Week 7(II)

Defn. (Vector Space)

Let F be a field. A vector space over F (or F - vector space) consists of an abelian group V under addition together with an operation of scalar multiplication $\varphi : F \times V \to V$ defined by $\varphi(a, \alpha) = a\alpha$ where $a \in F$ and $\alpha \in V$. Also, the followung properties hold.

1. $a(b\alpha) = (ab)\alpha$ where $a, b \in F$ and $\alpha \in V$.
2. $(a + b)\alpha = a\alpha + b\alpha$.
3. $a(\alpha + \beta) = a\alpha + a\beta$ where $\alpha, \beta \in V$
4. $1\alpha = \alpha$

The elements of V are vectors and elements of F are scalars. A vector spaces over F may be called a vector space if F is fixed and it is also called a linear space.

Example If $E \geq F$, then E can be consider as a vector space over F.

Example For any field F, $F[x]$ is a vector space over F.

Example $\mathbb{Z}_2[x]$ is a vector space over $GF(2)$.

Defn. Let V be a vector space over F. The vectors in $S = \{\alpha_i \mid i \in I\}$ of V span(or generate) V if $\forall\ \beta \in V$, $\beta = \sum_{j=1}^{n} a_j \alpha_{i_j}$ where $i_j \in I$. $\sum_{j=1}^{n} a_j \alpha_{i_j}$ is a linear combination of $\{\alpha_{i_j}\}$.

Defn. (Linearly independent over F) (自己寫)

Defn. (Linearly dependent)

Defn. (Basis)

Defn. (Dimension)

Theorem $E \geq F$ and $\alpha \in E$ ia algebraic over F. If $deg(\alpha, F) = n$, then $F(\alpha)$ is an $n-$dimensional vector space over F with basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. Furthermore, $\forall\ \beta \in F(\alpha)$ is algebraic over F, and $deg(\beta, F) \leq deg(\alpha, F)$

Proof. It suffices to prove the second part.

Consider $1, \beta, \beta^2, \cdots, \beta^n$. Then, it is a dependent set since $dim(F(\alpha)) = n$. Therefore $irr(\beta, F) \leq n$. ■

Finite Extension and Algebraic Extension

Defn. An extension E of a field F is an algebraic extension of F if $\forall$ $\alpha \in E$, α is algebraic over F.

Defn. An extension E of a field F is a finite extension of degree n over F if E is an $n-$dimensional vector space over F, denoted by $[E : F] = n$.

Example $[E : F] = 1$ iff $E = F$. $[\mathbb{C} : \mathbb{R}] = 2$.

Theorem A finite extension field E of F is an algebraic extension of F.

Proof. Let $[E:F]=n$. $\forall\ \alpha\in E$, consider $1,\alpha,\alpha^2,\cdots,\alpha^n$. Since $[E:F]=n$, $\exists\ a_i$, $i=0,1,\cdots,n$ such that $\sum_{i=0}^{n}a_i\alpha^i=0$ where not all a_i are zeros. Therefore, by letting $f(x)=a_0+a_1x+\cdots+a_nx^n$, we have a nonzero poly. in $F[x]$ such that $f(\alpha)=0$. ■

Theorem (very important) If K is a finite extension of E and E is a finite extension of F, then $[K:F]=[K:E][E:F]$.

令 E over F 的 basis 爲 $\{\alpha_i\mid i=1,2,\cdots,n\}$.

令 K over E 的 basis 爲 $\{\beta_j\mid j=1,2,\cdots,m\}$.

我們證明 $\{\alpha_i\beta_j\mid i=1,2,\cdots,n;j=1,2,\cdots,m\}$ 爲 K over F 的基底.

1. Span

   $\forall\ \ \gamma\in K,\ \ \gamma=\sum_{j=1}^{m}b_j\beta_j$,

   又 $b_j=\sum_{i=1}^{n}a_{i_j}\alpha_i$, 所以 $\gamma=\sum_{i,j}a_{i,j}(\alpha_i\beta_j)$.

2. Independent

   令 $\sum_{i,j}a_{i,j}(\alpha_i\beta_j)=0$

   則 $\sum_{j=1}^{m}(\sum_{i=1}^{n}a_{i,j}\alpha_i)\beta_j=0$

   $\Rightarrow\ \ a_{i,j}=0$ ■

推論 $\forall\ \ i=1,2,\cdots,\gamma,\ \ F_{i+1}$ 爲 F_i 的 finite extension field.

$\Rightarrow [F_{\gamma+1}:F_1]=[F_{\gamma+1}:F_r][F_r:F_{r-1}]\cdots[F_2:F_1]$..

推論 If $E\geq F$ and $\alpha\in E$ is algebraic over F, and $\beta\in F(\alpha)$, then $deg(\beta,F)\mid deg(\alpha,F)$ for each $\beta\in F(\alpha)$.

Proof. (自己證明)

Example $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{3})]=2,\ \ [\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2.$$

$$\Uparrow$$

$$irr(\sqrt{2}+\sqrt{3},\ Q(\sqrt{3}))=(x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}-\sqrt{3})=$$

$$(x-\sqrt{3}-\sqrt{2})(x-\sqrt{3}+\sqrt{2})=(x-\sqrt{3})^2-2=x^2-2\sqrt{3}x+1.$$

$F(\alpha_1)$ is the smallest extension field of F in E that contains α_1. $(F(\alpha_1))(\alpha_2)$ is the smallest extension field of $F(\alpha_1)$ in E that contains α_2, and thus the smallest extension field of F in E contains α_1 and α_2.

$$\Downarrow$$

$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ is the smallest extension field of F in E that contains all $\alpha_i,\ \ i=1,2,\cdots,n$

Defn. $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ is obtained from F by adjoining to F the elements α_i in E.

Example $[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}]=6$

Basis=$\{1,\sqrt{2},\sqrt[3]{2},2^{\frac{5}{6}},2^{\frac{2}{3}},2^{\frac{6}{7}}\}$.

$[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt[3]{2})]=2.\quad [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3.$

Note : $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})=\mathbb{Q}(\sqrt[6]{2})$.

Theorem Let E be an algebraic extension of F. Then, there exists finite number of elements $\alpha_1,\alpha_2,\cdots,\alpha_n\in E$ such that
$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ if and only if E is a finite extension of F.

Proof.($\Rightarrow$) Since $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ is an algebraic extension of F, each element α_i of E is algebraic over F. Hence, $F(\alpha_1, \alpha_2, \cdots, \alpha_j)$ is algebraic over $F(\alpha_1, \alpha_2, \cdots, \alpha_{j-1})$. Thus
$[F(\alpha_1, \alpha_2, \cdots, \alpha_j) : F(\alpha_1, \alpha_2, \cdots, \alpha_{j-1})]$ is finite. This implies that
$[E : F]$ is finite.
($\Leftarrow$) If $[E : F] = 1$, then $E = F$. The proof follows. Otherwise $E \neq F$, let $\alpha_1 \in E \backslash F$. Then $[F(\alpha_1) : F] > 1$. Since $E \geq F(\alpha_1)$, $[F(\alpha_1) : F]$ is finite. Now, if $E = F(\alpha_1)$, then we are done. Otherwise, the process continues to $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ since E is a finite extension of F. (每多接一個 α_i, 維數佈於 F 就會增加) ■

Note If α and β in E are algebraic over F, then so are $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$ and $\frac{\alpha}{\beta}$ where $\beta \neq 0$.

Proof. $F(\alpha, \beta)$ is a finite extension of F !

Defn. (Algebraic Closures)

Let E be an extension foeld of F.

Then $\overline{F}_E = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$ is a subfield of E (待證明), $\overline{F}_E$ is called the algebraic closure of F in E.

Proof. $[F(\alpha, \beta) : F]$ is finite. $\Rightarrow F(\alpha, \beta) \leq \overline{F}_E$, thus we have the proof. ■

Corollary The set of all algebraic numbers forms a field.

Proof. The set of all algebraic numbers is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. (By definition) ■

Defn. (Algebraically closed)

A field F is algebraically closed if every nonconstant polynomial in $F[x]$ has a zero in F.

Example $\mathbb{C}$ is algebraically closed.

Theorem A field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ factors in $F[x]$ onto linear factors.

Proof. Since every $f(x)$ has a zero a in F, $f(x) = f_1(x)(x-a)$. The process continues. ■

$(*)$ An algebraically closed field F has no proper algebraic extensions, i.e., no algebraic extensions E with $F < E$. (再也無法擴展上去了!)

Proof. Let E be an algebraic extension of F. Then for each $\alpha \in E$, $irr(\alpha, F) = x - \alpha \in F[x]$. Hence $\alpha \in F$. ■

$(*)$**Theorem** Every field has an algebraic closure.

Proof. (在此省略, 利用 Zorn's Lemma, P.290)

Theorem (Fundamental Theorem of Algebra)

The field $\mathbb{C}$ of complex numbers is an algebraically closed field.

Proof. 參考 p.288. (複變的概念)