1 Field extensions and algebraic elements

1.1 Field extensions

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 $M : K$)*

1.2 Algebraic elements

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 $f \in K[t]$.*

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 $m_\alpha(K)$ in $K[t]$ having the property that $\ker(E_\alpha) = (m_\alpha(K))$.*

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.

2 Review of finite fields and tests for irreducibility

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.*

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 $f = a_0 + a_1 X + \ldots + a_n X^n$ 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.

3 Extending field homomorphisms and the Galois group of an extension

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 $\sigma(\alpha) = \alpha$.*

4 Algebraic closures

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

Definition 18 (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.

Definition 19 (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 $a_j \leq a_i$.*

4.2 The existence of an algebraic closure

Definition 20 (Algebraic closure of K). *When K is a field, an algebraic extension $\overline{K} : K$ that is algebraically closed is called an algebraic closure of K.*

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.

6 Normal extensions and composita

6.1 Normal extensions

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.*

6.2 Composita of field extensions

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.*

7 Separability

Definition 24 (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.

8 Inseparable polynomials, differentiation, and the Frobenius map

8.1 Inseparable polynomials and differentiation

Definition 25 (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 K.*

Definition 26 (Formal derivative). *We define the derivative operator $\mathcal{D} : K[t] \to K[t]$ by*

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

8.2 The Frobenius map

Definition 27 (Frobenius map). *Suppose that $\operatorname{char}(K) = p > 0$. The Frobenius map $\phi : K \to K$ is defined by $\phi(\alpha) = \alpha^p$.*

9 The Primitive Element Theorem

Definition 28 (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 $L = \varphi(K)(\gamma)$.*

10 Fixed fields and Galois extensions

Definition 29 (Fixed field)**.** *Let $L : K$ be a field extension. When G is a subgroup of $\mathrm{Aut}(L)$, we define the fixed field of G to be*

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

Definition 30 (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.*

11 The main theorems of Galois theory

11.1 The Fundamental Theorem

Definition 31. *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 $\mathrm{Gal}(L : M)$.*

Definition 32 (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 Solvability by radicals: polynomials of degree 2, 3 and 4

Definition 33 (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}. We say $f \in K[t]$ is solvable by radicals if there is a radical extension of K over which f splits.*

13 Solvability and solubility

Definition 34 (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 ($0 \leq i < n$).

Definition 35 (Cyclic extension)**.** *The extension $L : K$ is cyclic if $L : K$ is a Galois extension and $\mathrm{Gal}(L : K)$ is a cyclic group.*