# Week 6(II)

## Extension Fields

**Defn.** A field $E$ is an extension field of a field $F$ if $F \leq E$, i.e., $F \subseteq E$ and $< F, +, \cdot >, < E, +.\cdot >$ are fields.

**Theorem** (Kronecker)

Let $F$ be a field and $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field $E$ of $F$ and an $\alpha \in E$ such that $f(\alpha) = 0$.

**Proof.** 這個證明的概念可分成三個步驟：

**step 1.** 找一個不分解的非常數項多項式 $p(x) \mid f(x)$.

**step 2.** 利用 Homomorphism $\varphi : F \to F[x]/ < p(x) >$ 把 $F$ 看成是 $F[x]/ < p(x) >$ 的一個 subfield：$\{a+ < p(x) > | \ a \in F\}$.

**step 3.** 於是 $E$ 就是所求的 $F[x]/ < p(x) >$, 而在 $E$ 中令 $x+ < p(x) >= \alpha$, $\alpha$ 爲所求.

**check** 令 $f(x) = p(x)q(x)$, 則 $f(\alpha) = p(\alpha)q(\alpha) =< p(x) >$.

**Example** Let $F = \mathbb{R}$, and let $f(x) = x^2 + 1$. Since $x^2 + 1$ is irreducible over $\mathbb{R}$, $\mathbb{R}[x]/ < x^2 + 1 >$ is a field with $\alpha = x+ < x^2 + 1 >$ a zero of $f(x)$. We may identify $\mathbb{R}[x]/ < x^2 + 1 >$ with the set of complex numbers, more precisely $\alpha \Rightarrow i$ or $-i$ in $\mathbb{C}$.

**Defn.** (Algebraic and Transcendental Elements)

An element $\alpha$ of an extension field $E$ of $F$ is algebraic over $F$ if $f(\alpha) = 0$ for some nonzero $f(x) \in F[x]$. If $\alpha$ is not algebraic over $F$, then $\alpha$ is transcendental over $F$.

**Example** $\mathbb{C}$ is an extension field of $\mathbb{Q}$.

$\sqrt{2}$ is algebraic over $\mathbb{Q}$, so are $\sqrt{3}$, $\sqrt[3]{5}$ and $i$ . (It is not easy to prove that both $\pi$ and $e$ are transcendental over $\mathbb{Q}$.)

**Example** $\pi$ is algebraic over "$\mathbb{R}$", so is $e$.

**Defn.** (Algebraic number and Transcendental number)

An element of $\mathbb{C}$ that is algebraic (transcendental) over $\mathbb{Q}$ is an algebraic (transcendental) number.

**Theorem** Let $E \geq F$ and $\alpha \in E$. Then $\alpha$ is transcendental over $F$ if and only if the evaluation homomorphism $\varphi_\alpha : F[x] \to E$ is 1-1.
$(\varphi_\alpha(f(x)) = f(\alpha))$

**Proof.**($\Rightarrow$) $\forall$ $f(x) \in Ker\varphi_\alpha$, $f(\alpha) = 0$.

Since $\alpha$ is transcendental over $F$, $f(x)$ must be a constant polynomial, in fact it is 0. This concludes the proof.
($\Leftarrow$) Since $\varphi_\alpha$ is 1-1, $Ker(\varphi_\alpha) = \{0\}$, i.e., the only $f(x) \in F[x]$ such that $f(\alpha) = 0$ is the constant polynomail 0. This implies that $\alpha$ is transcendental over $F$. ■

**Theorem** 1. $E \geq F$, 2. $\alpha \in E$ and $\alpha$ is algebraic over $F$.
$\Rightarrow \exists$ an irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.
Moreover, if $f(\alpha) = 0$ for $f(x) \in F[x]$, then $p(x) \mid f(x)$.

**Proof.** Consider the homomorphism $\varphi_\alpha : F[x] \to E$. Then $Ker\varphi_\alpha$ is an ideal of $F[x]$, thus $Ker\varphi_\alpha$ is a principal ideal generated by a polynomial $p(x) \in F[x]$. Since $p(x) \in Ker\varphi_\alpha$, $p(\alpha) = 0$. Now, if $f(\alpha) = 0$ for $f(x) \in F[x]$, then $f(x) \in < p(x) >$ $(f(x) \in Ker\varphi_\alpha)$ and thus $p(x) \mid f(x)$. ■

**Defn.** A monic polynomial in $F[x]$ is a polynomial where coefficient of the highest degree term is "1".

**Defn.** 1. $E \geq F$, 2. $\alpha \in E$ and 3. $\alpha$ is algebraic over $F$.
$\Rightarrow$ The unique monic polynomial $p(x)$ mentioned above is called the irreducible polynomial for $\alpha$ over $F$ and denoted by $p(x) = irr(\alpha, F)$, the degree of $irr(\alpha, F)$ is the degree of $\alpha$ over $F$, denoted by $deg(\alpha, F)$.

**Example** $irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2$; $irr(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$.
$irr(\sqrt{1+\sqrt{5}}, \mathbb{Q}) = x^4 - 2x^2 - 2$. (Thm 23.14 Eisenstein's method!)
$x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$. (?)

$(*)$ "The degree of $\alpha$" does not make sense! We have to say the degree of $\alpha$ over $\mathbb{Q}$.
更多的例子.(Ex.)

**Simple Extension**

假設$E \geq F$, $\alpha \in E$ 同時 $\varphi_\alpha$ 爲由 $F[x]$ 對應至 $E$ 的 Homomorphism. 這裡的 $\varphi_\alpha$ 是估值的 Homo. (Evaluation)

**Case 1.** $\alpha$ is algebraic over $F$.

Then $Ker\varphi_\alpha =< irr(\alpha, F) >=< p(x) >$ is a maximal ideal of $F[x]$. Hence $F[x]/ < p(x) >$ is a field and $F[x]/ < p(x) >$ is isomorphic to a subfield of $\varphi_\alpha[F[x]]$ of $E$. This subfield $\varphi_\alpha[F[x]]$ is the smallest subfield of $E$ containing $\alpha$ and $F$, denoted by $F(\alpha)$.

**Case 2.** $\alpha$ is transcendental over $F$.

Then $Ker\varphi_\alpha = \{0\}$ and therefore $\varphi_\alpha$ is 1-1. This implies that $\varphi_\alpha[F[x]]$ is isomorphic to a subdomain of $E$. ($\varphi_\alpha : F[x] \to E$ is 1-1.) $E$ contains a field of quotients of $F[\alpha]$, which is also the smallest field containing $\alpha$ and $F$, denoted by $F(\alpha)$.

**Simple extension** An extension field $E$ of $F$ is a simple extension of $F$ if $E = F(\alpha)$ for some $\alpha \in E$.

**Simple extension** 的特性

$E = F(\alpha)$ and $irr(\alpha, F) = p(x)$ ($\alpha$ is algebraic over $F$) where $deg(p(x)) = n$. Then $\forall\ \beta \in E$, $\beta = \sum_{i=0}^{n-1} b_i \alpha^i$, 而且表示法唯一.

$(*)$ $E$ 中的元素可以用 $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ 的線性組合表示出來.

**Proof.** 因爲

$irr(\alpha, F) = p(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$, 所以

$p(\alpha) = 0$, 亦即 $\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \cdots - a_1\alpha - a_0 ...(1)$

現在看 $E$ 中的元素 $\beta$, 因爲 $E = F(\alpha) \leq \varphi_\alpha[F[x]],\ \beta = g(\alpha)$, where

$deg(g(x)) = m$. 假如 $m \leq n-1$, 則沒有什麼可以證明; 如果 $m > n$, 則利用

(1), 可以把 $\beta$ 表成 degree 不大於 $n-1$ 的形式.

另外, 唯一性的證明可以假設 $\beta = \sum_{i=0}^{n-1} b_i\alpha^i = \sum_{i=0}^{n-1} b_i'\alpha^i$. 因此

$\sum_{i=0}^{n-1}(b_i - b_i')\alpha^i = 0$. 如果有一個 $i,\ b_i \neq b_i'$, 則與 $irr(\alpha, F)$ 的定義矛盾 (?),

所以 $b_i = b_i'\ \ \forall\ \ i = 0, 1, 2, \cdots, n-1$. ■

現在, 再回顧 $\mathbb{R}[x]/ < x^2 + 1 >$, 由於 $p(x) = x^2 + 1$ 的次數是 2, 所以

$\mathbb{R}[x]/ < x^2 + 1 >$ 中的元素可以用 $b_0 + b_1\alpha$ 來表示, 其中 $b_0, b_1 \in \mathbb{R}$,

$\alpha = x + < p(x) >$, 對應於 $\mathbb{C}$ 中的 $i$. (註 : $\mathbb{R}[x]/ < x^2 + 1 >= \mathbb{R}(\alpha)$.)

- 如果我們對於自己的前程失去了熱情, 那麼, 註定你 (妳) 的一生要漂泊四方, 經常是一事無成.
- 學會代數可能不具有太大意義; 學會不被面對的事物阻礙自己向前的動力, 才是最重要的試鍊.
- "放棄"絕對比"繼續"要容易許多.