大學基礎代數

李華介

國立台灣師範大學數學系

Part II

RING

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 2×2 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 α 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 ± 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*.

Chapter 6

中級 Ring 的性質

這一章中我們將介紹一些更進一步的 ring 的理論, 包括 ideals, quotient ring 以及三個 isomorphism theorems.

6.1. Ideals 和 Quotient Rings

我們在學習 group 時知道一個 group 的 subgroup 中有一種特別的 subgroup 在處理 group 的問題時特別好用, 就是 normal subgroup. 同樣的在一個 ring 中的 subring 裡, 也有一種很特別的 subring, 我們稱之為 ideal.

我們回憶一下, normal subgroup 之所以比一般的 subgroup 好用在於可以利用它得到一個新的 group 稱之為 quotient group. 也就是說對所有 G 的 subgroup H, 我們可以將 G 用 H 來分類, 然後將同類的元素看成一個新的元素. 不過這些新的元素間一般我們無法定義一個運算讓它成為一個 group, 除非 H 是 G 的一個 normal subgroup. 現在, 若 R 是一個 ring 且 S 是 R 的 subring, 由於 R 在加法之下是一個 abelian group, 而 S 在加法之下是 R 的一個 subgroup, 利用 abelian group 的 subgroup 都是 normal subgroup, 我們當然有 R/S 這一個加法之下的 quotient group. 我們當然還希望 R/S 中也有乘法, 這樣就可能得到一個新的 ring 了. 要怎樣在 R/S 中定一個和 R 的乘法相關的乘法呢? 我們可以學 2.4 節的方法來處理.

首先必須了解 R/S 中的元素長什麼樣子. 任取 R/S 中的一個元素都可以用 $\overline{a}$ 來表示, 其中 $a \in R$ 而 $\overline{a}$ 是將 R 中所有和 a 同類的元素看成是一個元素. 怎樣的元素會和 a 同類呢? 別忘了這裡我們是用加法所以依定義 a 和 a' 同類若且唯若 $a - a' \in S$. 現在若 $\overline{a}, \overline{b} \in R/S$, 因 S 在加法之下是 R 的 normal subgroup, 由前面知我們自然可定

$$\overline{a} + \overline{b} = \overline{a + b}.$$

我們當然希望定的乘法是

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

不過這樣定的乘法可能會有問題. 問題發生於 $\overline{a}$ 在 R/S 中表示法並不唯一, 也就是說存在 $a' \in R$ 且 $a' \neq a$ 滿足 $\overline{a} = \overline{a'}$ (只要 $a - a' \in S$ 就可). 因此我們要問的是: 如果 $\overline{a} = \overline{a'}$ 且 $\overline{b} = \overline{b'}$ 會不會發生 $\overline{a \cdot b} \neq \overline{a' \cdot b'}$ 的現象? 萬一發生了我們定的乘法就有問題.

S 要有怎樣的性質 R/S 上定的乘法才不會有問題呢? 也就是任取 $r, r' \in R$ 以及 $s, s' \in S$ 我們有 $\overline{r} = \overline{r+s}$ 且 $\overline{r'} = \overline{r'+s'}$ 因此 $\overline{r \cdot r'} = \overline{(r+s) \cdot (r'+s')}$ 表示 $r \cdot r'$ 和 $(r+s) \cdot (r'+s')$ 在 S 的分類之下是相同的. 換句話說: 我們要求

$$(r+s) \cdot (r'+s') - r \cdot r' = r \cdot s' + s \cdot r' + s \cdot s' \in S. \tag{6.1}$$

由於 S 是一個 subring, 當然得 $s \cdot s' \in S$, 因此式子 (6.1) 等同於要求對任意的 $r, r' \in R$ 及 $s, s' \in S$ 皆需符合

$$r \cdot s' + s \cdot r \in S \tag{6.2}$$

分別代 $s = 0$ 及 $s' = 0$ 的情況於式子 (6.2), 我們知這等同於要求對任意的 $r \in R$ 及 $s \in S$ 皆需符合

$$r \cdot s \in S \quad \text{且} \quad s \cdot r \in S.$$

因此我們自然有以下之定義:

Definition 6.1.1. 若 I 是 R 的一個 subring 且符合對任意的 $r \in R$ 及 $a \in I$ 皆有

$$r \cdot a \in I \quad \text{且} \quad a \cdot r \in I,$$

則稱 I 為 R 的一個 *ideal*.

雖然一個 ring 的 ideal 必須是一個 ring, 就如同 subring 的情況我們不必檢查 ring 的所有條件, 利用 Lemma 5.4.2 我們有以下判斷 ideal 的方法.

Lemma 6.1.2. 令 R 是一個 *ring*, $I \subseteq R$. 若 I 符合以下兩點, 則 I 是 R 的 *ideal*:

(1) 對於所有的 $a, b \in I$ 皆有 $a - b \in I$.

(2) 對任意的 $a \in I$, $r \in R$ 皆有 $r \cdot a \in I$ 且 $a \cdot r \in I$.

Proof. 若 $a, b \in I$, 則當然 $b \in R$, 故條件 (2) 告訴我們對所有的 $a, b \in I$ 皆有 $a \cdot b \in I$. 結合條件 (1), 利用 Lemma 5.4.2 知 I 是 R 的一個 subring. 因此再由條件 (2) 得 I 是 R 的 ideal. □

現在回到我們考慮 ideal 的真正目的. 若 I 是 R 這個 ring 的 ideal, 我們想利用 R 的 ring 的性質來創造另一個 ring. 首先我們利用 R 在加法之下是 abelian group 且 I 是其 normal subgroup, 用 I 將 R 分類, 然後將同類的元素所成的集合看成一個新的元素. 如此一來這一個分類後的集合 R/I 可定出一個加法, 而且是 abelian group. 然後再用 I 是 ideal 的性質, 給 R/I 乘法的結構. 也就是說若 $\overline{a}$ 是與 a 同類的元素所成的集合, $\overline{b}$ 是與 b 同類的元素所成的集合, 則我們定

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{且} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

以下我們將說明 R/I 在此 $+$ 和 $\cdot$ 之下是一個 ring.

首先利用我們知道的 group 理論, R/I 在 $+$ 之下是一個 abelian group, 也就是說 R/I 符合 (R1) 到 (R5) 這 5 項 ring 的條件. 我們只要檢查 (R6), (R7) 和 (R8) 即可.

(R6): 若 $\overline{a}, \overline{b} \in R/I$, 則由於 $a \cdot b \in R$ 故 $\overline{a \cdot b} \in R/I$. 也就是說 $\overline{a} \cdot \overline{b} \in R/I$.

(R7): 我們要證明 $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$. 然而

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a \cdot b} \cdot \overline{c} = \overline{(a \cdot b) \cdot c},$$

且

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{b \cdot c} = \overline{a \cdot (b \cdot c)}$$

再加上 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ 所以等式成立.

(R8): 同前面的證明, 由於 $a \cdot (b + c) = a \cdot b + a \cdot c$ 當然可得

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}.$$

同理知

$$(\overline{b} + \overline{c}) \cdot \overline{a} = \overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{a}.$$

我們稱 R/I 是 R 的一個 *quotient ring.*

6.2. Subring 和 Ideal 的基本性質

前一節中我們可以看出 normal subgroup 和 group 間的關係相當於 ideal 和 ring 的關係. 所以一些在 group 中有關 normal subgroup 的性質, 在 ring 中也有相對應有關 ideal 的性質. 不過要注意的是從前在 group 我們都是用 $\cdot$ 當運算, 但在 ring 中的 group 運算是用 $+$ 來表示, 所已相對應的性質要將 $\cdot$ 改成 $+$.

我們在 Lemma 2.6.3 中提過: 當 H, H' 是 G 的 subgroup, $H \cdot H'$ 這一個集合未必是 G 的 subgroup, 除非 H 和 H' 中有一個是 G 的 normal subgroup. 在 ring 中也有類似的結果: 一般來說若 S, T 是 R 的 subring, 那麼

$$S + T = \{s + t \,|\, s \in S, t \in T\}$$

未必是 R 的 subring. 原因是 $S+T$ 中任選兩元素 $s+t$ 和 $s'+t'$, 其乘積 $(s+t)\cdot(s'+t')$ 並不一定可以寫成一個 S 的元素加上一個 T 的元素這種形式, 也就是說當 S 和 T 只是 R 的 subring 時, $S+T$ 不一定是乘法封閉的. 不過當 S, T 其中之一是 R 的 ideal 時, $S+T$ 就乘法封閉了!

Lemma 6.2.1. 令 R 是一個 *ring,* S, T 是 R 的 *subring.*

(1) 若 S 是 R 的 *ideal,* 則 $S+T$ 是 R 的 *subring.*

(2) 若 S 和 T 都是 R 的 *ideal,* 則 $S+T$ 是 R 的 *ideal.*

Proof. (1) 利用加法的 group 性質, 我們知若 $a = s + t, b = s' + t' \in S + T$ 其中 $s, s' \in S$ 且 $t.t' \in T$, 則

$$a - b = (s + t) - (s' + t') = (s - s') + (t - t') \in S + T.$$

另外

$$a \cdot b = (s + t) \cdot (s' + t') = s \cdot s' + s \cdot t' + t \cdot s' + t \cdot t'.$$

由於 S 和 T 是 R 的 subring, 故 $s \cdot s' \in S$ 且 $t \cdot t' \in T$. 又因 S 是 R 的 ideal 且 $t, t' \in R$, 故 $s \cdot t' \in S$ 且 $t \cdot s' \in S$. 因此知 $s \cdot s' + s \cdot t' + t \cdot s' \in S$ 所以 $(s + t) \cdot (s' + t') \in S + T$. 故由 Lemma 5.4.2 知 $S + T$ 是 R 的 subring.

(2) 若 S 和 T 是 R 的 ideal, 則對任意的 $r \in R$, $s \in S$ 及 $t \in T$ 我們皆有 $r \cdot s$, $s \cdot r \in S$ 且 $r \cdot t$, $t \cdot r \in T$. 因此

$$r \cdot (s + t) = r \cdot s + r \cdot t \in S + T$$

且

$$(s + t) \cdot r = s \cdot r + t \cdot r \in S + T.$$

故由 Lemma 6.1.2 知 $S + T$ 是 R 的 ideal. □

我們在討論 group 時曾談過兩個 subgroup 的交集依然是 subgroup, 而兩個 normal subgroup 的交集也是 normal subgroup. 在 ring 的情況我們也有類似情形.

Lemma 6.2.2. 令 R 是一個 *ring,* S, T 是 R 的 *subring.*

(1) $S \cap T$ 是 R 的 *subring.*

(2) 若 S 和 T 都是 R 的 *ideal,* 則 $S \cap T$ 是 R 的 *ideal.*

Proof. (1) 利用加法的 group 性質我們知若 $a, b \in S \cap T$ 則 $a - b \in S \cap T$. 另又因 $a \in S$ 且 $b \in S$ 故利用 S 的乘法封閉性知 $a \cdot b \in S$, 同理得 $a \cdot b \in T$. 故知 $a \cdot b \in S \cap T$. 因此由 Lemma 5.4.2 知 $S \cap T$ 是 R 的 subring.

(2) 當 S 和 T 皆為 R 的 ideal 時, 對任意的 $r \in R$, $a \in S \cap T$, 由於 $a \in S$, 我們有 $r \cdot a \in S$. 又因 $a \in T$, 所以 $r \cdot a \in T$. 因此得 $r \cdot a \in S \cap T$. 同理得 $a \cdot r \in S \cap T$. 故由 Lemma 6.1.2 知 $S \cap T$ 是 R 的 ideal. □

注意若 S 和 T 若僅有一個為 R 的 ideal, 則 $S \cap T$ 當然還是 R 的 subring. 不過就不見得是 R 的 ideal 了! 另外在 group 時我們知道兩個 subgroup 的聯集不一定是 subgroup, 同理如果 S 和 T 是 R 的 subring, $S \cup T$ 也不一定是 R 的 subring.

既然 ring 中有乘法, 如果 S, T 是 R 的 subring 那麼考慮 $\{s \cdot t \,|\, s \in S, t \in T\}$ 這樣的集合會不會也是 R 的 subring 呢? 事實上若 $s, s' \in S$, $t, t' \in T$, 則 $(s \cdot t) \cdot (s' \cdot t')$ 不見得可以寫成 $s'' \cdot t''$, 其中 $s'' \in S$, $t'' \in T$ 這樣的形式 (除非 R 是 commutative). 不過即使 R 是 commutative, $s \cdot t + s' \cdot t'$ 也不見得可以寫成 $s'' \cdot t''$, 其中 $s'' \in S$,

$t'' \in T$. 所以如果考慮 $\{s \cdot t \,|\, s \in S, t \in T\}$ 這樣的集合是無法達到加法封閉的要求. 我們應考慮以下之集合

$$\{\sum_{i=1}^{n} s_i \cdot t_i \,|\, s_i \in S, t_i \in T, \text{ for some } n \in \mathbb{N}\}.$$

一般我們會將以上的集合記作 $S \cdot T$. 簡單來說, 每一個 $S \cdot T$ 的元素都可寫成有限多項的 S 中元素乘上 T 中元素的和.

Lemma 6.2.3. 令 R 是一個 *ring*, S 和 T 都是 R 的 *ideal*, 則 $S \cdot T$ 是 R 的 *ideal*.

Proof. 若 $a = s_1 \cdot t_1 + \cdots + s_n \cdot t_n$ 和 $b = s'_1 \cdot t'_1 + \cdots + s'_m \cdot t'_m$ 是 $S \cdot T$ 中任意的兩元素, 則

$$a - b = s_1 \cdot t_1 + \cdots + s_n \cdot t_n + (-s'_1) \cdot t'_1 + \cdots + (-s'_m) \cdot t'_m$$

仍可寫成有限多項的 S 中元素乘上 T 中元素的和. 故 $a - b \in S \cdot T$.

另外對任意的 $r \in R$,

$$r \cdot a = r \cdot \big(\sum_{i=1}^{n} s_i \cdot t_i\big) = \sum_{i=1}^{n} (r \cdot s_i) \cdot t_i.$$

由於 $s_i \in S$ 且 S 是 R 的 ideal, 所以 $r \cdot s_i \in S$. 因此 $r \cdot a$ 仍可寫成有限多項的 S 中元素乘上 T 中元素的和. 故 $r \cdot a \in S \cdot T$. 同理知 $a \cdot r \in S \cdot T$. 故由 Lemma 6.1.2 知 $S \cdot T$ 是 R 的 ideal. □

我們已看到許多有關 ideal 和 subring 的差異, 一般來說 subring 因其條件較少所以較難控制. 例如一個 subring 可能含有原本 ring 中的 unit ($\mathbb{Z}$ 是 $\mathbb{Q}$ 的 subring, 且 $1 \in \mathbb{Z}$), 但對 ideal 來說這就絕不可能發生了!

Lemma 6.2.4. 設 R 是一個 *ring with* 1, 且 I 為 R 的一個 *ideal*. 若在 I 中存在 $u \in I$ 是 R 的一個 *unit*, 則 $I = R$. 尤其當 R 是一個 *division ring* 時, R 的 *ideal* 就只有 $\{0\}$ 和 R 本身.

Proof. 因 I 是 R 的 ideal, 我們自然有 $I \subseteq R$. 現任取 $r \in R$, 因 u 是 R 的一個 unit, 由 Lemma 5.3.7 知存在 $r' \in R$ 滿足 $r' \cdot u = r$. 然而 $u \in I$, 由 ideal 的性質知 $r' \cdot u = r \in I$. 因此知 $R \subseteq I$, 故得 $R = I$.

現在若 R 是一個 division ring, 依定義, 任意 R 中的非 0 元素都是 unit. 故若 I 是 R 中一個不為 $\{0\}$ 的 ideal, 即 I 中存在非 0 的元素, 故由前面的結果知 $R = I$. □

通常依慣例, 我們會稱 R 和 $\{0\}$ 是 R 的 *trivial ideals*, 除此以外的 ideal 就稱為 *nontrivial proper ideal*. Lemma 6.2.4 告訴我們一個 division ring 中沒有 nontrivial proper ideal (不過當然有可能有 proper subring).

最後我們回顧一下在 Remark 2.4.2 中我們曾提到 subgroup 和 normal subgroup 相互之間要注意的事項, 同樣的對於 subring 和 ideal 我們也要注意以下事項:

假設 R 是一個 ring 且 $T \subseteq S \subseteq R$.

(1) 如果已知 S 是 R 的 subring 且 T 是 S 的 subring, 那麼 T 是 R 的 subring.

(2) 如果已知 S 是 R 的 subring 且 T 是 R 的 ideal , 那麼 T 也會是 S 的 ideal.

(3) 如果已知 S 是 R 的 subring 而 T 是 S 的 ideal, 那麼 T 不一定是 R 的 ideal.

(4) 如果已知 S 在 R 的 ideal 且 T 在 S 的 ideal, 那麼 T 不一定是 R 的 ideal.

6.3. Ring Homomorphism 和 Correspondence 定理

我們曾經利用 group homomorphism 來描繪兩個 group 之間的關係. 同樣的 ring 之間也有所謂的 ring homomorphism, 而 correspondence 定理就告訴我們如何由 ring homomorphism 來描繪兩個 ring 間 ideal 的關係.

Definition 6.3.1. 當 R, R' 是 rings 而 $\phi : R \to R'$ 是從 R 映射到 R' 的函數. 如果 ϕ 滿足對於所有 $a, b \in R$ 皆有

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{且} \quad \phi(a \cdot b) = \phi(a) \cdot \phi(b),$$

則稱此函數 ϕ 是一個 ring homomorphism.

要注意的是: 因為 $a, b \in R$, 所以這裡 $a+b$, $a \cdot b$ 是在 R 中的加法和乘法; 而 $\phi(a), \phi(b) \in R'$, 所以 $\phi(a)+\phi(b)$, $\phi(a)\cdot\phi(b)$ 是在 R' 中的加法和乘法. 簡單地說: 一個從 R 到 R' 的 ring homomorphism, 是加法的 group homomorphism 再加上保持乘法的運算. 所以一般來說有關於 group homomorphism 的性質都可以直接套用在 ring homomorphism 上. 比方說由 Lemma 2.5.2 知 $\phi(0) = 0$ (其中 ϕ 裡面的 0 是 R 的 0, 另一個 0 是 R' 的 0) 且 $\phi(-a) = -\phi(a)$. 因此以後要計算 $\phi(a-b)$ 時由於

$$\phi(a-b) = \phi(a+(-b)) = \phi(a) + \phi(-b) = \phi(a) + (-\phi(b)),$$

我們會直接寫成

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

在 group homomorphism 中我們介紹了兩個重要的集合 image 和 kernel, 在 ring homomorphism 這兩個集合仍然很重要. 我們再回顧一下它們的定義.

Definition 6.3.2. 若 $\phi : R \to R'$ 是一個 group homomorphism, 則

$$\mathrm{im}(\phi) = \{\phi(a) \in R' \,|\, a \in R\}$$

稱為 ϕ 的 *image.*

$$\ker(\phi) = \{a \in R \,|\, \phi(a) = 0\},$$

稱為 ϕ 的 *kernel.*

注意這裡 kernel 中的 0 是 R' 加法的 identity. 在 group homomorphism 中 image 和 kernel 分別是對應域的 subgroup 和定義域的 normal subgroup. 大家應不難猜出在 ring homomorphism 它們的性質吧!

Lemma 6.3.3. 若 $\phi : R \to R'$ 是一個 *ring homomorphism,* 則 $\mathrm{im}(\phi)$ 是 R' 的 *subring,* 而 $\ker(\phi)$ 是 R 的 *ideal.*

Proof. 我們利用 Lemma 2.5.4 直接知 $\mathrm{im}(\phi)$ 和 $\ker(\phi)$ 分別是 R' 和 R 加法之下的 subgroup. 所以我們只要驗證乘法.

若 $\phi(a), \phi(b) \in \mathrm{im}(\phi)$, 其中 $a, b \in R$, 則 $\phi(a) \cdot \phi(b) = \phi(a \cdot b)$. 又因 $a \cdot b \in R$, 故 $\phi(a) \cdot \phi(b) \in \mathrm{im}(\phi)$. 因此由 Lemma 5.4.2 知 $\mathrm{im}(\phi)$ 是 R' 的 subring.

至於 $\ker(\phi)$ 是 R 的 ideal, 我們只要證: 對任意的 $r \in R$ 和 $a \in \ker(\phi)$ 皆有 $r \cdot a \in \ker(\phi)$ 及 $a \cdot r \in \ker(\phi)$. 然而 $\phi(r \cdot a) = \phi(r) \cdot \phi(a) = \phi(r) \cdot 0$, 利用 Lemma 5.2.1 知 $\phi(r \cdot a) = 0$ 故 $r \cdot a \in \ker(\phi)$. 同理得 $a \cdot r \in \ker(\phi)$. 因此由 Lemma 6.1.2 知 $\ker(\phi)$ 是 R 的 ideal. □

在 Lemma 2.5.6 中我們知道可以用 kernel 來判斷一個 group homomorphism 是否為一對一, 既然 ring homomorphism 在加法之下是 group homomorphism 所下面的 Lemma 當然成立.

Lemma 6.3.4. 已知 $\phi : R \to R'$ 是一個 *ring homomorphism,* 則 ϕ 是一個 *monomorphism* (即一對一) 若且唯若 $\ker(\phi) = \{0\}$.

瞭解了 ring homomorphism, 接下來我們來談 ring homomorphism 的 correspondence 定理. 回顧一下 group homomorphism 中的 correspondence 定理描述了兩個 group 的 subgroup 和 normal subgroup 利用 group homomorphism 所得到的對應關係. 對 ring homomorphism 我們也有類似狀況.

Theorem 6.3.5 (Correspondence Theorem)**.** 若 $\phi : R \to R'$ 是一個 *onto* 的 *ring homomorphism.* 若 S' 是 R' 的 *subring* 且令

$$S = \{a \in R \,|\, \phi(a) \in R'\},$$

則 S 是 R 的一個 *subring* 且 $S \supseteq \ker(\phi)$. 另外若令

$$\phi(S) = \{\phi(a) \,|\, a \in S\},$$

則 $\phi(S) = S'$.

如果又假設 S' 是 R' 的 *ideal.* 則前面所定的 S 也會是 R 的 *ideal.*

Proof. 首先先證 S 是 R 的 subring. 若 $a, b \in S$, 我們要證明 $a - b \in S$ 且 $a \cdot b \in S$. 由定義知 $a, b \in S$ 表示 $\phi(a) \in S'$ 且 $\phi(b) \in S'$, 故 $\phi(a) - \phi(b) \in S'$ 且 $\phi(a) \cdot \phi(b) \in S'$. 又因 ϕ 是 ring homomorphism, 故 $\phi(a - b) = \phi(a) - \phi(b)$ 且 $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. 因此 $\phi(a - b) \in S'$ 且 $\phi(a \cdot b) \in S'$, 也就是說 $a - b \in S$ 且 $a \cdot b \in S$. 故知 S 是 R 的 subring. (注意這個部分的證明只用到 ϕ 是 ring homomorphism, 並不需要 onto.)

若 $a \in \ker(\phi)$, 則 $\phi(a) = 0$. 因 $0 \in S'$ 故 $a \in S$. 所以 $\ker(\phi) \subseteq S$. (這部分的證明也不需 onto.)

現在證 $\phi(S) = S'$. 首先證明 $\phi(S) \subseteq S'$ 這部份是容易的. 主要是因 $\phi(S)$ 的元素都是 $\phi(a)$ 這種形式, 其中 $a \in S$. 由定義 $a \in S$, 表示 $\phi(a) \in S'$. 故 $\phi(S)$ 的元素都落在 S' 中. 很多同學都會認為 S' 的元素也會在 $\phi(S)$ 中; 一般這是不一定對的. 因為在一般的情況 $b \in S'$ 不代表有元素 $a \in R$ 使得 $\phi(a) = b$. 這裡我們就要用到 onto 的性質了. 因為 ϕ 是 onto 故對任意 $b \in S' \subseteq R'$ 都可找到 $a \in R$ 使得 $\phi(a) = b$. 既然 $\phi(a) = b \in S'$, 這一個 a 也就在 S 中了. 所以 $b = \phi(a) \in \phi(S)$, 也就是說 $S' \subseteq \phi(S)$. 由此得證 $S' = \phi(S)$.

最後我們要證明若 S' 是 R' 的 ideal, 則 S 也是 R 的 ideal. 對任意的 $r \in R$, $a \in S$ 皆有 $\phi(r \cdot a) = \phi(r) \cdot \phi(a)$. 由於 $\phi(r) \in R'$ 且 $\phi(a) \in S'$ 及 S' 是 R' 的 ideal, 我們有 $\phi(r) \cdot \phi(a) \in S'$. 故 $r \cdot a \in S$, 同理得 $a \cdot r \in S$. 所以 S 是 R 的 ideal. □

再次強調這個定理中除了 $\phi(S) = S'$ 需用到 ϕ 是 onto 外, 其他性質並不需 onto 的假設.

Remark 6.3.6. Correspondence Theorem 告訴我們說若 $\phi : R \to R'$ 是一個 onto 的 ring homomorphism, 則在 R' 中任選一個 subring S' 都可在 R 中找到一個 subring S 使得 $\phi(S) = S'$, 而且 $\ker(\phi) \subseteq S$. 其實在 R 中符合 $\phi(S) = S'$ 及 $\ker(\phi) \subseteq S$ 的 subring 是唯一的. 假設 R 中有另一個 subring T 符合 $\phi(T) = S'$ 且 $\ker(\phi) \subseteq T$. 則對於所有 $a \in T$, 因 $\phi(a) \in \phi(T) = S'$, 故由假設 $\phi(S) = S'$ 知在 S 中必存在一元素 b 使得 $\phi(b) = \phi(a)$. 換句話說 $\phi(a) - \phi(b) = 0$. 由此得 $\phi(a - b) = 0$. 也就是說 $a - b \in \ker(\phi)$. 別忘了 $\ker(\phi) \subseteq S$ 且 $b \in S$ 故 $a \in S$, 也就是說 $T \subseteq S$. 用同樣的方法可得 $S \subseteq T$. 所以 $T = S$. 換句話說: 對於 R' 中任一 subring S', 在 R 中皆 '存在' "唯一" 的 subring S 滿足 $\phi(S) = S'$ 且 $\ker(\phi) \subseteq S$.

Correspondence Theorem 最常用的情況是當 I 是 R 的一個 ideal, 而 ϕ 是 R 到 R/I 的 ring homomorphism 其中對任意的 $a \in R$, 定義 $\phi(a) = \overline{a}$.

Corollary 6.3.7. 假設 R 是一個 *ring* 且 I 是 R 的一個 *ideal.* 則對任意 R/I 中的 *subring* S' 都可在 R 中找到 *subring* S 符合 $I \subseteq S$ 且 $S/I = S'$.

當 S' 是 R/I 的 *ideal* 時, 則 S 也會是 R 的 *ideal.*

Proof. ϕ 是 ring homomorphism 是因為

$$\phi(a - b) = \overline{a - b} = \overline{a} - \overline{b} = \phi(a) - \phi(b)$$

且

$$\phi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \phi(a) \cdot \phi(b).$$

再證明 ϕ 是 onto 的, 事實上對所有 $y \in R/I$ 都是 $y = \overline{a}$, 其中 $a \in R$ 這種形式. 故選 $a \in R$ 帶入 ϕ 得 $\phi(a) = \overline{a} = y$. 得證 ϕ 是 onto.

$\ker(\phi)$ 是甚麼呢? 若 $a \in \ker(\phi)$ 則 $\phi(a) = \overline{0}$, 但由 ϕ 的定義 $\phi(a) = \overline{a}$. 故由 $\overline{a} = \overline{0}$, 得 $a \in I$. 反之若 $a \in I$, 則 $\phi(a) = \overline{a} = \overline{0}$, 故 $a \in \ker(\phi)$. 由此得 $\ker(\phi) = I$.

現在 Correspondence Theorem 中的條件都找到了, 所以利用 Theorem 6.3.5 知任取 R/I 中的一個 subring (或 idealS'), 在 R 中都可以找到一個 subring (或 ideal) S 符合 $I = \ker(\phi) \subseteq S$ 且 $\phi(S) = S/I = S'$. □

有許多書也稱 Corollary 6.3.7 為 Correspondence Theorem. 它告訴我們 R/I 中的 subring (或 ideal) 都是長 S/I 這種形式, 其中 S 是 R 的 subring (或 ideal) 且 $I \subseteq S$.

6.4. 三個 Ring Isomorphism 定理

和 group 一樣, ring 也有三個 isomorphism 定理. 由於我們有現成的 group isomorphism 定理可用, 這三個 isomorphism 定理幾乎可以直接推得, 我們只要驗證乘法部分即可.

Definition 6.4.1. 如果兩個 rings R 和 R' 間你可以找到一個 ring homomorphism 是 isomorphism (即 1-1 且 onto), 則我們稱 R 和 R' 這兩個 ring 是 *isomorphic*, 記為: $R \simeq R'$.

Theorem 6.4.2 (First Isomorphism Theorem)**.** *若 $\phi : R \to R'$ 是一個 ring homomorphism,* 則

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

Proof. 首先注意由 Lemma 6.3.3 知 $\mathrm{im}(\phi)$ 是一個 ring 且 $\ker(\phi)$ 是 R 的 ideal, 所以 $R/\ker(\phi)$ 也是一個 ring. 利用和第一個 group isomorphism 定理相同的方法, 我們在 $R/\ker(\phi)$ 這一個 quotient ring 和 $\mathrm{im}(\phi)$ 這個 ring 之間找到一個函數. 再說明這個函數是 ring homomorphism, 最後再驗證它是 1-1 且 onto.

我們可以利用 ϕ 製造以下的函數:

$$\psi : R/\ker(\phi) \to \mathrm{im}(\phi); \quad \overline{a} \mapsto \phi(a),\ \forall\, \overline{a} \in R/\ker(\phi).$$

我們首先說明 ψ 是一個'好函數' (well defined function): 如果 $a, b \in R$ 使得 $\overline{a}$ 和 $\overline{b}$ 在 $R/\ker(\phi)$ 中是相同的. 我們必須說明 $\phi(a) = \phi(b)$. 雖然 $a \neq b$, 不過由 $\overline{a} = \overline{b}$ 知 a 和 b 在以 $\ker(\phi)$ 這個 ideal 的分類下是同類的. 別忘了 a 和 b 同類表示 $a - b \in \ker(\phi)$. 也就是說 $\phi(a - b) = 0$. 再利用 ϕ 是 ring homomorphism 的假設, 我們得 $\phi(a) - \phi(b) = \phi(a - b) = 0$. 即 $\phi(a) = \phi(b)$. 所以我們製造的 ψ 是一個 well defined function.

接下來證 ψ 是一個 ring homomorphism: 對任意的 $\overline{a}, \overline{b} \in R/\ker(\phi)$, 我們有

$$\psi(\overline{a} + \overline{b}) = \psi(\overline{a + b}) = \phi(a + b) \quad \text{且} \quad \psi(\overline{a} \cdot \overline{b}) = \psi(\overline{a \cdot b}) = \phi(a \cdot b).$$

另一方面因為 ϕ 是 ring homomorphism, 所以

$$\phi(a + b) = \phi(a) + \phi(b) = \psi(\overline{a}) + \psi(\overline{b}) \quad \text{且} \quad \phi(a \cdot b) = \phi(a) \cdot \phi(b) = \psi(\overline{a}) \cdot \psi(\overline{b}).$$

結合以上二式, 我們可得

$$\psi(\overline{a}+\overline{b})=\psi(\overline{a})+\psi(\overline{b}) \quad 且 \quad \psi(\overline{a}\cdot\overline{b})=\psi(\overline{a})\cdot\psi(\overline{b}).$$

我們最後要證明 ψ 是 1-1 且 onto. 這其實不必證了(當然你要多此一舉也沒關係), 因為我們在 Theorem 2.6.1 已證過 ψ 這個函數在加法看成是 group homomorphism 已經是 1-1 且 onto.

總結: 我們證得了 ψ 是一個從 $G/\ker(\phi)$ 到 $\mathrm{im}(\phi)$ 的 isomorphism. 所以 $G/\ker(\phi)\simeq\mathrm{im}(\phi)$. □

當然了如果定理中的 ϕ 是 onto. 那麼我們知 $\mathrm{im}(\phi)=R'$. 因此我們有以下的引理:

Corollary 6.4.3. *若 $\phi: R\to R'$ 是一個 onto 的 ring homomorphism,* 則

$$R/\ker(\phi)\simeq R'.$$

現在我們來看看 ring 的第二個 isomorphism 定理. 它應該是怎樣的形式呢? 我們先回顧一下 group 的情況: 給定一 group G, 若 H 是 G 的 subgroup 且 N 是 G 的 normal subgroup. 則 $H\cap N$ 是 H 的 normal subgroup, 且 $H/(H\cap N)\simeq(H\cdot N)/N$. 好現在我們把 group 換成 ring, subgroup 換成 subring, normal subgroup 換成 ideal, 最後別忘了將乘改為加.

Theorem 6.4.4 (Second Isomorphism Theorem)**.** *若 R 是一個 ring, S 是 R 的 subring 且 I 是 R 的 ideal,* 則 *$S\cap I$ 是 S 的 ideal,* 且

$$S/(S\cap I)\simeq(S+I)/I.$$

Proof. 首先注意的是由 Lemma 6.2.1 知 $S+I$ 是 R 的 subring, 且 $I\subseteq S+I$ 因此知 I 是 $S+I$ 的 ideal (請參考 6.2 節的最後). 所以 $(S+I)/I$ 確實是一個 ring.

如同在 group 的情況, 我們想用 first isomorphism 定理來證明此定理. 我們先找一個從 S 到 $(S+I)/I$ 的函數. 考慮 $\phi: S\to(S+I)/I$, 其中對所有的 $s\in S$ 我們有 $\phi(s)=\overline{s}$.

現在要證 ϕ 是一個 ring homomorphism. 事實上對任意的 $s,s'\in S$, 我們有

$$\phi(s+s')=\overline{s+s'}=\overline{s}+\overline{s'}=\phi(s)+\phi(s') \quad 且 \quad \phi(s\cdot s')=\overline{s\cdot s'}=\overline{s}\cdot\overline{s'}=\phi(s)\cdot\phi(s').$$

利用 Theorem 2.6.4 的證明, 我們得 $\phi: S\to(S+I)/I$ 是 onto. 因此可以用 First Isomorphism Theorem (Corollary 6.4.3) 得到

$$S/\ker(\phi)\simeq(S+I)/I.$$

甚麼是 $\ker(\phi)$ 呢? 依定義 $\ker(\phi)$ 是 S 中的元素 s 使得 $\phi(s)$ 是 $(S+I)/I$ 的 identity, $\overline{0}$. 也就是說 $\phi(s)=\overline{s}=\overline{0}$. 別忘了 $\overline{s}=\overline{0}$ 表示 $s-0=s\in I$. 由此知 $\ker(\phi)$ 的元素既要在 S 中也要在 I 中; 換句話說 $\ker(\phi)\subseteq S\cap I$. 反之若 $a\in S\cap I$, 則因 $a\in I$

得 $\phi(a) = \overline{a} = \overline{0}$. 故 $S \cap I \subseteq \ker(\phi)$. 由此知 $\ker(\phi) = S \cap I$. 因此我們由 Lemma 6.3.3 知 $S \cap I$ 是 S 的 ideal 也由 First Isomorphism Theorem 知

$$S/(S \cap I) \simeq (S + I)/I.$$

□

最後我們來看第三個 isomorphism 定理. 同樣的, 將 Theorem 2.6.5 中的 group 換成 ring 及 normal subgroup 換成 ideal, 我們有以下之第三 isomorphism 定理:

Theorem 6.4.5 (Third Isomorphism Theorem)**.** *若 $\phi : R \to R'$ 是一個 onto 的 ring homomorphism. 假設 J' 是 R' 的一個 ideal. 令*

$$J = \{a \in R \,|\, \phi(a) \in J'\}.$$

則 J 是 R 的 ideal 且

$$R/J \simeq R'/J'.$$

Proof. 我們定 $\psi : R \to R'/J'$, 滿足 $\psi(a) = \overline{\phi(a)}, \forall\, a \in R$.

由 ϕ 是 ring homomorphism 知

$$\psi(a+b) = \overline{\phi(a+b)} = \overline{\phi(a) + \phi(b)} = \overline{\phi(a)} + \overline{\phi(b)} = \psi(a) + \psi(b)$$

且

$$\psi(a \cdot b) = \overline{\phi(a \cdot b)} = \overline{\phi(a) \cdot \phi(b)} = \overline{\phi(a)} \cdot \overline{\phi(b)} = \psi(a) \cdot \psi(b).$$

故 ψ 是一個從 R 到 R'/J' 的 ring homomorphism.

如前, 我們可用 Theorem 2.6.5 的證明知 $\psi : R \to R'/J'$ 是一個 onto 的 ring homomorphism, 我們再次用 First Isomorphism Theorem 知

$$R/\ker(\psi) \simeq R'/J'.$$

甚麼是 $ker(\psi)$ 呢? 若 $a \in \ker(\psi)$ 即 $\psi(a) = \overline{\phi(a)} = \overline{0}$, 也就是說 $\phi(a)$ 和 0 在用 J' 的分類下是同類的. 所以 $\phi(a) - 0 = \phi(a) \in J'$. 由 J 的定義知, 這表示 $a \in J$. 故 $\ker(\psi) \subseteq J$. 另外若 $a \in J$, 則 $\phi(a) \in J'$ 故在 R'/J' 中 $\psi(a) = \overline{\phi(a)} = \overline{0}$. 因此 $a \in \ker(\psi)$, 得 $J \subseteq \ker(\psi)$. 也就是說 $\ker(\psi) = J$ 且由 Lemma 6.3.3 知 J 是 R 的 ideal (其實我們在 Theorem 6.3.5 已知 J 是 R 的 ideal). □

最後我們利用 Correspondence Theorem 來看 Third Isomorphism Theorem 的一個特殊狀況. 令 I 是 R 的 ideal, $\phi : R \to R/I$ 是定義成 $\phi(a) = \overline{a}$ 這個 onto 的 ring homomorphism. 任意 R/I 中的 ideal J' 由前 Corollary 6.3.7 知是由 R 中的某一 ideal J 利用 ϕ 得到: 也就是說 $J' = \phi(J) = J/I$. 故由 Theorem 6.4.5 我們有以下的定理(有的書是稱這個為 Third Isomorphism Theorem.)

Theorem 6.4.6 (Third Isomorphism Theorem)**.** 若 R 是一個 *ring,* I 是 R 的一個 *ideal.* 則 R/I 中的任一 *ideal* 都是 J/I 這種形式, 其中 $I \subseteq J$ 且 J 是 R 的 *ideal.* 而且我們有

$$(R/I)/(J/I) \simeq R/J.$$

Proof. 任一 R/I 的 ideal 都是 J/I 這種形式已在 Corollary 6.3.7 證得. 而

$$(R/I)/(J/I) \simeq R/J$$

可由 Theorem 6.4.5 直接得到. 也就是代: $R' = R/I$, $J' = J/I$ 且考慮 $\phi : R \to R/I$, 符合 $\phi(a) = \overline{a}$. 此時可得 $J = \{a \in R \,|\, \phi(a) \in J'\}$. 故由 $R/J \simeq R'/J'$ 得證. □

6.5. 在 Commutative Ring with 1 中特殊的 Ideals

我們前面討論的情況都是在一般的 ring 中, 因此所得的結果在一般的 ring 都適用. 在這節中我們僅考慮 **commutative ring with** 1 的情況. 我們將探討在這種 ring 中的 principle ideal, prime ideal 和 maximal ideal.

6.5.1. Principle ideals. 在 group 中我們介紹過 cyclic subgroup, 它可以是說包含某一個元素的最小的 subgroup. 在 ring 中我們也有所謂的 principle ideal, 它是包含某一元素的最小的 ideal.

假設 R 是一個 commutative ring with 1. 要了解 R 中的 ideal 長甚麼樣子, 我們首先會考慮包含某一元素之最小的 ideal 為何, 因為這是最簡單的 ideal. 若給定 $a \in R$, 則包含 a 的最小 ideal I 應該長甚麼樣子呢? 首先 I 至少要包含 a 所產生的加法的 cyclic group, 即 $\{0, a, -a, 2a, -2a, \ldots, na, -na, \ldots\}$. 注意前面提過這裡 $2a$ 不是 $2 \cdot a$ 而是 $(1+1) \cdot a$ (別忘了 $1 \in R$ 這個假設). 由於 $1+1 \in R$, 我們可以說存在某一元素 $\alpha \in R$ 使得 $2a = \alpha \cdot a$. 同理對其他的正整數 n, 由於

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

所以 (謝謝 $1 \in R$ 這個假設) 存在 $\beta \in R$ 滿足 $na = \beta \cdot a$. 另一方面由 Lemma 6.1.2, 知 I 中也必須包含對任意的 $r \in R$, $r \cdot a$ 和 $a \cdot r$ 這種元素. 然而 $r \cdot a = a \cdot r$ (謝謝 R 是 commutative ring 這個假設), 因此 I 中至少要包含所有的 $r \cdot a$ 這種形式的元素. 如果由所有的 $r \cdot a$ 這樣的元素所成的集合是 R 的一個 ideal, 那麼它自然就是包含 a 的最小 ideal 了.

Lemma 6.5.1. 假設 R 是一個 *commutative ring with* 1, 且 $a \in R$. 令 $A = \{r \cdot a \,|\, r \in R\}$, 則 A 是 R 的一個 *ideal.* 事實上, A 是 R 中包含 a 之最小的 *ideal.*

Proof. 從前面的討論我們已知: 若 I 是 R 中包含 a 之最小的 ideal, 則 $A \subseteq I$. 因此若能證得 A 是 R 的 ideal, 則知 $I = A$.

我們利用 Lemma 6.1.2 來證明 A 是 R 的 ideal. 任取 A 中兩元素 $r \cdot a$ 和 $r' \cdot a$, 其中 $r, r' \in R$. 由於 $r \cdot a - r' \cdot a = (r - r') \cdot a$ 且 $r - r' \in R$, 知 $r \cdot a - r' \cdot a \in A$. 另外任取

R 中一元素 r 及 A 中一元素 $r'\cdot a$, 其中 $r'\in R$. 由於 $(r'\cdot a)\cdot r = r\cdot(r'\cdot a) = (r\cdot r')\cdot a$ 且 $r\cdot r'\in R$, 知 $(r'\cdot a)\cdot r = r\cdot(r'\cdot a)\in A$. 因此 A 是 R 的 ideal. □

通常我們會將 Lemma 6.5.1 中的 A 用 $\big(a\big)$ 來表示. 注意我們是用大一點的括號 $\big(\ \big)$ 以免和一般運算間的小括號 ( ) 混淆.

Definition 6.5.2. 假設 R 是一個 commutative ring with 1, 且 $a\in R$. 則

$$\big(a\big) = \{r\cdot a \,|\, r\in R\}$$

稱為 the *principle ideal generated* by a in R. 若 I 為 R 的一個 ideal 且在 R 中存在一元素 a 滿足 $I = \big(a\big)$ 則稱 I 是 R 的一個 *principle ideal*.

Example 6.5.3. 在 $\mathbb{Z}$ 中, 任取 $n\in\mathbb{Z}$, 則所有 n 的倍數所成的集合是一個 principle ideal, 即 $\big(n\big) = \{z\cdot n \,|\, z\in\mathbb{Z}\}$.

將來我們會看到在 $\mathbb{Z}$ 中所有的 ideal 都是 principle ideal, 不過這對一般的 ring 並不一定對. 另外若 I 是一個 principle ideal, 並不表示產生 I 的元素是唯一的 (例如前面的例子我們有 $\big(n\big) = \big(-n\big)$), 事實上我們有以下的結果.

Lemma 6.5.4. 假設 R 是一個 *commutative ring with* 1. 如果 $a, b\in R$ 且存在一 *unit* $u\in R$ 滿足 $a = u\cdot b$, 則 $\big(a\big) = \big(b\big)$.

Proof. 由於 $a = u\cdot b$, 由定義知 $a\in\big(b\big)$. 又由於 $\big(b\big)$ 是一個 ideal 且 $\big(a\big)$ 是包含 a 最小的 ideal, 故得 $\big(a\big)\subseteq\big(b\big)$. 反之, 因 u 是 R 的 unit, 故存在 $v\in R$ 滿足 $v\cdot u = 1$. 所以由 $b = (v\cdot u)\cdot b = v\cdot a$ 知 $b\in\big(a\big)$. 再利用 $\big(b\big)$ 是包含 b 最小的 ideal 得 $\big(b\big)\subseteq\big(a\big)$. 故證得 $\big(a\big) = \big(b\big)$. □

以下介紹一個 principle ideal 的簡單應用. 我們在 lemma 6.2.4 中知道: 當 R 是一個 division ring 時, R 中只有 $\{0\}$ 和 R 這兩個 ideals. 當 R 是一個 field 時 (R 也就是一個 division ring), R 當然也就沒有 nontrivial proper ideal. 當 R 是 commutative ring with 1 時, 這是一個幫助我們判斷 R 是否為一個 field 的好方法.

Proposition 6.5.5. 若 R 是一個 *commutative ring with* 1, 則 R 是一個 *field* 若且唯若 R 沒有 *nontrivial proper ideal*.

Proof. 我們已知當 R 是一個 field 時, R 沒有 nontrivial proper ideal. 反之, 如果 R 沒有 nontrivial proper ideal, 我們想證明 R 是一個 field. 由於 R 已假設是 commutative ring with 1, 依定義我們只要證明 R 中非 0 的元素都是 unit. 任取 $a\in R$ 且 $a\neq 0$. 我們考慮 $\big(a\big)$ 這一個 principle ideal. 因為 $a\neq 0$ 且 $a\in\big(a\big)$, 故知 $\big(a\big)\neq\{0\}$. 不過依假設 R 中除了 $\{0\}$ 和 R 已外沒有其他的 ideal, 因此得 $\big(a\big) = R$. 然而 $1\in R$, 即 $1\in\big(a\big)$ 故由 $\big(a\big)$ 的定義知存在 $r\in R$ 使得 $1 = r\cdot a$. 也就是說 a 是一個 unit. □

最後我們要強調, 在 Proposition 3.1.3 中我們知道一個 cyclic group 中的 subgroup 都是 cyclic group. 不過對 principle ideal, 這就不一定對了. 也就是說若 I, I' 都是 R 的 ideal 且 $I' \subseteq I$. 如果已知 I 是 principle ideal, 這並不保證 I' 會是 principle ideal.

6.5.2. Prime ideals. 在 $\mathbb{Z}$ 中一個質數 p 有一個重要的性質, 即若 $p \mid a \cdot b$ 則 $p \mid a$ 或 $p \mid b$. 注意, $p \mid a$ 表示 a 是 p 的倍數, 因此用 principle ideal 的看法這表示 $a \in \big(p\big)$. 所以我們可以把質數的這個性質表示成: 若 $a \cdot b \in \big(p\big)$, 則 $a \in \big(p\big)$ 或 $b \in \big(p\big)$. 因此我們將質數的這一性質推廣成以下這一種很重要的 ideal 的定義.

Definition 6.5.6. 令 R 是一個 commutative ring with 1 且 P 是 R 的一個不等於 R 的 ideal. 如果 P 符合: 「對任意 R 中兩個元素 a 和 b 若 $a \cdot b \in P$, 則 $a \in P$ 或 $b \in P$」, 那麼我們稱 P 是 R 的一個 *prime ideal*.

有時在證明問題不好直接證明屬於, 我們通常會例用若 $a \notin P$ 且 $b \notin P$, 則 $a \cdot b \notin P$ 這種論述來證明 P 是一個 prime ideal. 例如我們知道兩個奇數相乘不可能成為偶數, 因此馬上可以知道所有偶數所成的 ideal, 即 $\big(2\big)$ 是 $\mathbb{Z}$ 的一個 prime ideal. 當然了從前面提過質數的性質我們知道任何質數產生的 principle ideal 皆是整數的 prime ideal.

接下來我們來看一個判斷 R 中的 ideal P 是否為一個 prime ideal 的好方法.

Theorem 6.5.7. 若 R 是一個 *commutative ring with* 1 且 P 是 R 的一個 *ideal,* 則 P 是 R 的一個 *prime ideal* 若且唯若 R/P 這個 *quotient ring* 是一個 *integral domain.*

Proof. 首先回顧一下: 既然 R 是 commutative ring with 1, 對任意 R 的 ideal I, R/I 這個 quotient ring 也會是一個 commutative ring with 1 (其乘法的 identity 是 $\overline{1}$). 因此要說 R/P 是一個 integral domain, 我們只要說明 R/P 中沒有 zero divisor 即可.

現假設 P 是一個 prime ideal. 對任意 R/P 的非 $\overline{0}$ 的元素都可以寫成 $\overline{a}$, 其中 $a \in R$ 但 $a \notin P$. 要說 $\overline{a}$ 不是 R/P 中的 zero divisor, 等於是說對任意 R/P 中非 $\overline{0}$ 的元素 $\overline{b}$ 皆不可使得 $\overline{a} \cdot \overline{b} = \overline{0}$. 然而 $\overline{b} \neq \overline{0}$, 表示 $b \notin P$. 既然 a, b 都不屬於 P, 由 P 是 prime ideal 的假設, 我們得 $a \cdot b \notin P$. 也就是說

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} \neq \overline{0}.$$

因此 R/P 是一個 integral domain.

反之, 若 R/P 是一個 integral domain, 即任取 $\overline{a}, \overline{b} \in R/P$ 符合 $\overline{a} \neq \overline{0}$ 且 $\overline{b} \neq \overline{0}$, 都會有 $\overline{a} \cdot \overline{b} \neq \overline{0}$. 換句話說: 如果 $a \notin P$ 且 $b \notin P$, 則 $a \cdot b \notin P$. 故知 P 是一個 prime ideal. □

因為 $R/\big(0\big) \simeq R$ 故利用 Lemma 6.5.7 我們有以下這個有趣的結果:

Corollary 6.5.8. 若 R 是一個 *commutative ring with* 1, 則 R 是一個 *integral domain* 若且唯若 $\big(0\big)$ 是 R 的 *prime ideal.*

6.5.3. Maximal ideals. 在 $\mathbb{Z}$ 中質數另一個重要的性質是除了 1 和本身外它不會是其他整數的倍數. 以後我們會知道在整數中所有的 ideal 皆是 principle ideal. 所以用 ideal 的觀點來看這表示一個質數所形成的 principle ideal 不會包含於其他的 nontrivial proper ideal. 因此我們有以下另一個推廣質數性質的特殊 ideal.

Definition 6.5.9. 若 R 是一個 ring 且 M 是 R 中的一個 nontrivial proper ideal, 如果 M 不會包含於 R 中其他的 nontrivial proper ideal, 則我們稱 M 是一個 *maximal ideal.*

注意, 別被 "maximal" 這個字給騙了. 在數學上很多情況下, maximal 是表示沒有東西比它大, 並不表示它比所有的東西大. (我們不這樣定主要是在很多情況下我們要探討的東西並不是 well-ordered, 也就是有時兩樣東西是不能比較的.) 因此, 若 M 是 R 的一個 maximal ideal 且 I 是 R 的一個 nontrivial proper ideal, 這並不表示 $I \subseteq M$, 而只是說如果 $M \subseteq I$, 則 $I = M$. 從這個看法大家應也可以看出有可能在 R 中有不只一個 maximal ideal. 希望下一個例子可以釐清這個觀念.

Example 6.5.10. 考慮 $\mathbb{Z}$ 中 $\big(6\big)$ 這一個 ideal. 我們很容易看出來 $\big(6\big) \subseteq \big(2\big)$ 且因 $2 \in \big(2\big)$ 但 $2 \notin \big(6\big)$, 我們知 $\big(6\big) \subsetneq \big(2\big)$. 再加上 $\big(2\big)$ 是 $\mathbb{Z}$ 的一個 nontrivial proper ideal, 故知 $\big(6\big)$ 不是 $\mathbb{Z}$ 的 maximal ideal. 不過 $\big(2\big)$ 是 $\mathbb{Z}$ 的 maximal ideal. 因為如果 $\big(2\big)$ 不是 maximal ideal, 則依定義知存在一個 $\mathbb{Z}$ 中的 nontrivial proper ideal I 滿足 $\big(2\big) \subsetneq I$. 換句說存在一整數 $a \in I$ 但 $a \notin \big(2\big)$ (這表示 a 是一個奇數). 所以存在一整數 n 使得 $a = 2 \cdot n + 1$. 別忘了我們假設 I 是 ideal 且 $2 \in I$, 所以 $2 \cdot n \in I$. 再加上 $a \in I$, 因此得 $1 = a - 2 \cdot n \in I$. 由 Lemma 6.2.4 知 $I = \mathbb{Z}$, 這和我們假設 I 是 nontrivial proper ideal 相矛盾, 故得 $\big(2\big)$ 是 $\mathbb{Z}$ 的 maximal ideal. 不過由於 $3 \notin \big(2\big)$, 我們知 $\big(3\big)$ 這個 ideal 並不包含於 $\big(2\big)$. 甚至對任意的 $n \in \mathbb{N}$, $\big(3^n\big)$ 都不會包含於 $\big(2\big)$. 所以 maximal ideal 會比所有的 nontrivial proper ideal 都大這樣的說法並不正確. 另一方面, 我們可以用前面類似的方法得到在 $\mathbb{Z}$ 中任意一個質數所產生的 principle ideal 都是 maximal ideal, 所以 $\mathbb{Z}$ 中的 maximal ideal 並不只一個 (其實有無窮多個).

接下來我們想用類似 Theorem 6.5.7 的方法利用 quotient ring 來判別一個 ideal 是否為 maximal ideal.

Theorem 6.5.11. 若 R 是一個 *commutative ring with* 1 且 M 是 R 的一個 *ideal,* 則 M 是 R 的一個 *maximal ideal* 若且唯若 R/M 這個 *quotient ring* 是一個 *field.*

Proof. 首先觀察由假設可知 R/M 是一個 commutative ring with 1, 所以 R/M 是一個 field 相當於只要說 R/M 中不等於 $\overline{0}$ 的元素都是 unit.

現假設 M 是 R 的 maximal ideal. 任取 R/M 中一元素 $\overline{a} \neq \overline{0}$, 我們有 $a \in R$ 且 $a \notin M$. 由 Lemma 6.2.1 知

$$M + \big(a\big) = \{m + r \cdot a \,|\, m \in M,\, r \in R\}$$

是 R 的一個 ideal. 由於 $M \subseteq M + \big(a\big)$ 且 $a \notin M$, 我們知 $M \neq M + \big(a\big)$, 即 $M + \big(a\big)$ 是一個比 M 大的 ideal. 但由 M 是 maximal ideal 的假設我們知 $M + \big(a\big)$ 不是 R 的 nontrivial proper ideal. 換句話說 $M + \big(a\big) = R$. 利用 $1 \in R = M + \big(a\big)$, 我們知存在 $m \in M$, $r \in R$ 滿足 $1 = m + r \cdot a$. 別忘了我們是要討論 R/M 的元素, 所以由上式以及在 R/M 中 $\overline{m} = \overline{0}$ 我們有

$$\overline{1} = \overline{m} + \overline{r \cdot a} = \overline{r} \cdot \overline{a}.$$

因此 $\overline{a}$ 是 R/M 的 unit, 故知 R/M 是一個 field.

反之若 R/M 是一個 field, 我們想證 M 是 R 的一個 maximal ideal. 再次強調我們不是要證明任意 R 中的 nontrivial proper ideal 都滿足 $I \subseteq M$, 而是要證明不可能 $M \subsetneq I$. 我們要用反證法: 假設 M 不是 maximal ideal, 即存在一個 nontrivial proper ideal I 滿足 $M \subsetneq I$. 由 $M \subseteq I$ 但 $M \neq I$ 知存在 $a \in I$ 但 $a \notin M$, 也就是說在 R/M 中 $\overline{a} \neq \overline{0}$. 但 R/M 是一個 field, 故存在 $r \in R$ 使得

$$\overline{r} \cdot \overline{a} = \overline{r \cdot a} = \overline{1}.$$

這告訴我們 $1 - r \cdot a \in M$, 也就是說 $1 = m + r \cdot a$ 其中 $m \in M$. 由於 $a \in I$ 且 I 是一個 ideal, 我們知 $r \cdot a \in I$. 因此由 $m \in M \subseteq I$ 得 $1 = m + r \cdot a \in I$. Lemma 6.2.4 告訴我們 $1 \in I$ 表示 $I = R$, 此和 I 是 nontrivial proper ideal 相矛盾, 故知 M 是 maximal ideal. □

Remark 6.5.12. 我們可以利用 Correspondence 定理很快的證明 Theorem 6.5.11. 回顧一下 Corollary 6.3.7 告訴我們 R/M 中的 ideal 都是由介於 R 和 M 間的 ideal 所形成. 因此若 M 是 maximal ideal, 表示介於 R 和 M 間所有的 ideal 只有 R 和 M. 換句話說 R/M 中只有 R/M 和 $M/M = \big(\overline{0}\big)$ 這兩個 ideal 而沒有 nontrivial proper ideal, 所以由 Proposition 6.5.5 知 R/M 是一個 field. 另一方面如果 R/M 是一個 field, 同樣的由 Proposition 6.5.5 我們知 R/M 沒有 nontrivial proper ideal. 因此由我們在 Remark 6.3.6 中提到的比較強(有唯一性)的 Correspondence 定理知沒有其他的 ideal 介於 R 和 M 之間, 故得 M 是 maximal ideal.

我們知道在一個 field 中非 0 的元素都是 unit, 然而 Lemma 5.3.7 告訴我們一個 unit 絕不會是 zero divisor, 所以我們知道一個 field 事實上是一個 integral domain. 現若 R/M 是一個 field, 則 R/M 是一個 integral domain. 所以由 Theorem 6.5.7 和 Theorem 6.5.11 可得以下之結果:

Corollary 6.5.13. 若 R 是一個 *commutative ring with* 1, 則 R 中的 *maximal ideal* 都是 *prime ideal.*

注意 Corollary 6.5.13 反過來並不一定對. 例如在 $\mathbb{Z}$ 中我們知 $\mathbb{Z}/\big(0\big) \simeq \mathbb{Z}$, 但 $\mathbb{Z}$ 是 integral domain 卻不是 field, 所以知 $\big(0\big)$ 是 $\mathbb{Z}$ 的 prime ideal 但不是 maximal ideal.

Chapter 7

一些常見的 Rings

這一章我們將介紹一些常見的 ring. 這裡介紹的 ring 都是 integral domain, 希望能從這一章介紹的 ring 幫助我們更了解下一章所要探討的內容.

7.1. The Ring of Integers

我們首先介紹大家最熟悉的 ring $\mathbb{Z}$. 其實代數上很多的理論都是為了探討和整數相關的問題而產生的, 所以雖然有些同學已對 $\mathbb{Z}$ 的性質相當了解, 我們還是簡單的瀏覽一下, 以備以後要討論相關問題時可以做很好的對照.

整數中最基本的定理應該就是整數的餘數定理 *Euclid's Algorithm*, 幾乎所有整數的基本性質都是由它推導出來的. 其實我們在前面已經用過這個定理好幾次了, 不過為了完整性我們還是給一個證明.

Theorem 7.1.1 (Euclid's Algorithm)**.** 給定一正整數 n, 對任意的 $m \in \mathbb{Z}$, 皆存在 $h, r \in \mathbb{Z}$, 其中 $0 \leq r < n$, 滿足 $m = h \cdot n + r$.

Proof. 這個定理我們習慣稱為餘數定理, 如此稱它當然就包含"除"這個概念. 不過因為我們現在在談 ring 的性質, 我們避免用除的概念.

首先考慮 $W = \{m - t \cdot n \,|\, t \in \mathbb{Z}\}$ 這一個集合. 因為 t 可取任何整數, 很容易就看出 W 一定包含一些非負的整數. 令 r 是 W 中最小的非負的整數, 因為 $r \in W$, 由定義知存在 $h \in \mathbb{Z}$ 滿足 $r = m - h \cdot n$. 我們最主要的目的就是要證明 $0 \leq r < n$.

假設 r 不合我們的條件, 也就是說 $r \geq n$ (別忘了 r 是非負整數的假設). 若如此, 我們可將 r 寫成 $r = n + r'$, 其中 $r' \geq 0$. 因此利用

$$m = h \cdot n + r = h \cdot n + (n + r') = (h + 1) \cdot n + r',$$

我們得到 $r' = m - (h + 1) \cdot n \in W$. 但 $0 \leq r' < r$, 這和 r 是 W 中最小的非負整數相矛盾. 故得證本定理. □

要注意 Theorem 7.1.1 的證明我們用到整數上可以排序的 *well-ordering principle*, 因此雖然證明很簡單, 但並不能直接套用到一般的 ring. 也就是說, 一般的 ring 不一定有所謂的 Euclid's Algorithm. 將來我們會看到一些特殊的 integral domain 也有所謂的 Euclid's Algorithm. 這樣的 integral domain 我們會給它一個名稱: 稱為 Euclidean domain.

接下來我們就來看看 Theorem 7.1.1 的魔力有多大吧!

Theorem 7.1.2. 在 $\mathbb{Z}$ 中所有的 *ideal* 都是 *principle ideal.*

Proof. 複習一下定義: 若 I 是一個 $\mathbb{Z}$ 的 ideal, 我們想說在 I 中存在一元素 a 使得

$$I = \big(a\big) = \{h \cdot a \,|\, h \in \mathbb{Z}\},$$

也就是說 I 是所有 a 的倍數所成的集合. 若已知一集合是由某數的所有倍數所成的集合, 你要怎麼找出這個數呢? 當然是找其中最小的正整數了!

$\mathbb{Z}$ 中的 trivial ideal Z 和 $\{0\}$, 分別由 1 和 0 生成, 所以都是 principle ideal. 因此我們只要考慮 $\mathbb{Z}$ 中 nontrivial proper ideal 就可. 假設 I 是 $\mathbb{Z}$ 的一個 nontrivial proper ideal, 由於 $I \neq \{0\}$, 故存在 $b \neq 0$, 且 $b \in I$. 由於 I 是 ideal, $-b$ 也在 I 中, 因此我們知 I 中必存在正整數. 現令 $a \in I$ 是 I 中最小的正整數, 我們要證明 $I = \big(a\big)$.

首先 $a \in I$, 所以對任意的 $h \in \mathbb{Z}$ 皆有 $h \cdot a \in I$, 故知 $\big(a\big) \subseteq I$. 因此我們僅剩下要證 $I \subseteq \big(a\big)$, 換句話就是要證明 I 中的元素都是 a 的倍數. 任取 $m \in I$ 怎麼說 m 是 a 的倍數呢? (當然就是拿 m 除以 a 看看餘數是什麼了.) 利用 Theorem 7.1.1, 我們知存在 $h, r \in \mathbb{Z}$, $0 \leq r < a$ 滿足 $r = m - h \cdot a$. 由於 $m \in I$ 且 $h \cdot a \in I$, 利用 I 是 ideal 知 $r = m - h \cdot a \in I$. 但已知 a 是 I 中最小的正整數, 故得 $r = 0$, 即 $m = h \cdot a \in \big(a\big)$. 也就是說 $I \subseteq \big(a\big)$. □

我們曾提醒過, 並不是所有的 ring 它的 ideal 都會是 principle ideal. 如果一個 integral domain 它的 ideal 都是 principle ideal, 這樣特別的 integral domain 我們稱之為 principle ideal domain. 注意以上 $\mathbb{Z}$ 是 principle ideal domain (Theorem 7.1.2) 的性質, 是由 $\mathbb{Z}$ 是 Euclidean domain (Theorem 7.1.1) 這個性質推導出來的.

這一節我們主要是談整數上元素的分解, 所以還是給因數, 公因數和最大公因數下一個定義.

Definition 7.1.3. 令 $a, b \in \mathbb{Z}$.

(1) 若 $d \in \mathbb{Z}$ 且存在 $h \in \mathbb{Z}$ 使得 $a = h \cdot d$, 則稱 d 是 a 的一個 *divisor*, 記做 $d \,|\, a$.

(2) 若 $c \in \mathbb{Z}$, 且 $c \,|\, a$ 及 $c \,|\, b$, 則稱 c 為 a, b 的 *common divisor.*

(3) 若 $d \in \mathbb{Z}$ 是 a, b 最大的 common divisor, 則稱 d 為 a, b 的 *greatest common divisor.*

一般都是利用所謂的輾轉相除法將兩個數的 greatest common divisor 求出, 在這裡我們將利用 Theorem 7.1.2 找到 greatest common divisor 並得到其基本性質.

Proposition 7.1.4. 給定 $a, b \in \mathbb{Z}$, 則存在 $d \in \mathbb{N}$ 滿足 $\big(d\big) = \big(a\big) + \big(b\big)$ 且 d 為 a, b 的 *greatest common divisor*

Proof. 由 Lemma 6.2.1 我們知

$$\big(a\big) + \big(b\big) = \{r \cdot a + s \cdot b \,|\, r, s \in \mathbb{Z}\}$$

是 $\mathbb{Z}$ 的一個 ideal. 由 Theorem 7.1.2 知存在 $d \in \mathbb{Z}$ 使得 $\big(d\big) = \big(a\big) + \big(b\big)$. 在這裡我們可以要求 d 是正的, 這是因為 -1 是 $\mathbb{Z}$ 的 unit 故 Lemma 6.5.4 告訴我們 $\big(d\big) = \big(-d\big)$.

接著我們要證明這個 $d \in \mathbb{N}$ 是 a, b 的 greatest common divisor. 首先當然是要證 d 是 a, b 的 common divisor. 然而因 $a \in \big(a\big) \subseteq \big(a\big) + \big(b\big) = \big(d\big)$, 故知存在 $r \in \mathbb{Z}$ 使得 $a = r \cdot d$. 也就是說 $d \,|\, a$. 同理, 由 $b \in \big(d\big)$ 可得 $d \,|\, b$. 故知 d 是 a, b 的 common divisor.

那為甚麼 d 會是 a, b 的 common divisor 中最大的呢? 由於 $d \in \big(d\big) = \big(a\big) + \big(b\big)$, 我們知道存在 $m, n \in \mathbb{Z}$ 使得 $d = m \cdot a + n \cdot b$. 然而若 c 是 a, b 的 common divisor, 即 $c \,|\, a$ 且 $c \,|\, b$, 知存在 $r, s \in \mathbb{Z}$ 使得 $a = r \cdot c$ 且 $b = s \cdot c$. 因此得

$$d = m \cdot (r \cdot c) + n \cdot (s \cdot c) = (m \cdot r + n \cdot s) \cdot c.$$

也就是說 $c \,|\, d$. 所以知 d 是所有 a, b 的 common divisor 中最大的. □

Proposition 7.1.4 不只告訴我們如何找到 greatest common divisor, 事實上在證明中我們也證得 greatest common divisor 的兩個重要性質.

Corollary 7.1.5. 令 $a, b \in \mathbb{Z}$ 且 d 為 a, b 的 *greatest common divisor,* 則 d 符合以下兩性質*:*

(1) 存在 $m, n \in \mathbb{Z}$ 滿足 $d = m \cdot a + n \cdot b$.

(2) 假設 $c \,|\, a$ 且 $c \,|\, b$, 則 $c \,|\, d$.

接下來我們要談整數的分解中最基本的元素: 質數. 大家都知道一個質數 p 就是因數只有 1 和本身的數. 利用這個性質我們可得到若 $p \,|\, a \cdot b$ 則 $p \,|\, a$ 或 $p \,|\, b$ 這個性質, 因此大家都會拿這兩種性質來判別一個數是否為質數. 不過在一般的 ring 這兩種性質是很不一樣的, 所以我們用不同的名字來稱呼.

Definition 7.1.6. 考慮 $\mathbb{Z}$ 中的元素 p.

(1) 若對任意滿足 $d \,|\, p$ 的 $d \in \mathbb{Z}$ 皆有 $d = \pm 1$ 或 $d = \pm p$, 則稱 p 是一個 *irreducible element.*

(2) 若對任意滿足 $p \,|\, a \cdot b$ 的 $a, b \in \mathbb{Z}$ 皆有 $p \,|\, a$ 或 $p \,|\, b$, 則稱 p 是一個 *prime element.*

很顯然這兩種定義是不一樣的, 不過下一個定理告訴我們在整數中這兩種定義的元素是相同的. 也因如此在整數中我們就統一稱之為質數 (prime).

Proposition 7.1.7. *在 $\mathbb{Z}$ 中若 p 是一個 irreducible element, 則 p 是一個 prime element. 反之, 若 p 是一個 prime element, 則 p 是一個 irreducible element.*

Proof. 首先我們證若 p 是 irreducible 則 p 是 prime. 也就是說假設已知 p 是 irreducible. 任取 $p \mid a \cdot b$ 我們要證明: $p \mid a$ 或 $p \mid b$. 然而 $p \mid a \cdot b$ 表示存在 $r \in \mathbb{Z}$ 使得 $a \cdot b = r \cdot p$. 如果 $p \mid a$ 那麼就得到我們要證的, 所以我們只要討論 $p \nmid a$ 的情況. 此時我們考慮 p, a 的 greatest common divisor 令之為 d. 由於 $d \mid p$ 故由 p 是 irreducible 的假設知 $d = 1$ 或 $d = p$. 然而 d 不可能等於 p, 否則由 d 是 p, a 的 common divisor 知 $p = d \mid a$: 此和 $p \nmid a$ 矛盾. 因此知 $d = 1$, 由 Corollary 7.1.5 知存在 $n, m \in \mathbb{Z}$ 滿足 $1 = n \cdot p + m \cdot a$. 等式兩邊乘上 b 得

$$b = (n \cdot b) \cdot p + m \cdot (a \cdot b) = (n \cdot b) \cdot p + m \cdot (r \cdot p) = (n \cdot b + m \cdot r) \cdot p,$$

所以 $p \mid b$.

反之, 若已知 p 是一個 prime element 我們要證明 p 是 irreducible. 也就是證明若 $d \mid p$, 則 $d = \pm 1$ 或 $d = \pm p$. 然而 $d \mid p$ 表示存在 $r \in \mathbb{Z}$ 滿足 $p = d \cdot r$, 也就是說 $p \mid d \cdot r$. 故由 p 是 prime 的假設, 我們得 $p \mid d$ 或 $p \mid r$. 當 $p \mid d$ 時, 由原先假設 $d \mid p$ 知 $d = \pm p$. 當 $p \mid r$ 時, 表示存在 $s \in \mathbb{Z}$ 滿足 $r = s \cdot p$. 故由 $p = d \cdot r = d \cdot (s \cdot p)$ 得 $d \cdot s = 1$. 因 $d, s \in \mathbb{Z}$, 故 $d \cdot s = 1$ 表示 $d = \pm 1$. □

最後我們來看整數最基本也最重要的唯一分解定理. 由於正整數和負整數的分解只差一個負號, 我們只需考慮正整數的情況.

Theorem 7.1.8. *假設 $a \in \mathbb{N}$ 且 $a > 1$, 則存在 $p_1, \ldots, p_r$, 其中 p_i 是相異的 prime, 滿足*

$$a = p_1^{n_1} \cdots p_r^{n_r}, \quad n_i \in \mathbb{N}, \forall i \in \{1, \ldots, r\}.$$

如果 a 可以分解成另外的形式 $a = q_1^{m_1} \cdots q_s^{m_s}$, 其中 q_i 是相異的 prime, 則 $r = s$ 且經過變換順序可得 $p_i = q_i$, $n_i = m_i$, $\forall\, i \in \{1, \ldots, r\}$.

Proof. 這又是一個典型的有關存在性與唯一性的定理, 我們仍然分開來證存在性與唯一性.

首先來看存在性: 簡單來說存在性就是要證明每一個大於 1 的整數都可以寫成有限多個(可以相同) prime 的乘積. 如果 a 本身是個 prime, 則 $a = p_1$ (即 $r = 1$, $n_1 = 1$), 得證存在性. 如果 a 不是 prime 呢? 由 Proposition 7.1.7 知 a 不是 irreducible, 也就是說存在 $a_1, b_1 \in \mathbb{N}$ 且 $a_1 \neq 1$, $b_1 \neq 1$ 滿足 $a = a_1 \cdot b_1$. 接下來就是看 a_1, b_1 是不是 prime 了. 如果其中有一個不是 prime, 我們就繼續分解下去直到得到 prime 為止. 這個過程一定會停下來因為每次分解後得的數越來越小. 當然最後就可以將 a 寫成一些 prime 的乘積了. 這樣的證明方式, 相信大家會有一種說不清楚的感覺, 所以我們還是用比較數學的方法來證明. 當 $a = 2$ 時由於 2 是 prime,

所以在這情況存在性是對的. 接著假設對所有介於 2 和 $a-1$ 的整數存在性是對的. 如果 a 是 prime, 那存在性自然成立, 如果 a 不是 prime, 則由 Proposition 7.1.7 知 $a = a_1 \cdot b_1$ 其中 $a_1, b_1 \in \mathbb{N}$ 且 $1 < a_1 < a$ 及 $1 < b_1 < a$. 故利用歸納假設知 a_1 和 b_1 都可寫成有限多個 prime 的乘積, 所以得證 a 也可以寫成有限多個 prime 的乘積.

我們依然用歸納法證唯一性, 假設

$$a = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s},$$

其中 $p_1, \ldots, p_r$ 是兩兩相異的 prime, 且 $q_1, \ldots, q_s$ 也是兩兩相異的 prime. 由於 p_1 是 prime, 故由 $p_1 \,|\, a = q_1^{m_1} \cdots q_s^{m_s}$ 知存在某個 $j \in \{1, \ldots, s\}$ 滿足 $p_1 \,|\, q_j$. 變換一下順序我們可以假設 $p_1 \,|\, q_1$. 由於 q_1 是 prime, 由 Proposition 7.1.7 知 q_1 是 irreducible. 換句話說, q_1 的 divisor 只能是 ± 1 或 $\pm q_1$. 故由 $p_1 \,|\, q_1$ 知 $p_1 = q_1$. 現在考慮

$$\frac{a}{p_1} = p_1^{n_1 - 1} \cdots p_r^{n_r} = q_1^{m_1 - 1} \cdots q_s^{m_s}.$$

由於 $a/p_1 < a$, 故利用唯一性的歸納法假設我們得 $r = s$ 且 $p_1 = q_1, \ldots, p_r = q_r$ 以及 $n_1 = m_1$, $n_2 = m_2, \ldots, n_r = m_r$, 故得證唯一性. □

如果一個 integral domain 有和 $\mathbb{Z}$ 一樣每個元素都可以唯一寫成一些 irreducible element 的乘積的性質, 我們便稱此 integral domain 為一個 unique factorization domain.

7.2. Ring of Polynomials over a Field

大家都知道有理係數的多項式有和整數很類似的性質, 就是所謂的餘式定理. 事實上這個定理對係數在一般的 field 的多項式也對的. 在這一節中我們將探討這種 polynomial ring. 大家會發現我們幾乎是把上一節中整數的那一套理論完完整整的搬過來.

令 F 是一個 field. 我們考慮由所有的係數在 F 的多項式

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n, \quad a_i \in F \; \forall \, i = 0, \ldots, n$$

所形成的集合 $F[x]$. 我們很自然給 $F[x]$ 中的元素定義以下的加法和乘法: 若 $f(x) = a_0 + a_1 x \cdots + a_n x^n$ 和 $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ 是 $F[x]$ 中的兩元素, 定 $f(x) + g(x) = c_0 + c_1 x + \cdots + c_r x^r$, 其中對所有的 $i \in \{1, \ldots, r\}$, $c_i = a_i + b_i$ 且 $r = \max\{m, n\}$. 另外我們定 $f(x) \cdot g(x) = d_0 + d_1 x + \cdots + d_{m+n} x^{m+n}$, 其中對所有的 $i \in \{1, \ldots, m+n\}$,

$$d_i = a_0 \cdot b_i + a_1 \cdot b_{i-1} + \cdots + a_{i-1} \cdot b_1 + a_i \cdot b_0.$$

注意這裡, 當 $j > n$ 時我們令 $a_j = 0$ 且 當 $k > m$ 時我們令 $b_k = 0$. 其實這就是我們熟知一般多項式的加法與乘法: 當相加時就是將同次項的係數相加; 相乘就是各項先展開後再合併同次項.

經由一番的驗算我們可以得到 $F[x]$ 是一個 commutative ring with 1, 這裡我們就略去驗算過程了. 不過要強調一下 $F[x]$ 這個 ring 的加法 identity 0 就是 0 多項

式, 也就是各項係數都是 0 (這裡的 0 是 F 的 0) 的多項式. 而乘法的 identity 1 就是 1 這一個常數多項式, 也就是常數項為 1 (這裡的 1 是 F 的 1) 其他項係數都是 0. 通常我們稱 $F[x]$ 為 the *ring of polynomials in x over F*.

當我們碰到一個新的 ring 時, 首先會問的是它的 zero divisor 和 unit 有哪些? 這裡由於我們處理的是 polynomial ring 有一個特別好用的工具來幫我們, 就是所謂的 degree.

Definition 7.2.1. 若 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ 且 $a_n \neq 0$, 則稱 $f(x)$ 的 degree 為 n 記為 $\deg(f(x)) = n$.

注意雖然 0 多項式我們看成是常數多項式, 不過由定義因為 0 多項式並找不到不為 0 的係數, 所以對 0 多項式我們不能說它的 degree 為 0. 通常我們就不訂 0 的 degree (有的書定義 $\deg(0) = -\infty$). 接下來我們來看 degree 的性質.

Lemma 7.2.2. 若 $f(x)$ 和 $g(x)$ 都是 $F[x]$ 中的非 0 多項式, 則

$$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

Proof. 若 $\deg(f(x)) = n$ 且 $\deg(g(x)) = m$ 也就是說 $f(x) = a_0 + a_1x + \cdots + a_nx^n$ 及 $g(x) = b_0 + b_1x + \cdots + b_mx^m$, 其中 $a_n \neq 0$ 且 $b_m \neq 0$. 現考慮 $f(x) \cdot g(x) = \sum c_kx^k$, 其中 $c_k = \sum_{i+j=k} a_i \cdot b_j$. 首先我們證明當 $k > n+m$ 時 $c_k = 0$. 若 $i \leq n$ 且 $j \leq m$, 則 $i + j \leq n + m$. 由此知當 $k > n + m$ 時若 $i + j = k$, 則 $i > n$ 或 $j > m$. 也就是說 $a_i = 0$ 或 $b_j = 0$. 故知當 $k > n + m$ 時 $c_k = 0$. 而當 $k = n + m$ 時, 考慮 $i + j = k$ 我們也可知唯有當 $i = n$ 且 $j = m$ 時 $a_i \neq 0$ 且 $b_j \neq 0$. 換句話說 $c_{n+m} = a_n \cdot b_m$. 由於 F 是一個 field, 所以 F 沒有 zero divisor, 故由 $a_n \neq 0$ 且 $b_m \neq 0$ 可得 $c_{n+m} \neq 0$. 換句話說 $\deg(f(x) \cdot g(x)) = n + m$. □

由 Lemma 7.2.2, 我們馬上可以知道 $F[x]$ 的 zero divisor 和 unit 有哪些.

Proposition 7.2.3. 令 F 是一個 *field.*

(1) $F[x]$ 中沒有 *zero divisor,* 換句話說 $F[x]$ 是一個 *integral domain.*

(2) $F[x]$ 中的 *unit* 就是所有非 0 的常數.

Proof. (1) 任取 $f(x), g(x) \in F[x]$ 且皆不為 0. 若 $\deg(f(x)) = n$ 且 $\deg(g(x)) = m$, 則由 Lemma 7.2.2 知 $deg(f(x) \cdot g(x)) = n + m$. 換句話說, $f(x) \cdot g(x)$ 的 x^{n+m} 項係數不為 0. 故知 $f(x) \cdot g(x)$ 不為 0 多項式. 故得證 $F[x]$ 沒有 zero divisor.

(2) 若 $f(x)$ 是 $F[x]$ 中的一個 unit, 依定義知存在 $g(x) \in F[x]$ 使得 $f(x) \cdot g(x) = 1$. 因為 1 是常數多項式其 degree 為 0, 故由 Lemma 7.2.2 知 $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)) = 0$. 又 $\deg(f(x)) \geq 0$ 且 $\deg(g(x)) \geq 0$, 故得 $\deg(f(x)) = 0$ 換句話說 $f(x)$ 是常數多項式. 又 0 不可能是 unit, 故得 $f(x)$ 是一個非 0 的常數. 反之, 若 $f(x) = c$ 是一個非 0 的常數, 也就是 $c \in F$ 且 $c \neq 0$. 因 F 是一個 field,

在 F 中可以找到 c 的 inverse c^{-1}. 故令 $g(x) = c^{-1} \in F[x]$, 則 $f(x) \cdot g(x) = 1$. 故知 $f(x) = c$ 是一個 unit. □

接下來我們來看 polynomial ring 的餘式定理.

Theorem 7.2.4 (Euclid's Algorithm)**.** *若 F 是一個 field, 給定兩 polynomials $f(x)$, $g(x) \in F[x]$, 其中 $g(x) \neq 0$, 則存在 $h(x)$, $r(x) \in F[x]$ 滿足 $f(x) = h(x) \cdot g(x) + r(x)$, 其中 $r(x) = 0$ 或 $\deg(r(x)) < \deg(g(x))$.*

Proof. 首先要注意, 這裡的餘式 $r(x)$ 由於可能是 0, 而 0 又沒有 degree, 所以我們不能只說 $\deg(r(x)) < \deg(g(x))$, 而必須加上 $r(x) = 0$ 這個可能性.

我們利用和 Theorem 7.1.1 相似的證明考慮 $W = \{f(x) - l(x) \cdot g(x) \mid l(x) \in F[x]\}$ 這一個集合. 如果 $0 \in W$, 也就是說存在 $h(x) \in F[x]$ 使得 $f(x) - h(x) \cdot g(x) = 0$, 故得證 $r(x) = 0$. 如果 $0 \notin W$, 則令 $r(x) \in W$ 是 W 中 degree 最小的 polynomial. 假設 $\deg(r(x)) = m$ 且 $\deg(g(x)) = n$, 我們想用反證法證明 $m < n$. 如果 $m \geq n$, 假設 $r(x)$ 的最高次 x^m 項的係數為 a, 而 $g(x)$ 的最高次 x^n 項係數為 b. 由於 $b \in F$ 且 $b \neq 0$, 考慮 $s(x) = r(x) - ((a \cdot b^{-1})x^{m-n}) \cdot g(x)$ 這個多項式. 由於 $r(x)$ 和 $((a \cdot b^{-1})x^{m-n}) \cdot g(x)$ 的最高次 x^m 的係數皆為 a, 故知 $\deg(s(x)) < m = \deg(r(x))$. 另外由假設 $r(x) \in W$ 知存在 $l(x) \in F[x]$ 使得 $r(x) = f(x) - l(x) \cdot g(x)$. 故得

$$s(x) = f(x) - l(x) \cdot g(x) - ((a \cdot b^{-1})x^{m-n}) \cdot g(x) = f(x) - (l(x) + (a \cdot b^{-1})x^{m-n}) \cdot g(x) \in W.$$

也就是說 $s(x)$ 是 W 中一個比 $r(x)$ degree 小的 polynomial, 此和 $r(x)$ 是 W 中 degree 最小的假設相矛盾. 故得 $m < n$ 也就是說存在 $h(x) \in F[x]$ 使得 $r(x) = f(x) - h(x) \cdot g(x)$ 且 $\deg(r(x)) < \deg(g(x)$. 故得證本定理. □

Remark 7.2.5. 這裡要強調一下, 在 Theorem 7.2.4 的証明中我們用到了 F 是一個 field 的性質 (即 $g(x)$ 的最高次係數 b 的 inverse b^{-1} 存在). 所以 Theorem 7.2.4 並不能套用到係數為一般的 ring 的 polynomials 上. 事實上在 $\mathbb{Z}[x]$ 中就沒有餘式定理. 例如考慮 $f(x) = x^2$, $g(x) = 2x$ 我們就沒辦法找到整係數的多項式 $h(x)$ 使得 $f(x) - h(x) \cdot g(x) = 0$ 或是 $\deg(f(x) - h(x) \cdot g(x)) < \deg(g(x))$.

我們曾利用整數的餘數定理 (Theorem 7.1.1) 證得 $\mathbb{Z}$ 中的 ideal 皆是 principle ideal (Theorem 7.1.2). 同樣的利用餘式定理 (Theorem 7.2.4), 我們可得以下的定理.

Theorem 7.2.6. *若 F 是一個 field, 則 $F[x]$ 中的 ideal 都是 principle ideal.*

Proof. 任取 $F[x]$ 的一個 ideal, I. 我們希望在 I 中找到一元素 $g(x)$ 使得 $\big(g(x)\big) = I$. 令 $g(x)$ 是 I 中 degree 最小的 polynomial, 我們希望證得 $\big(g(x)\big) = I$.

首先由於 $g(x) \in I$ 所以當然 $\big(g(x)\big) \subseteq I$. 反之, 要證明 $I \subseteq \big(g(x)\big)$ 也就是說任取 $f(x) \in I$ 都要找到 $h(x) \in F[x]$ 使得 $f(x) = h(x) \cdot g(x)$. 利用 Theorem 7.2.4 我們知道存在 $h(x), r(x) \in F[x]$ 使得 $f(x) = h(x) \cdot g(x) + r(x)$ 其中 $r(x) = 0$ 或 $\deg(r(x)) < \deg(g(x))$. 然而 $g(x), f(x) \in I$, 故得 $r(x) = f(x) - h(x) \cdot g(x) \in I$. 如

果 $r(x) \neq 0$, 表示 $r(x)$ 是 I 中一個比 $g(x)$ degree 還小的 polynomial, 這和當初 $g(x)$ 的選取相矛盾. 故知 $r(x) = 0$, 即 $f(x) = h(x) \cdot g(x) \in \big(g(x)\big)$. □

接下來要談 $F[x]$ 上多項式的分解. 所以還是給因式, 公因式和最大公因式下一個定義.

Definition 7.2.7. 令 $f(x), g(x) \in F[x]$.

(1) 若 $d(x) \in F[x]$ 且存在 $h(x) \in F[x]$ 使得 $f(x) = h(x) \cdot d(x)$, 則稱 $d(x)$ 是 $f(x)$ 的一個 *divisor*, 記做 $d(x) \,|\, f(x)$.

(2) 若 $l(x) \in F[x]$, 且 $l(x) \,|\, f(x)$ 及 $l(x) \,|\, g(x)$, 則稱 $l(x)$ 為 $f(x), g(x)$ 的 *common divisor*.

(3) 若 $d(x) \in F[x]$ 是 $f(x), g(x)$ 的 common divisor 中 degree 最大的 polynomial, 則稱 $d(x)$ 為 $f(x), g(x)$ 的 *greatest common divisor*.

要注意這裡 greatest common divisor 並不唯一. 有的書會定 greatest common divisor 是所有 common divisor 中 degree 最大且最高次係數為 1 的 polynomial, 若在此定義之下 greatest common divisor 就唯一了.

一般可以利用所謂的輾轉相除法將兩個多項式的 greatest common divisor 求出來, 在這裡我們將利用 Theorem 7.2.6 找到 greatest common divisor 並得到其基本性質.

Proposition 7.2.8. 給定 $f(x), g(x) \in F[x]$, 則存在 $d(x) \in F[x]$ 滿足 $\big(d(x)\big) = \big(f(x)\big) + \big(g(x)\big)$ 且 $d(x)$ 為 $f(x), g(x)$ 的 *greatest common divisor*

Proof. 由 Theorem 7.1.2 知存在 $d(x) \in F[x]$ 使得 $\big(d(x)\big) = \big(f(x)\big) + \big(g(x)\big)$. 接著我們要證明這個 $d(x) \in F[x]$ 是 $f(x), g(x)$ 的 greatest common divisor. 首先當然是要證 $d(x)$ 是 $f(x), g(x)$ 的 common divisor. 然而因 $f(x) \in \big(f(x)\big) \subseteq \big(f(x)\big) + \big(g(x)\big) = \big(d(x)\big)$, 故知存在 $h(x) \in F[x]$ 使得 $f(x) = h(x) \cdot d(x)$. 也就是說 $d(x) \,|\, f(x)$. 同理, 由 $g(x) \in \big(d(x)\big)$ 可得 $d(x) \,|\, g(x)$. 故知 $d(x)$ 是 $f(x), g(x)$ 的 common divisor.

那為甚麼 $d(x)$ 會是 $f(x), g(x)$ 的 common divisor 中 degree 最大的呢? 由於 $d(x) \in \big(d(x)\big) = \big(f(x)\big) + \big(g(x)\big)$, 我們知道存在 $m(x), n(x) \in F[x]$ 使得 $d(x) = m(x) \cdot f(x) + n(x) \cdot g(x)$. 然而若 $l(x)$ 是 $f(x), g(x)$ 的 common divisor, 即 $l(x) \,|\, f(x)$ 且 $l(x) \,|\, g(x)$, 知存在 $r(x), s(x) \in F[x]$ 使得 $f(x) = r(x) \cdot l(x)$ 且 $g(x) = s(x) \cdot l(x)$. 因此得

$$d(x) = m(x) \cdot (r(x) \cdot l(x)) + n(x) \cdot (s(x) \cdot l(x)) = (m(x) \cdot r(x) + n(x) \cdot s(x)) \cdot l(x).$$

也就是說 $l(x) \,|\, d(x)$. 所以知 $d(x)$ 是所有 $f(x), g(x)$ 的 common divisor 中 degree 最大的. □

Proposition 7.2.8 不只告訴我們如何找到 greatest common divisor, 事實上在證明中我們也證得 greatest common divisor 的兩個重要性質.

Corollary 7.2.9. 令 $f(x), g(x) \in F[x]$ 且 $d(x)$ 為 $f(x), g(x)$ 的 *greatest common divisor,* 則 $d(x)$ 符合以下兩性質*:*

(1) 存在 $m(x), n(x) \in F[x]$ 滿足 $d(x) = m(x) \cdot f(x) + n(x) \cdot g(x)$.

(2) 假設 $l(x) \,|\, f(x)$ 且 $l(x) \,|\, g(x)$, 則 $l(x) \,|\, d(x)$.

一般在一個 ring 中元素的分解, 我們是不將 unit 列入考慮. 例如在 $\mathbb{Z}$ 中的分解我們都不將 1 和 -1 列為因數來考慮. 在 $F[x]$ 中的 units 是所有非 0 的常數多項式 (Proposition 7.2.3), 所以我們也不考慮它們為真正的 divisor. 因此我們有以下不可分解多項式 (irreducible element) 的定義.

Definition 7.2.10. 考慮 $F[x]$ 中的元素 $p(x)$.

(1) 若對任意滿足 $d(x) \,|\, p(x)$ 的 $d(x) \in F[x]$, 皆有 $d(x) = c$ 或 $d(x) = c \cdot p(x)$, 其中 $0 \neq c \in F$, 則稱 $p(x)$ 是一個 *irreducible element.*

(2) 若對任意滿足 $p(x) \,|\, f(x) \cdot g(x)$ 的 $f(x), g(x) \in F[x]$ 皆有 $p(x) \,|\, f(x)$ 或 $p(x) \,|\, g(x)$, 則稱 $p(x)$ 是一個 *prime element.*

簡單來說一個 irreducible element 表示它不可以寫成兩個 degree 比它小的 polynomial 的乘積. 很顯然 irreducible 和 prime 這兩種定義是不一樣的, 不過下一個定理告訴我們在 $F[x]$ 中這兩種定義的 polynomial 是相同的.

Proposition 7.2.11. 在 $F[x]$ 中若 $p(x)$ 是一個 *irreducible element,* 則 $p(x)$ 是一個 *prime element. 反之, 若* $p(x)$ 是一個 *prime element,* 則 $p(x)$ 是一個 *irreducible element.*

Proof. 首先我們證若 $p(x)$ 是 irreducible 則 $p(x)$ 是 prime. 也就是說假設已知 $p(x)$ 是 irreducible. 任取 $p(x) \,|\, f(x) \cdot g(x)$ 我們要證明: $p(x) \,|\, f(x)$ 或 $p(x) \,|\, g(x)$. 然而 $p(x) \,|\, f(x) \cdot g(x)$ 表示存在 $r(x) \in F[x]$ 使得 $f(x) \cdot g(x) = r(x) \cdot p(x)$. 如果 $p(x) \,|\, f(x)$ 那麼就得到我們要證的, 所以我們只要討論 $p(x) \nmid f(x)$ 的情況. 此時我們考慮 $p(x), f(x)$ 的 greatest common divisor 令之為 $d(x)$. 由於 $d(x) \,|\, p(x)$ 故由 $p(x)$ 是 irreducible 的假設知 $d(x) = c$ 或 $d(x) = c \cdot p(x)$, 其中 $0 \neq c \in F$. 然而 $d(x)$ 不可能等於 $c \cdot p(x)$, 否則由 $d(x)$ 是 $p(x), f(x)$ 的 common divisor 知 $p(x) = c^{-1} \cdot d(x) \,|\, f(x)$ (注意 c 是 $F[x]$ 的 unit). 此和 $p(x) \nmid f(x)$ 矛盾. 因此知 $d(x) = c$, 由 Corollary 7.2.9 知存在 $n(x), m(x) \in F[x]$ 滿足 $c = n(x) \cdot p(x) + m(x) \cdot f(x)$. 等式兩邊乘上 $c^{-1} \cdot g(x)$ 得

$$\begin{aligned} g(x) &= c^{-1}\big(n(x) \cdot g(x)\big) \cdot p(x) + c^{-1}\big(m(x) \cdot (f(x) \cdot g(x))\big) \\ &= c^{-1}\big(n(x) \cdot g(x) + m(x) \cdot r(x)\big) \cdot p(x), \end{aligned}$$

所以 $p(x) \,|\, g(x)$.

反之, 若已知 $p(x)$ 是一個 prime element 我們要證明 $p(x)$ 是 irreducible. 也就是證明若 $d(x) \,|\, p(x)$, 則 $d(x) = c$ 或 $d(x) = c \cdot p(x)$. 然而 $d(x) \,|\, p(x)$ 表示存在

$r(x) \in F[x]$ 滿足 $p(x) = r(x) \cdot d(x)$, 也就是說 $p(x) \,|\, r(x) \cdot d(x)$. 故由 $p(x)$ 是 prime 的假設, 我們得 $p(x) \,|\, d(x)$ 或 $p(x) \,|\, r(x)$. 當 $p(x) \,|\, d(x)$ 時, 表示存在 $s(x) \in F[x]$ 使得 $d(x) = s(x) \cdot p(x)$. 由原先假設 $p(x) = r(x) \cdot d(x)$ 知 $d(x) = (s(x) \cdot r(x)) \cdot d(x)$. 也就是說 $d(x) \cdot (s(x) \cdot r(x) - 1) = 0$, 利用 $F[x]$ 沒有 zero divisor (Proposition 7.2.3) 及 $d(x) \neq 0$, 知 $s(x) \cdot r(x) = 1$, 即 $s(x)$ 是 unit. 也就是說 $s(x)$ 是一個常數多項式 c, 故得 $d(x) = s(x) \cdot p(x) = c \cdot p(x)$. 當 $p(x) \,|\, r(x)$ 時, 表示存在 $s(x) \in F[x]$ 滿足 $r(x) = s(x) \cdot p(x)$. 故由 $p(x) = d(x) \cdot r(x) = d(x) \cdot (s(x) \cdot p(x))$ 得 $d(x) \cdot s(x) = 1$. 表示 $d(x)$ 是 $F[x]$ 的 unit, 即 $d(x) = c$. □

從前面幾個定理看來, 不難發現 $\mathbb{Z}$ 的很多重要性質都可以推導到 $F[x]$ 上. 大家應該也會猜測 $F[x]$ 也會有和 $\mathbb{Z}$ 相似的唯一分解定理. 前面提過在談分解時我們不會把 unit 的差異納入考慮, 這就是為甚麼我們在 $\mathbb{Z}$ 中談因數時只考慮正數. 在 $F[x]$ 中若 $d(x)$ 是 $f(x)$ 的 divisor, 即存在 $h(x) \in F[x]$ 使得 $f(x) = d(x) \cdot h(x)$, 則對任意 $F[x]$ 中不等於 0 的常數 c 因為其為 $F[x]$ 的 unit, 當然我們知 $c^{-1} \cdot h(x) \in F[x]$. 因此由 $f(x) = (c \cdot d(x)) \cdot (c^{-1} \cdot h(x))$ 得到 $c \cdot d(x)$ 也是 $f(x)$ 的 divisor. 所以對所有的 $0 \neq c \in F$, 從分解的觀點我們將 $d(x)$ 和 $c \cdot d(x)$ 看成是 $f(x)$ 一樣的 divisor. 我們需要一個方法來選取一個適當的 $c \cdot d(x)$ 來當 $f(x)$ 的 divisor. 一般習慣上我們習慣選取 c 使得 $c \cdot d(x)$ 的最高次項係數為 1, 因此有以下的定義.

Definition 7.2.12. 若 $f(x) \in F[x]$ 且 $f(x)$ 的最高次項係數為 1 則稱 $f(x)$ 為一個 *monic polynomial*.

以下一個 Lemma 告訴我們選取 monic polynomial 的好處.

Lemma 7.2.13. 假設 $p(x), q(x) \in F[x]$ 都是 *monic irreducible element* 且 $p(x) \,|\, q(x)$, 則 $p(x) = q(x)$.

Proof. 由於 $q(x)$ 是 irreducible, $q(x)$ 的 divisor 只能是常數 c 或 $c \cdot q(x)$ 這種形式. 故由 $p(x)$ 不是常數 (因假設是 irreducible) 且 $p(x) \,|\, q(x)$ 知存在 $c \in F$ 滿足 $p(x) = c \cdot q(x)$. 不過由於 $p(x), q(x)$ 都是 monic polynomial, 它們的最高次項係數都是 1. 故得 $c = 1$, 即 $p(x) = q(x)$. □

現在我們就來看 $F[x]$ 上的唯一分解性質應該是甚麼樣子.

Theorem 7.2.14. 假設 $f(x) \in F[x]$ 且 $\deg(f(x)) \geq 1$, 則存在 $c \in F$ 以及 $p_1(x), \ldots, p_r(x)$, 其中這些 $p_i(x)$ 是相異的 *monic irreducible elements,* 滿足

$$f(x) = c \cdot p_1(x)^{n_1} \cdots p_r(x)^{n_r}, \quad n_i \in \mathbb{N}, \forall i \in \{1, \ldots, r\}.$$

如果 $f(x)$ 可以分解成另外的形式 $f(x) = d \cdot q_1(x)^{m_1} \cdots q_s(x)^{m_s}$, 其中 $d \in F$ 而且這些 $q_i(x)$ 是相異的 *monic irreducible elements,* 則 $c = d$, $r = s$ 且經過變換順序可得 $p_i(x) = q_i(x)$, $n_i = m_i$, $\forall\, i \in \{1, \ldots, r\}$.

Proof. 我們利用和 Theorem 7.1.8 類似的方法來證明. Theorem 7.1.8 用到了數學歸納法, 這裡雖然我們談的不是整數, 不過由於我們有 degree 這個很好的工具將 $F[x]$ 的元素送到整數, 所以我們可以對 degree 做 induction.

首先來看存在性 (也就是 $f(x)$ 可以寫成所要求的形式): 當 $\deg(f(x)) = 1$ 時由於 $f(x) = ax + b$, 其中 $0 \neq a \in F$, 所以我們可以將 $f(x)$ 寫成 $a \cdot (x + b \cdot a^{-1})$. 很顯然的 $x + b \cdot a^{-1}$ 不可能寫成兩個 degree 小於 1 的 polynomial 的乘積, 所以 $x + b \cdot a^{-1}$ 是一個 monic irreducible element. 所以在這情況存在性是成立的. 接著假設對所有 degree 介於 1 和 $n-1$ 間的 polynomials 存在性是成立的. 現在考慮 $\deg(f(x)) = n$ 情況. 如果 $f(x)$ 是 irreducible 且其最高次項係數為 a, 那麼 $a^{-1} \cdot f(x)$ 當然是一個 monic irreducible element, 所以 $f(x) = a \cdot (a^{-1} \cdot f(x))$, 存在性自然成立. 如果 $f(x)$ 不是 irreducible, 則知 $f(x) = g(x) \cdot h(x)$ 其中 $g(x), h(x) \in F[x]$ 且 $1 \leq \deg(g(x)) < n$ 及 $1 \leq \deg(h(x)) < n$. 故利用歸納假設知

$$g(x) = c_1 \cdot p_1(x)^{n_1} \cdots p_u(x)^{n_u} \text{ 和 } h(x) = c_2 \cdot \tilde{p_1}(x)^{m_1} \cdots \tilde{p_v}(x)^{m_v},$$

其中 $p_i(x), \tilde{p_j}(x)$ 都是 monic irreducible elements, 所以將相同的 monic irreducible elements 合併, 得證 $f(x)$ 也可以寫成所要求的形式.

接下來看唯一性: 假設 $\deg(f(x)) = 1$, 由於 $f(x) = ax + b$, 其唯一性自然成立. 接著假設唯一性對所有 degree 介於 1 和 $n-1$ 間的 polynomials 都成立, 現在考慮 $\deg(f(x)) = n$ 的情況. 假設

$$f(x) = c \cdot p_1(x)^{n_1} \cdots p_r(x)^{n_r} = d \cdot q_1(x)^{m_1} \cdots q_s(x)^{m_s},$$

其中 $c, d \in F$, $p_i(x)$ 是兩兩相異, $q_j(x)$ 也是兩兩相異, 而且 $p_i(x), q_j(x)$ 都是 monic irreducible element. 首先觀察, 由於 $p_i(x), q_j(x)$ 都是 monic, 所以 c 和 d 應該都是 $f(x)$ 最高次項的係數. 一個 polynomial 的最高次項應該是唯一的, 故得 $c = d$. 接著由於 $p_1(x)$ 是 irreducible 所以由 Proposition 7.2.11 知其為 prime, 故由 $p_1(x) \,|\, f(x) = cq_1(x)^{m_1} \cdots q_s(x)^{m_s}$ 知存在某個 $j \in \{1, \ldots, s\}$ 滿足 $p_1(x) \,|\, q_j(x)$. 變換一下順序我們可以假設 $p_1(x) \,|\, q_1(x)$, 故利用 $p_1(x)$ 和 $q_1(x)$ 都是 monic irreducible element 以及 Lemma 7.2.13 知 $p_1(x) = q_1(x)$. 因此我們可將 $f(x)$ 的分解改寫成

$$f(x) = c \cdot p_1(x)^{n_1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} = c \cdot p_1(x)^{m_1} \cdot q_2(x)^{m_2} \cdots q_s(x)^{m_s}.$$

將上式移項再提出 $c \cdot p_1(x)$, 我們可得

$$c \cdot p_1(x) \cdot \left(p_1(x)^{n_1 - 1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} - p_1(x)^{m_1 - 1} \cdot q_2(x)^{m_2} \cdots q_s(x)^{m_s}\right) = 0.$$

由於 $c \cdot p_1(x) \neq 0$ 且 $F[x]$ 是 integral domain, 我們得

$$p_1(x)^{n_1 - 1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} - p_1(x)^{m_1 - 1} \cdot q_2(x)^{m_2} \cdots q_s(x)^{m_s} = 0.$$

現令 $g(x) = p_1(x)^{n_1 - 1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r}$. 由於

$$\deg(g(x)) = \deg(f(x)) - \deg(p_1(x)) < \deg(f(x)) = n$$

且

$$g(x) = p_1(x)^{n_1-1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} = p_1(x)^{m_1-1} \cdot q_2(x)^{m_2} \cdots q_s(x)^{m_s}$$

是 $g(x)$ 的兩個分解, 故利用歸納法假設我們有 $r = s$ 且 $p_1(x) = q_1(x), \ldots, p_r(x) = q_r(x)$ 以及 $n_1 = m_1$, $n_2 = m_2, \ldots, n_r = m_r$, 故得證唯一性. □

7.3. Polynomials over the Integers

前一章節的結果當然都可以套用到有理係數的 polynomials, 但卻不能完完整整的套用到整係數的 polynomials. 這一章我們將看看整係數和有理係數 polynomials 的異同. 最後再利用前面章節提到整數的唯一分解性以及有理係數的 polynomial ring 的唯一分解性, 得到整係數的 polynomial ring 的唯一分解性.

我們令 $\mathbb{Q}[x]$ 表示所有有理係數 polynomials 所成的集合且令 $\mathbb{Z}[x]$ 表示所有整係數 polynomials 所成的集合. 前面已知 $\mathbb{Q}[x]$ 用一般的加法和乘法可形成一個 ring, 我們稱之為 polynomial ring over $\mathbb{Q}$. 同理我們也可以證出 $\mathbb{Z}[x]$ 也是一個 ring, 我們稱之為 polynomial ring over $\mathbb{Z}$.

$\mathbb{Z}[x]$ 的 0 和 1 和 $\mathbb{Q}[x]$ 的 0 和 1 相同. 我們也可在 $\mathbb{Z}[x]$ 中定義 degree (反正可以把 $\mathbb{Z}[x]$ 看成 $\mathbb{Q}[x]$ 的子集合). 所以利用和 Lemma 7.2.3 相同的證明, 我們可得 $\mathbb{Z}[x]$ 是一個 integral domain. $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 最大的不同是 $\mathbb{Q}[x]$ 中所有非 0 的常數都是 unit, 然而 $\mathbb{Z}[x]$ 中只有 ± 1 這兩個常數為其 unit. 這是因為利用 Lemma 7.2.3 的證明我們知道 $\mathbb{Z}[x]$ 中的 unit 其 degree 一定是 0, 所以只有常數才可能是 $\mathbb{Z}[x]$ 的 unit, 然而因我們只考慮整係數, 所以在 $\mathbb{Z}$ 中的 unit 才可以是 $\mathbb{Z}[x]$ 的 unit, 也就是 ± 1. 因此這裡我們必須提醒大家, 在 $\mathbb{Z}[x]$ 中談分解時要將常數的分解列入考慮.

在 Remark 7.2.5 中我們提及 $\mathbb{Z}[x]$ 中並沒有餘式定理, 所以在 $\mathbb{Q}[x]$ 中可利用餘式定理得到的所有 ideal 都是 principle ideal (Theorem 7.2.6) 對 $\mathbb{Z}[x]$ 就不一定對. 事實上我們可以在 $\mathbb{Z}[x]$ 中找到一個 (當然不只一個) ideal 它不是 principle ideal.

Example 7.3.1. 我們要說明在 $\mathbb{Z}[x]$ 中 $I = (2) + (x)$ 不是 principle ideal. 假設 I 是 principle ideal, 即存在 $f(x) \in \mathbb{Z}[x]$ 使得 $I = \big(f(x)\big)$. 利用 $2 \in I$, 我們得到 $2 \in \big(f(x)\big)$, 也就是存在 $h(x) \in \mathbb{Z}[x]$ 滿足 $2 = h(x) \cdot f(x)$. 利用 degree 馬上可知 $\deg(f(x)) = 0$, 也就是說 $f(x)$ 是一個常數 $c \in \mathbb{Z}$. 現在利用 $x \in I = \big(c\big)$ 知存在 $g(x) \in \mathbb{Z}[x]$ 使得 $x = c \cdot g(x)$. 注意 $c \cdot g(x)$ 這一個多項式它的係數一定是 c 的倍數 (別忘了 $g(x) \in \mathbb{Z}[x]$, 所以 $g(x)$ 的係數都是整數). 因此由 $x = c \cdot g(x)$ 知 x 這一個多項式的係數應該是 c 的倍數. 然而 x 這一個多項式只有 x 這一項且其係數是 1, 故得 $c \,|\, 1$, 也就是 $c = \pm 1$. 因 c 是 unit, Lemma 6.2.4 告訴我們 $I = \big(c\big) = \mathbb{Z}[x]$, 換句話說 $1 \in I = \big(2\big) + \big(x\big)$. 利用 $\big(2\big) + \big(x\big)$ 的定義知這表示存在 $n(x), m(x) \in \mathbb{Z}[x]$ 使得 $1 = 2 \cdot n(x) + x \cdot m(x)$. 不過 $x \cdot m(x)$ 沒有常數項, 而 $2 \cdot n(x)$ 的常數項一定是 2 的倍數, 所以 $2 \cdot n(x) + x \cdot m(x)$ 的常數項一定不可能為 1. 故當 $n(x), m(x) \in \mathbb{Z}[x]$ 時 $1 = 2 \cdot n(x) + x \cdot m(x)$ 不可能成立. 此矛盾發生於我們的假設 I 是 principle ideal, 故得 $I = \big(2\big) + \big(x\big)$ 不可能是 $\mathbb{Z}[x]$ 的 principle ideal.

好了既然 $\mathbb{Z}[x]$ 中的 ideal 不一定是 principle ideal 那麼我們就不能學 Proposition 7.2.11 的方法得到 $\mathbb{Z}[x]$ 中的 irreducible element 就是 prime element 了. 不能用這套方法並不表示結果會錯, 因為有可能用另一套方法可以得到想要的結果啊! 沒錯我們將會證明在 $\mathbb{Z}[x]$ 中的 irreducible element 和 prime element 是相同的, 不過我們要發展另一套的方法來得到.

這個方法其實就是要克服前面提到 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 最大的不同就是在 $\mathbb{Z}[x]$ 中要考慮常數的分解. 給定 $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ 要將 $f(x)$ 分解成 degree 比較小的 polynomials 相乘之前, 可以先考慮可不可以提出一個常數出來 (因為若這個常數不是 ± 1 那麼在 $\mathbb{Z}[x]$ 中這就算是一個"有效"的分解). 可以提出甚麼常數出來呢? 大家都會想到提出那些係數 $a_0, a_1, \ldots, a_n$ 的最大公因數吧! 所以我們有以下簡單但重要之結果.

Lemma 7.3.2. *若 $f(x) \in \mathbb{Z}[x]$ 是一個非 0 的 polynomial, 則 $f(x)$ 可唯一寫成 $f(x) = c \cdot f^*(x)$, 其中 $c \in \mathbb{N}$, $f^*(x) \in \mathbb{Z}[x]$ 且 $f^*(x)$ 的係數的最大公因數是 1.*

Proof. 首先證明存在性: 若 $f(x) = a_0 + a_1x + \cdots + a_nx^n$, 令 $d = \gcd(a_0, a_1, \ldots, a_n)$. 由最大公因數的性質知 $a_0 = d \cdot b_0$, $a_1 = d \cdot b_1, \ldots, a_n = d \cdot b_n$ 且 $\gcd(b_0, b_1, \ldots, b_n) = 1$. 故可將 $f(x)$ 寫成 $d \cdot (b_0 + b_1x + \cdots + b_nx^n)$ 為所要求的形式.

接著證明唯一性: 假設 $f(x) = c \cdot f^*(x)$, 其中 $c \in \mathbb{N}$ 且 $f^*(x) \in \mathbb{Z}[x]$. 將 c 乘入 $f^*(x)$ 的各項係數中, 知 $f(x)$ 的所有係數 $a_0, a_1, \ldots, a_n$ 都會是 c 的倍數. 也就是 c 是 $a_0, a_1, \ldots, a_n$ 的公因數. 如果 $c \neq d = \gcd(a_0, a_1, \ldots, a_n)$, 則 $f^*(x)$ 的係數中會有 d/c 這一個不是 1 的公因數, 此和 $f^*(x)$ 的各項係數的最大公因數為 1 相矛盾. 故得 $d = c$, 也就是說 $d \cdot f^*(x) = d \cdot (b_0 + b_1x + \cdots + b_nx^n)$. 最後因 $\mathbb{Z}[x]$ 是 integral domain, 我們得 $f^*(x) = b_0 + b_1x + \cdots + b_nx^n$. □

有了 Lemma 7.3.2, 我們有以下的定義.

Definition 7.3.3. *若 $f(x) \in \mathbb{Z}[x]$ 可寫成 $f(x) = c \cdot f^*(x)$, 其中 $c \in \mathbb{N}$, $f^*(x) \in \mathbb{Z}[x]$ 且 $f^*(x)$ 的係數的最大公因數是 1. 則稱 c 為 $f(x)$ 的 content, 記為 $c(f)$. 若 $f(x) \in \mathbb{Z}[x]$ 且 $c(f) = 1$, 則稱 $f(x)$ 是一個 primitive polynomial.*

其實 $c(f)$ 就是 $f(x)$ 的所有係數的最大公因數. Lemma 7.3.2 告訴我們說任意的 $f(x) \in \mathbb{Z}[x]$ 都可以寫成其 content 乘上一個 primitive polynomial. 我們可以將 Lemma 7.3.2 推廣到 $\mathbb{Q}[x]$ 中.

Proposition 7.3.4. *若 $f(x) \in \mathbb{Q}[x]$ 是一個非 0 的 polynomial, 則 $f(x)$ 可唯一寫成 $f(x) = c \cdot f^*(x)$, 其中 $c \in \mathbb{Q}$, $c > 0$ 且 $f^*(x) \in \mathbb{Z}[x]$ 是一個 primitive polynomial.*

Proof. 首先證明存在性: 若 $f(x) = a_0 + a_1x + \cdots + a_nx^n$, 其中 $a_i \in \mathbb{Q}$. 我們可找到一正整數 m 使得 $m \cdot f(x) \in \mathbb{Z}[x]$ (比方說令 m 為這些 a_i 分母的乘積). 既然 $m \cdot f(x) \in \mathbb{Z}[x]$ 由 Lemma 7.3.2 的存在性知存在正整數 a 以及 $f^*(x) \in \mathbb{Z}[x]$ 其中

$f^*(x)$ 是 primitive polynomial, 使得 $m \cdot f(x) = a \cdot f^*(x)$. 故得

$$f(x) = \frac{a}{m} \cdot f^*(x)$$

為所要求的形式.

至於唯一性我們假設 $f(x) = d \cdot f^*(x) = d' \cdot g(x)$ 其中 d, d' 都是正的有理數而 $f^*(x), g(x) \in \mathbb{Z}[x]$ 都是 primitive polynomials. 將 d 和 d' 分別寫成 a/b 和 a'/b', 其中 $a, a', b, b' \in \mathbb{N}$. 我們可得

$$(a \cdot b') \cdot f^*(x) = (a' \cdot b) \cdot g(x).$$

別忘了 $(a \cdot b') \cdot f^*(x), (a' \cdot b) \cdot g(x) \in \mathbb{Z}[x]$ 又因 $a \cdot b', a' \cdot b \in \mathbb{N}$ 且 $f^*(x), g(x)$ 都是 primitive polynomial, 由 Lemma 7.3.2 的唯一性知: $a \cdot b' = b \cdot a'$ (即 $d = d'$) 且 $f^*(x) = g(x)$. 故得證唯一性. □

由 Proposition 7.3.4, 我們可以把 content 的定義推廣到 $\mathbb{Q}[x]$, 以後我們將會把任意的 $f(x) \in \mathbb{Q}[x]$ 寫成 $f(x) = c(f) \cdot f^*(x)$, 其中 $0 < c(f) \in \mathbb{Q}$ 是 $f(x)$ 的 content, $f^*(x) \in \mathbb{Z}[x]$ 是一個 primitive polynomial.

當 $f(x), g(x) \in \mathbb{Q}[x]$, 要計算 $f(x) \cdot g(x)$ 的 content, 其實是很複雜的. 我們必須把兩個 polynomial 乘開, 移項整理, 再通分找最大公因數. 我們當然希望 $f(x) \cdot g(x)$ 的 content 可以由 $f(x)$ 和 $g(x)$ 的 contents 直接求出就好了. 讓我們先看一個特殊例子就是 $f(x)$ 和 $g(x)$ 的 contents 都是 1 的情況.

Lemma 7.3.5 (Gauss Lemma)**.** 若 $f(x), g(x) \in \mathbb{Z}[x]$ 都是 *primitive polynomials,* 則 $f(x) \cdot g(x)$ 也是一個 *primitive polynomial.*

Proof. 設 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $g(x) = b_m x^m + \cdots + b_1 x + b_0$, 我們要用反證法證明若 $c(f) = c(g) = 1$, 則 $c(f \cdot g) = 1$. 假設 $c(f \cdot g) = d \neq 1$, 取一質數 p 使得 $p \mid d$, 也就是 p 整除 $f(x) \cdot g(x)$ 的所有係數. 然因 $c(f) = c(g) = 1$, 故必存在 a_i, b_j 使得 $p \nmid a_i$ 且 $p \nmid b_j$. 令 r 是最小的整數使得 $p \nmid a_r$ (也就是 $p \nmid a_r$, 但對任意的 $i < r$, $p \mid a_i$), 同樣的令 s 是最小的整數使得 $p \nmid b_s$. 現觀察 $f(x) \cdot g(x)$ 的 x^{r+s} 項係數:

$$\sum_{i+j=r+s} a_i \cdot b_j.$$

除了 $a_r \cdot b_s$ 以外, 其他項的 $a_i \cdot b_j$ 要不是 $i < r$ 就是 $j < s$. 否則若 $i > r$ 且 $j > s$ 那麼 $i + j > r + s$ 就不可能符合 $i + j = r + s$ 了. 如果 $i < r$ 由當初 r 的選取知 $p \mid a_i$, 故知此情況下 $p \mid a_i \cdot b_j$. 同理, 若 $j < s$ 也可得 $p \mid a_i \cdot b_j$. 總而言之, $f(x) \cdot g(x)$ 的 x^{r+s} 項的係數除了 $a_r \cdot b_s$ 外其他的 $a_i \cdot b_j$ 都可被 p 整除. 然而當初假設 $p \nmid a_r$ 且 $p \nmid b_s$, 故知 $p \nmid a_r \cdot b_s$. 也就是說 $f(x) \cdot g(x)$ 的 x^{r+s} 項的係數不可被 p 整除. 這和當初假設 p 可整除 $f(x) \cdot g(x)$ 的每一項的係數相矛盾. 故知不可能 $c(f \cdot g) \neq 1$, 所以 $f(x) \cdot g(x)$ 也是 primitive polynomial. □

有了 Gauss Lemma 對於一般的 $f(x), g(x) \in \mathbb{Q}[x]$, 我們很快的就可以計算出 $c(f \cdot g)$.

Proposition 7.3.6. 若 $f(x), g(x) \in \mathbb{Q}[x]$ 都是非 0 的 *polynomial,* 則

$$c(f \cdot g) = c(f) \cdot c(g).$$

Proof. 由 Lemma 7.3.4 知可將 $f(x)$ 和 $g(x)$ 分別寫成 $f(x) = c(f) \cdot f^*(x)$ 和 $g(x) = c(g) \cdot g^*(x)$, 其中 $f^*(x)$ 和 $g^*(x)$ 都是 primitive polynomials. 故得

$$f(x) \cdot g(x) = \big(c(f) \cdot c(g)\big) \cdot \big(f^*(x) \cdot g^*(x)\big).$$

再由 Lemma 7.3.4 知 $f(x) \cdot g(x)$ 可唯一寫成 $c(f \cdot g) \cdot h(x)$ 其中 $h(x)$ 是 primitive polynomial. 然而 Lemma 7.3.5 告訴我們 $f^*(x) \cdot g^*(x)$ 是 primitive polynomial, 故由唯一性知 $f^*(x) \cdot g^*(x) = h(x)$ 且 $c(f) \cdot c(g) = c(f \cdot g)$. □

接下來我們要談 $\mathbb{Z}[x]$ 上的分解, 首先要區分一下在 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 中的整除概念. 給定 $f(x), g(x) \in \mathbb{Z}[x]$, 我們說 $f(x) \mid g(x)$ in $\mathbb{Z}[x]$ 表示存在 $h(x) \in \mathbb{Z}[x]$ 滿足 $g(x) = h(x) \cdot f(x)$. 而我們說 $f(x) \mid g(x)$ in $\mathbb{Q}[x]$ 表示存在 $l(x) \in \mathbb{Q}[x]$ 滿足 $g(x) = l(x) \cdot f(x)$. 這裡最大的不同在於 $h(x)$ 要求落在 $\mathbb{Z}[x]$, 而 $l(x)$ 要在 $\mathbb{Q}[x]$ 即可. 所以有可能發生 $f(x) \mid g(x)$ in $\mathbb{Q}[x]$ 但 $f(x) \nmid g(x)$ in $\mathbb{Z}[x]$ 的狀況.

Lemma 7.3.7. 假設 $f(x), g(x) \in \mathbb{Z}[x]$, 且 $f(x)$ 是一個 *primitive polynomial,* 則 $f(x) \mid g(x)$ *in* $\mathbb{Z}[x]$ 若且唯若 $f(x) \mid g(x)$ *in* $\mathbb{Q}[x]$.

Proof. 假設 $f(x) \mid g(x)$ in $\mathbb{Z}[x]$ 表示存在 $h(x) \in \mathbb{Z}[x]$ 滿足 $g(x) = h(x) \cdot f(x)$. 然而 $h(x) \in \mathbb{Z}[x]$ 當然得 $h(x) \in \mathbb{Q}[x]$, 故知 $f(x) \mid g(x)$ in $\mathbb{Q}[x]$. (注意這部分我們不需要 $f(x)$ 是 primitive 的假設.)

反之, 若 $f(x) \mid g(x)$ in $\mathbb{Q}[x]$, 表示存在 $l(x) \in \mathbb{Q}[x]$ 滿足 $g(x) = l(x) \cdot f(x)$. 我們希望能證得 $l(x) \in \mathbb{Z}[x]$. 利用 Lemma 7.3.4 將 $l(x)$ 寫成 $l(x) = c(l) \cdot l^*(x)$, 其中 $l^*(x)$ 是 primitive polynomials. 故得 $g(x) = c(l) \cdot (l^*(x) \cdot f(x))$. 因為 $f(x)$ 和 $l^*(x)$ 都是 primitive polynomials, 故利用 Lemma 7.3.5 知 $l^*(x) \cdot f(x)$ 是 primitive polynomial. 再利用 Lemma 7.3.4 的唯一性知 $c(g) = c(l)$. 因 $c(g) \in \mathbb{N}$, 故得 $c(l) \in \mathbb{N}$, 且又 $l^*(x) \in \mathbb{Z}[x]$, 故由 $l(x) = c(l) \cdot l^*(x)$ 得 $l(x) \in \mathbb{Z}[x]$. □

同樣的, 我們也要區分一下在 $\mathbb{Q}[x]$ 和 $\mathbb{Z}[x]$ 中分解的不同. 若 $f(x) \in \mathbb{Z}[x]$ 我們說 $f(x)$ 在 $\mathbb{Q}[x]$ 可分解表示 $f(x)$ 可寫成 $f(x) = g(x) \cdot h(x)$, 其中 $g(x), h(x) \in \mathbb{Q}[x]$ 且 $\deg(g(x))$ 和 $\deg(h(x))$ 皆小於 $\deg(f(x))$. 但這並不表示 $f(x)$ 可以在 $\mathbb{Z}[x]$ 中分解成 $f(x) = m(x) \cdot n(x)$, 其中 $m(x), n(x) \in \mathbb{Z}[x]$. 不過下一個 Lemma 告訴我們這是辦得到的.

Lemma 7.3.8. 假設 $f(x) \in \mathbb{Z}[x]$ 且 $f(x) = g(x) \cdot h(x)$ 其中 $g(x), h(x) \in \mathbb{Q}[x]$, 則存在 $m(x), n(x) \in \mathbb{Z}[x]$ 滿足 $f(x) = m(x) \cdot n(x)$ 且 $\deg(m(x)) = \deg(g(x))$ 及 $\deg(n(x)) = \deg(h(x))$.

Proof. 利用 Lemma 7.3.4 知 $g(x) = c(g) \cdot g^*(x)$ 且 $h(x) = c(h) \cdot h^*(x)$ 其中 $g^*(x), h^*(x) \in \mathbb{Z}[x]$ 且都是 primitive polynomial. 利用 Proposition 7.3.6 知

$$c(g) \cdot c(h) = c(g \cdot h) = c(f),$$

然而 $f(x) \in \mathbb{Z}[x]$, 故 $c(g) \cdot c(h) = c(f) \in \mathbb{N}$. 因此若令 $m(x) = \big(c(g) \cdot c(h)\big) \cdot g^*(x) \in \mathbb{Z}[x]$ 及 $n(x) = h^*(x) \in \mathbb{Z}[x]$, 則

$$\begin{aligned} f(x) &= g(x) \cdot h(x) = \big(c(g) \cdot g^*(x)\big) \cdot \big(c(h) \cdot h^*(x)\big) \\ &= \big(c(g) \cdot c(h)\big) \cdot g^*(x) \cdot h^*(x) \\ &= m(x) \cdot n(x). \end{aligned}$$

又

$$\deg(m(x)) = \deg(g^*(x)) = \deg(g(x)) \quad \text{且} \quad \deg(n(x)) = \deg(h^*(x)) = \deg(h(x)).$$

□

反之若 $f(x)$ 在 $\mathbb{Z}[x]$ 可以分解成 $f(x) = m(x) \cdot n(x)$, 其中 $m(x), n(x) \in \mathbb{Z}[x]$, 且 $m(x), n(x)$ 不是 $\mathbb{Z}[x]$ 中的 unit. 那麼大家一定認為由於 $m(x), n(x)$ 也在 $\mathbb{Q}[x]$ 中所以 $f(x)$ 在 $\mathbb{Q}[x]$ 中可以分解. 其實不然, 因為 $m(x), n(x)$ 在 $\mathbb{Z}[x]$ 中不是 unit, 但可能在 $\mathbb{Q}[x]$ 中就是 unit 了. 例如 $2x + 2$ 在 $\mathbb{Q}[x]$ 是 irreducible 但在 $\mathbb{Z}[x]$ 中 $2x + 2 = 2 \cdot (x + 1)$, 而且 2 和 $x + 1$ 在 $\mathbb{Z}[x]$ 中都不是 unit (但 2 在 $\mathbb{Q}[x]$ 是 unit), 所以 $2x + 2$ 在 $\mathbb{Z}[x]$ 並不是 irreducible. 從這裡看出 $\mathbb{Z}[x]$ 中的 irreducible element 和 $\mathbb{Q}[x]$ 的 irreducible element 不同.

回顧一下我們定義所謂的 irreducible element 是一個元素它的 divisor 只有 unit 和 本身乘上 unit 這兩種形式. 由於 $\mathbb{Z}[x]$ 中的 unit 只有 1 和 -1 所以我們有以下的定義.

Definition 7.3.9. 令 $p(x) \in \mathbb{Z}[x]$

(1) 若 $p(x)$ 在 $\mathbb{Z}[x]$ 中的 divisor 只有 ± 1 和 $\pm p(x)$, 則稱 $p(x)$ 是 $\mathbb{Z}[x]$ 的 *irreducible element.*

(2) 若對所有滿足 $p(x) \mid f(x) \cdot g(x)$ 的 $f(x), g(x) \in \mathbb{Z}[x]$ 都有 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$ 則稱 $p(x)$ 是 $\mathbb{Z}[x]$ 的 *prime element.*

由這個定義我們馬上得到以下的 Lemma.

Lemma 7.3.10. 假設 $p(x) \in \mathbb{Z}[x]$ 且 $\deg(p(x)) > 0$.

(1) 若 $p(x)$ 是一個 *irreducible element,* 則 $p(x)$ 是一個 *primitive polynomial.*

(2) 若 $p(x)$ 是一個 *prime element,* 則 $p(x)$ 是一個 *primitive polynomial.*

Proof. (1) 假設 $p(x)$ 是 irreducible. 因 $p(x) = c(p) \cdot p^*(x)$, 其中 $c(p) \in \mathbb{N} \subseteq \mathbb{Z}[x]$ 且 $p^*(x) \in \mathbb{Z}[x]$, 所以 $c(p)$ 是 $p(x)$ 的一個 divisor. 由 $p(x)$ 是 irreducible 及 $\deg(p^*(x)) = \deg(p(x)) > 0$ 知 $c(p) = 1$, 故得 $p(x)$ 是 primitive.

(2) 假設 $p(x)$ 是 prime. 因 $p(x) = c(p) \cdot p^*(x)$, 故知 $p(x) \mid c(p) \cdot p^*(x)$. 由 $p(x)$ 是 prime 的假設, 知 $p(x) \mid c(p)$ 或 $p(x) \mid p^*(x)$. 由於 $\deg(p(x)) > 0$ 知不可能 $p(x) \mid c(p)$. 故得 $p(x) \mid p^*(x)$. 也就是說存在 $\lambda(x) \in \mathbb{Z}[x]$ 使得 $p^*(x) = \lambda(x) \cdot p(x)$. 故得 $p^*(x) = \big(\lambda(x) \cdot c(p)\big) \cdot p^*(x)$. 利用 $\mathbb{Z}[x]$ 是 integral domain 及 $p^*(x) \neq 0$ 知 $\lambda(x) \cdot c(p) = 1$. 也就是說 $\lambda(x)$ 和 $c(p)$ 是 $\mathbb{Z}[x]$ 的 unit. 但由定義 $c(p)$ 是正整數, 故得 $\lambda(x) = c(p) = 1$. 也就是說 $p(x)$ 是 primitive. □

如前面幾節中的結果, 我們將會證得在 $\mathbb{Z}[x]$ 中的 irreducible element 和 prime element 是一樣的. 由於 $\mathbb{Z}[x]$ 沒有所有的 ideal 都是 principle ideal 的性質, 我們不能用前面的方法如法泡製. 我們將利用 $\mathbb{Q}[x]$ 中的 irreducible element 的性質來幫忙處理, 所以我們需要先了解在 $\mathbb{Z}[x]$ 中的 irreducible element 和 $\mathbb{Q}[x]$ 中的 irreducible element 之間的關係.

Lemma 7.3.11. *若 $p(x) \in \mathbb{Z}[x]$, $\deg(p(x)) > 0$ 且 $p(x)$ 是一個 primitive polynomial, 則 $p(x)$ 是 $\mathbb{Q}[x]$ 中的 irreducible element 若且唯若 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 irreducible element.*

Proof. 首先假設 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 irreducible element. 如果 $p(x)$ 在 $\mathbb{Q}[x]$ 中不是 irreducible element, 表示存在 $g(x), h(x) \in \mathbb{Q}[x]$ 滿足 $0 < \deg(g(x)) < \deg(p(x))$, $0 < \deg(h(x)) < \deg(p(x))$ 且 $p(x) = g(x) \cdot h(x)$. 利用 Lemma 7.3.8 知存在 $m(x), n(x) \in \mathbb{Z}[x]$ 且 $\deg(m(x)) = \deg(g(x))$, $\deg(n(x)) = \deg(h(x))$ 滿足 $p(x) = m(x) \cdot n(x)$. 也就是說 $m(x)$ 是 $p(x)$ 的 divisor. 但 $0 < \deg(m(x)) < \deg(p(x))$, 故知 $m(x) \neq \pm 1$ 且 $m(x) \neq \pm p(x)$. 此和 $p(x)$ 是 $\mathbb{Z}[x]$ 的一個 irreducible element 假設相矛盾. 故知 $p(x)$ 也是 $\mathbb{Q}[x]$ 中的 irreducible element.

反之, 若 $p(x)$ 是 $\mathbb{Q}[x]$ 中的 irreducible element. 若 $p(x) = m(x) \cdot n(x)$, 其中 $m(x), n(x) \in \mathbb{Z}[x]$. 由 $p(x)$ 在 $\mathbb{Q}[x]$ 是 irreducible 的假設知 $m(x)$ 和 $n(x)$ 中有一個是 $\mathbb{Q}[x]$ 的 unit, 即常數: 就假設 $m(x) = d$ 是常數吧! 因 $m(x) \in \mathbb{Z}[x]$ 故知 $d \in \mathbb{Z}$. 由 $p(x) = d \cdot n(x)$ 知 d 是 $p(x)$ 的所有係數的公因數. 但已知 $p(x)$ 是 primitive, 故得 $d = \pm 1$. 也就是說 $p(x)$ 的 divisor 只能是 ± 1 和 $\pm p(x)$ 這種形式, 故得 $p(x)$ 在 $\mathbb{Z}[x]$ 中是 irreducible. □

由於 $\mathbb{Q}$ 是一個 field, 所以上一節中 $F[x]$ 的性質都可套用在 $\mathbb{Q}[x]$ 上. 我們要利用 $\mathbb{Q}[x]$ 中的 irreducible 和 prime 是一樣的, 得到在 $\mathbb{Z}[x]$ 中的 irreducible 和 prime 也是一樣的.

Proposition 7.3.12. *假設 $p(x) \in \mathbb{Z}[x]$. 若 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 irreducible element, 則 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 prime element. 反之, 若 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 prime element, 則 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 irreducible element.*

Proof. 首先注意, 當 $\deg(p(x)) = 0$ 時表示 $p(x) \in \mathbb{Z}$ 是一個常數. 我們已知在 $\mathbb{Z}$ 中的 irreducible 和 prime 是一樣的 (Proposition 7.1.7), 所以我們只要關心 $\deg(p(x)) > 0$ 的情況.

首先假設 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 irreducible element. 由 Lemma 7.3.10 知其為 primitive, 故由 Lemma 7.3.11 知 $p(x)$ 也是 $\mathbb{Q}[x]$ 中的 irreducible element. 再由 Proposition 7.2.11 知 $p(x)$ 是 $\mathbb{Q}[x]$ 中的 prime element. 現若 $f(x), g(x) \in \mathbb{Z}[x]$ 且 $p(x) \mid f(x) \cdot g(x)$ in $\mathbb{Z}[x]$, 由 Lemma 7.3.7 知 $p(x) \mid f(x) \cdot g(x)$ in $\mathbb{Q}[x]$. 故由 $p(x)$ 在 $\mathbb{Q}[x]$ 是 prime 得 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$ in $\mathbb{Q}[x]$. 再由 Lemma 7.3.7 知 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$ in $\mathbb{Z}[x]$. 也就是說 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 prime element.

反之, 若 $p(x)$ 是 $\mathbb{Z}[x]$ 中的 prime element. 若 $p(x) = m(x) \cdot n(x)$ 其中 $m(x), n(x) \in \mathbb{Z}[x]$. 則由於 $p(x) \mid m(x) \cdot n(x)$, 可得 $p(x) \mid n(x)$ 或 $p(x) \mid m(x)$. 若 $p(x) \mid n(x)$, 即存在 $\lambda(x) \in \mathbb{Z}[x]$ 使得 $n(x) = \lambda(x) \cdot p(x)$. 故得

$$n(x) = \lambda(x) \cdot \big(n(x) \cdot m(x)\big) = \big(\lambda(x) \cdot m(x)\big) \cdot n(x).$$

由 $n(x) \neq 0$ 以及 $\mathbb{Z}[x]$ 是 integral domain, 得 $\lambda(x) \cdot m(x) = 1$. 也就是說 $m(x)$ 是 $\mathbb{Z}[x]$ 的 unit, 即 $m(x) = \pm 1$. 同理, 若 $p(x) \mid m(x)$ 可得 $n(x) = \pm 1$. 得證 $p(x)$ 的 divisor 都是 ± 1 和 $\pm p(x)$ 這種形式, 故知 $p(x)$ 是一個 irreducible element. □

現在要證明 $\mathbb{Z}[x]$ 上的唯一分解性質露出了一線曙光, 前面幾節中我們證明唯一分解性質並沒有用到每一個 ideal 都是 principle ideal 的性質, 而是用到如 Proposition 7.3.12 中每個 irreducible element 是 prime 的性質. 如同在整數的情況, 由於 $f(x)$ 和 $-f(x)$ 的分解僅差一個正負號, 我們可以只考慮最高次項係數是正整數的 polynomial.

Theorem 7.3.13. 若 $f(x) \in \mathbb{Z}[x]$ 是一個不為 $0, 1, -1$ 且最高次項係數是正整數的 *polynomial,* 則存在 $p_1(x), \ldots, p_r(x) \in \mathbb{Z}[x]$, 其中這些 $p_i(x)$ 是 $\mathbb{Z}[x]$ 中兩兩相異且最高次項係數是正整數的 *irreducible elements,* 滿足

$$f(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r}, \quad n_i \in \mathbb{N}, \forall i \in \{1, \ldots, r\}.$$

如果 $f(x)$ 可以分解成另外的形式 $f(x) = q_1(x)^{m_1} \cdots q_s(x)^{m_s}$, 其中這些 $q_i(x)$ 也是 $\mathbb{Z}[x]$ 中兩兩相異且最高次係數是正整數的 *irreducible elements,* 則 $r = s$ 且經過變換順序可得 $p_i(x) = q_i(x)$, $n_i = m_i$, $\forall\, i \in \{1, \ldots, r\}$.

Proof. 首先證明存在性, 也就是 $f(x)$ 可寫成有限多個 $\mathbb{Z}[x]$ 中的 irreducible elements 的乘積. 我們依然 (對 degree) 用數學歸納法來證明. 假設 $\deg(f(x)) = 0$, 因 $f(x) \in \mathbb{N}$ 且不是 unit, 故由 $\mathbb{Z}$ 的分解性質 (Theorem 7.1.8) 的存在性知 $f(x)$ 可寫成有限多個 irreducible elements 的乘積. 現假設存在性對 degree 小於 n 的 polynomial 皆成立. 當 $\deg(f(x)) = n$ 時, 若 $f(x)$ 本身是 irreducible, 存在性自然成立. 故僅剩 $f(x)$ 不是 irreducible 的情況要考慮. 此時要注意, 在 $\mathbb{Z}[x]$ 中一個 polynomial 是 irreducible 並不表示他一定可以寫成兩個 degree 比較小的 polynomials 的乘積 (例如前面提過的例子 $2x + 2$). 此時我們先將 $f(x)$ 寫成 $f(x) = c(f) \cdot f^*(x)$, 其中 $f^*(x) \in \mathbb{Z}[x]$

是 primitive polynomial. 由於 $c(f) \in \mathbb{N}$, 再一次利用 Theorem 7.1.8 知 $c(f) = 1$ 或是可以寫成有限多個 irreducible 常數 polynomials 的乘積. 所以我們只剩下考慮 $f^*(x)$ 是否可寫成有限多個 irreducible elements 的乘積. 當 $f^*(x)$ 是 irreducible 時, 存在性自然又成立了. 而當 $f^*(x)$ 不是 irreducible 時, Lemma 7.3.11 告訴我們 $f^*(x)$ 在 $\mathbb{Q}[x]$ 不是 irreducible, 也就是 $f^*(x) = g(x) \cdot h(x)$ 其中 $g(x), h(x) \in \mathbb{Q}[x]$ 且 $0 < \deg(g(x)) < \deg(f(x))$ 以及 $0 < \deg(h(x)) < \deg(f(x))$. 由 Lemma 7.3.8 知存在 $m(x), n(x) \in \mathbb{Z}[x]$ 且 $\deg(m(x)) = \deg(g(x))$ 以及 $\deg(n(x)) = \deg(h(x))$ 使得 $f^*(x) = m(x) \cdot n(x)$. 由於 $\deg(m(x)) < \deg(f(x)) = n$ 以及 $\deg(n(x)) < n$, 故利用歸納法假設知 $m(x)$ 和 $n(x)$ 都可寫成有限多個 irreducible elements 的乘積. 因此得證 $f^*(x)$ 可以寫成有限多個 irreducible elements 的乘積, 故知 $f(x) = c(f)f^*(x)$ 也可寫成有限多個 irreducible elements 的乘積.

至於唯一性我們依然用數學歸納法來處理. 若 $\deg(f(x)) = 0$, 因 $f(x) \in \mathbb{N}$, 故可以利用 Theorem 7.1.8 的唯一性得證唯一性. 現假設唯一性對 degree 小於 n 的 polynomial 皆成立. 當 $\deg(f(x)) = n$ 時, 若

$$f(x) = p_1(x)^{n_1} \cdots p_r(x)^{n_r} = q_1(x)^{m_1} \cdots q_s(x)^{m_s},$$

其中 $p_i(x)$ 兩兩相異, $q_j(x)$ 也是兩兩相異, 而且 $p_i(x), q_j(x)$ 都是 $\mathbb{Z}[x]$ 中最高次項係數是正整數的 irreducible elements. 由於 $\deg(f(x)) > 0$, 故知 $p_i(x)$ 中必存在一 polynomial 其 degree 大於 0, 經重排後我們令之為 $p_1(x)$. Proposition 7.3.12 告訴我們 $p_1(x)$ 是 $\mathbb{Z}[x]$ 的 prime element, 故由 $p_1(x) \mid f(x)$ 得知, $q_j(x)$ 中有一 polynomial 會被 $p_1(x)$ 整除, 經重排後我們令之為 $q_1(x)$. 也就是說 $p_1(x) \mid q_1(x)$. 然而 $q_1(x)$ 是 irreducible, 其 divisor 只有 ± 1 和 $\pm q_1(x)$. 又因已知 $\deg(p_1(x)) > 0$ 且 $p_1(x)$ 和 $q_1(x)$ 的最高次項係數都是正整數, 故得 $p_1(x) = q_1(x)$. 因此我們可將 $f(x)$ 的分解改寫成

$$f(x) = p_1(x)^{n_1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} = p_1(x)^{m_1} \cdot q_2(x)^{m_2} \cdots q_s(x)^{m_s}.$$

將上式移項再提出 $p_1(x)$, 我們可得

$$p_1(x) \cdot \left(p_1(x)^{n_1-1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} - p_1(x)^{m_1-1} \cdot q_2(x)^{m_2} \cdots q_s(x)^{m_s}\right) = 0.$$

由於 $p_1(x) \neq 0$ 且 $\mathbb{Z}[x]$ 是 integral domain, 我們得

$$p_1(x)^{n_1-1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} - p_1(x)^{m_1-1} \cdot q_2(x)^{m_2} \cdots q_s(x)^{m_s} = 0.$$

現令 $g(x) = p_1(x)^{n_1-1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r}$. 由於當初選取 $p_1(x)$ 滿足 $\deg(p_1(x)) > 0$, 故得

$$\deg(g(x)) = \deg(f(x)) - \deg(p_1(x)) < \deg(f(x)) = n$$

且

$$g(x) = p_1(x)^{n_1-1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} = p_1(x)^{m_1-1} \cdot q_2(x)^{m_2} \cdots q_s(x)^{m_s}$$

是 $g(x)$ 的兩個分解, 故利用歸納法假設我們有 $r = s$ 且 $p_1(x) = q_1(x), \ldots, p_r(x) = q_r(x)$ 以及 $n_1 = m_1$, $n_2 = m_2, \ldots, n_r = m_r$, 故得證唯一性. □

由 Theorem 7.3.13 知 $\mathbb{Z}[x]$ 中的 irreducible elements 就如同 $\mathbb{Z}$ 中的質數一樣重要. 另一方面利用 Lemma 7.3.8 也告訴我們在 $\mathbb{Z}[x]$ 中的 irreducible element 在 $\mathbb{Q}[x]$ 中也是 irreducible. 因此探討 $\mathbb{Z}[x]$ 中有哪些 irreducible elements 是一個重要的課題. 其實給定 $f(x) \in \mathbb{Z}[x]$ 要判斷其是否為 irreducible 並不容易. 以下我們介紹一種方法可以確認某一類的 polynomial 是 irreducible.

Proposition 7.3.14 (Eisenstein Criterion)**.** 令

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x],$$

其中 $n > 0$. 假設存在一質數 $p \in \mathbb{N}$ 滿足

$$p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1} \quad \text{但} \quad p^2 \nmid a_0,$$

則 $f(x)$ 是 $\mathbb{Z}[x]$ 中的 *irreducible element.*

Proof. 由於 $c(f) = 1$ 所以 $f(x)$ 是 primitive polynomial. 因此要說明 $f(x)$ 是 irreducible in $\mathbb{Z}[x]$ 只要說明 $f(x)$ 不可能寫成兩個 degree 小於 n 的 polynomials 的乘積. 我們利用反證法來證明.

假設 $f(x) = g(x) \cdot h(x)$ 其中

$$g(x) = c_rx^r + \cdots + c_1x + c_0 \in \mathbb{Z}[x], \quad 0 < r < n$$

且

$$h(x) = d_sx^s + \cdots + d_1x + d_0 \in \mathbb{Z}[x], \quad 0 < s < n.$$

考慮 $g(x) \cdot h(x)$ 的常數項 $c_0 \cdot d_0 = a_0$. 由假設 $p \mid a_0 = c_0 \cdot d_0$, 故知 $p \mid c_0$ 或 $p \mid d_0$. 然而又知 $p^2 \nmid c_0 \cdot d_0$, 故知 c_0 和 d_0 間只能有一個被 p 整除. 我們就假設是 c_0 吧! 也就是說 $p \mid c_0$ 但 $p \nmid d_0$. 現在觀察 $g(x) \cdot h(x)$ 的一次項係數 $c_0 \cdot d_1 + c_1 \cdot d_0 = a_1$. 由假設 $p \mid a_1$ 以及剛才得知的 $p \mid c_0$ 可得 $p \mid c_1 \cdot d_0$. 但又知 $p \nmid d_0$ 故得 $p \mid c_1$. 這樣一直下去我們想用數學歸納法證得 $p \mid c_r$. 也就是假設已知 $p \mid c_0, p \mid c_1, \ldots, p \mid c_{r-1}$, 我們欲證得 $p \mid c_r$. 現考慮 $g(x) \cdot h(x)$ 的 x^r 項係數

$$c_0 \cdot d_r + c_1 \cdot d_{r-1} + \cdots + c_{r-1} \cdot d_1 + c_r \cdot d_0 = a_r.$$

(這個式子裡若 $s < r$, 那當然是令 $d_{s+1} = \cdots = d_r = 0$) 由於 $0 < r < n$ 故知 $p \mid a_r$, 再加上歸納假設 $p \mid c_0, \ldots, p \mid c_{r-1}$, 我們可得 $p \mid c_r \cdot d_0$. 別忘了 $p \nmid d_0$, 故得證 $p \mid c_r$. 現在我們考慮 $g(x) \cdot h(x)$ 的最高次項係數 (即 $f(x)$ 的 x^n 項係數)

$$c_r \cdot d_s = 1.$$

大家馬上看出由 $p \mid c_r$ 不可能得到 $c_r \cdot d_s = 1$. 因此得到矛盾, 也就是說 $f(x)$ 是 $\mathbb{Z}[x]$ 的 irreducible element. □

最後我們重申一下, 由 Lemma 7.3.8 (或 Lemma 7.3.11) 我們知道符合 Proposition 7.3.14 的 polynomials 在 $\mathbb{Q}[x]$ 也是 irreducible.

7.4. Quotient Field of an Integral Domain

我們都知道 $\mathbb{Z}$ 是 integral domain 而 $\mathbb{Q}$ 是 field. 事實上 $\mathbb{Q}$ 是包含 $\mathbb{Z}$ 最小的 field. 我們將推廣從 $\mathbb{Z}$ 建構出 $\mathbb{Q}$ 的方法到任意的 integral domain D.

給定任意的 integral domain D, 令 $S = \{(a,b) \mid a,b \in D,\ b \neq 0\}$. 首先我們將在 S 中定一個 equivalence relation. 對於 S 中的兩元素 $(a,b),(c,d) \in S$, 我們令

$$(a,b) \sim (c,d) \quad \text{若且唯若} \quad a \cdot d = c \cdot b.$$

會定出這種 relation 並不奇怪, 大家可以想像在 $\mathbb{Q}$ 中的任意元素若可寫成 a/b 及 c/d, 其中 $a,b,c,d \in \mathbb{Z}$ 且 $b \neq 0, d \neq 0$, 那麼自然有 $a \cdot d = c \cdot b$ 這一個關係式.

我們要驗證 $\sim$ 這一個 relation 是一個 equivalence relation:

(equiv1): 對所有的 $(a,b) \in S$, 由於 D 是一個 integral domain 所以 commutative, 故知 $a \cdot b = b \cdot a$. 所以得證 $(a,b) \sim (a,b)$.

(equiv2): 若已知 $(a,b) \sim (c,d)$, 我們想要證得 $(c,d) \sim (a,b)$. 由 $(a,b) \sim (c,d)$ 我們有 $a \cdot d = c \cdot b$ 這一個關係式. 而要證得 $(c,d) \sim (a,b)$ 我們必須要有 $c \cdot b = a \cdot d$, 但這和假設的關係式相同, 故得 $(c,d) \sim (a,b)$.

(equiv3): 若已知 $(a,b) \sim (c,d)$ 且 $(c,d) \sim (e,f)$, 我們希望證得 $(a,b) \sim (e,f)$. 由假設條件我們有

$$a \cdot d = c \cdot b \tag{7.1}$$

$$c \cdot f = e \cdot d \tag{7.2}$$

要如何從以上 (7.1) 和 (7.2) 兩個關係式得到 $a \cdot f = e \cdot b$ 這個關係式呢? 首先將式子 (7.1) 的等式兩邊乘上 f, 得 $(a \cdot d) \cdot f = (c \cdot b) \cdot f = (c \cdot f) \cdot b$. 再利用式子 (7.2) 得 $(a \cdot d) \cdot f = (e \cdot d) \cdot b$, 也就是 $d \cdot (a \cdot f - e \cdot b) = 0$. 因 $d \neq 0$, 且 D 沒有 zero divisor (別忘了 D 是 integral domain), 故得 $a \cdot f = e \cdot b$.

好了, 既然 $\sim$ 是 S 中的一個 equivalence relation, 我們就可以將 S 中的元素利用 $\sim$ 來分類. 若 $(a,b) \in S$, 我們令 $[a,b]$ 表示在 S 中所有和 (a,b) 同類的元素所成的集合. 令 $\widetilde{S}$ 表示將 S 分類以後所成的新的集合. 也就是說 $\widetilde{S}$ 中的元素都是 $[a,b]$ 這種形式, 其中 $a,b \in D$ 且 $b \neq 0$, 而且若 $(a,b) \sim (c,d)$, 則在 $\widetilde{S}$ 中 $[a,b] = [c,d]$.

現在我們要在 $\widetilde{S}$ 中定義加法和乘法. 若 $[a,b] \in \widetilde{S}$ 且 $[c,d] \in \widetilde{S}$, 我們定:

$$[a,b] + [c,d] = [a \cdot d + c \cdot b, b \cdot d] \quad \text{以及} \quad [a,b] \cdot [c,d] = [a \cdot c, b \cdot d].$$

為什麼這樣定加法和乘法相信大家很快的看出這是從有理數上的加法和乘法衍生出來. 也相信大家知道下一步就是要檢驗這樣定的加法和乘法是 well-defined. 首先要檢查的是這樣定的 $[a,b]+[c,d]$ 和 $[a,b] \cdot [c,d]$ 會落在 $\widetilde{S}$ 中, 也就是說 $b \cdot d \neq 0$. 由 $b \neq 0$ 且 $d \neq 0$ 以及 D 是 integral domain, 當然可得 $b \cdot d \neq 0$. 接下來要檢查的是若 $[a,b] = [a',b']$ 且 $[c,d] = [c',d']$, 則 $[a,b] + [c,d] = [a',b'] + [c',d']$ 以及 $[a,b] \cdot [c,d] = [a',b'] \cdot [c',d']$. 從定義知要檢驗 $[a,b] + [c,d] = [a',b'] + [c',d']$ 等於要

驗證

$$(a\cdot d+c\cdot b)\cdot(b'\cdot d')=(a'\cdot d'+c'\cdot b')\cdot(b\cdot d).$$

然而利用 $a\cdot b'=a'\cdot b$ 以及 $c\cdot d'=c'\cdot d$ 得

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

同理, 要檢查 $[a,b]\cdot[c,d]=[a',b']\cdot[c',d']$ 等於要驗證 $(a\cdot c)\cdot(b'\cdot d')=(a'\cdot c')\cdot(b\cdot d)$. 然而利用 $a\cdot b'=a'\cdot b$ 以及 $c\cdot d'=c'\cdot d$ 得

$$(a\cdot c)\cdot(b'\cdot d')=(a\cdot b')\cdot(c\cdot d')=(a'\cdot b)\cdot(c'\cdot d)=(a'\cdot c')\cdot(b\cdot d).$$

既然在 $\widetilde{S}$ 中可定義加法和乘法, 我們自然會問 $\widetilde{S}$ 是否是一個 ring, 也就是要檢查 (R1)–(R8). 這一連串的檢查雖然不難, 但是很繁複我們就略過. 事實上 $\widetilde{S}$ 是一個 commutative ring with 1. 其中 $\widetilde{S}$ 的 0 是 $[0,1]$ 而 1 是 $[1,1]$. 這可以用 $\forall[a,b]\in\widetilde{S}$ 則 $[a,b]+[0,1]=[a,b]$ 以及 $[a,b]\cdot[1,1]=[a,b]$ 證得. 至於 $\widetilde{S}$ 是 commutative 可由 D 是 integral domain 的假設知 D 是 commutative 故得 $[a,b]\cdot[c,d]=[a\cdot c,b\cdot d]=[c,d]\cdot[a,b]$.

我們最終的目的要證明 $\widetilde{S}$ 是一個 field, 也就是說對任意的 $[a,b]\in\widetilde{S}$ 且 $[a,b]\neq[0,1]$ 可以找到 $[c,d]\in\widetilde{S}$ 使得 $[a,b]\cdot[c,d]=[1,1]$. 因為 $[a,b]\neq[0,1]$ 故知 $a\neq0$, 所以 $[b,a]\in\widetilde{S}$. 很容易得知 $[a,b]\cdot[b,a]=[a\cdot b,a\cdot b]=[1,1]$. 總之, 任意 $\widetilde{S}$ 中非 0 的元素都是 unit, 所以 $\widetilde{S}$ 是一個 field, 我們稱之為 D 的 *quotient field* 或 *fraction field*.

D 的 quotient field $\widetilde{S}$ 有一個重要的性質, 就是它是包含 D 最小的 field. 這裡有件事情我們得說明一下. 我們提過在代數中通常將兩個 isomorphic 的東西看成是一樣的. 事實上 $\widetilde{S}$ 並沒有真正的包含 D, 嚴格來說應該是 $\widetilde{S}$ 中有一個 subring 和 D 是 isomorphic. 所以這裡所謂 $\widetilde{S}$ 是包含 D 最小的 field 表示若 F 是一個 field 且有一個 subring 和 D isomorphic, 則 F 中有一個 subring 和 $\widetilde{S}$ isomorphic.

首先我們就來看 D 包含於它的 quotient field.

Proposition 7.4.1. 假設 D 是一個 *integral domain,* 且令 $\widetilde{S}$ 是 D 的 *quotient field,* 則可找到一個從 D 到 $\widetilde{S}$ 的 *injective* (一對一) *ring homomorphism* .

Proof. 考慮 $\phi:D\to\widetilde{S}$ 定義成對任意的 $a\in D$, $\phi(a)=[a,1]$. 由於若 $a,b\in D$ 則

$$\phi(a+b)=[a+b,1]=[a,1]+[b,1]=\phi(a)+\phi(b)$$

且

$$\phi(a\cdot b)=[a\cdot b,1]=[a,1]\cdot[b,1]=\phi(a)\cdot\phi(b).$$

故知 ϕ 是一個從 D 到 $\widetilde{S}$ 的 ring homomorphism. 至於要證 ϕ 是一對一, 我們只要檢查 $\ker(\phi)=\{0\}$. 由於 $\phi(0)=[0,1]$ 故知 $0\in\ker(\phi)$. 現若 $a\in\ker(\phi)$, 表示

$\phi(a) = [a, 1] = [0, 1]$. 利用定義, $[a, 1] = [0, 1]$ 表示 $a \cdot 1 = 0 \cdot 1$, 故得 $a = 0$. 因此得證 $\ker(\phi) = \{0\}$. □

回顧 Theorem 6.4.2 告訴我們 $D/\ker(\phi) \simeq \mathrm{im}(\phi)$ 而 Proposition 7.4.1 告訴我們 $\ker(\phi) = \{0\}$ 因此得 $D \simeq \mathrm{im}(\phi)$. 但是 $\mathrm{im}(\phi)$ 是 $\widetilde{S}$ 的 subring (Lemma 6.3.3), 故知 D 和 D 的 quotient field $\widetilde{S}$ 中的一個 subring 是 isomorphic. 接下來我們要證明 D 的 quotient field 是有這個特性之最小的 field.

Proposition 7.4.2. 假設 D 是一個 *integral domain,* 且令 $\widetilde{S}$ 是 D 的 *quotient field.* 若 F 是一個 *field* 其中包含一個 *subring* 和 D *isomorphic,* 則 F 中也有一個 *subring* 和 $\widetilde{S}$ *isomorphic.*

Proof. 由假設知存在一個一對一的 ring homomorphism $\phi : D \to F$. 我們想利用這個 ϕ 製造出另一個一對一的 ring homomorphism $\psi : \widetilde{S} \to F$.

對任意的 $[a, b] \in \widetilde{S}$, 我們定 $\psi([a, b]) = \phi(a) \cdot \phi(b)^{-1}$. 當然這裡我們要檢查 ψ 是否 well-defined.

首先我們檢查 $\psi([a, b])$ 是否是 F 中的元素. 由於 $[a, b] \in \widetilde{S}$, 知 $b \neq 0$, 因此由 ϕ 是一對一知 $\phi(b)$ 是 F 中的一個不等於 0 的元素. 所以由 F 是 field 的假設知 $\phi(b)^{-1} \in F$. 故得證 $\psi([a, b]) = \phi(a) \cdot \phi(b)^{-1} \in F$. 接著要檢查是否若 $[a, b] = [c, d]$ 則 $\psi([a, b]) = \psi([c, d])$. (再次提醒: 當我們建構一個函數時如果定義域裡的元素的表示法不唯一, 我們一定要檢查是否同一元素其不同的表示法會被映射到相同的值, 以免發生一對多的情況.) 也就是說若 $a \cdot d = c \cdot b$, 要檢查是否

$$\phi(a) \cdot \phi(b)^{-1} = \phi(c) \cdot \phi(d)^{-1}.$$

然而利用 ϕ 是 ring homomorphism 知 $\phi(a \cdot d) = \phi(a) \cdot \phi(d)$ 且 $\phi(c \cdot b) = \phi(c) \cdot \phi(b)$. 故由 $a \cdot d = c \cdot b$ 可得 $\phi(a \cdot d) = \phi(c \cdot b)$ 也就是說 $\phi(a) \cdot \phi(d) = \phi(c) \cdot \phi(b)$. 上式兩邊各乘上 $\phi(d)^{-1} \cdot \phi(b)^{-1}$ (別忘了 $\phi(b)$ 和 $\phi(d)$ 皆不等於 0) 可得 $\phi(a) \cdot \phi(b)^{-1} = \phi(c) \cdot \phi(d)^{-1}$. 因此 ψ 是一個 well-defined 的函數.

接下來我們證 ψ 是一個 ring homomorphism. 對任意的 $[a, b], [c, d] \in \widetilde{S}$, 依 ψ 的定義我們有

$$\psi([a, b] + [c, d]) = \psi([a \cdot d + c \cdot b, b \cdot d]) = \phi(a \cdot d + c \cdot b) \cdot \phi(b \cdot d)^{-1}$$

且

$$\psi([a, b]) + \psi([c, d]) = \phi(a) \cdot \phi(b)^{-1} + \phi(c) \cdot \phi(d)^{-1}.$$

然而利用 ϕ 是 ring homomorphism, 乘上 $\phi(b \cdot d) = \phi(b) \cdot \phi(d)$ 我們很容易檢驗

$$\phi(a \cdot d + c \cdot b) \cdot \phi(b \cdot d)^{-1} = \phi(a) \cdot \phi(b)^{-1} + \phi(c) \cdot \phi(d)^{-1}.$$

故知

$$\psi([a, b] + [c, d]) = \psi([a, b]) + \psi([c, d]).$$

同理可證

$$\psi([a,b]\cdot[c,d]) = \psi([a\cdot c, b\cdot d]) = \phi(a\cdot c)\cdot\phi(b\cdot d)^{-1} = \psi([a,b])\cdot\psi([c,d]),$$

故知 ψ 是一個 ring homomorphism.

最後我們驗證 ψ 是一對一的, 也就是驗證 $\ker(\psi) = \{[0,1]\}$. 假設 $[a,b] \in \ker(\psi)$, 即 $\psi([a,b]) = \phi(a)\cdot\phi(b)^{-1} = 0$. 乘上 $\phi(b)$ 馬上可得 $\phi(a) = 0$. 但由於 ϕ 是一對一, 故由 $a \in \ker(\phi) = \{0\}$, 得 $a = 0$. 換句話說 $[a,b] = [0,1]$. 所以得證 ψ 是一對一. □

從今以後, 若 $\widetilde{S}$ 為 D 的 quotient field, 我們將直接看成 D 包含於 $\widetilde{S}$, 也就是將 $[a,1]$ 寫成 a. 另外我們將 $[a,b] \in \widetilde{S}$ 直接寫成 a/b.

Chapter 8

Integral Domain 上的分解性質

我們將推廣上一章的所介紹的特殊的 ring 到更一般的狀況. 在這一章中我們的 ring 永遠是 **integral domain**. 大家會發現這一章的內容並不困難, 很多性質只是將上一章的結果做簡單的推廣.

8.1. Divisor

在 integral domain 裡元素的分解大家應該都了解最基本的元素就是 irreducible elements 和 prime elements. 我們將有系統的探討它們的基本性質.

首先我們還是對一個元素的因數給一個正式的定義.

Definition 8.1.1. 令 R 是一個 integral domain 且 $a, d \in R$ 是 R 中兩個不為 0 的元素. 如果存在 $r \in R$ 滿足 $a = d \cdot r$, 則稱 d 為 a 在 R 中的一個 *divisor* 且記為 $d \mid a$.

回顧一下若 R 是 integral domain 且 $d \in R$, 則 $\big(d\big) = \{d \cdot r \mid r \in R\}$ 所以由上一個定義我們很容易知 $d \mid a$ 若且唯若 $a \in \big(d\big)$. 然而若 $a \in \big(d\big)$, 由 $\big(d\big)$ 是一個 ideal 知對任意的 $r \in R$ 皆有 $a \cdot r \in \big(d\big)$. 故得 $\big(a\big) \subseteq \big(d\big)$. 反之若 $\big(a\big) \subseteq \big(d\big)$, 由 $a \in \big(a\big)$ 得知 $a \in \big(d\big)$. 換句話說 $a \in \big(d\big)$ 若且唯若 $\big(a\big) \subseteq \big(d\big)$, 因此我們有以下的結論:

Lemma 8.1.2. 令 R 是一個 *integral domain* 且 $a, d \in R \setminus \{0\}$. 則 $d \mid a$ 若且唯若 $\big(a\big) \subseteq \big(d\big)$.

Lemma 8.1.2 雖然簡單但相當實用, 它告訴我們元素間的整除關係可以轉換成 ideal 間的包含關係. 以後我們要談論兩元素間的整除關係時我們有時不用 divisor 的定義處理, 我們會用這種 ideal 的關係來探討, 大家會發現這個方法是簡潔又方便的.

若 $a \in R$ 且 $a \neq 0$, 我們很快的就知道任意 R 中的一個 unit 都會是 a 的一個 divisor. 這是由於若 u 是 R 中的 unit, 則 $\big(u\big) = R$ (Lemma 6.2.4). 故由 $\big(a\big) \subseteq R = \big(u\big)$ 知 $u \mid a$. 另一方面當 u 是 unit 時, $a \cdot u$ 也是 a 的 divisor. 這也可由 $\big(a \cdot u\big) = \big(a\big)$ (Lemma 6.5.4) 及 Lemma 8.1.2 馬上得到. u 和 $a \cdot u$ 這種 a 的 divisor 對 a 的分解沒有甚麼幫助, 我們稱之為 a 的 *trivial divisor*. 以下 Lemma 是探討 $a \cdot u$ 這個 a 的 trivial divisor 和 a 的簡單關係.

Lemma 8.1.3. 令 R 是一個 *integral domain* 且 a 和 b 是 R 中兩個不為 0 的元素. 下列三項 a 和 b 的關係是等價的.

(1) 存在 $u \in R$ 是 R 的一個 *unit* 滿足 $a = b \cdot u$.

(2) $\big(a\big) = \big(b\big)$.

(3) $a \mid b$ 且 $b \mid a$.

Proof. (1) $\Rightarrow$ (2): 可由 Lemma 6.5.4 知 $\big(a\big) = \big(b\big)$.

(2) $\Rightarrow$ (3): 可由 Lemma 8.1.2 直接推得.

(3) $\Rightarrow$ (1): 由 $a \mid b$ 知存在 $r \in R$ 使得 $b = a \cdot r$, 再由 $b \mid a$ 知存在 $r' \in R$ 使得 $a = b \cdot r'$. 故知

$$a = b \cdot r' = (a \cdot r) \cdot r' = a \cdot (r \cdot r').$$

也就是說

$$a \cdot (1 - r \cdot r') = a - a \cdot (r \cdot r') = 0.$$

利用 $a \neq 0$ 且 R 是一個 integral domain, 得 $r \cdot r' = 1$. 換句話說 r' 是 R 的一個 unit. □

為了方便起見, 我們給有 Lemma 8.1.3 中的關係一個特殊的名稱.

Definition 8.1.4. 若 $a, b \in R \setminus \{0\}$ 且存在 $u \in R$ 是 R 中的一個 unit 滿足 $a = b \cdot u$, 則稱 a 和 b 是 associates. 記為 $a \sim b$.

利用 Lemma 8.1.3 中的 (2) 我們知 $a \sim b$ 若且唯若 $\big(a\big) = \big(b\big)$, 所以馬上得知 $\sim$ 是一個 equivalence relation.

回顧一下在 $\mathbb{Z}$ 中我們定 a, b 的 greatest common divisor 是 a, b 的 common divisor 中最大的, 而在 $F[x]$ 中我們定 $f(x), g(x)$ 的 greatest common divisor 是 $f(x), g(x)$ 的 common divisor 中 degree 最大的. 在一般的 integral domain 是無法定大小或 degree 的. 不過前兩種情況的 greatest common divisor 都有一個共同的性質 (參見 Corollary 7.1.5 (2) 以及 Corollary 7.2.9 (2)), 我們就用這個性質來定 integral domain 中的 greatest common divisor.

Definition 8.1.5. 若 R 是一個 integral domain, $a_1, \ldots, a_n$ 是 R 中的非 0 元素.

(1) 若 $c \in R$ 滿足 $c \mid a_i$, $\forall i \in \{1, \ldots, n\}$ 則稱 c 是 $a_1, \ldots, a_n$ 的一個 *common divisor*.

(2) 若 $d \in R$ 是 $a_1, \ldots, a_n$ 的一個 common divisor 且滿足對任意 $a_1, \ldots, a_n$ 的 common divisor c 皆滿足 $c \mid d$, 則稱 d 是 $a_1, \ldots, a_n$ 的一個 *greatest common divisor*.

若 u 是 R 中的 unit, 則由於 $\big(u\big) = R$ (Lemma 6.2.4) 可知對任意 $a_1, \ldots, a_n$ 皆有 $\big(a_i\big) \subseteq \big(u\big)$, $\forall i \in \{1, \ldots, n\}$. 也就是說 $u \mid a_i$, $\forall i \in \{1, \ldots, n\}$. 故知 R 中的 unit 都是 $a_1, \ldots, a_n$ 的 common divisor. 不過對一般的 integral domain, 對任意的 $a_1, \ldots, a_n$ 其 greatest common divisor 未必存在. 即使存在其 greatest common divisor 也不一定唯一 (在 $F[x]$ 的情況就是一例). 另外要注意的是在此定義之下 $\mathbb{Z}$ 中的 greatest common divisor 和 Section 7.1 中 Definition 7.1.3 的 greatest common divisor 相差了一個正負號. 接著我們列出 greatest common divisor 的基本性質.

Lemma 8.1.6. 設 R 是一個 *integral domain.*

(1) 假設 d 和 d' 皆為 $a_1, \ldots, a_n$ 的 *greatest common divisor,* 則 d 和 d' *associates.*

(2) 假設 R 中任兩個非 0 元素的 *greatest common divisor* 存在, 則 R 中任意 n 個非 0 元素的 *greatest common divisor* 也存在.

Proof. (1) 若 d 和 d' 皆是 $a_1, \ldots, a_n$ 的 greatest common divisor, 則由定義知 d 是 $a_1, \ldots, a_n$ 的 common divisor. 再利用 d' 是 $a_1, \ldots, a_n$ 的 greatest common divisor 得證 $d \mid d'$. 同理得 $d' \mid d$. 故利用 Lemma 8.1.3 知 $d \sim d'$.

(2) 假設 R 中任兩個非 0 元素的 greatest common divisor 存在, 我們利用數學歸納法證明任意 n 個非 0 元素 $a_1, \ldots, a_n$ 的 greatest common divisor 也存在. 假設任意 $n-1$ 個非 0 元素 $a_1, \ldots, a_{n-1}$ 的 greatest common divisor 存在且為 d_0. 因 d_0 和 a_n 皆是 R 中的非 0 元素, 由假設知其 greatest common divisor 存在. 令 d 為 d_0 和 a_n 的 greatest common divisor, 我們要證明 d 為 $a_1, \ldots, a_n$ 的 greatest common divisor.

首先由 $d \mid d_0$ 且 d_0 是 $a_1, \ldots, a_{n_1}$ 的 common divisor 知 $d \mid d_0 \mid a_i$, $\forall i \in \{1, \ldots, n-1\}$. 再由 $d \mid a_n$ 知 d 是 $a_1, \ldots, a_n$ 的一個 common divisor.

接著若 c 是 $a_1, \ldots, a_n$ 的一個 common divisor, 則 c 當然是 $a_1, \ldots, a_{n-1}$ 的一個 common divisor. 故由 d_0 是 $a_1, \ldots, a_{n-1}$ 的 greatest common divisor 知 $c \mid d_0$. 換言之 c 是 d_0 和 a_n 的一個 common divisor. 故由 d 是 d_0 和 a_n 的 greatest common divisor 知 $c \mid d$. 因此由定義知 d 是 $a_1, \ldots, a_n$ 的 greatest common divisor. □

最後我們要定義 irreducible element 和 prime element. Irreducible 是不可分解的意思, 換言之就是除了 trivial divisor 外沒有其他的 divisor.

Definition 8.1.7. 設 R 是一個 integral domain.

(1) 若 a 是 R 中的非 0 元素且滿足 a 的 divisor 都是 trivial divisor (也就是說, 若 $d \mid a$ 則 d 是一個 unit 或 $d \sim a$), 則稱 a 是 R 的一個 *irreducible element.*

(2) 若 p 是 R 中的非 0 元素且對任意滿足 $p \mid c \cdot d$ 的 $c, d \in R$ 皆有 $p \mid c$ 或 $p \mid d$, 則稱 p 是 R 的一個 *prime element.*

我們提過 irreducible element 和 prime element 的定義基本上是不同的, 所以它們原則上是兩種不同的特性. 不過以下的結果告訴我們在 integral domain 之下 prime element 一定是 irreducible element.

Lemma 8.1.8. 假設 R 是 *integral domain.* 若 $a \in R$ 是一個 *prime element,* 則 a 也是一個 *irreducible element.*

Proof. 任取 $d \mid a$, 要說 a 是 irreducible 就是要證明 d 是一個 unit 或 $d \sim a$. 由於 $d \mid a$, 故存在 $r \in R$ 滿足 $a = d \cdot r$. 所以我們有 $a \mid d \cdot r$. 利用 a 是 prime 的性質知 $a \mid d$ 或 $a \mid r$. 如果 $a \mid d$, 由 $d \mid a$ 的假設以及 Lemma 8.1.3 知 $d \sim a$. 如果 $a \mid r$, 同樣的由 Lemma 8.1.3 知 $a \sim r$. 換句話說, 存在一個 unit u 使得 $a = u \cdot r$. 由 $a = d \cdot r = u \cdot r$ 以及 R 是一個 integral domain 知 $d = u$ 是一個 unit. □

前面曾經提過我們喜歡用 ideal 的關係來描繪元素間的整除關係. 下面的 Lemma 就是告訴我們 irreducible element 和 prime element 所產生的 principle ideal 所對應的性質.

Lemma 8.1.9. 假設 R 是一個 *integral domain,* $a \in R$ 且 $a \neq 0$.

(1) a 是一個 *irreducible element* 若且唯若沒有 *nontrivial principle ideal* 包含 $\big(a\big)$.

(2) a 是一個 *prime element* 若且唯若 $\big(a\big)$ 是一個 *prime ideal.*

Proof. (1) $\Rightarrow$: 假設 a 是一個 irreducible element, 如果存在 $b \in R$ 滿足 $\big(a\big) \subseteq \big(b\big)$, 由 Lemma 8.1.2 知 $b \mid a$. 故由 a 是 irreducible 得 b 是一個 unit 或是 $b \sim a$. 換言之 $\big(b\big) = R$ (Lemma 6.2.4) 或 $\big(b\big) = \big(a\big)$ (Lemma 6.5.4). 所以找不到 nontrivial principle ideal 包含 $\big(a\big)$.

$\Leftarrow$: 反之若 $d \mid a$, 則知 $\big(a\big) \subseteq \big(d\big)$. 由假設沒有 nontrivial principle ideal 包含 $\big(a\big)$, 得 $\big(d\big)$ 是一個 trivial principle ideal 包含 $\big(a\big)$. 換言之 $\big(d\big) = R$ 或 $\big(d\big) = \big(a\big)$. 若 $\big(d\big) = R$ 表示 $\big(d\big) = \big(1\big)$ 故由 Lemma 8.1.3 知 $d \sim 1$, 也就是說 d 是一個 unit. 若 $\big(d\big) = \big(a\big)$ 同樣由 Lemma 8.1.3 知 $d \sim a$. 故得 a 是一個 irreducible element.

(2) $\Rightarrow$: 假設 a 是一個 prime element. 如果 $c \cdot d \in \big(a\big)$, 知 $a \mid c \cdot d$. 故由 a 是 prime 的假設知 $a \mid c$ 或 $a \mid d$. 這告訴我們 $c \in \big(a\big)$ 或 $d \in \big(a\big)$, 故得證 $\big(a\big)$ 是一個 prime ideal.

$\Leftarrow$: 假設 $\big(a\big)$ 是一個 prime ideal. 任取 $c, d \in R$ 滿足 $a \mid c \cdot d$, 知 $c \cdot d \in \big(a\big)$. 故由 $\big(a\big)$ 是一個 prime ideal 的假設得 $c \in \big(a\big)$ 或 $d \in \big(a\big)$. 換言之 $a \mid c$ 或 $a \mid d$, 故得證 a 是一個 prime element. □

8.2. Euclidean Domain

我們知道 $\mathbb{Z}$ 和 $F[x]$ 有所謂的 Euclid's Algorithm (餘數及餘式定理). 在這一節中, 我們將利用這個性質的特性定義一種特殊的 ring 稱為 Euclidean domain. 要注意我們的定義比一般書上的定義簡化, 主要的原因是我們只重視目前有用的特性. 不過事實上我們定義的 Euclidean domain 和一般書上定義的 Euclidean domain 可以證明是相同的.

回顧一下 $\mathbb{Z}$ 中的 Euclid's Algorithm 可以說是任取 $a, b \in \mathbb{Z}$, 其中 $b \neq 0$, 則存在 $h, r \in \mathbb{Z}$, 其中 r 符合 $r = 0$ 或 $|r| < |b|$ 使得 $a = b \cdot h + r$. 而在 $F[x]$ 中的 Euclid's Algorithm 是說任取 $f(x), g(x) \in F[x]$ 其中 $g(x) \neq 0$, 則存在 $h(x), r(x) \in F[x]$, 其中 $r(x)$ 符合 $r(x) = 0$ 或 $\deg(r(x)) < \deg(g(x))$ 使得 $f(x) = g(x) \cdot h(x) + r(x)$. 這裡重要的是在 $\mathbb{Z}$ 中有一個絕對值函數將 $\mathbb{Z}$ 中的非 0 元素送到非負的整數, 而在 $F[x]$ 中有一個 degree 函數將 $F[x]$ 中的非 0 元素送到非負的整數. 我們就是要擷取這樣的函數的特性.

Definition 8.2.1. 設 R 是一個 integral domain. 如果存在一函數

$$\Phi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

使得對任意的 $a, b \in R$ 其中 $b \neq 0$ 都可以找到 $h, r \in R$, 其中 r 符合 $r = 0$ 或 $\Phi(r) < \Phi(b)$, 滿足 $a = b \cdot h + r$, 則稱 R 為一個 *Euclidean domain*.

除了 $\mathbb{Z}$ 和 $F[x]$ 外還有許多的 Euclidean domain. 例如 $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ 這一個 integral domain 利用 $\Phi(a+bi) = a^2+b^2$ 這個函數就可得 $\mathbb{Z}[i]$ 是一個 Euclidean domain (在此我們略去證明, 若有興趣的同學可到網站 http://math.ntnu.edu.tw/∼li/note 下載講義 "Factorization of Commutative Rings" 有詳細證明).

一般而言要驗證一個 integral domain 是否為一個 Euclidean domain 是很困難的. 在此我們並不討論這類的問題. 我們僅列出 Euclidean domain 的重要性質. 回顧我們曾利用 Euclid's Algorithm 證出在 $\mathbb{Z}$ 和 $F[x]$ 中所有的 ideal 都是 principle ideal. 這一套證明可以完完整整搬到 Euclidean domain 上.

Theorem 8.2.2. 若 R 是一個 *Euclidean domain* 則 R 中的 *ideal* 都是 *principle ideal.*

Proof. 若 I 是 R 中的一個 ideal. 考慮 $T = \{\Phi(a) \mid a \in I \setminus \{0\}\}$ 這一個集合. 由於 Φ 的值域在 $\mathbb{N} \cup \{0\}$ 所以 T 是 $\mathbb{N} \cup \{0\}$ 的一個子集合. 因此 T 必存在最小的元素. 換句話說存在 $d \in I \setminus \{0\}$ 使得對任意的 $a \in I \setminus \{0\}$ 皆有 $\Phi(d) \leq \Phi(a)$. 我們欲證 $I = \big(d\big)$.

由於 $d \in I$, 自然得 $\big(d\big) \subseteq I$. 另外對任意 $a \in I$, 由 Euclidean domain 的假設知存在 $h, r \in R$ 滿足 $a = d \cdot h + r$ 且 $r = 0$ 或 $\Phi(r) < \phi(d)$. 如果 $r \neq 0$, 由 $r = a - d \cdot h$ 且 $a, d \in I$ 可知 $r \in I$. 也就是說 $r \in I \setminus \{0\}$ 且 $\Phi(r) < \Phi(d)$. 這和 $\Phi(d)$ 是 T 中最小的假設相矛盾, 故知 $r = 0$. 換言之 $a = d \cdot h$, 即 $a \in \big(d\big)$. 故得證 $I \subseteq \big(d\big)$. □

由於一個 integral domain 的 ideal 都是 principle ideal 這樣的 ring 非常特別, 我們也給它一個特別的名稱.

Definition 8.2.3. 如果 R 是一個 integral domain 且 R 中的 ideal 都是 principle ideal, 則稱 R 為一個 *principle ideal domain.*

Theorem 8.2.2 告訴我們一個 Euclidean domain 一定是一個 principle ideal domain. 要注意, 一個 principle ideal domain 未必會是一個 Euclidean domain. 有興趣的同學可以參考我的講義 "Factorization of Commutative Rings" 其中有給一個 principle ideal domain 但不是 Euclidean domain 的例子.

8.3. Principle Ideal Domain

這一節中我們將探討 principle ideal domain 的基本性質. 由於已知一個 Euclidean domain 一定是 principle ideal domain, 所以這一節所談的性質當然適用於 Euclidean Domain.

前面提過對一般的 integral domain 任給兩個非 0 元素其 greatest common divisor 不一定存在. 不過對於 principle ideal domain, 任意兩個非 0 元素之 greatest common divisor 就一定存在了!

Proposition 8.3.1. 假設 R 是一個 *principle ideal domain.* 對任意 $a, b \in R$ 且 $a, b \neq 0$ 其 *greatest common divisor* 存在. 而且, *若* d 是 a, b 的一個 *greatest common divisor,* 則存在 $r, s \in R$ 使得 $d = r \cdot a + s \cdot b$.

Proof. 首先考慮 $\big(a\big) + \big(b\big)$ 這一個 ideal. 由於 R 是 principle ideal domain, 故存在 $d \in R$ 滿足 $\big(d\big) = \big(a\big) + \big(b\big)$. 我們想要證明 d 就是 a, b 的 greatest common divisor.

首先先證明 d 是 a, b 的 common divisor. 由於

$$\big(a\big) \subseteq \big(a\big) + \big(b\big) = \big(d\big),$$

故由 Lemma 8.1.2 知 $d \mid a$. 同理可證 $d \mid b$, 故得 d 是 a, b 的一個 common divisor.

接下來證明若 c 是 a, b 的一個 common divisor, 則 $c \mid d$. 然而若 $c \mid a$ 且 $c \mid b$, 表示 $\big(a\big) \subseteq \big(c\big)$ 且 $\big(b\big) \subseteq \big(c\big)$. 由於 $\big(c\big)$ 是一個 ideal, 它有加法的封閉性, 故得 $\big(a\big) + \big(b\big) \subseteq \big(c\big)$. 也就是說 $\big(d\big) \subseteq \big(c\big)$. 故得證 $c \mid d$.

最後由定義, $\big(a\big) + \big(b\big)$ 中的元素都是 $r \cdot a + s \cdot b$, 其中 $r, s \in R$ 這種形式. 故由 $d \in \big(d\big) = \big(a\big) + \big(b\big)$ 知一定存在 $r, s \in R$ 使得 $d = r \cdot a + s \cdot b$. 這個特性對於任意 a, b 的 greatest common divisor 皆對. 這是因為由 Lemma 8.1.6 知若 d' 是 a, b 另一個 greatest common divisor, 則我們依然有 $\big(d'\big) = \big(d\big) = \big(a\big) + \big(b\big)$. □

"若 d 是 a, b 的一個 greatest common divisor, 則存在 $r, s \in R$ 滿足 $d = r \cdot a + s \cdot r$" 這一個特性非常有用. 大家可以利用這個特性再仿照 Proposition 7.1.7 或 Proposition 7.2.11 的証明方式證得一個 principle ideal domain 中的 irreducible element 都是 prime element. 不過這裡我們介紹另一種利用 ideal 方法的證明.

Lemma 8.3.2. 假設 R 是一個 *principle ideal domain,* $a \in R$ 且 $a \neq 0$. 若 a 是 R 的一個 *irreducible element* 則 $\big(a\big)$ 是 R 的一個 *maximal ideal.* 反之, 若 $\big(a\big)$ 是 R 的一個 *maximal ideal,* 則 a 是 R 的一個 *irreducible element.*

Proof. 如果 a 是一個 irreducible element, 由 Lemma 8.1.9 (1) 我們知道找不到一個 nontrivial 的 principle ideal 介於 $\big(a\big)$ 和 R 之間. 不過由 R 是 principle ideal 的假設知 R 中的 ideal 都是 principle ideal. 換句話說就是找不到一個 ideal 介於 $\big(a\big)$ 和 R 之間. 故得 $\big(a\big)$ 是一個 maximal ideal.

反之, 如果 $\big(a\big)$ 是一個 maximal ideal, 當然找不到 nontrivial principle ideal 包含 $\big(a\big)$. 故利用 Lemma 8.1.9 (1) 知 a 是一個 irreducible element. □

回顧一下 Lemma 8.1.9 的另一部分是說 a 是 prime element 若且唯若 $\big(a\big)$ 是一個 prime ideal. 所以我們很快的就可以得到以下之結果.

Proposition 8.3.3. 假設 R 是一個 *principle ideal domain,* 則 R 中的 *irreducible element* 都是 *prime element.* 反之, R 中的 *prime element* 都是 *irreducible element.*

Proof. 因為 R 是 integral domain, Lemma 8.1.8 告訴我們 R 中的 prime element 都是 irreducible element.

反之, 若 a 是 R 中的 irreducible element, 由 Lemma 8.3.2 知 $\big(a\big)$ 是 R 的一個 maximal ideal. 然而 Corollary 6.5.13 告訴我們 R 中的 maximal ideal 都是 prime ideal, 故知 $\big(a\big)$ 是 R 的一個 prime ideal. 因此利用 Lemma 8.1.9 (2) 得證 a 是一個 prime element. □

前面提過在一般的 commutative ring with 1 中的 maximal ideal 都是 prime ideal, 但是 prime ideal 未必是 maximal ideal. 然而 Lemma 8.3.2 以及 Proposition 8.3.3 將 principle ideal domain 中的 maximal ideal 和 prime ideal 給了一個重要的關連.

Corollary 8.3.4. 假設 R 是一個 *principle ideal domain* 且 I 是 R 中一個非 0 的 *ideal.* 則 I 是一個 *prime ideal* 若且唯若 I 是一個 *maximal ideal.*

Proof. 我們已知一個 maximal ideal 一定是 prime ideal. 所以只要證明若 I 是一個非 0 的 prime ideal, 則 I 是一個 maximal ideal.

因 R 是一個 principle ideal domain, 故存在 $a \neq 0$ 使得 $I = \big(a\big)$. 如果 $\big(a\big)$ 是一個 prime ideal, 則由 Lemma 8.1.9 知 a 是一個 prime element. 故由 Proposition

8.3.3 (或 Lemma 8.1.8) 知 a 是一個 irreducible element. 因此由 Lemma 8.3.2 知 $\big(a\big) = I$ 是一個 maximal ideal. □

我們曾經利用 $\mathbb{Z}$ 和 $F[x]$ 中的 irreducible element 和 prime element 是相同的證明 $\mathbb{Z}$ 和 $F[x]$ 的唯一分解性質. 我們現在幾乎已到達可以證明 principle ideal domain 的唯一分解性質的目標. 不過當時我們在 $\mathbb{Z}$ 和 $F[x]$ 中是利用數學歸納法來證明唯一分解性質, 現在在一般的 principle ideal domain 我們沒辦法使用數學歸納法. 下一個 Lemma 可以幫助我們克服這個困難.

Lemma 8.3.5. 假設 R 是一個 *principle ideal domain,* 則無法在 R 中找到無窮多個嚴格遞增的 *ideals.* 換句話說如果 $\{I_n\}_{n=1}^{\infty}$ 是一組 R 中的 *ideal* 滿足

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots,$$

則存在 $m \in \mathbb{N}$ 使得 $I_m = I_{m+1} = \cdots$.

Proof. 首先我們考慮 $I = \cup_{n=1}^{\infty} I_n$ 這一個集合. 我們想要證明 I 是 R 中的 ideal. (要注意一般來講若 J_1, J_2 是 R 的 ideal 那麼 $J_1 \cup J_2$ 不一定是 R 的 ideals. 不過在這裡由於 I_n 有包含的關係, 我們可以證出 I 是一個 ideal.)

假設 $a, b \in I$, 換句話說存在 $i, j \in \mathbb{N}$ 使得 $a \in I_i$ 且 $b \in I_j$. 假設 $i \geq j$, 由假設知 $I_j \subseteq I_i$. 故得 $a, b \in I_i$. 因此由 I_i 是一個 ideal, 我們有 $a - b \in I_i$. 所以得 $a - b \in I$. 另外若 $a \in I$ 且 $r \in R$, 由假設知存在 $i \in \mathbb{N}$ 使得 $a \in I_i$. 故得 $a \cdot r \in I_i$, 也就是說 $a \cdot r \in I$. 故由 Lemma 6.1.2 知 I 是 R 中的一個 ideal.

既然 I 是 R 的 ideal 且 R 是 principle ideal domain, 故存在 $a \in R$ 使得 $\big(a\big) = I$. 然而利用 $a \in \big(a\big) = I$ 知存在 $m \in \mathbb{N}$ 使得 $a \in I_m$. 故利用 $\big(a\big)$ 是包含 a 最小的 ideal (Lemma 6.5.1) 知 $I = \big(a\big) \subseteq I_m$. 換句話說 $I = I_m$, 因此利用對所有的 $i > m$ 皆有 $I_m \subseteq I_i$ 以及 $I_i \subseteq I$ 得證 $I = I_m = I_i, \forall\, i > m$. □

我們要藉用 Lemma 8.3.5 的主要原因是如果 d 是 a 的一個 nontrivial divisor (即 $d \mid a$ 但 d 不是 unit 且和 a 不 associates), 則 $\big(a\big) \subsetneq \big(d\big)$. 如此一來, 可以證出 R 中的元素只能寫成有限多個 irreducible element 的乘積.

Theorem 8.3.6. 假設 R 是一個 *principle ideal domain* 且 a 是 R 中不為 0 且不是 *unit* 的元素, 則 a 可以寫成有限多個 R 中的 *irreducible elements* 的乘積, 而且若忽略 *associates* 的關係以及乘法的順序, 這個乘積的寫法唯一. 也就是說如果

$$\begin{aligned} a &= p_1^{n_1} \cdots p_r^{n_r} \\ &= q_1^{m_1} \cdots q_s^{m_s} \end{aligned}$$

其中 $p_1, \ldots, p_r$ 是兩兩不相 *associates* 的 *irreducible elements* 且 $q_1, \ldots, q_s$ 是兩兩不相 *associates* 的 *irreducible elements,* 則經過適當的變換順序, 我們有 $r = s$, $p_i \sim q_i$ 以及 $n_i = m_i$, $\forall\, i = 1, \ldots, r$.

Proof. 首先我們證明 a 可以寫成有限多個 irreducible elements 的乘積. 如果 a 不能寫成有限多個 irreducible elements 的乘積, 表示 a 本身不是 irreducible, 因此 $a = a_1 \cdot b_1$, 其中 $a_1, b_1 \in R$ 是 a 的 nontrivial divisors 且 a_1, b_1 中必有一個不能寫成有限多個 irreducible elements 的乘積. 假設是 a_1, 同上我們知存在 $a_2, b_2 \in R$ 使得 $a_1 = a_2 \cdot b_2$, 其中a_2 是 a_1 的 nontrivial divisor 且 a_2 不能寫成有限多個 irreducible elements 的乘積. 如此一直下去我們製造了一連串的 ideals 符合

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots .$$

此和 Lemma 8.3.5 矛盾, 故知 a 一定可以寫成有限多個 irreducible elements 的乘積.

接下來我們證唯一性. 一般來說若已證得 irreducible element 就是 prime element 唯一性就自動成立. 這是因為如果

$$a = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s},$$

任取 p_i 由於

$$p_i \mid q_1^{m_1} \cdots q_s^{m_s},$$

且 p_i 是 prime (Proposition 8.3.3) 知存在 $j \in \{1, \ldots, s\}$ 使得 $p_i \mid q_j$. 換言之 p_i 是 q_j 的一個 divisor. 然而 q_j 是 irreducible 且 p_i 不是 unit, 故得 $p_i \sim q_j$ (即 p_i 和 q_j associates). 因此我們知道對這個 p_i, 在 $\{q_1, \ldots, q_s\}$ 中只能找到唯一的 q_j 使得 $p_i \sim q_j$. 否則若 $j \neq j'$ 但 $p_i \mid q_{j'}$, 則同理可得 $p_i \sim q_{j'}$, 利用 associates 是個 equivalence relation 我們得 $q_j \sim q_{j'}$, 這和假設若 $j \neq j'$ 則不可能 $q_j \sim q_{j'}$ 相矛盾. 反之對任意的 q_j 我們可以在 $\{p_1, \ldots, p_r\}$ 中找到唯一的 p_i 使得 $q_j \sim p_i$. 因此我們在 $\{p_1, \ldots, p_r\}$ 和 $\{q_1, \ldots, q_s\}$ 這兩個集合中找到一對一的對應. 也就是說 $r = s$ 且經過適當的重排我們有 $p_1 \sim q_1, \ldots, p_r \sim q_r$. 現假設某個 $n_i \neq m_i$, 為了方便起見我們就假設 $n_1 \neq m_1$ 且 $n_1 > m_1$ 吧! 由於 $q_1 = u \cdot p_1$, 其中 u 是 R 的一個 unit, 我們有

$$p_1^{m_1}(p_1^{n_1 - m_1} \cdot p_2^{n_2} \cdots p_r^{n_r} - u^{m_1} \cdot q_2^{m_2} \cdots q_r^{m_r}) = 0.$$

利用 $p_1^{m_1} \neq 0$ 且 R 是 integral domain, 我們有

$$p_1^{n_1 - m_1} \cdot p_2^{n_2} \cdots p_r^{n_r} = u^{m_1} \cdot q_2^{m_2} \cdots q_r^{m_r}.$$

然而由於 $n_1 - m_1 > 0$, 可得在 $\{q_2, \ldots, q_r\}$ 中存在 q_j 使得 $p_1 \mid q_j$ (注意 u 是 unit 故不可能 $p_1 \mid u$). 也就是說 $p_1 \sim q_j$, 但這和 q_1 是 $\{q_1, \ldots, q_r\}$ 中唯一滿足和 p_1 associates 的元素相矛盾. 得證本定理. □

滿足 Theorem 8.3.6 中的唯一分解性質的 ring 非常重要, 我們也給它一個特殊的名子.

Definition 8.3.7. 假設 R 是一個 integral domain 而且 R 中非 0 且不是 unit 的元素都可以寫成有限多個 R 中的 irreducible elements 的乘積, 而且若忽略 associates

的關係以及乘法的順序, 這個乘積的寫法唯一, 則稱 R 是一個 *unique factorization domain*.

Theorem 8.3.6 告訴我們一個 principle ideal domain 一定是一個 unique factorization domain. 但是一個 unique factorization domain 並不一定是 principle ideal domain. 我們曾經見過 $\mathbb{Z}[x]$ 是一個 unique factorization domain (Theorem 7.3.13) 但其中 $\big(2\big)+\big(x\big)$ 這一個 ideal 並不是 principle ideal (Example 7.3.1).

8.4. Unique Factorization Domain

這一節中我們將探討 unique factorization domain 的性質, 並利用這些性質建構出一系列的 unique factorization domains.

8.4.1. Unique factorization domain 的基本性質. 對於一個 unique factorization domain 我們可以像處理整數的情況來處理一些有關於 divisor 的問題. 比方說在 $\mathbb{Z}$ 中要找到兩元素 a,b 的 greatest common divisor 除了利用輾轉相除法外, 我們還可將 a,b 做質因數分解以求出 greatest common divisor.

對於一般的 unique factorization domain R 由於 R 不一定是 Euclidean domain, 所以無法用類似輾轉相除法的方法求 greatest common divisor. 然而若 $a,b\in R$, 我們可以利用 unique factorization domain 的性質將 a,b 分解成

$$a=u\cdot p_1^{n_1}\cdots p_r^{n_r},\quad \text{及}\quad b=v\cdot p_1^{m_1}\cdots p_r^{n_r},\tag{8.1}$$

其中 u,v 是 R 中的 units, $p_1,\dots,p_r$ 是 R 中兩兩不 associates 的 irreducible elements, 而對任意的 $i\in\{1,\dots,r\}$, n_i 和 m_i 都是非負但不同時為 0 的整數. 這裡我們可以要求 $p_1,\dots,p_r$ 都出現在 a,b 的質因數的分解中主要是我們容許 n_i 或 m_i 為 0, 所以若 $p_i\mid a$ 但 $p_i\nmid b$ 我們令 $m_i=0$. 反之若 $p_j\mid b$ 但 $p_j\nmid a$, 則令 $n_j=0$. 因此若令

$$d=p_1^{t_1}\cdots p_r^{t_r},$$

其中 $t_i=\min\{n_i,m_i\}$, 我們可以證明 d 是 a,b 的 greatest common divisor.

Proposition 8.4.1. 假設 R 是一個 *unique factorization domain* 且 $a_1,\dots,a_n$ 是 R 中的非 0 元素, 則 $a_1,\dots,a_n$ 的 *greatest common divisor* 存在.

Proof. 利用 Lemma 8.1.6 我們只要證明 R 中任意兩個非 0 元素 a 和 b 的 greatest common divisor 存在即可.

首先我們將 a,b 的分解寫成式子 (8.1) 的形式, 且令

$$d=p_1^{t_1}\cdots p_r^{t_r},$$

其中 $t_i=\min\{n_i,m_i\}$. 我們要證明 d 是 a,b 的 greatest common divisor.

首先由 $t_i\le m_i$ 以及 $t_i\le n_i$, $\forall\, i=1,\dots,r$, 很容易得知 $d\mid a$ 且 $d\mid b$. 因此知 d 是 a,b 的 common divisor. 現若 c 是 a,b 的一個 common divisor, 假設 p 是一個 irreducible element 且 $p\mid c$, 則由 $p\mid a$ 且 $p\mid b$ 知 p 一定和 $p_1,\dots,p_r$ 中某一個

p_i associates. 這告訴我們在 c 的分解中不可能出現和 $p_1, \ldots, p_r$ 不 associates 的 irreducible divisor, 也就是說我們也可將 c 分解成

$$c = w \cdot p_1^{s_1} \cdots p_r^{s_r},$$

其中 w 是 unit 且 s_i 是非負整數. 現如果有個 i 符合 $s_i > n_i$, 為了方便就假設 $s_1 > n_1$ 吧! 利用 $p_1^{s_1} \mid c$ 以及 $c \mid a$ 知 $p_1^{s_1} \mid a$. 換言之

$$p_1^{s_1 - n_1} \mid p_2^{n_2} \cdots p_r^{n_r}.$$

由 $s_1 - n_1 \geq 1$ 得

$$p_1 \mid p_2^{n_2} \cdots p_r^{n_r}.$$

然而 p_1 是 prime, 這表示 p_1 和 $p_2, \ldots, p_r$ 中某個 p_i associates. 這和當初假設 $p_1, \ldots, p_r$ 兩兩不 associates 相矛盾, 故得 $s_i \leq n_i$, $\forall\, i = 1, \ldots, r$. 同理 $s_i \leq m_i$, $\forall\, i = 1, \ldots, r$. 故得知對所有的 $i = 1, \ldots, r$ 皆有 $s_i \leq \min\{n_i, m_i\} = t_i$. 也就是說 $c \mid d$. 故知 d 是 a, b 的 greatest common divisor. □

在前面幾節中要證明一個 integral domain 是一個 unique factorization domain, 我們都去證明這個 integral domain 中的 irreducible elements 和 prime elements 是一樣的. 事實上, 在 unique factorization domain 中 irreducible element 和 prime element 總是相同的.

Proposition 8.4.2. *若 R 是一個 unique factorization domain, 則 R 中的 irreducible elements 和 prime elements 是相同的.*

Proof. 我們已知在一個 integral domain 中 prime element 會是 irreducible element (Lemma 8.1.8). 所以我們只要證明 irreducible element 也會是 prime element.

假設 $p \in R$ 是一個 irreducible element 且 $p \mid a \cdot b$, 其中 $a, b \in R$. 由假設知存在 $h \in R$ 滿足 $a \cdot b = h \cdot p$. 首先我們將 a, b 用式子 (8.1) 的形式分解, 因此有

$$a \cdot b = (u \cdot v) \cdot p_1^{n_1 + m_1} \cdots p_r^{n_r + m_r}.$$

利用 R 是 unique factorization domain, 由 $a \cdot b$ 的分解知 p 一定和 $p_1, \ldots, p_r$ 中某一個 p_i associates. 然而 n_i 和 m_i 不同時為 0, 也就是說 $n_i \neq 0$ 或 $m_i \neq 0$. 若 $n_i \neq 0$, 則知 $p \mid a$, 而若 $m_i \neq 0$ 則有 $p \mid b$. 故得證 p 是 prime element. □

8.4.2. Polynomials over unique factorization domain. 我們將利用類似推導 $\mathbb{Z}[x]$ 是 unique factorization domain 的方法推導當 R 是 unique factorization domain 時

$$R[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in R\}$$

這種以 R 為係數的 polynomials 所形成的 polynomial ring 是一個 unique factorization domain.

若 $f(x) \in R[x]$ 且 $f(x) \neq 0$, 則我們可將 $f(x)$ 寫成 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 其中 $a_n \neq 0$. 如同前面討論 $F[x]$ 的情況我們可以定義 $\deg(f(x)) = n$. 利用和 Lemma 7.2.2 同樣的證明我們可以得到: 若 $f(x), g(x) \in R[x]$ 且皆不為 0, 則

$$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

主要的原因是 Lemma 7.2.2 的証明僅用到兩個非 0 元素相乘不為 0 (即 integral domain) 的性質, 並沒有用到 field 的性質. 利用 degree 的這個特性我們馬上有以下的性質.

Lemma 8.4.3. 令 R 是一個 *integral domain.*

(1) $R[x]$ 也是一個 *integral domain.*

(2) $R[x]$ 中的 *unit* 就是 R 中的 *unit.*

(3) 若 $a \in R$ 是 R 中的 *irreducible element* 則 a 看成是 $R[x]$ 中的元素 (即常數多項式) 時也是 *irreducible.*

Proof. (1) 若 $f(x) \neq 0$ 且 $g(x) \neq 0$, 假設 $f(x)$ 的最高次項係數是 a_n 且 $g(x)$ 的最高次項係數是 b_m, 則 $f(x) \cdot g(x)$ 的最高次項係數是 $a_n \cdot b_m$. 由於 $a_n, b_m \in R$, 且 $a_n \neq, b_m \neq 0$ 利用 R 是 integral domain 知 $a_n \cdot b_m \neq 0$. 也就是說 $f(x) \cdot g(x)$ 不可能為 0 多項式.

(2) 若 $f(x) \in R[x]$ 是 $R[x]$ 中的 unit, 則利用存在 $g(x) \in R[x]$ 滿足 $f(x) \cdot g(x) = 1$ 知 $\deg(f(x)) + \deg(g(x)) = 0$ (注意 1 是常數多項式故 degree 為 0). 故得 $\deg(f(x)) = \deg(g(x)) = 0$. 換句話說 $f(x), g(x)$ 都是常數多項式, 也就是說 $f(x), g(x) \in R$. 然而由假設 $f(x) \cdot g(x) = 1$ 知 $f(x)$ 是 R 中的 unit.

(3) 假設 $a \in R$ 是 R 中的 irreducible element. 注意由 degree 的性質知若 $g(x)$ 是 $f(x)$ 的 divisor (由於存在 $h(x) \in R[x]$ 滿足 $g(x) \cdot h(x) = f(x)$), 則 $\deg(g(x)) \leq \deg(f(x))$. 現若將 a 看成是常數多項式, 由於 $\deg(a) = 0$, 故知在 $R[x]$ 中 a 的 divisor 其 degree 也是 0. 換句話說在 $R[x]$ 中 a 的 divisor 都是 R 的元素. 故利用 a 在 R 中是 irreducible 知這些 divisor 要不是 R 中的 unit 就是和 a associates. 然而由 (2) 知 R 中的 unit 當然也是 $R[x]$ 中的 unit, 故知 a 在 $R[x]$ 依然是 irreducible. □

當 R 是一個 unique factorization domain 時, 令 F 為 R 的 quotient field. 接下來我們想利用 R 和 $F[x]$ 都是 unique factorization domain (Theorem 7.2.14) 證明 $R[x]$ 是一個 unique factorization domain.

為了將 $R[x]$ 和 $F[x]$ 的關係相連結, 我們還是得介紹和 $\mathbb{Z}[x]$ 中類似的 content 的概念. 首先由 Proposition 8.4.1 知若 $f(x) = a_n x^n + \cdots a_1 x + a_0 \in R[x]$, 則 $a_n, \ldots, a_1, a_0$ 的 greatest common divisor 是存在的.

Definition 8.4.4. 若 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ 且 $a_n, \ldots, a_1, a_0$ 的 greatest common divisor 是 R 中的 unit, 則稱 $f(x)$ 是 $R[x]$ 中的 *primitive polynomial.*

Lemma 8.4.5. 假設 R 是一個 *unique factorization domain,* 則對任意 $f(x) \in R[x]$ 且 $f(x) \neq 0$, 都可找到 $c \in R$ 且 $f^*(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomial* 滿足

$$f(x) = c \cdot f^*(x).$$

又假設

$$\begin{aligned} f(x) &= c \cdot f^*(x) \\ &= c' \cdot g(x) \end{aligned}$$

其中 $c, c' \in R$, 且 $f^*(x), g(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomials,* 則 $c \sim c'$ 且 $f^*(x) \sim g(x)$.

Proof. 首先證明存在性: 若 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 令 c 為 $a_n, \ldots, a_1, a_0$ 的 greatest common divisor. 所以對所有的 $i = 0, 1, \ldots, n$ 皆有 $a_i = c \cdot b_i$, 其中 $b_i \in R$, 而且 $b_0, \ldots, b_n$ 的 greatest common divisor 是 R 的 unit. 故令 $f^*(x) = b_n x^n + \cdots + b_1 x + b_0$, 則 $f^*(x)$ 是 $R[x]$ 的 primitive polynomial 且 $f(x) = c \cdot f^*(x)$. 故得證存在性.

接著證明唯一性: 若 $f(x) = c' \cdot g(x)$, 其中 $g(x)$ 是 $R[x]$ 的 primitive polynomial. 假設 $g(x) = a'_n x^n + \cdots + a'_1 x + a'_0$, 則對所有 $i = 0, 1, \ldots, n$, 皆有 $a_i = c' \cdot a'_i$. 換句話說 c' 是 $a_n, \ldots, a_0$ 的一個 common divisor. 因此由 c 是 $a_n, \ldots, a_0$ 的 greatest common divisor 知 $c' \mid c$. 即存在 $d \in R$ 使得 $c = c' \cdot d$. 利用 $a_i = c \cdot b_i = c' \cdot a'_i$, 我們知對所有的 $i = 0, 1, \ldots, n$, 皆有

$$c' \cdot (d \cdot b_i) = (c' \cdot d) \cdot b_i = c \cdot b_i = c' \cdot a'_i.$$

例用 $c' \neq 0$ 且 R 是 integral domain, 可得對所有的 $i = 0, 1, \ldots, n$, 皆有 $a'_i = d \cdot b_i$. 換句話說 d 是 $a'_n, \ldots, a'_0$ 的一個 common divisor. 然而由假設 $a'_n, \ldots, a'_0$ 的 greatest common divisor 是 unit, 故得 d 是 R 的一個 unit. 換句話說 $c \sim c'$. 再利用 $f(x) = c \cdot f^*(x) = c' \cdot g(x)$, 以及 $R[x]$ 是 integral domain, 得 $d \cdot f^*(x) = g(x)$. 由於 d 是 R 的 unit 也是 $R[x]$ 的 unit, 故得 $f^*(x) \sim g(x)$. □

利用 Lemma 8.4.5 的唯一性, 我們自然有以下的定義.

Definition 8.4.6. 假設 R 是一個 unique factorization domain. 若 $f(x) \in R[x]$ 可寫成 $f(x) = c \cdot f^*(x)$ 其中 $c \in R$ 且 $f^*(x)$ 是 $R[x]$ 的 primitive polynomial, 則稱 c 為 $f(x)$ 的 *content*, 定為 $c(f)$.

要注意由 Lemma 8.4.5 的證明我們知道 $f(x)$ 的 content 其實就是 $f(x)$ 所有係數的 greatest common divisor. 另外要注意的是 $f(x)$ 的 content 其實並不是一個固定的值, content 之間會差個 associates.

我們可以將 content 的定義推廣到 $F[x]$. 別忘了 F 是 R 的 quotient field, 所以 F 中每個元素都可以寫成 a/b 的形式, 其中 $a, b \in R$ 且 $b \neq 0$. 現對任意的 $f(x) = r_n x^n + \cdots + r_1 x + r_0 \in F[x]$, 由於對任意的 $i = 0, 1, \ldots, n$, 皆有 $r_i = a_i / b_i$,

其中 $a_i, b_i \in R$, 我們可找到 $d \in R$ 且 $d \neq 0$ 使得 $d \cdot f(x) \in R[x]$ (比方說令 $d = b_n \cdots b_0$). 因此利用 Lemma 8.4.5 知存在 $c \in R$ 以及 $f^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomial 使得 $d \cdot f(x) = c \cdot f^*(x)$. 由於 $d \neq 0$, 我們可將 $f(x)$ 寫成

$$f(x) = \frac{c}{d} \cdot f^*(x).$$

換句話說任意 $F[x]$ 中非 0 的 polynomial $f(x)$ 皆可寫成 $f(x) = r \cdot f^*(x)$, 其中 $r \in F$ 且 $f^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomial. 我們依然稱此 r 是 $f(x)$ 的 content 且仍記作 $c(f)$.

Corollary 8.4.7. 假設 R 是一個 *unique factorization domain,* 且 F 是 R 的 *quotient field.* 則對任意 $f(x) \in F[x]$ 且 $f(x) \neq 0$, 都可找到 $c \in F$ 且 $f^*(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomial* 滿足

$$f(x) = c \cdot f^*(x).$$

又假設

$$\begin{aligned} f(x) &= c \cdot f^*(x) \\ &= c' \cdot g(x) \end{aligned}$$

其中 $c, c' \in F$, 且 $f^*(x), g(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomials,* 則存在 $u \in R$ 是 R 的 *unit* 使得 $c = u \cdot c'$ 且 $u \cdot f^*(x) = g(x)$.

Proof. 前面已證存在性, 我們僅證唯一性. 我們將 c 和 c' 分別寫成 $c = a/b$ 且 $c' = a'/b'$, 其中 $a, a', b, b' \in R$ 且 $b \neq 0$, $b' \neq 0$. 將 $f(x)$ 乘上 $b \cdot b'$, 我們有 $(b \cdot b') \cdot f(x) \in R[x]$ 且

$$\begin{aligned} (b \cdot b') \cdot f(x) &= (a \cdot b') \cdot f^*(x) \\ &= (a' \cdot b) \cdot g(x). \end{aligned}$$

既然 $(b \cdot b') \cdot f(x) \in R[x]$ 我們可以將 Lemma 8.4.5 套用在 $(b \cdot b') \cdot f(x)$ 上, 故知存在 $u \in R$ 是 R 中的 unit 滿足 $a \cdot b' = u \cdot (a' \cdot b)$. 也就是說 $c = u \cdot c'$. 再利用 $c' \neq 0$ 及 $F[x]$ 是 integral domain 得 $u \cdot f^*(x) = g(x)$. □

和 $\mathbb{Z}[x]$ 一樣的狀況, 我們有以下的 Gauss Lemma 來幫助我們計算兩個 polynomials 相乘後之 content.

Lemma 8.4.8 (Gauss)**.** 假設 R 是一個 *unique factorization domain.* 若 $f(x), g(x) \in R[x]$ 是 $R[x]$ 中的 *primitive polynomials,* 則 $f(x) \cdot g(x)$ 依然是 $R[x]$ 中的 *primitive polynomial.*

Proof. 我們利用和 Lemma 7.3.5 相同的証明, 所以只給大略的証明. 假設 $f(x) \cdot g(x)$ 不是 primitive polynomial, 表示 $f(x) \cdot g(x)$ 所有係數的 greatest common divisor 不是 R 中的 unit. 因此利用 R 是 unique factorization domain 知存在 $p \in R$ 是 R 中的一個 irreducible (也是 prime) element 是 $f(x) \cdot g(x)$ 所有係數的 common

divisor. 然而 $f(x)$ 和 $g(x)$ 皆是 primitive polynomials, p 不可能整除所有 $f(x)$ 的係數也不可能整除所有 $g(x)$ 的係數. 所以若 i 是最小的數使得 $f(x)$ 的 x^i 項係數不能被 p 整除, 而 j 是最小的數使得 $g(x)$ 的 x^j 項係數不能被 p 整除, 則很容易看出 $f(x)\cdot g(x)$ 的 x^{i+j} 項係數不可能被 p 整除. 這和 p 是 $f(x)\cdot g(x)$ 各項係數的 common divisor 矛盾, 故得證 $f(x)\cdot g(x)$ 是 $R[x]$ 的 primitive polynomial. □

Primitive polynomial 在 $R[x]$ 中是和 $F[x]$ 溝通的橋樑, 事實上在 $R[x]$ 中不是常數的 irreducible element 都是 primitive polynomial.

Lemma 8.4.9. 假設 R 是一個 *unique factorization domain.* 若 $f(x)\in R[x]$ 是 $R[x]$ 的 *irreducible element* 且 $\deg(f(x))\geq 1$, 則 $f(x)$ 是 $R[x]$ 中的 *primitive polynomial.*

Proof. 若 $f(x)$ 是 $R[x]$ 中的 irreducible element, 由於 $f(x)$ 可寫成 $f(x)=c(f)\cdot f^*(x)$ 其中 $c(f)\in R\subseteq R[x]$ 且 $f^*(x)\in R[x]$, 故知 $c(f)$ 是 $f(x)$ 的一個 divisor. 由 $f(x)$ 是 irreducible element 的假設知 $c(f)$ 是 R 中的 unit ($f(x)$ 不可能和 $c(f)$ associates 因 $\deg(f(x))\geq 1$ 但 $\deg(c(f))=0$), 故知 $f(x)$ 是 primitive polynomial. □

若 $f(x),g(x)\in R[x]$, 由於 $R\subseteq F$, $f(x)$ 和 $g(x)$ 可同時看成是 $R[x]$ 的 polynomials 也可以看成是 $F[x]$ 的 polynomials. 因此這兩個 polynomials 間關係看成是 $R[x]$ 或 $F[x]$ 中的情況就會不同. 例如若 $g(x)=f(x)\cdot h(x)$, 其中 $h(x)\in R[x]$ 我們就說 $f(x)\mid g(x)$ in $R[x]$. 然而若 $h(x)\in F[x]$, 我們就說 $f(x)\mid g(x)$ in $F[x]$. 由於 $R[x]\subseteq F[x]$, 很自然的我們知道若 $f(x)\mid g(x)$ in $R[x]$ 則 $f(x)\mid g(x)$ in $F[x]$. 然而一般來說 $f(x)\mid g(x)$ in $F[x]$ 不見得會有 $f(x)\mid g(x)$ in $R[x]$. 不過當 $f(x)$ 是 $R[x]$ 的 primitive polynomial 時, 就對了.

Lemma 8.4.10. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field.* 假設 $f(x),g(x)\in R[x]$ 且 $f(x)$ 是 $R[x]$ 的一個 *primitive polynomial,* 則 $f(x)\mid g(x)$ *in* $F[x]$ 若且唯若 $f(x)\mid g(x)$ *in* $R[x]$.

Proof. 我們只要證明: 若 $f(x)\mid g(x)$ in $F[x]$ 則 $f(x)\mid g(x)$ in $R[x]$. 由假設知存在 $h(x)\in F[x]$ 使得 $g(x)=f(x)\cdot h(x)$. 利用 content, 我們得

$$c(g)\cdot g^*(x)=(c(f)\cdot c(h))\cdot(f^*(x)\cdot h^*(x)).$$

其中 $c(g),c(f)\in R$ 是 $g(x),f(x)$ 的 content, 而 $c(h)\in F$ 是 $h(x)$ 的 content, 且 $g^*(x)$, $f^*(x)$ 以及 $h^*(x)$ 都是 $R[x]$ 的 primitive polynomials. 利用 Lemma 8.4.8 知 $f^*(x)\cdot h^*(x)$ 是 $R[x]$ 的 primitive polynomial. 再利用 Corollary 8.4.7 知存在 $u\in R$ 是 R 的 unit 滿足 $u\cdot c(g)=c(f)\cdot c(h)$. 然而由 $f(x)$ 是 $R[x]$ 的 primitive polynomial, 知 $c(f)$ 是 R 的 unit. 又由假設 $g(x)\in R[x]$ 知 $c(g)\in R$. 故得

$$c(h)=c(f)^{-1}\cdot u\cdot c(g)\in R.$$

然而 $h(x)=c(h)\cdot h^*(x)$, 故由 $c(h)\in R$ 以及 $h^*(x)\in R[x]$ 可得 $h(x)\in R[x]$. 換句話說 $f(x)\mid g(x)$ in $R[x]$. □

利用 Lemma 8.4.10 我們可以得到 $R[x]$ 和 $F[x]$ 中 prime element 的關係.

Corollary 8.4.11. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field* 且假設 $p(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomial.* 若 $p(x)$ 是 $F[x]$ 中的 *prime element* 則 $p(x)$ 是 $R[x]$ 中的 *prime element.*

Proof. 假設 $p(x)$ 是 $F[x]$ 中的 prime element. 要證明 $p(x)$ 是 $R[x]$ 中的 prime element, 我們必須證明若 $p(x) \mid f(x) \cdot g(x)$ in $R[x]$, 其中 $f(x), g(x) \in R[x]$, 則 $p(x) \mid f(x)$ in $R[x]$ 或 $p(x) \mid g(x)$ in $R[x]$. 因 $p(x)$ 是 $R[x]$ 中的 primitive polynomial, 由 Lemma 8.4.10 我們有 $p(x) \mid f(x) \cdot g(x)$ in $F[x]$. 故利用 $p(x)$ 是 $F[x]$ 的 prime element, 我們知 $p(x) \mid f(x)$ in $F[x]$ 或 $p(x) \mid g(x)$ in $F[x]$. 再一次利用 Lemma 8.4.10, 我們知 $p(x) \mid f(x)$ in $R[x]$ 或 $p(x) \mid g(x)$ in $R[x]$, 故得證 $p(x)$ 是 $R[x]$ 的 prime element. □

另外在 $R[x]$ 和 $F[x]$ 中要區分清楚的是一個 $R[x]$ 中的 polynomial 在 $R[x]$ 和 $F[x]$ 中可否分解 (即是否 irreducible) 的關聯性.

Lemma 8.4.12. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field* 且假設 $f(x) \in R[x]$ 及 $\deg(f(x)) \geq 1$. 若存在 $g(x), h(x) \in F[x]$ 滿足 $\deg(g(x)) \geq 1$ 且 $\deg(h(x)) \geq 1$, 使得 $f(x) = g(x) \cdot h(x)$, 則存在 $m(x), n(x) \in R[x]$ 滿足 $\deg(g(x)) = \deg(m(x))$ 且 $\deg(h(x)) = \deg(n(x))$ 使得 $f(x) = m(x) \cdot n(x)$.

Proof. 利用 content 我們將 $f(x) = g(x) \cdot h(x)$ 寫成:

$$c(f) \cdot f^*(x) = (c(g) \cdot c(h)) \cdot (g^*(x) \cdot h^*(x)),$$

其中 $c(f) \in R$, $c(g), c(h) \in F$, 而 $f^*(x), g^*(x)$ 和 $h^*(x)$ 都是 $R[x]$ 的 primitive polynomial. 利用 Lemma 8.4.8 知 $g^*(x) \cdot h^*(x)$ 是 $R[x]$ 的 primitive polynomial, 故由 Lemma 8.4.5 知存在 $u \in R$ 是 R 的 unit 使得 $c(g) \cdot c(h) = c(f) \cdot u$. 換言之, $c(g) \cdot c(h) \in R$. 故若令 $m(x) = (c(g) \cdot c(h)) \cdot g^*(x) \in R[x]$, $n(x) = h^*(x)$, 則 $m(x)$, $n(x)$ 符合定理所要求. □

由 Lemma 8.4.12 我們可得 $R[x]$ 和 $F[x]$ 間 irreducible element 的關係.

Corollary 8.4.13. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field.* 若 $p(x) \in R[x]$ 滿足 $\deg(p(x)) \geq 1$ 是 $R[x]$ 的 *primitive polynomial,* 則 $p(x)$ 是 $R[x]$ 的 *irreducible element* 若且唯若 $p(x)$ 是 $F[x]$ 的 *irreducible element.*

Proof. 首先假設 $p(x)$ 是 $R[x]$ 的 irreducible element, 要證明 $p(x)$ 也是 $F[x]$ 的 irreducible element. 假如 $p(x)$ 在 $F[x]$ 不是 irreducible element, 則存在 $g(x), h(x) \in F[x]$ 滿足 $\deg(g(x)) \geq 1$ 且 $\deg(h(x)) \geq 1$ 使得 $p(x) = g(x) \cdot h(x)$. 故由 Lemma 8.4.12 知存在 $m(x), n(x) \in R[x]$ 滿足 $\deg(m(x)) \geq 1$ 且 $\deg(n(x)) \geq 1$ 使得 $p(x) = m(x) \cdot n(x)$. 換句話說由 $1 \leq \deg(m(x)) < \deg(p(x))$ 知, $m(x)$ 是 $p(x)$ 在

$R[x]$ 的一個 divisor 且既不是 unit 也不和 $p(x)$ associates. 故知 $p(x)$ 不是 $R[x]$ 的 irreducible element. 此和假設矛盾, 故知 $p(x)$ 是 $F[x]$ 的 irreducible element.

反之, 假設 $p(x)$ 是 $F(x)$ 的 irreducible element. 如果 $p(x)$ 在 $R[x]$ 中不是 irreducible, 即存在 $l(x), m(x) \in R[x]$ 滿足 $p(x) = l(x) \cdot m(x)$, 其中 $l(x)$ 和 $m(x)$ 都不是 $R[x]$ 中的 unit. 但 $l(x), m(x) \in R[x] \subseteq F[x]$, 故利用 $p(x)$ 是 $F[x]$ 中的 irreducible element 知 $l(x)$ 和 $m(x)$ 中必有一個是 $F[x]$ 中的 unit (即常數多項式). 就假設是 $l(x) = a \in R$ 吧! 由假設 a 不能是 R 的 unit, 否則 $l(x) = a$ 是 $R[x]$ 的 unit (Lemma 8.4.3). 然而由 $f(x) = l(x) \cdot m(x) = a \cdot m(x)$ 且 $m(x) \in R[x]$ 知 a 是 $f(x)$ 各項係數之 common divisor, 即 $a \mid c(f)$ in R. 但由假設 $f(x)$ 是 primitive polynomial 知 $c(f)$ 是 R 中的 unit, 故由 $a \mid c(f)$ in R 知 a 是 R 的 unit; 此和 a 不是 R 的 unit 相矛盾. 故知 $f(x)$ 在 $R[x]$ 中是 irreducible. □

接著我們來看證明 $R[x]$ 是 unique factorization domain 最關鍵的性質.

Proposition 8.4.14. 假設 R 是一個 *unique factorization domain,* 則 $R[x]$ 中的 *irreducible element* 和 *prime element* 是相同的.

Proof. 由於 $R[x]$ 是 integral domain, 我們知 $R[x]$ 的 prime element 就是 irreducible element (Lemma 8.1.8). 因此只要證明若 $f(x) \in R[x]$ 是一個 irreducible element, 則 $f(x)$ 是一個 prime element. 我們想藉由 $F[x]$ (這裡 F 是 R 的 quotient field) 中的 irreducible element 是 prime element (Proposition 7.2.11) 來證明.

首先考慮 $\deg(f(x)) = 0$ (即 $f(x) = a \in R$ 是常數) 的情形. 因 $a \in R$ 是 irreducible 且 R 是 unique factorization domain, 由 Proposition 8.4.2 知 a 是 R 的 prime element. 我們要證明 a 也是 $R[x]$ 中的 prime element. 假設 $g(x), h(x) \in R[x]$ 滿足 $a \mid g(x) \cdot h(x)$ in $R[x]$, 即存在 $l(x) \in R[x]$ 使得 $a \cdot l(x) = g(x) \cdot h(x)$. 利用 content 得

$$(a \cdot c(l)) \cdot l^*(x) = (c(g) \cdot c(h)) \cdot (g^*(x) \cdot h^*(x)),$$

其中 $c(l), c(g), c(h) \in R$ 且 $l^*(x), g^*(x), h^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomials. 由 Lemma 8.4.8 知 $g^*(x) \cdot h^*(x)$ 依然是 primitive polynomial, 故由 Lemma 8.4.5 知存在 $u \in R$ 是 R 的 unit 滿足

$$u \cdot a \cdot c(l) = c(g) \cdot c(h),$$

換句話說 $a \mid c(g) \cdot c(h)$ in R. 利用 a 是 R 的 prime element 之假設得 $a \mid c(g)$ 或 $a \mid c(h)$. 然而 $g(x) = c(g) \cdot g^*(x)$, 故若 $a \mid c(g)$ 則 $a \mid g(x)$. 同理若 $a \mid c(h)$, 則 $a \mid h(x)$. 故知 $a = f(x)$ 是 $R[x]$ 中的 prime element.

現考慮 $\deg(f(x)) \geq 1$ 的情形. 令 F 是 R 的 quotient field. 因為 $f(x)$ 是 $R[x]$ 的 irreducible element 由 Corollary 8.4.13 知 $f(x)$ 是 $F[x]$ 的 irreducible element. 然而 Proposition 7.2.11 告訴我們此時 $f(x)$ 也是 $F[x]$ 中的 prime element. 由於 Lemma 8.4.9 告訴我們 $f(x)$ 是 $R[x]$ 的 primitive polynomial, 故可套用 Corollary 8.4.11 得證 $f(x)$ 也是 $R[x]$ 中的 prime element. □

現在我們有足夠的性質來幫助我們證明 $R[x]$ 也是一個 unique factorization domain. 大家可以沿用證明 $\mathbb{Z}[x]$ 是 unique factorization domain (Theorem 7.3.13) 的方法來處理. 這裡我們想藉由 $F[x]$ 是 unique factorization domain (Theorem 7.2.14) 這個事實來推導. 這個證明不見的比較簡明, 不過可以幫助我們多了解 $R[x]$ 和 $F[x]$ 間的關聯.

Theorem 8.4.15. 假設 R 是一個 *unique factorization domain,* 則 $R[x]$ 也是一個 *unique factorization domain.*

Proof. 令 F 是 R 的 quotient field.

首先證明存在性: 即任一 $R[x]$ 中非 0 且不是 unit 的元素 $f(x)$ 可寫成有限多個 $R[x]$ 的 irreducible elements 的乘積. 首先將 $f(x)$ 寫成 $f(x) = c(f) \cdot f^*(x)$, 其中 $c(f) \in R$ 且 $f^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomial. 若 $c(f)$ 不是 unit, 則利用 R 是 unique factorization domain 我們可以將 $c(f)$ 寫成有限多個 R 中的 irreducible elements 的乘積. 利用 Lemma 8.4.3 (3) 知道 $c(f)$ 可以寫成有限多個 $R[x]$ 中的 irreducible elements 的乘積. 所以我們只要證明 $f^*(x)$ 可以寫成有限多個 irreducible elements 的乘積. 現將 $f^*(x)$ 看成是 $F[x]$ 中的元素, 則利用 $F[x]$ 是 unique factorization domain, 知道 $f^*(x) = p_1(x) \cdots p_m(x)$, 其中 $p_1(x), \ldots, p_m(x) \in F[x]$ 是 $F[x]$ 中的 irreducible elements. 再利用 content, 知每個 $p_i(x)$ 都可寫成 $p_i(x) = c(p_i) \cdot p_i^*(x)$, 其中 $p_i^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomial. 換句話說

$$f^*(x) = (c(p_1) \cdots c(p_m)) \cdot p_1^*(x) \cdots p_m^*(x).$$

利用 Lemma 8.4.8 知 $p_1^*(x) \cdots p_m^*(x)$ 是 $R[x]$ 的 primitive polynomial, 故由 $f^*(x)$ 是 $R[x]$ 的 primitive polynomial 以及 Lemma 8.4.5 知 $c(p_1) \cdots c(p_m) = u$ 是 R 中的 unit, 由 Lemma 8.4.3 知 u 也是 $R[x]$ 的 unit. 因此我們只要證明 $p_1^*(x), \ldots p_m^*(x)$ 是 $R[x]$ 中的 irreducible elements 就可. 如此一來

$$f^*(x) = (u \cdot p_1^*(x)) \cdot p_2^*(x) \cdots p_m^*(x),$$

所以 $f^*(x)$ 可以寫成有限多個 irreducible elements 的乘積 (注意 $u \cdot p_1^*(x)$ 和 $p_1^*(x)$ associates, 所以也是 $R[x]$ 中的 irreducible element). 然而因 $p_i(x) = c(p_i) \cdot p_i^*(x)$, 由 $p_i(x)$ 在 $F[x]$ 中 irreducible 知 $p_i^*(x)$ 也是 $F[x]$ 的 irreducible element. 由於 $p_i^*(x)$ 是 $R[x]$ 的 primitive polynomial, 套用 Corollary 8.4.13 知 $p_i^*(x)$ 也是 $R[x]$ 的 irreducible element.

接著證明分解的唯一性: 其實我們可以利用 Proposition 8.4.14 直接證明唯一性, 不過這裡我們依然利用 $F[x]$ 和 R 是 unique factorization domain 來證明. 首先假設

$$\begin{aligned} f(x) &= (a_1^{n_1} \cdots a_r^{n_r}) \cdot p_1^{n_{r+1}}(x) \cdots p_v^{n_{r+v}}(x) \\ &= (b_1^{m_1} \cdots b_s^{m_s}) \cdot q_1^{m_{s+1}}(x) \cdots q_w^{m_{s+w}}(x), \end{aligned}$$

其中 $a_1, \dots a_r \in R$ (即 $\deg(a_i) = 0$) 是 $R[x]$ 中兩兩不 associates 的 irreducible elements 而 $p_1(x), \dots, p_v(x) \in R[x]$ 是 $R[x]$ 中兩兩不 associates 且 degree 大於 0 的 irreducible elements, 對於 $b_1, \dots, b_s \in R$ 以及 $q_1(x), \dots, q_w(x) \in R[x]$ 也是同樣的假設. 首先注意由於這些 $p_i(x)$ 和 $q_j(x)$ 都是 $R[x]$ 中的 irreducible elements 且 $\deg(p_i(x)) \geq 1$ 以及 $\deg(q_j(x)) \geq 1$, 由 Lemma 8.4.9 知這些 $p_i(x)$ 和 $q_j(x)$ 都是 primitive polynomial, 故由 Lemma 8.4.8 以及 Lemma 8.4.5 知存在 R 中的 unit u 滿足

$$a_1^{n_1} \cdots a_r^{n_r} = u \cdot b_1^{m_1} \cdots b_s^{m_s},$$

故利用 R 是 unique factorization domain 的性質知經過適當順序掉換我們有 $r = s$, $a_i \sim b_i$ 且 $n_i = m_i, \forall\, i = 1, \dots, r$. 所以最後我們只要考慮

$$\begin{aligned} f_0(x) &= u \cdot p_1^{n_{r+1}}(x) \cdots p_v^{n_{r+v}}(x) \\ &= q_1^{m_{s+1}}(x) \cdots q_w^{m_{s+w}}(x) \end{aligned}$$

這一部分的唯一性. 由於 $f_0(x) \in R[x] \subseteq F[x]$, 且 $p_i(x), q_i(x)$ 是 $R[x]$ 中的 irreducible elements 所以也是 $F[x]$ 中的 irreducible elements (Corollary 8.4.13), 故利用 $F[x]$ 是 unique factorization domain 知經過重排後 $v = w$, $p_i(x) = k_i \cdot q_i(x)$ 且 $n_i = m_i$, $\forall\, i = r+1, \dots r+v$, 其中 $k_i \in F$. 然而 $p_i(x)$ 和 $q_i(x)$ 都是 $R[x]$ 的 primitive polynomial, 故知 k_i 是 R 的 unit. 換言之, 對所有的 $i = r+1, \dots, r+v$, 皆有 $p_i(x) \sim q_i(x)$. 故得證唯一性. □

最後我們來看 Theorem 8.4.15 一個重要的應用. 若 R 是一個 unique factorization domain, 由 Theorem 8.4.15 知 $R' = R[x]$ 也是一個 unique factorization domain. 現考慮 $R'[y]$ 這一個以 y 為變數 R' 的元素為係數的 polynomial ring, 也就是 $R'[y]$ 的元素都是

$$f_n(x)y^n + f_{n-1}(x)y^{n-1} + \cdots + f_1(x)y + f_0(x),$$

其中對所有的 $i = 0, 1, \dots, n$, $f_i(x) \in R' = R[x]$ 是係數在 R 的 x 的多項式. 很容易看出 $R'[y] = R[x][y] = R[x, y]$ 就是以 R 的元素為係數 x, y 為變數的兩個變數的多項式所成的集合, 故再次由 Theorem 8.4.15 知 $R[x, y]$ 是 unique factorization domain. 我們可以將以上的論述推廣到 $R[x_1, \dots, x_n]$ 這個以 R 的元素為係數 $x_1, \dots, x_n$ 為變數的 n 個變數的 polynomial ring:

Theorem 8.4.16. 假設 R 是一個 *unique factorization domain,* 則 $R[x_1, \dots, x_n]$ 這個 n 個變數的 *polynomial ring* 也是一個 *unique factorization domain.*

Proof. 利用數學歸納法, 當 $n = 1$ 時 Theorem 8.4.15 告訴我們 $R[x_1]$ 是一個 integral domain. 假設 $n-1$ 時, $R' = R[x_1, \dots, x_{n-1}]$ 是 unique factorization domain. 再由 Theorem 8.4.15 知 $R'[x_n] = R[x_1, \dots, x_n]$ 也是 unique factorization domain. □

Theorem 8.4.16 是一個代數上很重要的定理, 最常見的狀況是當 F 是一個 field 時因 $F[x_1]$ 是一個 unique factorization domain, 故知 $F[x_1, \ldots, x_n]$ 也是一個 unique factorization domain.