

## 1 Field Extensions II

**Definition 1** (Smallest subring/subfield). Let  $L : K$  with  $K \subseteq L$ .

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

Then

$$K[\alpha] = \left\{ \sum_{i=0}^d c_i \alpha^i : d \in \mathbb{Z}_{\leq 0}, c_0, \dots, c_d \in K \right\}$$

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

**Definition 2** (Algebraic/transcendental element). Suppose that  $L : K$  is a field extension with  $K \subseteq L$  and  $\alpha \in L$ .

- (i) We say  $\alpha$  is algebraic over  $K$  if  $\exists f \neq 0 \in K[t]$  such that  $f(\alpha) = 0$ .
- (ii) If  $\alpha$  is not algebraic over  $K$ , then we say  $\alpha$  is transcendental over  $K$ .
- (iii) When every element of  $L$  is algebraic over  $K$ , we say that  $L$  is algebraic over  $K$ .

**Definition 3** (Evaluation map). Suppose that  $L : K$  is a field extension with  $K \subseteq L$ , and that  $\alpha \in L$ . We define the evaluation map  $E_\alpha : K[t] \rightarrow L$  by putting  $E_\alpha(f) = f(\alpha)$  for each  $f \in K[t]$ .

**Definition 4** (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  $\alpha$  over  $K$  is the unique monic polynomial  $\mu_\alpha^K$  having the property that  $\ker(E_\alpha) = (\mu_\alpha^K)$ .

**Lemma 1.1.** 1.  $\mu_\alpha^K$  is irreducible over  $K$ ;

2. If  $f \in K[t]$  such that  $f(\alpha) = 0$ , then  $\mu_\alpha^K \mid f$ ;

3. If  $f \in K[t]$  such that  $f(\alpha) = 0$  and  $f$  is irreducible over  $K$ , then  $\exists k \in K$  such that  $f = k\mu_\alpha^K$ .

**Theorem 1.2.** Let  $L : K$  with  $K \subseteq L$ , and suppose that  $\alpha \in L$  is algebraic over  $K$ .

- (i)  $K[\alpha]$  is a field, and  $K[\alpha] = K(\alpha)$ ;
- (ii) If  $n = \deg \mu_\alpha^K$ , then  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  is a basis for  $K(\alpha)$  over  $K$  ( $\implies [K(\alpha) : K] = \deg \mu_\alpha^K$ ).

**Theorem 1.3** (Rational Root Theorem). Let  $\frac{p}{q}$  be a root of  $f = a_0 t^n + \dots + a_{n-1} t^{n-1} + a_n$ , for  $a_j \in \mathbb{Z}$ , where  $p$  and  $q$  are coprime. Then  $p \mid a_n$  and  $q \mid a_0$ .

**Note:** If  $\alpha$  is transcendental over  $K$ , then  $K(\alpha) \cong K(x)$  (where  $x$  is a formal variable).

**Corollary 1.** Let  $L : K$  with  $K \subseteq L$ , and suppose that  $\alpha \in L$  is algebraic over  $K$ . Then every element of  $K(\alpha)$  is algebraic over  $K$ .

**Corollary 2.** Let  $L : K$  with  $K \subseteq L$ . Then  $[L : K] < \infty \iff L = K(\alpha_1, \dots, \alpha_n)$  for  $\alpha_j \in L$ .

**Theorem 1.4.** Let  $L : K$  be a field extension, and define

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

Then  $L^{\text{alg}}$  is a subfield of  $L$ .