are fields and that $\varphi : K \to L$ is a homomorphism. With t and y denoting indeterminates, extend the homomorphism φ to the mapping $\psi : K[t] \to L[y]$ by defining*

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

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

Definition 4 (Algebraic/transcendental element)**.** *Suppose that $L : K$ is a field extension with associated embedding φ. Suppose also that $\alpha \in L$.*

(i) We say that α is algebraic over K when α is the root of $\varphi(f)$ for some non-zero polynomial $f \in K[t]$.

(ii) If α is not algebraic over K, then we say α is transcendental over K.

(iii) When every element of L is algebraic over K, we say that the field L is algebraic over K.

Definition 5 (Evaluation map)**.** *Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\alpha \in L$. We define the evaluation map $E_\alpha : K[t] \to L$ by putting $E_\alpha(f) = f(\alpha)$ for each $f \in K[t]$.*

Proposition 1.5. *Suppose $L : K$ is a field extension with $K \subseteq L$, and $\alpha \in L$. Then E_α is a ring homomorphism.*

Proposition 1.6. *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 $m_\alpha(K) \in K[t]$ that generates I.

Definition 6 (Minimal polynomial)**.** *Suppose that $L : K$ is a field extension with $K \subseteq L$, and suppose that $\alpha \in L$ is algebraic over K. Then the minimal polynomial of α over K is the unique monic polynomial $m_\alpha(K)$ having the property that $\ker(E_\alpha) = (m_\alpha(K))$.*

Theorem 1.7. *Suppose that $L : K$ is a field extension, and that $\alpha \in L$ is algebraic over K. Let g be the minimal polynomial $m_\alpha(K)$ of α over K. Then g is irreducible over K, and $K[t]/(g)$ is a field.*

Theorem 1.8. *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 $\varphi : K[t] \to L[y]$, having the property that L contains a root of $\varphi(f)$.*

Definition 7 (Smallest subring/subfield)**.** *Let $L : K$ be a field extension with $K \subseteq L$.*

(i) When $\alpha \in L$, we denote by $K[\alpha]$ the smallest subring of L containing K and α, and by $K(\alpha)$ the smallest subfield of L containing K and α;

(ii) More generally, when $A \subseteq L$, we denote by $K[A]$ the smallest subring of L containing K and A, and by $K(A)$ the smallest subfield of L containing K and A.

Proposition 1.9. *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 1.10. *Let $L : K$ be a field extension with $K \subseteq L$, and suppose that $\alpha \in L$. Then*

$$K[\alpha] = \left\{c_0 + c_1\alpha + \cdots + c_d\alpha^d : d \in \mathbb{Z}_{\leq 0},\ c_0, \ldots, c_d \in K\right\}$$

and

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

Theorem 1.11. *Let $L : K$ be a field extension with $K \subseteq L$, and suppose that $\alpha \in L$ is algebraic over K.*

(i) The ring $K[\alpha]$ is a field, and $K[\alpha] = K(\alpha)$;

(ii) Let $n = \deg m_\alpha(K)$. Then $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$ is a basis for $K(\alpha)$ over K, and hence $[K(\alpha) : K] = \deg m_\alpha(K)$.

Proposition 1.12. *Let $L : K$ be a field extension with $K \subseteq L$, and suppose that $\alpha \in L$. Then α is algebraic over K if and only if $[K(\alpha) : K] < \infty$.*

Proposition 1.13. *Suppose that $L : K$ is a field extension with $K \subseteq L$, and suppose that $\alpha \in L$ is algebraic over K. Then every element of $K(\alpha)$ is algebraic over K.*

Theorem 1.14. *Let $L : K$ be a field extension with $K \subseteq L$. Then the following are equivalent:*

(i) one has $[L : K] < \infty$;

(ii) the extension $L : K$ is algebraic, and there exist $\alpha_1, \ldots, \alpha_n \in L$ having the property that $L = K(\alpha_1, \ldots, \alpha_n)$.

Proposition 1.15. *Let $L : K$ be a field extension, and define*

$$L^{\mathrm{alg}} = \{\alpha \in L : \alpha \text{ is algebraic over } K\}.$$

Then L^{alg} is a subfield of L.

Definition 8 (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 $1_K + \ldots + 1_K$ (as an n-fold sum). We define the characteristic of K, denoted by $\mathrm{char}(K)$, 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 1.16. *Let K be a field with $\mathrm{char}(K) > 0$. Then $\mathrm{char}(K)$ is equal to a prime number p, and then for all $x \in K$ one has $p \cdot x = 0$.*

Theorem 1.17. *Suppose that $\mathrm{char}(K) = p > 0$, and put $F = \{c \cdot 1_K : c \in \mathbb{Z}\}$. Then F is a subfield (called the prime subfield) of K, and $F \cong \mathbb{Z}/p\mathbb{Z}$.*

Theorem 1.18. *Let K be a field, and denote by $K^\times$ the abelian multiplicative group $K \setminus \{0\}$. Then every finite subgroup G of $K^\times$ is cyclic. In particular, if K is a finite field then $K^\times$ is cyclic.*

Definition 9 (Highest common factor, content, primitive)**.** *Let R be a UFD. When $a_0, \ldots, a_n \in R$ are not all 0, we define as a highest common factor of $a_0, \ldots, a_n$ (written hcf($a_0, \ldots, a_n$)) any element $c \in R$ satisfying*

(i) $c \mid a_i$ $(0 \leq i \leq n)$, and

(ii) whenever $d \mid a_i$ $(0 \leq i \leq n)$, then $d \mid c$.

When $f = a_0 + a_1X + \ldots + a_nX^n$ is a non-zero polynomial in $R[X]$, we define a content of f to be any hcf($a_0, \ldots, a_n$). We say that $f \in R[X]$ is primitive if $f \neq 0$ and the content of f is divisible only by units of R.

Theorem 1.19 (Gauss' Lemma)**.** *Suppose that R is a UFD with field of fractions Q. Suppose that f is a primitive element of $R[X]$ with $\deg f > 0$. Then f is irreducible in $R[X]$ if and only if f is irreducible in Q.*

Theorem 1.20 (Eisenstein's Criterion)**.** *Suppose that R is a UFD, and that $f = a_0+a_1X+\ldots+a_nX^n \in R[X]$ is primitive. Then provided that there is an irreducible element p of R having the property that*

(i) $p \mid a_i$ for $0 \leq i < n$,

(ii) $p^2 \nmid a_0$, and

(iii) $p \nmid a_n$,

then f is irreducible in $R[X]$, and hence also in $Q[X]$, where Q is the field of fractions of R.

Theorem 1.21 (Localisation principle)**.** *Let R be an integral domain, and let I be a prime ideal of R. Define $\varphi : R[X] \to (R/I)[X]$ by putting*

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

where $\overline{a}_j = a_j + I$. Then φ 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 $(R/I)[X]$.

3 Extending field homomorphisms and the Galois group of an extension

Definition 16 (Extension of field homomorphism, isomorphic field extensions)**.** *For $i = 1$ and 2, let $L_i : K_i$ be a field extension relative to the embedding $\varphi_i : K_i \to L_i$. Suppose that $\sigma : K_1 \to K_2$ and $\tau : L_1 \to L_2$ are isomorphisms. We say that τ extends σ if $\tau \circ \varphi_1 = \varphi_2 \circ \sigma$. In such circumstances, we say that $L_1 : K_1$ and $L_2 : K_2$ are isomorphic field extensions.*

When $\sigma : K_1 \to K_2$ and $\tau : L_1 \to L_2$ are homomorphisms (instead of isomorphisms), then τ extends σ as a homomorphism of fields when the isomorphism $\tau : L_1 \to L_1' = \tau(L_1)$ extends the isomorphism $\sigma : K_1 \to K_1' = \sigma(K_1)$.

Definition 17 (F-homomorphism)**.** *Let $L : K$ be a field extension relative to the embedding $\varphi : K \to L$, and let M be a subfield of L containing $\varphi(K)$. Then, when $\sigma : M \to L$ is a homomorphism, we say that σ is a K-homomorphism if σ leaves $\varphi(K)$ pointwise fixed, which is to say that for all $\alpha \in \varphi(K)$, one has $\sigma(\alpha) = \alpha$.*

Proposition 3.1. *Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\tau : L \to L$ is a K-homomorphism. Suppose that $f \in K[t]$ has the property that $\deg f \geq 1$, and additionally that $\alpha \in L$. Then*

(i) if $f(\alpha) = 0$, one has $f(\tau(\alpha)) = 0$;

(ii) when τ is a K-automorphism of L, one has that $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.

Theorem 3.2. *Let $\sigma : K_1 \to K_2$ be a field isomorphism. Suppose that L_i is a field with $K_i \subseteq L_i$ $(i = 1, 2)$. Suppose also that $\alpha \in L_1$ is algebraic over K_1, and that $\beta \in L_2$ is algebraic over K_2. Then we can extend σ to an isomorphism $\tau : K_1(\alpha) \to K_2(\beta)$ in such a manner that $\tau(\alpha) = \beta$ if and only if $m_\beta(K_2) = \sigma(m_\alpha(K_1))$.*

Note: When $\tau : K_1(\alpha) \to K_2(\beta)$ is a homomorphism, and τ extends the homomorphism $\sigma : K_1 \to K_2$, then τ is completely determined by σ and the value of $\tau(\alpha)$.

Corollary 3.3. *Let $L : M$ be a field extension with $M \subseteq L$. Suppose that $\sigma : M \to L$ is a homomorphism, and $\alpha \in L$ is algebraic over M. Then the number of ways we can extend σ to a homomorphism $\tau : M(\alpha) \to L$ is equal to the number of distinct roots of $\sigma(m_\alpha(M))$ that lie in L.*

Definition 18 (Galois group of)**.** *Suppose that $L : K$ is a field extension. With $\mathrm{Aut}(L)$ denoting the automorphism group of L, we set*

$$\mathrm{Gal}(L : K) = \{\sigma \in \mathrm{Aut}(L) : \sigma \textit{ is a } K\textit{-homomorphism}\}$$

and we call $\mathrm{Gal}(L : K)$ the Galois group of $L : K$.

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

Theorem 3.4. *Suppose that $L : K$ is an algebraic extension, and $\sigma : L \to L$ is a K-homomorphism. Then σ is an automorphism of L.*

Theorem 3.5. *If $L : K$ is a finite extension, then $|\mathrm{Gal}(L : K)| \leq [L : K]$.*

Corollary 3.6. *Suppose that $L : F$ and $L : F'$ are finite extensions with $F \subseteq L\ tand F' \subseteq L$, and further that $\psi : F \to F'$ is an isomorphism. Then there are at most $[L : F]$ ways to extend ψ to a homomorphism from L into L.*

Corollary 3.7. *Let $L : K$ be a finite extension with $K \subseteq L$. Suppose that $\alpha_1, \ldots, \alpha_n \in L$ and put $L = K(\alpha_1, \ldots, \alpha_n)$. Let $K_0 = K$, and for $1 \leq i \leq n$, let $K_i = K_{i-1}(\alpha_i)$. Then every automorphism $\tau \in \mathrm{Gal}(L : K)$ corresponds to a sequence of homomorphisms $\sigma_1, \ldots, \sigma_n$, having the property that $\sigma_0 : K \to L$ is the inclusion map, one has $\sigma_n = \tau$, and for $1 \leq i \leq n$, the map $\sigma_i : K_i \to L$ is a homomorphism extending $\sigma_{i-1} : K_{i-1} \to L$.*

4 Algebraic closures

Definition 19 (Algebraically closed field, algebraic closure)**.** *Let M be a field.*

(i) We say that M is algebraically closed if every non-constant polynomial $f \in M[t]$ has a root in M.

(ii) We say that M is an algebraic closure of K if $M : K$ is an algebraic field extension having the property that M is algebraically closed.

Lemma 4.1. *Let M be a field. The following are equivalent:*

(i) The field M is algebraically closed;

(ii) every non-constant polynomial $f \in M[t]$ factors in $M[t]$ as a product of linear factors;

(iii) every irreducible polynomial in $M[t]$ has degree 1;

(iv) the only algebraic extension of M containing M is itself.

Definition 20 (Chain)**.** *Suppose that X is a nonempty, partially ordered set with $\leq$ denoting the partial ordering. A chain C in X is a collection of elements $\{a_i\}_{i \in I}$ of X having the property that for every $i, j \in I$, either $a_i \leq a_j$ or $a_j \leq a_i$.*

Zorn's Lemma: Suppose that X is a nonempty, partially ordered set with $\leq$ the partial ordering. Suppose that every non-empty chain C in X has an upper bound in X. Then X has at least one maximal element m, meaning that if $b \in X$ with $m \leq b$, then $b = m$.

Proposition 4.2. *Any proper ideal A of a commutative ring R is contained in a maximal ideal.*

Lemma 4.3. *Let K be a field. Then there exists an algebraic extension $E : K$, with $K \subseteq E$, having the property that E contains a root of every irreducible $f \in K[t]$, and hence also every $g \in K[t] \setminus K$.*

Theorem 4.4. *Suppose that K is a field. Then there exists an algebraic extension $\overline{K}$ of K having the property that $\overline{K}$ is algebraically closed.*

Corollary 4.5. *When K is a field, the field $\overline{K}$ is a maximal algebraic extension of K.*

Theorem 4.6. *Let E be an algebraic extension of K with $K \subseteq E$, and let $\overline{K}$ be an algebraic closure of K. Given a homomorphism $\varphi : K \to \overline{K}$, the map φ can be extended to a homomorphism from E into $\overline{K}$.*

Corollary 4.7. *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 $\sigma : K \to \overline{K}$ is a homomorphism. Then the number of distinct roots of $m_\alpha(K)$ in $\overline{K}$ is equal to the number of distinct roots of $\sigma(m_\alpha(K))$ in $\overline{K}$.*

Proposition 4.8. *Suppose that L and M are fields having the property that L is algebraically closed, and $\psi : L \to M$ is a homomorphism. Then $\psi(L)$ is algebraically closed.*

Proposition 4.9. *If L and M are both algebraic closures of K, then $L \cong M$.*

Proposition 4.10. *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 $\overline{K} = \overline{L}$.*

Proposition 4.11. *Let $L : K$ be an extension with $K \subseteq L$. Suppose that $g \in L[t]$ is irreducible over L, and that $g \bigm| f$ in $L[t]$, where $f \in K[t] \setminus \{0\}$. The g divides a factor of f that is irreducible over K. Thus, there exists an irreducible $h \in K[t]$ having the property that $h \bigm| f$ in $K[t]$, and $g \bigm| h$ in $L[t]$.*

5 Splitting field extensions

Definition 21 (Splitting field, splitting field extension)**.** *Suppose that $L : K$ is a field extension relative to the embedding $\varphi : K \to L$, 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 $\alpha_1, \ldots, \alpha_n \in L$.

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

Proposition 5.2. *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 5.3. *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 $\varphi : \overline{K} \to K$. Let*

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

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

Theorem 5.4. *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 5.5. *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 $[L : K] = [M : K]$.*

6 Normal extensions and composita

Definition 22 (Normal extension)**.** *The extension $L : K$ is normal if it is algebraic, and every irreducible polynomial $f \in K[t]$ either splits over L or has no root in L.*

Proposition 6.1. *Suppose that $L : K$ is a normal extension with $K \subseteq L \subseteq \overline{K}$. Then for any K-homomorphism $\tau : L \to \overline{K}$, we have $\tau(L) = L$.*

Proposition 6.2. *An extension $L : K$ is a finite, normal extension if and only if it is a splitting field extension for some $f \in K[t] \setminus K$. More generally, an extension $L : K$ is normal if and only if it is a splitting field extension for some $S \subseteq K[t] \setminus K$.*

Proposition 6.3. *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.*

Theorem 6.4. *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 $\sigma : M \to M$ is a K-automorphism, then $\sigma(L) \subseteq L$.*

Proposition 6.5. *Suppose that $M : K$ is a normal extension. Then:*

(a) *for any $\sigma \in \mathrm{Gal}(M : K)$ and $\alpha \in M$, we have $m_{\sigma(\alpha)}(K) = m_\alpha(K)$;*

(b) *for any $\alpha, \beta \in M$ with $m_\alpha(K) = m_\beta(K)$, there exists $\tau \in \mathrm{Gal}(M : K)$ having the property that $\tau(\alpha) = \beta$.*

Definition 23 (Compositum)**.** *Let K_1 and K_2 be fields contained in some field L. The compositum of K_1 and K_2 in L, denoted by K_1K_2, is the smallest subfield of L containing both K_1 and K_2.*

Proposition 6.6. *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 6.7. *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.*

7 Separability

Definition 25 (Separable)**.** *Let K be a field.*

(i) *An irreducible polynomial $f \in K[t]$ is separable over K if it has no multiple roots, meaning that $f = \lambda(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_d)$, where $\alpha_1, \ldots, \alpha_d \in \overline{K}$ are distinct.*

(ii) *A non-zero polynomial $f \in K[t]$ is separable over K if its irreducible factors in $K[t]$ are separable over K.*

(iii) *When $L : K$ is a field extension, we say that $\alpha \in L$ is separable over K when α is algebraic over K and $m_\alpha(K)$ is separable.*

(iv) *An algebraic extension $L : K$ is a separable extension if every $\alpha \in L$ is separable over K.*

Proposition 7.1. *Suppose that $L : M : K$ is a tower of algebraic field extensions. Assume that $K \subseteq M \subseteq L \subseteq \overline{K}$, and suppose that $f \in K[t] \setminus K$ satisfies the property that f is separable over K. If $g \in M[t] \setminus M$ has the property that $g \mid f$, then g is separable over M. Thus, if $\alpha \in L$ is separable over K then α is separable over M, and if $L : K$ is separable then so is $L : M$.*

Proposition 7.2. *Suppose that $L : M$ is an algebraic field extension. Let $\alpha \in L$ and $\sigma : M \to \overline{M}$ be a homomorphism. Then $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$ if and only if $m_\alpha(M)$ is separable over M.*

Theorem 7.3. *Let $L : K$ be a finite extension with $K \subseteq L \subseteq \overline{K}$, whence $L = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in L$. Put $K_0 = K$, and for $1 \le i \le n$, set $K_i = K_{i-1}(\alpha_i)$. Finally, let $\sigma_0 : K \to \overline{K}$ be the inclusion map.*

(i) If α_i is separable over K_{i-1} for $1 \le i \le n$, then there are $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \to \overline{K}$.

(ii) If α_i is not separable over K_{i-1} for some i with $1 \le i \le n$, then there are fewer than $[L : K]$ ways to extend σ_0 to a homomorphism $\tau : L \to \overline{K}$.

Theorem 7.4. *Let $L : K$ be a finite extension with $L = K(\alpha_1, \dots, \alpha_n)$. Set $K_0 = K$, and for $1 \le i \le n$, inductively define K_i by putting $K_i = K_{i-1}(\alpha_i)$. Then the following are equivalent:*

(i) the element α_i is separable over K_{i-1} for $1 \le i \le n$;

(ii) the element α_i is separable over K for $1 \le i \le n$;

(iii) the extension $L : K$ is separable.

Corollary 7.5. *Suppose that $L : K$ is a finite extension. If $L : K$ is a separable extension, then the number of K-homomorphism $\sigma : L \to \overline{K}$ is $[L : K]$, and otherwise the number is smaller than $[L : K]$.*

Corollary 7.6. *Suppose that $f \in K[t] \setminus K$ and that $L : K$ is a splitting field extension for f. Then $L : K$ is a separable extension if and only if f is separable over K. More generally, suppose that $L : K$ is a splitting field extension for $S \subseteq K[t] \setminus K$. Then $L : K$ is a separable extension if and only if each $f \in S$ is separable over K.*

Theorem 7.7. *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 7.8. *Suppose tht $E : K$ 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 $E \cap F : K$.

8 Inseparable polynomials, differentiation, and the Frobenius map

Definition 26 (Inseparable)**.** *A polynomial $f \in K[t]$ is inseparable over K if f is not separable over K, meaning that f has an irreducible factor $g \in K[t]$ having the property that g has fewer than* $\deg g$ *distinct roots in $\overline{K}$.*

Definition 27 (Formal derivative)**.** *We define the derivative operator $\mathcal{D} : K[t] \to K[t]$ by*

$$\mathcal{D}\left(\sum_{k=0}^{n} a_k t^k\right) = \sum_{k=1}^{n} k a_k t^{k-1}.$$

Theorem 8.1. *Let $f \in K[t] \setminus K$, and let $L : K$ be a splitting field extension for f. Assume that $K \subseteq L$. Then the following are equivalent:*

(i) The polynomial f has a repeated root over L;

(ii) There is some $\alpha \in L$ for which $f(\alpha) = 0 = (\mathcal{D}f)(\alpha)$;

(iii) There is some $g \in K[t]$ having the property that $\deg g \ge 1$ *and g divides both f and $\mathcal{D}f$.*

Theorem 8.2. *Suppose that $f \in K[t]$ is irreducible over K. Then f is inseparable over K if and only if* $\mathrm{char}(K) = p > 0$, *and $f \in K[t^p]$, which is to say that $f = a_0 + a_1 t^p + \cdots + a_m t^{mp}$, for some $a_0, \dots, a_m \in K$.*

Corollary 8.3. *Suppose that* $\operatorname{char}(K) = 0$*. Then all polynomials in* $K[t]$ *are separable over* K*.*

Definition 28 (Frobenius map)**.** *Suppose that* $\operatorname{char}(K) = p > 0$*. The Frobenius map* $\phi : K \to K$ *is defined by* $\phi(\alpha) = \alpha^p$*.*

Note: $\operatorname{Fix}_\phi(K) = \{\alpha \in K : \phi(\alpha) = \alpha\}$.

Theorem 8.4. *Suppose that* $\operatorname{char}(K) = p > 0$*, and let* F *be the prime subfield of* K*. Let* $\phi : K \to K$ *denote the Frobenius map. Then* ϕ *is an injective homomorphism, and* $\operatorname{Fix}_\phi(K) = F$*.*

Corollary 8.5. *Suppose that* $\operatorname{char}(K) = p > 0$ *and* K *is algebraic over its prime subfield. Then the Frobenius map is an automorphism of* K*.*

Corollary 8.6. *Suppose that* $\operatorname{char}(K) = p > 0$ *and* K *is algebraic over its prime subfield. Then all polynomials in* $K[t]$ *are separable over* K*.*

Theorem 8.7. *Suppose that* $\operatorname{char}(K) = p > 0$*. Let*

$$f(t) = g(t^p) = a_0 + a_1 t^p + \cdots + a_{n-1} t^{(n-1)p} + t^{np}$$

be a non-constant monic polynomial over K*. Then* $f(t)$ *is irreducible in* $K[t]$ *if and only if* $g(t)$ *is irreducible in* $K[t]$ *and not all the coefficients* a_i *are* p*-th powers in* K*.*

9 The Primitive Element Theorem

Definition 29 (Simple extension)**.** *Suppose* $L : K$ *is a field extension relative to the embedding* $\varphi : K \to L$*. We say that* $L : K$ *is a simple extension if there is some* $\gamma \in L$ *having the property that* $L = \varphi(K)(\gamma)$*.*

Theorem 9.1 (The Primitive Element Theorem)**.** *Let* $L : K$ *be a finite, separable extension with* $K \subseteq L$*. Then* $L : K$ *is a simple extension.*

Corollary 9.2. *Suppose that* $L : K$ *is an algebraic, separable extension, and suppose that for every* $\alpha \in L$*, the polynomial* $m_\alpha(K)$ *has degree at most* n *over* K*. Then* $[L : K] \leq n$*.*

10 Fixed fields and Galois extensions

Definition 30 (Fixed field)**.** *Let* $L : K$ *be a field extension. When* G *is a subgroup of* $\operatorname{Aut}(L)$*, we define the fixed field of* G *to be*

$$\operatorname{Fix}_L(G) = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

Proposition 10.1. *Let* K*,* M *and* L *be fields with* $K \subseteq L$ *and* $M \subseteq L$*. Suppose that* G *and* H *are subgroups of* $\operatorname{Aut}(L)$*. Then one has the following:*

(a) if $K \subseteq M$*, then* $\operatorname{Gal}(L : K) \geqslant \operatorname{Gal}(L : M)$*;*

(b) if $G \leq H$*, then* $\operatorname{Fix}_L(G) \supseteq \operatorname{Fix}_L(H)$*;*

(c) one has $K \subseteq \operatorname{Fix}_L(\operatorname{Gal}(L : K))$*;*

(d) one has $G \leq \operatorname{Gal}(L : \operatorname{Fix}_L(G))$*;*

(e) one has $\operatorname{Gal}(L : K) = \operatorname{Gal}(L : \operatorname{Fix}_L(\operatorname{Gal}(L : K)))$*;*

(f) one has $\operatorname{Fix}_L(G) = \operatorname{Fix}_L(\operatorname{Gal}(L : \operatorname{Fix}_L(G)))$*.*

Definition 31 (Galois extension)**.** *When* $L : K$ *is a field extension, we say that* $L : K$ *is a Galois extension if it is an extension that is normal and separable.*

Theorem 10.2. *Suppose that* $L : K$ *is an algebraic extension. Then* $L : K$ *is Galois if and only if* $K = \operatorname{Fix}_L(\operatorname{Gal}(L : K))$*.*

Theorem 10.3. *Suppose that L is a field and G is a finite subgroup of $\mathrm{Aut}(L)$, and put $K = \mathrm{Fix}_L(G)$. Then $L : K$ is a finite Galois extension with $[L : K] = |\mathrm{Gal}(L : K)|$, and furthermore $G = \mathrm{Gal}(L : K)$.*

Theorem 10.4. *Suppose that $L : K$ is a finite extension. Then, if $L : K$ is a Galois extension, one has $|\mathrm{Gal}(L : K)| = [L : K]$ and $K = \mathrm{Fix}_L(\mathrm{Gal}(L : K))$. If $L : K$ is not Galois, meanwhile, one has $|\mathrm{Gal}(L : K)| < [L : K]$ and K is a proper subfield of $\mathrm{Fix}_L(\mathrm{Gal}(L : K))$.*

Proposition 10.5. *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.*

11 The main theorems of Galois theory

Definition 32. *Suppose that $L : K$ is a field extension. When G is a subgroup of $\mathrm{Aut}(L)$, we write $\phi(G)$ for $\mathrm{Fix}_L(G)$, and when $L : M : K_0$ is a tower of field extensions with $K_0 = \phi(\mathrm{Gal}(L : K))$, we write $\gamma(M)$ for $\mathrm{Gal}(L : M)$.*

Theorem 11.1 (The Fundamental Theorem of Galois Theory)**.** *Suppose that $L : K$ is a finite extension, let $G = \mathrm{Gal}(L : K)$, and put $K_0 = \phi(G)$. Then one has the following:*

(a) the map ϕ is a bijection from the set of subgroups of G onto the set of fields M intermediate between L and K_0, and γ is the inverse map;

(b) if $H \le G$, then $H \trianglelefteq G$ if and only if $\phi(H) : K_0$ is a normal extension;

(c) if $H \trianglelefteq G$, one has $\mathrm{Gal}(\phi(H) : K_0) \cong G/H$. In particular, if $\sigma \in G$, one has $\sigma|_{\phi(H)} \in \mathrm{Gal}(\phi(H) : K_0)$, and the map $\sigma \mapsto \sigma|_{\phi(H)}$ is a homomorphism of G onto $\mathrm{Gal}(\phi(H) : K_0)$ with kernel H.

Definition 33 (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 $\mathrm{Gal}_K(f) = \mathrm{Gal}(L : K)$.*

12 Finite fields

Theorem 12.1. *Let p be a prime, and let $q = p^n$ for some $n \in \mathbb{N}$. Then:*

(a) There exists a field $\mathbb{F}_q$ of order q, and this field is unique up to isomorphism.

(b) All elements of $\mathbb{F}_q$ satisfy the equation $t^q = t$, and hence $\mathbb{F}_q : \mathbb{F}_p$ is a splitting field extension for $t^q - t$.

(c) There is a unique copy of $\mathbb{F}_q$ inside any algebraically closed field containing $\mathbb{F}_p$.

Theorem 12.2. *Let p be a prime, and suppose that $q = p^n$ for some natural number n. Then:*

(a) the field extension $\mathbb{F}_q : \mathbb{F}_p$ is Galois with $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$;

(b) The field $\mathbb{F}_q$ contains a subfield of order p^d if and only if $d \mid n$. When $d \mid n$, moreover, there is a unique subfield of $\mathbb{F}_q$ of order p^d.

13 Solvability by radicals: polynomials of degree 2, 3 and 4

Definition 34 (Radical element/extension)**.** *Suppose that $L : K$ is a field extension, and $\beta \in L$. We say that β is radical over K when $\beta^n \in K$ for some $n \in \mathbb{N}$ (so $\beta = \alpha^{1/n}$ for some $\alpha \in K$ and some $n \in \mathbb{N}$). We say that $L : K$ is an extension by radicals when there is a tower of field extensions $L = L_r : L_{r-1} : \cdots : L_0 = K$ such that $L_i = L_{i-1}(\beta_i)$ with β_i radical over L_{i-1} $(1 \le i \le r)$. We say $f \in K[t]$ is solvable by radicals if there is a radical extension of K over which f splits.*

14 Solvability and solubility

Definition 35 (Soluble group). *A finite group G is soluble if there is a series of groups*

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

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

Theorem 14.1. *Let K be a field of characteristic 0. Then $f \in K[t]$ is solvable by radicals if and only if $\mathrm{Gal}_K(f)$ is soluble.*

Lemma 14.2. *Suppose $\mathrm{char}(K) = 0$ and $L : K$ is a radical extension. Then there exists an extension $N : L$ such that $N : K$ is normal and radical.*

Definition 36 (Cyclic extension). *The extension $L : K$ is cyclic if $L : K$ is a Galois extension and $\mathrm{Gal}(L : K)$ is a cyclic group.*

Lemma 14.3. *Suppose that $\mathrm{char}(K) = 0$ and let p be a prime number. Also, let $L : K$ be a splitting field extension for $t^p - 1$. Then $\mathrm{Gal}(L : K)$ is cyclic, and hence $L : K$ is a cyclic extension.*

Lemma 14.4. *Let $\mathrm{char}(K) = 0$ 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 $\mathrm{Gal}(L : K)$ is abelian.*

Theorem 14.5. *Let $\mathrm{char}(K) = 0$ and suppose that $L : K$ is Galois. Suppose that there is an extension $M : L$ with the property that $M : K$ is radical. Then $\mathrm{Gal}(L : K)$ is soluble.*

Corollary 14.6. *Suppose that $\mathrm{char}(K) = 0$. Then $\mathrm{Gal}_K(f)$ is soluble whenever $f \in K[t]$ is soluble by radicals.*

Corollary 14.7. *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 14.8. *Let $\mathrm{char}(K) = 0$, 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 β is a root of $t^n - \theta$ over L, then $L = K(\beta)$.*

Theorem 14.9. *Let $\mathrm{char}(K) = 0$, and suppose that $f \in K[t] \setminus K$. Then f is solvable by radicals whenever $\mathrm{Gal}_K(f)$ is soluble.*