# 大學基礎代數

李華介

國立台灣師範大學數學系

*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 $\phi$ 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 $\phi$ 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 $\phi$ 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 $\phi$ 的 *image.*

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

稱為 $\phi$ 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 $\phi$ 是一個 *monomorphism* (即一對一) 若且為若 $\ker(\phi) = \{0\}$.

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 $\phi$ 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 $\phi$ 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 $\phi$ 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 $\phi$ 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 $\phi$ 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.** $\phi$ 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 $\phi$ 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 $\phi$ 得 $\phi(a) = \overline{a} = y$. 得證 $\phi$ 是 onto.

$\ker(\phi)$ 是甚麼呢? 若 $a \in \ker(\phi)$ 則 $\phi(a) = \overline{0}$, 但由 $\phi$ 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 ideal$S'$), 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 $\phi$ 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 $\psi$ 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 $\phi$ 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 $\psi$ 是一個 well defined function.

接下來證 $\psi$ 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 $\phi$ 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 $\psi$ 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 $\psi$ 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 $\psi$ 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 $\phi$ 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 $\phi$ 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 $\phi$ 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 $\psi$ 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 $\phi$ 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 $\{0, a, -a, 2a, -2a, \dots na, -na, \dots\}$. 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.