Lecture Notes

2009.5.21

Field Extensions

Definition. A *field* is a set K with two operations $+, \cdot$ such that $(K, +), (K^*, \cdot)$ are abelian groups and $a(b+c) = ab + ac, (b+c)a = ba + ca$ for $a, b, c \in K$, where $K^* = K - 0$.

Example 1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field. $\mathbb{Z}_{|}$ is a field, where p is a prime number.

Example 2. $F_4 = 0, 1, a, 1 + a$ is a field under $+, \cdot$ defined as following tables.

$+$	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

$\cdot$	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

Example 3. Suppose F is a field, then

$$F[x] = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid a_i \in F, a_n \neq 0\}$$

is the set of polynomials over F ($F[x]$ is not a field), and

$$F(x) = \{f(x)/g(x) \mid f(x), g(x) \in F[x], g(x) \neq 0\}$$

is the smallest field containg F and x.

Example 4. Let $F = \mathbb{Z}_p$ and $p(x) \in F[x]$ *irreducible* of degree n (degree of a polynomial is denoted by $\deg p(x)$), then

$$F_{p^n} = \mathbb{Z}_p[x]/\langle p(x)\rangle = \{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \mid a_i \in \mathbb{Z}_p\}$$

is a field of order p^n , with usually addition and mutiplication is modulo $p(x)$.

Definition. If $K \subseteq F$ are fields with the same operations, then F is said to be an *extension field* of K.

NOTE

(a) If F is an *extension field* of a field K, then F is also a *vector space over* K. In this case, we denote the dimension of the vector space by $[F : K]$.

(b) If $K \subseteq F \subseteq E$, then E is a vector space over K and

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

(c) If $K \subseteq F$, $\alpha \in F$, and $p(x) \in K[x]$ with $\deg p(x) = n$ is an irreducible polynomial and $p(\alpha) = 0$, then

$$K(\alpha) = K[\alpha] = \left\{ \sum_{0 \leq i \leq n-1} a_i\alpha_i \middle| a_i \in K \right\}$$

$K(\alpha)$ is the smallest field contain K and α. $[K(\alpha) : K] = n$, $\{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}\}$ is a basis of $K(\alpha)$ over K. Then α is said to be *algebraic* over K.

Definition. Let F be an extension field of K. An element of α of F is said to be *transcendental* over K if α is not algebraic over K.

If α is transcendental over K, then i)$K(\alpha) \neq K[\alpha]$, ii)$K(\alpha) \cong K[x]$ by sending α to x, iii)$[K(\alpha) : K] = \infty$. If F is an extension field of K and $\alpha, \beta \in F$

(a) $K[\alpha, \beta] = \{f(\alpha, \beta) \mid f(x, y) \in K[x, y]\}$

(b) $K(\alpha, \beta) = \{f(\alpha, \beta)/g(\alpha, \beta) \mid f(x, y), g(x, y) \in K[x, y]$ with $g(\alpha, \beta) \neq 0\}$

(c) If α, β are algebraic numbers over K, the $K[\alpha, \beta] = K(\alpha, \beta)$.