大學基礎代數

李華介

國立台灣師範大學數學系

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.