Lecture 2 : Algebraic Extensions I

Objectives

(1) Main examples of fields to be studied.
(2) The minimal polynomial of an algebraic element.
(3) Simple field extensions and their degree.

Key words and phrases: Number field, function field, algebraic element, transcendental element, irreducible polynomial of an algebraic element, algebraic extension.

The main examples of fields that we consider are :

(1) **Number fields:** A number field F is a subfield of $\mathbb{C}$. Any such field contains the field $\mathbb{Q}$ of rational numbers.

(2) **Finite fields :** If K is a finite field, we consider $\psi : \mathbb{Z} \to K, \psi(1) = 1$. Since K is finite, $\ker \psi \neq 0$, hence it is a prime ideal of $\mathbb{Z}$, say generated by a prime number p. Hence $\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ is isomorphic to a subfield of K. The finite field $\mathbb{F}_p$ is called the prime field of K.

(3) **Function fields:** Let x be an indeteminate and $\mathbb{C}(x)$ be the field of rational functions, i.e. it consists of $p(x)/q(x)$ where $p(x), q(x)$ are polynomials and $q(x) \neq 0$. Let $f(x, y) \in \mathbb{C}[x, y]$ be an irreducible polynomial. Suppose $f(x, y)$ is not a polynomial in x alone and write

$$f(x, y) = y^n + a_1(x)y^{n-1} + \cdots + a_n(x), a_i(x) \in \mathbb{C}[x].$$

By Gauss' lemma $f(x, y) \in \mathbb{C}(x)[y]$ is an irreducible polynomial. Thus $(f(x, y))$ is a maximal ideal of $\mathbb{C}(x)[y]/(f(x, y))$ is a field. K is called the function field of the curve defined by $f(x, y) = 0$ in $\mathbb{C}^2$.

Characteristic of a field : Let R be a commutative ring with identity e. Define the ring homomorphism $f : \mathbb{Z} \to R$ by $f(n) = ne$. Then $\ker f = (n)$ for some integer n. If $n = 0$, then $\mathbb{Z}$ is isomorphic to a subring of R. In this case we say that R **has characteristic zero.** If R is a domain then $\mathbb{Z}/(n)$ is a domain as it is isomorphic to a subring of R. Hence n is a prime number, say p. Therefore the finite field $\mathbb{F}_p$ is isomorphic to a subfield of R. In this

case, we say that R **has characteristic** p. Thus any field F contains either an isomorphic copy of $\mathbb{Q}$ or $\mathbb{F}_p$.

Definition 2.1. (i) *Let K be a subfield of a field F. We say F is an* **extension field of** K**.** *We also say that K is a base field. We also write this as F/K.*

(ii) *An element $a \in F$ is called* **algebraic over** K *if there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(a) = 0$. If every element of F is algebraic over K then we say that F is an* **algebraic extension** *of K.*

(iii) *An element $a \in F$ which is not algebraic over K is called a* **transcendental element** *over K.*

Example 2.2. It is known that the base e of the natural logarithm and π are transcendental over $\mathbb{Q}$. Since $(\pi i)^2 = -\pi^2, \pi i$ is a root of $x^2 - \pi^2 \in \mathbb{R}[x]$. Hence πi is algebraic over $\mathbb{R}$. However πi is not algebraic over $\mathbb{Q}$. Thus the property of being algebraic depends upon the base field.

Example 2.3. Let K be a finite field whose characteristic is a prime number p. Then K has a subfield F with p elements. Since K is finite, it is a finite dimensional F-vector space. If $\dim_F K = n$ then K has p^n elements. If $a \in K$ then the set $\{1, a, a^2, \ldots, a^n\}$ is linearly dependent. Let $b_0, b_1, \ldots, b_n \in F$, not all zero, so that $b_0 + b_1 a + \cdots + b_n a^n = 0$. Hence a is a root of the nonzero polynomial $b_0 + b_1 x + \cdots + b_n x^n$. Therefore b is algebraic over F and hence K/F is an algebraic extension.

Proposition 2.4. *Let F/K be a field extension and $\alpha \in F$ be algebraic over K. Then there exists a unique monic irreducible polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$.*

Proof. Define $\psi : K[x] \to F$ by $\psi(g(x)) = g(\alpha)$. Since ψ is a ring homomorphism and α is algebraic, $\ker \psi = I$ is a nonzero ideal of $K[x]$. Since $K[x]$ is a PID and $K[x]/I$ is isomorphic to a subfield of F, I is generated by an irreducible polynomial $h(x) \in K[x]$.. If $g(\alpha) = 0$ then $g(x) = h(x)h_1(x)$ for some polynomial $h_1(x) \in K[x]$. If g is irreducible, then $g = \alpha h(x)$ for some $\alpha \in K^\times = K \setminus \{0\}$. If g and h are taken to be monic, then $g = h$. $\square$

Definition 2.5. *The irreducible monic polynomial in $F[x]$ whose root is $\alpha \in K$ is denoted by $irr(\alpha, F)$ and it is called the* **irreducible monic polynomial of α over F.** *The degree of $irr\,(\alpha, F)$ is called the* **degree of α** *and it is written as $\deg_F \alpha$.*

Example 2.6. (i) $\sqrt{i} \in \mathbb{C}$ satisfies $f(x) = x^4 + 1 = 0$. Show that $f(x) = \text{irr}(\sqrt{i}, \mathbb{Q})$. Consider the field $\mathbb{Q}(i) =$ smallest field containing $\mathbb{Q}$ and i. Then irr $(\sqrt{i}, \mathbb{Q}(i)) = x^2 - i$.

(ii) Let p be a prime number and $\zeta_p = e^{2\pi i/p}$. Then $x^p - 1 = 0$ is satisfied by ζ_p. Since $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$ and $\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$, $\text{irr}(\zeta_p, \mathbb{Q}) = \Phi_p(x)$.

Simple field extensions: Let $K \subset F$ be a field extension. Let $\alpha, \beta \in F$ be transcendental. Define $\psi : K[x] \to F$ such that $\psi(g(x)) = g(\alpha)$. Then $\ker \psi = \{0\}$. Thus $K[x] \simeq K[\alpha]$ and hence $K(\alpha) \simeq K(\beta)$ by an isomorphism σ such that $\sigma(\alpha) = \beta$ and $\sigma|_K = id_K$. The situation is quite different for algebraic elements.

Proposition 2.7. *Let $F \subset K$ be a field extension and $\alpha \in K$ be algebraic over F and $f(x) = irr\,(\alpha, F)$. Let $n = \deg f$. Then*

(i) $F[\alpha] = F(\alpha) \simeq F[x]/(f(x))$. (ii) $\dim_F F(\alpha) = n$ *and* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *is an F- basis of $F(\alpha)$.*

Proof. Consider the substitution homomorphism

$$\psi : F[x] \to F[\alpha] \text{ such that } \psi(x) = \alpha, \;\; \psi|_F = id_F$$

Then $ker\psi = (f(x))$ where $f(x) = irr(\alpha, F)$. Hence $F[x]/(f(x)) \simeq F[\alpha]$.
since $(f(x))$ is a maximal ideal, $F[\alpha]$ is a field, so $F[\alpha] = F(\alpha)$.

(ii) Let $g(\alpha) \in F[\alpha]$ and $g(x) = f(x)q(x) + r(x)$ where $q, r \in F[x]$, and $\deg r(x) < degf(x)$ or $r(x) = 0$. Then $g(\alpha) = r(\alpha)$. Thus $F[\alpha]$ is an $F-$vector space generated by $1, \alpha, \ldots, \alpha^{n-1}$ where $n = \deg f(x)$. Suppose that $\sum_{i=0}^{n-1} a_i \alpha^i = 0$. If a_i are not all zero then $\sum_{i=0}^{n-1} a_i x^i$ is a nonzero polynomial of degree less than $\deg f(x)$ satisfied by α. This contradicts minimality of $\deg f(x)$. Thus $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an F- vector space basis of $F[\alpha]$. Hence $\dim_F F[\alpha] = \deg$ irr (α, F).

□

Proposition 2.8. *Let K/F be a field extension and $\alpha \in K$ be algebraic over F. Then $F(\alpha)/F$ is an algebraic extension.*

Proof. If $\beta \in F(\alpha)$ and $\beta \neq 0$ then $\{1, \beta, \beta^2, \ldots, \beta^n\}$ is a linearly dependent subset of $F(\alpha)$ since $\dim_F F(\alpha) = n$. Hence there exist $a_0, a_1, \ldots, a_n \in F$ not all zero so that $a_0 + a_1\beta + \cdots + a_n\beta^n = 0$. Hence β is algebraic. Therefore $F(\alpha)/F$ is an algebraic extension. □

Proposition 2.9. *Let $\alpha, \beta \in K \supseteq F$ be algebraic over F. Then there exists an F-isomorphism $\psi : F(\alpha) \to F(\beta)$ such that $\psi(\alpha) = \beta$ if and only if irr $(\alpha, F) =$ irr (β, F).*

Proof. Let $f(x) =$ irr (α, F) and $g(x) =$ irr (β, F). Then $\psi(f(\alpha)) = f(\beta) = 0$. Thus $g(x)|f(x)$. Since g, f are monic and irreducible, $g(x) = f(x)$.

Conversely, suppose irr $(\alpha, F) =$ irr (β, F). Then $F(\alpha) \simeq F[x]/(f(x)) \simeq F(\beta)$ and the isomorphisms are F-isomorphisms. Hence $F(\alpha)$ and $F(\beta)$ are F-isomorphic. □

Proposition 2.10. *Let $F \subseteq K, K'$ be two field extensions of F. Let $\psi : K \to K'$ be an F- isomorphism. Let $\alpha \in K$ be a root of $f(x) \in F[x]$. Then $\psi(\alpha)$ is a root of $f(x)$.*

Proof. $\psi(f(\alpha)) = f(\psi(\alpha)) = 0$ □

Example 2.11. (i) Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. By Eisenstein's criterion $f(x)$ is irreducible over $\mathbb{Q}$. The roots of $f(x)$ are $\alpha, \alpha w, \alpha w^2$ where α is the real cube root of 2 and w is the complex cube root of 1. Thus the fields $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha w)$, $\mathbb{Q}(\alpha w^2)$ are $\mathbb{Q}-$isomorphic.

(ii) Since irr $(i, \mathbb{R}) = x^2 + 1$, $\mathbb{R}[x]/(x^2 + 1) = \mathbb{R}(i) = \mathbb{C}$.

(iii) The polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$. Hence $K = \mathbb{F}_2[x]/(f(x))$ is a field which is a two dimensional $\mathbb{F}_2-$vector space. Hence K is a field with four elements.

(iv) The polynomial $g(x, y) = y^3 - x(x + 1)(x - 1)$ is irreducible in $\mathbb{C}(x)[y]$ by Eisenstein's criterion. Hence $\mathbb{C}(x)[y]/(g(x, y))$ is a simple field extension of the function field $\mathbb{C}(x)$.