# 大學基礎代數

李華介

國立台灣師範大學數學系

*Chapter 5*

# 初級 Ring 的性質

在本章中我們將介紹 ring 的定義及其基本性質, 我們也會介紹一些重要常見的 ring 的例子.

## 5.1. Ring 的基本定義

Ring 的結構比 Group 豐富, 它必須有兩種運算. 一般我們分別用「$+$」和「$\cdot$」表示此二運算. 其中在 $+$ 的運算下我們要求是一個 **abelian group**, 而 $\cdot$ 的運算僅要求封閉性和結合率. 當然了如果這兩種運算沒有甚麼關聯, 那就沒甚麼意思了. 我們需要分配率 (distributive laws) 來將它們連結在一起.

**Definition 5.1.1.** 一個集合 $R$ 中如果有 $+$ 和 $\cdot$ 兩種運算且符合以下性質, 則稱之為一個 *ring*:

**(R1):** 對任意的 $a, b \in R$ 皆有 $a + b \in R$.

**(R2):** 對任意的 $a, b, c \in R$ 皆有 $(a + b) + c = a + (b + c)$.

**(R3):** 在 $R$ 中存在一元素定之為 0 滿足對任意的 $a \in R$ 皆有 $a+0 = 0+a = a$.

**(R4):** 給定 $R$ 中任一元素 $a$, 在 $R$ 中皆存在一元素 $b$ 滿足 $a + b = b + a = 0$.

**(R5):** 對任意的 $a, b \in R$ 皆有 $a + b = b + a$.

**(R6):** 對任意的 $a, b \in R$ 皆有 $a \cdot b \in R$.

**(R7):** 對任意的 $a, b, c \in R$ 皆有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

**(R8):** 對任意的 $a, b, c \in R$ 皆有 $a \cdot (b+c) = a \cdot b + a \cdot c$ 且 $(b+c) \cdot a = b \cdot a + c \cdot a$.

(R1) 到 (R5) 告訴我們 $R$ 在加法 $(+)$ 運算下是一個 abelian group. 所以在 group 中的一些基本理論我們都可以直接套用. 比方說 0 是 $R$ 中唯一符合 $a+0 = 0+a = a$ 的元素 (Proposition 1.2.1), 以及給定 $a \in R$ 只存在唯一的 $b \in R$ 滿足 $a+b = b+a = 0$ (Proposition 1.2.2). 依習慣我們將此 $b$ 記做 $-a$. 還是要強調一下這裡的 0 並不一

定是大家常看到整數或實數上的 0, 而 $-a$ 也僅表示為 $a$ 的加法之 inverse, 並沒有一般正負號的意義.

我們列出一些 group 的性質方便以後直接引用.

**Lemma 5.1.2.** 假設 $R$ 是一個 *ring,* 則*:*

(1) 對任意的 $a \in R$, $-(-a) = a$.

(2) 若 $a, b \in R$ 則存在一個唯一的 $c \in R$ 滿足 $a + c = b$.

**Proof.** 請參考 Theorem 1.2.3 及 Corollary 1.2.5. □

再次強調 $-(-a) = a$ 的性質僅表示 $-a$ 在加法之下的 inverse 為 $a$, 並沒有 '負負得正' 的意思.

(R6) 和 (R7) 說明 $R$ 中乘法 $(\cdot)$ 這個運算本身的要求. 注意這裡我們並未要求乘法的 identity 必須存在. 不過若一個 ring 對於乘法其 identity 存在的話, 即使在乘法之下 $R$ 不一定會是一個 group 但利用和 Proposition 1.2.1 相同的証明我們可知此 identity 必唯一. 習慣上我們會用 1 來表示這一個乘法上的 identity (注意: 這裡的 1 並不一定是大家常看到整數或實數上的 1). 如果一個 ring $R$ 其乘法的 identity 存在, 那麼我們就會特別說明而稱 $R$ 是一個 *ring with* 1.

另外 (R6) 和 (R7) 也沒要求 $a \cdot b = b \cdot a$. 如果一個 ring $R$ 中對所有的 $a, b \in R$ 皆滿足 $a \cdot b = b \cdot a$, 我們也會特別說明而稱 $R$ 是一個 *commutative ring* (注意: 不是 abelian ring 這個名稱). 在大學的基礎代數中我們會比較專注於 commutative ring with 1 這一種 ring.

最後 (R8) 就是結合 ring 的加法和乘法的橋樑. 也是因為它讓 ring 擁有很多漂亮的性質, 我們在下一節會看到一些利用 (R8) 所得的 ring 的性質. 這裡要注意的是 ring 不一定是 commutative ring, 所以對於兩邊的分配率我們都要要求.

## 5.2. 由 Ring 的定義所得的性質

在這節中我們介紹一些直接用 ring 的定義 (尤其是分配率) 就可推得的基本性質.

若 $R$ 是一個 ring, 其加法的 identity 我們曾經提過習慣上是用 0 來表示. 雖然這一個 0 並非大家熟悉的那個 0 不過就因為它和大家熟悉的 0 有許多共通的性質, 所以我們用 0 來表示它. 哪些共通的性質呢? 除了 $a + 0 = 0$ 與 $a + x = a \Rightarrow x = 0$ 外, 以下的 Lemma 大家應也很熟悉吧!

**Lemma 5.2.1.** 若 $R$ 是一個 *ring* 且 0 是其加法的 *identity,* 則對任意的 $a \in R$ 皆有

$$a \cdot 0 = 0 \cdot a = 0.$$

**Proof.** 大家應可以觀察出 0 是和加法有關的, 而 $a \cdot 0$ 又和乘法有關, 所以不難想像這個 Lemma 一定和分配率有關.

由於 0 是加法的 identity, 故由 (R3) 知 $0+0=0$. 因此由 (R8) 得:

$$a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0.$$

然而由 (R3) 知: $a\cdot 0+0 = a\cdot 0$, 也就是說 $x=0$ 和 $x=a\cdot 0$ 皆為 $a\cdot 0+x=a\cdot 0$ 的解. 故利用 Lemma 5.1.2 (2) 可知 $a\cdot 0=0$.

同理利用 $(0+0)\cdot a = 0\cdot a$ 可得 $0\cdot a = 0$. □

**Remark 5.2.2.** 有的同學或許會利用

$$a\cdot 0 = a\cdot(a-a) = a\cdot a - a\cdot a = 0 \tag{5.1}$$

這一個等式來證明 Lemma 5.2.1. 式子 (5.1) 其實是有問題的. 問題發生在 $R$ 中並沒有「$-$」這一個運算. 換句話說大家習慣寫的 $0=a-a$ 應該寫成 $0=a+(-a)$. 因此式子 (5.1) 應該改寫成

$$a\cdot 0 = a\cdot(a+(-a)) = a\cdot a + a\cdot(-a).$$

然而 $a\cdot a+a\cdot(-a)$ 會等於 0 嗎? 若是 0 就表示 $a\cdot(-a)$ 應該是 $a\cdot a$ 的加法 inverse, 也就是 $a\cdot(-a) = -(a\cdot a)$. 這一點到目前為止我們還不知道是對還是錯 (見 Lemma 5.2.3). 所以這並不能證明 Lemma 5.2.1.

到底我們熟悉的 $a\cdot(-a) = -(a\cdot a)$ 對嗎? 下一個 Lemma 告訴我們其實是對的.

**Lemma 5.2.3.** *若 $R$ 是一個 ring, 則對任意的 $a, b\in R$ 皆有*

$$a\cdot(-b) = (-a)\cdot b = -(a\cdot b).$$

**Proof.** 首先分清楚 $a\cdot(-b)$ 是 $a$ 乘上 $b$ 的加法 inverse, $-a\cdot b$ 是 $a$ 的加法 inverse 乘上 $b$ 而 $-(a\cdot b)$ 是 $a\cdot b$ 的加法 inverse. 所以要證明 $a\cdot(-b) = -(a\cdot b)$ 我們只要證明 $(a\cdot(-b))+(a\cdot b)=0$. 然而利用 (R8) 和 Lemma 5.2.1 知

$$(a\cdot(-b))+(a\cdot b) = a\cdot((-b)+b) = a\cdot 0 = 0,$$

故得證. 同理可得 $(-a)\cdot b = -(a\cdot b)$. □

在一般的 ring, $R$ 中 $-a$ 不一定可以寫成 $(-1)\cdot a$. 主要的原因是 1 不一定在 $R$ 中, 所以 $-1$ 不一定在 $R$ 中. 因此有可能在 $R$ 中 $(-1)\cdot a$ 是沒有意義的. 不過如果 $R$ 是一個 ring with 1, 則利用 Lemma 5.2.3 我們確實可得

$$(-1)\cdot a = 1\cdot(-a) = -a \quad \text{且} \quad a\cdot(-1) = -(a\cdot 1) = -a.$$

利用 Lemma 5.2.3 我們可以得到以下大家熟悉的等式.

**Corollary 5.2.4.** *若 $R$ 是一個 ring 且 $a, b\in R$ 則*

$$(-a)\cdot(-b) = a\cdot b.$$

**Proof.** 先把 $-b$ 看成是一元素, 故利用 Lemma 5.2.3 可得 $(-a)\cdot(-b) = -(a\cdot(-b))$. 然而在套用一次 Lemma 5.2.3 得 $a\cdot(-b) = -(a\cdot b)$. 結合以上二等式得

$$(-a)\cdot(-b) = -(-(a\cdot b)).$$

最後利用 Lemma 5.1.2 (1) 知 $-(-(a\cdot b)) = a\cdot b$, 故得證 $(-a)\cdot(-b) = a\cdot b$. □

由 Lemma 5.2.3 和 Corollary 5.2.4 我們知道「$-$」的運算和我們一般熟悉的運算相同, 以後我們將依習慣將 $a+(-b)$ 寫成 $a-b$.

大家初次看到 ring 的定義時或許會疑惑加法的結構中為何要求是一個 abelian group? 事實上如果當初僅要求加法是一個 group 但乘法有 identity 1, 則這會'強迫' $R$ 在加法之下是一個 abelian group. 這是因為對任意的 $a, b \in R$, 考慮 $(a+b)\cdot(1+1)$ 我們會有以下兩個等式:

$$(a+b)\cdot(1+1) = a\cdot(1+1) + b\cdot(1+1) = (a+a)+(b+b),$$

$$(a+b)\cdot(1+1) = (a+b)\cdot 1 + (a+b)\cdot 1 = (a+b)+(a+b).$$

也就是說 $a+a+b+b = a+b+a+b$, 故可得 $a+b = b+a$.

最後我們要注意的是: 當 $n$ 是一個正整數時, 為了方便一般我們會習慣用 $na$ 來表示 $n$ 個 $a$ 相加所得之值. 例如 $2a = a+a$, $3a = a+a+a$, ... 等. 不過千萬不要把 $2a$ 寫成 $2\cdot a$, $na$ 寫成 $n\cdot a$. 這是因為 2 或是其他的 $n$ 不一定會在 $R$ 中, 所以 $n$ 和 $a$ 是不能相乘的. 那麼對任意的正整數 $n$ 和 $m$, 我們一般熟悉的 $(na)\cdot(mb) = (nm)(a\cdot b)$ 會對嗎? 這是沒有問題的, 你將 $na$ 寫成 $n$ 個 $a$ 相加, $mb$ 寫成 $m$ 個 $b$ 相加, 再利用分配率 (R8) 自然可的 $nm$ 個 $a\cdot b$ 相加.

## 5.3. Zero Divisor 和 Unit

我們已經知道一個 ring 中的任意元素乘上 0 等於 0, 不過在一般的 ring 中有可能存在兩個不等於 0 的元素相乘以後等於 0. 另外在一般的 ring 中有可能有些元素沒有乘法的 inverse, 所以有乘法 inverse 的元素就顯得很特別了. 在這一節中我們將討論這兩種特別的元素.

**Definition 5.3.1.** 令 $R$ 是一個 ring. 如果 $a \neq 0$ 是 $R$ 中一個元素且在 $R$ 中存在 $b \neq 0$ 使得 $a\cdot b = 0$ 或 $b\cdot a = 0$, 則稱 $a$ 是 $R$ 的一個 *zero-divisor*.

當然了在定義裡的 $b$ 也是 $R$ 的 zero-divisor.

**Example 5.3.2.** 相信大家都很了解

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$$

這一個 abelian group. $\overline{a}+\overline{b}$ 的取值是取 $a+b$ 除以 6 的餘數. 例如 $\overline{2}+\overline{5} = \overline{1}$. 相同的我們也可以在 $\mathbb{Z}/6\mathbb{Z}$ 中定一個乘法. $\overline{a}\cdot\overline{b}$ 的值就是 $a\cdot b$ 除以 6 的餘數. 例如 $\overline{2}\cdot\overline{5} = \overline{4}$. 大家很容易檢查在這樣的加法和乘法之下 $\mathbb{Z}/6\mathbb{Z}$ 是一個 ring. 其中 $\overline{0}$ 是 $\mathbb{Z}/6\mathbb{Z}$ 的 0 (加法的 identity). 因為 $\overline{2} \neq \overline{0}$ 且 $\overline{3} \neq \overline{0}$, 但 $\overline{2}\cdot\overline{3} = \overline{0}$. 故由定義知 $\overline{2}$ 和 $\overline{3}$

是 $\mathbb{Z}/6\mathbb{Z}$ 的 zero-divisor. 又因 $\overline{4}\cdot\overline{3}=\overline{0}$, 所以 $\overline{4}$ 也是 zero-divisor. 另外我們可以檢查 $\overline{1}$ 和 $\overline{5}$ 乘上不等於 $\overline{0}$ 的元素都不會等於 $\overline{0}$, 所以我們知 $\overline{1}$ 和 $\overline{5}$ 都不是 $\mathbb{Z}/6\mathbb{Z}$ 的 zero-divisor.

當 $a$ 是一個 zero-divisor 時, 很不好的事會發生: 就是很可能 $a\cdot x=a\cdot y$ 但是 $x\neq y$ (或是 $x\cdot a=y\cdot a$ 但是 $x\neq y$). 例如在 $\mathbb{Z}/6\mathbb{Z}$ 中我們不難發現 $\overline{2}\cdot\overline{1}=\overline{2}\cdot\overline{4}=\overline{2}$. 會導致這樣的是發生是因為若 $a$ 是 zero-divisor, 假設 $b\neq 0$ 滿足 $a\cdot b=0$ (或 $b\cdot a=0$). 則

$$a\cdot(b+c)=a\cdot b+a\cdot c=0+a\cdot c=a\cdot c$$
$$(\text{或 } (b+c)\cdot a=b\cdot a+c\cdot a=0+c\cdot a=c\cdot a),$$

但是由於 $b\neq 0$, 故 $b+c\neq c$.

當 $a$ 不是 zero-divisor 時, 上面所說的不好情況就不會發生.

**Lemma 5.3.3.** 當 $a\in R$ 不是 *ring* $R$ 中的 *zero-divisor* 時, 若 $a\cdot b=a\cdot c$ 或 $b\cdot a=c\cdot a$, 則 $b=c$.

**Proof.** 假如 $a\cdot b=a\cdot c$, 即 $a\cdot b-a\cdot c=0$. 由 Lemma 5.2.3 知 $-(a\cdot c)=a\cdot(-c)$ 故

$$0=a\cdot b-a\cdot c=a\cdot b+a\cdot(-c)=a\cdot(b-c).$$

然而 $a$ 不是 zero-divisor, 因此若 $b-c\neq 0$, 則 $a\cdot(b-c)\neq 0$. 故由此知 $b-c=0$, 也就是說 $b=c$. 同理可證若 $b\cdot a=c\cdot a$, 則 $b=c$. □

總之, 當你在處理 ring 的問題時發現 $a\neq 0$ 且 $a\cdot b=a\cdot c$ 你不可以馬上下結論說 $b=c$, 除非你知道這個 ring 中沒有 zero-divisor. 所以一個沒有 zero-divisor 的 ring 值得特別給它一個名子.

**Definition 5.3.4.** 如果 $R$ 是一個 ring 且 $R$ 中沒有 zero-divisor, 則稱 $R$ 是一個 *domain*. 如果 $R$ 是一個 commutative ring with 1 且是一個 domain, 則稱之為一個 *integral domain*.

整數 $\mathbb{Z}$ 所形成的 ring 就是最典型的 integral domain.

若 $R$ 是一個 ring with 1, 則 $R$ 中有可能存在元素它的乘法 inverse 也在 $R$ 中. 這樣的元素也有很特別的性質.

**Definition 5.3.5.** 若 $R$ 是一個 ring with 1, 如果 $a\in R$ 且存在 $b\in R$ 使得 $a\cdot b=b\cdot a=1$, 則稱 $a$ 是 $R$ 的一個 *unit*.

當然了在定義裡的 $b$ 也是 $R$ 的 unit. 利用 Proposition 1.2.2 一樣的證明我們可以得到這個 $b$ 在 $R$ 中是唯一的. 所以當 $a$ 是一個 unit 時我們通常會用 $a^{-1}$ 表示其乘法的 inverse.

**Example 5.3.6.** 在 $\mathbb{Z}/6\mathbb{Z}$ 這個 ring 中 $\overline{1}$ 是 $\mathbb{Z}/6\mathbb{Z}$ 的 1 (乘法的 identity). 因 $\overline{5}\cdot\overline{5}=\overline{1}$, 故 $\overline{1}$ 和 $\overline{5}$ 是 unit. 其他的元素 $\overline{0},\overline{2},\overline{3},\overline{4}$ 都不是 unit.

Unit 有以下很好的性質:

**Lemma 5.3.7.** *若 $R$ 是一個 ring with 1 且 $a \in R$ 是一個 unit, 則*

(1) *$a$ 絕對不會是 0, 也不會是 $R$ 中的一個 zero-divisor.*

(2) *對任意的 $b \in R$, 方程式 $a \cdot x = b$ 和 $y \cdot a = b$ 在 $R$ 中都會有唯一的解.*

**Proof.** (1) 若 $a = 0$, 則由 Lemma 5.2.1 知 $a$ 乘上 $R$ 中任何的元素都等於 0, 故不可能找到一元素 $b$ 使得 $a \cdot b = 1$. 此和 $a$ 是 unit 矛盾, 所以 $a \neq 0$.

如果 $a$ 是一個 zero divisor, 表示存在 $c \neq 0$ 使得 $a \cdot c = 0$ 或 $c \cdot a = 0$. 假設是 $a \cdot c = 0$, 由假設 $a$ 是 unit 知 $a^{-1} \in R$, 故得

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

此和 $c \neq 0$ 矛盾, 故知 $a$ 不是 zero-divisor. 同理可證 $c \cdot a = 0$ 的情況.

(2) 對任意 $b \in R$, 由假設 $a$ 是 unit 知 $a^{-1} \in R$, 故令 $x = a^{-1} \cdot b \in R$ 可得

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

若 $x' \in R$ 也滿足 $a \cdot x' = b$, 也就是說 $a \cdot x = a \cdot x'$, 則由 (1) 知 $a$ 不是 zero-divisor 再加上 Lemma 5.3.3 知 $x = x'$. 因此可知 $a \cdot x = b$ 在 $R$ 中存在唯一的解. 同理 $y \cdot a = b$ 在 $R$ 中也有唯一的解. □

我們強調一下, 一個 ring 中的 unit 絕對不是 zero-divisor, 不過若一個元素不是 zero-divisor 並不表示它會是 unit. 例如在 $\mathbb{Z}$ 中 2 不是 zero-divisor, 但它也不是 $\mathbb{Z}$ 的 unit.

由 Lemma 5.3.7 知在 $R$ 中 0 絕對不會是一個 unit. 如果除了 0 以外其他的元素都是 unit 這麼特別的 ring 也值得給它一個特別的名子.

**Definition 5.3.8.** *若 $R$ 是一個 ring with 1 且 $R$ 中非 0 的元素都是 unit, 則稱 $R$ 是一個 division ring. 若 $R$ 是一個 commutative ring 且是一個 division ring, 則稱 $R$ 是一個 field.*

有理數 $\mathbb{Q}$ 所成的 ring 就是一個典型的 field.

最後我們要強調: 如果 $R$ 是一個 division ring, 則由於 $R$ 中的非 0 元素都是 unit 所以都不是 zero-divisor. 因此兩個非 0 元素相乘都不等於 0. 也就是 $R$ 中非 0 的元素所成的集合在乘法之下是封閉的. 再加上這些元素都有乘法的 inverse, 所以 $R$ 中非 0 的元素所成的集合在乘法之下是一個 group. 尤其當 $R$ 是一個 field 時, $R$ 中非 0 的元素所成的集合在乘法之下是一個 abelian group.

## 5.4. Subring

在研究 group 時我們曾經探討過 subgroup. 同樣的對於一個 ring 我們也探討它的 subring.

首先我們給 subring 一個正式的定義.

**Definition 5.4.1.** 若 $R$ 是一個 ring, $S \subseteq R$ 且利用 $R$ 的加法與乘法為其運算 $S$ 也是一個 ring, 則稱 $S$ 是 $R$ 的一個 *subring*.

雖然 $S$ 必須符合 (R1) 到 (R8) 的性質 $S$ 才可成為 $R$ 的一個 subring, 不過和 subgroup 的情況一樣結合率因在 $R$ 中已經符合了所以 (R2) 和 (R7) 是不必檢查的. 另外加法的交換性 (R5) 和分配率 (R8) 也在 $R$ 中已符合了所以我們只要檢查 (R1), (R3), (R4) 和 (R5). 也就是說我們只要檢查 $S$ 在加法之下是否為 $R$ 加法之下的 subgroup 以及 $S$ 在乘法之下是否封閉就可以了. 因此我們有以下之結果.

**Lemma 5.4.2.** 若 $R$ 是一個 *ring*, $S \subseteq R$. 如果對於任意的 $a, b \in S$ 皆有 $a - b \in S$ 且 $a \cdot b \in S$, 則 $S$ 是 $R$ 的 *subring*.

**Proof.** 由 Lemma 1.3.4 知, 若對任意 $a, b \in S$ 皆有 $a - b \in S$, 表示 $S$ 在加法之下是 $R$ 的 subgroup. 再加上 $a \cdot b \in S$ 表示乘法是封閉的, 所以 $S$ 是 $R$ 的一個 subring. □

**Example 5.4.3.** 讓我們考慮 $\mathbb{Z}/6\mathbb{Z}$ 有哪些 subring? 由於 subring 在加法之下一定是 subgroup. 所以我們只要先把 $\mathbb{Z}/6\mathbb{Z}$ 加法的 subgroup 都找出來, 再看看他們是否乘法封閉就可以了. 因 $\mathbb{Z}/6\mathbb{Z}$ 在加法之下是一個 order $6 = 2 \times 3$ 的 abelian group, 由 Lagrange 和 Cauchy 定理 (Theorem 2.2.2 & Theorem 3.3.2) 知其有 order 3 和 order 2 的 subgroups (事實上這可以由 $\mathbb{Z}/6\mathbb{Z}$ 在加法之下是一個 cyclic group 直接看出). 也就是 $\{\overline{0}, \overline{2}, \overline{4}\}$ 和 $\{\overline{0}, \overline{3}\}$ 這兩個 subgroups. 很容易就可以知道這兩個子集合都是乘法封閉的, 所以它們也都是 $\mathbb{Z}/6\mathbb{Z}$ 的 subrings.

在討論 subgroup 時我們提過: 若 $G$ 是一個 group, $H$ 為其 subgroup, 則 $H$ 的 identity 就是 $G$ 的 identity. 所以當 $R$ 是一個 ring 時, 若 $S$ 為其 subring, 則 $S$ 的 0 就是 $R$ 的 0. 不過因 $R$ 和 $S$ 的乘法不一定是 group, 即使 $R$ 有乘法的 identity 1, $S$ 未必會有 1. 縱使 $S$ 有 1, $S$ 的 1 和 $R$ 的 1 也未必相同. 例如前面 Example 5.4.3 中 $\mathbb{Z}/6\mathbb{Z}$ 的 1 是 $\overline{1}$. 而在 $\{\overline{0}, \overline{2}, \overline{4}\}$ 這個 subring 中

$$\overline{0} \cdot \overline{4} = \overline{0}, \quad \overline{2} \cdot \overline{4} = \overline{2}, \quad \overline{4} \cdot \overline{4} = \overline{4},$$

所以 $\overline{4}$ 是 $\{\overline{0}, \overline{2}, \overline{4}\}$ 這個 subring 的 1. 注意這並沒有和前面提過一個 ring 若有乘法的 identity 則其 identity 唯一相違背. $\overline{1}$ 是 $\mathbb{Z}/6\mathbb{Z}$ 中唯一的 1, 而 $\overline{4}$ 是 $\{\overline{0}, \overline{2}, \overline{4}\}$ 中唯一的 1. 只是 $\overline{4}$ 在 $\mathbb{Z}/6\mathbb{Z}$ 中它不再是 1 罷了! (它碰到 $\overline{3}$ 和 $\overline{5}$ 就沒輒了.)

另外大家應也發現 $\overline{4}$ 在 $\mathbb{Z}/6\mathbb{Z}$ 是一個 zero-divisor, 但在 $\{\overline{0}, \overline{2}, \overline{4}\}$ 中卻是一個 unit. 這當然也沒和 Lemma 5.3.7 (1) 相衝突, 因為這是在不同的 ring 之下. 總之, 一個 ring 中的元素很可能在 ring 中和在 subring 中會有截然不同的表現.

## 5.5. 一些 Noncommutative Ring

我們看到很多 commutative ring 的例子. 這一節中我們將介紹一些 noncommutative ring. 由於大學基礎代數中幾乎不談 noncommutative ring, 本節的結果後面的章節並不會用到. 我們僅希望利用這一節的介紹將前面幾節的定義再做一次複習和探討. 同學若對前幾節的內容已深入的了解或是對 noncommutative ring 沒什麼興趣可直接跳過這一節.

**5.5.1. Matrix ring $M_2(R)$.** 令 $R$ 是一個 commutative ring with 1. 考慮集合 $M_2(R)$ 是所有係數在 $R$ 的 $2\times 2$ 矩陣所成的集合, 也就是說 $M_2(R)$ 中的元素都是

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

這種形式其中 $a,b,c,d\in R$. 因為 $R$ 是一個 ring 我們可以定 $M_2(R)$ 中的加法和乘法就是一般矩陣的加法和乘法, 即:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}+\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}=\begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} \quad \text{和}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}=\begin{pmatrix} a\cdot a'+b\cdot c' & a\cdot b'+b\cdot d' \\ c\cdot a'+d\cdot c' & c\cdot b'+d\cdot d' \end{pmatrix}.$$

因為 $R$ 是一個 ring with 1, 不難發現以上的加法和乘法使得 $M_2(R)$ 成為一個 ring, 而且 $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 和 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 分別是 $M_2(R)$ 的 0 和 1. 所以說 $M_2(R)$ 是一個 ring with 1. 不過即使 $R$ 是 commutative, $M_2(R)$ 也不會是 commutative ring. 這可由以下的例子看出:

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{但是} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

(注意: 當我們要說明一個 ring $R$ 是 commutative 時, 我們必須證明對任意的 $a,b\in R$ 皆有 $a\cdot b=b\cdot a$. 不過若要說明 $R$ 是 noncommutative 時, 只要找到一組 $a,b\in R$ 使得 $a\cdot b\neq b\cdot a$ 即可.)

從上面的式子我們知道 $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ 和 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ 是 $M_2(R)$ 的 zero-divisor. 同時在這個例子裡我們也發現在一個 noncommutative ring 中是有可能發生 $a\cdot b=0$ 但 $b\cdot a\neq 0$ 的現象.

接下來我們想找到 $M_2(R)$ 中所有的 zero-divisor 和 unit. 首先觀察以下的式子:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}=\begin{pmatrix} a\cdot d-b\cdot c & 0 \\ 0 & a\cdot d-b\cdot c \end{pmatrix}. \tag{5.2}$$

要注意我們需要 $R$ 是 commutative 式子 (5.2) 才會對. 大家應該對 $a\cdot d-b\cdot c$ 這個值不陌生, 它是 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 的 *determinant*. 通常給一矩陣 $A\in M_2(R)$ 我們用 $\det(A)$ 表示其 determinant. 由於 $R$ 是一個 ring, 所以對任意的 $A\in M_2(R)$, 我們都可得 $\det(A)\in R$. Determinant 還有以下這個重要的性質:

$$\det(A\cdot B)=\det(A)\cdot\det(B),\quad \forall\, A,B\in M_2(R). \tag{5.3}$$

到底 $M_2(R)$ 中有哪些 zero-divisor 呢? 同學可能想到 determinant 為 0 的元素. 沒錯, 當 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 但 $\det(A)=0$ 時, 由於 $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, 由式子 (5.2) 知 $A$ 是一個 zero-divisor.

還有沒有其他的 zero-divisor 呢? 其實當 $\det(A)$ 是 $R$ 的 zero-divisor 時, $A$ 也會是 $M_2(R)$ 的 zero-divisor. 這是因為如果 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 且 $\det(A)=\alpha$ 是 $R$ 的一個 zero-divisor. 設 $\beta \neq 0$ 是 $R$ 中一元素滿足 $\alpha \cdot \beta = 0$. 有以下兩種可能發生:

(1) $a\cdot\beta$, $b\cdot\beta$, $c\cdot\beta$ 和 $d\cdot\beta$ 都等於 0: 此時令 $B=\begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix}$, 如此一來因 $\beta \neq 0$, 所以 $B \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, 但是

$$A\cdot B=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot\begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix}=\begin{pmatrix} a\cdot\beta & b\cdot\beta \\ c\cdot\beta & d\cdot\beta \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

因此在這個情形時, $A$ 是 $M_2(R)$ 的一個 zero-divisor.

(2) $a\cdot\beta$, $b\cdot\beta$, $c\cdot\beta$ 和 $d\cdot\beta$ 不全為 0: 則我們考慮

$$B=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\cdot\begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix}=\begin{pmatrix} d\cdot\beta & -b\cdot\beta \\ -c\cdot\beta & a\cdot\beta \end{pmatrix}\neq\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

然而

$$A\cdot B=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\cdot\begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix},$$

由式子 (5.2) 知

$$A\cdot B=\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}\cdot\begin{pmatrix} \beta & 0 \\ 0 & \beta \end{pmatrix}=\begin{pmatrix} \alpha\cdot\beta & 0 \\ 0 & \alpha\cdot\beta \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

所以在這個情況 $A$ 還是 $M_2(R)$ 的一個 zero-divisor.

那麼當 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 且 $\det(A)=\alpha$ 不是 $R$ 的 zero-divisor 時又會怎樣呢? 假設存在 $B=\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\neq\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (也就是說 $a'$, $b'$, $c'$ 和 $d'$ 不全為 0) 滿足 $A\cdot B=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. 此時考慮 $C=\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, 則由式子 (5.2) 知

$$(C\cdot A)\cdot B=\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}\cdot\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}=\begin{pmatrix} \alpha\cdot a' & \alpha\cdot b' \\ \alpha\cdot c' & \alpha\cdot d' \end{pmatrix}.$$

因為 $\alpha$ 不是 zero-divisor 且 $a'$, $b'$, $c'$ 和 $d'$ 不全為 0, 所以知 $\alpha\cdot a'$, $\alpha\cdot b'$, $\alpha\cdot c'$ 和 $\alpha\cdot d'$ 不全為 0. 也就是說 $(C\cdot A)\cdot B\neq\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. 這和

$$(C\cdot A)\cdot B=C\cdot(A\cdot B)=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

相矛盾, 所以不可能找到 $B \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 滿足 $A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. 同理可知不可能找到 $B \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 滿足 $B \cdot A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. 所以 $A$ 絕對不會是 $M_2(R)$ 的一個 zero-divisor. 因此我們得證:

**Proposition 5.5.1.** 若 $R$ 是一個 *commutative ring* 且 $A \in M_2(R)$, 則 $A$ 是 $M_2(R)$ 的一個 *zero-divisor* 若且唯若 $\det(A) = 0$ 或 $\det(A)$ 是 $R$ 的一個 *zero-divisor.*

由 Proposition 5.5.1 我們知在 $M_2(\mathbb{Z})$ 和 $M_2(\mathbb{Q})$ 中 determinant 為 0 的矩陣會是 zero-divisor, 而 determinant 不為 0 的矩陣就不會是 zero-divisor.

當 $R$ 是 commutative ring with 1 時 $M_2(R)$ 會有哪些 unit 呢? 我們有以下的結果:

**Proposition 5.5.2.** 若 $R$ 是一個 *commutative ring with* 1 且 $A \in M_2(R)$, 則 $A$ 是 $M_2(R)$ 的一個 *unit* 若且唯若 $\det(A)$ 是 $R$ 的一個 *unit.*

**Proof.** 假設 $A$ 是 $M_2(R)$ 的一個 unit, 則存在 $B \in M_2(R)$ 滿足

$$A \cdot B = B \cdot A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

利用式子 (5.3) 得

$$\det(A) \cdot \det(B) = \det(B) \cdot \det(A) = 1.$$

然而 $\det(A), \det(B) \in R$, 故得 $\det(A)$ 是 $R$ 的一個 unit.

反之, 若 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 且 $\det(A) = \alpha$ 是 $R$ 的一個 unit, 則考慮

$$B = \begin{pmatrix} \alpha^{-1} \cdot d & \alpha^{-1} \cdot (-b) \\ \alpha^{-1} \cdot (-c) & \alpha^{-1} \cdot a \end{pmatrix}.$$

因 $\alpha^{-1} \in R$, 我們知 $B \in M_2(R)$. 利用式子 (5.2), 可得

$$A \cdot B = B \cdot A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

因此 $A$ 是 $M_2(R)$ 的一個 unit. □

由 Proposition 5.5.2 知在 $M_2(\mathbb{Z})$ 中惟有 determinant 是 $\pm 1$ 的矩陣才會是 unit, 而在 $M_2(\mathbb{Q})$ 中所有 determinant 不是 0 的矩陣都會是 unit.

**5.5.2. The Hamilton quaternions.** 大家都知道複數 $\mathbb{C}$ 的元素可寫成 $a + b\mathbf{i}$, 其中 $a, b \in \mathbb{R}$ 而 $\mathbf{i} \notin \mathbb{R}$ 滿足 $\mathbf{i}^2 = -1$. 我們都知道如何定 $\mathbb{C}$ 中的加法和乘法, 也就是: 若 $a + b\mathbf{i}, a' + b'\mathbf{i} \in \mathbb{C}$, 則

$$(a + b\mathbf{i}) + (a' + b'\mathbf{i}) = (a + a') + (b + b')\mathbf{i}$$

和

$$(a + b\mathbf{i}) \cdot (a' + b'\mathbf{i}) = aa' + ab'\mathbf{i} + ba'\mathbf{i} + bb'\mathbf{i}^2 = (aa' - bb') + (ab' + ba')\mathbf{i}.$$

不難驗證在此加法和乘法之下 $\mathbb{C}$ 是一個 commutative ring with 1, 其中 $0+0\mathbf{i}$ 和 $1+0\mathbf{i}$ 分別是 $\mathbb{C}$ 的 0 和 1. 利用大家熟悉的式子

$$(a+b\mathbf{i})\cdot(a-b\mathbf{i}) = (a^2+b^2)+0\mathbf{i}, \tag{5.4}$$

我們很容易得到若 $a+b\mathbf{i}\neq 0+0\mathbf{i}$ (即 $a\neq 0$ 或 $b\neq 0$), 則

$$(a+b\mathbf{i})\cdot\left(\frac{a}{a^2+b^2}+\frac{b}{a^2+b^2}\mathbf{i}\right) = 1+0\mathbf{i}.$$

也就是說在 $\mathbb{C}$ 中不等於 0 的數都是 unit, 所以 $\mathbb{C}$ 是一個 field.

利用和由 $\mathbb{R}$ 創造出 $\mathbb{C}$ 類似的方法, Hamilton 引進了下列的數:

$$\mathbb{H} = \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \,|\, a,b,c,d\in\mathbb{R}\},$$

其中 $\mathbf{i},\mathbf{j},\mathbf{k}\neq\mathbb{R}$, 我們稱 $\mathbb{H}$ 為 the *Hamilton quaternions*. 我們可以定 $\mathbb{H}$ 的加法如下: 若 $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}, a'+b'\mathbf{i}+c'\mathbf{j}+d'\mathbf{k}\in\mathbb{H}$, 則

$$(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})+(a'+b'\mathbf{i}+c'\mathbf{j}+d'\mathbf{k}) = (a+a')+(b+b')\mathbf{i}+(c+c')\mathbf{j}+(d+d')\mathbf{k}.$$

要定義 $\mathbb{H}$ 的乘法我們首先定義 $\mathbf{i}$, $\mathbf{j}$ 和 $\mathbf{k}$ 間的乘法如下:

(1) $\mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-1$,

(2) $\mathbf{i}\cdot\mathbf{j}=\mathbf{k}=-\mathbf{j}\cdot\mathbf{i}$,

(3) $\mathbf{j}\cdot\mathbf{k}=\mathbf{i}=-\mathbf{k}\cdot\mathbf{j}$,

(4) $\mathbf{k}\cdot\mathbf{i}=\mathbf{j}=-\mathbf{i}\cdot\mathbf{k}$.

對任意的 $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}, a'+b'\mathbf{i}+c'\mathbf{j}+d'\mathbf{k}\in\mathbb{H}$, 我們定其相乘為一項一項用分配率展開再將 '實數項' 及 $\mathbf{i},\mathbf{j},\mathbf{k}$ 項的係數合併. 也就是說

$$(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})\cdot(a'+b'\mathbf{i}+c'\mathbf{j}+d'\mathbf{k}) = \alpha+\beta\mathbf{i}+\gamma\mathbf{j}+\delta\mathbf{k},$$

其中

$$\begin{aligned}
\alpha &= aa'-bb'-cc'-dd'\\
\beta &= ab'+ba'+cd'+dc'\\
\gamma &= ac'-bd'+ca'+db'\\
\delta &= ad'+bc'-cb'+da'
\end{aligned}$$

不難驗證在此加法和乘法之下 $\mathbb{H}$ 是一個 ring with 1, 其中 $0+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}$ 和 $1+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}$ 分別是 $\mathbb{H}$ 的 0 和 1. 不過 $\mathbb{H}$ 不再是 commutative ring, 這可以由

$$(0+1\mathbf{i}+0\mathbf{j}+0\mathbf{k})\cdot(0+0\mathbf{i}+1\mathbf{j}+0\mathbf{k}) = 0+0\mathbf{i}+0\mathbf{j}+1\mathbf{k}$$

但

$$(0+0\mathbf{i}+1\mathbf{j}+0\mathbf{k})\cdot(0+1\mathbf{i}+0\mathbf{j}+0\mathbf{k}) = 0+0\mathbf{i}+0\mathbf{j}-1\mathbf{k}$$

看出. 大家很容易就可證出, $\mathbb{H}$ 也有類似式子 (5.4) 的重要等式:

$$(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})\cdot(a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}) = (a^2+b^2+c^2+d^2)+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}. \tag{5.5}$$

利用式子 (5.5) 我們可以看出, 若 $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \neq 0+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}$ (即 $a,b,c,d$ 不全為 0), 令 $\lambda = a^2+b^2+c^2+d^2$, 則

$$(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})\cdot(\frac{a}{\lambda}-\frac{b}{\lambda}\,\mathbf{i}-\frac{c}{\lambda}\,\mathbf{j}-\frac{d}{\lambda}\,\mathbf{k}) = 1+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}.$$

也就是說在 $\mathbb{H}$ 中不等於 0 的數都是 unit, 所以 $\mathbb{H}$ 是一個 noncommutative division ring.

如果大家不健忘的話, 應該記得 $\{\pm 1 \pm \mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ 就是我們在 4.7 節介紹的 quaternion group $Q_8$. 事實上對任意的 group 你都可以用類似的方法建構出一個 ring, 這樣的 ring 我們稱為 *group ring*.