Lecture 3 : Algebraic Extensions II

Objectives

(1) Degree of a field extension and its multiplicative nature.
(2) A field extension of finite degree is algebraic.
(3) Transitivity of algebraic extensions.
(4) Compositum of two fields.

Key words and phrases: Simple field extension, degree of a field extension, compositum of fields.

Definition 3.1. *Let $F \subseteq K$ be a field extension. The dimension of the F-vector space K, denoted by $[K : F]$ is called the* **degree of the field extension** *K/F.*

For an algebraic element $\alpha \in K$, $\dim_F F(\alpha) = \deg \text{ irr}(\alpha, F)$. If $[K : F] < \infty$, then $F \subseteq K$ is called a **finite extension**.

Proposition 3.2. *A finite extension K/F is an algebraic extension.*

Proof. Let $[K : F] = n$ and $\beta \in K$. Then $1, \beta, \ldots, \beta^n$ are linearly dependent over F. Hence there exist $a_0, a_1, \ldots, a_n$, not all zero in F such that $a_0 + a_1\beta + \cdots + a_n\beta^n = 0$. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Then β is a root of $f(x)$. Hence β is algebraic over F.

□

Corollary 3.3. *Every irreducible polynomial over $\mathbb{R}$ has degree ≤ 2.*

Proof. Let $f(x) \in \mathbb{R}[x]$ be irreducible and $\alpha \in \mathbb{C}$ a root of $f(x)$. Then $\mathbb{R}[\alpha] \subseteq \mathbb{C}$. If $\alpha \in \mathbb{R}, \deg f(x) = 1$. If $\alpha \notin \mathbb{R}$, then $[\mathbb{R}[\alpha] : \mathbb{R}] \geq 2$. Thus $\mathbb{C} = \mathbb{R}[\alpha]$. Since $[\mathbb{C} : \mathbb{R}] = 2, \deg f(x) = 2$.

□

Example 3.4. (1) Since irr $(i, \mathbb{R}) = x^2 + 1, [\mathbb{C} : \mathbb{R}] = 2$ as $\mathbb{C} \simeq \mathbb{R}(i)$.

(2) Since irr $(\zeta_p, \mathbb{Q}) = x^{p-1} + x^{p-2} + \cdots + x + 1$, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

(3) Algebraic extension of a field may not be finite. Consider the chain of fields $\mathbb{Q} \subseteq \mathbb{Q}(2^{1/2}) \subseteq \cdots \subseteq \mathbb{Q}(2^{1/2^n}) \subseteq \cdots$. Their union K contains the algebraic numbers $\alpha_n = 2^{1/2^n}$ for all n and α_n is a root of the irreducible polynomial $f_n(x) = x^{2^n} - 2$. Hence $[K : \mathbb{Q}] \geq 2^n$ for all n. Thus $[K : \mathbb{Q}] = \infty$.

(4) **Quadratic Extensions:** If $[K : F] = 2$ then K is called a quadratic extension of F. Let $\alpha \in K \setminus F$ then $\{1, \alpha\}$ is a basis of K over F. Hence $\alpha^2 = a\alpha + b$ for some $a, b \in F$. Therefore $f(x) = \text{irr}(\alpha, F) = x^2 - ax - b$. The roots of $f(x)$ are $(a \pm \sqrt{a^2 + 4ab})/2$ if char F $\neq 2$. Therefore $K = F(\sqrt{a^2 + 4b})$.

Definition 3.5. *A chain of fields $F_1 \subset F_2 \subset \cdots \subset F_n$ is called a tower of fields if F_i is a subfield of F_{i+1}, for all $i = 1, 2, \ldots, n - 1$.*

Proposition 3.6. *If $K \subseteq F \subseteq L$ is a tower of fields then*

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

Proof. If either F/K or L/F are infinite dimensional, then L/K is also infinite dimensional. Thus we may assume that F/K and L/F are finite. Suppose that $[F : K] = m$ and $[L : F] = n$. Let $x_1, x_2, \ldots, x_n$ be a basis of L over F and $y_1, y_2, \ldots, y_m$ be a basis of F over K.

We claim that the set

$$B = \{x_j y_j \mid i = 1, 2, \ldots n, \text{ and } j = 1, 2, \ldots, m\}$$

is a vector space basis of L over K. Let $z \in L$. Thus $z = f_1 x_1 + \cdots + f_n x_n$, for some $f_1, \ldots, f_n \in F$. We write $f_i = \sum_{j=1}^{m} k_{ij} y_j$. Therefore

$$z = \sum_{l=1}^{n} x_l f_l = \sum_{l=1}^{n} \sum_{j=1}^{m} x_l k_{lj} y_j.$$

Thus B generates L as a K- vector space. Suppose $\sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} x_i y_j = 0$. Then

$$\sum_{i=1}^{n} \left[\sum_{j=1}^{m} a_{ij} y_j \right] x_i = 0.$$

Since $x_1 \ldots, x_n$ are F-linearly independent. Therefore $\sum_{j=1}^{n} a_{ij} y_j = 0$ for each i. By linear independence of $y_1, \ldots, y_n$ to see that all the $a_{ij} = 0$. $\square$

Corollary 3.7. *Let $F \subseteq K$ be a finite field extension. Then* $\deg irr(\alpha, F)$ *divides* $[K : F]$*, for all* $\alpha \in K$*.*

Proof. Since $F \subseteq F(\alpha) \subseteq K$, we have

$$[K : F] = [K : F(\alpha)][F(\alpha) : F].$$

Thus $\deg \mathrm{irr}(\alpha, F)$ divides $[K : F]$. □

Proposition 3.8. *Let K/F be a field extension. If $a_1, a_2, \ldots, a_n \in K$ are algebraic over F then $F(a_1, a_2, \ldots, a_n)$ is a finite algebraic extension of F.*

Proof. Since a_i is algebraic over F, it is algebraic over $F(a_1, a_2, \ldots, a_{i-1})$. Thus $[F(a_1, a_2, \ldots, a_i) : F(a_1, a_2, \ldots, a_{i-1})]$ is finite for all i. Therefore the field $F(a_1, a_2, \ldots, a_n)$ is a finite extension of F. Hence it is algebraic. □

Corollary 3.9. *Let E/F and K/E be algebraic extensions. Then K/F is an algebraic extension.*

Proof. Let $a \in K$ and let a be a root of $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in E[x]$. Consider the field $L = F(a_0, a_1, \ldots, a_{n-1})$. Then a is algebraic over L. Hence $L(a)$ is a finite extension of L. Since $a_0, a_1, \ldots, a_{n-1}$ are algebraic over F, L is a finite extension of F. Hence $L(a)$ is a finite extension of F. Hence a is algebraic over F. □

Corollary 3.10. *Let K/F be a field extension. Then the set of elements of K which are algebraic over F is a subfield of K.*

Proof. Let $a, b \in K$ be algebraic over F. Then $F(a, b)$ is a finite extension of F. Hence all elements of $F(a, b)$ are algebraic over F. In particular, $a \pm b, ab$ and a/b if $b \neq 0$, are all algebraic over F. □

Compositum of fields: Let L/k be a field extensions and E/k and F/k be intermediate field extensions. Then the smallest field containing E and F, to be denoted by EF, is called the **compositum of F and F**. Suppose $E = k(a_1, a_2, \ldots, a_n)$ and F is an extension of k. Then $EF = F(a_1, a_2, \ldots, a_n)$.

Example 3.11. Let m and n be co prime positive integers. Consider the subfields $E = \mathbb{Q}(\zeta_m)$ and $F = \mathbb{Q}(\zeta_n)$ of $\mathbb{C}$. Then the compositum of E and

F is $\mathbb{Q}(\zeta_{mn})$. Indeed, as m and n are coprime, there exist $p, q \in \mathbb{N}$ such that $mp + nq = 1$. Therefore

$$\zeta_{mn} = \exp(2\pi i/mn) = \exp(2p\pi i/n)\exp(2q\pi i/m) = (\zeta_n)^p(\zeta_m)^q.$$

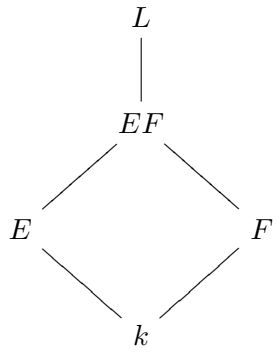
We can estimate the degree of the compositum of two finite field extensions in terms of their degrees.

Proposition 3.12. *Let L/k be a field extension and $E/k, F/k$ be intermediate finite extensions fields. Then*

$$[EF : k] \leq [E : k][F : k].$$

If $[E : k]$ and $[F : k]$ are coprime then equality holds.

Proof. Let $x_1, x_2, \ldots, x_m$ and $y_1, y_2, \ldots, y_n$ be bases of the k-vector spaces E and F respectively. Then it is easy to see that $E = k(x_1, x_2, \ldots, x_m)$ and $F = k(y_1, y_2, \ldots y_n)$. Therefore $EF = k(x_1, x_2, \ldots, x_m; y_1, y_2, \ldots y_n)$. We have the following diagram of field extensions:



Since $EF = E(y_1, y_2, \ldots, y_n)$ we have $[EF : F] \leq n$. Since the degree is multiplicative in a tower of finite extensions, we have

$$[EF : k] = [EF : E][E : k] \leq mn.$$

Since m and n both divide $[EF : k]$, and $(m, n) = 1$, we get $mn \mid [EF : k]$. Hence $[EF : k] = mn$. □