大學基礎代數

李華介

國立台灣師範大學數學系

Chapter 9

初級 Field 的性質

這一章中我們介紹一些 field 的基本性質. 由於很多有關於 field 的性質可以用線性代數的觀點得到, 所以我們也會簡單的複習一下線性代數的基本概念.

9.1. Field 的基本性質

這一節中我們首先介紹一些直接由定義得到的 field 的性質.

回顧一下一個 field 是一個 commutative ring with 1 而且其中非 0 的元素都是 unit. 也就是若 F 是一個 field, 則 F 中的 $+$ 和 $\cdot$ 需滿足 Definition 5.1.1 中 (R1) 到 (R8) 的性質, 另外需有:

- 對任意 $a, b \in F$ 皆滿足 $a \cdot b = b \cdot a$.
- 存在 $1 \in F$ 使得對任意 $a \in F$ 皆滿足 $a \cdot 1 = 1 \cdot a = a$.
- 對任意 $a \in F$ 且 $a \neq 0$, 皆存在 $a^{-1} \in F$ 使得 $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

前兩項是要求 F 是一個 commutative ring with 1; 最後一項是要求 F 中不為 0 的元素都是 unit.

很快的利用以上的定義我們可以得到以下有關 field 簡單但重要的性質.

Lemma 9.1.1. 若 F 是一個 *field,* 則 F 是一個 *integral domain.*

Proof. 由 field 的定義已知 F 是一個 commutative ring with 1, 所以我們只要證明 F 中沒有 zero-divisor 即可. 這可有由 Lemma 5.3.7 馬上得知, 不過為了完整性我們再給一次證明.

若 $a \in F$ 是 F 中的一個 zero-divisor, 即 $a \neq 0$ 且存在 $b \neq 0$ 滿足 $a \cdot b = 0$. 然而由 $b \neq 0$ 知 b 是 F 中的 unit, 故知存在 $b^{-1} \in F$ 滿足 $b \cdot b^{-1} = 1$. 因此可得

$$0 = (a \cdot b) \cdot b^{-1} = a \cdot (b \cdot b^{-1}) = a \cdot 1 = a.$$

此和 $a \neq 0$ 的假設相矛盾, 故 a 不可能是 F 中的 zero-divisor. □

以後我們會看到 Lemma 9.1.1 在有關 field 的性質的推導過程中很多地方占了關鍵性的地位. 首先看一個簡單的例子:

Corollary 9.1.2. *假設 F 是一個 field, 令 $F^* = F \setminus \{0\}$ 表示 F 中不為 0 的元素所成的集合, 則 F^* 在乘法的運算之下是一個 abelian group.*

Proof. 利用 F 是一個 ring with 1, 我們知道 F^* 滿足 Definition 1.1.1 中 (GP2) 和 (GP3) 的條件. 再來若 $a \in F^*$ 我們知存在 $a^{-1} \in F$ 滿足 $a \cdot a^{-1} = 1$, 然而 a^{-1} 不可能是 0, 否則會造成 $a \cdot a^{-1} = a \cdot 0 = 0$. 故知 $a^{-1} \in F^*$, 也就是說 F^* 也滿足 Definition 1.1.1 中 (GP4) 的性質. 因此要證明 F^* 在乘法的運算之下是一個 group 我們僅要檢查 (GP1). 也就是說若 $a, b \in F^*$, 則 $a \cdot b \in F^*$. 然而 $a, b \in F^*$ 表示 $a, b \in F$ 且 $a \neq 0, b \neq 0$, 故由 Lemma 9.1.1 知 $a \cdot b \neq 0$, 即 $a \cdot b \in F^*$. 至於 F^* 是 abelian, 則由 F 是 commutative ring 馬上得知. □

Example 9.1.3. 考慮

$$\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

這一個 ring. 由於 5 是 $\mathbb{Z}$ 中的 irreducible element 且 $\mathbb{Z}$ 是 principle ideal domain 利用 Lemma 8.3.2 知 $5\mathbb{Z} = \big(5\big)$ 是 $\mathbb{Z}$ 中的 maximal ideal. 所以知 $\mathbb{Z}/5\mathbb{Z}$ 是一個 field (Theorem 6.5.11). 我們可以驗證

$$(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

在乘法之下是一個 abelian group. 事實上由

$$\overline{2}^2 = \overline{4}, \quad \overline{2}^3 = \overline{3}, \quad \overline{2}^4 = \overline{1},$$

可知 $(\mathbb{Z}/5\mathbb{Z})^*$ 在乘法之下是一個 cyclic group (因 $|(\mathbb{Z}/5\mathbb{Z})^*| = 4$ 且 $\mathrm{ord}(\overline{2}) = 4$).

假設 F 是一個 field 且 $S \subseteq F$. 如果將 F 的加法與乘法運算限制在 S 中來看, S 也是一個 field, 則稱 S 是 F 的*subfield*. 因此如果 S 在 F 的加法之下是 F 的 subgroup 且 $S^* = S \setminus \{0\}$ 在 F^* 的乘法之下是 F^* 的 subgroup, 則 S 就會是 F 的 subfield. 因此利用 Lemma 1.3.4 我們有以下的檢查 subfield 的方法.

Lemma 9.1.4. *假設 F 是一個 field 且 $S \subseteq F$. 如果對任意 $a, b \in S$, 其中 $b \neq 0$ 皆有 $a - b \in S$ 且 $a \cdot b^{-1} \in S$, 則 S 是 F 的 subfield.*

接下來我們來看 field 之間 homomorphism 的性質. 若 R 和 R' 是兩個 ring 且 $\psi : R \to R'$, 其中對任意的 $a \in R$ 皆有 $\psi(a) = 0$, 則依定義 ψ 當然是 R 到 R' 的一個 ring homomorphism. 不過這種 ring homomorphism 對我們來說是無用的, 一般我們稱之為*trivial homomorphism*.

Proposition 9.1.5. *假設 F 和 F' 都是 field 且 1_F 和 $1_{F'}$ 分別是 F 和 F' 中乘法的 identity. 如果 $\psi : F \to F'$ 是一個 nontrivial 的 ring homomorphism, 則*

(1) $\psi(1_F) = 1_{F'}$.

(2) ψ 是一對一的 *homomorphism.*

Proof. (1) 我們要證明 $\psi(1_F)$ 是 F' 的乘法 identity. 由於 ψ 不是 trivial, 故存在 $a \in F$ 使得 $\psi(a) \neq 0$. 然而 $\psi(a) = \psi(a \cdot 1_F)$, 利用 ψ 是 ring homomorphism 我們得 $\psi(a) = \psi(a) \cdot \psi(1_F)$. 然而在 F' 中我們仍然有 $\psi(a) \cdot 1_{F'} = \psi(a)$, 故得 $\psi(a) \cdot \psi(1_F) = \psi(a) \cdot 1_{F'}$, 也就是說

$$\psi(a) \cdot \big(\psi(1_F) - 1_{F'}\big) = 0.$$

利用 F' 是一個 integral domain (Lemma 9.1.1) 且 $\psi(a) \neq 0$, 我們得證 $\psi(1_F) = 1_{F'}$.

(2) 要證明 ψ 是一對一的等價於要證明 $\ker(\psi) = \big(0\big)$ (Lemma 6.3.4). 然而因 $\ker(\psi)$ 一定是 F 的一個 ideal (Lemma 6.3.3) 且 F 中僅有 F 和 $\big(0\big)$ 這兩個 trivial ideals (Lemma 6.2.4) 所以可知 $\ker(\psi) = F$ 或 $\ker(\psi) = \big(0\big)$. 但如果 $\ker(\psi) = F$, 表示對任意 $a \in F$ 皆使得 $\psi(a) = 0$, 此與 ψ 不是 trivial 的 ring homomorphism 相矛盾. 故知 $\ker(\psi) = \big(0\big)$, 也就是說 ψ 是一對一的 ring homomorphism. □

9.2. Field 的 Characteristic

對一般的 field F, 若 $a \in F$, 由於 $1 \in F$, 故對任意的 $n \in \mathbb{N}$ 我們有

$$\underbrace{a + \cdots + a}_{n \text{ 次}} = \underbrace{(1 + \cdots + 1)}_{n \text{ 次}} \cdot a. \tag{9.1}$$

要注意在這裡 1 加 n 次並不等於 n, 這是由於這裡的 1 是 F 中的 1 並不是自然數 $\mathbb{N}$ 中的 1. 例如上例中 $\overline{1}$ 是 $\mathbb{Z}/5\mathbb{Z}$ 中的 1, 但

$$\overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{0},$$

而在 $\mathbb{N}$ 中 5 是不等於 0 的. 所以我們不能把式子 (9.1) 寫成

$$\underbrace{a + \cdots + a}_{n \text{ 次}} = n \cdot a.$$

不過為了方便, 對任意 $a \in F$ 且 $n \in \mathbb{N}$ 我們用 na 來表示 a 自己加自己 n 次, 也就是說

$$\underbrace{a + \cdots + a}_{n \text{ 次}} = na.$$

希望不會造成大家的困擾. 因此我們可以將式子 (9.1) 寫成

$$na = \underbrace{a + \cdots + a}_{n \text{ 次}} = \underbrace{(1 + \cdots + 1)}_{n \text{ 次}} \cdot a = (n1) \cdot a.$$

Lemma 9.2.1. 假設 F 是一個 *field,* 則對 F 下面兩種情況之一會發生*:*

(1) 對任意 $n \in \mathbb{N}$ 且 $a \in F \setminus \{0\}$ 皆有 $na \neq 0$.

(2) 存在一個 *prime* $p \in \mathbb{N}$ 使得對任意的 $a \in F$ 皆有 $pa = 0$.

Proof. 考慮 $\phi : \mathbb{Z} \to F$ 其中 $\phi(0) = 0$, 且對任意 $n \in \mathbb{N}$, $\phi(n) = n1$, $\phi(-n) = n(-1)$. 即

$$\phi(n) = \underbrace{1 + \cdots + 1}_{n \text{ 次}} \quad \text{且} \quad \phi(-n) = \underbrace{(-1) + \cdots + (-1)}_{n \text{ 次}}.$$

注意這裡的 1 是 F 中的 1, 而 -1 是 F 中 1 的加法 inverse. 很容易檢查 ϕ 是一個從 $\mathbb{Z}$ 到 F 的 ring homomorphism.

現考慮 ϕ 的 kernel. 由 ring 的 1st isomorphism theorem (Theorem 6.4.2) 我們有

$$\mathbb{Z}/\ker(\phi) \simeq \mathrm{im}(\phi).$$

然而 $\mathrm{im}(\phi)$ 會是 F 的一個 subring (Lemma 6.3.3), 故由 F 是 integral domain (Lemma 9.1.1) 知 $\mathrm{im}(\phi)$ 也是一個 integral domain. 換句話說 $\mathbb{Z}/\ker(\phi)$ 是一個 integral domain. 另一方面 $\ker(\phi)$ 會是 $\mathbb{Z}$ 的一個 ideal (Lemma 6.3.3) 故利用 Theorem 6.5.7 知 $\ker(\phi)$ 是 $\mathbb{Z}$ 的一個 prime ideal. 因 $\mathbb{Z}$ 是一個 principle ideal domain, 故存在 $a \in \mathbb{N}$ 滿足 $\ker(\phi) = \big(a\big)$. 利用 Lemma 8.1.9 我們知 $a = 0$ 或 $a = p$, 其中 p 是 $\mathbb{Z}$ 中的一個 prime.

(1) $\ker(\phi) = \big(0\big)$ 的情形: 此時因對任意的 $n \in \mathbb{N}$, 皆有 $n1 \neq 0$ (因 $n \notin \ker(\phi)$), 故知對任意的 $a \in F$ 且 $a \neq 0$, 因 F 是 integral domain, 皆有

$$na = (n1) \cdot a \neq 0.$$

(2) $\ker(\phi) = \big(p\big)$ 的情形: 此時因 $p \in \ker(\phi)$, 我們有 $p1 = 0$. 故得對任意的 $a \in F$ 皆有

$$pa = (p1) \cdot a = 0.$$

□

在 Lemma 9.2.1 中的 0 或 p 對 field 的分類上是很重要的, 因此我們有以下之定義.

Definition 9.2.2. 假設 F 是一個 field. 若對任意的 $n \in \mathbb{N}$ 且 $a \in F \setminus \{0\}$ 皆有 $na \neq 0$, 則稱 F 的 *characteristic* 是 0. 記為 $\mathrm{char}(F) = 0$. 反之若存在 $p \in \mathbb{N}$ 是 $\mathbb{Z}$ 中的 prime 使得對任意的 $a \in F$ 皆有 $pa = 0$, 則稱 F 的 *characteristic* 是 p. 記為 $\mathrm{char}(F) = p$.

例如有理數所成的 field $\mathbb{Q}$ 的 characteristic 就是 0. 又例如在 Example 9.1.3 中的 $\mathbb{Z}/5\mathbb{Z}$ 就符合對任意的 $a \in \mathbb{Z}/5\mathbb{Z}$ 皆有 $5a = 0$, 所以我們有 $\mathrm{char}(\mathbb{Z}/5\mathbb{Z}) = 5$.

要注意由 Lemma 9.2.1 我們知若 F 是一個 field, 則 $\mathrm{char}(F)$ 要不是等於 0 就是等於一個 prime p. 如果 $\mathrm{char}(F) = p \neq 0$, 則此 p 是滿足 $pa = 0$ 其中 $a \in F \setminus \{0\}$ 的最小的正整數. 因為若 $n \in \mathbb{N}$ 且 $na = 0$, 則由 F 是 integral domain 以及

$$na = (n1) \cdot a = 0$$

知 $n1 = 0$. 也就是說 $n \in \ker(\phi) = \big(p\big)$. 這告訴我們 $n \geq p$.

若 F 是一個 field 且 F 只有有限多個元素, 則我們稱 F 為一個 *finite field*.

Lemma 9.2.3. 若 F 是一個 *finite field,* 則存在一 *prime* $p \in \mathbb{N}$ 使得 $\mathrm{char}(F) = p$.

Proof. 由 Lemma 9.2.1 我們知 $\mathrm{char}(F) = 0$ 或 $\mathrm{char}(F) = p$ 其中 p 是一個質數. 我們要說明 $\mathrm{char}(F)$ 不可能是 0. 其實如果 $\mathrm{char}(F) = 0$, 表示前面定的那個 ring homomorphism $\phi : \mathbb{Z} \to F$ 符合 $\ker(\phi) = \big(0\big)$, 也就是說 ϕ 是一對一的. 換言之 $\mathbb{Z} \simeq \mathrm{im}(\phi) \subseteq F$. 然而 $\mathbb{Z}$ 有無窮多個元素, 故得到 F 中有一個 subring 其元素有無窮多個. 此和 F 是 finite field 相矛盾, 故知 $\mathrm{char}(F) = p \neq 0$. □

利用 Proposition 9.1.5 我們可得以下有關於 characteristic 的性質. 它告訴我們當兩個 field 的 characteristic 不相同時, 它們之間不可能存在 nontrivial 的 ring homomorphism.

Proposition 9.2.4. 假設 F 和 F' 是 *fields* 且 F 和 F' 之間存在 *nontrivial* 的 *ring homomorphism,* 則 $\mathrm{char}(F) = \mathrm{char}(F')$.

Proof. 假設 $\psi : F \to F'$ 不是一個 trivial 的 ring homomorphism, 由 Proposition 9.1.5 (1) 知 $\psi(1_F) = 1_{F'}$. 因此若 $\mathrm{char}(F) = p \neq 0$, 利用

$$\psi(p1_F) = \psi(0) = 0$$

以及

$$\psi(p1_F) = \psi(\underbrace{1_F + \cdots 1_F}_{p \text{ 次}}) = p\psi(1_F) = p1_{F'},$$

我們得

$$p1_{F'} = 0.$$

故知 $\mathrm{char}(F') \neq 0$. 然而若 $\mathrm{char}(F') = q \neq p$, 則因 p 和 q 皆是質數所以互質, 故存在 $m, n \in \mathbb{Z}$ 使得 $mp + nq = 1$. 因此由 $p1_{F'} = q1_{F'} = 0$ 可得

$$1_{F'} = (mp + nq)1_{F'} = 0,$$

造成矛盾. 故知 $\mathrm{char}(F) = \mathrm{char}(F')$.

另外若 $\mathrm{char}(F) = 0$, 此時對任意 $n \in \mathbb{N}$ 皆有 $n1_F \neq 0$. 利用 Proposition 9.1.5 (2) 知 $\psi(n1_F) \neq 0$. 換句話說

$$\psi(n1_F) = n\psi(1_F) = n1_{F'} \neq 0,$$

這表示 $\mathrm{char}(F') = 0$. □

最後我們來看當 $\mathrm{char}(F) = p \neq 0$ 時, 在運算上的一個特殊性質.

Lemma 9.2.5. 假設 F 是一個 *field* 且 $\mathrm{char}(F) = p \neq 0$, 則對任意 $a, b \in F$, 我們有

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \quad \text{and} \quad (a - b)^{p^n} = a^{p^n} - b^{p^n}, \quad \forall\, n \in \mathbb{N}.$$

Proof. 我們先用 induction 證明 $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. 首先考慮 $n = 1$ 的情況. 我們先檢查 $(a+b)^2$ 為何? 由於 $(a+b)^2 = a^2 + a\cdot b + b\cdot a + b^2$, 利用 F 是一個 field 知 $a\cdot b = b\cdot a$, 因此我們得 $(a+b)^2 = a^2 + 2(a\cdot b) + b^2$. 再次強調這裡 $2(a\cdot b)$ 是 $(a\cdot b) + (a\cdot b)$ 而不是 $2\cdot(a\cdot b)$. 所以繼續下去我們可以利用類似二項式定理得

$$(a+b)^p = a^p + p(a^{p-1}\cdot b) + \cdots + \binom{p}{i}(a^i\cdot b^{p-i}) + \cdots + b^p.$$

由於 $\mathrm{char}(F) = p$, 對任意 $\alpha \in F$, α 自己連加自己 p 次等於 0 (即 $p\alpha = 0$). 大家都知道當 p 是質數且當 $i = 1, \ldots, p-1$ 時, $\binom{p}{i}$ 是 p 的倍數, 故知此時 $\binom{p}{i}(a^i\cdot b^{p-i}) = 0$. 因此我們可得

$$(a+b)^p = a^p + b^p. \tag{9.2}$$

現利用歸納假設

$$(a+b)^{p^{n-1}} = a^{p^{n-1}} + b^{p^{n-1}}, \tag{9.3}$$

故利用式子 (9.2) 和 (9.3) 我們知

$$(a+b)^{p^n} = \big((a+b)^{p^{n-1}}\big)^p = (a^{p^{n-1}} + b^{p^{n-1}})^p = a^{p^n} + b^{p^n}.$$

接下來證明 $(a-b)^{p^n} = a^{p^n} - b^{p^n}$. 首先注意當 $\mathrm{char}(F) = 2$ 時, 對任意 $\alpha \in F$ 我們有 $\alpha + \alpha = 2\alpha = 0$, 故知 $\alpha = -\alpha$. 因此在 $p = 2$ 時我們自然有

$$(a-b)^{p^n} = (a+b)^{p^n} = a^{p^n} + b^{p^n} = a^{p^n} - b^{p^n}.$$

而當 p 是 odd prime number 時, 由於對任意 α 皆有 $(-\alpha)^{p^n} = -\alpha^{p^n}$ (Corollary 5.2.4), 我們得

$$(a-b)^{p^n} = \big(a + (-b)\big)^{p^n} = a^{p^n} + (-b)^{p^n} = a^{p^n} - b^{p^n}.$$

□

Lemma 9.2.5 也可以推廣到 $F[x]$ 上的運算. 注意 $F[x]$ 上的 polynomial 的係數都在 F 中, 而且 $F[x]$ 上的加法依定義是將同次項的係數都加起來. 因此若 $\mathrm{char}(F) = p$ 時, 對任意的 $f(x) = a_n x^n + \cdots + a_0 \in F[x]$ 我們都有

$$\underbrace{f(x) + \cdots + f(x)}_{p\text{ 次}} = \underbrace{(a_n + \cdots + a_n)}_{p\text{ 次}}x^n + \cdots + \underbrace{(a_0 + \cdots + a_0)}_{p\text{ 次}} = 0.$$

因此利用類似 Lemma 9.2.5 的證明我們有以下的性質:

Lemma 9.2.6. 假設 F 是一個 *field* 且 $\mathrm{char}(F) = p \neq 0$, 則對任意 $f(x) = a_m x^m + \cdots + a_0 \in F[x]$, 我們有

$$(f(x))^{p^n} = a_m^{p^n} x^{mp^n} + \cdots + a_0^{p^n}, \quad \forall\, n \in \mathbb{N}.$$

特別當 $a \in F$ 時, 我們有

$$(x-a)^{p^n} = x^{p^n} - a^{p^n}, \quad \forall\, n \in \mathbb{N}.$$

9.3. 線性代數的應用

這一節中我們先簡單的回顧一些線性代數的基本概念, 以便以後將這些概念應用在相關 field 的性質.

9.3.1. 線性代數基本性質. 在這裡我們僅簡單回顧什麼是 vector space, basis 以及 dimension. 我們不給這些基本性質的証明, 若不清楚的同學請參考一般有關線性代數的書籍.

Definition 9.3.1. 令 F 是一個 field. 我們說 V 是一個 *vector space over* F, 如果 V 本身元素間有加法 "+" 運算, 而且對任意 $c \in F$, $v \in V$ 皆有 $c \cdot v \in V$, 且滿足:

(VS1): V 在加法之下是一個 abelian group.

(VS2): 對所有的 $c \in F$ 以及 $v_1, v_2 \in V$ 皆有 $c \cdot (v_1 + v_2) = c \cdot v_1 + c \cdot v_2$.

(VS3): 對所有 $c_1, c_2 \in F$ 以及 $v \in V$ 皆有 $(c_1 + c_2) \cdot v = c_1 \cdot v + c_2 \cdot v$ 且 $c_1 \cdot (c_2 \cdot v) = (c_1 \cdot c_2) \cdot v$.

(VS4): 對任意 $v \in V$ 皆有 $1 \cdot v = v$, 其中 $1 \in F$ 是 F 乘法的 identity.

這裡要注意一般 vector space 的定義裡並沒有要求 $F \subseteq V$, 也沒有要求 V 的元素間有乘法運算. 不過將來我們討論 field 的性質時所碰到的 vector space 都會額外有 $F \subseteq V$ 以及 V 的元素間有乘法運算這兩種特性. 也就是這兩種特性使得 field 的性質比一般的 vector space 強得多.

Definition 9.3.2. 假設 F 是一個 field 且 V 是一個 vector space over F, 如果 $v_1, \ldots, v_n \in V$ 滿足對任意 $v \in F$ 皆存在 $c_1, \ldots, c_n \in F$ 使得

$$v = c_1 \cdot v_1 + \cdots + c_n \cdot v_n,$$

則稱 $v_1, \ldots, v_n$ *span* V over F.

如果一個 vector space 存在一組 $v_1, \ldots, v_n \in V$ span V over F, 則我們稱 V 是一個 *finite dimensional vector space* over F.

如果 $v_1, \ldots, v_n$ span V over F, 當然也有可能有另一組 $w_1, \ldots, w_m \in V$ 也 span V over F. 我們當然希望能找到一組元素最少的 $v_1, \ldots, v_n$ 可以 span V over F. 要達到這一點 $v_1, \ldots, v_n$ 之間至少要沒有線性關係, 要不然其中的某個 v_i 可以被其他的 v_j 展成, 我們就可以找到更少的元素 span V 了. 因此我們有以下的定義.

Definition 9.3.3. 假設 F 是一個 field 且 V 是一個 vector space over F, 如果對於 V 中的一組元素 $v_1, \ldots, v_n \in V$ 我們都找不到不全為 0 的 $c_1, \ldots, c_n \in F$ 使得

$$c_1 \cdot v_1 + \cdots + c_n \cdot v_n = 0,$$

則稱這組 $v_1, \ldots, v_n$ 是 *linearly independent* over F.

如果 $v_1, \ldots, v_n \in F$ span V 且是 linearly independent over F, 則稱 $v_1, \ldots, v_n$ 是一組 *basis* of V over F.

線性代數中最基本的性質就是當 V 是 finite dimensional vector space over F 時, 一定可以找到 V over F 的一組 basis. 雖然 basis 並不是唯一的, 不過任一組 basis 其元素個數都是相同的. 這個 basis 的個數稱之為 V over F 的 *dimension*, 我們記為 $\dim_F(V)$. 也就是說若 $\dim_F(V) = n$, 則可以找到一組 $v_1, \ldots, v_n \in V$ 是 linearly independent over F 且 span V over F.

如果 $W \subseteq V$ 且利用 V 和 F 間的運算 W 也是一個 vector space over F, 則稱 W 是 V 的一個 *subspace* over F. 以下是 dimension 一些基本的性質, 我們略去證明.

Lemma 9.3.4. 假設 F 是一個 *field* 且 V 是一個 *finite dimensional vector space over* F.

(1) 若 $v_1, \ldots, v_n$ *span* V *over* F, 則 $\dim_F(V) \leq n$.

(2) 若 $w_1, \ldots, w_m \in F$ 是 *linearly independent over* F, 則 $\dim_F(V) \geq m$.

(3) 若 W 是 V 的一個 *subspace over* F, 則 $\dim_F(V) \geq \dim_F(W)$.

9.3.2. 將 ring 看成是 vector space. 我們首先來看一些例子, 且計算其 dimension.

假設 F 是一個 field, 我們考慮 $F[x]$ 這一個 polynomial ring. 很容易看出來 $F[x]$ 和 F 滿足 Definition 9.3.1 中 (VS1) 到 (VS4) 性質, 故知 $F[x]$ 是一個 vector space over F. 至於 $F[x]$ 會不會是 finite dimensional vector space over F 呢?

Proposition 9.3.5. 假設 F 是一個 *field*, 若將 $F[x]$ 看成是一個 *vector space over* F, 則 $F[x]$ 不是 *finite dimensional vector space over* F.

Proof. 我們利用反證法. 假設 $F[x]$ 是 finite dimensional over F 且 $\dim_F(F[x]) = n$, 則考慮 $1, x, x^2, \ldots, x^n \in F[x]$, 我們要驗證 $1, x, x^2, \ldots, x^n$ 是 linearly independent over F. 這是因為對任意不全為 0 的 $c_0, c_1, \ldots, c_n$ 我們知

$$c_0 \cdot 1 + c_1 \cdot x + \cdots + c_n \cdot x^n \neq 0.$$

注意 $1, x, x^2, \ldots, x^n$ 共有 $n+1$ 個元素, 故利用 Lemma 9.3.4 (2) 知

$$n + 1 \leq \dim_F(F[x]) = n,$$

因而得到矛盾. 所以 $F[x]$ 不可能是 finite dimensional over F. □

接著我們考慮另一個 ring. 假設 $f(x) \in F[x]$ 且 $\deg(f(x)) \geq 1$, 我們考慮 $R = F[x]/\big(f(x)\big)$ 這一個 quotient ring. 回顧一下 R 中的元素都是 $\overline{g(x)}$ 的形式, 其中 $g(x) \in F[x]$. 對任意的 $c \in F$, $\overline{g(x)} \in R$, 我們定義

$$c \cdot \overline{g(x)} = \overline{c \cdot g(x)}.$$

這個運算是 well-defined. 因為若 $\overline{g(x)} = \overline{h(x)}$ 表示, $g(x) - h(x) \in \big(f(x)\big)$. 又因為 $c \in F \subseteq F[x]$ 且 $\big(f(x)\big)$ 是 $F[x]$ 的一個 ideal, 我們當然有 $c \cdot (g(x) - h(x)) \in \big(f(x)\big)$,

故知 $c\cdot\overline{g(x)}=c\cdot\overline{h(x)}$. 利用這個 F 對 R 的運算我們很容易驗證 R 是一個 vector space over F. 那麼 R 會不會是 finite dimensional vector space over F 呢?

Lemma 9.3.6. 假設 F 是一個 *field,* 若 $f(x)\in F[x]$ 且 $\deg(f(x))\geq 1$, 則 $R=F[x]/\big(f(x)\big)$ 這一個 *quotient ring* 是一個 *finite dimensional vector space over* F 而且 $\dim_F(R)=\deg(f(x))$.

Proof. 假設 $\deg(f(x))=n$, 我們要證明 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}\in R$ 是 R over F 的一組 basis.

首先證明 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}$ span R over F. 任取 $\overline{g(x)}\in R$, 其中 $g(x)\in F[x]$, 我們要找到 $c_0,c_1,\ldots,c_{n-1}\in F$ 使得

$$\overline{g(x)}=c_0\cdot\overline{1}+c_1\cdot\overline{x}+\cdots+c_{n-1}\cdot\overline{x}^{n-1}.$$

由 Theorem 7.2.4, 我們知道存在 $h(x),r(x)\in F[x]$ 滿足 $g(x)=f(x)\cdot h(x)+r(x)$, 其中 $r(x)=0$ 或 $\deg(r(x))<\deg(f(x))$. 因為 $g(x)-r(x)=f(x)\cdot h(x)\in\big(f(x)\big)$, 由 quotient ring 的定義知 $\overline{g(x)}=\overline{r(x)}$. 現若 $r(x)=0$, 知 $\overline{g(x)}=\overline{0}$, 故取 $c_0=c_1=\cdots=c_{n-1}=0$ 時可得

$$\overline{g(x)}=\overline{0}=c_0\cdot\overline{1}+c_1\cdot\overline{x}+\cdots+c_{n-1}\cdot\overline{x}^{n-1}.$$

另一方面若 $r(x)\neq 0$, 則由 $\deg(r(x))\leq n-1$ 知存在 $a_0,a_1,\ldots,a_{n-1}\in F$ 使得 $r(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$, 故令 $c_0=a_0,\ldots,c_{n-1}=a_{n-1}$ 時我們有

$$\overline{g(x)}=\overline{r(x)}=c_0\cdot\overline{1}+c_1\cdot\overline{x}+\cdots+c_{n-1}\cdot\overline{x}^{n-1}.$$

所以 R 中的元素都可由 $\overline{1},\ldots,\overline{x}^{n-1}$ span over F 得到.

接著證明 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}$ 是 linearly independent over F. 我們利用反證法. 假設存在不全為 0 的 $c_0,c_1,\cdots,c_{n-1}\in F$ 使得

$$c_0\cdot\overline{1}+c_1\cdot\overline{x}+\cdots+c_{n-1}\cdot\overline{x}^{n-1}=\overline{0},$$

表示 $g(x)=c_0+\cdots+c_{n-1}x^{n-1}$ 這個非 0 的多項式符合 $\overline{g(x)}=\overline{0}$. 換句話說 $g(x)\in\big(f(x)\big)$. 因 $g(x)\neq 0$, 故知存在 $h(x)\in F[x]$ 且 $h(x)\neq 0$ 使得 $g(x)=f(x)\cdot h(x)$. 觀察 degree 知

$$\deg(g(x))=\deg(f(x))+\deg(h(x))\geq\deg(f(x))=n,$$

不過由當初 $g(x)$ 的選取, 我們知道 $\deg(g(x))\leq n-1$, 因此得到矛盾. 故知 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}$ 是 linearly independent over F.

我們已證得 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}\in R$ 是 R over F 的一組 basis. 又因 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}$ 中共有 n 個元素, 故知 $\dim_F(R)=n=\deg(f(x))$. □

當 R 是一個 integral domain 且 F 是一個包含於 R 的 field 時, 我們也可以將 R 看成是一個 vector space over F. 事實上由 ring 的性質加上 $F\subseteq R$, Definition 9.3.1 中的 (VS1), (VS2) 以及 (VS3) 自然都符合, 我們唯一要檢查的是 (VS4). 假

設 $1_F, 1_R$ 分別是 F 和 R 乘法的 identity, 我們只要檢察 $1_F = 1_R$ 即可. 這是因為 (VS4) 是說對任意的 $a \in R$ 要符合 $1_F \cdot a = a$. 因此若能證得 $1_F = 1_R$, 那麼上式自然成立. 要注意我們曾經看過例子一個 subring 的 identity 不一定會是原來的 ring 的 identity. 不過由於現在 R 是 integral domain, 事情就沒有那麼複雜了. 我們只要任取 F 中的一個非 0 元素 c, 將它考慮成是 F 的元素, 我們有 $1_F \cdot c = c$; 另一方面將它看成是 R 的元素, 我們有 $1_R \cdot c = c$. 結合上面兩個等式得: $(1_F - 1_R) \cdot c = 0$. 由於 R 是 integral domain 且 $c \neq 0$, 所以我們有 $1_F = 1_R$.

既然 R 是一個 over F 的 vector space, 我們來看當 R 是 finite dimensional over F 時它有什麼重要特性.

Theorem 9.3.7. 假設 R 是一個 *integral domain*, F 是一個 *field* 且 $F \subseteq R$. 又假設 R 看成是一個 *vector space over* F 時是 *finite dimensional over* F, 則

(1) 對任意 $a \in R$, 皆存在一個非 0 的 $f(x) \in F[x]$ 使得 $f(a) = 0$.

(2) R 是一個 *field*.

Proof. 我們假設 $\dim_F(R) = n$.

(1) 考慮 $1, a, a^2, \ldots, a^n$ 這 $n+1$ 個 R 中的元素. 如果它們是 linearly independent over F, 則由 Lemma 9.3.4 (2) 得

$$n = \dim_F(R) \geq n + 1,$$

造成矛盾, 故知 $1, a, a^2, \ldots, a^n$ 不是 linearly independent over F. 換句話說存在不全為 0 的 $c_0, c_1, \ldots, c_n \in F$, 滿足

$$c_0 \cdot 1 + c_1 \cdot a + \cdots + c_n \cdot a^n = 0.$$

故令 $f(x) = c_0 + c_1 x + \cdots + c_n x^n$, 我們得 $f(x) \neq 0$ 且 $f(a) = 0$.

(2) 因 R 已知是 integral domain, 要證明 R 是一個 field, 我們只要證明 R 中不為 0 的元素都是 unit. 換句話說要證明對任意 $a \in R$ 且 $a \neq 0$, 皆存在 $b \in R$ 滿足 $a \cdot b = 1$. 由 (1) 知存在非 0 的多項式 $f(x)$ 滿足 $f(a) = 0$. 我們假設

$$f(x) = c_0 + c_1 x + \cdots + c_m x^m \in F[x]$$

是 $F[x]$ 中非 0 且滿足 $f(a) = 0$ 的 degree 最小的 polynomial. 由 degree 最小的假設, 我們可得 $c_0 \neq 0$. 這是因為若 $c_0 = 0$, 則由

$$f(a) = c_1 \cdot a + \cdots + c_m \cdot a^m = (c_1 + c_2 \cdot a + \cdots + c_m \cdot a^{m-1}) \cdot a = 0$$

以及 R 是 integral domain 得 $g(a) = 0$, 其中 $g(x) = c_1 + c_2 x + \cdots + c_m x^{m-1} \in F[x]$ 不為 0 且 $\deg(g(x)) < \deg(f(x))$. 此和 $f(x)$ 是 degree 最小的找法相矛盾, 故得 $c_0 \neq 0$. 現將 $f(a) = 0$ 的 c_0 移至等式的另一邊, 我們得

$$(c_1 + c_2 \cdot a + \cdots + c_m \cdot a^{m-1}) \cdot a = -c_0.$$

因此若令

$$b = (-c_0)^{-1} \cdot (c_1 + c_2 \cdot a + \cdots + c_m \cdot a^{m-1}),$$

則我們有 $a \cdot b = 1$. 注意由於 $-c_0 \in F$ 且 $-c_0 \neq 0$ 以及 F 是一個 field, 我們有 $(-c_0)^{-1} \in F \subseteq R$, 再加上 $c_1 + c_2 \cdot a + \cdots + c_m \cdot a^{m-1} \in R$ 我們得 $b \in R$, 故知 a 是 R 的一個 unit. □

利用 Theorem 9.3.7 我們可以很快的給 Proposition 9.3.5 另一個證明: 假如 $F[x]$ 是 finite dimensional over F, 由於 $F[x]$ 是 integral domain 利用 Theorem 9.3.7 我們得 $F[x]$ 會是一個 field. 但這是不可能的, 因為 $F[x]$ 中只有 degree 為 0 的元素才是 unit.

9.4. Extension Field

給定一個 field F, 我們當然可以討論其 subfield, 不過因一般 field 的理論關心的是給定 $f(x) \in F[x]$ 如果在 F 中 $f(x)$ 沒有根, 那麼如何在比 F 大的 field 找到根. 所以我們比較關心的就是所謂 F 的 extension field.

Definition 9.4.1. 給定 F 是一個 field, 若 $L \supseteq F$ 也是一個 field 而且 L 的運算限制在 F 中就是原本 F 的運算, 則我們稱 L 是 F 的一個 *extension* (或稱 *extension field*). 當然了我們也可以稱 F 是 L 的一個 *subfield*.

假設 F 是一個 field 且 L 是 F 的一個 extension field, 由 Lemma 9.1.1 知 L 是一個 integral domain, 故由前一節的討論我們知 L 是一個 vector space over F. 我們當然可以討論 L over F 的 dimension.

Definition 9.4.2. 假設 F 是一個 field 且 L 是 F 的一個 extension field. 如果將 L 看成是 over F 的一個 vector space 是一個 finite dimensional vector space over F, 則稱 L 是 F 的一個 *finite extension*. 通常我們會將 $\dim_F(L)$ 用 $[L : F]$ 來表示, 稱之為 the *degree* of L over F (而不是說 the dimension of L over F).

我們可以利用 Theorem 9.3.7 得到以下有趣的結果:

Proposition 9.4.3. 假設 F 是一個 *field* 且 L 是 F 的一個 *finite extension*. 如果 R 是 L 的一個 *subring* 且符合 $F \subseteq R \subseteq L$, 則 R 是一個 *field*.

Proof. 我們不打算用定義直接證明 R 是一個 field, 而是想套用 Theorem 9.3.7 來得到. 要套用 Theorem 9.3.7, 我們必須說明 R 是一個 integral domain 且 $\dim_F(R)$ 是有限的.

因為 L 已經是一個 integral domain (Lemma 9.1.1), 而 R 是 L 的 subring, 所以 R 當然是 integral domain. 另一方面, 我們可以把 R 看成是 L 的一個 subspace over F. 故利用 L 是 F 的一個 finite extension 的假設以及 Lemma 9.3.4 知 $\dim_F(R) \leq \dim_F(L)$, 換句話說 R 是一個 finite dimensional vector space over F. 因此利用 Theorem 9.3.7 (2) 得證 R 是一個 field. □

若 L 是 F 的一個 finite extension, 則直接將 Theorem 9.3.7 (1) 套用在 L 上, 我們馬上知對任意的 $a \in L$ 皆存在一個 $F[x]$ 中的 polynomial $f(x) \neq 0$ 滿足 $f(a) = 0$. 這樣的元素我們給它一個特殊的名字.

Definition 9.4.4. 假設 F 是一個 field 且 L 是 F 的一個 extension field. 假設 $a \in L$, 如果存在 $F[x]$ 中的一個非 0 的 polynomial $f(x)$ 滿足 $f(a) = 0$, 則稱 a 是 *algebraic* over F.

所以 Theorem 9.3.7 告訴我們以下結果:

Lemma 9.4.5. 假設 F 是一個 *field* 且 L 是 F 的一個 *finite extension,* 則 L 中的元素都是 *algebraic over* F.

當一個 extensional field of F 中的元素都是 algebraic over F 時, 我們稱這個 extension 是一個 *algebraic extension*. Lemma 9.4.5 告訴我們任何的 finite extension of F 也都是 algebraic extension of F. 不過要注意的是一個 algebraic extension of F 不一定是 finite extension of F.

最後我們再看一個有關 finite extension 重要的性質. 如果 F 是一個 field, K 是 F 的 一個 extension field, 而又 L 是 K 的一個 extension field. 也就是我們有 $F \subseteq K \subseteq L$ 這一個關係. 當然了 L 也可看成是 F 的一個 extension. 現若假設 K over F 和 L over K 都是 finite extension, 我們自然會問那麼 L 看成是 F 的 extension 時是否也是 finite extension?

Theorem 9.4.6. 假設 F 是一個 *field,* L 和 K 都是 F 的 *extensions* 且符合 $F \subseteq K \subseteq L$. 若已知 K 是 F 的一個 *finite extension* 且 L 是 K 的一個 *finite extension,* 則 L 也是 F 的一個 *finite extension,* 而且

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

Proof. 假設 $[K : F] = m$ 以及 $[L : K] = n$, 我們想證明 L 是一個 finite extension of F 且其 degree 為 $m \cdot n$. 由 $[K : F] = m$ 的假設知 $\dim_F(K) = m$, 即存在 $a_1, \ldots, a_m \in K$ 是 K over F 的一組 basis. 同樣的存在 $b_1, \ldots, b_n \in L$ 是 L over K 的一組 basis. 我們想證明

$$\{a_i \cdot b_j\}, \quad i = 1, \ldots, m \text{ 且 } j = 1, \ldots, n$$

是 L over F 的一組 basis. 如此自然得證本定理. 首先要注意的是因為 $K \subseteq L$ 所以由 $a_i \in K$, $b_j \in L$ 自然可得 $a_i \cdot b_j \in L$. 我們要證明這些 $a_i \cdot b_j$ span L over F 且是 linearly independent over F.

首先證明 $\{a_i \cdot b_j\}$ span L over F: 任取 $\alpha \in L$, 我們要找到 $c_{i,j} \in F$ 使得

$$\alpha = \sum_{j=1}^{n} \sum_{i=1}^{m} c_{i,j} \cdot (a_i \cdot b_j).$$

然而因 $b_1, \ldots, b_n$ span L over K, 我們可以找到 $d_1, \ldots, d_n \in K$ 使得

$$\alpha = d_1 \cdot b_1 + \cdots + d_n \cdot b_n. \tag{9.4}$$

再利用 $a_1, \ldots, a_m$ span K over F, 對任一 $d_j \in K$, 我們都可以找到 $c_{1,j}, \ldots, c_{m,j} \in F$ 使得

$$d_j = c_{1,j} \cdot a_1 + c_{2,j} \cdot a_2 + \cdots + c_{m,j} \cdot a_m.$$

將這些 d_j 帶入式子 (9.4), 得證$\{a_i \cdot b_j\}$ span L over F.

接著證明 $\{a_i \cdot b_j\}$ 是 linearly independent over F. 利用反證法, 假設存在一組不全為 0 的 $c_{i,j} \in F$ 使得 $\sum c_{i,j} \cdot (a_i \cdot b_j) = 0$. 這表示

$$\begin{aligned} 0 \;=\; & (c_{1,1} \cdot a_1 + c_{2,1} \cdot a_2 + \cdots + c_{m,1} \cdot a_m) \cdot b_1 \\ & + \cdots + (c_{1,n} \cdot a_1 + c_{2,n} \cdot a_2 + \cdots + c_{m,n} \cdot a_m) \cdot b_n \end{aligned}$$

注意對任意的 $j = 1, \ldots, n$, 若令

$$d_j = c_{1,j} \cdot a_1 + c_{2,j} \cdot a_2 + \cdots + c_{m,j} \cdot a_m,$$

因為 $c_{i,j} \in F$, $a_i \in K$ 且 $F \subseteq K$, 我們有 $d_j \in K$ 且

$$0 = d_1 \cdot b_1 + d_2 \cdot b_2 + \cdots + d_n \cdot b_n.$$

因為 $b_1, \ldots, b_n$ 是 linearly independent over K, 故得 $d_1 = d_2 = \cdots = d_n = 0$. 換句話說對任意的 $j = 1, \ldots, n$, 皆有

$$0 = d_j = c_{1,j} \cdot a_1 + c_{2,j} \cdot a_2 + \cdots + c_{m,j} \cdot a_m.$$

再利用 $a_1, \ldots, a_m$ 是 linearly independent over F 以及這些 $c_{i,j}$ 皆屬於 F, 我們得這些 $c_{i,j}$ 皆等於 0. 此和當初假設 $c_{i,j}$ 不全為 0 相矛盾, 故得證 $\{a_i \cdot b_j\}$ 是 linearly independent over F. □

要注意 Theorem 9.4.6 中的條件是要求 K 是 F 的 finite extension 且 L 是 K 的 finite extension 才能推得 L 是 F 的 finite extension. 我們自然會問反過來對嗎? 也就是說但如果已知 L 是 F 的 finite extension, 我們是否可得 K 是 F 的 finite extension 且 L 是 K 的 finite extension 呢? 答案是肯定的, 事實上我們有以下的結果:

Corollary 9.4.7. 假設 F 是一個 *field,* L 和 K 都是 F 的 *extensions* 且符合 $F \subseteq K \subseteq L$. 若已知 L 是 F 的一個 *finite extension,* 則 K 是 F 的一個 *finite extension* 且 L 是 K 的一個 *finite extension,* 而且

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

Proof. 由 $F \subseteq K \subseteq L$ 這個關係式, 我們可將 K 看成是 L over F 的 subspace, 所以由 Lemma 9.3.4 (3) 知 $\dim_F(L) \geq \dim_F(K)$, 換句話說若 L over F 是一個 finite extension 那麼 K over F 當然也是 finite extension. 另一方面若假設 $[L : F] = \dim_F(L) = n$, 也就說存在 $a_1, \ldots, a_n \in L$ 是一組 L over F 的 basis, 由於

$a_1, \ldots, a_n$ span L over F 再加上 $F \subseteq K$, 我們當然知 $a_1, \ldots, a_n$ 也 span L over K. 所以利用 Lemma 9.3.4 (1) 知 $\dim_K(L) \leq n = \dim_F(L)$. 因此得 L 是 K 的一個 finite extension.

上面已證若 L 是 F 的一個 finite extension, 則 K 是 F 的一個 finite extension 且 L 是 K 的一個 finite extension. 因此可套用 Theorem 9.4.6 得證

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

□