14. Field theory

Recall that a field is a commutative ring with 1 in which all elements are invertible.

14.1. **Field extensions.**

Definition. A field extension is a pair of fields (K, F) where K contains F. The standard notation for a field extension is K/F.

Definition. If F and K are two fields, a map $\iota : F \to K$ is called a field embedding if ι is an injective ring homomorphism.

Remark: Any non-trivial homomorphism between fields is an embedding. If $\iota : F \to K$ is a field embedding, then $K/\iota(F)$ is a field extension. By abuse of terminology we will often say that K/F is a field extension.

If K/F is a field extension, then K is a vector space over F. The dimension of this vector space is called the degree of K over F and denoted by $[K : F]$. Thus $[K : F] = \dim_F K$. The extension K/F is called finite if $[K : F]$ is finite.

Proposition 14.1. *For any fields $F \subseteq K \subseteq L$ we have*

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

Proof. Let $\{\alpha_i\}$ be a basis of K over F and $\{\beta_i\}$ a basis of L over K. Then it is easy to see that $\{\alpha_i\beta_j\}$ is a basis of L over F (check details). $\square$

14.2. **Constructing field extensions.**

Let L/F be a field extension. For any subset S of L we can consider the field $F(S)$ = the smallest subfield of L containing both F and S. We have $F \subseteq F(S) \subseteq L$.

Definition. (a) A field extension K/F is called simple if K can be obtained from F by adjoining one element, that is, $K = F(\alpha)$ for some $\alpha \in K$. Note:

$$F(\alpha) = \{\beta \in K : \beta = \frac{p(\alpha)}{q(\alpha)} \text{ for some } p(x), q(x) \in F[x] \text{ with } q(\alpha) \neq 0.\}$$

(b) K/F is called finitely generated if K can be obtained from F by adjoining finitely mant elements, that is, $K = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in K$.

Proposition 14.2. *(a) Any finite extension is finitely generated.*
(b) Assume that K/F is finitely generated. Then there exist subfields $F = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = K$ s.t. K_i/K_{i-1} is simple for each i.

Proof. (a) Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K over F. Then $F(\alpha_1, \ldots, \alpha_n)$ contains $\sum_{i=1}^{n} \lambda_i \alpha_i$ for any $\lambda_i \in F$, and so $F(\alpha_1, \ldots, \alpha_n) = K$.
(b) Suppose that $K = F(\alpha_1, \ldots, \alpha_n)$, and define $K_i = F(\alpha_1, \ldots, \alpha_i)$ for $1 \le i \le n$. It is easy to see that $K_i(\alpha_{i+1}) = K_{i+1}$, so K_{i+1}/K_i is simple for each i. □

14.3. **Simple extensions.** Let K/F be a field extension. Given any $\alpha \in K$ let $V(\alpha) = \{f \in F[x] : f(\alpha) = 0\}$. Clearly $V(\alpha)$ is an ideal of $F[x]$. We have two cases.

Case 1: $V(\alpha) \neq \{0\}$. In this case α is called algebraic over F. The unique monic polynomial which generates $V(\alpha)$ as an ideal is called the minimal polynomial of α over F and denoted by $\mu_{\alpha,F}(x)$.

Case 2: $V(\alpha) = \{0\}$. In this case α is called transcendental over F.

Lemma 14.3. *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Let $p(x) \in F[x]$ be monic. The following are equivalent:*

(i) $p(x) = \mu_{\alpha,F}(x)$
(ii) $p(x)$ *is irreducible and* $p(\alpha) = 0$.

Proof. Exercise. □

Theorem 14.4. *Assume that $K = F(\alpha)$ for some α.*

(a) *If α is algebraic over F, then*
  (i) $K = F[\alpha] =$ *polynomials in α with coefficients from F*
  (ii) $K \cong F[x]/(\mu_\alpha(x))$
  (iii) *If $n = \deg \mu_\alpha(x)$, then $[K : F] = n$ and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of K over F.*
(b) *If α is transcendental over F, then $K \cong F(x)$, the field of rational functions over F in one variable.*

Proof. (a) Define the homomorphism $\varphi : F[x] \to K$ by $\varphi(p(x)) = p(\alpha)$. Then $\mathrm{Im}\varphi = F[\alpha]$ and $\mathrm{Ker}\,\varphi = (\mu_\alpha(x))$ (by definition). Therefore,

$$F[\alpha] \cong F[x]/(\mu_\alpha(x)).$$

Since $\mu_\alpha(x)$ is irreducible by Lemma 14.3, $F[\alpha]$ is a field. Thus, $F[\alpha]$ is a field containing F and α, so $F[\alpha] = F(\alpha)$ (as the inclusion $F[\alpha] \subseteq F(\alpha)$ always holds). This proves (i) and (ii). (iii) is left as an exercise.

(b) Define $\varphi : F(x) \to K$ by $\varphi\left(\frac{p(x)}{q(x)}\right) = \frac{p(\alpha)}{q(\alpha)}$. Note that φ is well defined since α is transcendental (so $q(\alpha) \neq 0$ if $q \neq 0$). This time φ is surjective by definition, and finally $\mathrm{Ker}\,\varphi = \{0\}$ again because α is transcendental. □

14.4. **Algebraic extensions.**

Definition. An extension K/F is called algebraic if any $\alpha \in K$ is algebraic over F.

Lemma 14.5. *Let K/F be a finitely generated extension. The following are equivalent:*

(a) *K/F is finite*
(b) *K/F is algebraic*
(c) *$K = F(\alpha_1, \ldots, \alpha_n)$ for some algebraic elements $\alpha_1, \ldots, \alpha_n$.*

Proof. "(a)⇒ (b)" Let $n = [K : F]$. Then for any $\alpha \in K$ the elements $1, \alpha, \ldots, \alpha^n$ are linearly dependent over F, so α is algebraic over F.

"(b)⇒ (c)" Since K/F is finitely generated, $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$, and since K/F is algebraic, each α_i must be algebraic over F.

"(c)⇒ (a)" Let $K_i = F(\alpha_1, \ldots, \alpha_i)$. Then $K_i = K_{i-1}(\alpha_i)$ for each i. Since α_i is algebraic over F, it is surely algebraic over K_{i-1}, so by Theorem 14.4 we have $[K_i : K_{i-1}] < \infty$. Hence

$$[K : F] = [K_n : K_0] = \prod_{i=1}^{n} [K_i : K_{i-1}] < \infty.$$

□