FMCS:Math/April 15h, 2014

Lecture 2

2 Field Extension

2.1 Extension

- What is a field extension K/k ?
- Extension K/k is finite if K is of finite dimensional as a vector space over k.
- **Example :** $\mathbb{C}/\mathbb{R}$ finite, $\mathbb{R}/\mathbb{Q}$ not finite.
- Simple extension $k(\alpha)$: The smallest subfield of K containing k and $\alpha \in K$.
- **Example :** $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\,;\, a, b \in \mathbb{Q}\}$.

  Proof. $\supset$ is obvious. To see $\subset$, show that the right hand side is a field. $\square$

- Multiple extension $k(\alpha_1, \alpha_2, \cdots, \alpha_n)$: $k(\alpha_1, \alpha_2, \cdots, \alpha_{n-1})(\alpha_n)$ inductively.
- **Example :** $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

  Proof. $\supset$ is obvious. To see $\subset$, we let $\alpha = \sqrt{2} + \sqrt{3}$, then $\sqrt{2} = \dfrac{\alpha^2 - 1}{2\alpha}$ and $\sqrt{3} = \dfrac{\alpha^2 + 1}{2\alpha}$. $\square$

- Algebraic versus Transcendental : $\alpha \in K$ is algebraic over k if $1, \alpha, \alpha^2, \cdots, \alpha^n$ are linearly dependent over k for some n, and transcendental otherwise.
- The set of algebraic numbers over $\mathbb{Q}$ is countable (Homework 1). Thus there are uncountably many transcendental numbers over $\mathbb{Q}$ in $\mathbb{C}$.

2.2 Algebraic Extension

- Another formulation of algebraicity : α is algebraic if the evaluation map $\varphi_\alpha : k[X] \to K$ defined by $\varphi_\alpha(f) = f(\alpha)$ has nontrivial kernel.
- The kernel of φ_α is generated by a single polynomial $p(X)$ since $k[X]$ is a principal ideal domain.

- The homomorphism theorem implies

$$k[X]/(p(X)) \simeq k[\alpha],$$

and since $k[\alpha]$ is an integral domain, $p(X)$ is irreducible over k.

- The irreducible polynomial (minimal polynomial) $\mathrm{Irr}_k(\alpha)$ of $\alpha \in K$: a monic (the leading coefficient is 1) polynomial generating $\mathrm{Ker}\,\varphi_\alpha$.

- **Example :** If $k = \mathbb{Q}$, $\alpha = \sqrt[n]{2}$, then $\mathrm{Irr}_k(\alpha) = X^n - 2$.

  Proof. Use Eisenstein's Criterion (see Homework 6) ! □

- **Example :** If $k = \mathbb{Q}(\sqrt{2})$, $\alpha = \sqrt[4]{2}$, then $\mathrm{Irr}_k(\alpha) = X^2 - \sqrt{2}$.

- Algebraic extension K/k : If any element $\alpha \in K$ is algebraic over k.

- **Proposition 2.2.1 :** If K/k is a finite extension, then K is algebraic over k.

  Proof. If the dimension of K as a k vector space is n, then $1, \alpha, \alpha^2, \cdots, \alpha^n$ cannot be linearly independent for any nonzero $\alpha \in K$. □

- **Remark :** The converse is not true. For example, the set of all algebraic numbers over $\mathbb{Q}$ turns out to be a field (Homework 7) and an infinite algebraic extension over $\mathbb{Q}$.

- Degree of extension $[K : k]$: Dimension of K as a k vector space. It is either a positive integer or ∞.

- **Proposition 2.2.2 :** Let K/k and L/K be field extensions. Then, L is an extension of k and

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

  Proof. The first statement is routine to check. To see the identity, choose a basis $\{x_i \in L\,;\, i \in I\}$ of L over K and a basis $\{y_j \in K\,;\, j \in J\}$ of K over k, and show that $\{x_i y_j\,;\, i \in I,\, j \in J\}$ forms a basis of L over k. □

- **Corollary 2.2.3 :** L/k is finite if and only if both L/K and K/k are finite.

- **Proposition 2.2.4 :** Let $\alpha \in K$ be algebraic over k. Then $k[\alpha] = k(\alpha)$, and $k(\alpha)$ is finite over k. The degree $[k(\alpha), k]$ is equal to the degree of $\mathrm{Irr}_k(\alpha)$.

Proof. Let $p(X)$ denote $\mathrm{Irr}_k(\alpha)$ and $f(X) \in k[X]$ such that $f(\alpha) \neq 0$. Then since $(p, f) = 1$, there exist $g,\ h \in k[X]$ such that

$$g \cdot p + h \cdot f = 1.$$

This implies that f is invertible in $k[\alpha]$, and hence $k[\alpha] = k(\alpha)$.

The rest is to show that $\{1, \alpha, \cdots, \alpha^{\deg p - 1}\}$ forms a basis of $k(\alpha)$.

Suppose that $1, \alpha, \cdots, \alpha^{\deg p-1}$ are not linearly independent, then there is a polynomial g of degree $\leq \deg p - 1$ such that $g(\alpha) = 0$. This contradicts to the irreducibility of $p(X)$.

Choose $f(\alpha) \in k(\alpha)$ where $f \in k[X]$. Then there are unique polynomials $q, r \in k[X]$ with $\deg r(X) < \deg p(X)$ such that

$$f(X) = q(X)p(X) + r(X),$$

and $f(\alpha) = r(\alpha)$. Thus $1, \alpha, \cdots, \alpha^{\deg p-1}$ generate $k(\alpha)$. □

2.3 Algebraic Closure

- Algebraically closed field K : If every polynomial in $K[X]$ of degree ≥ 1 has a root in K.

- **Example :** By the fundamental theorem of algebra, $\mathbb{C}$ is algebraically closed.

- **Theorem 2.3.1 :** Let k be a field. Then there exits an algebraic extension K^{alg} which is algebraically closed (called algebraic closure of k). K^{alg} is unique up to isomorphism inducing the identity on k.

  Proof. See some textbook, for example, S. Lang; Algebra, GTM Springer, 2002. □

- **Example :** The algebraic closure of $\mathbb{R}$ is $\mathbb{C}$.

- **Example :** The algebraic closure of $\mathbb{Q}$ is the field of algebraic numbers.

2.4 Homework

1. Show that the set of algebraic numbers over $\mathbb{Q}$ is countable.

2. Show that π and e are transcendental over $\mathbb{Q}$.

3. Let α be a root of the equation

$$X^3 + X^2 + X + 2 = 0.$$

Express $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ and $(\alpha - 1)^{-1}$ in $\mathbb{Q}(\alpha)$ in the form

$$a\alpha^2 + b\alpha + c$$

with $a, b, c \in \mathbb{Q}$.

4. Suppose α is algebraic over k of odd degree. Show that $K(\alpha) = k(\alpha^2)$.

5. Show that $\sqrt{2} + \sqrt{3}$ is algebraic of degree 4 over $\mathbb{Q}$.

6. Prove **Eisenstein's criterion :** Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ be a polynomial of integer coefficients. If there exists a prime p such that

   (1) p divides each a_j for $j \neq n$,

   (2) p does not divide a_n, and

   (3) p^2 does not divide a_0,

   then $f(X)$ is irreducible over $\mathbb{Q}$.

7. Show that the set of algebraic numbers over $\mathbb{Q}$ forms a field.