大學基礎代數

李華介

國立台灣師範大學數學系

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.