大學基礎代數

李華介

國立台灣師範大學數學系

前言

在大學數學系的課程中代數學是一門必修的課程, 不過一般同學覺得它既抽象又難以理解. 本講義希望用能比較簡單的方法介紹大學應該知道的代數理論, 讓大家免除對代數的恐懼. 在使用本講義之前請注意下列事項：

(1) 本講義不是甚麼萬靈丹, 若平時不努力考前想隨便讀讀此講義就能融會貫通那是 “不可能的”.

(2) 本講義並不是為了提升同學們對代數的興趣而寫, 因此內容並不會生動有趣. 如果同學對於一些代數的歷史典故有興趣, 建議查詢其他的參考書籍.

(3) 本講義只觸及基礎的代數知識, 因此並不適合對代數有興趣而想多了解更進階理論的同學. 若要學習更多進階的代數理論, 建議查詢其他的參考書籍〔或將來我寫的進階代數講義〕.

(4) 本講義雖然主要以中文撰寫, 不過當涉及定義或專有名詞時, 為免翻譯的困擾將以英文取代. 因此將以中英夾雜較不傳統的方式顯現, 若有不便請見諒.

Contents

Part III. FIELD

Part I

GROUP

Chapter 1

初級 Group 的性質

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

1.1. Group 的基本定義

任意給一集合 S 若要在這集合內的元素之間給一個運算「$*$」怎樣的運算才算是好的運算呢？首先我們很自然的會希望集合中任兩元素運算後仍然在原集合內：也就是說若 $a, b \in S$ 則 $a * b \in S$. 這個性質就是所謂的封閉性 *closed*. 比方說在負整數中的乘法運算就不是 closed, 而在正整數中的乘法運算就是 closed.

好了！既然我們要求運算有封閉性, a 和 b 運算後仍然在 S 我們自然可以再和 S 中的元素再運算. 一般來說我們定義元素間的運算是兩個、兩個來定義的. 如何讓三個元素或更多的元素運算在一起呢？ 換句話說：該如何定 $a*b*c$ 呢？我們可以先讓 a 和 b 運算然後再和 c 運算；即$(a*b)*c$；或是先運算 b 和 c 再和 a 運算：即 $a*(b*c)$. 若這兩種運算的結果得到不同的結果那你將遭遇到天大的麻煩. 因為當你要更多元素運算在一起時你得小心翼翼的注意哪些元素要先運算. 甚至當你要算 $a*a*a$ 時到底要算 $a*(a*a)$ 或 $(a*a)*a$ 都會讓你搞昏頭. 為了省卻這些複雜性我們可以進一步要求：$a*(b*c) = (a*b)*c$. 這樣一來當你要運算 $a*b*c*d$ 時你可以算 $a*(b*(c*d))$, $(a*b)*(c*d)$ 或 $((a*b)*c)*d$ 都沒關係, 你都會得到同樣的結果. $a*(b*c) = (a*b)*c$ 這個性質我們稱之為結合率 *associative law*.

一般來說給定一集合要定義一個符合上面兩個性質的運算 (尤其是結合率) 並不是容易的事. (當然除了一些很簡單的運算, 比方說：定義每個元素運算後都取相同值.) 符合這兩個性質的集合與其運算我們稱之為 *semigroup*. 在本課程中我們將不會討論 semigroup. 畢竟它的條件太少, 很難依此得到有趣的性質. 在一般我們有興趣的代數體系中通常都有一個很特別的元素稱為 *identity*. 這個元素我們通常會用 e 來表示, 它擁有的特殊性質是對集合中任意的元素 a, $a*e$ 和 $e*a$ 的值都還是 a.

有了 e 這一個重要的元素外, 我們進而要求在集合中任意給定一個元素 a, 我們都能在集合中找到一個元素 b 使得 $a*b=b*a=e$. 這個元素我們稱之為 a 的 *inverse*. 要注意的是 e 是一個固定的元素它和任意的元素 a 運算後還是 a, 而這裡的 b 是隨 a 而變的, 不同的 a 會有不同的 b 為其 inverse. 為了強調這一點我們通常用 a^{-1} 來表示 a 的 inverse.

一個集合若有一個運算擁有前面所提的這四個性質我們稱這個集合及其運算為一個 *group*. 我們正式將這個定義寫下：

Definition 1.1.1. 一個集合 G 若元素間有一個運算 $*$ 且符合下列性質則稱為一個 *group*.

(GP1): 若 $a,b\in G$ 則 $a*b\in G$.

(GP2): 若 $a,b,c\in G$ 則 $(a*b)*c=a*(b*c)$.

(GP3): 在 G 中存在一個元素 e 使得 G 中所有元素 g 都有 $g*e=e*g=g$.

(GP4): 對 G 任一元素 g 都可在 G 中找到某一元素 g' 使得 $g*g'=g'*g=e$.

Remark 1.1.2. 要注意我們不能說一個集合是一個 group, 嚴格來說還必須指出在哪種運算下才是 group. 所以我們不能說整數 $\mathbb{Z}$ 是一個 group, 而必須說整數在加法的運算下是個 group. 不過在以後我們談到 group 時因為已經假設有運算在其中所以我們往往會省略地說 G 是一個 group. 而且除非在具體的例子中我們將統一用 「$\cdot$」 來表示運算.

我們簡單的看看哪些熟悉的東西是 group. 前面提到 $\mathbb{Z}$ 在加法的運算下是 group, 其中 0 是其 identity, 而任意的整數 n, $-n$ 是其 inverse. 不過若考慮 $\mathbb{Z}$ 在乘法的運算下它就不再是一個 group. 雖然 1 是乘法的 identity 不過並不是所有的整數都有乘法的 inverse, 例如 2 就沒法在 $\mathbb{Z}$ 中找到一個數使得 2 乘以它以後會是 1. 當然了你很快的會反應說：有理數 $\mathbb{Q}$ 在乘法下是一個 group. 可惜不是, 因為 $0\in\mathbb{Q}$ 不過 0 沒有乘法 inverse. 但如果我們考慮非 0 的有理數所成的集合, 則在乘法的運算下它就是一個 group. 要說明這件事很簡單但別忘了我們不只要說明所有非 0 的有理數有乘法反元素, 我們還要注意其他的性質. 在這裡 (GP1) 中 closed 的性質還是被保持著, 因為兩個非 0 的有理數相乘還是一個不等於 0 的有理數.

要特別注意的是, 一些我們熟悉的例子往往都有 $a\cdot b=b\cdot a$ 的性質, 不過在 group 的定義中並沒有這項要求. 以後我們將會看到很多不符合這性質的 group. 不過若一個 group 有上述這個性質我們就多給它一個名字稱之為 *abelian group*；而不符合這性質的 group 就稱為 *nonabelian group*.

Definition 1.1.3. 若 G 是一個 group 且對任意的 $a,b\in G$ 我們都有 $a\cdot b=b\cdot a$, 則稱 G 為一個 *abelian group*.

Group 的定義也沒有對元素的個數有所要求. 事實上有很多重要的 group 它只有有限多個元素. 我們也對這類的 group 給特殊的名字.

Definition 1.1.4. 若 G 是一個 group 且只有有限多個元素, 則我們稱 G 為一個 *finite group*；若 G 中元素的個數為 n, 則我們稱 G 是一個 *order* n 的 group. 通常用 $|G| = n$ 來表示.

事實上在大學的基礎代數中我們只討論 finite group.

1.2. 由 Group 的定義所得的性質

在 Group 的定義中既然我們對其有些特殊的要求, 當然很自然的想看看能否因為這些要求推得一些性質. 簡單的來說我們檢驗一個集合是否為一個 group 只需檢查其是否符合 (GP1) 到 (GP4) 這四項要求, 然而會不會因為符合了這四項要求而讓 group 有其他更多更有用的共通性質呢？答案是有的. 事實上這四項要求就讓 group 有很豐富的結構性質. 將來我們會更進一步的討論這些衍生出來的重要性質. 在這一節我們只討論幾項直接用定義得到的基本性質.

首先我們注意到在 group 的定義中 (GP3) 的性質提到存在一個 identity, 而我們也提到用 e 來表示它. 有警覺性的同學馬上會注意到 something is wrong. 甚麼問題呢？我們並不知道 identity 是否唯一怎們可以這麼快就給它一個代號. 還好, 雖然在 (GP3) 並沒有提及唯一性, 不過以下我們可以發現它的唯一性會自動成立.

在數學中證明一個東西的存在性及唯一性是非常重要的課題, 將來大家會不時的碰到這一類的問題. 一般的同學在碰到存在唯一的證明時往往分不清楚哪個是證明存在哪個是證明唯一, 所以我們將很小心的談論這類的問題.

(GP3)的性質很明顯的就是所謂的存在性. 怎樣用它來得到唯一性呢？一般的直覺證明唯一就是說找不到另外一個元素符合這個性質, 但這是很難直接證明的. 所以幾乎在證明唯一性時我們都用反證法, 也就是說假設找到兩個相異的東西有這個性質我們要證明這是矛盾的. 矛盾這個辭的由來相信大家都知道：有個人在賣矛和盾. 他一下子說他的矛無堅不催可以刺穿所有的盾牌；一下子又說他的盾堅固無比沒有矛可以刺穿它. 所以有人就問說那你的矛刺你的盾後會怎樣呢？我們就用這以子之矛攻子之盾的方法來證明矛盾. 也就是如果 e 和 e' 是 G 中兩個相異的元素且都符合 identity 的性質, 那麼 $e \cdot e'$ 會是什麼呢？

Proposition 1.2.1. 若 G 是一個 *group,* 則 G 中只有唯一的元素會符合 *identity* 的性質.

Proof. 假設 e 和 e' 是 G 中兩個相異的元素且都符合 identity 的性質, 則考慮 $e \cdot e'$. 因為 e 是 identity 所以 $e \cdot e' = e'$. 另一方面由於 e' 也是 identity 所以 $e \cdot e' = e$. 因此我們得 $e = e'$, 此和原假設 $e \neq e'$ 矛盾, 故 G 中僅有一個元素會是 identity. □

注意在以上的証明中 e 是乘在左邊而 e' 是在右邊, 也就是說在 (GP3) 中 identity 的性質若只要求對所有的 $a \in G$ 要符合 $e \cdot a = a$ (或只要求 $a \cdot e = a$) 則 identity 的唯一性並不一定會對. 所以要謹記 identity 必須要符合 $e \cdot a = a$ 且 $a \cdot e = a$.

我們很自然會問：那給定 G 中的任一元素 a, 其 inverse 是否也唯一呢？用類似的方法, 我們有以下之結果：

Proposition 1.2.2. *若 G 是一個 group, 則給定 G 中任一元素 a, 在 G 中只有唯一的元素 b 會符合 $a \cdot b = b \cdot a = e$.*

Proof. 假設 G 中有兩相異元素 b 和 b' 符合 a 的 inverse 之條件. 也就是 $a \cdot b = b \cdot a = e$ 且 $a \cdot b' = b' \cdot a = e$. 則

$$b = b \cdot e = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'$$

此與 $b \neq b'$ 矛盾, 故得証. □

注意以上之證明我們用到 (GP2) 及 (GP3), 另外 inverse 必須是乘在兩邊都會成 identity. 如果我們對 inverse 的條件只要求 $a \cdot b = e$ (或只要求 $b \cdot a = e$) 那麼 inverse 的唯一性定不一定會成立. 所以要謹記若 b 為 a 之 inverse, 則必須符合 $a \cdot b = e$ 且 $b \cdot a = e$.

在此再次強調由於 Proposition 1.2.2, 給定一元素 a 我們將記 a^{-1} 為其 inverse.

事實上 group 有比以上兩個 Propositions 更強的性質：

Theorem 1.2.3. *若 G 是一個 group, 給定 G 中任意元素 a 和 b, 則方程式 $a \cdot x = b$ 在 G 中有解且其解唯一. 同理, 方程式 $y \cdot a = b$ 在 G 中也有唯一解.*

Proof. 這就是一個證明存在及唯一的典型例子.

要證明存在性, 我們只要在 G 中真的找到一個元素 c 使得 $a \cdot c = b$. 很容易就知道若令 $c = a^{-1} \cdot b$, 則由於 $a^{-1} \in G$ 且 $b \in G$, 由 (GP1) 我們知 $c \in G$. 然而,

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

故知 c 是 $a \cdot x = b$ 在 G 中的一個解.

好了, 我們找到一個解了如何證明唯一呢？一個同學經常犯的錯誤是說：因為 a^{-1} 是唯一的所以解 $a^{-1} \cdot b$ 是唯一的. 這裡出錯的原因是：要證明唯一性就是要你說明為何此解一定是 $a^{-1} \cdot b$. 上述的證法並沒有真正回答這個問題. 前面提過要直接證明唯一性是頗困難的, 我們還是用反證法比較好.

假設 c 和 c' 是 G 中方程式 $a \cdot x = b$ 的兩個相異的解, 則由 $a \cdot c = a \cdot c'$ 我們可得 $a^{-1} \cdot (a \cdot c) = a^{-1} \cdot (a \cdot c')$. 由於 $a^{-1} \cdot (a \cdot c) = (a^{-1} \cdot a) \cdot c = c$ 及 $a^{-1} \cdot (a \cdot c') = (a^{-1} \cdot a) \cdot c' = c'$ 我們得 $c = c'$. 此與 $c \neq c'$ 矛盾, 故得証. □

Remark 1.2.4. 前面提過, 若我們不知道 G 是否是一個 group 時若要說 G 中的某一元素 a 是 G 的 identity, 我們必需驗證對所有的 $g \in G$ 皆有 $g \cdot a = a \cdot g = g$. 不過若已知 G 是一個 group, 那麼 Theorem 1.2.3 告訴我們說: 如果要說明 a 是 G 的 identity, 我們只要在 G 中找到一個元素 b 使得 $a \cdot b = b$ (或 $b \cdot a = b$) 就好. 不必驗證 G 中所有的元素 g 都要滿足 $g \cdot a = a \cdot g = g$.

利用 Theorem 1.2.3 我們很快的有以下的很基本但也很重要的等式：

Corollary 1.2.5. 若 G 是一個 *group*, 給定 G 中任意元素 a 和 b, 則

$$(a^{-1})^{-1} = a \quad \text{and} \quad (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$$

Proof. 由於 $(a^{-1})^{-1}$ 須符合 $a^{-1} \cdot x = e$, 然而已知 $x = a$ 符合此方程式, 故由 Theorem 1.2.3 的唯一性知 $(a^{-1})^{-1} = a$.

同理 $(a \cdot b)^{-1}$ 須符合 $(a \cdot b) \cdot x = e$, 然而已知 $x = b^{-1} \cdot a^{-1}$ 符合此方程式, 故由 Theorem 1.2.3 的唯一性知 $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. □

1.3. Subgroup

上一節提到 group 的基本性質幾乎是由定義直接推得, 我們若想得到更豐富的性質, 則不得不引進特殊的技巧來處理. 當然一開始最直接的想法就是如果一個 group 不是很容易被掌握, 我們是不是可以考慮其內部的子集合來幫助我們了解它. 當然了我們知道一般的子集合幫不了我們什麼忙, 因為 group 本身的運算才是我們關注的重點. 所以我們有興趣的是那些在原本 group 的運算下也是 group 的子集合. 這樣的子集合我們稱之為 *subgroup*. 以後我們將會學到如何利用 subgroup 來進一步了解原先的 group. 在本節中我們先了解一些 subgroup 的特性.

首先我們還是給 subgroup 一個正式的定義.

Definition 1.3.1. 給定一個 group G, 如果 G 中的一個非空的子集 H 在 G 的運算之下也是一個 group, 則稱 H 為 G 的一個 *subgroup*.

要注意的是, 我們強調要在 G 原本的運算下才可以. 例如在整數的加法運算下所有的偶數所成的子集合就是其 subgroup；然而集合 $\{1, -1\}$ 雖然是整數的一個子集合而且在乘法的運算下是一個 group, 不過它卻不是整數這個 group 的一個 subgroup.

給定一個 group G, 我們很容易找到兩個 subgroup: 一個就是 G 本身, 另一個就是僅由 identity 一個元素所成的子集合. 這兩個 subgroup 對我們來說沒有什麼用處, 所以稱之為 *trivial subgroups*, 其他的 subgroup 則稱之為 *nontrivial proper subgroups*. 要注意的是將來我們會看到有些 group 並沒有 nontrivial proper subgroups.

介紹完基本定義, 我們自然想知道如何判定一個 group 之子集合 H 是否為 G 的 subgroup？ 當然就是前面 group 的定義 (GP1) 到 (GP4) 都要符合. 首先注意在 subgroup 的定義中並沒有要求 H 的 identity 就是 G 的 identity. 不過若給定 H 中一元素 a, H 的 identity 必須符合 $a \cdot x = x \cdot a = a$. 由 Theorem 1.2.3, 知道在 G 中只有唯一的元素符合 $a \cdot x = a$ (或 $x \cdot a = a$), 而 G 中的 identity 又符合這等式, 所以 H 的 identity 非得是 G 中的 identity. 同理在 (GP4) 中要求對任意 H 中之元素 a 都可以在 H 中找到 a 的 inverse. 再由 Theorem 1.2.3 我們可得 a 在 H

中的 inverse 恰就是 a 在 G 中的 inverse. 由這些觀察我們用比較數學的方法再重寫 subgroup 的定義.

Definition 1.3.2. 給定一個 group G, 如果 G 中的一個非空的子集 H 在 G 的運算之下符合：

(SGP1): 若 $a, b \in H$ 則 $a \cdot b \in H$.

(SGP2): 若 $a, b, c \in H$ 則 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(SGP3): G 的 identity e 必須屬於 H.

(SGP4): 對 H 中任一元素 h 其在 G 中的 inverse h^{-1} 必須也屬於 H.

則稱 H 為 G 的一個 subgroup.

其實要檢查 H 是否為 G 之 subgroup 我們不必全部檢查 (SGP1) 到 (SGP4) 這四項. 事實上 G 中的元素都符合 (GP2), 而 H 中的元素必定在 G, 所以 H 中的元素自然符合 (SGP2). 另外 (SGP3) 也是可以省略的. 這是因為既然 H 是非空的, 我們可以在 H 中任找一元素 a. 而 (SGP4) 告訴我們若 $a \in H$ 則 $a^{-1} \in H$ 又 (SGP1) 告訴我們若 $a \in H$ 且 $a^{-1} \in H$ 則 $e = a \cdot a^{-1} \in H$, 故 (SGP3) 可由 (SGP1) 及 (SGP4) 推得. 總結以上討論, 我們有：

Lemma 1.3.3. 給定一個 *group* G, H 為 G 中的一個非空的子集. 則 H 是 G 的 *subgroup* 若且為若 H 在 G 的運算之下符合以下兩點：

(1) 若 $a, b \in H$ 則 $a \cdot b \in H$.

(2) 若 $a \in H$ 則 $a^{-1} \in H$.

有許多書將以上驗證 subgroup 的方法用更簡明的方式表示. 在實際狀況下它並沒有比較好用; 只是大部分的同學都覺得它比較好記憶所以我們還是介紹一下吧!

Lemma 1.3.4. 給定一個 *group* G, 且 H 為 G 中的一個非空的子集. 則 H 是 G 的 *subgroup* 若且為若在 G 的運算之下給定任意的 $a, b \in H$, 皆有 $a \cdot b^{-1} \in H$.

Proof. (先證明 trivial 的一邊) $\Rightarrow$: 若 H 是 G 的 subgroup, 則給定任意的 $a, b \in H$, 因 $b \in H$, 由 (SGP4) 我們可得 $b^{-1} \in H$. 又因 $a \in H$ 及 $b^{-1} \in H$, 再由 (SGP1) 我們可得 $a \cdot b^{-1} \in H$. 故得證.

(再證明較難的一邊) $\Leftarrow$: 我們主要的策略是找到 H 中特殊的 a 和 b 來證明 H 符合 (SGP1) 到 (SGP4) 這四個性質. 雖然 Lemma 1.3.3 告訴我們只要驗證 (SGP1) 及 (SGP4) 就可, 不過由於技術性上的困難我們得先證明 (SGP3) 再利用它來證明 (SGP4) 及 (SGP1). 也就是說我們先證明 $e \in H$: 這其實不難, 因為已知 H 是非空的故任取 $a \in H$, 知因 $a \in H$ 故當 $b = a$ 時, $b \in H$. 故由假設知

$$e = a \cdot a^{-1} = a \cdot b^{-1} \in H.$$

現在既然知道 $e \in H$, 則對任意的 $b \in H$ 我們可令 $a = e \in H$, 再由假設的條件 $a \cdot b^{-1} \in H$ 可得

$$a \cdot b^{-1} = e \cdot b^{-1} = b^{-1} \in H.$$

這證明了 (GP4). 接下來給定任意的 $c, d \in H$, 由前已知 $d^{-1} \in H$. 故可令 $a = c$ 和 $b = d^{-1}$, 我們有 $a, b \in H$. 所以由假設知 $a \cdot b^{-1} \in H$. 也就是說 $a \cdot b^{-1} = c \cdot (d^{-1})^{-1} = c \cdot d \in H$. 這證明了 (SGP1), 故知 H 是 G 的一個 subgroup. □

注意: 如果 H 中的元素符合若 $a, b \in H$ 則 $a^{-1} \cdot b \in H$, 那麼我們也可用同樣的方法證明 H 是 G 的一個 subgroup.

前面提過以後我們將會專注於 finite group 的 case. 當我們碰到 finite group 時要檢查其中的子集合是否為 subgroup 時所要檢查的項目就更少了. 事實上我們有以下的定理:

Proposition 1.3.5. 給定一個 *"finite" group* G, 且 H 為 G 中的一個非空的子集. 則 H 是 G 的 *subgroup* 若且為若在 G 的運算之下 H 是 *closed.*

Proof. 我們僅要證明當 H 在 G 的運算下是 closed 則 H 是 G 的 subgroup. 然而利用 Lemma 1.3.3, 因為已知 H 在 G 的運算下是 closed, 所以要證明H 是 G 的 subgroup 我們只要證明給定任何的 $a \in H$ 皆有 $a^{-1} \in H$ 就可. 若 $a \in H$, 因 H 在 G 的運算下是 closed, 故 $a^2 = a \cdot a \in H$, $a^3 = a \cdot a^2 \in H$, ... 這樣一直下去我們可得對任一的 $n \in \mathbb{N}$, 皆有 $a^n \in H$. 然而 G 只有有限多個元素, 而 H 是 G 的一個子集合, 所以 H 必只有有限多個元素. 換句話說 $\{a, a^2, a^3, \dots a^n, \dots\}$ 這些 H 的元素一定不可能兩兩相異. 所以可以找到兩個相異的整數 m 和 n 使得 $a^n = a^m$. 不失一般性, 我們假設 $m > n$. 等式兩邊同乘 $(a^n)^{-1}$, 我們得 $a^{m-n} = e$. 如果 $m - n = 1$, 這表示 $a = e$, 所以 $a^{-1} = e = a \in H$. 如果 $m - n > 1$, 則 $m - n - 1 \in \mathbb{N}$. 故知 $a^{m-n-1} \in H$. 再由 $a^{m-n} = e$ 知 $a^{m-n-1} \cdot a = a \cdot a^{m-n-1} = e$. 故得 $a^{-1} = a^{m-n-1} \in H$. □

1.4. 一些特殊的 subgroup

前面提及我們希望利用一個 group 的 subgroup 來幫我們了解這一個 group. 給定一個 group 除了 trivial subgroup 外到底要怎樣找到其他的 subgroup 呢?當然了有些 group 是沒有 nontrivial proper subgroup 的(以後我們會介紹), 在這一節我們希望介紹一些可能找到 nontrivial proper subgroup 的方法.

當 G 是一個 group 給定 $a \in G$, 我們希望用 a 來產生一個 subgroup. 很自然的我們知道 $a^2, a^3, \dots, a^n, \dots$ 都要在這個 subgroup 中, 還有 $a^{-1}, (a^2)^{-1}, \dots, (a^n)^{-1}, \dots$ 也要在其中, 最後別忘了 e 也要在裡面. 由 Corollary 1.2.5, 我們知 $(a^n)^{-1} = (a^{-1})^n$, 所以我們很自然的會定義以下的集合:

$$\langle a \rangle := \{a^n \mid n \in \mathbb{N}\} \cup \{(a^{-1})^m \mid m \in \mathbb{N}\} \cup \{e\}.$$

很容易由 Lemma 1.3.3 (或 Lemma 1.3.4) 知道 $\langle a\rangle$ 會是 G 的一個 subgroup. 我們稱 $\langle a\rangle$ 為 the *cyclic subgroup* of G generated by a. 當然了, 如果我們選到 $a = e$ 則 $\langle a\rangle = \{e\}$ 這一個 trivial subgroup. 另一方面如果我們可以找到一個 a 使得 $\langle a\rangle = G$, 那麼我們就稱 G 為一個 *cyclic group*. 要注意的是並不是所有的 group G 都可以找到 $a \in G$ 使得 $\langle a\rangle = G$.

Example 1.4.1. 我們給一個有些同學會搞混的例子. 會搞混的原因是前面提過, 為了簡便的因素我們都用 「$\cdot$」 來表示 group 的運算, 所以 $a^2 = a\cdot a$ 表示 a 和 a 運算兩次, a^3 表示運算三次... 依此類推. 現在我們考慮 $\mathbb{Z}$ 以加法形成的 group. 那麼 $\langle 2\rangle$ 應該是怎樣的 subgroup 呢? 它應該是由 $2, 4 = 2+2, 6 = 2+2+2$, ...(千萬別搞錯, 不是由 $2, 4 = 2^2, 8 = 2^3$,...) 以及 $-2, -4, -6$, ... 等所組成. 換句話說在此 group 中以 2 所形成的 cyclic subgroup 即是由所有偶數所組成的. 另外大家很容易看出來 -2 也可產生同樣的 subgroup. 大家也可很容易看出 1 所產生的 cyclic subgroup 就是 $\mathbb{Z}$ 本身所以我們知道 $\mathbb{Z}$ 所形成的加法群是一個 cyclic group.

大家應該都還記得, 在一般的 group 中, $a\cdot b$ 不見得等於 $b\cdot a$. 不過因 $a\cdot e = e\cdot a = a$ 所以 identity 總是和所有元素可交換的. 至於給定一元素, 有哪些元素可以和它交換是一個很有趣的話題. 給定 $a \in G$, 我們可以考慮

$$C(a) = \{g \in G \,|\, g\cdot a = a\cdot g\}.$$

這個集合就是搜集 G 中可以和 a 交換的元素. 我們稱之為 the *centralizer* of a. 給定任意的 $a \in G$, 事實上 $C(a)$ 會是 G 的一個 subgroup. 例如 the centralizer of identity $C(e)$ 就是 G 本身.

Proposition 1.4.2. *若 G 是一個 group 且 $a \in G$, 則 $C(a)$ 是 G 的一個 subgroup.*

Proof. 由 Lemma 1.3.3, 我們要證明: 若 $g_1, g_2 \in C(a)$ 則 $g_1\cdot g_2 \in C(a)$ 還有 $g_1^{-1} \in C(a)$. 事實上 $g_1, g_2 \in C(a)$ 告訴我們 $g_1\cdot a = a\cdot g_1$ 及 $g_2\cdot a = a\cdot g_2$. 因此

$$(g_1\cdot g_2)\cdot a = g_1\cdot(g_2\cdot a) = g_1\cdot(a\cdot g_2) = (g_1\cdot a)\cdot g_2 = (a\cdot g_1)\cdot g_2 = a\cdot(g_1\cdot g_2).$$

也就是說 $g_1\cdot g_2 \in C(a)$. 另一方面, 由於 $g_1\cdot a = a\cdot g_1$, 各乘上 g_1^{-1} 在兩邊等式的右邊. 我們得到 $(g_1\cdot a)\cdot g_1^{-1} = a$. 再乘以 g_1^{-1} 於兩邊等式之左邊. 我們得 $a\cdot g_1^{-1} = g_1^{-1}\cdot a$. 也就是說 $g_1^{-1} \in C(a)$. □

另外一種常見的 subgroup 是考慮

$$Z(G) = \{g \in G \,|\, g\cdot x = x\cdot g, \forall\, x \in G\}.$$

我們一般稱 $Z(G)$ 為 G 的 *center*. 注意 $C(a)$ 是和 G 中的特定元素 a 可交換的元素所成的集合, 而 $Z(G)$ 是和 G 中所有的元素可交換的元素所成的集合. 所以我們很容易可證得

$$Z(G) = \bigcap_{a\in G} C(a).$$

類似於證明 $C(a)$ 是 G 的 subgroup 的方法我們也可以證明 $Z(G)$ 也是 G 的 subgroup. 在這裡我們不再給證明不過等一下我們將會用另一種看法來說明 $Z(G)$ 是 G 的 subgroup.

1.5. 製造更多的 subgroups

前一節中我們介紹了幾種 subgroup. 如果你已有了一些 subgroups 這一節中我們將介紹一些簡單的利用這些 subgroups 製造出新的 subgroup 的方法.

Lemma 1.5.1. *若 H_1, H_2 是 G 的 subgroups, 則 $H_1 \cap H_2$ 也是 G 的 subgroup.*

Proof. 我們先證明封閉性. 若 $x, y \in H_1 \cap H_2$, 則利用 $x, y \in H_1$ 及 H_1 是一個 subgroup, 我們有 $x \cdot y \in H_1$. 同理可得 $x \cdot y \in H_2$. 故 $x \cdot y \in H_1 \cap H_2$.

另外證明 inverse 存在. 若 $x \in H_1 \cap H_2$, 則利用 $x \in H_1$ 及 H_1 是一個 subgroup, 我們有 $x^{-1} \in H_1$. 同理可得 $x^{-1} \in H_2$. 故 $x^{-1} \in H_1 \cap H_2$. □

注意從證明中不難發現若將此 Lemma 1.5.1 中的交集改成聯集則結果不一定成立. 即 $H_1 \cup H_2$ 不一定會是 subgroup. 例如在整數 $\mathbb{Z}$ 所成的加法群中, $2\mathbb{Z}$ 和 $3\mathbb{Z}$ 這兩個 subgroups 的聯集不是 subgroup. 很容易就知 $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ 且 $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ 但是 $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

從 Lemma 1.5.1 的證明也不難看出不只兩個 subgroups 的交集是 subgroup, 其實任意有限多個 subgroups 的交集也是 subgroup. 甚至無窮多個 subgroups 的交集也是 subgroup. 所以我們可利用 $C(a)$ 是 subgroup 得到 $Z(G) = \cap_{a \in G} C(a)$ 也是一個 subgroup.

給定 G 中的任一元素 a 及一個 subgroup H, 我們可以考慮

$$a^{-1} \cdot H \cdot a = \{a^{-1} \cdot h \cdot a \,|\, h \in H\}$$

這個集合 (當然了若 G 是 abelian 則 $H = a^{-1} \cdot H \cdot a$).

Lemma 1.5.2. *若 $a \in G$ 且 H 是 G 的一個 subgroup, 則 $a^{-1} \cdot H \cdot a$ 也是 G 的 subgroup. 若又知 H 是 finite group, 則 $|H| = |a^{-1} \cdot H \cdot a|$.*

Proof. 若 $x_1, x_2 \in a^{-1} \cdot H \cdot a$, 表示存在 $h_1, h_2 \in H$ 使得 $x_1 = a^{-1} \cdot h_1 \cdot a$ 且 $x_2 = a^{-1} \cdot h_2 \cdot a$. 故由結合率知

$$x_1 \cdot x_2 = (a^{-1} \cdot h_1 \cdot a) \cdot (a^{-1} \cdot h_2 \cdot a) = a^{-1} \cdot (h_1 \cdot h_2) \cdot a.$$

又 $h_1 \cdot h_2 \in H$, 故 $x_1 \cdot x_2 \in a^{-1}Ha$. 這證明了封閉性.

又若 $x \in a^{-1} \cdot H \cdot a$, 則存在 $h \in H$ 使得 $x = a^{-1} \cdot h \cdot a$. 故

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

再由 $h^{-1} \in H$ 故得 $x^{-1} \in a^{-1} \cdot H \cdot a$.

最後若 H 是 G 的一個 finite subgroup, 我們要證明 $|H| = |a^{-1} \cdot H \cdot a|$. 一般來說要證明兩個集合的元素個數是相同的, 我們只要在這兩個集合間找到一個 1-1 且 onto 的函數就可. 固定 $a \in G$, 我們考慮 f 是從 H 到 $a^{-1} \cdot H \cdot a$ 的函數, 定義為: 對於所有 $h \in H$, $f(h) = a^{-1} \cdot h \cdot a$. 由定義知 $f(h) \in a^{-1} \cdot H \cdot a$. 我們現在檢查 f 是 1-1, 也就是若 $h \neq h'$ 則要證明 $f(h) \neq f(h')$. (一般來說我們不容易直接證明不等, 所以都會用反證法.) 如果 $f(h) = f(h')$, 即 $a^{-1} \cdot h \cdot a = a^{-1} \cdot h' \cdot a$, 馬上知 $h = h'$. 這和 $h \neq h'$ 的假設矛盾, 故知 $f(h) \neq f(h')$. 最後證明 f 是 onto, 也就是任取 $a^{-1} \cdot H \cdot a$ 中的元素 y, 我們要在 H 中找到一個 x 使得 $f(x) = y$. 不過由定義, $y \in a^{-1} \cdot H \cdot a$ 表示存在 $h \in H$ 使得 $y = a^{-1} \cdot h \cdot a$, 故取 $x = h$, 則得 $f(x) = y$. 我們證得了 $|H| = |a^{-1} \cdot H \cdot a|$. □

Chapter 2

中級 Group 的性質

這一章中我們將介紹一些更進一步的 group 的理論, 包括 Lagrange's Theorem, Cauchy's Theorem for abelian groups 以及三個 isomorphism theorems.

2.1. 分類

一般來說要將一個集合分類必須符合以下三個要素. 第一個就是, 自己和自己是同類的; 另一要素是若甲和乙是同類的則乙也必須和甲是同類的; 最後一個要素是如果甲和乙同類且乙和丙同類, 則甲必須和丙同類. 很多同學應該知道這樣的分類同類間的關係稱之為 *equivalence relation*. 我們還是用數學的方法給 equivalence relation 正式的定義.

Definition 2.1.1. 若一集合 S 中我們用 $a \sim b$ 表示 a 和 b 是同類的, 則這樣的分類若符合以下性質我們稱之為 equivalence relation:

(equiv1): 對所有 $a \in S$, 我們都有 $a \sim a$ (reflexivity).

(equiv2): 若 $a \sim b$, 則 $b \sim a$ (symmetry).

(equiv3): 若 $a \sim b$ 且 $b \sim c$, 則 $a \sim c$ (transitivity).

有些同學可能會覺得奇怪既然 (equiv2) 說: 若 $a \sim b$ 則 $b \sim a$. 那麼再利用 (equiv3) 我們可得 $a \sim a$. 為什麼還要強調 (equiv1) 呢? 主要原因是 (equiv1) 強調是 S 中的任一元素 a 都須符合 $a \sim a$. 如果我們只要求 (equiv2) 和 (equiv3), 那麼如果 S 中有一元素 a 在 S 中找不到任何的元素 b 使得 $a \sim b$, 那麼 a 就不一定滿足 $a \sim a$ 了. 因此會造成有的元素有可能沒有被分類到. 而符合 equivalence relation 的分類就確保每一個元素都會被分到某一類 (不過有可能某一類中只有一個元素).

到底用 equivalence relation 分類有什麼好處呢? 首先當然是如前所說由 (equiv1) 可得每一個元素都會被分到某一類. 另外由 (equiv2) 和 (equiv3) 知兩個不同類的集合不會有交集; 這是因為如果 b 在 A 類且在 B 類中, 則在 A 類中的任一元素 a 因和 b 是同類的故 $a \sim b$ 而 B 類中的任一元素 c 因也和 b 同類故 $b \sim c$. 故由

(equiv2) 和 (equiv3) 知 $a \sim c$. 也就是說 A 中的所有元素和 B 中的所有元素都同類. 這和 A 與 B 是不同類的假設相矛盾。

這樣的分類到底有什麼好處呢? 它可以幫我們計算一個有限集合的個數. 事實上我們有以下的 Lemma.

Lemma 2.1.2. 假設 S 是一個有限集合, 且用一個 *equivalence relation* 將其分成 $C_1, \ldots, C_n$ 等不同的類別. 若 $|S|$ 及 $|C_i|$ 表示這些集合的元素的個數, 則

$$|S| = \sum_{i=1}^{n} |C_i|.$$

Proof. 由前面說明已知利用 (equiv2) 和 (equiv3) 可得: 當 $i \neq j$ 時, $C_i \cap C_j = \emptyset$. 也就是說這些 C_i 是兩兩不相交的. 再加上由 (equiv1) 知每個 S 中的元素都會落在某個 C_i 中, 所以 S 的元素的個數剛好是這些 $C_1, \ldots, C_n$ 的元素個數之和. □

這個 Lemma 2.1.2 和 group 會有什麼關係呢? 若 H 是 group G 的一個 subgroup, 我們可以利用 H 對 G 中的元素定義一種分類的方法. 當然我們希望這種分類法是一個 equivalence relation, 因此可以用 Lemma 2.1.2 來算出 G 的個數.

怎樣利用 H 來定一個 equivalence relation 呢? 我們定 $a \sim b$ 如果 $a^{-1} \cdot b \in H$. 也就是說如果 $a^{-1} \cdot b \in H$, 則我們就說 a 和 b 是同類的. 這樣的分類會符合 equivalence relation 的三要素嗎? 我們一個一個來檢查:

首先, 給訂任一 G 中的元素 a, 由於 $a^{-1} \cdot a = e$, 且 H 是 subgroup 所以 $e \in H$. 因此 $a^{-1} \cdot a \in H$. 也就是說 $a \sim a$. 這證明了 (equiv1).

再來, 如果 $a \sim b$, 也就是說 $a^{-1} \cdot b \in H$. 則因 H 是 subgroup, 由 $a^{-1} \cdot b \in H$ 可得

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

也就是說 $b \sim a$. 這證明了 (equiv2).

最後, 若 $a \sim b$ 且 $b \sim c$, 則 $a^{-1} \cdot b \in H$ 且 $b^{-1} \cdot c \in H$. 再由 subgroup 的封閉性 (SGP1), 我們可得

$$(a^{-1} \cdot b) \cdot (b^{-1} \cdot c) = a^{-1} \cdot c \in H.$$

換句話說 $a \sim c$, 所以我們證了 (equiv3).

既然這個分類法是一個 equivalence relation. 由 Lemma 2.1.2, 如果 G 是一個 finite group, 我們只要想辦法算出這種分類法之下每一類的個數, 就可以算出 G 的個數.

2.2. Lagrange's Theorem

Lagrange 的定理告訴我們一個 finite group 和它的 subgroup 之間各數的關係. 我們想利用上一節的結果來計算, 所以必須要知道若用上節提到的分類法, 那麼每一類的元素個數有多少.

Lemma 2.2.1. 如果 G 是一個 *group,* H 是其 *subgroup.* 若利用 $a^{-1}\cdot b\in H$ 則 a 和 b 同類 $(a\sim b)$ 的方法來將 G 分類, 則和 a 同類的元素所成的集合為

$$a\cdot H=\{a\cdot h\,|\,h\in H\}.$$

倘若 H 是一個 *finite subgroup,* 則和 a 同類的元素的個數和 H 的元素個數一樣多.

Proof. 若 a 和 b 同類, 則表示 $a\sim b$. 故 $a^{-1}\cdot b=h$ 且 $h\in H$. 所以 $b=a\cdot h\in a\cdot H$. 反之, 若 $b\in a\cdot H$, 則表示在 H 中可找到一元素 h 使得 $b=a\cdot h$. 故 $a^{-1}\cdot b=h\in H$. 也就是說 a 和 b 同類.

前面提過要證明兩個集合有相同的元素個數最好的方法就是在兩集合中找到 1-1 且 onto 的函數. 因為和 a 同類的元素所成的集合是 $a\cdot H$, 所以我們只要找到一個函數從 H 送到 $a\cdot H$ 且證明這個函數是 1-1 且 onto 就可. 給定任一 $h\in H$, 我們可以定義 $f(h)=a\cdot h$. 這樣一來 $f:H\to a\cdot H$ 就是一個從 H 到 $a\cdot H$ 的函數. 給定任一 $y\in a\cdot H$, 由定義知必可找到一 $h\in H$ 使得 $y=a\cdot h$. 因此我們得 $f(h)=y$, 也就是說 f 是 onto. 假設 $h\neq h'$ 是 H 中任兩個相異元素, 則 $f(h)=a\cdot h$ 和 $f(h')=a\cdot h'$ 是 $a\cdot H$ 中兩相異元素. 這是因為如果 $a\cdot h=a\cdot h'$, 則兩邊同乘 a^{-1}, 可得 $h=h'$ 而與當初假設 $h\neq h'$ 矛盾. 這證明了 f 是一對一的, 也因此證得了 H 和 $a\cdot H$ 有相同的元素個數. □

現在如果 G 是一個 finite group 且 H 是其 subgroup, 其中 G 的 order 為 n, H 的 order 為 m. 如果用我們一直討論的分類方法利用 H 可將 G 分成 k 類, 由 Lemma 2.2.1 知每一類共有 m 個元素, 再由 Lemma 2.1.2 知 G 的個數 $n=m\cdot k$. 所以我們證得了以下 Lagrange's Theorem.

Theorem 2.2.2 (Lagrange)**.** 若 G 是一個 *finite group* 且 H 是其 *subgroup,* 其中 G 的 *order* 為 n, H 的 *order* 為 m, 則 $m\,|\,n$.

這裡要注意的是: 一般同學們最常犯的錯是以為 Lagrange's Theorem 的逆命題是對的. 其實不然! 也就是說若 G 的 order 為 n, 且 $m\,|\,n$, 並不表示一定存在一個 G 的 subgroup H 使得 H 的 order 為 m. 另外要注意的是: Lagrange's Theorem 只適用於 G 是一個 finite group. 若 G 的個數是無窮大時, 我們無從得知 H 個數的訊息. 此時 H 的 order 有可能為 ∞, 或是任何的正整數.

Lagrange's Theorem 有許多的應用我們先介紹一個特殊的狀況的應用, 更一般的狀況我們留到下一節討論.

Corollary 2.2.3. 若 G 是一個 *finite group* 且其 *order* 為 p, 其中 p 為一個質數. 則 G 為一個 *cyclic group,* 而且 G 中的任一元素除了 *identity* 以外皆可 *generates* G.

Proof. 我們複習一下: G 是一個 cyclic group 且 a generates G 表示 a 產生的 cyclic group $\langle a\rangle$ 就是 G. 今若 a 不是 identity, 則 $\langle a\rangle$ 的 order 必不等於 1, 因為已知 $\langle a\rangle$ 中必有 e 和 a 這兩個元素. 但由 Lagrange's Theorem (2.2.2) 知 $|\langle a\rangle|$ 一定是 $|G|=p$ 的一個因數. 但是 p 是個質數, 其因數只有 1 及 p. 故可得 $|\langle a\rangle|=p$. 既然 $\langle a\rangle$ 是 G 的 subgroup 且它們的個數又相等, 故得 $\langle a\rangle = G$. □

2.3. 元素的 order

前面定義過一個 group 的 order 為其元素的個數. 而一個 group 中的元素 a, 其產生的 cyclic group $\langle a\rangle$ 的 order 就稱為此元素 a 的 order. 我們記為 $\mathrm{ord}(a)$. 若 G 為一個 group 且 $a\in G$, 由 Lagrange's Theorem 知 $\mathrm{ord}(a)\,|\,|G|$. 因此若我們知 G 中元素的 order 或多或少就可知道 G 的 order 的一些訊息, 反之亦然.

以下的 Lemma 給我們一個明確的方法來計算一個元素的 order.

Lemma 2.3.1. 令 a 為一個 *group* G 中的元素, e 為 G 的 *identity.* 假設 $n\in\mathbb{N}$ 是最小的正整數使得 $a^n=e$, 則 $\mathrm{ord}(a)=n$.

Proof. 我們要證明當 n 是最小的正整數使得 $a^n=e$ 則 $\langle a\rangle$ 有 n 個元素. 事實上我們要證明 $\langle a\rangle=\{e,a,a^2,\ldots,a^{n-1}\}$. 首先回顧 $\langle a\rangle$ 中的元素都是 a^k, $k\in\mathbb{Z}$ 這種形式. 利用整數的餘數定理: 當 $n>1$ 時, 可以找到整數 h 和 r 使得 $k=h\cdot n+r$, 其中 $0\le r<n$. 因此

$$a^k=a^{h\cdot n+r}=(a^n)^h\cdot a^r=e\cdot a^r=a^r.$$

換句話說我們利用 $a^n=e$ 得到 $\langle a\rangle$ 中的元素可表為 a^r, $0\le r<n$ 這種形式, 也就是說 $\langle a\rangle=\{e,a,a^2,\ldots,a^{n-1}\}$. 但這並不表示 $\langle a\rangle$ 有 n 個元素, 除非我們知道它們都相異. 因此我們還得證明當 $0\le i<j<n$ 時, $a^i\neq a^j$. 別忘了我們尚未用到 n 是最小的這個性質. 如果 $0\le i<j<n$ 且 $a^i=a^j$, 則 $a^{j-i}=a^j\cdot a^{-i}=e$. 但 $j-i\in\mathbb{N}$ 且 $n>j-i$. 這和 n 是最小的正整數使得 $a^n=e$ 矛盾. 故 $a^j\neq a^i$. 也就是說 $\langle a\rangle$ 的 order 為 n. □

假設 a 的 order 為 n. 由 n 是最小的正整數使得 $a^n=e$ 這個性質知如果 $m\in\mathbb{N}$ 且 $a^m=e$, 則 $m\ge n$. 事實上我們可得到 m 與 n 更好的關係式.

Lemma 2.3.2. 令 a 為 *group* G 中的一元素. 若 $a^m=e$, 則 $\mathrm{ord}(a)\,|\,m$.

Proof. 假設 $\mathrm{ord}(a)=n$. 利用整數的餘數定理, 存在整數 h 及 r, 其中 $0\le r<n$ 使得 $m=n\cdot h+r$. 故得

$$a^m=a^{n\cdot h}\cdot a^r=e\cdot a^r=a^r.$$

也就是說 $a^r=e$. 如果 $r\neq 0$, 則 r 是一個比 n 還小的正整數使得 $a^r=e$. 此和 Lemma 2.3.1 相違背. 故知 $r=0$; 換句話說 n 可整除 m. □

當然了, 從若 $a^m = e$ 則 $n \mid m$ 這個性質我們可推得 n 是最小的正整數滿足 $a^n = e$. 所以整合 Lemma 2.3.1 及 Lemma 2.3.2, 當我們要說 $\mathrm{ord}(a) = n$ 時, 我們只要驗證:

(1) $a^n = e$.

(2) 若 $a^m = e$ 則 $n \mid m$.

下一個 Proposition 不但是一個很有用的定理, 而且其證明可以幫助我們了解前面提到如何驗證一個元素的 order 的方法.

Proposition 2.3.3. 令 a 為 *group* G 中的一元素. 若 $\mathrm{ord}(a) = n$, 則對於任意的整數 i,

$$\mathrm{ord}(a^i) = \frac{n}{\gcd(i, n)}.$$

Proof. 為了方便, 我們令 $d = \gcd(i, n)$. 欲證明 $\mathrm{ord}(a^i) = n/d$, 首先得證明 $(a^i)^{n/d} = e$. 事實上因為 d 是 i 的因數, i/d 是個整數. 再加上由假設 n 為 a 的 order, 故 $a^n = e$. 所以可得 $(a^i)^{n/d} = (a^n)^{i/d} = e$.

接下來我們須證明, 若 $(a^i)^m = e$ 則 $(n/d) \mid m$. 若 $(a^i)^m = e$, 即 $a^{mi} = e$. 故由 Lemma 2.3.2, 我們可得 $n \mid mi$. 但因 d 是 n 和 i 的最大公因數. 我們有 n/d 和 i/d 皆為整數且互質. 故由 $n \mid mi$ 可得 $(n/d) \mid m(i/d)$. 再由 n/d 和 i/d 互質, 得 $(n/d) \mid m$.

□

讓我們回到 Lagrange's Theorem 的應用. 若 G 是一個 finite group, 而 $a \in G$, 則 Lagrange's Theorem (2.2.2) 告訴我們說: $\langle a \rangle$ 的 order 整除 G 的 order. 也就是說若 a 的 order 為 m, G 的 order 為 n, 則存在 $r \in \mathbb{N}$ 使得 $n = m \cdot r$. 又因 a 的 order 為 m, 由 Lemma 2.3.1 知 $a^m = e$. 故 $a^n = a^{mr} = (a^m)^r = e$. 因此我們有以下重要的結果.

Corollary 2.3.4. 若 G 是一個 *finite group,* 且其 *order* 為 n. 令 $a \in G$ 是 G 中一元素. 則 $a^n = e$.

2.4. Normal Subgroups 和 Quotient Groups

當 H 是 G 的 subgroup 時, 前面介紹過我們可以用 $a^{-1} \cdot b \in H$ 的方法將 G 分類. 如果我們將同類的元素收集起來看成一個元素, 那麼這個新的集合的元素就明顯比 G 少多了. 如果能在這個新集合上定義一個運算和原來 G 的運算有關, 那麼這個小一點的集合或多或少能幫助我們了解一些有關 G 的性質. 怎樣來定這個運算呢? 給定 $a \in G$, 若 $\overline{a}$ 表示所有和 a 同類的元素所成的集合. 那麼要如何定 $\overline{a} \cdot \overline{b}$ 呢? 很自然的我們會希望定成 $\overline{a \cdot b}$. 也就是說我們希望和 a 同類的元素乘以和 b 同類的元素會和 $a \cdot b$ 同類. 一般來講這是不一定對的, 除非 H 有一些特性. 現在就讓我們談談 H 要有怎樣的特性才能達到我們的希望.

首先若 a 和 a' 同類, b 和 b' 同類; 也就是說 $a^{-1}\cdot a' = h_1 \in H$ 且 $b^{-1}\cdot b' = h_2 \in H$. 則 $a'\cdot b' = (a\cdot h_1)\cdot(b\cdot h_2)$. 要怎樣才能保證 $a\cdot b$ 和 $a'\cdot b'$ 同類呢? 也就是說

$$(a\cdot b)^{-1}\cdot(a'\cdot b') \in H?$$

事實上

$$(a\cdot b)^{-1}\cdot(a'\cdot b') = (b^{-1}\cdot a^{-1})\cdot(a\cdot h_1)\cdot(b\cdot h_2) = (b^{-1}\cdot h_1\cdot b)\cdot h_2.$$

所以要求 $a\cdot b$ 和 $a'\cdot b'$ 同類, 也就是要求 $(b^{-1}\cdot h_1\cdot b)\cdot h_2 \in H$. 又因 $h_2 \in H$, 這等同於要求 $b^{-1}\cdot h_1\cdot b \in H$. 但是別忘了, 我們希望這是對於任意的 $a \sim a'$ 和 $b \sim b'$ 都對, 所以這裡 b 可以是 G 中任意的元素, 同樣的 h_1 可以是 H 中的任意元素. 因此我們很自然的有下列的定義:

Definition 2.4.1. 若 H 是 G 的一個 subgroup 且 H 滿足對所有的 $a \in G$ 及 $h \in H$ 都有 $a^{-1}\cdot h\cdot a \in H$. 則稱 H 為 G 的一個 *normal subgroup*.

千萬要記得這裡我們要求對 G 中的所有元素都要符合這個性質. 如果將上面定義的 a 用 a^{-1} 替代, 則 normal 的條件會變成 $(a^{-1})^{-1}\cdot h\cdot a^{-1} = a\cdot h\cdot a^{-1} \in H$. 有的書用 $a\cdot h\cdot a^{-1} \in H$ 這個定義, 其實都是一樣的. 我們以後會因問題的方便性兩種替換選擇使用.

Remark 2.4.2. 對一個 group 我們若要提到其 normal 的性質, 則一定要確切的提到是在哪一個 group 之下是 normal 的. 同學經常會把以下的幾種情況搞混, 我們特別把它們列出來: 假設有三個 groups, N, H, G, 且 $N \subseteq H \subseteq G$.

(1) 如果已知 N 是 G 的 normal subgroup, 那麼 N 也會是 H 的 normal subgroup. 這是因為若 $n \in N, h \in H$, 則由於 h 也在 G 中, 所以由 N 在 G 中 normal 知 $h^{-1}\cdot n\cdot h \in N$.

(2) 如果已知 N 在 H 中 normal, 那麼 N 不一定在 G 中 normal. 這是因為 G 中可能有元素不在 H 中. 所以我們不能擔保所有 $g \in G$ 都會符合 $g^{-1}\cdot n\cdot g \in N$.

(3) 如果已知 H 在 G 中 normal, 那麼 N 不一定在 G 或 H 中 normal. 這是因為雖然可由 $n \in N$ 得到 $n \in H$. 不管如何, 利用 H 在 G 中 normal, 我們僅能得到 $g^{-1}\cdot n\cdot g \in H$, 而不是在 N.

(4) 如果已知 N 在 H 中 normal 且 H 在 G 中normal, 那麼 N 還是不一定能在 G 中 normal. 這利用和 (2), (3) 相同的解釋就可知.

有的書習慣用集合的方式來表示 normal. 也就是說 N 在 G normal 表示 $\forall a \in G$, $a^{-1}\cdot N\cdot a \subseteq N$. 這和我們前面用元素來定義是一樣的. 還有的書定義 normal subgroup 是要求: $\forall a \in G$, $a^{-1}\cdot N\cdot a = N$. 這樣的定義看似條件比較強不過其實是一樣的. 主要的原因是既然對於所有的 $a \in G$, $a^{-1}\cdot N\cdot a \subseteq N$. 所以在兩邊分別乘上 a 和 a^{-1} 得

$$N = a\cdot(a^{-1}\cdot N\cdot a)\cdot a^{-1} \subseteq a\cdot N\cdot a^{-1}.$$

也就是說 $N = a \cdot N \cdot a^{-1}$, 同理得 $a^{-1} \cdot N \cdot a = N$.

所以當你要證明一個 group N 是 G 的 normal subgroup 時, 你只要證明 $a \cdot N \cdot a^{-1} \subseteq N$ 就好, 然而若你已知 N 在 G 中 normal 時, 那你當然可以用 $a \cdot N \cdot a^{-1} = N$ 這個等式了. 畢竟條件越強越好用啊!

若 N 是 G 的 normal subgroup, 則用元素的寫法我們可以寫成: 對於所有 $g \in G$, $n \in N$ 都可找到 $n' \in N$ 使得 $g \cdot n = n' \cdot g$ (或是找到 $n'' \in N$ 使得 $n \cdot g = g \cdot n''$). 當然了若 G 是 abelian, 則當 $n' = n$ (或 $n'' = n$) 時, 上面的等式都對. 也就是說:

Lemma 2.4.3. 當 G 是一個 *abelian group* 時, 所有的 *subgroup* 都是 *normal subgroup*.

現在回到我們考慮 normal subgroup 的真正目的. 我們想利用 G 來創造另一個小一點的 group 來幫助我們了解 G. 給定一個 subgroup N 若我們考慮用前面的分類方法用 N 將 G 分類然後將同類的元素所成的集合看成一個新的元素, 那麼從集合的觀點來看這些新的元素所成的集合自然比原來 G 小. 例如前面在證明 Lagrange 定理時, 我們知道若 G 是 finite group 則可用 N 將 G 分成 $|G|/|N|$ 類. 所以在這情況下新的集合就只有 $|G|/|N|$ 個元素了. 然而若 N 是 G 的 normal subgroup 時, 前面提到我們就可以給這一個新的集合一個運算. 也就是說若 $\overline{a}$ 是與 a 同類的元素所成的集合, $\overline{b}$ 是與 b 同類的元素所成的集合, 則我們定 $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. (再次強調一定要是 normal subgroup 定出的運算才是 well defined. 否則和 a 同類的元素乘以和 b 同類的元素不一定和 $a \cdot b$ 同類.) 我們將說明這一個運算給了這個新的集合一個 group 的結構. 這個新的 group 我們稱之為 the *quotient group of* G *by* N (有的書稱作 *factor group*), 記作: G/N.

(GP1): 若 $\overline{a}, \overline{b} \in G/N$, 則由於 $a \cdot b \in G$ 故 $\overline{a \cdot b} \in G/N$. 也就是說 $\overline{a} \cdot \overline{b} \in G/N$.

(GP2): 我們要證明 $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$. 然而

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

且

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

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

(GP3): 甚麼會是 G/N 的 identity 呢? 若 e 是 G 的 identity, 則對所有的 $\overline{a} \in G/N$. 我們自然有 $\overline{a} \cdot \overline{e} = \overline{a \cdot e} = \overline{a}$. 同理 $\overline{e} \cdot \overline{a} = \overline{e \cdot a} = \overline{a}$. 所以 $\overline{e}$ 是 G/N 的 identity.

(GP4): 若 $\overline{a} \in G/N$ 甚麼會是 $\overline{a}$ 的 inverse 呢? 相信大家都可以猜到就是 $\overline{a^{-1}}$ 了. 我們驗證 $\overline{a} \cdot \overline{a^{-1}} = \overline{a \cdot a^{-1}} = \overline{e}$. 同理 $\overline{a^{-1}} \cdot \overline{a} = \overline{e}$. 所以 $\overline{a^{-1}}$ 就是 $\overline{a}$ 的 inverse. 我們可以記作 $(\overline{a})^{-1} = \overline{a^{-1}}$.

Example 2.4.4. Quotient group 的例子很多. 大家最常見的例子就是在整數用加法所成的 group 中的 quotient group. 例如 $5\mathbb{Z}$ 就是 $\mathbb{Z}$ 的一個 normal subgroup (別忘了 $\mathbb{Z}$ 是 abelian). 而 $\mathbb{Z}/5\mathbb{Z}$ 就是 the quotient group of $\mathbb{Z}$ by $5\mathbb{Z}$. 到底 $\mathbb{Z}/5\mathbb{Z}$ 是甚

麼呢? 比方說利用 $5\mathbb{Z}$ 來分類哪些整數和 1 同類呢? 照定義來看就是那些 $n \in \mathbb{Z}$ 使得 $1 \cdot (n)^{-1} \in 5\mathbb{Z}$. 錯! 別忘了我們是看加法群你必須把上式的 $\cdot$ 改成 $+$, 而 n^{-1} 改成 $-n$. 所以和 1 同類的就是那些整數符合 $1 - n \in 5\mathbb{N}$. 也就是除以 5 餘 1 的整數. 由此知 $\mathbb{Z}/5\mathbb{Z}$ 可以用 $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ 來表示. 其中 $\overline{0}$, 也就是所有 5 的倍數所成的集合, 是其 identity. 這就是大家在基礎數論學的 congruence.

2.5. Group Homomorphisms

在數學中要描繪兩種東西間的關係最好的方法就是利用函數 function. 當然並不是所有這兩東西間的函數都很重要. 例如我們只關心兩個 groups 間的 group 架構, 因此我們只對某種特殊的函數有興趣. 這種函數我們稱之為 *group homomorphism.*

Definition 2.5.1. 當 G, G' 是 groups 而 $\phi : G \to G'$ 是從 G 映射到 G' 的函數. 如果 ϕ 滿足對於所有 $a, b \in G$ 皆有 $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, 則稱此函數 ϕ 是一個 group homomorphism.

要注意的是: 因為 $a, b \in G$, 所以這裡 $a \cdot b$ 是在 G 中的乘法; 而 $\phi(a), \phi(b) \in G'$, 所以 $\phi(a) \cdot \phi(b)$ 是在 G' 中的乘法. 簡單地說: 一個從 G 到 G' 的 group homomorphism 就是一個函數它能保持 G 和 G' 元素間的運算. 以下的 Lemma 就是說明這個觀點的一個很好的例子. 它告訴我們 group homomorphism 會把 identity 送到 identity, 把 inverse 送到 inverse.

Lemma 2.5.2. 設 G 和 G' 是 *groups* 且 e 和 e' 分別為其 *identity.* 若 ϕ 是一個從 G 映到 G' 的 *group homomorphism,* 則*:*

(1) $\phi(e) = e'$.

(2) 給定任意的 $a \in G$, $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof. 由 Theorem 1.2.3 知: 要證明 $\phi(e)$ 是 G' 的 identity, 我們只要在 G' 中找到一元素 b 使得 $b \cdot \phi(e) = b$ 就可以 (再次強調我們不需證所有的 $g \in G'$ 都會使得 $g \cdot \phi(e) = g$). 其實我們只要找 $b = \phi(e) \in G'$ 就好了. 這樣一來,

$$b \cdot \phi(e) = \phi(e) \cdot \phi(e) = \phi(e \cdot e) = \phi(e) = b.$$

所以得證 $\phi(e)$ 是 G' 的 identity.

同樣的要證明 $\phi(a^{-1})$ 是 $\phi(a)$ 的 inverse, 我們只要證 $\phi(a^{-1}) \cdot \phi(a) = e'$ 就可. 然而

$$\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1} \cdot a) = \phi(e) = e'.$$

所以 $\phi(a^{-1}) = \phi(a)^{-1}$. □

一般的函數有兩個集合是很重要的: 一個是在對應域裡的值域(像); 另一個就是定義域裡的解集合(送到 0 的元素所成的集合). 同樣的在 group homomorphism 中這兩個集合也很重要. 一個稱為 *image*; 另一個稱為 *kernel*.

Definition 2.5.3. 若 $\phi : G \to G'$ 是一個 group homomorphism, 則

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

稱為 ϕ 的 *image.*

$$\ker(\phi) = \{a \in G \,|\, \phi(a) = e'\},$$

稱為 ϕ 的 *kernel.*

從定義可知 $\mathrm{im}(\phi)$ 是 G' 的一個子集合, 而 $\ker(\phi)$ 是 G 的子集合. 事實上它們有很好的性質.

Lemma 2.5.4. 若 $\phi : G \to G'$ 是一個 *group homomorphism,* 則 $\mathrm{im}(\phi)$ 是 G' 的 *subgroup,* 而 $\ker(\phi)$ 是 G 的 *normal subgroup.*

Proof. 我們可以利用定義直接證 $\mathrm{im}(\phi)$ 和 $\ker(\phi)$ 分別是 G' 和 G 的 subgroup. 我們這裡想直接利用 Lemma 1.3.4 來證.

若 $\phi(a), \phi(b) \in \mathrm{im}(\phi)$, 其中 $a, b \in G$, 則利用 Lemma 2.5.2 我們知 $\phi(b)^{-1} = \phi(b^{-1})$. 故

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

又因 $a \cdot b^{-1} \in G$, 故 $\phi(a) \cdot \phi(b)^{-1} \in \mathrm{im}(\phi)$. 另外若 $a, b \in \ker(\phi)$, 即 $\phi(a) = \phi(b) = e'$, 則

$$\phi(a \cdot b^{-1}) = \phi(a) \cdot \phi(b)^{-1} = e' \cdot e' = e'.$$

也就是說 $a \cdot b^{-1} \in \ker(\phi)$. 由以上二式知 $\mathrm{im}(\phi)$ 和 $\ker(\phi)$ 分別是 G' 和 G 的 subgroup.

最後我們證 $\ker(\phi)$ 事實上是 G 的 normal subgroup. 也就是要證明: 對於所有的 $g \in G$, 我們都有 $g \cdot \ker(\phi) \cdot g^{-1} \subseteq \ker(\phi)$. 換句話說: 若 $a \in \ker(\phi)$, 則我們要證 $g \cdot a \cdot g^{-1} \in \ker(\phi)$. 然而

$$\phi(g \cdot a \cdot g^{-1}) = \phi(g) \cdot \phi(a) \cdot \phi(g^{-1}).$$

再利用 $\phi(a) = e'$ 及 $\phi(g^{-1}) = \phi(g)^{-1}$, 我們可得

$$\phi(g \cdot a \cdot g^{-1}) = \phi(g) \cdot e' \cdot \phi(g)^{-1} = e'.$$

故 $g \cdot a \cdot g^{-1} \in \ker(\phi)$. □

Definition 2.5.5. 令 $\phi : G \to G'$ 是一個 group homomorphism:

(1) 若 ϕ 是 onto, 則稱之為 *epimorphism.*

(2) 若 ϕ 1-1, 則稱之為 *monomorphism.*

(3) 若 ϕ 是 1-1 且 onto, 則稱之為 *isomorphism.*

當然了我們可以用 $\mathrm{im}(\phi)$ 來判定 ϕ 是否為 epimorphism. 事實上若 $\mathrm{im}(\phi) = G'$, 則 ϕ 為 onto, 故為 epimorphism. 我們也可以用 $\ker(\phi)$ 來判定 ϕ 是否為 monomorphism.

Lemma 2.5.6. 已知 $\phi : G \to G'$ 是一個 *group homomorphism,* 則 ϕ 是一個 *monomorphism* 若且為若 $\ker(\phi) = \{e\}$.

Proof. 假設 ϕ 是 monomorphism (即 1-1). 若 $g \in \ker(\phi)$, 則由 Lemma 2.5.2 知 $\phi(g) = \phi(e) = e'$. 但若 $g \neq e$, 則由 ϕ 是 1-1 知 $\phi(g) \neq \phi(e)$. 故得 $g = e$, 也就是說 $\ker(\phi) = \{e\}$.

反之, 假設 $\ker(\phi) = \{e\}$. 若存在 $g_1 \neq g_2$ 使得 $\phi(g_1) = \phi(g_2)$, 則

$$\phi(g_1 \cdot g_2^{-1}) = \phi(g_1) \cdot \phi(g_2)^{-1} = e'.$$

也就是說 $g_1 \cdot g_2^{-1} \in \ker(\phi)$. 但這代表 $g_1 \cdot g_2^{-1} = e$, 即 $g_1 = g_2$, 和當初假設 $g_1 \neq g_2$ 矛盾. 換句話說若 $g_1 \neq g_2$ 則 $\phi(g_1) \neq \phi(g_2)$. 這告訴我們 ϕ 是 1-1 的. □

這個定理告訴我們: 要檢查一個 group homomorphism 是否為 1-1, 只要檢查其 kernel 是否為 identity 即可. 不過千萬要切記, 我們是在假設 ϕ 是一個 group homomorphism 的前題之下才有這個結果. 你不可以拿到一個函數馬上就檢查其 kernel 為 identity 然後就下斷語說它是 1-1. 除非你已先知其為一個 group homomorphism. 最簡單的反例就是若 $f : \mathbb{R} \to \mathbb{R}$ 是一個實數到實數的函數, 你不能因為 $x = 0$ 是 $f(x) = 0$ 的唯一解就說 $f(x)$ 是 1-1.

有時候兩個 groups 的元素看起來是不一樣的不過它們在結構上是相同的. 在代數的眼光中不應該把它們看成是不同的 groups. 不過怎樣來判定兩個 groups 結構相同呢? 如果兩個 groups G 和 G' 間你可以找到一個 group homomorphism 是 isomorphism (即 1-1 且 onto), 則我們稱 G 和 G' 這兩個 group 是 *isomorphic*, 記為: $G \simeq G'$. 意思是我們把它們看作是同樣的 group. 這樣的看法是合理的: 因為 1-1 和 onto 表示 G 和 G' 看成集合是一樣的, 在加上 group homomorphism 保持它們 group 的結構, 所以我們把它們看作是一樣的 group.

這樣的看法在 finite group 之下大致上同學們就知道兩個 groups 若是 isomorphic 則它們的 order (元素個數) 要一樣. 不過要注意的是若兩個 groups 其 order 相同不見得它們就 isomorphic. 不管如何若兩個 groups 其 order 不同則它們一定不 isomorphic.

當考慮 infinite group 情況複雜多了; 主要是此時我們無法算個數. 這時有很多特殊現象發生, 例如一個 group 的 subgroup 可以和它 isomorphic. 我們有以下的簡單例子:

Example 2.5.7. 考慮 $\mathbb{Z}$ 是一個加法之下的 group, 則所有偶數所成的集合 $2\mathbb{Z}$ 是其 subgroup. 考慮 $\phi : \mathbb{Z} \to 2\mathbb{Z}$ 是一個 group homomorphism 定義成: $\phi(n) = 2n$. 很容易看出來 ϕ 是一個 isomorphism. 所以 $\mathbb{Z}$ 和 $2\mathbb{Z}$ 是 isomorphic.

其實我們可以證得 $\mathbb{Z}$ 中所有的 nontrivial subgroup 都和 $\mathbb{Z}$ isomorphic. 不過我們別擔心太多 infinite group 因為前面已提過了, 在大學代數課中我們只要關心 finite group 就好了.

最後要強調的是: G 和 G' 是 isomorphic 表示在 G 和 G' 之間可以找到一個 isomorphism. 這並不表示 G 和 G' 間所有的 homomorphism 都是 isomorphism. 同學們常常誤解這一點以致於當碰到要你證明 G 和 G' 不是 isomorphic 時, 有的同學會在 G 和 G' 中找到一個 homomorphism 不是 1-1 及 onto 就斷言 G 和 G' 不是 isomorphism. 這是大錯特錯的!

2.6. 三個 Isomorphism 定理

給定 G 和 G' 要說明它們是 isomorphic 時, 若想真正找到它們之間一個具體的 isomorphism 一般來說並不容易. 在這一節中我們將介紹三個定理來幫助我們確認 $G \simeq G'$ 而不必真正找到一個 isomorphism. 別害怕! 雖然是三個定理, 不過後兩個定理可以利用第一個定理輕鬆推得. 所以大家務必要學好第一個 isomorphism 定理.

Theorem 2.6.1 (First Isomorphism Theorem)**.** *若 $\phi : G \to G'$ 是一個 group homomorphism,* 則

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

Proof. 首先我們回顧一下: 因 $\phi : G \to G'$ 是一個 group homomorphism, 由 Lemma 2.5.4 知 $\mathrm{im}(\phi)$ 是 G' 的 subgroup, 而 $\ker(\phi)$ 是 G 的 normal subgroup. 所以要證得這一個定理, 我們必須先在 $G/\ker(\phi)$ 這一個 quotient group 和 $\mathrm{im}(\phi)$ 這個 group 之間找到一個函數. 再說明這個函數是 group homomorphism, 最後再驗證它是 1-1 且 onto.

$G/\ker(\phi)$ 和 $\mathrm{im}(\phi)$ 長甚麼樣子我們都不知道, 如何能無中生有創造出一個函數呢? 當然不可能無中生有! 我們可以用已經有的函數來創造它. 別忘了在假設中有一個 ϕ, 我們可以利用 ϕ 製造以下的函數:

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

具體來說 ψ 是把和 a 同類的元素送到 $\phi(a)$ 這個值. 先別急著驗證 ψ 是一個 group homomorphism. 你確定 ψ 是一個'好函數' (well defined function) 嗎? 別忘了要成為一個好函數必須有以下兩個要素:(1) 每一個定義域裡的元素都必須送到對應域裡; (2) 不可以"一對多": 也就是同一個元素不可以有兩種送法. 關於 (1) 我們的函數 ψ 是 O.K. 的. 因為每個定義域 (即 $G/\ker(\phi)$) 裡的元素都是長 $\overline{a}$ 這個樣子, 其中 $a \in G$. 所以 ψ 把 $\overline{a}$ 送到 $\phi(a)$. 依定義 $\phi(a)$ 當然在對應域 $\mathrm{im}(\phi)$ 內. 至於 (2) 就需要驗證了. 這是因為 $G/\ker(\phi)$ 內的元素並沒有唯一的方法用 G 中的元素表示出來. 也就是說在 G 中可以找到兩個不同的元素 a, b 使得 $\overline{a}$ 和 $\overline{b}$ 在 $G/\ker(\phi)$ 中是相同的. 所以要說明 ψ 不是一對多, 我們必須說明 $\phi(a) = \phi(b)$. 雖然 $a \neq b$, 不過由 $\overline{a} = \overline{b}$ 知 a 和 b 在以 $\ker(\phi)$ 這個 subgroup 的分類下是同類的. 別忘了 a 和 b 同類表示 $a^{-1} \cdot b \in \ker(\phi)$. 也就是說 $\phi(a^{-1} \cdot b) = e'$. 再利用 ϕ 是 group homomorphism 的假設, 我們得

$$\phi(a)^{-1} \cdot \phi(b) = \phi(a^{-1} \cdot b) = e'.$$

等式兩邊乘上 $\phi(a)$, 可得 $\phi(a) = \phi(b)$. 所以我們製造的 ψ 是一個 well defined function.

接下來證 ψ 是一個 group homomorphism: 這不難, 只要記住 $G/\ker(\phi)$ 中的乘法是定義成: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. 因此對任意的 $\overline{a}, \overline{b} \in G/\ker(\phi)$, 我們有

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

另一方面因為 ϕ 是 group homomorphism, 所以

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

結合以上二式, 我們可得 $\psi(\overline{a} \cdot \overline{b}) = \psi(\overline{a}) \cdot \psi(\overline{b})$.

證明 ψ 是 onto 純粹是定義: 給定任意元素 $y \in \mathrm{im}(\phi)$, 依定義知存在 $x \in G$ 使得 $y = \phi(x)$. 因此我們可找 $\overline{x} \in G/\ker(\phi)$ 代入 ψ 得 $\psi(\overline{x}) = \phi(x) = y$. 因此 ψ 是 onto.

既然 ψ 是 group homomorphism, 我們可以利用 Lemma 2.5.6: 也就是證明 $\ker(\psi)$ 是 $G/\ker(\phi)$ 的 identity. 別忘了 $G/\ker(\phi)$ 的 identity 是 $\overline{e}$. 假設 $\overline{x} \in \ker(\psi)$, 即 $\psi(\overline{x}) = e'$, 其中 e' 是 G' 的 identity. 但是由 ψ 的定義: $\psi(\overline{x}) = \phi(x)$, 故知 $x \in \ker(\phi)$. 然而 G 中元素用 $\ker(\phi)$ 來分類的話 x 和 e 是同類的 (因 $e^{-1} \cdot x = x \in \ker(\phi)$). 故在 $G/\ker(\phi)$ 中 $\overline{x} = \overline{e}$.

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

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

Corollary 2.6.2. *若 $\phi : G \to G'$ 是一個 group epimorphism,* 則

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

First Isomorphism Theorem 告訴我們甚麼呢? 如果有一個 group G, 而 N 是其 normal subgroup. 則當我們要證明另一個 group G' 和 G/N 是 isomorphic 時. 我們不必辛苦的去找 G/N 和 G' 間的 isomorphism. 我們只要去找到一個 G 到 G' 的 epimorphism, ϕ, 如果又剛好 $\ker(\phi) = N$. 那麼由 First Isomorphism Theorem 我們就可知 $G/N \simeq G'$ 了.

讓我們就利用證明第二個 isomorphism 定理來說明 First Isomorphism Theorem 的妙用吧! 給定一 group G, 若 H, N 是 G 的 subgroups, 考慮以下之集合:

$$H \cdot N = \{h \cdot n \,|\, h \in H, n \in N\}.$$

因為 H 和 N 都在 G 中所以 $H \cdot N$ 當然是 G 的一個子集合. 不過它不一定是 G 的 subgroup 喔! 主要的問題出在封閉性. 在 $H \cdot N$ 中任取兩元素, $h \cdot n$ 和 $h' \cdot n'$, 其中 $h, h' \in H$, $n, n' \in N$. 則 $(h \cdot n) \cdot (h' \cdot n')$ 不一定可以寫成一個 H 中的元素乘上一個

N 中的元素這樣的形式. 不過若 H 和 N 其中一個是 G 的 normal subgroup, 那麼 $H \cdot N$ 就是 G 的 subgroup 了. 我們就把這個事實寫成 Lemma 吧!

Lemma 2.6.3. *若 H 是 G 的 subgroup 且 N 是 G 的 normal subgroup. 則 $H \cdot N = N \cdot H$ 且是 G 的 subgroup.*

Proof. 因為 N 是 G 的 normal subgroup, 故因 $H \subseteq G$, 對於所有 $h \in H$ 及 $n \in N$, $h \cdot n \cdot h^{-1} \in N$. 換句話說存在 $n' \in N$ 使得 $h \cdot n \cdot h^{-1} = n'$. 因此 $h \cdot n = n' \cdot h$. 由此可得 $H \cdot N \subseteq N \cdot H$. 同理可得 $N \cdot H \subseteq H \cdot N$.

利用以上的結果, 前面所提的封閉性就可以解決了. 因為存在 $n'' \in N$ 使得 $h' \cdot n' = n'' \cdot h'$ 故

$$(h \cdot n) \cdot (h' \cdot n') = (h \cdot n) \cdot (n'' \cdot h') = h \cdot (n \cdot n'') \cdot h'.$$

又因 $n \cdot n'' \in N$, 故存在 $\hat{n} \in N$ 使得 $(n \cdot n'') \cdot h' = h' \cdot \hat{n}$. 故

$$(h \cdot n) \cdot (h' \cdot n') = (h \cdot h') \cdot \hat{n} \in H \cdot N.$$

反元素的存在也可用相同的看法: 若 $h \cdot n \in H \cdot N$, 則

$$(h \cdot n)^{-1} = n^{-1} \cdot h^{-1} \in N \cdot H.$$

又 $N \cdot H = H \cdot N$, 故 $(h \cdot n)^{-1} \in H \cdot N$. □

現在讓我們看看第二個 isomorphism 定理在談甚麼?

Theorem 2.6.4 (Second Isomorphism Theorem)**.** *若 H 是 G 的 subgroup 且 N 是 G 的 normal subgroup. 則 $H \cap N$ 是 H 的 normal subgroup, 且*

$$H/(H \cap N) \simeq (H \cdot N)/N.$$

Proof. 雖然定理提到 $H \cap N$ 是 H 的 normal subgroup, 不過我們先不證它, 而直接用 first isomorphism 定理, normal subgroup 的部分會自然成立. 另外要注意的是定理中有另一個 quotient group $(H \cdot N)/N$. 前面提到這是一個 group 非得要 N 在 $H \cdot N$ 中 normal, 為甚麼定理不談 N 在 $H \cdot N$ 中 normal 呢? 學代數到現在你應該了解這是很 trivial 的事實了. 因為 H 中有 identity 故對任意的 $n \in N$ 皆可寫成 $n = e \cdot n \in H \cdot N$. 因此得 $N \subseteq H \cdot N$. 換句話說 H 是 $H \cdot N$ 的 subgroup. 那為甚麼 normal? 既然 N 在 G 中 normal, 當然對任意的元素 $g \in H \cdot N \subseteq G$ 都有 $g \cdot N \cdot g^{-1} = N$ 了.

怎麼用 first isomorphism 定理呢? 前面提到你要證明一個 quotient group 和另一個 group 是 isomorphism 時, 可以先不管 quotient group 中那個在底下的 normal subgroup. 在目前的情況我們有兩種選擇: (1) 從 H 到 $(H \cdot N)/N$ 的 homomorphism; (2) 從 $H \cdot N$ 到 $H/(H \cap N)$ 的 homomorphism. 你會選哪一個呢? 當然是 (1) 了! 主要原因不只是 (2) 中的 $H \cap N$ 在 H 中 normal 還沒證. 更重要的是從 H 到

$(H\cdot N)/N$ 的 homomorphism 比從 $H\cdot N$ 到 $H/(H\cap N)$ 的 homomorphism 更自然更好找. (為甚麼呢? 只能說是憑感覺吧!)

讓我們先找一個從 H 到 $(H\cdot N)/N$ 的函數吧! 因為 H 是 $H\cdot N$ 的 subgroup, 我們有一個很自然的映射把 H 的元素送到 $H\cdot N$: 也就是把 H 中的元素乖乖的原封不動的放到 $H\cdot N$ 中. 即 $\iota : H \to H\cdot N$ 其中 $\iota(h) = h$. 又 N 在 $H\cdot N$ 中 normal, 我們又有一個很自然的可將 $H\cdot N$ 的元素用 N 分類的函數. 即 $\pi : H\cdot N \to (H\cdot N)/N$ 其中對所有的 $g \in H\cdot N$ 我們有 $\pi(g) = \overline{g}$. 將 π 和 ι 合成, 我們自然有一個函數

$$\phi = \pi\circ\iota : H \to (H\cdot N)/N,$$

其中對所有的 $h \in H$ 我們有

$$\phi(h) = \pi(\iota(h)) = \overline{h}.$$

現在要證 ϕ 是一個 group homomorphism. (我們不必證 ϕ 是 well defined, 這是因為 ϕ 這個函數'明明白白'的把 h 送到 $\overline{h}$ 這一個元素. 沒有前面那種一對多的可能.) 事實上對任意的 $h, h' \in H$, 我們有

$$\phi(h\cdot h') = \overline{h\cdot h'} = \overline{h}\cdot\overline{h'} = \phi(h)\cdot\phi(h').$$

接下來證 ϕ 是 onto. 任意的 $H\cdot N$ 中的元素可寫成 $h\cdot n$, 其中 $h \in H$, $n \in N$. 所以任意的 $(H\cdot N)/N$ 中的元素都可寫成 $\overline{h\cdot n}$. 但是 $\overline{h\cdot n} = \overline{h}\cdot\overline{n}$. 別忘了我們是用 N 來分類所以 N 中的元素都和 identity 同類. 也就是說 $\overline{n} = \overline{e}$. 因此 $\overline{h\cdot n} = \overline{h}$. 由此知任意 $(H\cdot N)/N$ 中的元素 $\overline{h\cdot n}$ 我們都可找 $h \in H$ 使得 $\phi(h) = \overline{h} = \overline{h\cdot n}$. 因此 ϕ 是 onto.

既然 ϕ 是一個從 H 到 $(H\cdot N)/N$ 的 epimorphism, 我們可以用 First Isomorphism Theorem (Corollary 2.6.2) 得到

$$H/\ker(\phi) \simeq (H\cdot N)/N.$$

甚麼是 $\ker(\phi)$ 呢? 依定義 $\ker(\phi)$ 是 H 中的元素 h 使得 $\phi(h)$ 是 $(H\cdot N)/N$ 的 identity, $\overline{e}$. 也就是說 $\phi(h) = \overline{h} = \overline{e}$. 別忘了 $(H\cdot N)/N$ 中的元素是對 N 分類, 故 $\overline{h} = \overline{e}$ 表示 h 和 e 同類, 也就是說 $e^{-1}\cdot h = h \in N$. 由此知 $\ker(\phi)$ 的元素既要在 H 中也要在 N 中; 換句話說 $\ker(\phi) \subseteq H\cap N$. 反之若 $a \in H\cap N$, 則因 $a \in N$ 得 $\phi(a) = \overline{a} = \overline{e}$. 故 $H\cap N \subseteq \ker(\phi)$. 由此知 $\ker(\phi) = H\cap N$. 因此我們由 Lemma 2.5.4 知 $H\cap N$ 是 H 的 normal subgroup 也由 First Isomorphism Theorem 知

$$H/(H\cap N) \simeq (H\cdot N)/N.$$

□

相信大家已經看出 First Isomorphism Theorem 的妙用了. 讓我們再用它來證第三個 isomorphism 定理吧!

Theorem 2.6.5 (Third Isomorphism Theorem)**.** 若 $\phi : G \to G'$ 是一個 *group epimorphism.* 假設 N' 是 G' 的一個 *normal subgroup.* 令

$$N = \{a \in G \,|\, \phi(a) \in N'\}.$$

則 N 是 G 的 *normal subgroup* 且

$$G/N \simeq G'/N'.$$

Proof. 令 $\pi : G' \to G'/N'$ 是 G' 對 N' 來分類的函數. 如前一定理的證明我們可定 $\psi = \pi \circ \phi : G \to G'/N'$. 也就是說 $\psi(a) = \overline{\phi(a)}, \forall\, a \in G$.

由 ϕ 是 group homomorphism 知

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

故 ψ 是一個從 G 到 G'/N' 的 group homomorphism.

任意 G'/N' 的元素都可寫成 $\overline{g}$ 其中 $g \in G'$ 這種形式. 但因 ϕ 是 onto, 故存在 $a \in G$ 使得 $\phi(a) = g$. 所以

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

因此 ψ 也是 onto. (其實若同學了解一些合成函數的性質, 馬上可以利用兩個 onto 的函數其合成函數也是 onto 知 ψ 是 onto.)

既然知 $\psi : G \to G'/N'$ 是一個 epimorphism, 我們再次用 First Isomorphism Theorem 知

$$G/\ker(\psi) \simeq G'/N'.$$

甚麼是 $ker(\psi)$ 呢? 若 $a \in \ker(\psi)$ 即 $\psi(a) = \overline{\phi(a)} = \overline{e'}$, 其中 e' 是 G' 的 identity. 也就是說 $\phi(a)$ 和 e' 在用 N' 的分類下是同類的. 所以 $\phi(a) \in N'$. 由 N 的定義知, 這表示 $a \in N$. 故 $\ker(\psi) \subseteq N$. 另外若 $a \in N$, 則 $\phi(a) \in N'$ 故在 G'/N 中 $\psi(a) = \overline{\phi(a)} = \overline{e'}$, 因此 $a \in \ker(\psi)$. 得 $N \subseteq \ker(\psi)$. 也就是說 $\ker(\psi) = N$ 且 N 是 G 的 normal subgroup.

□

2.7. Correspondence Theorem

既然 group homomorphism 保持了兩 group 間乘法的運算結構. 那麼這兩個 group 在某種程度來說應該有些關係. Correspondence Theorem 就是描繪這種關係.

Theorem 2.7.1 (Correspondence Theorem)**.** 若 $\phi : G \to G'$ 是一個 *group epimorphism.* 若 H' 是 G' 的 *subgroup* 且令

$$H = \{a \in G \,|\, \phi(a) \in H'\},$$

則 H 是 G 的一個 *subgroup* 且 $H \supseteq \ker(\phi)$. 另外若令

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

則 $\phi(H) = H'$ 且

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

如果又假設 H' 是 G' 的 *normal subgroup.* 則前面所定的 H 也會是 G 的 *normal subgroup.*

Proof. 首先先證 H 是一個 subgroup of G. 若 $a, b \in H$, 我們要證明 $a \cdot b \in H$ 且 $a^{-1} \in H$. 由定義知 $a, b \in H$ 表示 $\phi(a) \in H'$ 且 $\phi(b) \in H'$, 故 $\phi(a) \cdot \phi(b) \in H'$. 又因 ϕ 是 group homomorphism, 故 $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. 因此 $\phi(a \cdot b) \in H'$, 也就是說 $a \cdot b \in H$. 另外又因 $\phi(a) \in H'$ 故 $\phi(a)^{-1} \in H'$, 再加上 $\phi(a^{-1}) = \phi(a)^{-1}$, 可知 $\phi(a^{-1}) \in H'$. 故 a^{-1} 也在 H 中. (注意這個部分的證明只用到 ϕ 是 group homomorphism, 並不需要 onto.)

若 $a \in \ker(\phi)$, 則 $\phi(a) = e'$. 因 e' 是 G' 的 identity 且 H' 是 G' 的 subgroup, 當然 $e' \in H'$. 也就是說 $\phi(a) \in H'$, 故 $a \in H$. 所以 $\ker(\phi) \subseteq H$. (這部分的證明也不需 epimorphism.)

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

$\phi(H) = H'$ 告訴我們 ϕ 這個函數若限制在 H 中來看是把 H onto 送到 H'. ϕ 對 G 中所有的元素來看是 group homomorphism, 那限制在 H 中當然是 group homomorphism. 而 ϕ 限制在 H 中來看它的 kernel 會是甚麼呢? 當然是在原本的 $\ker(\phi)$ 中也在 H 中的元素. 也就是 $\ker(\phi) \cap H$. 但已知 $\ker(\phi) \subseteq H$ 故 $\ker(\phi) \cap H = \ker(\phi)$. 故由 First Isomorphism Theorem 知

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

別忘了在 Theorem 2.6.5 已證過: 若 H' 在 G' 中 normal 則 H 在 G 中 normal. 我們這裡再給一個一般的證明(因為這不需用到 ϕ 是 onto.) 我們要證明若 $a \in H$ 對任意的 $g \in G$ 皆有 $g \cdot a \cdot g^{-1} \in H$. 要驗證 $g \cdot a \cdot g^{-1}$ 有沒有在 H 當然就是帶入 ϕ 看看是否送到 H'. 然而

$$\phi(g \cdot a \cdot g^{-1}) = \phi(g) \cdot \phi(a) \cdot \phi(g)^{-1}.$$

再因 $\phi(g) \in G'$, $\phi(a) \in H'$ 及 H' 是 G' 的 normal subgroup, 我們有

$$\phi(g) \cdot \phi(a) \cdot \phi(g)^{-1} \in H'.$$

故 $\phi(g \cdot a \cdot g^{-1}) \in H'$, 也就是說 $g \cdot a \cdot g^{-1} \in H$. 所以 H 是 G 的 normal subgroup. □

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

Remark 2.7.2. Correspondence Theorem 告訴我們說若 $\phi : G \to G'$ 是一個 epimorphism, 則在 G' 中任選一個 subgroup H' 都可在 G 中找到一個 subgroup H 使得 $\phi(H) = H'$, 而且 $\ker(\phi) \subseteq H$. 其實在 G 中符合 $\phi(H) = H'$ 及 $\ker(\phi) \subseteq H$ 的 subgroup 是唯一的. 假設 G 中有另一個 subgroup N 符合 $\phi(N) = H'$ 及 $\ker(\phi) \subseteq N$. 則對於所有 $a \in N$, 因 $\phi(a) \in \phi(N) = H'$, 故由假設 $\phi(H) = H'$ 知在 H 中必存在一元素 b 使得 $\phi(b) = \phi(a)$. 換句話說 $\phi(a) \cdot \phi(b)^{-1} = e'$. 由此得 $\phi(a \cdot b^{-1}) = e'$. 也就是說 $a \cdot b^{-1} \in \ker(\phi)$. 由此知 $a \in \ker(\phi) \cdot b$. 別忘了 $\ker(\phi) \subseteq H$ 且 $b \in H$ 故 $\ker(\phi) \cdot b \subseteq H$. 所以 $a \in H$, 也就是說 $N \subseteq H$. 用同樣的方法 (將 H 和 N 角色互換) 可得 $H \subseteq N$. 所以 $H = N$. 由上知真正的 Correspondence Theorem 是說:

若 $\phi : G \to G'$ 是一個 epimorphism, 則對於 G' 中任一 subgroup H', 在 G 中皆 '存在' "唯一" 的 subgroup H 使得 $\phi(H) = H'$ 且符合 $\ker(\phi) \subseteq H$.

不過在大學的代數中我們只要用到存在性而已, 所以我們不去強調唯一性.

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

Corollary 2.7.3. 假設 G 是一個 *group* 且 N 是 G 的一個 *normal subgroup.* 則對任意 G/N 中的 *subgroup* H' 都可在 G 中找到 *subgroup* H 符合 $N \subseteq H$ 且 $H/N = H'$.

當 H' 是 G/N 的 *normal subgroup* 時, 則 H 也會是 G 的 *normal subgroup.*

Proof. ϕ 是 group homomorphism 是因為

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

且

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

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

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

現在 Correspondence Theorem 中的條件都找到了, 所以利用 Theorem 2.7.1 知任取 G/N 中的一個 subgroup H', 在 G 中都可以找到一個 subgroup H 符合 $N = \ker(\phi) \subseteq H$ 且 $\phi(H) = H/N = H'$. □

有許多書也稱 Corollary 2.7.3 為 Correspondence Theorem. 它告訴我們 G/N 中的 subgroup 都是長 H/N 這種形式, 其中 H 是 G 的 subgroup 且 $N \subseteq H$. G/N 中的 normal subgroup 也是有 H/N 這種形式不過其中 H 是 G 的 normal subgroup.

最後我們想利用 Correspondence Theorem 來談談 Third Isomorphism Theorem 的一個特殊狀況. 令 K 是 G 的 normal subgroup, $\phi : G \to G/K$ 是定義成 $\phi(a) = \overline{a}$ 的 epimorphism. 任意 G/K 中的 normal subgroup N' 由前 Corollary 2.7.3 知是由 G 中的某一 normal subgroup N 利用 ϕ 得到: 也就是說 $N' = \phi(N) = N/K$. 故由 Theorem 2.6.5 我們有以下的定理通常也稱之為 Third Isomorphism Theorem.

Theorem 2.7.4 (Third Isomorphism Theorem)**.** *若 G 是一個 group, K 是 G 的一個 normal subgroup. 則 G/K 中的任一 normal subgroup 都是 N/K 這種形式, 其中 $K \subseteq N$ 且 N 是 G 的 normal subgroup. 而且我們有*

$$(G/K)/(N/K) \simeq G/N.$$

Proof. 任一 G/K 的 normal subgroup 都是 N/K 這種形式已在 Corollary 2.7.3 證得. 而

$$(G/K)/(N/K) \simeq G/N$$

可由 Theorem 2.6.5 直接得到. 也就是代: $G' = G/K$, $N' = N/K$. 此時可得 $N = \{a \in G \,|\, \phi(a) \in N'\}$. 故由 $G/N \simeq G'/N'$ 得證. □

Chapter 3

一些常見的 Groups

這一章中我們介紹一些常見的 groups: cyclic groups, abelian groups 和 symmetric groups.

3.1. Cyclic Groups

回顧一下, 一個 group G 是所謂的 cyclic group 就是在 G 中可以找到一個元素 $a \in G$ 使得 a 產生的 cyclic group $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$ 就是 G. 換句話說 G 中的元素都是 a^i 這種形式. Cyclic group 可以說是 group 中最簡單的一種. 其實我們可以知道所有的 cyclic groups 有哪些.

Theorem 3.1.1. *若 G 是一個 cyclic group. 則:*

(1) *若 G 的個數有無窮多 (infinite group), 則 $G \simeq \mathbb{Z}$.*

(2) *若 G 的個數有 n 個 (order 為 n), 則 $G \simeq \mathbb{Z}/n\mathbb{Z}$.*

Proof. 若 G 是 cyclic, 假設 G 可由 a 生成. 考慮 $\phi : \mathbb{Z} \to G$ 定義成 $\phi(i) = a^i$. 很容易看出

$$\phi(i+j) = a^{i+j} = a^i \cdot a^j = \phi(i) \cdot \phi(j).$$

所以 ϕ 是由 $\mathbb{Z}$ 這個加法 group 到 G 的 group homomorphism. 再加上 G 中的元素都是 a^i 這種形式所以可知 ϕ 是 onto 的. 既然 ϕ 是 epimorphism 我們就可以利用 First Isomorphism 定理 (Corollary 2.6.2).

(1) 若 G 是 infinite group. 我們欲證 ϕ 是一對一的. 由於 0 是 $\mathbb{Z}$ 的 identity, Lemma 2.5.6 告訴我們這等同於要證明 $\ker(\phi) = \{0\}$. 若 $m \in \ker(\phi)$, 則 $\phi(m) = a^m = e$. 若 $m \neq 0$, 則利用任何整數 i 都可寫成 $i = mh + r$ 的形式, 其中 $h \in \mathbb{Z}$, $0 \leq r < |m|$. 可得任何 G 中的元素 a^i 都可寫成

$$a^i = (a^m)^h \cdot a^r = e^h \cdot a^r = a^r.$$

換句話說 G 的元數都可寫成 a^r, 其中 $0 \le r < |m|$; 也就是說 G 最多只有 $|m|$ 個元素. 這和 G 有無窮多個元素相違背. 所以我們的假設 $m \neq 0$ 是不可能發生的. 不過 $\phi(0) = a^0 = e$, 故 $0 \in \ker(\phi)$. 因此得 $\ker(\phi) = \{0\}$.

(2) 若 G 是一個 cyclic group of order n, 由於 $G = \langle a \rangle$ 故 $\mathrm{ord}(a) = n$. 而 Lemma 2.3.2 告訴我們若 $a^m = e$ 則 $n \,|\, m$. 今若 $m \in \ker(\phi)$, 及 $\phi(m) = a^m = e$. 故由前述結果知 $n \,|\, m$: 也就是說 m 是 n 的倍數. 另一方面若 $m = nh$ 是 n 的倍數, 則 $\phi(m) = a^m = (a^n)^h = e$: 也就是說 $m \in \ker(\phi)$. 我們得到 $\ker(\phi)$ 是由 n 的倍數所成的集合. 因此 $\ker(\phi) = n\mathbb{Z}$. 故由 Corollary 2.6.2 知 $G \simeq \mathbb{Z}/n\mathbb{Z}$. □

Theorem 3.1.1 告訴我們說 cyclic groups 是可以用其個數來分類的. 也就是說給定一正整數 n 用 isomorphism 的觀點來看就只有一種 cyclic group 其 order 為 n, 但是要注意這並不表示沒有其他的 group 其 order 是 n. 然而若是給定的是一個質數 p, 那麼 Corollary 2.2.3 告訴我們的確只有一種 group 其 order 為 p, 就是 cyclic group $\mathbb{Z}/p\mathbb{Z}$. 事實上在證明 Corollary 2.2.3 時我們是利用 Lagrange's Theorem 知道當 $|G| = p$ 時除了 identity 及 G 本身外 G 不會有其他的 nontrivial proper subgroup. 反之下一個 Lemma 告訴我們如果 G 沒有 nontrivial proper subgroup, 則 G 一定是 cyclic group.

Lemma 3.1.2. 如果 G 是一個 *group* 且沒有 *nontrivial* 的 *nontrivial proper subgroup,* 則 G 一定是一個 *cyclic group* 且 $|G| = p$, 其中 p 為一個質數.

Proof. 任選 $a \in G$ 且 $a \neq e$, 則由 a 產生的 cyclic group $\langle a \rangle$ 是 G 的一個 subgroup. 不過由於 $\langle a \rangle \neq \{e\}$, 故由假設 G 沒有 nontrivial proper subgroup 知, $\langle a \rangle = G$. 另外若 $|G| = \mathrm{ord}(a)$ 不是質數, 即 $\mathrm{ord}(a) = mn$ 其中 $m > 1$ 且 $n > 1$, 則由 Proposition 2.3.3 知

$$\mathrm{ord}(a^m) = \frac{mn}{\gcd(mn, m)} = n,$$

也就是說 a^m 產生的 cyclic subgroup of G 其個數是 n. 故 $\langle a^m \rangle \neq \{e\}$ 且 $\langle a^m \rangle \neq G$. 換句話說 $\langle a^m \rangle$ 是 G 的 nontrivial proper subgroup. 這與假設不符, 故 G 的 order 是一個質數. □

若 G 是一個 cyclic group, 大家或許會猜它的 subgroup 應該也都是 cyclic group. 沒錯, 可是數學不能用猜的, 我們還是得給個證明.

Proposition 3.1.3. 若 G 是一個 *cyclic group,* 則 G 中任意的 *subgroup* 也是一個 *cyclic group.*

Proof. 假設 $G = \langle a \rangle$ 是一個 cyclic group, 且 H 是 G 中任意的一個 subgroup. 別忘了要證明 H 也是一個 cyclic group 就必須找一個元素可以產生 H. 要找甚麼元素呢? 當然要靠 a 來幫忙了.

如果 H 中的元素只有 identity e, 那當然 $H = \langle e \rangle$ 是一個 cyclic group. 如果 H 不是 $\langle e \rangle$, 由於 $H \subseteq G$, H 中的元素都是 a^i, $i \in \mathbb{Z}$ 這種形式, 我們一定可以找到

一個最小的正整數 n 滿足 $a^n \in H$. 我們要證明 $H = \langle a^n \rangle$. 由於 $a^n \in H$ 所以自然知 $\langle a^n \rangle \subseteq H$. 我們只剩下要說明 $H \subseteq \langle a^n \rangle$, 也就是說 H 中的元素都是 $(a^n)^h$, $h \in \mathbb{Z}$ 這種形式. 假設 $a^m \in H$, 我們利用整數的餘數定理, 知存在整數 h 及 r, 其中 $0 \leq r < n$ 使得 $m = n \cdot h + r$. 因此得

$$a^r = a^m \cdot (a^{nh})^{-1}.$$

不過由假設 $a^m \in H$ 且 $(a^{nh})^{-1} \in H$, 故知 $a^r \in H$. 但是我們已選 n 是最小的正整數滿足 $a^n \in H$, 而又 $0 \leq r < n$, 所以 $a^r \in H$ 表示 $r = 0$. 因此我們得證 H 中的元素都是 $(a^n)^h$ 這種形式. □

3.2. Direct Product

若給定兩個(或更多) groups, 在這節中我們將介紹一種方法可以利用這些 groups 創造出新的 group. 這個方法稱之為 direct product.

Definition 3.2.1. 給定兩 groups, G_1 和 G_2, 則定義

$$G_1 \times G_2 = \{(a_1, a_2) \,|\, a_1 \in G_1,\, a_2 \in G_2\}.$$

若 $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$, 則定義其乘法為

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2).$$

我們稱 $G_1 \times G_2$ 為 G_1 和 G_2 的 *direct product*.

事實上利用上述的乘法 $G_1 \times G_2$ 是一個 group. 其中封閉性和結合率可以用原來 G_1 和 G_2 的封閉性與結合濾輕鬆得證. 什麼會是 $G_1 \times G_2$ 的 identity 呢? 若 e_1 和 e_2 分別是 G_1 和 G_2 的 identity, 應該很容易看出 (e_1, e_2) 就是 $G_1 \times G_2$ 的 identity 吧! 至於 (a_1, a_2) 的 inverse 是 (a_1^{-1}, a_2^{-1}) 直接相乘就可得知.

Proposition 3.2.2. 若 G_1 和 G_2 都是 *cyclic groups,* 且其 *order* 分別為 n 和 m.

(1) 若 n 和 m 互質, 則 $G_1 \times G_2$ 仍是一個 *cyclic group.*

(2) 若 n 和 m 不互質, 則 $G_1 \times G_2$ 不是 *cyclic group.*

Proof. 因 G_1 和 G_2 是 cyclic, 假設 G_1 和 G_2 分別是由 a 和 b 生成. 注意: 從定義知 $G_1 \times G_2$ 的 order 為 nm.

(1) 假設 n 和 m 互質, 要證明 $G_1 \times G_2$ 是 cyclic 我們只要證明 $G_1 \times G_2$ 中存在一元素其 order 為 nm. 因為如此一來, 這個元素生成的 group 和 $G_1 \times G_2$ 個數一樣多, 所以 $G_1 \times G_2$ 就可由其生成. 該找什麼元素呢? 讓我們試試 (a, b) 吧. 由 Lemma 2.3.1 要說 (a, b) 的 order 為 nm, 等同於說 nm 是最小的正整數使得

$$(a, b)^{nm} = (e_1, e_2).$$

首先觀察

$$(a, b)^{nm} = ((a^n)^m, (b^m)^n) = (e_1^m, e_2^n) = (e_1, e_2).$$

接著要說明 nm 是符合上式的最小的正整數. 假設 $(a,b)^r=(e_1,e_2)$, 則因 $(a,b)^r=(a^r,b^r)$, 故得 $a^r=e_1$ 且 $b^r=e_2$. 因 $\mathrm{ord}(a)=n$ 且 $\mathrm{ord}(b)=m$, 由 Lemma 2.3.2 知 $n\,|\,r$ 且 $m\,|\,r$. 然而由假設 n 和 m 互質可得 $nm\,|\,r$, 故若 r 是一個正整數使得 $(a,b)^r=(e_1,e_2)$ 則 $r\geq nm$. 由此證得 (a,b) 的 order 為 nm, 換句話說 $G_1\times G_2$ 是一個由 (a,b) 生成的 cyclic group.

(2) 假設 n 和 m 不互質, 令 l 為 n 和 m 的最小公倍數. 注意因 n 和 m 不互質, 此時 $l<nm$. 因 a 生成 G_1, 故 G_1 的元素都可寫成 a^i 這種形式. 同理 G_2 的元素都可寫成 b^j 這種形式. 因此 $G_1\times G_2$ 的元素都可寫成 (a^i,b^j) 這種形式. 考慮

$$(a^i,b^j)^l=(a^{il},b^{jl}).$$

因 l 是 n 的倍數, 故 $a^{il}=e_1$. 同理 $b^{jl}=e_2$. 也就是說 $(a^i,b^j)^l=(e_1,e_2)$. 由 Lemma 2.3.1 知 $G_1\times G_2$ 中的任一元素 (a^i,b^j) 其 order 小於或等於 l. 所以在 $G_1\times G_2$ 中找不到一個元素其 order 為 nm. 故 $G_1\times G_2$ 不可能是 cyclic. □

Corollary 3.2.3. *若 m, n 互質, 則*

$$\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}\simeq\mathbb{Z}/(nm)\mathbb{Z}.$$

Proof. 由 Proposition 3.2.2 知 $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ 是一個 cyclic group. 然而 $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ 的 order 為 nm, 故由 Theorem 3.1.1 知其和 $\mathbb{Z}/(nm)\mathbb{Z}$ isomorphic. □

由 Proposition 3.2.2 知道兩個 cyclic groups 的 direct product 並不一定會依然是 cyclic, 所以 direct product 確實能幫我們產生新的 group. 以後我們可以看到所有的 finite abelian group 都可以用 cyclic groups 作 direct product 得到.

接下來我們來看看一個 group 若是由其他的 groups 用 direct product 得到, 那麼這一個 group 會有甚麼特性? 若 G_1 和 G_2 是兩個 groups, 且 e_1 和 e_2 分別為其 identity. 若 $G'=G_1\times G_2$, 我們觀察 G' 中兩個很特別的集合:

$$N'=\{(a,e_2)\,|\,a\in G_1\}\quad\text{and}\quad M'=\{(e_1,b)\,|\,b\in G_2\}.$$

很容易就可檢查出 N' 和 M' 都是 G' 的 subgroups. 事實上它們都是 G' 的 normal subgroups. 這是因為對於 G' 中的任一元素 (g_1,g_2), 由於 $g_1\in G_1$ 所以 若 $a\in G_1$ 則 $g_1\cdot a\cdot g_1^{-1}\in G_1$, 因此

$$(g_1,g_2)\cdot(a,e_2)\cdot(g_1,g_2)^{-1}=(g_1\cdot a\cdot g_1^{-1},g_2\cdot e_2\cdot g_2^{-1})=(g_1\cdot a\cdot g_1^{-1},e_2)\in N'.$$

同理

$$(g_1,g_2)\cdot(e_1,b)\cdot(g_1,g_2)^{-1}\in M'.$$

我們也很容易看出 $N'\simeq G_1$: 這是因為考慮函數 $\pi_1:N\to G_1$ 定為 $\pi_1((a,e_2))=a$, 則不難看出 π_1 是一個 group isomorphism. 同理可得 $M'\simeq G_2$. 另外 N' 和 M' 的特點是

$$G=N'\cdot M'\quad\text{and}\quad N'\cap M'=\{(e_1,e_2)\}.$$

因為 G' 中的元素都是 (g_1, g_2) 這種形式, 其中 $g_1 \in G_1$, $g_2 \in G_2$. 然而 $(g_1, e_2) \in N'$ 且 $(e_1, g_2) \in M'$, 故

$$(g_1, g_2) = (g_1, e_2) \cdot (e_1, g_2) \in N' \cdot M'.$$

另一方面若 $(g_1, g_2) \in N' \cap M'$, 則由 $(g_1, g_2) \in N'$ 得 $g_2 = e_2$, 再由 $(g_1, g_2) \in M'$ 得 $g_1 = e_1$. 故知 $\{(e_1, e_2)\} = N' \cap M'$.

Theorem 3.2.4. $G \simeq G_1 \times G_2$ 若且為若 G 中存在兩個 *normal subgroups* N 和 M 符合以下條件

(1) $N \simeq G_1$ 且 $M \simeq G_2$.

(2) $G = N \cdot M$

(3) $N \cap M = \{e\}$, 其中 e 是 G 的 *identity.*

Proof. 利用前面所定的 N' 及 M', 我們知 N' 和 M' 是 $G_1 \times G_2$ 的 normal subgroups, 且 $N' \simeq G_1$ 及 $M' \simeq G_2$. 我們也知 $G_1 \times G_2 = N' \cdot M'$ 及 $N' \cap M' = \{(e_1, e_2)\}$.

假設 $\phi : G \to G_1 \times G_2$ 是一個 isomorphism. 則令

$$N = \{a \in G \,|\, \phi(a) \in N'\} \quad \text{and} \quad M = \{b \in G \,|\, \phi(b) \in M'\}.$$

由 Correspondence 定理 (Theorem 2.7.1), 知 N 和 M 都是 G 的 normal subgroups, 又 $N/\ker(\phi) \simeq N'$ 且 $M/\ker(\phi) \simeq M'$. 但因 ϕ 是一對一, 故由 Lemma 2.5.6 得 $\ker(\phi) = \{e\}$. 因此

$$N \simeq N' \simeq G_1 \quad \text{and} \quad M \simeq M' \simeq G_2.$$

再來對於所有 $x \in G$, 我們得 $\phi(x) \in G_1 \times G_2$, 但因 $G_1 \times G_2 = N' \cdot M'$, 故知 $\phi(x) = N' \cdot M'$. 也就是說存在 $n' \in N'$ 和 $m' \in M'$ 使得 $\phi(x) = n' \cdot m'$. 但因 ϕ 是 onto 的故存在 $n \in N$ 和 $m \in M$ 使得 $\phi(n) = n'$ 且 $\phi(m) = m'$. 換句話說:

$$\phi(x) = \phi(n) \cdot \phi(m) = \phi(n \cdot m).$$

然而 ϕ 是一對一的故上式得 $x = n \cdot m$. 我們得 G 中的任一元素都可寫成 $n \cdot m$ 這種形式, 其中 $n \in N$, $m \in M$. 換句話說

$$G = N \cdot M.$$

最後, 若 $x \in N \cap M$, 則由 $x \in N$ 得 $\phi(x) \in N'$, 再由 $x \in M$ 得 $\phi(x) \in M'$. 也就是 $\phi(x) \in N' \cap M'$. 然而已知 $N' \cap M'$ 是 $G_1 \times G_2$ 的 identity, 故知 $x \in \ker(\phi)$. 再由 $\ker(\phi) = \{e\}$ 知 $x = e$. 故得證

$$N \cap M = \{e\}.$$

反知若 G 中存在兩個 normal subgroup N 和 M 滿足 (1), (2), (3). 考慮函數 $\psi : G \to N \times M$ 定義成: 若 $x = n \cdot m \in G$, 其中 $n \in N$ 和 $m \in M$, 則 $\psi(x) = (n, m)$. 這裡要注意 ψ 是否為 well-defined function? G 中的任一元素由於 $G = N \cdot M$, 確實可以寫成 $n \cdot m$ 這種形式, 不過寫法唯一嗎? 萬一不唯一, 即 $x = n \cdot m = n' \cdot m'$,

其中 $n \neq n'$ 或 $m \neq m'$, 則 $\psi(x) = (n, m)$ 又等於 (n', m') 表示 ψ 是一對多, 那就不是好函數了. 事實上這種寫法是唯一的: 這是因為若 $n \cdot m = n' \cdot m'$ 其中 $n, n' \in N$, $m, m' \in M$. 則

$$n'^{-1} \cdot n = m' \cdot m^{-1}.$$

然而 $n'^{-1} \cdot n \in N$ 且 $m' \cdot m^{-1} \in M$, 故知

$$n'^{-1} \cdot n \in N \cap M.$$

再利用假設 $N \cap M = \{e\}$ 知 $n'^{-1} \cdot n = e$, 也就是說 $n = n'$. 同理可得 $m = m'$. 所以寫法唯一. 好了! 既然 ψ 是一個好函數, 我們接下來證 ψ 是一個 group homomorphism. 也就是若 $x = n \cdot m$, $x' = n' \cdot m'$ 其中 $n, n' \in N$ 且 $m, m' \in M$, 則要證明 $\psi(x \cdot x') = \psi(x) \cdot \psi(x')$. 不過

$$\psi(x) \cdot \psi(x') = (n, m) \cdot (n', m') = (n \cdot n', m \cdot m'),$$

如果我們能證明 $x \cdot x' = (n \cdot n') \cdot (m \cdot m')$, 則由於 $n \cdot n' \in N$ 且 $m \cdot m' \in M$, 故利用 ψ 的定義我們有

$$\psi(x \cdot x') = (n \cdot n', m \cdot m').$$

因此得 $\psi(x \cdot x') = \psi(x) \cdot \psi(x')$. 換句話說要證明 ψ 是一個 group homomorphism 等於要證

$$(n \cdot m) \cdot (n' \cdot m') = (n \cdot n') \cdot (m \cdot m').$$

利用結合率

$$(n \cdot m) \cdot (n' \cdot m') = n \cdot (m \cdot n') \cdot m'$$

且

$$(n \cdot n') \cdot (m \cdot m') = n \cdot (n' \cdot m) \cdot m',$$

也就是說我們只要證明 $m \cdot n' = n' \cdot m$ 就可. 要怎麼證 $m \cdot n' = n' \cdot m$ 呢? 我們知 $a = b$ 若且為若 $a \cdot b^{-1} = e$. 所以我們考慮

$$(m \cdot n') \cdot (n' \cdot m)^{-1} = m \cdot n' \cdot m^{-1} \cdot n'^{-1}.$$

然而 $m \cdot n' \cdot m^{-1} \in N$ (這是因為 $n' \in N$ 且 N 是 G 的 normal subgroup), 我們有

$$m \cdot n' \cdot m^{-1} \cdot n'^{-1} = (m \cdot n' \cdot m^{-1}) \cdot n'^{-1} \in N.$$

同理利用 M 是 G 的 normal subgroup, 我們有

$$m \cdot n' \cdot m^{-1} \cdot n'^{-1} = m \cdot (n' \cdot m^{-1} \cdot n'^{-1}) \in M.$$

因此知

$$(m \cdot n') \cdot (n' \cdot m)^{-1} \in N \cap M.$$

再利用 $N \cap M = \{e\}$ 得 $(m \cdot n') \cdot (n' \cdot m)^{-1} = e$, 也就是說 $m \cdot n' = n' \cdot m$. 最後我們證 ψ 是 1-1 and onto. 若 $x \in \ker(\psi)$, 也就是說 $\psi(x)$ 是 $N \times M$ 中的 identity (e, e) (別忘了 e 是 G 的 identity 所以當然是 N 和 M 的 identity). 因 $x \in G$ 故存在 $n \in N$, $m \in M$ 使得 $x = n \cdot m$. 由此得 $\psi(x) = (n, m) = (e, e)$. 也就是說 $n = e$ 且 $m = e$, 故 $x = e \cdot e = e$. 得證 $\ker(\psi) = \{e\}$ 故 ψ 是一對一. 要證明 ψ 是

onto, 我們必須任取 $N \times M$ 中的任一元素 (n, m), 然後說 G 中存在一元素 x 使得 $\psi(x) = (n, m)$. 我們只要令 $x = n \cdot m$ 即可, 因為由定義此時 $\psi(x) = (n, m)$. 好了我們證得 ψ 是一個 isomorphism 故

$$G \simeq N \times M.$$

不過我們不是該證 $G \simeq G_1 \times G_2$ 嗎? 沒關係, 因為由假設 $N \simeq G_1$ 且 $M \simeq G_2$, 利用下一個 Lemma, 我們就可知

$$G \simeq N \times M \simeq G_1 \times G_2.$$

□

Lemma 3.2.5. 若 $G_1 \simeq G_1'$ 且 $G_2 \simeq G_2'$ 則

$$G_1 \times G_2 \simeq G_1' \times G_2'.$$

Proof. 由假設我們之存在 isomorphisms: $\phi_1 : G_1 \to G_1'$, 且 $\phi_2 : G_2 \to G_2'$. 定義新的函數 $\phi : G_1 \times G_2 \to G_1' \times G_2'$, 使得對所有的 $(g_1, g_2) \in G_1 \times G_2$,

$$\phi((g_1, g_2)) = (\phi_1(g_1), \phi_2(g_2)).$$

因為 $\phi_1(g_1) \in G_1'$, $\phi_2(g_2) \in G_2'$, ϕ 真的把 $G_1 \times G_2$ 的元素送到 $G_1' \times G_2'$. 利用 ϕ_1 和 ϕ_2 是 group homomorphism, 我們很容易驗證 ϕ 也是一個 group homomorphism.

ϕ 是 onto 的嗎? 若 $(y_1, y_2) \in G_1' \times G_2'$, 即 $y_1 \in G_1'$ 且 $y_2 \in G_2'$, 則因 ϕ_1 和 ϕ_2 是 onto, 故存在 $x_1 \in G_1$ 且 $x_2 \in G_2$ 使得 $\phi_1(x_1) = y_1$ 且 $\phi_2(x_2) = y_2$. 故選 $(x_1, x_2) \in G_1 \times G_2$, 則

$$\phi((x_1, x_2)) = (\phi_1(x_1), \phi_2(x_2)) = (y_1, y_2).$$

所以 ϕ 是 onto.

什麼是 $\ker(\phi)$ 呢? 若 $(a, b) \in \ker(\phi)$, 因 $G_1' \times G_2'$ 的 identity 是 (e_1', e_2'), 其中 e_1' 和 e_2' 分別是 G_1' 和 G_2' 的 identity, 故得

$$\phi((a, b)) = (\phi_1(a), \phi_2(b)) = (e_1', e_2').$$

由此知 $\phi_1(a) = e_1'$ 且 $\phi_2(b) = e_2'$. 換句話說 $a \in \ker(\phi_1)$ 且 $b \in \ker(\phi_2)$. 然而 ϕ_1 和 ϕ_2 由假設都是一對一的, 故 $\ker(\phi_1) = \{e_1\}$ 且 $\ker(\phi_2) = \{e_2\}$, 其中 e_1 和 e_2 分別是 G_1 和 G_2 的 identity. 故得 $a = e_1$, $b = e_2$, 換句話說 $\ker(\phi)$ 是 $G_1 \times G_2$ 的 identity, 故由 Lemma 2.5.6 知 ϕ 是一對一的. 因而得證 ϕ 是一個 isomorphism, 即

$$G_1 \times G_2 \simeq G_1' \times G_2'.$$

□

我們已了解兩個 group 的 direct product 相關的性質, 其實兩個 groups G_1 和 G_2 的 direct product $G_1 \times G_2$ 仍是一個 group 所以還可以和第三個 group G_3 作 direct product 得 $(G_1 \times G_2) \times G_3$. 這樣一直推演下去, 可以得到任意 n 個 groups 的 direct product.

3.3. Finite Abelian Groups

這一節我們討論另一種簡單的 groups, abelian groups. 回憶一下所謂 G 是一個 abelian group 表示 G 中的任意兩元素 a 和 b 都滿足 $a \cdot b = b \cdot a$.

3.3.1. Cauchy and Sylow's Theorems for finite abelian groups. G 是 abelian 最好的地方是 G 的任意的 subgroup 都是 normal. 所以很多有關 abelian groups 的性質我們都可以在 G 中找到一個 subgroup 然後再做 quotient group 這樣新的 group 的 order 變小了, 我們就可以用數學歸納法.

要用這種取 quotient group 的數學歸納法一般來說會牽扯上 Correspondence 定理 (忘記這是什麼的同學趕快退回去看一下 Corollary 2.7.3), 另外就是考慮 $\mathrm{ord}(a)$ 和 $\mathrm{ord}(\overline{a})$ 的關係了. 下一個 Lemma 就是告訴我們這個關係, 要注意的是這個 Lemma 並不需要 abelian 的假設:

Lemma 3.3.1. *若 N 是 group G 的一個 normal subgroup, $a \in G$. 考慮 $\overline{a} \in G/N$,* 則

$$\mathrm{ord}(\overline{a}) \,|\, \mathrm{ord}(a).$$

而且 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$ 若且為若

$$N \cap \langle a \rangle = \{e\}.$$

Proof. 假設 $\mathrm{ord}(a) = n$. 則因 $a^n = e$ 得 $\overline{a}^n = \overline{a^n} = \overline{e}$, 故由 Lemma 2.3.2 知 $ord(\overline{a}) \,|\, n$.

假設 $\mathrm{ord}(\overline{a}) = m$. 今若 $N \cap \langle a \rangle = \{e\}$, 則因 $\overline{a}^m = \overline{e}$ 表示 $a^m \in N$, 所以得 $a^m \in N \cap \langle a \rangle = \{e\}$. 換句話說 $a^m = e$, 再由 Lemma 2.3.2 得 $\mathrm{ord}(a) = n \,|\, m$. 然而前已知 $m \,|\, n$, 所以 $n = m$: 也就是說如果 $N \cap \langle a \rangle = \{e\}$, 則 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$.

反之, 假設 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$. 若 $x \in N \cap \langle a \rangle$, 由 $x \in \langle a \rangle$ 知: 存在一整數 i 使得 $x = a^i$. 不過又由 $x \in N$, 知 $\overline{a}^i = \overline{x} = \overline{e}$. 由此知 $\mathrm{ord}(\overline{a}) \,|\, i$. 然而由假設 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$ 得 $\mathrm{ord}(a) \,|\, i$, 因此得證 $x = a^i = e$. 也就是說若 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$ 則 $N \cap \langle a \rangle = \{e\}$. □

以下就是利用數學歸納法來證明一些 abelian groups 的性質的例子:

Theorem 3.3.2 (Cauchy's Theorem for Abelian Groups)**.** *若 G 是一個 finite abelian group, p 是一個質數, 且 p 整除 G 的 order,* 則 *G 中存在一個元素其 order 為 p.*

Proof. 前面提過我們要用 induction 來證明此定理. 如何用 induction 呢? 我們將對所有的 finite abelian group 的 order 作 induction. 也就是我們將證明這個定理對 order 為 p 的 abelian group 是對的. 然後利用歸納法假設對 order 小於 pk 的 abelian group 也對, 來證出對於 order 為 pk 的 abelian group 也對.

假設 G 的 order 為 p, 由 Corollary 2.2.3 知 G 是一個 cyclic group, 所以若 $a \in G$ 使得 $G = \langle a \rangle$, 則 $\mathrm{ord}(a) = p$.

現在假設對於所有的 abelian group G' 如果 $|G'| = pr$ 且 $r < k$, 則存在 $a \in G'$ 使得 $\text{ord}(a) = p$. 若 $|G| = pk$, 則有以下三種狀況:

(1) G 中無 nontrivial proper subgroup.

(2) G 中有一 nontrivial proper subgroup H 且 p 整除 $|H|$.

(3) G 中所有的 nontrivial proper subgroup 其 order 都不能被 p 整除.

如果是狀況 1. 則由 Lemma 3.1.2 知 $|G| = p$, 這情形已證過. 如果是狀況 2. 則因 H 是 nontrivial proper subgroup 故 $|H| < |G|$, 而 p 整除 $|H|$ 故 $|H| = pr$, 其中 $r < k$. 故由 induction 的假設之存在 $a \in H \subset G$ 且 $\text{ord}(a) = p$. 所以在這情況也得證. 我們真正得處理的就是狀況 3. 在這情況之下我們任取一個 G 的 nontrivial proper subgroup H, 然後考慮 G/H 這個 quotient group (別忘了在此我們用到 G 是 abelian 故 H 是 normal). 由於 $p \nmid |H|$, 所以 p 整除 $|G/H| = |G|/|H|$. 再加上 G/H 仍是 abelian group 且 $|G/H| < |G|$ 所以我們可以套用 induction 的假設在 G/H 上, 也就是存在 $\overline{a} \in G/H$ 且 $\text{ord}(\overline{a}) = p$. 現在我們利用前面的 Lemma 3.3.1 知 $p \,|\, \text{ord}(a)$; 也就是存在正整數 t 使得 $\text{ord}(a) = pt$. 利用 Proposition 2.3.3 得

$$\text{ord}(a^t) = \frac{pt}{\gcd(pt, t)} = p.$$

得證在 G 中存在一元素 a^t 其 order 為 p. □

這裡要強調這裡我們證的 Cauchy's Theorem 是利用 G 是 abelian 的假設下證明, 雖然這一個證明對 G 不是 abelian 時並不適用, 不過將來我們會用另外的方法證明一般的 Cauchy's Theorem. 也就是說這個定理在 G 不是 abelian 時仍是對的.

我們可以用類似的方法證以下的定理:

Theorem 3.3.3 (Sylow's Theorem for Abelian Groups)**.** *若 G 是一個 finite abelian group, 且 $|G| = p^n m$, 其中 p 是質數且 $p \nmid m$, 則在 G 中存在一個 subgroup P 其 order 為 p^n.*

Proof. 我們用類似前面 Theorem 3.3.2 的 induction. 當 $|G| = pm$ 時, Theorem 3.3.2 告訴我們存在 $a \in G$ 其 order 為 p, 故此時取 $P = \langle a \rangle$ 即可.

現在假設當 $|G'| = p^r m$, $r < n$ 時, 在 G' 中可找到 subgroup P' 其 order 為 p^r. 當 $|G| = p^n m$ 時, 由 Theorem 3.3.2 知存在 G 的 subgroup N 其 order 為 p. 因 G 是 abelian 故 N 是 G 的 normal subgroup, 故考慮 G/N 這一個 quotient group. G/N 的 order 是 $|G|/|N| = p^{n-1}m$. 故由 induction 的假設知在 G/N 中存在一個 subgroup P' 其 order 為 p^{n-1}. 再利用 Correspondence 定理 (Corollary 2.7.3) 知 G 中存在一 subgroup P 使得 $P' = P/N$. 然而 $|P| = |P'| \cdot |N| = p^{n-1} \cdot p = p^n$, 故得證. □

若 p 是一個質數, 而一個 group 的個數是 p^n 這種形式時, 我們稱這種 group 為一個 *p-group*. 當 G 的個數是 $p^n m$, 其中 p 和 m 互質時, 若 G 中的 subgroup H

其 order 又剛好是 p^n, 則稱 H 是 G 的一個 *Sylow p-subgroup*. Theorem 3.3.3 告訴我們當 G 是一個 abelian group 時, 其 Sylow p-subgroup 一定存在. 以後我們也會學到在一般的 group 中 Sylow p-subgroup 也一定存在, 這就是所謂的 Sylow 定理.

3.3.2. 一些 abelian groups 特有的性質. 現在我們來探討一些在一般 groups 不一定對但在 abelian groups 會對的一些性質.

當 G 是 abelian 時, 任取 $a, b \in G$, 因 $a \cdot b = b \cdot a$ 我們可以得

$$(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) = a \cdot (b \cdot a) \cdot b = a \cdot (a \cdot b) \cdot b = a^2 \cdot b^2.$$

利用數學歸納法我們很容易知對所有的 $n \in \mathbb{N}$,

$$(a \cdot b)^n = a^n \cdot b^n.$$

以下的 Lemma 告訴我們 G 是 abelian 的另一個好處:

Lemma 3.3.4. *若 G 是一個 finite abelian group, m 是一個大於 1 的整數且 m 整除 G 的 order. 考慮集合 $M = \{g \in G \,|\, g^m = e\}$. 則 M 是 G 的一個 subgroup 且 $M \neq \{e\}$.*

Proof. 因 $m > 1$ 故必存在一質數 p 使得 $p \,|\, m$. 由 Theorem 3.3.2 知存在一元素 $a \in G$ 其 order 為 p. 故知 $a \neq e$ 且 $a^p = e$, 但 $p \,|\, m$ 故 $a^m = e$. 也就是 $a \in M$ 故 $M \neq \{e\}$.

現在證 M 是 G 的 subgroup. 首先證封閉性: 若 $a, b \in M$, 即 $a^m = e$, $b^m = e$. 故 $(a \cdot b)^m = a^m \cdot b^m = e$, 也就是說 $a \cdot b \in M$. 接下來證反元素存在: 若 $a \in M$, 因 $a^m = e$ 故 $(a^m)^{-1} \cdot a^m = (a^m)^{-1} = (a^{-1})^m$. 然而又 $(a^m)^{-1} \cdot a^m = e$, 故 $(a^{-1})^m = e$. 也就是說 $a^{-1} \in M$. □

別忘了因 G 是 abelian 所以 M 會是 G 的一個 normal subgroup, 利用這一點我們可以得到以下有關 finite abelian group 非常重要的性質.

Lemma 3.3.5. *設 G 是一個 finite abelian group, 且 $|G| = p^n m$, 其中 $p \nmid m$. 令*

$$P = \{g \in G \,|\, g^{p^n} = e\} \quad \text{and} \quad M = \{g \in G \,|\, g^m = e\},$$

則

$$G \simeq P \times M.$$

Proof. 由 Lemma 3.3.4 知 P 和 M 都是 G 的 normal subgroups. 要證明 $G \simeq P \times M$, 我們得利用 Theorem 3.2.4 證明 $G = P \cdot M$ 及 $P \cap M = \{e\}$ 就好. 這兩個性質都要用到 p^n 和 m 互質來得到.

因為 p^n 和 m 互質, 故存在整數 r 和 s 使得 $rp^n + sm = 1$. 因此對任意的 $a \in G$, 我們都可寫成

$$a = a^{rp^n + sm} = a^{sm} \cdot a^{rp^n}.$$

因為

$$((a^{sm})^{p^n} = (a^{p^n m})^s,$$

而 $|G| = p^n m$, 由 Corollary 2.3.4 知

$$(a^{sm})^{p^n} = e;$$

也就是說 $a^{sm} \in P$. 同理知 $a^{rp^n} \in M$. 由此知任意的 G 中元素都可寫成一個 P 中的元素乘以 M 中的元素, 所以 $G = P \cdot M$.

另一方面, 若 $g \in P \cap M$, 因 $g \in M$, 故 $g^m = e$. 則由 Lemma 2.3.2 知 $\mathrm{ord}(g) \,|\, m$. 同理得 $\mathrm{ord}(g) \,|\, p^n$. 也就是說 $\mathrm{ord}(g)$ 整除 g^n 和 m 的最大公因數. 但 g^n 和 m 互質, 故得 $\mathrm{ord}(g) = 1$; 也就是說 $g = e$. 因此得證 $P \cap M = \{e\}$. □

Lemma 3.3.5 中 P 元素的個數是多少呢? 雖然是收集所有 G 中元素 g 符合 $g^{p^n} = e$ 的元素但不表示其 order 就是 p^n. 不過很巧妙的利用 Cauchy 的定理我們確實可以得到 $|P| = p^n$.

Lemma 3.3.6. 設 G 是一個 *finite abelian group,* 且 $|G| = p^n m$, 其中 $p \nmid m$. 令

$$P = \{g \in G \,|\, g^{p^n} = e\},$$

則 P 是 G 的一個 *Sylow p-subgroup,* 而且 P 是 G 中唯一的 *Sylow p-subgroup.*

Proof. 首先我們說明若令 $M = \{g \in G \,|\, g^m = e\}$, 則 p 不能整除 M 的 order. 這是因為若 p 整除 M 的 order, 則由 Cauchy's Theorem 知 M 中存在一元素 a 其 order 為 p, 但 $a^m = e$, 由 Lemma 2.3.2 知 $p \,|\, m$. 這和假設 $p \nmid m$ 矛盾. 故 p 不能整除 $|M|$.

接下來我們證 P 是一個 p-group. 假設除了 p 以外存在另一質數 q 整除 $|P|$, 則用和前面相同的方法可得 $q \,|\, p^n$, 這又和 p, q 是相異質數矛盾. 換句話說 $|P|$ 除了 p 以外不會有其他的質因數, 所以知存在 $r \in \mathbb{N}$ 使得 $|P| = p^r$.

由 Lemma 3.3.5 知 $G \simeq P \times M$, 故 $|G| = |P| \cdot |M|$. 因此得

$$|M| = |G|/|P| = p^{n-r} m.$$

但 p 不整除 M, 故得 $n = r$. 也就是說 P 是 G 的一個 Sylow p-subgroup.

最後假設 P' 是 G 中任意的一個 Sylow p-subgroup. 因 $|P'| = p^n$, 由 Lagrange 定理(Corollary 2.3.4) 知對於所有 $a \in P'$, $a^{p^n} = e$. 也就是說 $a \in P$. 得證 $P' \subseteq P$. 然而 $|P'| = |P| = p^n$, 故 $P' = P$. 這證明了唯一性. □

這一次我們要強調 Lemma 3.3.6 是 abelian groups 特有的性質. 它告訴我們此時 Sylow p-subgroup 是長什麼樣子的, 而且是唯一的. 在一般的 group 這不一定是對的.

綜合以上幾個 Lemmas, 我們有以下的結論:

Proposition 3.3.7. 設 G 是一個 *finite abelian group,* 其 *order* 為

$$|G| = p_1^{n_1} \cdots p_r^{n_r},$$

其中 $p_1, \ldots, p_r$ 是相異的質數. 令 P_i 是 G 中對每一個 p_i 所對應的 *Sylow* p_i*-subgroup,* $i \in \{1, \ldots, r\}$. 則

$$G \simeq P_1 \times \cdots \times P_r.$$

Proof. 若令 $m = p_2^{n_2} \cdots p_r^{n_r}$, 且令 $M = \{g \in G \mid g^m = e\}$, 則由 Lemmas 3.3.5, 3.3.6 知 $G \simeq P_1 \times M$. 然而因 $|M| = p_2^{n_2} \cdots p_r^{n_r}$ 故由數學歸納法可知 $M \simeq P_2 \times \cdots \times P_n$. 因此由 Lemma 3.2.5 得

$$G \simeq P_1 \times M \simeq P_1 \times P_2 \times \cdots \times P_r.$$

□

3.3.3. Abelian p-groups. Proposition 3.3.7 告訴我們一個 finite abelian group 可以寫成一些 p-subgroups 的 direct product, 這些 p-subgroup 當然都還是 abelian. 因此若我們能了解 abelian p-groups, 則對於一般的 finite abelian groups 就完全清楚了.

大家都知道 cyclic group 一定是 abelian. 不過若只知一個 group 是 abelian 它並不一定會是 cyclic. 下一個 Lemma 告訴我們一個判斷 abelian group 是否為 cyclic 的方法.

Lemma 3.3.8. 若 G 是一個 *abelian p-group,* 且 $a \in G$ 是 G 中任一個 *order* 最大的元素. 則*:*

(1) 若 G 是 *cyclic* 則 $G = \langle a \rangle$.

(2) 若 G 不是 *cyclic* 則在 G 中存在 $b \notin \langle a \rangle$, 使得 $\mathrm{ord}(b) = p$.

Proof. 若 $|G| = p^n$, 由 Lagrange 定理 (Corollary 2.3.4) 知 $\mathrm{ord}(a) = p^r$, 其中 r 是一個正整數且 $r \leq n$.

(1) 若 G 是 cyclic, 即 G 中存在一元素 x 使得 $G = \langle x \rangle$. 也就是說 $\mathrm{ord}(x) = p^n$. 然而已知 a 是 G 中元素 order 最大的之一. 所以知 $\mathrm{ord}(a) = p^n$ (注意這個元素並不唯一, 所以我們並不可得 $x = a$). 換句話說 G 和 $\langle a \rangle$ 的元素個數一樣多, 即 $G = \langle a \rangle$.

(2) 若 G 不是 cyclic, 則當然 $\langle a \rangle \subsetneq G$. 記 $A = \langle a \rangle$. 可知 quotient group G/A 仍是一個 abelian p-group, 即 $|G/A| = p^{n-r}$. 利用 Cauchy 定理 (Theorem 3.3.2) 知存在 $\overline{x} \in G/A$ 使得 $\mathrm{ord}(\overline{x}) = p$. 也就是說 $\overline{x} \neq \overline{e}$ 不過 $\overline{x}^p = \overline{e}$, 因此 $x \notin A$ 但 $x^p \in A$. 因為 $A = \langle a \rangle$, $x^p \in A$ 表示存在一整數 i 使得 $x^p = a^i$. 我們用反證法證明 $p \mid i$.

如果 $p \nmid i$, 則由 Proposition 2.3.3 知

$$\mathrm{ord}(a^i) = \frac{p^r}{\gcd(p^r, i)} = p^r.$$

也就是說 $\mathrm{ord}(x^p) = \mathrm{ord}(a) = p^r$. 別忘了 $x \in G$, 而 G 是 p-group, 因此如前知 $\mathrm{ord}(x) = p^s$, 其中 s 是一正整數. 再用一次 Proposition 2.3.3 知

$$\mathrm{ord}(x^p) = \frac{p^s}{\gcd(p^s, p)} = p^{s-1}.$$

利用前面所求之 $\mathrm{ord}(x^p) = p^r$ 得 $s = r + 1$. 也就是說 $\mathrm{ord}(x) = p^s = p^{r+1}$. 別忘了當初我們假設 $\mathrm{ord}(a) = p^r$. $\mathrm{ord}(x) > \mathrm{ord}(a)$ 這和 a 的 order 是最大的相矛盾. 所以得證 $p \mid i$.

假設 $i = pt$, 令 $b = a^{-t} \cdot x$. 注意若 $b \in A$, 則因 $x = a^t \cdot b$, 會導致 $x \in A$, 這和 $x \notin A$ 相矛盾, 故知 $b \notin A$, 且當然 $b \neq e$ (因 $e \in A$). 然而因 G 是 abelian, $b^p = a^{-pt} \cdot x^p$. 利用 $pt = i$ 及 $a^i = x^p$, 我們推得 $b^p = e$. 由此可得 $\mathrm{ord}(b) = p$. 這是因為由 Lemma 2.3.2 知 $\mathrm{ord}(b) \mid p$. 但 p 是質數, 所以得 $\mathrm{ord}(b) = 1$ or $\mathrm{ord}(b) = p$. 然而已知 $b \neq e$ 即 $\mathrm{ord}(b) \neq 1$, 故可得 $\mathrm{ord}(b) = p$. □

下一個 Lemma 告訴我們如果一個 abelian p-group 不是 cyclic 那麼它在某種程度上和 cyclic group 還是相差不遠.

Lemma 3.3.9. *若 G 是一個 abelian p-group, 且 $a \in G$ 是 G 中任一個 order 最大的元素. 則要不然 G 是一個 cyclic group; 要不然就是在 G 中存在一個 subgroup Q 使得*

$$G \simeq \langle a \rangle \times Q.$$

Proof. 令 $A = \langle a \rangle$. 若 G 不是 cyclic 則由 Lemma 3.3.8 知存在 $b \in G$ 但 $b \notin A$ 使得 $\mathrm{ord}(b) = p$. 令 $B = \langle b \rangle$. 首先證明 $A \cap B = \{e\}$. 這是因為 $A \cap B$ 會是 B 的一個 subgroup. 利用 Lagrange 定理 (Theorem 2.2.2) 知 $A \cap B$ 的 order 需整除 B 的 order. 但 B 的 order 為質數 p, 故知 $|A \cap B| = 1$ 或 $|A \cap B| = p$. 若 $|A \cap B| = p$, 表示 $A \cap B = B$, 即 $B \subseteq A$. 這和 $b \notin A$ 不合. 因此 $A \cap B$ 的 order 不是 p. 故得 $|A \cap B| = 1$, 即 $A \cap B = \{e\}$.

接下來我們想用 B 來幫我們以數學歸納法證明這個 Lemma. 若 G 的 order 為 p, 由 Corollary 2.2.3 知 G 是一個 cyclic group. 若 $|G| = p^n$. 假設此 Lemma 在所有 order 小於 p^n 的 abelian p-groups 都對.

當然若 G 是 cyclic 則證明完成, 但 G 是有可能不是 cyclic 的. 若 G 不是 cyclic, 考慮 G/B 這一個 abelian group. 因 $|G/B| = p^{n-1}$, 故 G/B 是一個 order 小於 p^n 的 abelian p-group. 此時我們就可以用 induction 的假設, 不過要用這個假設我們得先在 G/B 中找到一個 order 最大的元素. 事實上 $\overline{a}$ 會是 G/B 中 order 最大的元素. 主要原因是由 Lemma 3.3.1 知對所有的 $\overline{x} \in G/B$, 都有 $\mathrm{ord}(\overline{x}) \leq \mathrm{ord}(x)$. 又因 $B \cap \langle a \rangle = \{e\}$ 故再由 Lemma 3.3.1 得 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$. 因為 a 是 G 中 order 最大的元素, 故得在 G/B 中對任意的 $\overline{x} \in G/B$ 皆有

$$\mathrm{ord}(\overline{a}) = \mathrm{ord}(a) \geq \mathrm{ord}(x) \geq \mathrm{ord}(\overline{x}).$$

現在我們可以套用歸納的假設了. 由假設知有可能 G/B 是 cyclic, 要不然在 G/B 中存在一個 subgroup Q' 使得 $G/B \simeq \langle \overline{a} \rangle \times Q'$.

若 G/B 是 cyclic, 由 Lemma 3.3.8 知 $G/B = \langle \overline{a} \rangle$. 此時我們要證明 $G \simeq \langle a \rangle \times B$. 由 Theorem 3.2.4 知這相當於要證明 $G = A \cdot B$ 且 $A \cap B = \{e\}$ (別忘了 A, B 都是 normal). 不過由於我們已證得 $A \cap B = \{e\}$, 所以只要證 $G = A \cdot B$. 對任意的 $x \in G$, 考慮 $\overline{x} \in G/B$. 則由於 $G/B = \langle \overline{a} \rangle$, 故存在一整數 i 使得 $\overline{x} = \overline{a}^i$. 這表示 x 和 a^i 在 B 的分類下是同類的. 也就是 $(a^i)^{-1} \cdot x \in B$. 換句話說存在一整數 j 使得 $x = a^i \cdot b^j$. 得證 G 中的元素都可寫成一個 A 中元素乘上一個 B 中元素的形式, 即 $G = A \cdot B$. 故加上 $A \cap B = \{e\}$ 得 $G \simeq A \times B$.

若 G/B 不是 cyclic 則由 induction 的假設知在 G/B 中存在一個 subgroup Q' 使得 $G/B \simeq \langle \overline{a} \rangle \times Q'$. 利用 Theorem 3.2.4 知此時 $G/B = \langle \overline{a} \rangle \cdot Q'$ 且 $\langle \overline{a} \rangle \cap Q' = \{\overline{e}\}$. 因為我們要把問題拉回到 G 來看, 利用 Correspondence 定理 (Corollary 2.7.3) 知在 G 中存在一個 subgroup Q 符合 $B \subseteq Q$ 且 $Q/B = Q'$. 我們要證明 $G \simeq \langle a \rangle \times Q$.

首先證 $G = A \cdot Q$. 任取 $x \in G$, 由於 $\overline{x} \in G/B$, 且 $G/B = \langle \overline{a} \rangle \cdot Q/B$, 故存在一整數 i 和 $q \in Q$ 使得

$$\overline{x} = \overline{a}^i \cdot \overline{q} = \overline{a^i \cdot q}.$$

也就是說 $(a^i \cdot q)^{-1} \cdot x \in B$. 因 $B = \langle b \rangle$, 由此知存在一整數 j 使得 $(a^i \cdot q)^{-1} \cdot x = b^j$. 換句話說 $x = a^i \cdot (q \cdot b^j)$. 然而 $a^i \in A$, 且 $q \cdot b^j \in Q$ (別忘了 $B \subseteq Q$). 故知 $G = A \cdot Q$.

最後要證 $A \cap Q = \{e\}$. 若 $x \in A \cap Q$, 由 $x \in A = \langle a \rangle$ 知 存在一整數 i 使得 $x = a^i$. 故在 G/B 中 $\overline{x} = \overline{a^i} = \overline{a}^i$. 另一方面 $a \in Q$ 故在 G/B 中 $\overline{x} \in Q/B = Q'$. 也就是說

$$\overline{x} \in \langle \overline{a} \rangle \cap Q' = \{\overline{e}\}.$$

由此知在 G/B 中 $\overline{x} = \overline{e}$, 也就是說 $x \in B$. 但一開始已假設 $x \in A \cap Q$, 當然有 $x \in A$. 所以得 $x \in A \cap B$. 別忘了我們已知 $A \cap B = \{e\}$, 故得 $x = e$. 也就是說 $A \cap Q = \{e\}$. □

Lemma 3.3.9 告訴我們什麼呢? 如果 G 是 abelian p-group, 且 $|G| = p^n$. 則有可能 G 是 cyclic group: 若是如此則由 Theorem 3.1.1 知 $G \simeq \mathbb{Z}/p^n\mathbb{Z}$. G 也有可能不是 cyclic, 那麼 Lemma 3.3.9 就告訴我們若 G 中 order 最大的元素其 order 是 p^{n_1}, 則存在一個 subgroup Q 使得 $G \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times Q$. 這裡因 G 是 abelian p-group, 其 subgroup Q 當然也是 abelian p-group. 如果 Q 是 cyclic, 那麼我們就可得 $G \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times Q \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times (\mathbb{Z}/p^{n_2}\mathbb{Z})$; 如果 Q 不是 cyclic 則再用一次 Lemma 3.3.9 知 Q 會 isomorphic to 一個 cyclic group 和 Q 的 subgroup 的 direct product. 這樣一直下去, 由於 G 的 order 是有限的經過有限次後一定會停. 我們可以有以下的結果:

Proposition 3.3.10. 如果 G 是一個 *abelian p-group,* 且 $|G| = p^n$. 則存在 $n_1, \ldots, n_r \in \mathbb{N}$ 符合 $n_1 + \cdots + n_r = n$ 使得

$$G \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{n_r}\mathbb{Z}).$$

Proof. 由前面的討論之 G 可以寫成一些 cyclic groups 的 direct product. 這些 cyclic groups 由於都是 G 的 subgroups, 所以也都是 p-group. 因此它們都會是 isomorphic to $\mathbb{Z}/p^{n_i}\mathbb{Z}$ 這種形式, 最後由於

$$p^n = |G| = |\mathbb{Z}/p^{n_1}\mathbb{Z}| \cdots |\mathbb{Z}/p^{n_r}\mathbb{Z}| = p^{n_1} \cdots p^{n_r},$$

我們知 $n = n_1 + \cdots + n_r$. □

3.3.4. Finite abelian groups 的基本定理. 既然每一個 finite abelian group 都可寫成一些 abelian p-groups 的 direct product, 而每一個 abelian p-group 也都可寫成一些 cyclic groups 的 direct product, 因此由這兩個結果我們可以說完整的掌握了 finite abelian groups.

Theorem 3.3.11 (Fundamental Theorem on Finite Abelian Groups)**.** 若 G 是一個 *finite abelian group,* 則 G 可以寫成一些 *cyclic groups* 的 *direct product.*

Proof. 由 Proposition 3.3.7 知 $G \simeq P_1 \times \cdots \times P_r$, 其中 P_i 都是某個質數 p_i 的 abelian p_i-group. 再由 3.3.10 知對所有的 P_i, 都可找到 cyclic groups $C_{i1}, \ldots C_{in_i}$ 使得 $P_i \simeq C_{i1} \times \cdots \times C_{in_i}$. 因此得證本定理. □

這裡很有趣的是我們都知道所有的 cyclic groups 長什麼樣子, 既然 finite abelian groups 都是 cyclic groups 的 direct product, 我們當然就知道所有的 finite abelian groups 長什麼樣子了. 比方說若 G 是一個 abelian group 且 $|G| = 6$, 那麼 G 有可能長什麼樣子呢? 由 Proposition 3.3.7 知 $G \simeq P_1 \times P_2$ 其中 P_1 的 order 是 2, P_2 的 order 是 3. 而 order 是 2 的 group 一定是 cyclic (Corollary 2.2.3) 故 $P_1 \simeq \mathbb{Z}/2\mathbb{Z}$. 同理 $P_2 \simeq \mathbb{Z}/3\mathbb{Z}$. 故 $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. 不過由 3.2.2 知 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$, 所以 $G \simeq \mathbb{Z}/6\mathbb{Z}$. 也就是所有的元素個數為 6 的 abelian group 都是 cyclic group. 相信大家不難利用這個例子推廣到以下的 Corollary:

Corollary 3.3.12. 若 G 是一個 *abelian group* 且 $|G| = p_1 \cdots p_r$ 其中 $p_1, \ldots p_r$ 是相異的質數, 則 G 是一個 *cyclic group.*

至於若 G 的 order 的質因數分解中存在高次方的話, 那麼問題就複雜一點了. 例如考慮 order 為 144 的 abelian group G. 因 $144 = 2^4 \cdot 3^2$, 由 Proposition 3.3.7 知 $G \simeq P_1 \times P_2$ 其中 P_1 的 order 是 2^4, P_2 的 order 是 3^2. 再由 Proposition 3.3.10 計算

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$$

知 P_1 有可能是 isomorphic to

$$(1)\ \mathbb{Z}/16\mathbb{Z} \quad \text{or} \quad (2)\ \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad (3)\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z},$$

$$(4)\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad (5)\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$

這五種情況. 同理 P_3 可能 isomorphic to

$$(1)\ \mathbb{Z}/9\mathbb{Z} \quad \text{or} \quad (2)\ \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$$

這兩種情況. 因此元素個數為 144 的 abelian groups 共有十種可能.

3.4. The Symmetric Group

這一節我們將討論一個複雜但重要的 group 稱之為 symmetric group.

3.4.1. The group $A(S)$ and Cayley's Theorem. 給定一集合 S 我們定義 $A(S)$ 是所有從 S 到 S 的 1-1 且 onto 的函數所成的集合. 若 $f, g \in A(S)$ 那麼它們的合成函數 $f\circ g$ 依然是 1-1 且 onto, 所以知 $f\circ g \in A(S)$. 因此我們就考慮合成 $\circ$ 為 $A(S)$ 中的運算. 前面已知這個運算有封閉性, 相信大家也知合成運算有結合率. 至於在這個運算之下 $A(S)$ 的 identity 是什麼呢? 當然就是所謂的 identity function I_S 了: I_S 是一個從 S 到 S 的函數它符合 $I_S(x) = x, \forall\, x \in S$. 而對任意的 $f \in A(S)$ 由 1-1 和 onto 的性質知存在 $g \in A(S)$ 使得 $f\circ g = g\circ f = I_S$ (即 g 是 f 的反函數), 所以知任何 $A(S)$ 的元素其 inverse 存在. 我們說明了 $A(S)$ 是一個 group. 下一個定理告訴我們為何 $A(S)$ 這一個 group 這麼重要.

Theorem 3.4.1 (Cayley's Theorem)**.** 給定任一個 *group* G, 則 G 會 *isomorphic to* $A(G)$ 的一個 *subgroup.*

Proof. 這裡我們先強調在 $A(G)$ 中我們僅將 G 視為一個集合, 所以 $A(G)$ 是從 G 到 G 的 1-1 和 onto 的函數所成的集合而不是 group homomorphism 所成的集合.

我們現在想定一個從 G 這一個 group 到 $A(G)$ 這一個 group 的 group homomorphism $\phi : G \to A(G)$. 對任意的 $a \in G$, 我們定義 $\phi(a) \in A(S)$ 這一個函數為 $T_a : G \to G$, 其中對於任意的 $x \in G$, $T_a(x) = a\cdot x$.

我們當然要檢查 ϕ 是不是一個 well-defined function. 這裡唯一要檢查的就是: 是否 $\phi(a) = T_a \in A(S)$? 由定義當然知道 T_a 是一個從 G 送到 G 的函數. 所以我們只要檢查是否 T_a 是一個 1-1 且 onto 的函數. 這裡千萬不要搞錯了, T_a 只是一個函數所以要證它是一對一的不能看 kernel (事實上 $\ker(T_a)$ 是無定義的). 給定任意的 $b \in G$, 要證明 T_a 是 1-1 且 onto 就是要證明 G 中存在唯一的元素 c 使得 $T_a(c) = b$. 然而 $T_a(x) = a\cdot x$, 故由 Theorem 1.2.3 知 T_a 是 1-1 且 onto.

接下來我們證明 $\phi : a \mapsto T_a$ 是一個從 G 到 $A(G)$ 的 group homomorphism. 也就是證對所有的 $a, b \in G$, $\phi(a\cdot b) = \phi(a)\circ\phi(b)$ (別忘了 $\phi(a)$ 和 $\phi(b)$ 是在 $A(G)$ 中所以它們間的乘法是 $\phi(a)\circ\phi(b)$). 要檢查 $\phi(a\cdot b)$ 和 $\phi(a)\circ\phi(b)$ 這兩個函數是否相

同, 就是要檢驗這兩個函數對定義域裡的每個元素取值是否相同. 因 $\phi(a\cdot b)=T_{a\cdot b}$ 故對所有的 $x\in G$, 皆有

$$T_{a\cdot b}(x)=(a\cdot b)\cdot x.$$

而 $\phi(a)\circ\phi(b)=T_a\circ T_b$, 故對所有的 $x\in G$, 皆有

$$T_a\circ T_b(x)=T_a(T_b(x))=T_a(b\cdot x)=a\cdot(b\cdot x).$$

因此由 G 的結合率知對所有的 $x\in G$, $T_{a\cdot b}(x)=T_a\circ T_b(x)$. 也就是說 $\phi(a\cdot b)=\phi(a)\circ\phi(b)$.

最後證 ϕ 是一對一的. 已證 ϕ 是 group homomorphism, 所以只要證 $\ker(\phi)=\{e\}$. 若 $a\in\ker(\phi)$, 即 $\phi(a)$ 為 $A(G)$ 的 identity I_G. 換句話說, 對所有的 $x\in G$ 皆有 $T_a(x)=x$. 但 $T_a(x)=a\cdot x$, 故得 $a=e$. 因此我們證得了 $G\simeq\mathrm{im}(\phi)$. 利用 Lemma 2.5.4 知 $\mathrm{im}(\phi)$ 是 $A(G)$ 的一個 subgroup, 故得證此定理. □

Cayley's Theorem 是想將抽象的 group 用具體的方法表示出來. 或許大家會疑惑: 原本 G 都不知是什麼樣子了, 用 $A(G)$ 來表示能告訴我們什麼訊息呢? 仔細想想 $A(G)$ 的結構, 它和 G 的 group 性質無關, 事實上只和 G 的個數有關. 換句話說當我們要了解有多少 order 為 n 的 group 時, 只要任選一個元素個數為 n 的集合 S, 再討論 $A(S)$ 中有多少個 order 為 n 的 subgroup 就好了 (因為 Cayley's Theorem 告訴我們所有的 order 為 n 的 group 必在其中). 可惜 $A(S)$ 這一個 group 經常是太大了. 有時是可以考慮小一點的集合 S', 不過這裡我們就不多做討論.

3.4.2. The symmetric group of degree n. 前面提過 $A(S)$ 這一個 group 只和 S 的元素個數有關. 今若 S 有 n 個元素, 那麼我們不妨考慮 $S=\{1,2,\ldots,n\}$ 這一個集合. 此時我們將 $A(S)$ 也就是從 $\{1,2,\ldots,n\}$ 到 $\{1,2,\ldots,n\}$ 所有 1-1 且 onto 的函數所成的集合特別記做 S_n, 稱之為 the *symmetric group of degree* n. Cayley's Theorem 告訴我們所有 order 為 n 的 group 都會 isomorphic 到 S_n 的某一個 subgroup, 所以研究 S_n 顯得特別重要.

從 $\{1,2,\ldots,n\}$ 到 $\{1,2,\ldots,n\}$ 所有 1-1 且 onto 的函數到底有多少個呢? 相信大家在高中都已學過了. 先考慮 1 可以送到什麼? 結果有 n 種選擇, 不過因 1 已選擇去哪個數了, 因要求一對一, 2 只剩下 $n-1$ 個選擇. 由此繼續下去我們得知 S_n 的 order.

Lemma 3.4.2.

$$|S_n|=n\cdot(n-1)\cdots2\cdot1=n!.$$

一般談 S_n 我們是不談 $n=1$ 和 $n=2$ 的狀況: 因 S_1 只有一個元素, 所以只有 identity. 而 S_2 只有 2 個元素, 一定是 cyclic. 所以我們以後只談 $n\geq3$ 的狀況.

要討論 S_n 我們當然要想個法子將其元素表示出來. 例如在 S_5 中若 σ 是將 $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, $4 \mapsto 5$ 及 $5 \mapsto 4$, 則我們可以用

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \tag{3.1}$$

來表示. 而

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \tag{3.2}$$

表示 τ 將 $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 5$, $4 \mapsto 1$ 且 $5 \mapsto 2$. 那麼 $\sigma \circ \tau$ 是甚麼呢? 因為 τ 將 $1 \mapsto 3$, 而 σ 將 $3 \mapsto 1$ 所以合成起來得 $\sigma \circ \tau$ 將 $1 \mapsto 1$. 而 τ 將 $2 \mapsto 4$, σ 將 $4 \mapsto 5$ 故 $\sigma \circ \tau$ 將 $2 \mapsto 5$. 同理一個一個計算下去我們可得

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix} \tag{3.3}$$

同理考慮 $\tau \circ \sigma$ 可得

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} \tag{3.4}$$

由式子 (3.3) 和 (3.4) 知 $\sigma \circ \tau \neq \tau \circ \sigma$ 所以 S_5 不是 abelian. 事實上對於所有的 $n \geq 3$, S_n 都不是 abelian.

當 $\sigma, \tau \in S_n$, 由於 σ, τ 都是函數, 其乘法就是函數的合成. 為了方便起見以後我們不再用 $\sigma \circ \tau$ 表示其合成而用 $\sigma \cdot \tau$ 取代.

3.4.3. Disjoint cycle decomposition. 用如式子 (3.1) 的方法表示 S_n 的元素有時稍嫌麻煩. 我們介紹一個簡便的表示法. 這個方法稱為 cycle 表示法. 它不只使用簡便, 而且許多 S_n 的性質都可利用這方法簡單求得. 可以說是相當的重要.

Definition 3.4.3. 令 $i_1, i_2 \ldots, i_k$ 是在 $\{1, 2, \ldots, n\}$ 中 k 個相異整數. 我們用

$$(i_1\ i_2\ \cdots\ i_k)$$

表示 S_n 中的一個元素 σ 將 $s \in \{1, 2, \ldots, n\}$ 送到

$$\sigma(s) = \begin{cases} i_{j+1}, & \text{若 } s = i_j \text{ 且 } 1 \leq j \leq k-1; \\ i_1, & \text{若 } s = i_k; \\ s, & \text{若 } s \notin \{i_1, \ldots, i_k\}. \end{cases}$$

換句話說 σ 將 $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$, 而將 i_k 送回 i_1, 而將 $i_1, \ldots, i_k$ 以外的元素原封不動.

我們稱 $(i_1\ i_2\ \cdots\ i_k)$ 是一個 k-cycle.

例如在 S_5 中我們有以下的等式:

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

一個 cycle 是 S_n 中的元素, 反之任一 S_n 中的元素未必是一個 cycle. 不過它們都可寫成一些 cycle 的乘積 (別忘了這裡指的是合成). 我們就用式子 (3.1) 當例子

來將 σ 用 cycle 表示出來. 因 σ 將 $1 \mapsto 2$ 所以我們先寫下

$$(1\ 2$$

接著 σ 將 $2 \mapsto 3$ 所以繼續寫下

$$(1\ 2\ 3$$

然後 σ 將 $3 \mapsto 1$ 所以我們寫下

$$(1\ 2\ 3)$$

用 ")" 將 3 框住表示 σ 將 3 送回 1. 這樣我們寫下了一個 3-cycle. 不過這 (1 2 3) 並不是 σ, 別忘了 σ 還將 $4 \mapsto 5$ 及 $5 \mapsto 4$. 所以需補上 (4 5) 這一個 cycle. 因此我們將式子 (3.1) 表成

$$\sigma = (4\ 5)(1\ 2\ 3).$$

這裡其實我們是將 (1 2 3) 看成是 S_5 中的

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

這一個元素, 而

$$(4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

所以將之相乘得 σ. 同法式子 (3.2) 中的 τ 將 $1 \mapsto 3$, 故先寫下

$$(1\ 3$$

接著 τ 將 $3 \mapsto 5$ 所以繼續寫下

$$(1\ 3\ 5$$

而後 τ 將 $5 \mapsto 2$, 故寫

$$(1\ 3\ 5\ 2$$

接著 τ 將 $2 \mapsto 4$, 所以寫下

$$(1\ 3\ 5\ 2\ 4$$

最後 τ 將 4 送回 1 故補上 ")" 得

$$\tau = (1\ 3\ 5\ 2\ 4).$$

注意此時每一個元素的動作都用這一個 cycle 表示出來了, 所以 τ 是一個 5-cycle.

接下來我們看

$$\sigma \cdot \tau = (4\ 5)(1\ 2\ 3)(1\ 3\ 5\ 2\ 4)$$

會是甚麼? 當然了你可以將這些 cycles 還原成原來複雜的形式再計算, 不過這裡我們想直接用 cycle 的看法來處理. 首先觀察 (1 3 5 2 4) 將 $1 \mapsto 3$, 不過後面的 (1 2 3) 將 $3 \mapsto 1$, 最後 (4 5) 固定 1 所以知 $\sigma \cdot \tau$ 將 $1 \mapsto 1$. 也就是說在 $\sigma \cdot \tau$ 的 cycle 寫法中 1 不會出現. 現在看 2: (1 3 5 2 4) 將 $2 \mapsto 4$, 而後面的 (1 2 3) 將 4 固定住, 最後 (4 5) 將 $4 \mapsto 5$ 故知 $\sigma \cdot \tau$ 將 $2 \mapsto 5$, 所以我們寫下

$$(2\ 5$$

然而 (1 3 5 2 4) 將 $5 \mapsto 2$, 而後面的 (1 2 3) 將 $2 \mapsto 3$, 最後 (4 5) 固定 3, 所以得 $\sigma \cdot \tau$ 將 $5 \mapsto 3$, 我們記下

$$(2\ 5\ 3$$

然而 (1 3 5 2 4) 將 $3 \mapsto 5$, 且 (1 2 3) 將 5 固定住, 最後 (4 5) 將 $5 \mapsto 4$ 故知 $\sigma \cdot \tau$ 將 $3 \mapsto 4$, 所以繼續寫下

$$(2\ 5\ 3\ 4$$

最後 (1 3 5 2 4) 將 $4 \mapsto 1$, 而後面的 (1 2 3) 將 $1 \mapsto 2$, 然後 (4 5) 固定 2, 所以得 $\sigma \cdot \tau$ 將 4 送回了 2, 我們得知

$$\sigma \cdot \tau = (2\ 5\ 3\ 4).$$

兩個 cycles $(i_1\ \cdots\ i_k)$ 和 $(j_1\ \cdots\ j_l)$ 如果其中 $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$ 則稱此兩 cycle 為 *disjoint cycles.* 如果將 S_n 中的元素寫成一些兩兩 disjoint 的 cycles 的乘積 (當然包括只有一個 cycle 的情況), 我們就稱之為 disjoint cycle decomposition. 如前面 (4 5)(1 2 3) 和 (1 3 5 2 4) 就分別是 σ 和 τ 的 disjoint cycle decomposition.

我們簡單的說明一下對任意的 $\sigma \in S_n$, 其 disjoint cycle decomposition 是存在的. 作法就如同前面的例子, 任取一數 $a_1 \in \{1, \ldots, n\}$ 我們先考慮 σ 將 a_1 送到何處? 若 $\sigma(a_1) = a_1$, 則知 a_1 不會出現在 cycle decomposition 之中, 所以我們繼續考慮其他的數. 如果 $\sigma(a_1) = a_2 \neq a_1$ 則寫下

$$(a_1\ a_2$$

接下來看 $\sigma(a_2)$ 為何? ...如此繼續下去直到第一個 a_k 使得 $\sigma(a_k)$ 會和前面的某數相同. 也就是說 $a_1, \ldots, a_k$ 都相異但 $\sigma(a_k) \in \{a_1, \ldots, a_{k-1}\}$. 不過此時 $\sigma(a_k)$ 非得等於 a_1 不可, 因為若 $\sigma(a_k) = a_i$, 其中 $i > 1$, 則已知 $\sigma(a_{i-1}) = a_i$, 由 σ 是 1-1 知 $a_k = a_{i-1}$ 這和 $a_1, \ldots, a_k$ 兩兩相異矛盾, 所以得 $\sigma(a_k) = a_1$. 也就是說我們得到一個 cycle:

$$(a_1\ \cdots\ a_k).$$

接下來我們考慮 $\{a_1, \ldots, a_k\}$ 以外的數 b_1, 再利用同樣的方式得到一個 cycle. 如此繼續下去直到將所有 $\{1, \ldots, n\}$ 考慮完畢, 然後得 σ 就是這些 cycles 的乘積. 當然了利用 σ 是 1-1 我們很容易看出這樣做出的 cycles 都是 disjoint.

接下來我們要說 disjoint cycle decomposition 是唯一的. 不過這裡的唯一性要說明一下. 首先觀察 (1 2 3) 這一個 cycle 其實它和 (2 3 1) 及 (3 1 2) 都表示同一個函數: 即 $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. 因此我們將之視為同一 cycle (不過要注意 (1 3 2) 是不同的 cycle). 另外 (1 2 3)(4 5) 和 (4 5)(1 2 3) 也是同一個函數所以我們也將之視為同樣的 decomposition.

Lemma 3.4.4. 令 $\sigma = (a_1\ a_2 \cdots a_k)$ 和 $\tau = (b_1\ b_2 \cdots b_l)$ 是 S_n 的兩個 *cycles.*

(1) 如果 $k = l$ 且 $a_1 = b_2$, $a_2 = b_3$, ..., $a_{k-1} = b_k$, $a_k = b_1$, 則 $\sigma = \tau$.

(2) 如果 σ 和 τ 是 *disjoint,* 即 $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset$, 則 $\sigma \cdot \tau = \tau \cdot \sigma$.

Proof. 我們曾經強調過, 要說明兩個 S_n 中的元素是相同的只要將之視為函數, 將 $\{1,\ldots,n\}$ 中任意數代入都相等就可.

(1) 若 $x \in \{1,\ldots,n\}$ 但 $x \notin \{a_1,\ldots,a_k\}$, 則知 $\sigma(x) = x$, 但由假設知

$$\{a_1,\ldots,a_k\} = \{b_1,\ldots,b_l\},$$

所以 $x \notin \{b_1,\ldots,b_l\}$, 也就是說 $\tau(x) = x$.

若 $x \in \{a_1,\ldots,a_k\}$, 假設 $x = a_i$, $1 \le i \le k-2$, 則

$$\sigma(x) = \sigma(a_i) = a_{i+1} = b_{i+2}.$$

此時因 $a_i = b_{i+1}$, 所以

$$\tau(x) = \tau(b_{i+1}) = b_{i+2}.$$

而當 $x = a_{k-1}$ 時,

$$\sigma(x) = \sigma(a_{k-1}) = a_k = b_1.$$

此時因 $a_{k-1} = b_k$, 故

$$\tau(x) = \tau(b_k) = b_1.$$

最後當 $x = a_k$ 時,

$$\sigma(x) = \sigma(a_k) = a_1 = b_2.$$

此時因 $a_k = b_1$ 所以

$$\tau(x) = \tau(b_1) = b_2.$$

得證對所有的 $x \in \{1,\ldots,n\}$ 皆有 $\sigma(x) = \tau(x)$, 因此知 $\sigma = \tau$.

(2) 此時由假設 σ 和 τ 是 disjoint, 所以 $x \in \{1,\ldots,n\}$ 可分成三種情況: (a) $x \notin \{a_1,\ldots,a_k\} \cup \{b_1,\ldots,b_l\}$; (b) $x \in \{a_1,\ldots,a_k\}$; (c) $x \in \{b_1,\ldots,b_l\}$.

當 x 是屬狀況 (a) 時, 得 $\sigma(x) = \tau(x) = x$ 故

$$(\sigma\cdot\tau)(x) = \sigma(\tau(x)) = \sigma(x) = x,$$

同理知 $(\tau\cdot\sigma)(x) = x$.

當 x 是屬狀況 (b) 時, 得 $\sigma(x) \in \{a_1,\ldots,a_k\}$ 但由 disjoint 知 x 和 $\sigma(x)$ 皆不屬於 $\{b_1,\ldots,b_l\}$ 故 $\tau(x) = x$ 且 $\tau(\sigma(x)) = \sigma(x)$. 所以知

$$(\sigma\cdot\tau)(x) = \sigma(\tau(x)) = \sigma(x)$$

且

$$(\tau\cdot\sigma)(x) = \tau(\sigma(x)) = \sigma(x).$$

最後若 x 是屬狀況 (c) 時, 同狀況 (b) 可知

$$(\sigma\cdot\tau)(x) = \tau(x) = (\tau\cdot\sigma)(x).$$

故得 $\sigma\cdot\tau = \tau\cdot\sigma$. □

Remark 3.4.5. 在 Lemma 3.4.4 中我們證得

$$(a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$$

和

$$(a_k\ a_1\ \cdots\ a_{k-2}\ a_{k-1})$$

為同一 cycle. 對 $(a_k\ a_1\ \cdots\ a_{k-2}\ a_{k-1})$ 再套用一次 Lemma 3.4.4 可得

$$(a_{k-1}\ a_k\ \cdots\ a_{k-3}\ a_{k-2})$$

也是同一 cycle. 如此一直循環下去我們可得到同一個 k-cycle 有 k 種寫法.

另外我們要強調的是若 σ 和 τ 不是 disjoint 時, 則 $\sigma\cdot\tau$ 並不一定等於 $\tau\cdot\sigma$ (前面已給過例子了).

現在我們可以說如果將 Lemma 3.4.4 的這兩種狀況忽略 (即不管一個 cycle 的循環或兩個 disjoint cycle 的順序), 那麼任一個 S_n 的元素寫成 disjoint cycle decomposition 的寫法唯一. 假設 $\sigma \in S_n$ 有兩種 disjoint cycle decompositions: $\sigma = \sigma_1\cdots\sigma_r$ 和 $\sigma = \tau_1\cdots\tau_s$, 其中 $\sigma_1,\ldots,\sigma_r$ 和 $\tau_1,\ldots,\tau_s$ 分別是兩組 disjoint cycles. 假設 $a_1 \in \{1,\ldots,n\}$ 在 σ_1 這個 cycle 出現, 而 $\sigma_1(a_1) = a_2$, 則我們有

$$\sigma_1 = (a_1\ a_2\ \cdots$$

然而 $\sigma_1,\ldots,\sigma_r$ 是 disjoint 所以 a_1, a_2 不會在 $\sigma_2,\ldots,\sigma_r$ 中出現; 也就是說當 i 符合 $2 \le i \le r$ 時 $\sigma_i(a_1) = a_1$ 因此由 $\sigma = \sigma_1\cdots\sigma_r$ 知

$$\sigma(a_1) = (\sigma_1\cdots\sigma_r)(a_1) = \sigma_1(a_1) = a_2. \tag{3.5}$$

不過由於 $\sigma = \tau_1\cdots\tau_s$, a_1 一定會在某一個 τ_i 中出現, 否則如果 a_1 在所有的 τ_i 都沒出現則知 $\tau_i(a_1) = a_1$, 然而若真如此, 則得

$$\sigma(a_1) = \tau_1\cdots\tau_s(a_1) = a_1.$$

此和上式 (3.5) 相矛盾. 其實由於 $\tau_1,\ldots,\tau_s$ 是 disjoint, a_1 只會出現在唯一的 τ_i 中. 我們不妨假設 a_1 出現在 τ_1 中 (別忘了 $\tau_1,\ldots,\tau_s$ 是 disjoint 所以它們可以兩兩交換). 因為 a_1 不會在其他的 τ_i 出現, 當 i 符合 $2 \le i \le s$ 時, 我們有 $\tau_i(a_1) = a_1$. 因此知

$$\sigma(a_1) = (\tau_1\cdots\tau_s)(a_1) = \tau_1(a_1). \tag{3.6}$$

結合 (3.5) 和 (3.6) 兩式, 我們得 $\tau_1(a_1) = a_2$. 也就是說

$$\tau_1 = (a_1\ a_2\ \cdots$$

對 a_2 用同樣的論述可得 $\sigma_1(a_2) = \tau_1(a_2)$, 如此一直下去我們可得 $\sigma_1 = \tau_1$. 因此用歸納法可知 $r = s$ 且 對所有的 i 皆有 $\sigma_i = \tau_i$. 我們證得了 S_n 中所有的元素皆存在唯一的 disjoint cycle decomposition.

3.4.4. Disjoint cycle 的性質. 我們現在來看看寫成 disjoint cycle 到底有哪些好處.

其中一個好處就是很容易求出 inverse. 首先來看單一一個 cycle 的情況.

Lemma 3.4.6. *若*

$$\sigma = (a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$$

是 S_n 中的一個 k-cycle. 則 σ^{-1} 也是一個 k-cycle 且

$$\sigma^{-1} = (a_k\ a_{k-1}\ \cdots\ a_2\ a_1).$$

Proof. 令 $\tau = (a_k\ a_{k-1}\ \cdots\ a_2\ a_1)$ 我們直接證明 $\tau\cdot\sigma$ 是 identity. 也就是要證對所有 $x \in \{1,\ldots,n\}$, $(\tau\cdot\sigma)(x) = x$.

如果 $x \notin \{a_1,\ldots,a_k\}$ 則自然 $\sigma(x) = \tau(x) = x$, 所以此時

$$(\tau\cdot\sigma)(x) = \tau(\sigma(x)) = \tau(x) = x.$$

反之, 如果 $x \in \{a_1,\ldots,a_k\}$, 則當 $x = a_i$, 其中 $1 \le i \le k-1$ 時, 因 $\sigma(x) = \sigma(a_i) = a_{i+1}$ 且 $2 \le i+1 \le k$, 故

$$(\tau\cdot\sigma)(x) = \tau(\sigma(a_i)) = \tau(a_{i+1}) = a_i = x.$$

而當 $x = a_k$ 時

$$(\tau\cdot\sigma)(x) = \tau(\sigma(a_k)) = \tau(a_1) = a_k = x.$$

故得 $\tau\cdot\sigma$ 是 S_n 的 identity, 也就是說 $\tau = \sigma^{-1}$. □

若 $\sigma = \sigma_1\cdots\sigma_r$ 是 σ 的 disjoint cycle decomposition. 則我們可以利用 Lemma 3.4.6 將每一個 σ_i 的 inverse 求出. Lemma 3.4.6 也告訴我們這些 $\sigma_1^{-1},\ldots,\sigma_r^{-1}$ 是 disjoint cycles. 所以可以很容易的就將 σ^{-1} 的 disjoint cycle decomposition 寫出. 例如若 $\sigma = (1\ 2\ 3)(4\ 5)$, 我們馬上得 $\sigma^{-1} = (3\ 2\ 1)(5\ 4)$.

寫成 disjoint cycle 的另一個好處是能夠很快的求出 S_n 中元素的 order. 我們還是先來看單一一個 cycle 的情況.

Lemma 3.4.7. *若 σ 是 S_n 中的一個 k-cycle. 則 $\mathrm{ord}(\sigma) = k$.*

Proof. 若 $\sigma = (a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$, 我們要證當 $1 \le i \le k-1$ 時, σ^i 不是 S_n 中的 identity, 而 σ^k 是 S_n 的 identity.

當 $1 \le i \le k-1$ 時, $\sigma^i(a_1) = a_{i+1}$. 由於 $2 \le i+1 \le k$, 我們知 $a_{i+1} \ne a_1$, 也就是說 $\sigma^i(a_1) \ne a_1$. 所以 σ^i 不可能是 identity.

另外,若 $x \notin \{a_1,\ldots,a_k\}$ 時, 當然有 $\sigma^k(x) = x$. 而由定義知對所有的 $x \in \{a_1,\ldots a_k\}$ 皆有 $\sigma^k(x) = x$. 所以得 σ^k 是 identity. □

我們已知一個 cycle 的 order 為何, 但要求一些 disjoint cycles 的乘積的 order 我們需要以下這個一般 group 的性質:

Lemma 3.4.8. 令 $a, b \in G$ 且 $a \cdot b = b \cdot a$. 若 $\langle a \rangle \cap \langle b \rangle = \{e\}$, 則

$$\mathrm{ord}(a \cdot b) = \mathrm{lcm}[\mathrm{ord}(a), \mathrm{ord}(b)],$$

其中 lcm 表最小公倍數.

Proof. 回顧一下, $\mathrm{ord}(a) = n$ 等價於下面兩條件: (1) $a^n = e$; (2) 如果 $a^r = e$ 則 $n \mid r$.

若令 $\mathrm{ord}(a) = n$ 且 $\mathrm{ord}(b) = m$, 而 $l = \mathrm{lcm}[n, m]$, 則由 $a \cdot b = b \cdot a$ 知 $(a \cdot b)^l = a^l \cdot b^l = e$. 此證明了 l 符合 $\mathrm{ord}(a \cdot b)$ 的條件 (1).

現若 $(a \cdot b)^r = e$, 知 $a^r \cdot b^r = e$, 也就是 $a^r = b^{-r}$. 然而 $a^r \in \langle a \rangle$ 且 $b^{-r} \in \langle b \rangle$, 故知 $a^r \in \langle a \rangle \cap \langle b \rangle$. 利用假設 $\langle a \rangle \cap \langle b \rangle = \{e\}$, 得 $a^r = e$ 且 $b^{-r} = (b^r)^{-1} = e$ (也就是 $b^r = e$). 因 $\mathrm{ord}(a) = n$, $\mathrm{ord}(b) = m$, 利用條件 (2) 知 $n \mid r$ 且 $m \mid r$. 也就是 r 是 n, m 的公倍數. 再利用最小公倍數的性質知 $l = \mathrm{lcm}[n, m] \mid r$. 此證明了 l 符合 $\mathrm{ord}(a \cdot b)$ 的條件 (2). 所以 $\mathrm{ord}(a \cdot b) = l = \mathrm{lcm}[\mathrm{ord}(a), \mathrm{ord}(b)]$. □

Proposition 3.4.9. 令 $\sigma \in S_n$, 若 $\sigma = \sigma_1 \cdot \sigma_2 \cdots \sigma_r$ 是 σ 的 *disjoint cycle decomposition,* 其中 σ_i 是一個 n_i-*cycle.* 則

$$\mathrm{ord}(\sigma) = \mathrm{lcm}[n_1, n_2, \ldots, n_r].$$

Proof. 我們首先證 $\mathrm{ord}(\sigma_1 \cdot \sigma_2) = \mathrm{lcm}[n_1, n_2]$. 因 σ_1 和 σ_2 是 disjoint, 所以 $\sigma_1 \cdot \sigma_2 = \sigma_2 \cdot \sigma_1$. 因此只要我們證得 $\langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle = \{e\}$, 則由 Lemma 3.4.7 和 Lemma 3.4.8 知 $\mathrm{ord}(\sigma_1 \cdot \sigma_2) = \mathrm{lcm}[n_1, n_2]$. 現若 $\tau \in \langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle$, 則存在 i 和 j 使得 $\tau = \sigma_1^i = \sigma_2^j$. 若 τ 不是 S_n 的 identity, 即存在 $a \in \{1, \ldots, n\}$ 使得 $\tau(a) \neq a$. 也就是說 $\sigma_1^i(a) \neq a$. 這當然就保證 a 必須出現在 σ_1 的 cycle 中 (否則 $\sigma_1(a) = a$ 會得到 $\sigma_1^i(a) = a$). 然而 σ_2 和 σ_1 是 disjoint, 故 a 必不會出現在 σ_2 的 cycle 中. 也就是說 $\sigma_2(a) = a$. 這會造成 $\sigma_2^j(a) = a$, 與當初假設 $\sigma_2^j(a) = \tau(a) \neq a$ 相矛盾. 因此 τ 非得是 S_n 的 identity 不可. 因此得證 $\langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle = \{e\}$, 同時得 $\mathrm{ord}(\sigma_1 \cdot \sigma_2) = \mathrm{lcm}[n_1, n_2]$.

接下來我們可以用數學歸納法. 因 $\sigma_1, \ldots \sigma_{r-1}, \sigma_r$ 是 disjoint, 故有

$$(\sigma_1 \cdots \sigma_{r-1}) \cdot \sigma_r = \sigma_r \cdot (\sigma_1 \cdots \sigma_{r-1}).$$

再套用前面的論述, 我們有

$$\langle \sigma_1 \cdots \sigma_{r-1} \rangle \cap \langle \sigma_r \rangle = \{e\}.$$

因此由歸納假設 $\mathrm{ord}(\sigma_1 \cdots \sigma_{r-1}) = \mathrm{lcm}[n_1, \ldots, n_{r-1}]$ 及 Lemma 3.4.8 得

$$\begin{aligned} \mathrm{ord}(\sigma) &= \mathrm{ord}((\sigma_1 \cdots \sigma_{r-1}) \cdot \sigma_r) \\ &= \mathrm{lcm}[\mathrm{lcm}[n_1, \ldots, n_{r-1}], n_r] \\ &= \mathrm{lcm}[n_1, \ldots, n_{r-1}, n_r]. \end{aligned}$$

□

Proposition 3.4.9 告訴我們一個很快的方法計算 S_n 的元素的 order. 例如若 $\sigma = (1\ 2\ 3)(4\ 5)$ 則 $\mathrm{ord}(\sigma) = \mathrm{lcm}[2,3] = 6$. 這比你一個一個去乘快多了. 不過要記住 Proposition 3.4.9 只能當 disjoint cycle 乘在一起才適用. 例如 $(1\ 2\ 3)(3\ 2\ 1)$ 是 identity. 其 order 為 1 不是 $\mathrm{lcm}[3,3] = 3$.

3.4.5. 一些 cycles 的運算. 我們曾經提過 cycles 如何相乘, 由於有一些型態的 cycles 的運算以後經常會出現, 在這裡我們將其整理出來以方便以後使用.

Conjugation 是一種運算, 若 $a \in G$, 則對任意的 $x \in G$, $x \cdot a \cdot x^{-1}$ 就稱為 a 的一個 conjugate. 在 S_n 中, 若 $\sigma = \sigma_1 \cdots \sigma_r$ 是 σ 的一個 disjoint cycle decomposition, 則對任意的 $\tau \in S_n$ 我們有

$$\tau \cdot \sigma \cdot \tau^{-1} = \tau \cdot (\sigma_1 \cdots \sigma_r) \cdot \tau^{-1} = (\tau \cdot \sigma_1 \cdot \tau^{-1}) \cdots (\tau \cdot \sigma_r \cdot \tau^{-1}).$$

因此要算出這一個 conjugate 我們只要算出每一個 cycle 的 conjugate 為何即可.

Lemma 3.4.10. 若

$$\sigma = (a_1\ a_2 \cdots a_{k-1}\ a_k)$$

是 S_n 中的一個 *k-cycle*. 則對任意的 $\tau \in S_n$, $\tau \cdot \sigma \cdot \tau^{-1}$ 是一個 *k-cycle* 且

$$\tau \cdot \sigma \cdot \tau^{-1} = \big(\tau(a_1)\ \tau(a_2) \cdots \tau(a_{k-1})\ \tau(a_k)\big).$$

Proof. 首先注意因 $(a_1 \cdots a_k)$ 是一個 k-cycle, 這些 a_i 都相異, 再利用 $\tau \in S_n$ 是 1-1 所以 $\tau(a_i)$ 也都相異. 因此 $(\tau(a_1) \cdots \tau(a_k))$ 確實是一個 k-cycle.

令 $\delta = \big(\tau(a_1) \cdots \tau(a_k)\big)$, 要證明 $\tau\cdot\sigma\cdot\tau^{-1} = \delta$, 我們只要證明對所有 $x \in \{1, \ldots, n\}$, $\tau(\sigma(\tau^{-1}(x)))$ 和 $\delta(x)$ 相同就好.

若 $x \notin \{\tau(a_1), \ldots, \tau(a_k)\}$ 則 $\tau^{-1}(x) \notin \{a_1, \ldots, a_k\}$, 故得 $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$. 因此

$$\tau(\sigma(\tau^{-1}(x))) = \tau(\tau^{-1}(x)) = x,$$

然而 $x \notin \{\tau(a_1), \ldots, \tau(a_k)\}$, 故 $\delta(x) = x$. 所以在這情況下它們的作用相同.

若 $x = \tau(a_1)$ 則

$$\tau(\sigma(\tau^{-1}(x))) = \tau(\sigma(a_1)) = \tau(a_2)$$

且 $\delta(x) = \delta(\tau(a_1)) = \tau(a_2)$. 同理得對所有的 $x \in \{\tau(a_1), \ldots, \tau(a_k)\}$, $\tau \cdot \sigma \cdot \tau^{-1}$ 和 δ 對 x 的作用都相同. 因此知在 S_n 中它們是相同的元素. □

Example 3.4.11. 若 $\sigma = (1\ 2\ 3)(4\ 5)$, 而 $\tau = (3\ 4)$ 則

$$\begin{aligned} \tau \cdot \sigma \cdot \tau^{-1} &= (\tau \cdot (1\ 2\ 3) \cdot \tau^{-1}) \cdot (\tau \cdot (4\ 5) \cdot \tau^{-1}) \\ &= \big(\tau(1)\ \tau(2)\ \tau(3)\big)\big(\tau(4)\ \tau(5)\big) \\ &= (1\ 2\ 4)(3\ 5) \end{aligned}$$

另一種常見的運算是 S_n 中的一個 2-cycle 和另一元素的乘法. 我們看兩種基本的形式.

Lemma 3.4.12. 令 $\tau = (a\ b)$ 是 S_n 中的一個 2-*cycle*.

(1) 若 $\sigma = (a\ a_2 \cdots a_k)$ 是一個 S_n 中的 k-*cycle*, 其中 $a_2, \ldots, a_k \neq b$, 則

$$\tau \cdot \sigma = (a\ a_2 \cdots a_k\ b)$$

(2) 若 $\sigma = (a\ a_2 \cdots a_k\ b\ b_2 \cdots b_l)$ 是一個 S_n 中的 $k+l$-*cycle*, 則

$$\tau \cdot \sigma = (a\ a_2 \cdots a_k)(b\ b_2 \cdots b_l)$$

Proof. (1) 當 $\sigma = (a\ a_2 \cdots a_k)$ 時, 若 $x \in \{1, \ldots, n\}$ 但 $x \notin \{a, a_2, \ldots, a_k, b\}$, 則 $(\tau \cdot \sigma)(x) = \tau(x) = x$, 故 x 不回出現在 $\tau \cdot \sigma$ 的 disjoint cycle decomposition 中. 若 $x \in \{a, a_2, \ldots, a_{k-1}\}$, 則 $\sigma(x) \notin \{a, b\}$, 故 $(\tau \cdot \sigma)(x) = \sigma(x)$. 故可寫下

$$(a\ a_2 \cdots a_k$$

而當 $x = a_k$ 時 $(\tau \cdot \sigma)(a_k) = \tau(\sigma(a_k)) = \tau(a) = b$, 故可繼續寫下

$$(a\ a_2 \cdots a_k\ b$$

最後因 $(\tau \cdot \sigma)(b) = \tau(\sigma(b)) = \tau(b) = a$, 故可得一個 cycle

$$(a\ a_2 \cdots a_k\ b)$$

由於我們已考慮 $\tau \cdot \sigma$ 對所有 $x \in \{1, \ldots, n\}$ 的作用故可得

$$(a\ b)(a\ a_2 \cdots a_k) = (a\ a_2 \cdots a_k\ b) \tag{3.7}$$

(2) 同前面, 當 $x \notin \{a, a_2, \ldots, a_k, b, b_2, \ldots, b_l\}$ 時, $(\tau \cdot \sigma)(x) = \tau(x) = x$, 故 x 不回出現在 $\tau \cdot \sigma$ 的 disjoint cycle decomposition 中. 若 $x \in \{a, a_2, \ldots, a_{k-1}\}$, 則 $\sigma(x) \notin \{a, b\}$, 故 $(\tau \cdot \sigma)(x) = \sigma(x)$. 故可寫下

$$(a\ a_2 \cdots a_k$$

而當 $x = a_k$ 時 $(\tau \cdot \sigma)(a_k) = \tau(\sigma(a_k)) = \tau(b) = a$, 故可得一個 cycle

$$(a\ a_2 \cdots a_k)$$

然而這還並不一定是 $\tau \cdot \sigma$ 因為還有 $x \in \{b, b_2, \ldots, b_l\}$ 的情況未討論. 事實上同前一情況此時我們可得另一 cycle

$$(b\ b_2 \cdots b_l)$$

因我們已考慮完所有的 $x \in \{1, \ldots, n\}$ 故得

$$(a\ b)(a\ a_2 \cdots a_k\ b\ b_2 \cdots b_l) = (a\ a_2 \cdots a_k)(b\ b_2 \cdots b_l) \tag{3.8}$$

□

Remark 3.4.13. 在式子 (3.8) 中若在等式兩邊乘上 τ, 則因 τ^2 是 identity, 我們有

$$\sigma = \tau \cdot (\tau \cdot \sigma) = \tau \cdot (a\ a_2 \cdots a_k)(b\ b_2 \cdots b_l)$$

換句話說得到另一個有用的式子

$$(a\ b)(a\ a_2 \cdots a_k)(b\ b_2 \cdots b_l) = (a\ a_2 \cdots a_k\ b\ b_2 \cdots b_l) \tag{3.9}$$

3.4.6. Even and odd permutations. 因為 S_n 中的元素可以看成將 $\{1,\dots,n\}$ 的元素做排列組合, S_n 中的元素稱之為一個 *permutation.* 一個 permutation 應該是可以用每次只將 $\{1,\dots,n\}$ 中某兩個元素互換的方式組合得到. 將 $\{1\dots,n\}$ 中的某兩個元素互換的這個動作我們稱之為 *transposition.* 其實它只是 S_n 中的一個 2-cycle 罷了. 為了方便起見, 在這兒我們還是用 2-cycle 這個稱呼.

前面提到每個 permutation 可以用一些 transposition 組合而成, 這用數學的方法表達就是如下:

Lemma 3.4.14. *若 $\sigma \in S_n$, 則存在 S_n 的 2-cycles, $\tau_1,\dots,\tau_s$ 使得*

$$\sigma = \tau_1 \cdots \tau_s.$$

Proof. 因為 σ 可以寫成一些 cycles 的乘積, 要證明 σ 可以寫成 2-cycles 的乘積, 我們只要證明每一個 cycle 都可寫成 2-cycles 的乘積即可. 事實上由式子 (3.7) 知 $(a_1\ a_3)(a_1\ a_2) = (a_1\ a_2\ a_3)$, 如此一直下去可之任意的 k-cycle $(a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$ 可寫成

$$(a_1\ a_2\ \cdots\ a_{k-1}\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_2).$$

□

這裡要注意: Lemma 3.4.14 並沒有說每一個 S_n 的元素都可以寫成 'disjoint' 2-cycle 的乘積. 事實上這是不對的, 如 (1 2 3) 就沒法子寫成 disjoint 2-cycle 的乘積. 你知道為什麼嗎? 其實很簡單: 因為若 (1 2 3) 是一些 disjoint 2-cycle 的乘積, 則利用 Proposition 3.4.9 知其 order 應該為 2, 不過 (1 2 3) 的 order 是 3 故一定不可能寫成 disjoint 2-cycle 的乘積. 另外 Lemma 3.4.14 也沒有提及寫成 2-cycle 的乘積寫法會唯一, 因為這也是錯的. 例如

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3)$$

其實連可寫成多少個 2-cycle 的乘積都不一定. 例如 (1 2) 這一個 2-cycle 就可以寫成 (1 3)(2 3)(1 3) 這三個 2-cycle 的乘積.

從上面這個觀點來看, 將一個 S_n 的元素寫成 2-cycle 的乘積好像沒什麼好處. 事實上在大學的代數中我們學 2-cycle decomposition 只是為了方便去定義什麼是 even permutation 和 odd permutation 罷了. 我們稱 S_n 中的元素是 even 如果它可以寫成偶數個 2-cycle 的乘積, 反之則稱為 odd. 你應該會覺得這個定義有點奇怪吧! 前面提過一個 S_n 的元素可以寫成多少個 2-cycle 的乘積是不一定的. 有沒有可能它一下可寫成偶數個乘積, 而又可以寫成奇數個呢? 下一個定理告訴我們這是不可能的.

Theorem 3.4.15. *若 $\sigma \in S_n$ 且 $\sigma = \tau_1\cdot\tau_2\cdots\tau_r = \tau_1'\cdot\tau_2'\cdots\tau_s'$, 其中 $\tau_1,\dots,\tau_r$ 和 $\tau_1',\dots,\tau_s'$ 都是 2-cycles.* 則

$$r \equiv s \pmod 2 \quad (\text{即 } r \text{ 和 } s \text{ 同奇同偶：}\ \ 2 \mid r-s).$$

Proof. 我們利用大家都學過的線性代數裡有關行列式的性質來證明此定理. 回顧一下: 給定一 $n \times n$ 的矩陣 A, 如果將 A 中的某兩列互換所得的矩陣 A', 其行列式 $\det(A')$ 會等於 $-\det(A)$.

現在任取 $\sigma \in S_n$ 我們定義 $\sigma * A$ 這個矩陣是將 A 的第 i 列換到第 $\sigma(i)$ 列. 例如若 $\sigma = (i\ j)$ 則 $\sigma * A$ 就是將 A 的第 i 列換到第 j 列, 且將第 j 列換到第 i 列, 換句話說若 σ 是一個 2 cycle 則 $\sigma * A$ 就是如上述將 A 的某兩列互換. 若 $\sigma, \tau \in S_n$, 則 $(\sigma \cdot \tau) * A$ 是將 A 的第 i 列換到第 $(\sigma \cdot \tau)(i) = \sigma(\tau(i))$ 列. 而 $\tau * A$ 的第 $\tau(i)$ 列是 A 的第 i 列 且 $\sigma * (\tau * A)$ 是將 $\tau * A$ 的第 $\tau(i)$ 列換到第 $\sigma(\tau(i))$ 列. 換句話說 $\sigma * (\tau * A)$ 是將 A 的第 i 列換到第 $\sigma(\tau(i))$ 列. 這和 $(\sigma \cdot \tau) * A$ 是一樣的, 所以我們有

$$(\sigma \cdot \tau) * A = \sigma * (\tau * A) \quad \forall \sigma, \tau \in S_n. \tag{3.10}$$

現在若 $\sigma = \tau_1 \cdot \tau_2 \cdots \tau_r = \tau'_1 \cdot \tau'_2 \cdots \tau'_s$, 考慮 $\sigma * I_n$, 其中 I_n 是 $n \times n$ 的單位矩陣. 則由式子 (3.10) 知

$$\sigma * I_n = \tau_1 * (\cdots * (\tau_r * I_n)) = \tau'_1 * (\cdots * (\tau'_s * I_n)).$$

然而 τ_i, τ'_j 是 2-cycles, 它們每作用一次行列式值會變號, 所以得

$$\det(\sigma * I_n) = (-1)^r = (-1)^s.$$

也就是說 $r - s$ 是一個偶數. □

Theorem 3.4.15 告訴我們如果你找到偶數個 2-cycles 將 σ 寫成這些 2-cycle 的乘積, 則 σ 就不可能寫成奇數個 2-cycle 的乘積. 反之亦然. 因此我們有下面這個正式的定義:

Definition 3.4.16. 若 $\sigma \in S_n$ 可寫成偶數個 2-cycles 的乘積, 則稱 σ 為一個 *even permutation.* 反之, 若 σ 可寫成奇數個 2-cycles 的乘積, 則稱 σ 為一個 *odd permutation*

在 Lemma 3.4.14 的證明中我們曾證得一個 k-cycle 可以寫成 $k-1$ 個 2-cycle 的乘積, 因此一個 k-cycle 是 even 若 k 是奇數. 反之, 若 k 是偶數則此 k-cycle 就是 odd 了. 另外若 σ 可寫成 r 個 2-cycles 的乘積, 而 τ 可寫成 s 個 2-cycles 的乘積, 則 $\sigma \cdot \tau$ 可寫成 $r + s$ 個 2-cycles 的乘積. 因此我們有下一個結果:

Lemma 3.4.17. 令 $\sigma, \tau \in S_n$.

(1) 若 σ, τ 同為 *even permutations,* 或同為 *odd permutations,* 則 $\sigma \cdot \tau$ 為 *even permutation.*

(2) 若 σ 和 τ 其中一個是 *even permutation* 另一個是 *odd permutation,* 則 $\sigma \cdot \tau$ 為 *odd permutation.*

利用 Lemma 3.4.17 若將一個 S_n 的元素寫成 disjoint cycle decomposition, 就可以很快的判斷其為 even 或 odd. 這也是寫成 disjoint cycle decomposition 的另一個好處.

3.4.7. The alternating group. 在 S_n 中的 even permutations 所成的集合形成一個 group 稱之為 alternating group.

Theorem 3.4.18. 令 A_n 是 S_n 中所有的 *even permutation* 所成的集合.

(1) A_n 是 S_n 的一個 *normal subgroup.*

(2)
$$|A_n| = \frac{1}{2}n \cdot (n-1) \cdots 2 \cdot 1 = \frac{n!}{2}.$$

Proof. 考慮 $\text{sgn} : S_n \to \{1, -1\}$ 這個函數其中
$$\text{sgn}(\sigma) = \begin{cases} 1, & \text{若 } \sigma \text{ 是 even;} \\ -1, & \text{若 } \sigma \text{ 是 odd.} \end{cases}$$
若將 $\{1, -1\}$ 看成是一個乘法群, 則 1 是其 identity, 且 Lemma 3.4.17 告訴我們 sgn 是一個 group homomorphism. 由定義知 $\ker(\text{sgn}) = A_n$, 故由 Lemma 2.5.4 知 A_n 是 S_n 的一個 normal subgroup. 又任意的 2-cycle 是 odd, 故知 sgn 是 onto, 所以由 First Isomorphism 定理 (Corollary 2.6.2) 知 $S_n/A_n \simeq \{1, -1\}$. 也就是說 $|A_n| = |S_n|/2$. □

Definition 3.4.19. 我們將 S_n 中所有的 even permutation 所成的集合定為 A_n 稱之為 the *alternating group* of degree n.

Remark 3.4.20. 由於 A_n 的個數是 S_n 的一半, 那麼令一半當然是 S_n 中的 odd permutations 了, 所以在 S_n 中 odd permutation 和 even permutation 的個數一樣多.

每一個 S_n 的元素可以寫成一些 2-cycle 的乘積 (Lemma 3.4.14). 那麼 A_n 的元素都可以有甚麼特殊的表示法嗎?

Lemma 3.4.21. 若 $\sigma \in A_n$, 則存在 S_n 的 3-*cycles,* $\gamma_1, \ldots, \gamma_s$ 使得
$$\sigma = \gamma_1 \cdots \gamma_s.$$

Proof. 因 $\sigma \in A_n$ 故存在 $2r$ 個 2-cycles $\tau_1, \ldots, \tau_{2r}$ 使得 $\sigma = \tau_1 \cdot \tau_2 \cdots \tau_{2r-1} \cdot \tau_{2r}$. 我們將這些 τ_i 兩個兩個先擺一起, 也就是考慮 $\sigma = (\tau_1 \cdot \tau_2) \cdots (\tau_{2r-1} \cdot \tau_{2r})$. 若能證明任兩個 2-cycle 相乘都能寫成一些 3-cycles 的乘積, 那麼證明就完成了.

考慮 $\tau = (a\ b)$, $\tau' = (c\ d)$ 是 S_n 中兩個 2-cycle. 有三種可能情況:

(1) $\{a, b\} = \{c, d\}$, 此時 $\tau \cdot \tau'$ 是 identity, 所以我們可以將 $\tau \cdot \tau'$ 寫成
$$(1\ 2\ 3)(3\ 2\ 1)$$

(2) $\{a,b\}$ 和 $\{c,d\}$ 中恰有一數相同, 不失一般性我們假設 $a=c$ 但 $b\neq d$. 此時由式子 (3.7) 知

$$\tau\cdot\tau' = (a\ b)(a\ d) = (a\ d\ b)$$

(3) $\{a,b\}$ 和 $\{c,d\}$ 皆相異, 此時我們有

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

□

因為 3-cycle 是 even permutation, 所以所有的 3-cycles 都在 A_n 中. 下一個定理告訴我們反過來也是對的.

Proposition 3.4.22. *若 H 是 S_n 的一個 nontrivial proper subgroup, 假如 H 中含有所有的 3-cycles, 則 $H=A_n$.*

Proof. 若 $\sigma\in A_n$, 則由 Lemma 3.4.21 知存在 3-cycles, $\gamma_1,\ldots,\gamma_s$ 使得 $\sigma=\gamma_1\cdots\gamma_s$. 由假設, 這些 γ_i 都在 H 中. 又因 H 是 group, 由封閉性知 $\gamma_1\cdots\gamma_s\in H$. 也就是說 $\sigma\in H$. 故得 $A_n\subseteq H$. 然而 $H\neq S_n$ 故 $|H|<n!=2|A_n|$ 再由 Lagrange 定理 (Theorem 2.2.2) 知 $|H|$ 是 $|A_n|$ 的倍數. 唯一的可能就是 $|H|=|A_n|$. 故得 $H=A_n$ □

3.4.8. S_n 的 normal subgroup. 我們將介紹當 $n\geq 5$ 時 A_n 是 S_n 中唯一的 nontrivial normal subgroup.

因 S_3 只有 6 個元素, 我們將它們一一列出, 記有: (1 2), (1 3), (2 3), (1 2 3), (1 3 2) 和 identity. 其中 A_3 就是由 (1 2 3) 所產生的 cyclic group. 其他的 2-cycle 都只生成 order 2 的 subgroup. 考慮 (1 2) 所生成的 cyclic group $\langle(1\ 2)\rangle$, 由於

$$(1\ 3)(1\ 2)(1\ 3) = (3\ 2)\notin\langle(1\ 2)\rangle$$

可知 $\langle(1\ 2)\rangle$ 不是 S_3 的 normal subgroup. 同理知其他 order 為 2 的 subgroup 皆不是 normal. 因此在 S_3 中只有一個 nontrivial normal subgroup, 就是 A_3.

在 S_4 中情況就不一樣了. 除了 A_4 外 還有一個 normal subgroup

$$N=\{I,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}.$$

很容易看出 N 中除了 identity 以外, 每個元素都是 order 2, 也就是自己是自己的 inverse. 我們來檢查 N 是乘法封閉的. 由

$$(1\ 2)(3\ 4)\cdot(1\ 3)(2\ 4) = (1\ 4)(2\ 3)$$

就可以知 N 是乘法封閉的, 由此知 N 是 S_4 的 subgroup. (由於 N 中的元素都是 even permutation 可知 N 也是 A_4 的 subgroup.) 仔細觀察 N 中除了 identity 外其他的元素都是兩個 disjoint 2-cycle 相乘. 而且在 S_4 中所有可能的兩個 disjoint

2-cycle 相乘的 permutation 都在 N 中. 若 $\sigma = (a\ b)(c\ d)$ 是兩個 disjoint 2-cycle 相乘, 則由 Lemma 3.4.10 知對任意的 $\tau \in S_4$,

$$\tau \cdot \sigma \cdot \tau^{-1} = (\tau(a)\ \tau(b))(\tau(c)\ \tau(d))$$

也是由兩個 disjoint 2-cycle 相乘的 permutation. 換言知, 若 $\sigma \in N$, 則對任意的 $\tau \in S_4$ 皆得 $\tau \cdot \sigma \cdot \tau^{-1} \in N$, 故 N 是 S_4 的 normal subgroup.

當 $n \geq 5$ 時, 由於 S_n 的 order 已很大, 我們不可能如前面的方式討論下去. 我們有一個很重要的 Lemma 可以幫我們處理一般的狀況.

Lemma 3.4.23. 若 N 是 S_n 的一個 *nontrivial proper normal subgroup,* 且 N 中存在一個 3-*cycle,* 則 $N = A_n$.

Proof. Proposition 3.4.22, 告訴我們要證明 $N = A_n$, 只要證明所有的 3-cycle 皆在 N 中就可. 因此若 $(a\ b\ c)$ 是 N 中的一個 3-cycle, 我們想利用 N 是 normal 的性質證明任意的 3-cycle $(a'\ b'\ c')$ 也在 N 中.

由於 N 在 S_n 中 normal, 對任意的 $\tau \in S_n$, 因為 $(a\ b\ c) \in N$, 故有 $\tau \cdot (a\ b\ c) \cdot \tau^{-1} \in N$. 然而由 Lemma 3.4.10 知

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

因此對任意的 3-cycle $(a'\ b'\ c')$, 我們只要在 S_n 找到一個 τ 滿足 $\tau(a) = a'$, $\tau(b) = b'$ 和 $\tau(c) = c'$ 即可. 這當然做得到, 因為 a, b, c 皆相異, 而 a', b', c' 也都相異, 我們當然可找到一個 1-1 的函數將 $a \mapsto a'$, $b \mapsto b'$, $c \mapsto c'$. 也就是說對任意的 3-cycle $(a'\ b'\ c')$, 我們都可以在 S_n 找到一個 τ 滿足 $\tau \cdot (a\ b\ c) \cdot \tau^{-1} = (a'\ b'\ c')$. 所以由 $\tau \cdot (a\ b\ c) \cdot \tau^{-1} \in N$ 得 $(a'\ b'\ c') \in N$. □

綜合一下我們所知的結果: Lemma 3.4.22 告訴我們若已知 H 是 S_n 的一個 nontrivial proper subgroup, 則要證明 $H = A_n$ 須證明所有 S_n 的 3-cycle 都在 H 中才行; 然而若已知 H 是 normal 那麼 Lemma 3.4.23 告訴我們只要在 H 中找到一個 3-cycle 就可得 $H = A_n$.

現在我們可以證明當 $n \geq 5$ 時 A_n 是 S_n 唯一的 nontrivial normal subgroup.

Theorem 3.4.24. 當 $n \geq 5$ 時, 若 N 是 S_n 的 *nontrivial proper normal subgroup,* 則 $N = A_n$.

Proof. 由 Lemma 3.4.23 知我們只要想辦法在 N 中找到一個 3-cycle, 就可得 $N = A_n$.

現因 N 是 nontrivial, 所以 N 不是 identity. 換句話說在 N 中存在一個 σ 不是 identity. 既然 σ 不是 identity, 那麼 σ 必將 $\{1 \ldots, n\}$ 中某一整數 a 送到另一數 b, 即 $\sigma(a) = b \neq a$. σ 是我們在 N 中隨便挑的非 identity 的元素, 它長怎樣我們一點都不清楚. 它有可能將 b 送回到 a 也有可能送到另一個數 a', 所以我們可分成以下兩個 cases:

(1) $\sigma(a) = b$, 且 $\sigma(b) = a$;

(2) $\sigma(a) = b$ 但 $\sigma(b) = a' \neq a$.

我們接下來想利用 N normal 和利用 σ 這個微弱的訊息來幫我們在 N 中找到更具體一點的元素. 我們的方法是這樣的: 試著在 S_n 中找到一個 2-cycle τ, 使得 $\sigma \cdot \tau \cdot \sigma^{-1} \neq \tau$. 如此一來 $(\sigma \cdot \tau \cdot \sigma^{-1}) \cdot \tau^{-1}$ 就不會是 identity. 然而

$$(\sigma \cdot \tau \cdot \sigma^{-1}) \cdot \tau^{-1} = \sigma \cdot (\tau \cdot \sigma^{-1} \cdot \tau^{-1})$$

由 $\sigma \in N$, 得 $\sigma^{-1} \in N$ 再利用 N 是 normal 知 $\tau \cdot \sigma^{-1} \cdot \tau^{-1} \in N$. 因此 $\sigma \cdot (\tau \cdot \sigma^{-1} \cdot \tau^{-1}) \in N$. 也就是我們又在 N 中找到一個新的不是 identity 的元素.

當 σ 是 case 1 時, 我們在 $\{1, \ldots, n\}$ 中找另一個數 c, 使得 $c \neq a$ 且 $c \neq b$. 令 $\tau = (a\ c)$. 則由 Lemma 3.4.10 知

$$\sigma \cdot \tau \cdot \sigma^{-1} = (\sigma(a)\ \sigma(c)) = (b\ \sigma(c)).$$

注意此時因 $\sigma(b) = a$ 但 $c \neq b$ 故知 $\sigma(c) \neq a$. 也就是說

$$\sigma \cdot \tau \cdot \sigma^{-1} = (b\ \sigma(c)) \neq (b\ a) = \tau.$$

當 σ 是 case 2 時, 我們只要考慮 $\tau = (a\ b)$ 就可. 因為此時 $\sigma(b) = a' \neq a$, 故

$$\sigma \cdot \tau \cdot \sigma^{-1} = (\sigma(a)\ \sigma(b)) = (b\ a') \neq (a\ b) = \tau.$$

綜合以上 cases 1 和 2, 我們知: 不管 σ 為何我們都可以在 S_n 中找到一個 2-cycle τ 使得

$$(\sigma \cdot \tau \cdot \sigma^{-1}) \cdot \tau^{-1} \in N$$

且不是 identity. 更重要的是 $\tau = \tau^{-1}$ 和 $\sigma \cdot \tau \cdot \sigma^{-1}$ 都是 2-cycles. 也就是在 N 中存在一個元素 δ 是兩個 2-cycle 相乘且不是 identity.

這個 N 中的元素 δ 有可能是以下兩種情況:

甲: $\delta = (i\ j)(j\ k)$, 其中 i, j, k 皆相異.

乙: $\delta = (i\ j)(k\ l)$, 其中 i, j, k, l 皆相異.

若是 case 甲, 則

$$\delta = (i\ j)(j\ k) = (i\ j\ k) \in N,$$

故知 N 中有一個 3-cycle.

若是 case 乙, 我們選一個在 $\{1, \ldots, n\}$ 中但在 $\{i, j, k, l\}$ 以外的元素 m (這就是為何此定理需假設 $n \geq 5$ 的原因). 令 $\gamma = (i\ m)$, 則因 $\delta \in N$ 且 N 是 normal, 知 $\gamma \cdot \delta \cdot \gamma^{-1} = (m\ j)(k\ l) \in N$. 再由 $\delta \in N$ 知 $\delta \cdot (\gamma \cdot \delta \cdot \gamma^{-1}) \in N$. 然而

$$\begin{aligned} \delta \cdot (\gamma \cdot \delta \cdot \gamma^{-1}) &= (i\ j)(k\ l)(m\ j)(k\ l) \\ &= (i\ j)(m\ j) \\ &= (i\ j\ m) \end{aligned}$$

故知 N 中有一個 3-cycle.

我們證明了在任何狀況下 N 中皆有一個 3-cycle, 故得 $N = A_n$. □

記得我們在 S_4 中找到一個不是 A_4 的 normal subgroup, 它是由一些兩個 disjoint 2-cycle 相乘的 permutation 所形成. 當初我們證這些元素相乘有封閉性, 不過在 Theorem 3.4.24 的證明 (case 乙) 我們證得在 $n \geq 5$ 時這類元素相乘不再封閉.

3.4.9. A_n 的 **normal subgroup.** 若 B 是 A 的 subgroup, C 是 B 的 subgroup, 且知 C 是 A 的 normal subgroup, 則當然 C 也會是 B 的 normal subgroup. 然而若僅知 C 是 B 的 subgroup, 並不表示 C 會是 A 的 normal subgroup (參見 Remark 2.4.2). 所以雖然我們知在 $n \geq 5$ 時除了 A_n 外, S_n 沒有其他的 nontrivial proper normal subgroup, 但這並不表示 A_n 本身不會有 nontrivial normal subgroup.

我們將證事實上當 $n \geq 5$ 時 A_n 確實沒有 nontrivial normal subgroup. 我們將利用類似在 S_n 的方法處理, 唯一要克服的是我們只能考慮 A_n 裡的元素.

Lemma 3.4.25. 當 $n \geq 5$, 若 N 是 A_n 的一個 *normal subgroup,* 且 N 中存在一個 3-*cycle,* 則 $N = A_n$.

Proof. 首先再次強調在 Lemma 3.4.23 中的假設是 N 是 S_n 的 normal subgroup, 而這裡我們僅假設 N 是 A_n 的 normal subgroup, 由於此時 N 未必會是 S_n 的 normal subgroup 所以無法用 Lemma 3.4.23 來直接證明本 Lemma. 不過我們還是用類似的想法, 利用存在一個 3-cycle 和 N 在 A_n 中 normal 的假設得到所有的 3-cycle 都會在 N 中. 再利用 Proposition 3.4.22 得到 $N = A_n$.

假設 $(a\ b\ c) \in N$, 在 Lemma 3.4.23 的証明中我們是證明: 對任意的 3-cycle, $(a'\ b'\ c')$ 皆可找到 $\tau \in S_n$ 使得

$$\tau \cdot (a\ b\ c) \cdot \tau^{-1} = (a'\ b'\ c').$$

如今這件事還是對的. 唯一不同的是當初 N 是在 S_n 中 normal, 所以因 $(a\ b\ c) \in N$ 可得 $\tau \cdot (a\ b\ c) \cdot \tau^{-1} \in N$, 如今 N 只在 A_n 中 normal, 如果當初選的 τ 不屬於 A_n 則無法保證 $\tau \cdot (a\ b\ c) \cdot \tau^{-1}$ 會在 N 中 (回顧一下: N 在 A_n 中 normal 只告訴我們若 $\sigma \in N$, 且 $\tau \in A_n$ 才可保證 $\tau \cdot \sigma \cdot \tau^{-1} \in N$). 所以我們現在的策略是利用這個 τ 找到另一個 γ 在 A_n 使得 $\gamma \cdot (a\ b\ c) \cdot \gamma^{-1} = (a'\ b'\ c')$.

當然了, 如果當初找的 τ 已在 A_n 中那麼令 $\gamma = \tau$ 即可. 如果 τ 不在 A_n 呢? 這表示 τ 是 odd permutation, 所以只要找到一個 2-cycle 乘上 τ 就會成為 even permutation, 也就落入 A_n 了. 別忘了和 Lemma 3.4.23 不同, 這裡我們還多假設了 $n \geq 5$. 所以我們可選 $i, j \in \{1, \ldots, n\}$ 但 i 和 j 都不屬於 $\{a, b, c\}$, 而令 $\gamma = \tau \cdot (i\ j)$. 如此一來不但 $\gamma \in A_n$ 且

$$\begin{aligned}
\gamma \cdot (a\ b\ c) \cdot \gamma^{-1} &= (\tau \cdot (i\ j)) \cdot (a\ b\ c) \cdot (\tau \cdot (i\ j))^{-1} \\
&= \tau \cdot (i\ j)(a\ b\ c)(i\ j) \cdot \tau^{-1} \\
&= \tau \cdot (a\ b\ c) \cdot \tau^{-1} \quad (\text{因 } (a\ b\ c) \text{ 和 } (i\ j) \text{ disjoint}) \\
&= (a'\ b'\ c').
\end{aligned}$$

故由 $(a\ b\ c) \in N$ 且 N 在 A_n 中 normal, 得 $(a'\ b'\ c') \in N$. □

這裡要說明一下: 雖然 Lemma 3.4.25 我們用到了 $n \geq 5$ 這個假設, 不過當 $n = 3, 4$ 時, 我們可以直接證明 Lemma 3.4.25 也是對的.

最後我們依然要用類似證明 Theorem 3.4.24 的方法來證明以下的 Theorem.

Theorem 3.4.26. 當 $n \geq 5$ 時 A_n 沒有 *nontrivial proper normal subgroup.*

Proof. 我們要證明, 若 N 不是 identity 且是 A_n 的 normal subgroup, 則存在一個 3-cycle 在 N 中. 如此一來, 由 Lemma 3.4.25 知 $N = A_n$, 因而得證本定理.

回顧一下在 Theorem 3.4.24 的証明中, 我們是利用 N 中一個非 identity 的元素 σ, 找到一個 2-cycle τ 使得 $\sigma \cdot \tau \cdot \sigma^{-1} \neq \tau$. 如此就可以得到另一個在 N 中但不等於 identity 的元素, $\sigma \cdot (\tau \cdot \sigma^{-1} \cdot \tau^{-1})$. 這個元素當初會在 N 中完全是由於當時 N 假設是 S_n 的 normal subgroup, 所以利用 σ^{-1} 也在 N 中可得 $\tau \cdot \sigma^{-1} \cdot \tau^{-1} \in N$. 如今 N 是在 A_n normal, 而 τ 是 2-cycle 並不在 A_n 中, 我們不再有 $\tau \cdot \sigma^{-1} \cdot \tau^{-1} \in N$. 因此我們不能再用原來的 τ, 而是要找一個 A_n 中的元素. 事實上我們要找的是一個 3-cycle 就可. 也就是說我們希望找到一個 3-cycle ρ 使得 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$.

由於假設 $\sigma \in N$ 且不是 identity, 故存在 $a \in \{1, \ldots, n\}$ 使得 $\sigma(a) = b \neq a$. 由於我們要找的是 3-cycle, 我們要把 σ 細分成以下三種狀況:

(1) $\sigma(a) = b$, 且 $\sigma(b) = a$;

(2) $\sigma(a) = b$, $\sigma(b) = c$ 且 $\sigma(c) = a$;

(3) $\sigma(a) = b$, $\sigma(b) = c$ 且 $\sigma(c) = d \neq a$.

當σ 是 case 1 時, 我們可找 $\rho = (a\ b\ i)$, 其中 $i \in \{1 \ldots, n\}$ 但 $i \notin \{a, b\}$. 此時由 Lemma 3.4.10 得

$$\sigma \cdot \rho \cdot \sigma^{-1} = (b\ \ a\ \ \sigma(i)).$$

注意 $\sigma(a) = b$, 而 $i \neq a$ 故 $\sigma(i) \neq b$. 由於 ρ 是將 $a \mapsto b$, 而 $\sigma \cdot \rho \cdot \sigma^{-1}$ 是將 $a \mapsto \sigma(i)$ 故知 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$.

當σ 是 case 2 時, 我們可找 $\rho = (a\ b\ i)$, 其中 $i \in \{1 \ldots, n\}$ 但 $i \notin \{a, b, c\}$ (別忘了 $n \geq 5$ 所以一定可以找到這樣的 i). 此時由 Lemma 3.4.10 得

$$\sigma \cdot \rho \cdot \sigma^{-1} = (b\ \ c\ \ \sigma(i)).$$

由於 ρ 是將 $b \mapsto i$, 而 $\sigma \cdot \rho \cdot \sigma^{-1}$ 是將 $b \mapsto c$, 故由 $i \neq c$ 知 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$.

當σ 是 case 3 時, 我們令 $\rho = (a\ b\ c)$ 就可. 因為此時

$$\sigma \cdot \rho \cdot \sigma^{-1} = (b\ \ c\ \ d),$$

由 $a \neq d$ 的假設知 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$.

綜合以上的結果我們知: 在 N 中任取一個不是 identity 的元素 σ, 存在一個 3-cycle ρ 符合 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$. 由於 $\rho \in A_n$, 而 N 在 A_n 中 normal, 故由 $\sigma^{-1} \in N$

得 $\rho \cdot \sigma^{-1} \cdot \rho^{-1} \in N$. 因此若令 $\gamma = (\sigma \cdot \rho \cdot \sigma^{-1}) \cdot \rho^{-1}$ 則 γ 不是 identity, 且 $\gamma = \sigma \cdot (\rho \cdot \sigma^{-1} \cdot \rho^{-1}) \in N$. 更重要的是由於 ρ 是一個 3-cycle, Lemma 3.4.10 告訴我們 $\sigma \cdot \rho \cdot \sigma^{-1}$ 也是一個 3-cycle. 所以 $\gamma = (\sigma \cdot \rho \cdot \sigma^{-1}) \cdot \rho^{-1}$ 是由兩個 3-cycle 相乘所得的 permutation. 簡言之: 我們在 N 中找到一個非 identity 的元素 γ, 而且 γ 是由兩個 3-cycle 相乘而得.

現在我們將 γ 的這兩個 3-cycles 可能的形式列出:

甲: 此二 3-cycles 中的元素都相同;

乙: 此二 3-cycles 中, 有兩個元素相同;

丙: 此二 3-cycles 中, 僅有一個元素相同;

丁: 此二 3-cycles 中的元素皆相異.

若是 case 甲, γ 可寫成 $(i\ j\ k)(i\ j\ k)$ (不可能是 $(i\ j\ k)(i\ k\ j)$ 因若如此則為 identity). 在此情形我們得

$$\gamma = (i\ \ j\ \ k)(i\ \ j\ \ k) = (i\ \ k\ \ j) \in N.$$

故知 N 中有一個 3-cycle.

若是 case 乙, γ 可寫成 $(i\ j\ k)(j\ i\ r)$ 或 $(i\ j\ k)(i\ j\ r)$. 在第一種情形,

$$\gamma = (i\ \ j\ \ k)(j\ \ i\ \ r) = (i\ \ r\ \ k) \in N;$$

在第二種情形,

$$\gamma = (i\ \ j\ \ k)(i\ \ j\ \ r) = (i\ \ k)(j\ \ r).$$

此時由於 $n \geq 5$, 在 $\{1, \ldots, n\}$ 中我們選擇 $s \notin \{i, j, k, r\}$, 而令 $\delta = (i\ k\ s) \in N$. 則由於 $\gamma \in N$ 且 N 在 A_n 中 normal, 故 $\delta \cdot \gamma \cdot \delta^{-1} \in N$. 然而 $\delta \cdot \gamma \cdot \delta^{-1} = (k\ s)(j\ r)$ 故得

$$\gamma \cdot (\delta \cdot \gamma \cdot \delta^{-1}) = (i\ \ k)(j\ \ r)(k\ \ s)(j\ \ r) = (i\ \ k\ \ s) \in N.$$

所以在此情形, N 中有一個 3-cycle.

若是 case 丙, γ 可寫成 $(i\ j\ k)(i\ s\ t)$. 在此情形我們得

$$\gamma = (i\ \ j\ \ k)(i\ \ s\ \ t) = (i\ \ s\ \ t\ \ j\ \ k).$$

故知 N 中有一個 5-cycle. 此時令 $\delta = (i\ s\ t) \in A_n$, 則 $\delta \cdot \gamma \cdot \delta^{-1} = (s\ t\ i\ j\ k) \in N$. 故得

$$\gamma^{-1} \cdot (\delta \cdot \gamma \cdot \delta^{-1}) = (k\ \ j\ \ t\ \ s\ \ i)(s\ \ t\ \ i\ \ j\ \ k) = (i\ \ t\ \ k) \in N.$$

所以在此情形, N 中有一個 3-cycle.

最後若是 case 丁, γ 可寫成 $(i\ j\ k)(r\ s\ t)$. 此時令 $\delta = (i\ j\ r) \in A_n$, 則 $\delta \cdot \gamma \cdot \delta^{-1} = (j\ r\ k)(i\ s\ t) \in N$. 故得

$$\gamma^{-1} \cdot (\delta \cdot \gamma \cdot \delta^{-1}) = (k\ \ j\ \ i)(t\ \ s\ \ r)(j\ \ r\ \ k)(i\ \ s\ \ t) = (i\ \ r\ \ j\ \ t\ \ k) \in N.$$

也就是說 N 中有一個 5-cycle. 此時用和上一個 (case 丙) 處理 5-cycle 相同的方法, 可得 N 中有一個 3-cycle.

由以上之結果知, 在任何情況下 N 中都有一個 3-cycle. 所以由 Lemma 3.4.25 知 $N = A_n$. □

當一個 group 它沒有 nontrivial proper normal subgroup 時, 我們稱這種 group 是 *simple group*. 若 G 是 abelian, 它所有的 subgroup 都是 normal subgroup, 所以此時若 G 又是 simple, 表示 G 沒有 nontrivial proper subgroup. 之前已知在這種情形 G 一定是 cyclic 且其個數一定是一質數. 不過在一般情況下, simple group 並不如其名那麼 "simple". Theorem 3.4.26 告訴我們當 $n \geq 5$ 時 A_n 是 simple group, 不過事實上 A_n 是蠻複雜的.

Chapter 4

進階 Group 的性質

在這一章中我們將介紹另一種方法來處理更深一點的 group 理論. 這個方法稱之為 group action. 其實 group action 的理論基礎並不難, 困難的是當你碰到問題時要用哪種 group action 來解決問題. 不過這一點是經驗上的問題, 大家不必太在意. 所以當我們在介紹某種 group action 來處理問題時, 希望大家不要太害怕不知為何會想到用這種 action, 而將注意力集中在如何用這種 group action 產生的結果結合我們之前學的理論來得到更深的理論.

4.1. Group Action

給定一集合 S 和一個 group G, 如果對於任意 $a \in G$, $s \in S$, a 可作用在 s 上, 其作用的結果我們定成 $a * s$. 注意: 這裡我們稱為'作用'不稱為'運算', 主要原因是在我們想區分清楚在介紹 group 時我們稱的運算是指 group 同一個集合自己元素間的運算, 而這裡我們是可以有兩個不同的集合 G 和 S. 當然了照定義當 $S = G$ 時, G 當然還是可以作用在 G 上, 所以這裡還是要區分清楚作用和運算的不同.

Definition 4.1.1. 當 G 對 S 的作用 $*$ 符合以下三點我們就稱 $(G, S, *)$ 為一個 group action.

(Act1): $\forall\, a \in G$, $s \in S$, 皆有 $a * s \in S$.

(Act2): $\forall\, s \in S$, 皆有 $e * s = s$, 其中 e 是 G 的 identity.

(Act3): $\forall\, a, b \in G$, $s \in S$, 皆有 $(a \cdot b) * s = a * (b * c)$.

條件 (Act1) 是說 action 必須是封閉的, 也就是說 G 中的元素對 S 中的元素作用後還是要在 S 中. 這樣 G 中的元素就可以一直作用下去. 也就是說若 $b \in G$, $s \in S$, 則 $b * s$ 會在 S 中所以 G 中的元素 a 才可以再對 $b * s$ 作用得 $a * (b * s)$. 就因如此 (Act3) 中 $a * (b * s)$ 才有意義. (Act3) 告訴我們: b 對 s 作用後 a 再作用上去和 $a \cdot b$ 直接作用在 s 上是一樣的. 這有點像結合率對吧! 事實上若考慮 $S = G$, 而 G 對 G 的作用是 G 上的乘法, 則沒錯 G 上的乘法事實上就是一個 group action.

其實在證明 Theorem 3.4.15 時我們就引進了 S_n 對 $n \times n$ 矩陣的 group action. 我們不在這裡介紹其他的 group action 的例子, 我們留待要用到時再個別介紹.

談 group action 最主要的原因就是想用 G 的 action 將 S 中的元素分類. 若 $(G, S, *)$ 是一個 group action. 我們說 $x, y \in S$ 是同類的 (記作 $x \sim y$) 若且為若存在 $a \in G$ 使得 $a * x = y$. 我們曾說過一個好的分類必須是一個 equivalence relation. 下一個 Lemma 告訴我們當 $(G, S, *)$ 是一個 group action 時, 這樣的分類是一個好的分類.

Lemma 4.1.2. 若 $(G, S, *)$ 是一個 *group action,* 對於 $x, y \in S$ 我們定

$$x \sim y \Leftrightarrow \text{存在 } a \in G \text{ 使得 } a * x = y,$$

則 $\sim$ 是 S 中的一個 *equivalence relation.*

Proof. 我們證明 $\sim$ 符合 Definition 2.1.1 中的三個性質.

(equiv1) 任取 $x \in S$, 由 (Act2) 知 $e * x = x$ 故 $x \sim x$.

(equiv2) 若 $x \sim y$, 則由定義知: 存在 $a \in G$ 使得 $a * x = y$. 等式兩邊用 a^{-1} 作用, 由 (Act2) 和 (Act3) 得

$$a^{-1} * y = a^{-1} * (a * x) = (a^{-1} \cdot a) * x = e * x = x.$$

因為 $a^{-1} \in G$, 故知 $y \sim x$.

(equiv3) 若 $x \sim y$ 且 $y \sim z$, 知存在 $a, b \in G$ 使得 $a * x = y$ 且 $b * y = z$. 故由 (Act3) 知 $(b \cdot a) * x = b * (a * x) = b * y = z$. 因為 $b \cdot a \in G$, 故知 $x \sim z$. □

在第二章我們提過用 equivalence relation 分類的好處是 S 內的每一個元素都會被分到某一類, 且不同類的集合不會有交集. 現在若 S 是一個有限集合, 且 S 可分成 $[x_1], \ldots, [x_r]$ 這 r 個同類集, 其中 $[x_i]$ 表示 S 中與 x_i 同類的元素所成的集合. 則由 Lemma 2.1.2 知

$$|S| = \sum_{i=1}^{r} |[x_i]|. \tag{4.1}$$

所以現在重要的工作就是計算每個 $[x_i]$ 的個數.

Lemma 4.1.3. 若 $(G, S, *)$ 是一個 *group action,* $x \in S$.

(1) 若令 $G_x = \{g \in G \mid g * x = x\}$, 則 G_x 是 G 的一個 *subgroup.*

(2) 令 $[x]$ 表示 S 中所有和 x 同類的元素所成的集合. 若 G 和 S 都是 *finite,* 則

$$|[x]| = \frac{|G|}{|G_x|}.$$

Proof. (1) 若 $a, b \in G_x$, 即 $a * x = x$ 且 $b * x = x$, 故利用 (Act3) 知

$$(a \cdot b) * x = a * (b * x) = a * x = x,$$

也就是說 $a \cdot b \in G_x$. 再來因

$$x = e * x = a^{-1} * (a * x) = a^{-1} * x,$$

故得 $a^{-1} \in G_x$. 由此知 G_x 是 G 的 subgroup.

(2) 首先我們觀察若 $y \in [x]$, 表示存在 $a \in G$ 使得 $y = a * x$. 反之, 若給定 $a \in G$, 令 $y = a * x$, 則 y 和 x 是同類. 所以我們知 $[x] = \{g * x \,|\, g \in G\}$, 也就是每個 $[x]$ 中的元素都是 $g * x$ 這種形式. 不過要注意有可能存在 $a, b \in G$ 且 $a \neq b$ 但 $a * x = b * x$. 所以要真正算出 $[x]$ 有多少元素, 等於要算出到底有多少 G 中的元素會讓 $g * x$ 相異. 然而若 $a, b \in G$ 且 $a * x = b * x$, 則在等式兩邊用 a^{-1} 作用, 得

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

也就是說 $a^{-1} \cdot b \in G_x$. 反之, 若 $a^{-1} \cdot b \in G_x$ 可得 $a * x = b * x$. 大家該記得 $a^{-1} \cdot b \in G_x$ 表示什麼吧! 這表示若用 G_x 這個 subgroup 對 G 中的元素分類, 和 a 同類的元素對 x 作用都會等於 $a * x$. 反之若 $a, b \in G$ 在用 G_x 這個 subgroup 分類之下是不同類的, 則 $a * x \neq b * x$. 所以 $[x]$ 內的元素個數是和 G 中用 G_x 分類之下可分成多少類是一樣的. 在證明 Lagrange 定理 (Theorem 2.2.2) 時我們曾證明若用 G_x 將 G 分類, 則 G 可分成 $|G|/|G_x|$ 類, 故得證本定理. □

Lemma 4.1.3 告訴我們, 給定 $x \in S$, 可由 G_x 得到 $[x]$ 的訊息. 例如若 $G_x = G$ (即所有 G 中的元素對 x 作用仍是 x), 則知 $|[x]| = 1$. 也就是說在 S 中和 x 同類的只有 x 本身, 其他的元素都和 x 不同類. 這樣的 x 對我們很有用, 我們將這種特別的 x 所成的集合記為 S_0.

Proposition 4.1.4. 令 p 是一個質數. 若 G 是一個 *p-group,* 且 $(G, S, *)$ 是一個 *group action,* 其中 S 是一個有限集合. 令

$$S_0 = \{s \in S \,|\, g * s = s, \forall\, g \in G\},$$

則

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. 假設 S 可分成 $[x_1], \ldots, [x_r]$ 這 r 個同類集, 其中 $x_1, \ldots, x_t$ 在 S_0, 而 $x_{t+1}, \ldots, x_r$ 皆不屬於 S_0. 由此假設我們可知 $S_0 = \{x_1, \ldots, x_t\}$. 這是因為由假設已知 $\{x_1, \ldots, x_t\} \subseteq S_0$, 然而若 $x \in S_0$, 由於 x 只和自己同類, 它必是某個 x_i 但由 $x_{t+1}, \ldots, x_r$ 皆不屬於 S_0 的假設知 $x \in \{x_1, \ldots, x_t\}$.

回顧一下 G 是一個 p-group, 表示 $|G| = p^n$ 這種形式. 由 Lagrange 定理 (Theorem 2.2.2) 知 G 的所有的 subgroup 也是 p-group. 現若 $x \notin S_0$, 由定義知 $G_x \neq G$, 因此 $|G_x| = p^m$ 其中 $0 \leq m < n$. 也就是說 p 整除 $|G|/|G_x|$. 因此當 $i \in \{t+1, \ldots, r\}$ 時, 由於 $x_i \notin S_0$, 故由 Lemma 4.1.3 知 p 整除 $|[x_i]| = |G|/|G_{x_i}|$.

由於

$$|S| = \sum_{i=1}^{r} |[x_i]| = |S_0| + \sum_{i=t+1}^{r} |[x_i]|,$$

且由前面的討論知 p 整除 $\sum_{i=t+1}^{r} |[x_i]|$, 因此 p 整除 $|S| - |S_0|$, 也就是說 $|S| \equiv |S_0| \pmod{p}$. □

最後我們要強調, 之後我們就是要利用 Proposition 4.1.4 來證明幾個重要的定理, 因此給了一個 group action, 要知道 S_0 是哪些元素就顯得特別重要.

4.2. Cauchy's Theorem

我們曾在 Theorem 3.3.2 證明 Cauchy's Theorem, 不過當時的証明仰賴著 abelian group 的假設. 在這一節中我們將利用 group action 的方法證明 Cauchy's Theorem 事實在一般的 finite group 都是對的.

4.2.1. 證明 Cauchy's Theorem 所用的 group action. Cauchy's Theorem 有許多種的證明, 大部分都是用 group action 來處理. 而我們這裡要介紹的證明最簡明, 唯一的缺憾是所用的 group action 很特別. 不過我們曾提過, 我們不要把重點放在如何想到用這種 group action, 而是把重點放在如何利用這種 group action 所得的結果.

設 $m \in \mathbb{N}$ 是一個正整數, 令 H 是 S_m 中由 $(1\ 2 \cdots m)$ 這一個 m-cycle 所產生的 cyclic subgroup. 給定一個 group G, 我們考慮以下的一個集合 S:

$$S = \{(a_1, a_2, \ldots, a_m) \in G^m \mid a_1 \cdot a_2 \cdots a_m = e\}.$$

也就是說每一個 S 中的元素是由 m 個 G 中的元素所形成, 不過這 m 個元素是有次序性的, 而且按照這次序相乘的乘積是 identity.

現在我們要定義一個 H 對 S 的 group action. 任取 $\rho \in H, x \in S$. 我們定義 $\rho * x$ 是將原來 x 的第 i 個位置的元素放在第 $\rho(i)$ 個位置, 也就是將第 1 個位置的放在第 $\rho(1)$ 個位置, ... 依此類推. 例如若 $\sigma = (1\ 2 \cdots m)$, 任取 $x = (a_1, a_2, \ldots, a_m) \in S$. 我們有

$$\sigma * x = (a_m, a_1, a_2, \ldots, a_{m-1}).$$

也就是 $\sigma * x$ 是將原來 x 的第一個位置的元素放在第二個位置, 第二個位置的放在第三個, 依此類推, 最後因為 σ 是將 $m \mapsto 1$, 故 $\sigma * x$ 是將原來 x 第 m 個位置的元素放到第一個位置.

要證明 $(H, S, *)$ 是一個 group action, 我們首先證明 (Act3). 若 $\rho, \tau \in H$, 對任意的 $x \in S$, $\rho * x$ 是將原來 x 的第 i 個位置的元素放在第 $\rho(i)$ 個位置; 而 $\tau * x$ 是將原來 x 的第 i 個位置的元素放在第 $\tau(i)$ 個位置. 因此 $\tau * (\rho * x)$ 是將原來 $\rho * x$ 的第 $\rho(i)$ 個位置的元素放在第 $\tau(\rho(i))$ 個位置. 但 $\rho * x$ 的第 $\rho(i)$ 個位置的元素是原來 x 的第 i 個位置的元素, 因此知 $\tau * (\rho * x)$ 是將原來 x 的第 i 個位置的元素放在第 $\tau(\rho(i))$ 個位置. 而按照定義 $(\tau \cdot \rho) * x$ 是將原來 x 的第 i 個位置的元素放在第 $(\tau \cdot \rho)(i) = \tau(\rho(i))$ 個位置. 因為這是對所有的 $i \in \{1, \ldots, m\}$ 都對故得 $\tau * (\rho * x) = (\tau \cdot \rho) * x$.

接下來證明 (Act1). 因為 H 是由 $\sigma = (1\ 2\ \cdots\ m)$ 產成的 cyclic group, 故任意的 $\rho \in H$ 都是 σ^j 這種形式, 其中 $j \in \mathbb{N}$. 因此若我們證得對任意的 $x \in S$ 皆有 $\sigma * x \in S$, 則由於 (Act3) 知 $\sigma^2 * x = \sigma * (\sigma * x)$ (別忘了我們已證明了 (Act3)), 故可得 $\sigma^2 * x \in S$. 依此用數學歸納法就可得對任意的 $j \in \mathbb{N}$ 皆有 $\sigma^j * x \in S$. 所以現在我們只要證明若 $x = (a_1, a_2, \ldots, a_{m-1}, a_m) \in S$ 則 $\sigma * x \in S$. 前面我們已知 $\sigma * x = (a_m, a_1, a_2, \ldots, a_{m-1})$, 由於這些 a_i 皆在 G 中, 要證明 $\sigma * x \in S$, 我們只要證明 $a_m \cdot a_1 \cdot a_2 \cdots a_{m-1} = e$ 就可. 已知 $x = (a_1, a_2, \ldots, a_{m-1}, a_m) \in S$, 因此 $(a_1 \cdot a_2 \cdots a_{m-1}) \cdot a_m = e$. 換句話說 $a_1 \cdot a_2 \cdots a_{m-1} = a_m^{-1}$. 由於 G 是一個 group, $a_m \cdot a_m^{-1} = a_m^{-1} \cdot a_m = e$, 所以我們有 $a_m \cdot a_m^{-1} = a_m \cdot (a_1 \cdot a_2 \cdots a_{m-1}) = e$. 故知 $\sigma * x \in S$.

最後我們證 (Act2). 若 $I \in H$ 是 H 的 identity, 則由定義知 $I(i) = i$, $\forall i \in \{1, \ldots, m\}$. 所以由我們定的作用知 $I * x$ 是將 x 的第 i 個位置的元素放在第 i 個位置. 換句話說對所有的 $x \in S$, $I * x = x$.

好了, 我們已知 $(H, S, *)$ 是一個 group action. 現在來看看 S 有多少個元素. 若 $|G| = n$, 如果 S 的元素只是要求是 $(a_1, \ldots, a_m)$ 這種形式, 由於每一個座標可以任填 G 中的元素, 所以 S 共有 n^m 個元素. 不過我們的 S 還有另一個條件就是 $a_1 \cdot a_2 \cdots a_{m-1} \cdot a_m = e$. 所以前面 $m-1$ 個座標我們可以任填 G 中的元素 $a_1, \ldots, a_{m-1}$ 只要在第 m 個位置填上 $(a_1 \cdots a_{m-1})^{-1}$ 就可. 因為每一個 S 的元素都可以用這種方法得到, 所以知

$$|S| = n^{m-1}. \tag{4.2}$$

最後我們來討論 S_0 是由哪些元素組成. 若 $x = (a_1, a_2, \ldots, a_{m-1}, a_m) \in S_0$, 表示 $\sigma * x = x$. 不過已知 $\sigma * x = (a_m, a_1, \ldots, a_{m-1})$, 故得

$$a_m = a_1,\ a_1 = a_2, \ldots,\ a_{m-1} = a_m.$$

換句話說

$$a_1 = a_2 = \cdots = a_{m-1} = a_m.$$

也就是說 S_0 的元素必須是 $(a, a, \ldots, a)$ 這種形式, 但並不是任意的 $a \in G$ 都可以; 別忘了 $S_0 \subseteq S$, 故 $(a, a, \ldots, a) \in S$ 的條件告訴我們 $a^m = e$. 反之我們很容易檢驗若 $x = (a, a, \ldots, a)$, 其中 $a^m = e$, 則 $x \in S_0$. 所以我們得

$$S_0 = \{(a, a, \ldots, a) \in G^m \,|\, a \in G,\ a^m = e\}. \tag{4.3}$$

最後我們強調因 $e^m = e$, 故 $(e, e, \ldots, e) \in S_0$. 也就是說 S_0 是非空的, 即

$$|S_0| \geq 1. \tag{4.4}$$

4.2.2. Cauchy 定理. 我們現在用前面介紹的 group action 證明 Cauchy's Theorem. 再次強調前面的 G 並沒有要求 abelian, 所以我們的証明適用於一般的 group.

Theorem 4.2.1 (Cauchy's Theorem)**.** 若 G 是一個 *group* 且 p 整除 G 的個數, 其中 p 是一個質數, 則存在 $a \in G$ 滿足 $\mathrm{ord}(a) = p$.

Proof. 我們利用前面介紹的 group action, 這裡我們令 $m = p$, H 是 S_p 中由 $(1\ 2\ \cdots\ p)$ 這一個 p-cycle 所產生的 cyclic subgroup. 而

$$S = \{(a_1, \ldots, a_p) \in G^p \mid a_1 \cdot a_2 \cdots a_p = e\}.$$

若 $|G| = n$ 利用前面式子 (4.2) 知 $|S| = n^{p-1}$, 故由假設 $p \mid n$ 得 p 整除 $|S|$. 也就是說

$$|S| \equiv 0 \pmod{p} \tag{4.5}$$

由 lemma 3.4.7 知 $(1\ 2 \cdots p)$ 這一個 p-cycle 的 order 為 p, 故知 $|H| = p$. 也就是說 H 是一個 p-group. 因此利用 Proposition 4.1.4 和式子 (4.5) 知

$$|S_0| \equiv |S| \equiv 0 \pmod{p}.$$

也就是說 p 整除 $|S_0|$. 不過由式子 (4.4) 知 $|S_0| \geq 1$, 再加上 p 整除 $|S_0|$, 也就是 $|S_0|$ 是 p 的倍數且不是 0. 因此我們知

$$|S| > 1.$$

換句話說 S_0 中除了已知的 $(e, e, \ldots, e)$ 這個元素外還有其他的元素. 由式子 (4.3), 我們知道在這些元素都是 $(a, a, \ldots, a)$ 這種形式, 且 $a^p = e$. 因此得 $a \neq e$ 且 $a^p = e$, 也就是說 $\mathrm{ord}(a) = p$. □

回顧一下從前我們先證明了在 abelian group 情形下的 Cauchy 定理, 再利用它證得 abelian group 的 Sylow 定理. 將來我們也會用這一般 group 的 Cauchy 定理證明一般 group 的 Sylow 定理.

4.3. p-Group

我們曾探討過 abelian p-group. 在這一節我們特別來談一般的 p-group.

4.3.1. Conjugation as a group action. 回顧一下我們曾提過若固定 $x \in G$, 對任意的 $g \in G$, $g \cdot x \cdot g^{-1}$ 稱為 x 的一個 conjugation. 事實上這是 G 對 $S = G$ 的一個 group action.

若 G 是一個 group. 令 $S = G$, 而僅把 S 看成是一個集合. 考慮 G 對 S 的作用如下: 對任意的 $a \in G$, $x \in S$, 我們定義 $a * x = a \cdot x \cdot a^{-1}$.

我們要證明這種 $(G, S, *)$ 是一個 group action. 首先檢查 (Act1). 若 $a \in G$, $x \in S$, 則 $a * x = a \cdot x \cdot a^{-1}$. 因 a, x, a^{-1} 皆在 G 中而 G 是一個 group, 故 $a \cdot x \cdot a^{-1} \in G = S$. 得知 $a * x \in S$. 再來因 $e * x = e \cdot x \cdot e^{-1} = x$, 故知 (Act2) 也符合. 最後若 $a, b \in G$, $x \in S$, 則

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

然而

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

故由結合率知 $a * (b * x) = (a \cdot b) * x$, 得證 (Act3).

在這個 action 中因 $S = G$, 故自然知 $|S| = |G|$. 現在來看 S_0 是什麼? 照定義若 $x \in S_0$ 表示對所有的 $g \in G$ 皆有 $g * x = x$. 也就是對於此 x, 對任意的 $g \in G$, 皆須符合 $g \cdot x \cdot g^{-1} = x$. 由此推得 $g \cdot x = x \cdot g, \forall\, g \in G$. 換句話說 S_0 的元素皆需和所有 G 中的元素可交換. 反之若 $x \in S$ 可以和 G 中所有元素交換的話, 則

$$g * x = g \cdot x \cdot g^{-1} = x \cdot g \cdot g^{-1} = x,$$

也就是說 $x \in S_0$.

如果大家不健忘的話, 我們曾在 1.4 節中介紹這樣的元素所成的集合 $Z(G)$ 稱為 G 的 center, 且利用 Lemma 1.5.1 說明過 $Z(G)$ 是一個 G 的 subgroup. 總知, 我們證得了

$$S_0 = Z(G) = \{x \in G \,|\, g \cdot x = x \cdot g, \forall\, g \in G\}. \tag{4.6}$$

最後我們還是要強調因已知 $e \in Z(G)$, 故知

$$|S_0| \geq 1. \tag{4.7}$$

4.3.2. *p*-group 的性質. 在 abelian group 最好用的性質就是其每個 subgroup 都是 normal subgroup, 所以每次碰到有關 abelian group 的性質時, 我們都可先找一個 nontrivial subgroup 再利用其為 normal 得到一個 order 比較小的 quotient group, 然後就可以用 induction. 在一般的 group 這方法就不再適用了, 因為可能並不存在 nontrivial normal subgroup 讓你做 quotient group. 接下來我們將證明 p-group 就有類似的好處, 除了個數是 p 的情況外 (這是 cyclic group 所以也不會造成麻煩), 其他的 p-group 都可找到一個 nontrivial normal subgroup. 所以一些 p-group 的性質就可以用 induction 得到.

Theorem 4.3.1. *若 G 是一個 p-group, 則*

$$Z(G) \neq \{e\}.$$

也就是說在 G 中存在一個元素 $a \neq e$ 且 $a \cdot g = g \cdot a, \forall\, g \in G$.

Proof. 我們利用前面介紹的 conjugation 所造的 group action $(G, S, *)$. 由於 $|G| = |S|$, 且因 G 是一個 p-group, 故得

$$|S| \equiv 0 \pmod{p}. \tag{4.8}$$

再因 G 是 p-group, 我們可以利用 Lemma 4.1.4 和式子 (4.8) 得

$$|S_0| \equiv |S| \equiv 0 \pmod{p}.$$

再加上式子 (4.7) 我們知 $|S_0|$ 是一個正整數且是 p 的倍數. 故由式子 (4.6) 知 $|Z(G)| = |S_0| > 1$. 也因此得 $Z(G)$ 中存在著 identity 以外的元素, 故得證本定理. □

Theorem 4.3.1 和前面談的 normal subgroup 有什麼關係呢? 其實 $Z(G)$ 不只是 G 的 subgroup, 它是 G 的 normal subgroup. 因為若 $a \in Z(G)$, 則對任意的 $g \in G$, 我們皆有 $g \cdot a \cdot g^{-1} = a \in Z(G)$. 所以 $Z(G)$ 是 G 的 normal subgroup.

Corollary 4.3.2. *若 G 是一個 p-group 且 $|G| \neq p$, 則 G 不是一個 simple group.*

Proof. 若 G 是 abelian, 從前已提過這時只有當 $|G| = p$ 時才會是 simple group. 所以由假設 $|G| \neq p$ 知 G 不會是 simple group.

若 G 不是 abelian, 則 $Z(G) \subsetneq G$ 且由 Theorem 4.3.1 知 $Z(G) \neq \{e\}$, 故知 $Z(G)$ 是 G 的一個 nontrivial proper normal subgroup. 所以 G 不是一個 simple group. □

我們已知最簡單的 p-group, 即 order 為 p 的 group 是 cyclic. 我們現在來探討 order 為 p^2 的 group.

Proposition 4.3.3. *若 G 是一個 group 且 $|G| = p^2$, 則 G 是一個 abelian group.* 也就是說我們有

$$G \simeq \mathbb{Z}/p^2\mathbb{Z} \quad \text{or} \quad G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Proof. 如果 G 不是 abelian group 即表示 $Z(G) \neq G$, 再由 Theorem 4.3.1 知 $Z(G) \neq \{e\}$, 故由 Lagrange 定理 (Theorem 2.2.2) 知 $|Z(G)| = p$. 現任取 $a \in G$ 但 $a \notin Z(G)$. 考慮 a 的 centralizer

$$C(a) = \{g \in G \,|\, g \cdot a = a \cdot g\}.$$

由 Proposition 1.4.2 我們知 $C(a)$ 是 G 的一個 subgroup. 不過若 $x \in Z(G)$, 則 $x \cdot a = a \cdot x$, 故知 $x \in C(a)$. 也就是說 $Z(G) \subseteq C(a)$. 不過由假設 $a \notin Z(G)$, 但 a 本身在 $C(a)$ 中 (因 $a \cdot a = a \cdot a$), 故知 $Z(G) \subsetneq C(a)$. 這告訴我們 $|C(a)| > |Z(G)| = p$. 然而 Lagrange 定理告訴我們 $|C(a)|$ 必須整除 p^2, 因此得 $|C(a)| = p^2$. 由此推得 $C(a) = G$, 也就是所有 G 中的元素都在 $C(a)$. 換句話說所有 G 的元素都可和 a 交換. 這和我們當初假設 $a \notin Z(G)$ 相矛盾. 所以知 G 一定是 abelian group. □

Proposition 4.3.3 並不能推廣到 $|G| = p^n$, 其中 $n \geq 3$ 的狀況. 比方說將來我們將會看到存在 order 為 $8 = 2^3$ 的 nonabelian group. 不過我們倒可以用前面所提的歸納法得到以下的結果:

Proposition 4.3.4. *若 G 是一個 group, 且 $|G| = p^n$, 則 G 中存在一個 normal subgroup N 其 order 為 p^{n-1}.*

Proof. 我們用數學歸納法證明此定理. 當 $n = 1$ 時 $|G| = p$, 而 $\{e\}$ 是 G 的 normal subgroup 且 $|\{e\}| = p^{1-1} = 1$. 故在此情形是成立的.

假設對於 $|G| = p^r$, 且 $1 \leq r \leq n-1$ 時, 本定理也成立. 當 $|G| = p^n$ 時, 由 Theorem 4.3.1 知 $Z(G) \neq \{e\}$, 故由 Lagrange 定理知 $Z(G)$ 也是一個 p-group. 因 p

整除 $|Z(G)|$, 故由 Cauchy 定理 (Theorem 4.2.1) 知存在一個 $Z(G)$ 的 subgroup H 其 order 為 p. 因 $H \subseteq Z(G)$, 故若 $a \in H$, 對於所有的 $g \in G$ 皆有 $a \cdot g = g \cdot a$. 因此 $g \cdot a \cdot g^{-1} = a \cdot g \cdot g^{-1} = a \in H$, 故知 H 是 G 的一個 normal subgroup. 因 H 在 G 中 normal, 我們可考慮 $G' = G/H$ 這個 quotient group. 因 $|G'| = |G|/|H| = p^{n-1}$ 我們可以用 induction 的假設知 G' 中存在一個 normal subgroup N' 其 order 為 p^{n-2}. 然而 Correspondence 定理 (Theorem 2.7.3) 告訴我們 G 中存在一個 normal subgroup N, 符合 $H \subseteq N$ 且 $N/H = N'$. 也就是說

$$|N| = |H| \cdot |N'| = p \cdot p^{n-2} = p^{n-1}.$$

故完成本定理的証明. □

Proposition 4.3.4 的結果當然比 Corollary 4.3.2 強, 它告訴我們當 $|G| = p^n$ 時我們可找到一個 G 的 normal subgroup G_{n-1} 其 order 為 p^{n-1}. 再對 G_{n-1} 使用 Proposition 4.3.4 可得一個 G_{n-1} 的 normal subgroup G_{n-2} 其 order 為 p^{n-2}. 如此一直下去我們可得一串 G 的 subgroup:

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G,$$

其中 $|G_i| = p^i$, 且是 G_{i+1} 的 normal subgroup. 由於 G_{i+1}/G_i 是一個 order 為 p 的 group, 所以這一個 quotient group 是一個 cyclic group. 一般來說一個 group G 中若可以找到一串 subgroups: $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$, 其中 G_i 是 G_{i+1} 的 normal subgroup, 且 G_{i+1}/G_i 是一個 cyclic group, 則我們就說這個 group G 是一個 *solvable group*. Proposition 4.3.4 告訴我們一個 p-group 一定是一個 solvable group.

4.4. First Sylow's Theorem

接下來我們將介紹 Sylow 定理. Sylow 定理也有三個, 不過不像 Isomorphism 定理其他兩個可以用第一個輕鬆得到. 我們將用不同的 group action 來處理這三個定理, 為了避免造成混搖我們分成三節來個別討論它們. 在這一節我們介紹第一個 Sylow 定理.

4.4.1. Group action on left coset. 若 H 是 G 的一個 subgroup, 用 $a^{-1} \cdot b \in H$ 表示 a, b 同類的分類方法, 我們在 Lemma 2.2.1 中知道和 a 同類的元素所成的集合可用

$$a \cdot H = \{a \cdot h \,|\, h \in H\}$$

來表示. 因此我們將用 $a \cdot H$ 來表示和 a 同類的元素所成的集合, 一般來說稱 $a \cdot H$ 這樣的集合為 H 在 G 中 的一個 *left coset*. 我們再次強調一次若 $a \cdot H = b \cdot H$ 表示 $a^{-1} \cdot b \in H$. 反之, 若 $a \cdot H \neq b \cdot H$, 則 $a^{-1} \cdot b \notin H$.

若 G 是一個 finite group, 且 H 是 G 的一個 subgroup. 令 S 為所有 H 在 G 中的 left coset 所成的集合. 換言之,

$$S = \{a \cdot H \,|\, a \in G\}.$$

也就是說我們將 $a \cdot H$ 看成是一個元素. 現在我們要定一個 H 對 S 的作用: 對任意的 $h \in H$, $a \cdot H \in S$, 我們定義

$$h * (a \cdot H) = (h \cdot a) \cdot H.$$

我們要證明這樣定的 $(H, S, *)$ 是一個 group action. 首先證明 (Act1). 對任意的 $h \in H$, $a \cdot H \in S$, 由於 $h * (a \cdot H) = (h \cdot a) \cdot H$, 而 $h \cdot a$ 是 G 的一個元素, 由定義知它當然是 H 在 G 中的一個 left coset. 再來因

$$e * (a \cdot H) = (e \cdot a) \cdot H = a \cdot H,$$

故知 (Act2) 也成立. 最後若 $h, h' \in H$, 則對於任意的 $a \cdot H \in S$, 我們皆有

$$h * (h' * (a \cdot H)) = h * ((h' \cdot a) \cdot H) = (h \cdot (h' \cdot a)) \cdot H,$$

和

$$(h \cdot h') * (a \cdot H) = ((h \cdot h') \cdot a) \cdot H.$$

所以利用結合率知 (Act3) 也成立.

S 是所有 H 在 G 中的 left coset 所成的集合, 也就是說 S 的個數就是 H 在 G 中分類後可分的類別個數. 我們在證明 Lagrange 定理 (Theorem 2.2.2) 時已算出此數為 $|G|/|H|$, 故得

$$|S| = \frac{|G|}{|H|}. \tag{4.9}$$

什麼會是 S_0 呢? 若 $a \cdot H \in S_0$, 則對於所有 $h \in H$ 皆有 $h * (a \cdot H) = a \cdot H$. 然而 $h * (a \cdot H) = (h \cdot a) \cdot H$, 這告訴我們

$$a \cdot H = (h \cdot a) \cdot H.$$

也就是 $a^{-1} \cdot h \cdot a \in H$. 所以若 $a \cdot H \in S_0$ 則對於所有的 $h \in H$, 皆有 $a^{-1} \cdot h \cdot a \in H$. 反之, 若 a 符合對於所有的 $h \in H$, 皆有 $a^{-1} \cdot h \cdot a \in H$, 則 $a \cdot H \in S_0$. 所以我們得到

$$S_0 = \{a \cdot H \,|\, a^{-1} \cdot h \cdot a \in H,\ \forall\, h \in H\}. \tag{4.10}$$

由於我們想了解 S_0, 我們必須更深入的討論像 a 這種對於所有的 $h \in H$, 皆有 $a^{-1} \cdot h \cdot a \in H$ 這樣性質的元素. 若 a 有這種性質, 由定義知 $a^{-1} \cdot H \cdot a \subseteq H$. 由於 G 是一個 finite group, 由 Lemma 1.5.2 我們知 $|a^{-1} \cdot H \cdot a| = |H|$, 因此得 $a^{-1} \cdot H \cdot a = H$. 所以我們可以將式子 (4.10) 改寫成

$$S_0 = \{a \cdot H \,|\, a^{-1} \cdot H \cdot a = H\}. \tag{4.11}$$

其實我們常把符合 $a^{-1} \cdot H \cdot a = H$ 的 a 所成的集合寫成 $N(H)$, 也就是

$$N(H) = \{a \in G \,|\, a^{-1} \cdot H \cdot a = H\}.$$

其實 $N(H)$ 是 G 的一個 subgroup. 這是因為若 $a, b \in N(H)$, 則 $a^{-1} \cdot H \cdot a = H$ 且 $b^{-1} \cdot H \cdot b = H$, 所以

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

也就是 $b \cdot a \in N(H)$, 這證得了封閉性. 至於 inverse, 由於 $a^{-1} \cdot H \cdot a = H$, 所以

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

不過以上等式左邊等於 H, 而右邊可寫成 $(a^{-1})^{-1} \cdot H \cdot a^{-1}$, 故知 $a^{-1} \in N(H)$.

若 $h \in H$, 因 H 是一個 group, 我們知 $h^{-1} \in H$, 所以對於所有的 $h' \in H$ 皆有 $h^{-1} \cdot h' \cdot h \in H$. 由此知 $h^{-1} \cdot H \cdot h = H$, 也就是 $h \in N(H)$. 所以 $H \subseteq N(H)$, 換句話說 H 是 $N(H)$ 的一個 subgroup. 既然 H 是 $N(H)$ 的一個 subgroup, 由 Lagrange 定理知 $|H|$ 整除 $|N(H)|$. 別忘了由式子 (4.11) 我們有 $S_0 = \{a \cdot H \,|\, a \in N(H)\}$, 也就是說 S_0 的個數應該是 $N(H)$ 裡的元素用 H 分類後所得的類別個數, 因此我們有

$$|S_0| = \frac{|N(H)|}{|H|}. \tag{4.12}$$

我們要強調因 H 是 $N(H)$ 的 subgroup, 所以在分類時至少有 $e \cdot H = H$ 這一類. 所以知

$$|S_0| \geq 1. \tag{4.13}$$

通常我們稱 $N(H)$ 是 H 的 *normalizer*, 這是因為 H 不只是 $N(H)$ 的 subgroup, 其實是 $N(H)$ 的 normal subgroup. 要證 normal, 我們需要證: 給定 $h \in H$, 對任意的 $a \in N(H)$ 皆有 $a^{-1} \cdot h \cdot a \in H$. 然而 $a^{-1} \cdot H \cdot a = H$, 當然得 $a^{-1} \cdot h \cdot a \in H$. 我們將此寫成以下的 Lemma.

Lemma 4.4.1. *若 H 是 G 的 subgroup. 令 $N(H) = \{a \in G \,|\, a^{-1} \cdot H \cdot a = H\}$, 則 H 是 $N(H)$ 的一個 normal subgroup.*

4.4.2. Sylow p-subgroup 的存在性. 回顧一下: 若 $|G| = p^n m$, 其中 p 是一個質數且 $p \nmid m$. 如果 H 是 G 的一個 p-subgroup 且其 order 為 p^n, 則我們稱 H 是 G 的一個 Sylow p-subgroup. 第一個 Sylow 定理是說 G 中一定存在一個 Sylow p-subgroup. 事實上我們將證明比這更強一點的定理.

Theorem 4.4.2 (First Sylow's Theorem)**.** *若 G 是一個 group 且 $|G| = p^n m$, 其中 $n \geq 1$, p 是一個質數且 $p \nmid m$.*

(1) *若在 G 中存在一個 subgroup H 其 order 為 p^r 其中 $1 \leq r \leq n-1$, 則在 G 中可找到一個 subgroup K 其 order 為 p^{r+1} 且 H 是 K 的 normal subgroup.*

(2) *G 中存在一個 subgroup P 其 order 為 p^n, 也就是說 G 中存在 Sylow p-subgroup.*

Proof. (1) 我們考慮如前面提的 action 將 H 作用在 $S = \{a \cdot H \,|\, a \in G\}$. 式子 (4.10) 告訴我們

$$|S| = |G|/|H| = p^n m/p^r = p^{n-r}m.$$

故由 $r < n$ 知

$$|S| \equiv 0 \pmod{p}. \tag{4.14}$$

由於 H 是 p-group, 利用 Proposition 4.1.4 和式子 (4.14) 知

$$|S_0| \equiv |S| \equiv 0 \pmod{p}. \tag{4.15}$$

不過由 Lemma 4.4.1 知 H 是 $N(H)$ 的 normal subgroup, 所以我們可以考慮 $G' = N(H)/H$ 這一個 quotient group. 因為 $|G'| = |N(H)|/|H|$, 故式子 (4.12) 告訴我們 $|G'| = |S_0|$. 所以利用式子 (4.15) 知 p 整除 $|G'|$. 對 G' 使用 Cauchy 定理知在 G' 中存在一個 subgroup K' 其 order 為 p. 然而 $G' = N(H)/H$ 利用 Correspondence 定理 (Corollary 2.7.3) 知 $N(H)$ 中存在一個 subgroup K 符合 $H \subseteq K$ 且 $K' = K/H$. 故

$$|K| = |K'| \cdot |H| = p \cdot p^r = p^{r+1}.$$

又因為 $H \subseteq K \subseteq N(H)$, 且 H 在 $N(H)$ 中 normal, 所以當然 H 在 K 中 normal (見 Remark 2.4.2 (1)).

(2) 我們要利用 (1) 來證明 Sylow p-subgroup 是存在的. 首先因 p 整除 $|G|$ 故由 Cauchy 定理知 G 中存在一個 subgroup H_1 其 order 為 p. 如果 $n = 1$, 則證明完成. 否則因 $1 \leq n-1$ 利用 (1) 得到 G 的 subgroup H_2 其 order 為 p^2. 如此一直下去直到我們得到一個 G 的 subgroup 其 order 為 p^n. □

Theorem 4.4.2 告訴我們可以由一個小一點的 p-subgroup H 往上找到大一點的 p-subgroup K 且 H 是 K 的 normal subgroup. 而 Proposition 4.3.4 是說我們可以由一個大一點的 p-subgroup k 往下找到小一點的 p-subgroup h 且 H 是 K 的 normal subgroup. 希望大家能分辨其不同.

4.5. Second Sylow's Theorem

第一個 Sylow 定理告訴我們若 p 整除 $|G|$ 則 G 中存在 Sylow p-subgroup. 既然存在我們自然會想知道會唯一嗎? 第二個 Sylow 定理就是回答此問題.

4.5.1. Another group action on left coset. 前一節證明 First Sylow's Theorem 我們是用 H 對 G 中 H 的 left coset 作用. 這裡我們考慮 H 對 G 中令一個 subgroup P 的 left coset 作用.

若 G 是一個 finite group, H 和 P 是 G 的 subgroups. 令 $S = \{a \cdot P \,|\, a \in G\}$ 是 G 中 P 的 left coset 所成的集合. 我們定義 H 對 S 的作用如下: 對任意的 $h \in H$, $a \cdot P \in S$, 我們定義

$$h * (a \cdot P) = (h \cdot a) \cdot P.$$

利用和前一節相同的證明可知 $(H, S, *)$ 是一個 group action. 同樣的我們也知

$$|S| = \frac{|G|}{|P|}. \tag{4.16}$$

而什麼會是 S_0 呢? 若 $a \cdot P \in S_0$, 則對於所有 $h \in H$ 皆有

$$(h \cdot a) \cdot P = h * (a \cdot P) = a \cdot P.$$

這告訴我們 a 和 $h \cdot a$ 在 P 的分類之下是同類的, 也就是 $a^{-1} \cdot h \cdot a \in P$. 因為這是對所有的 $h \in H$ 都是對的, 我們可以寫成 $a^{-1} \cdot H \cdot a \subseteq P$. 因此若 $a \cdot P \in S_0$ 則我們有 $a^{-1} \cdot H \cdot a \subseteq P$. 反之, 若 a 符合 $a^{-1} \cdot H \cdot a \subseteq P$, 則 $a \cdot P \in S_0$. 所以我們得到

$$S_0 = \{a \cdot P \,|\, a^{-1} \cdot H \cdot a \subseteq P\}. \tag{4.17}$$

這裡我們要說明一件事 (和 Sylow 定理無關只是要釐清觀念). 若我們如前一節收集 G 中的元素 a 符合 $a^{-1} \cdot H \cdot a \subseteq P$ 成為一個集合 $\{a \in G \,|\, a^{-1} \cdot H \cdot a \subseteq P\}$. 這一個集合並不一定會是 G 的 subgroup (缺封閉性), 而且 P 也不會包含於它 (除非 $H \subseteq P$). 所以我們沒有如前面幾種 group action 去算 $|S_0|$ 的式子. 不過沒有關係, 在證 Second Sylow's Theorem 時我們不需要直接算 $|S_0|$.

4.5.2. Sylow p-subgroups 之間的關係. 由第一 Sylow 定理我們可找到一個 G 的 Sylow p-subgroup. 第二 Sylow 定理告訴我們如何由這一個 Sylow p-subgroup, 得到所有 G 的 Sylow p-subgroup.

Theorem 4.5.1 (Second Sylow's Theorem)**.** *令 p 是一質數. 若 G 是一個 finite group, 而 P 是 G 的一個 Sylow p-subgroup.*

(1) *若 H 是 G 的一個 p-subgroup, 則存在 $a \in G$ 使得*

$$H \subseteq a \cdot P \cdot a^{-1}.$$

(2) *若 P' 是 G 的另一個 Sylow p-subgroup, 則存在 $a \in G$ 使得*

$$P' = a \cdot P \cdot a^{-1}.$$

Proof. (1) 我們考慮前面所述 H 對 $S = \{a \cdot P \,|\, a \in G\}$ 的 group action. 假設 $|G| = p^n m$, 其中 $p \nmid m$. 因 P 是 G 的 Sylow p-subgroup, 由定義知 $|P| = p^n$. 故由式子 (4.16) 知 $|S| = |G|/|P| = m$. 然而 $p \nmid m$, 故知 p 不能整除 $|S|$, 也就是說

$$|S| \not\equiv 0 \pmod{p}. \tag{4.18}$$

由假設 H 是一個 p-group, 故由 Proposition 4.1.4 和前一式子 (4.18) 知

$$|S_0| \equiv |S| \not\equiv 0 \pmod{p}.$$

也就是說 p 不能整除 $|S_0|$. 這告訴我們 S_0 是非空的集合; 否則 $|S_0| = 0$, 這和 p 不能整除 $|S_0|$ 矛盾. 既然 S_0 是非空的, 所以存在 $a \in G$ 使得 $a \cdot P \in S_0$. 故由式子 (4.17) 知 $a^{-1} \cdot H \cdot a \subseteq P$. 這告訴我們 $H \subseteq a \cdot P \cdot a^{-1}$.

(2) 當 P' 是 G 中另一個 Sylow p-subgroup, 我們直接套用 (1) 的結果知存在 $a \in G$ 使得 $P' \subseteq a \cdot P \cdot a^{-1}$. 然而 Lemma 1.5.2 告訴我們 $|P| = |a \cdot P \cdot a^{-1}|$, 且又由定義 $|P'| = |P|$, 故得 $|P'| = |a \cdot P \cdot a^{-1}|$. 所以得證 $P' = a \cdot P \cdot a^{-1}$. □

Theorem 4.5.1 告訴我們若在 G 找到一個 Sylow p-subgroup P, 則所有的 Sylow p-subgroup 都是 $a \cdot P \cdot a^{-1}$, 這種形式. 如果 P 剛好是 G 的一個 normal subgroup, 則知任意的 $a \in G$ 都符合 $a \cdot P \cdot a^{-1} = P$, 換句話說 G 只有一個 Sylow p-subgroup. 反之, 若 P 不是 G 的 normal subgroup, 則存在一個 $a \in G$ 使得 $a \cdot P \cdot a^{-1} \neq P$. 然而 Lemma 1.5.2 告訴我們 $a \cdot P \cdot a^{-1}$ 是 G 的一個 subgroup, 且 $|a \cdot P \cdot a^{-1}| = |P|$, 換句話說 $a \cdot P \cdot a^{-1}$ 是 G 中另一個不等於 P 的 Sylow p-subgroup. 故此時 Sylow p-subgroup 並不唯一. 我們證得:

Corollary 4.5.2. *若 P 是 G 的一個 Sylow p-subgroup, 則 G 僅有一個 Sylow p-subgroup 若且為若 P 是 G 的 normal subgroup.*

Example 4.5.3. 我們知 $|A_4| = 4!/2 = 2^2 \cdot 3$. 我們考慮 A_4 的 Sylow 2-subgroup 和 Sylow 3-subgroup. 已知 A_4 中有一個 order 4 的 normal subgroup

$$N = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

因為 N 是 A_4 的 Sylow 2-subgroup, 故知 A_4 中不會有其他 order 為 4 的 subgroup. 而 $(1\ 2\ 3)$ 在 A_4 中產生的 cyclic subgroup 是 order 3, 故 $\langle(1\ 2\ 3)\rangle$ 是 A_4 的一個 Sylow 3-subgroup. 同理 $\langle(1\ 2\ 4)\rangle$ 是另一個 Sylow 3-subgroup. 所以知 $\langle(1\ 2\ 3)\rangle$ 不可能是 A_4 的 normal subgroup.

4.6. Third Sylow's Theorem

第二個 Sylow 定理很清楚的告訴我們什麼時候 Sylow p-subgroup 是唯一的. 而萬一不唯一它也告訴我們此時其他的 Sylow p-subgroup 長什麼樣子. 不過並沒有告訴我們若不唯一那麼應該有多少個. 第三 Sylow Theorem 給了我們一個還算不錯的答案.

4.6.1. Group action on the set of Sylow p-subgroups. 若 G 是一個 finite group, p 是一個整除 $|G|$ 的質數. 令 S 為 G 中所有的 Sylow p-subgroup 所成的集合 (也就是每個 Sylow p-subgroup 都看成是 S 的一個元素). 我們要介紹兩種 group action, 一個是將 G 作用在 S 上. 另一個是選定 G 中任一個 Sylow p-subgroup P 而考慮 P 對 S 的作用.

我們定義 G 對 S 的作用如下: 對任意 $a \in G$, $P' \in S$, 我們定義

$$a * P' = a \cdot P' \cdot a^{-1}.$$

我們證明 $(G, S, *)$ 是一個 group action. 首先證明 (Act1). 因 P' 是 G 的 Sylow p-subgroup, 前面已提過 Lemma 1.5.2 告訴我們 $a \cdot P' \cdot a^{-1}$ 也是 G 的 Sylow

p-subgroup. 故得 $a * P' \in S$. 而 $e * P' = e \cdot P' \cdot e^{-1} = P'$ 故 (Act2) 也成立. 最後若 $a, b \in G$, 因為

$$(a \cdot b) * P' = (a \cdot b) \cdot P' \cdot (a \cdot b)^{-1} = (a \cdot b) \cdot P' \cdot (b^{-1} \cdot a^{-1}),$$

且

$$a * (b * P') = a \cdot (b * P') \cdot a^{-1} = a \cdot (b \cdot P' \cdot b^{-1}) \cdot a^{-1},$$

故由結合率知 $(a \cdot b) * P' = a * (b * P')$. 這證明了 (Act3).

$|S|$ 是什麼呢? 無庸置疑的就是 G 中所有 Sylow p-subgroup 的個數. 這裡我們並不關心 S_0 是什麼, 主要原因在這個 group action 之下只分成一類, 所以我們可以直接計算 $|S|$. 為什麼只分成一類呢? 任選 $P_1, P_2 \in S$ 由第二 Sylow 定理 (Theorem 4.5.1) 我們知存在 $a \in G$ 使得

$$P_2 = a \cdot P_1 \cdot a^{-1} = a * P_1.$$

換句話說任選 S 中的兩元素都是同類的, 所以在此分類之下當然只有一類了. 現在我們任取一 $P' \in S$, 由式子 (4.1) 知 $|S| = |[P']|$. 所以我們只要算 $[P']$ 有多少就可以了. Lemma 4.1.3 告訴我們 $|[P']| = |G|/|G_{P'}|$, 其中 $G_{P'} = \{a \in G \,|\, a * P' = P'\}$. $G_{P'}$ 到底是什麼呢? 由定義知任何 $G_{P'}$ 中的元素 a 皆須滿足

$$P' = a * P' = a \cdot P' \cdot a^{-1}.$$

如果大家還不健忘的話該記得我們曾在 4.4 節中介紹過這樣的元素所成的集合就是 P' 的 normalizer $N(P')$. 所以我們知 $G_{P'} = N(P')$. 因此我們可得

$$|S| = |[P']| = \frac{|G|}{|N(P')|} \tag{4.19}$$

現在我們介紹另一個類似的 group action. 選定 G 中任一個 Sylow p-subgroup P, 我們定義 P 對 S (和前面同樣的 S) 的作用如下: 對任意 $x \in P$, $P' \in S$, 我們定義

$$x * P' = x \cdot P' \cdot x^{-1}.$$

這個作用和前一個幾乎相同, 只是我們拿比較小的 group 去作用. 不難看出 $(P, S, *)$ 也是一個 group action.

同樣的 S 的個數仍是所有 G 的 Sylow p-subgroup 的個數. 要注意的是這次我們作用的 group 比較小, 所以同類的元素會比較少, 因此前一次所得只分成一類的結果這兒並不一定對. 這一次我們需要算 $|S_0|$.

S_0 是什麼呢? 由定義若 $P' \in S_0$, 表示對所有 $x \in P$,

$$x \cdot P' \cdot x^{-1} = x * P' = P',$$

由 normalizer 的定義知這表示 $x \in N(P')$. 換句話說若 $P' \in S_0$ 則 P' 必須具有對所有 $x \in P$ 皆可得 $x \in N(P')$ 的性質. 也就是說: 若 $P' \in S_0$, 則 $P \subseteq N(P')$. 反

之, 若 P' 是 G 的一個 Sylow p-subgroup 且符合 $P \subseteq N(P')$, 則對任意的 $x \in P$, 皆有 $x * P' = P'$. 所以我們證得

$$S_0 = \{P' \in S \mid P \subseteq N(P')\}. \tag{4.20}$$

最後我們強調因 $P \in S$ 且 Lemma 4.4.1 告訴我們 $P \subseteq N(P)$, 故知

$$P \in S_0. \tag{4.21}$$

4.6.2. Sylow p-subgroups 的個數. 第三 Sylow 定理可以幫我們由 G 的 order 來判斷 G 的 Sylow p-subgroups 大致有多少個.

Theorem 4.6.1 (Third Sylow's Theorem)**.** 若 G 是一個 *group* 且 $|G| = p^n m$, 其中 $n \geq 1$, p 是一個質數且 $p \nmid m$. 令 r 表示 G 中所有 *Sylow p-subgroup* 的個數, 則

$$(1) \quad r \mid m; \qquad (2) \quad r \equiv 1 \pmod{p}.$$

Proof. (1) 我們利用第一個 group action $(G, S, *)$ 來證明 $r \mid m$. 由式子 (4.19) 知: 任選 $P' \in S$, 我們有 $r = |G|/|N(P')|$. 不過 Lemma 4.4.1 告訴我們 P' 是 $N(P')$ 的 subgroup. 由於 $|P'| = p^n$, Lagrange 定理告訴我們 $|N(P')|$ 是 p^n 的倍數, 又由於 $N(P')$ 是 G 的 subgroup, 再用一次 Lagrange 定理得 $|N(P')| = p^n d$ 其中 $d \mid m$. 故知

$$r = \frac{|G|}{|N(P')|} = \frac{p^n m}{p^n d} = \frac{m}{d}.$$

因此 $r \mid m$.

(2) 我們利用第二個 group action $(P, S, *)$ 來證明 $r \equiv 1 \pmod{p}$. 因 P 是一個 p-group, 由 Proposition 4.1.4 知

$$r = |S| \equiv |S_0| \pmod{p}. \tag{4.22}$$

我們現在來計算 $|S_0|$. 由式子 (4.20) 知若 $P' \in S_0$ 則 $P \subseteq N(P')$. 不過前面已知 $|N(P')| = p^n d$, 其中 $d \mid m$. 然而由 $p \nmid m$ 知 $p \nmid d$, 因此由 $|P| = p^n$ 知 P 是 $N(P')$ 的一個 Sylow p-subgroup. 另一方面, 由 Lemma 4.4.1 知, P' 是 $N(P')$ 的 normal subgroup. 但 P' 也是 $N(P')$ 的 Sylow p-subgroup. Corollary 4.5.2 告訴我們 P' 是 $N(P')$ 唯一的 Sylow p-subgroup. 故得 $P = P'$. 換句話說 S_0 中只可能有 P 這個元素. 因此由式子 (4.21) 知 $S_0 = \{P\}$, 也就是說 S_0 只有一個元素. 故由式子 (4.22) 得 $r \equiv 1 \pmod{p}$. □

Example 4.6.2. (1) 我們知道在 A_4 中 Sylow 3-subgroup 並不唯一 (Example 4.5.3), 那麼 A_4 到底有多少個 Sylow 3-subgroup 呢? 假設有 r 個, 由於 $|A_4| = 4 \cdot 3$, 由第三 Sylow 定理 (Theorem 4.6.1) 知 $r \mid 4$ 且 $r = 3k + 1$. 也就是 $r = 1$ 或 $r = 4$. 由於已知 $r \neq 1$, 故得 $r = 4$. 事實上在 A_4 中由

$$(1\ 2\ 3), \quad (1\ 2\ 4), \quad (1\ 3\ 4), \quad (2\ 3\ 4)$$

這四個 3-cycles 個別產生的 cyclic group 皆相異, 故知這些就是所有 A_4 的 Sylow 3-subgroup.

(2) 在 A_5 中有多少 Sylow 5-subgroups 呢? 假設有 r 個, 由於 $|A_5| = 5!/2 = 5\cdot 12$, 由第三 Sylow 定理 (Theorem 4.6.1) 知 $r \mid 12$ 且 $r = 5k+1$. 也就是 $r = 1$ 或 $r = 6$. 由於已知 A_5 是 simple (Theorem 3.4.26) 所以 A_5 的 Sylow 5-subgroup 不可能是 A_5 的 normal subgroup. 因此由第二 Sylow 定理 (Corollary 4.5.2) 知 $r \neq 1$. 故得 $r = 6$. 事實上在 A_5 中所有的 5-cycle 共有 $4! = 24$ 個 (為甚麼呢? 這是高中的排列組合中五個人坐圓桌的問題吧!). 不過任一個 5-cycle 所產生的 cyclic group 中有 4 個 5-cycle 出現. 例如:

$$\langle (1\ 2\ 3\ 4\ 5)\rangle = \{(1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2), I\}$$

因此這 24 個 5 cycle 只產生 $24/4 = 6$ 個相異的 order 5 的 subgroup. 這就是所有 A_5 的 Sylow 5-subgroup.

大家不要被 Example 4.6.2 誤導. 第三 Sylow 定理並不是萬靈丹, 一般來說並不能單單由一個 group 的 order 再利用第三 Sylow 定理就能算出有多少個 Sylow p-subgroup. 有時要加入所考慮的 group 的性質, 例如在 A_5 中 Sylow 2-subgroup 只用 Third Sylow's Theorem 來算就有可能有 3, 5 或 15 個. 所以要進一層的考量才可算出真正有幾個.

4.7. Sylow 定理的應用

我們已大致介紹完了 group 的一些基本性質. 在這有關 group 的最後一節中我們介紹一些可以利用 Sylow 定理得到的性質. 其實這些性質不只要用到 Sylow 定理, 還需要一些前面學過的定理輔助, 所以把它放在 group 的最後一節讓大家複習一下前面所學的, 也算給 group 一個完美的結局.

我們曾碰過有些特殊 order 的 group, 我們可以僅由其 order 就能判斷出這個 group 長甚麼樣子 (例如 order p 的 group 是 cyclic, order p^2 的 group 是 abelian). 現在我們要談更多類似的結果.

Proposition 4.7.1. *若 G 是一個 group 且 $|G| = p^n q$, 其中 $n \geq 1$, p 和 q 是相異質數且 $p > q$. 則 G 的 Sylow p-group 是 G 的 normal subgroup.*

Proof. 我們只知道 group 的 order, 沒有其他的訊息, 所以知道不可能用 normal 的定義來直接證得本定理. 相信大家會想到 Second Sylow's Theorem 吧. 如果我們能證得 G 中的 Sylow p-subgroup 只有一個, 那麼利用第二 Sylow 定理 (Corollary 4.5.2) 就可知它是 G 的 normal subgroup 了.

假設 G 有 r 個 Sylow p-subgroup. 由第三 Sylow 定理 (Theorem 4.6.1) 知 $r \mid q$ 且 $r = pk+1$. 不過若 $r \neq 1$, 表示 $r \geq p+1 > q$, 這和 $r \mid q$ 相矛盾. 因此得 $r = 1$, 故知 G 的 Sylow p-group 是 G 的 normal subgroup. □

我們接下來看 $n = 1$ 的情況.

Proposition 4.7.2. 若 G 是一個 *group* 且 $|G| = pq$, 其中 p 和 q 是相異質數且 $p > q$. 若又知 $q \nmid p-1$, 則 G 是一個 *cyclic group.*

Proof. 這就更難直接證明了. 首先由於 p, q 皆是質數, Cauchy 定理 (Theorem 4.2.1) 告訴我們 G 中有兩個 subgroups P 和 Q 其 order 分別為 p 和 q. 其實 P 是 G 的 Sylow p-subgroup, Q 是 Sylow q-subgroup. 由 Proposition 4.7.1 知 P 是 G 的 normal subgroup, 而 Q 呢? 假設 G 中有 r 個 Sylow q-subgroup. 由第三 Sylow 定理 (Theorem 4.6.1) 知 $r \mid p$ 且 $r = qk+1$. 如果 $r \neq 1$, 由 $r \mid p$ 知 $r = p$, 因此得 $p = qk+1$. 也就是 $qk = p-1$. 此和 $q \nmid p-1$ 相矛盾. 故知 $r = 1$, 也因此由第二 Sylow 定理 (Corollary 4.5.2) 知 Q 也是 G 的 normal subgroup.

P 和 Q 既然都是 normal subgroup, 如果能證明 $P \cap Q = \{e\}$ 的話由 Theorem 3.2.4 可得 $G \simeq P \times Q$. 然而 $P \cap Q$ 同時是 P 和 Q 的 subgroup (Lemma 1.5.1), 故由 Lagrange 定理 (Theorem 2.2.2) 知 $|P \cap Q|$ 同時整除 $|P| = p$ 和 $|Q| = q$. 因此得 $|P \cap Q| = 1$, 也就是說 $P \cap Q = \{e\}$.

好了我們知 $G \simeq P \times Q$, 然而 $|P| = p$, $|Q| = q$ 都是質數, 故由 Corollary 2.2.3 和 Theorem 3.1.1 知 $P \simeq \mathbb{Z}/p\mathbb{Z}$ 且 $Q \simeq \mathbb{Z}/q\mathbb{Z}$. 因此利用 Lemma 3.2.5 和 Corollary 3.2.3 得

$$G \simeq P \times Q \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}.$$

故得 G 是一個 cyclic group. □

如果 $q \mid p-1$ 怎麼辦? 我們來看最簡單的 $q = 2$ 的情況. 也就是說 $|G| = 2p$, 其中 p 是一個奇質數. 此時由 Proposition 4.7.1 知, G 中唯一的 Sylow p-subgroup P 是 G 的 normal subgroup. 又由於 $|P| = p$, 故由 Corollary 2.2.3 知存在 $a \in G$ 且 $\mathrm{ord}(a) = p$ 使得 $P = \langle a \rangle$. 因 2 整除 $|G|$, 利用 Cauchy 定理 (Theorem 4.2.1) 知存在 $b \in G$ 且 $\mathrm{ord}(b) = 2$. (注意: 此時因 Lagrange's Theorem 知 $b \notin P$ 且 $P \cap \langle b \rangle = \{e\}$.) 由 P 是 G 的 normal subgroup 知存在 $i \in \mathbb{N}$, 使得 $b \cdot a \cdot b^{-1} = a^i$. 我們要知道 i 是多少. 由於

$$b \cdot (b \cdot a \cdot b^{-1}) \cdot b^{-1} = b \cdot a^i \cdot b^{-1} = (b \cdot a \cdot b^{-1})^i = a^{i^2}.$$

而 $b^2 = (b^{-1})^2 = e$, 故 $a = a^{i^2}$. 也就是說 $a^{i^2-1} = e$. 利用 Lemma 2.3.2 得 $\mathrm{ord}(a) = p \mid i^2 - 1$. 由於 p 是質數, 我們得 $p \mid i-1$ 或 $p \mid i+1$. 也就是說 $i = pk+1$ 或 $i = pk-1$.

若 $i = pk+1$, 表示 $b \cdot a = a \cdot b$. 然而 $\langle a \rangle \cap \langle b \rangle = \{e\}$. 由 Lemma 3.4.8 知 $\mathrm{ord}(a \cdot b) = 2p = |G|$. 換句話說 G 是一個 cyclic group.

若 $i = pk-1$, 表示 $b \cdot a = a^{-1} \cdot b$, 而 $a^{-1} \neq a$ (因 $\mathrm{ord}(a) = p \neq 2$), 故知 G 不是 abelian. 若令 $B = \langle b \rangle$, 因 P 是 G 的 normal subgroup, 由第二 Isomorphism 定理 (Theorem 2.6.4) 知 $P \cdot B$ 是 G 的一個 subgroup, 且

$$P \cdot B/P \simeq B/P \cap B.$$

由於 $P \cap B = \{e\}$, 知 $|P \cdot B| = |P| \cdot |B| = 2p$. 也就是說 $P \cdot B = G$. 換句話說

$$G = \{a^i \cdot b^j \,|\, 0 \le i \le p-1,\, 0 \le j \le 1\}.$$

事實上我們可證明存在這樣的一個 group. 我們稱之為 *dihedral group of degree p*, 記作 D_p. 綜合以上我們證得了以下的結果.

Proposition 4.7.3. *若 G 是一個 group 且 $|G| = 2p$, 其中 p 是一個奇質數, 則*

$$G \simeq \mathbb{Z}/2p\mathbb{Z} \quad \text{or} \quad G \simeq D_p.$$

Proposition 4.7.3 告訴我們 D_p 是唯一的 order 為 $2p$ 的 nonabelian group. 事實上對所有的 $n \ge 3$, 都存在一個 nonabelian group

$$D_n = \{a^i \cdot b^j \,|\, 0 \le i \le n-1,\, 0 \le j \le 1\},$$

是由兩個元素 a, b 所產生, 其中 $\mathrm{ord}(a) = n$, $\mathrm{ord}(b) = 2$ 且 $b \cdot a = a^{-1} \cdot b$. 這樣的 nonabelian group, 我們稱之為 *dihedral group of degree n*. 它的 order 為 $2n$. 不過當 n 不是質數時, D_n 就不一定是唯一的 order 為 $2n$ 的 nonabelian group 了.

最後我們想以探討所有 order 小於 10 的 group 有哪些作為 group 這個部份的結束.

當然 order 為 1 的就只有 identity. order 為 2, 3, 5, 7 的 group 都是 cyclic 分別 isomorphic to, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$.

order 為 4 的 group 由 Proposition 4.3.3 知有兩種, 分別 isomorphic to $\mathbb{Z}/4\mathbb{Z}$ 和 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 同理 order 為 9 的也只有兩種, 分別 isomorphic to $\mathbb{Z}/9\mathbb{Z}$ 和 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

order 為 6 的 group 由 Proposition 4.7.3 知也有兩種, 一個是 abelian 另一個是 nonabelian, 它們分別 isomorphic to $\mathbb{Z}/6\mathbb{Z}$ 和 D_3. 有的同學或許會疑問: 我們學過 S_3 它也有 $3! = 6$ 個元素, 為何沒有列出呢? 別緊張! 事實上 S_3 是 nonabelian, 我們可以證得 $S_3 \simeq D_3$. 其中 S_3 的 (1 2 3) 就對應到 D_3 中的 order 為 3 的元素 a, 而 (1 2) 就對應到 D_3 中的 order 為 2 的元素 b, 且

$$(1\ 2)(1\ 2\ 3) = (2\ 3) = (3\ 2\ 1)(1\ 2).$$

同理 order 為 10 的 group 也有兩種, 它們分別 isomorphic to $\mathbb{Z}/10\mathbb{Z}$ 和 D_5.

最後有點棘手的是 order 為 8 的 group. Abelian 的部分還好處理, 我們知道有 $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 和 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 至於 nonabelian 部分我們已知有個

$$D_4 = \{a^i \cdot b^j \,|\, 0 \le i \le 3,\, 0 \le j \le 1\},$$

其中 $\mathrm{ord}(a) = 4$, $\mathrm{ord}(b) = 2$ 且 $b \cdot a = a^{-1} \cdot b$. 事實上還有另一個很常見的 order 為 8 的 nonabelian group Q_8, 稱之為 *quaternion group*. 最常見的 Q_8 表示法如下:

$$Q_8 = \{\pm 1, \pm i, \pm j \pm k\},$$

其中 $i^2 = j^2 = k^2 = -1$ 且 $i \cdot j = -j \cdot i = k$. 因為 Q_8 中 order 為 4 的元素有 6 個 (即 $\pm i, \pm j$ 和 $\pm k$), 而 D_4 中只有兩個 (即 a 和 a^3) 故知 Q_8 和 D_4 並不 isomorphic. 我們要證明 order 8 的 nonabelian group 只有這兩種.

Proposition 4.7.4. *若 G 是一個 order 為 8 的 nonabelian group, 則*

$$G \simeq D_4 \quad \text{or} \quad G \simeq Q_8.$$

Proof. 因 $|G| = 8$, 由 Lagrange 定理 (Corollary 2.3.4) 知 G 中元素的 order 只能是 1, 2, 4 或 8. 我們要證明 G 中必有一元素其 order 為 4. 若 G 中有元素之 order 為 8, 知 G 為 cyclic 和 G 是 nonabelian 相矛盾. 因此若沒有元素 order 為 4 表示任意 G 中非 identity 的元素的 order 皆為 2, 也就是說所有的 $g \in G$ 都滿足 $g^2 = e$. 若真如此, 任取 $a, b \in G$, 我們知

$$e = (a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b),$$

故得

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

這又和 G 是 nonabelian 相矛盾. 故知 G 中必存在 order 為 4 的元素.

現取 $a \in G$ 其中 $\text{ord}(a) = 4$. 因 $\langle a \rangle$ 是一個 order 為 $4 = 2^2$ 的 subgroup 而 $|G| = 8 = 2^3$, 故由第一 Sylow 定理 (Theorem 4.4.2) 知, G 存在一個 subgroup K 其中 $|K| = 2^{2+1}$ 且 $\langle a \rangle$ 是 K 的 normal subgroup. 但由於 $|K| = |G|$, 故知 $K = G$. 因此 $\langle a \rangle$ 是 K 的 normal subgroup.

既然 $\langle a \rangle$ 是 K 的 normal subgroup, 任取 $b \in G$ 但 $b \notin \langle a \rangle$, 皆存在 $i \in \mathbb{N}$ 使得 $b \cdot a \cdot b^{-1} = a^i$. 我們想要知道 i 為多少. 首先觀察若 $\text{ord}(b \cdot a \cdot b^{-1}) = r$, 即

$$(b \cdot a \cdot b^{-1})^r = b \cdot a^r \cdot b^{-1} = e,$$

則得 $a^r = e$. 故由 Lemma 2.3.2 知 $4 \,|\, r$. 然而 $(b \cdot a \cdot b^{-1})^4 = b \cdot a^4 \cdot b^{-1} = e$ 故知 $r \,|\, 4$. 也就是說 $\text{ord}(b \cdot a \cdot b^{-1}) = 4$. 由 Lemma 2.3.3 之只有當 $i = 1, 3$ 時 $\text{ord}(a^i) = 4$, 故知若 $b \cdot a \cdot b^{-1} = a^i$, 則 $i = 1$ 或 $i = 3$. 不過如果 $i = 1$ 表示 $b \cdot a = a \cdot b$ 故知 G 是 abelian, 此又和 G 是 nonabelian 的假設相矛盾. 因此知

$$b \cdot a = a^3 \cdot b = a^{-1} \cdot b.$$

最後由於 $b \notin \langle a \rangle$, 只有可能 $\text{ord}(b) = 2$ 或 $\text{ord}(b) = 4$. 若 $\text{ord}(b) = 2$ 則知 $G \simeq D_4$; 若 $\text{ord}(b) = 4$, 則知 $G \simeq Q_8$. 故得證 order 8 的 nonabelian group 只有兩種. □

如果同學有興趣當然可以一直找下去: order 11 的 group 有多少 (這個簡單)? order 12 的有多少? 這樣一直下去問題越來越困難. 大家應不難了解問題的困難度和 order 大小無關, 而是和其質因數的分解有關. 大家應能體會次方越大就越複雜, 例如 order 16 的 group 就有 14 個, 而 order 32 的 group 就有高達 51 個之多.

Part II

RING

Chapter 5

初級 Ring 的性質

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

5.1. Ring 的基本定義

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

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

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

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

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

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

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

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

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

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

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

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

我們列出一些 group 的性質方便以後直接引用.

Lemma 5.1.2. 假設 R 是一個 *ring,* 則*:*

(1) 對任意的 $a \in R$, $-(-a) = a$.

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

Proof. 請參考 Theorem 1.2.3 及 Corollary 1.2.5. □

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

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

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

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

5.2. 由 Ring 的定義所得的性質

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

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

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

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

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

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

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

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

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

Remark 5.2.2. 有的同學或許會利用

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

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

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

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

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

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

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

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

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

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

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

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

利用 Lemma 5.2.3 我們可以得到以下大家熟悉的等式.

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

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

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

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

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

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

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

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

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

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

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

5.3. Zero Divisor 和 Unit

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

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

當然了在定義裡的 b 也是 R 的 zero-divisor.

Example 5.3.2. 相信大家都很了解

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

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

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

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

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

但是由於 $b\neq 0$, 故 $b+c\neq c$.

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

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

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

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

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

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

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

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

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

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

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

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

Unit 有以下很好的性質:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.4. Subring

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

首先我們給 subring 一個正式的定義.

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

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

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

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

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

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

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

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

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

5.5. 一些 Noncommutative Ring

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

然而

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

由式子 (5.2) 知

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

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

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

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

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

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

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

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

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

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

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

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

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

利用式子 (5.3) 得

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

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

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

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

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

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

因此 A 是 $M_2(R)$ 的一個 unit. □

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

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

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

和

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

其中

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

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

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

但

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

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

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

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

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

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

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

Chapter 6

中級 Ring 的性質

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

6.1. Ideals 和 Quotient Rings

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

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

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

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

我們當然希望定的乘法是

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

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

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

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

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

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

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

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

因此我們自然有以下之定義:

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

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

則稱 I 為 R 的一個 *ideal*.

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

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

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

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

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

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

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

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

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

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

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

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

且

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

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

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

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

同理知

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

我們稱 R/I 是 R 的一個 *quotient ring.*

6.2. Subring 和 Ideal 的基本性質

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

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

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

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

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

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

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

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

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

另外

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

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

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

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

且

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

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

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

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

(1) $S \cap T$ 是 R 的 *subring.*

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

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

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

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

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

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

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

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

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

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

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

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

另外對任意的 $r \in R$,

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

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

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

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

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

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

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

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

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

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

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

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

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

6.3. Ring Homomorphism 和 Correspondence 定理

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

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

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

則稱此函數 ϕ 是一個 ring homomorphism.

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

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

我們會直接寫成

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

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

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

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

稱為 ϕ 的 *image.*

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

稱為 ϕ 的 *kernel.*

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

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

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

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

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

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

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

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

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

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

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

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

則 $\phi(S) = S'$.

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

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

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

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

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

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

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

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

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

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

Proof. ϕ 是 ring homomorphism 是因為

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

且

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

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

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

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

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

6.4. 三個 Ring Isomorphism 定理

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

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

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

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

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

我們可以利用 ϕ 製造以下的函數:

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

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

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

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

另一方面因為 ϕ 是 ring homomorphism, 所以

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

結合以上二式, 我們可得

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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

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

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

則 J 是 R 的 ideal 且

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

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

由 ϕ 是 ring homomorphism 知

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

且

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

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

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

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

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

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

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

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

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

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

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

6.5. 在 Commutative Ring with 1 中特殊的 Ideals

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

因此 R/P 是一個 integral domain.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chapter 7

一些常見的 Rings

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

7.1. The Ring of Integers

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

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

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

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

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

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

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

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

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

接下來我們就來看看 Theorem 7.1.1 的魔力有多大吧!

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proof. 由 Lemma 6.2.1 我們知

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

所以 $p \mid b$.

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

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

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

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

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

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

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

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

我們依然用歸納法證唯一性, 假設

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

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

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

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

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

7.2. Ring of Polynomials over a Field

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

令 F 是一個 field. 我們考慮由所有的係數在 F 的多項式

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

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

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

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

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

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

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

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

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

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

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

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

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

Proposition 7.2.3. 令 F 是一個 *field.*

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

(2) $F[x]$ 中的 *unit* 就是所有非 0 的常數.

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

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

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

接下來我們來看 polynomial ring 的餘式定理.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

所以 $p(x) \,|\, g(x)$.

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

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

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

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

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

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

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

現在我們就來看 $F[x]$ 上的唯一分解性質應該是甚麼樣子.

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

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

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

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

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

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

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

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

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

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

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

將上式移項再提出 $c \cdot p_1(x)$, 我們可得

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

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

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

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

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

且

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

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

7.3. Polynomials over the Integers

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

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

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

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

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

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

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

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

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

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

有了 Lemma 7.3.2, 我們有以下的定義.

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

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

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

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

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

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

為所要求的形式.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

又

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

□

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

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

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

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

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

由這個定義我們馬上得到以下的 Lemma.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

將上式移項再提出 $p_1(x)$, 我們可得

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

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

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

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

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

且

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

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

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

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

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

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

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

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

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

假設 $f(x) = g(x) \cdot h(x)$ 其中

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

且

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

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

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

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

$$c_r \cdot d_s = 1.$$

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

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

7.4. Quotient Field of an Integral Domain

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

驗證

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

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

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

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

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

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

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

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

首先我們就來看 D 包含於它的 quotient field.

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

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

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

且

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

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

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

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

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

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

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

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

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

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

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

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

且

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

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

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

故知

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

同理可證

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

故知 ψ 是一個 ring homomorphism.

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

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

Chapter 8

Integral Domain 上的分解性質

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

8.1. Divisor

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

首先我們還是對一個元素的因數給一個正式的定義.

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

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

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

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

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

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

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

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

(3) $a \mid b$ 且 $b \mid a$.

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

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

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

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

也就是說

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

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

為了方便起見, 我們給有 Lemma 8.1.3 中的關係一個特殊的名稱.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Definition 8.1.7. 設 R 是一個 integral domain.

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

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

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

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

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

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

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

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

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

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

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

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

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

8.2. Euclidean Domain

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

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

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

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

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

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

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

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

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

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

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

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

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

8.3. Principle Ideal Domain

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

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

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

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

首先先證明 d 是 a, b 的 common divisor. 由於

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

任取 p_i 由於

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

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

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

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

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

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

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

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

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

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

8.4. Unique Factorization Domain

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

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

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

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

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

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

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

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

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

首先我們將 a,b 的分解寫成式子 (8.1) 的形式, 且令

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

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

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

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

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

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

$$p_1^{s_1 - n_1} \mid p_2^{n_2} \cdots p_r^{n_r}.$$

由 $s_1 - n_1 \geq 1$ 得

$$p_1 \mid p_2^{n_2} \cdots p_r^{n_r}.$$

然而 p_1 是 prime, 這表示 p_1 和 $p_2, \ldots, p_r$ 中某個 p_i associates. 這和當初假設 $p_1, \ldots, p_r$ 兩兩不 associates 相矛盾, 故得 $s_i \leq n_i$, $\forall\, i = 1, \ldots, r$. 同理 $s_i \leq m_i$, $\forall\, i = 1, \ldots, r$. 故得知對所有的 $i = 1, \ldots, r$ 皆有 $s_i \leq \min\{n_i, m_i\} = t_i$. 也就是說 $c \mid d$. 故知 d 是 a, b 的 greatest common divisor. □

在前面幾節中要證明一個 integral domain 是一個 unique factorization domain, 我們都去證明這個 integral domain 中的 irreducible elements 和 prime elements 是一樣的. 事實上, 在 unique factorization domain 中 irreducible element 和 prime element 總是相同的.

Proposition 8.4.2. *若 R 是一個 unique factorization domain, 則 R 中的 irreducible elements 和 prime elements 是相同的.*

Proof. 我們已知在一個 integral domain 中 prime element 會是 irreducible element (Lemma 8.1.8). 所以我們只要證明 irreducible element 也會是 prime element.

假設 $p \in R$ 是一個 irreducible element 且 $p \mid a \cdot b$, 其中 $a, b \in R$. 由假設知存在 $h \in R$ 滿足 $a \cdot b = h \cdot p$. 首先我們將 a, b 用式子 (8.1) 的形式分解, 因此有

$$a \cdot b = (u \cdot v) \cdot p_1^{n_1 + m_1} \cdots p_r^{n_r + m_r}.$$

利用 R 是 unique factorization domain, 由 $a \cdot b$ 的分解知 p 一定和 $p_1, \ldots, p_r$ 中某一個 p_i associates. 然而 n_i 和 m_i 不同時為 0, 也就是說 $n_i \neq 0$ 或 $m_i \neq 0$. 若 $n_i \neq 0$, 則知 $p \mid a$, 而若 $m_i \neq 0$ 則有 $p \mid b$. 故得證 p 是 prime element. □

8.4.2. Polynomials over unique factorization domain. 我們將利用類似推導 $\mathbb{Z}[x]$ 是 unique factorization domain 的方法推導當 R 是 unique factorization domain 時

$$R[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in R\}$$

這種以 R 為係數的 polynomials 所形成的 polynomial ring 是一個 unique factorization domain.

若 $f(x) \in R[x]$ 且 $f(x) \neq 0$, 則我們可將 $f(x)$ 寫成 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 其中 $a_n \neq 0$. 如同前面討論 $F[x]$ 的情況我們可以定義 $\deg(f(x)) = n$. 利用和 Lemma 7.2.2 同樣的證明我們可以得到: 若 $f(x), g(x) \in R[x]$ 且皆不為 0, 則

$$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

主要的原因是 Lemma 7.2.2 的証明僅用到兩個非 0 元素相乘不為 0 (即 integral domain) 的性質, 並沒有用到 field 的性質. 利用 degree 的這個特性我們馬上有以下的性質.

Lemma 8.4.3. 令 R 是一個 *integral domain.*

(1) $R[x]$ 也是一個 *integral domain.*

(2) $R[x]$ 中的 *unit* 就是 R 中的 *unit.*

(3) 若 $a \in R$ 是 R 中的 *irreducible element* 則 a 看成是 $R[x]$ 中的元素 (即常數多項式) 時也是 *irreducible.*

Proof. (1) 若 $f(x) \neq 0$ 且 $g(x) \neq 0$, 假設 $f(x)$ 的最高次項係數是 a_n 且 $g(x)$ 的最高次項係數是 b_m, 則 $f(x) \cdot g(x)$ 的最高次項係數是 $a_n \cdot b_m$. 由於 $a_n, b_m \in R$, 且 $a_n \neq, b_m \neq 0$ 利用 R 是 integral domain 知 $a_n \cdot b_m \neq 0$. 也就是說 $f(x) \cdot g(x)$ 不可能為 0 多項式.

(2) 若 $f(x) \in R[x]$ 是 $R[x]$ 中的 unit, 則利用存在 $g(x) \in R[x]$ 滿足 $f(x) \cdot g(x) = 1$ 知 $\deg(f(x)) + \deg(g(x)) = 0$ (注意 1 是常數多項式故 degree 為 0). 故得 $\deg(f(x)) = \deg(g(x)) = 0$. 換句話說 $f(x), g(x)$ 都是常數多項式, 也就是說 $f(x), g(x) \in R$. 然而由假設 $f(x) \cdot g(x) = 1$ 知 $f(x)$ 是 R 中的 unit.

(3) 假設 $a \in R$ 是 R 中的 irreducible element. 注意由 degree 的性質知若 $g(x)$ 是 $f(x)$ 的 divisor (由於存在 $h(x) \in R[x]$ 滿足 $g(x) \cdot h(x) = f(x)$), 則 $\deg(g(x)) \leq \deg(f(x))$. 現若將 a 看成是常數多項式, 由於 $\deg(a) = 0$, 故知在 $R[x]$ 中 a 的 divisor 其 degree 也是 0. 換句話說在 $R[x]$ 中 a 的 divisor 都是 R 的元素. 故利用 a 在 R 中是 irreducible 知這些 divisor 要不是 R 中的 unit 就是和 a associates. 然而由 (2) 知 R 中的 unit 當然也是 $R[x]$ 中的 unit, 故知 a 在 $R[x]$ 依然是 irreducible. □

當 R 是一個 unique factorization domain 時, 令 F 為 R 的 quotient field. 接下來我們想利用 R 和 $F[x]$ 都是 unique factorization domain (Theorem 7.2.14) 證明 $R[x]$ 是一個 unique factorization domain.

為了將 $R[x]$ 和 $F[x]$ 的關係相連結, 我們還是得介紹和 $\mathbb{Z}[x]$ 中類似的 content 的概念. 首先由 Proposition 8.4.1 知若 $f(x) = a_n x^n + \cdots a_1 x + a_0 \in R[x]$, 則 $a_n, \ldots, a_1, a_0$ 的 greatest common divisor 是存在的.

Definition 8.4.4. 若 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ 且 $a_n, \ldots, a_1, a_0$ 的 greatest common divisor 是 R 中的 unit, 則稱 $f(x)$ 是 $R[x]$ 中的 *primitive polynomial.*

Lemma 8.4.5. 假設 R 是一個 *unique factorization domain,* 則對任意 $f(x) \in R[x]$ 且 $f(x) \neq 0$, 都可找到 $c \in R$ 且 $f^*(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomial* 滿足

$$f(x) = c \cdot f^*(x).$$

又假設

$$\begin{aligned} f(x) &= c \cdot f^*(x) \\ &= c' \cdot g(x) \end{aligned}$$

其中 $c, c' \in R$, 且 $f^*(x), g(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomials,* 則 $c \sim c'$ 且 $f^*(x) \sim g(x)$.

Proof. 首先證明存在性: 若 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 令 c 為 $a_n, \ldots, a_1, a_0$ 的 greatest common divisor. 所以對所有的 $i = 0, 1, \ldots, n$ 皆有 $a_i = c \cdot b_i$, 其中 $b_i \in R$, 而且 $b_0, \ldots, b_n$ 的 greatest common divisor 是 R 的 unit. 故令 $f^*(x) = b_n x^n + \cdots + b_1 x + b_0$, 則 $f^*(x)$ 是 $R[x]$ 的 primitive polynomial 且 $f(x) = c \cdot f^*(x)$. 故得證存在性.

接著證明唯一性: 若 $f(x) = c' \cdot g(x)$, 其中 $g(x)$ 是 $R[x]$ 的 primitive polynomial. 假設 $g(x) = a'_n x^n + \cdots + a'_1 x + a'_0$, 則對所有 $i = 0, 1, \ldots, n$, 皆有 $a_i = c' \cdot a'_i$. 換句話說 c' 是 $a_n, \ldots, a_0$ 的一個 common divisor. 因此由 c 是 $a_n, \ldots, a_0$ 的 greatest common divisor 知 $c' \mid c$. 即存在 $d \in R$ 使得 $c = c' \cdot d$. 利用 $a_i = c \cdot b_i = c' \cdot a'_i$, 我們知對所有的 $i = 0, 1, \ldots, n$, 皆有

$$c' \cdot (d \cdot b_i) = (c' \cdot d) \cdot b_i = c \cdot b_i = c' \cdot a'_i.$$

例用 $c' \neq 0$ 且 R 是 integral domain, 可得對所有的 $i = 0, 1, \ldots, n$, 皆有 $a'_i = d \cdot b_i$. 換句話說 d 是 $a'_n, \ldots, a'_0$ 的一個 common divisor. 然而由假設 $a'_n, \ldots, a'_0$ 的 greatest common divisor 是 unit, 故得 d 是 R 的一個 unit. 換句話說 $c \sim c'$. 再利用 $f(x) = c \cdot f^*(x) = c' \cdot g(x)$, 以及 $R[x]$ 是 integral domain, 得 $d \cdot f^*(x) = g(x)$. 由於 d 是 R 的 unit 也是 $R[x]$ 的 unit, 故得 $f^*(x) \sim g(x)$. □

利用 Lemma 8.4.5 的唯一性, 我們自然有以下的定義.

Definition 8.4.6. 假設 R 是一個 unique factorization domain. 若 $f(x) \in R[x]$ 可寫成 $f(x) = c \cdot f^*(x)$ 其中 $c \in R$ 且 $f^*(x)$ 是 $R[x]$ 的 primitive polynomial, 則稱 c 為 $f(x)$ 的 *content*, 定為 $c(f)$.

要注意由 Lemma 8.4.5 的證明我們知道 $f(x)$ 的 content 其實就是 $f(x)$ 所有係數的 greatest common divisor. 另外要注意的是 $f(x)$ 的 content 其實並不是一個固定的值, content 之間會差個 associates.

我們可以將 content 的定義推廣到 $F[x]$. 別忘了 F 是 R 的 quotient field, 所以 F 中每個元素都可以寫成 a/b 的形式, 其中 $a, b \in R$ 且 $b \neq 0$. 現對任意的 $f(x) = r_n x^n + \cdots + r_1 x + r_0 \in F[x]$, 由於對任意的 $i = 0, 1, \ldots, n$, 皆有 $r_i = a_i / b_i$,

其中 $a_i, b_i \in R$, 我們可找到 $d \in R$ 且 $d \neq 0$ 使得 $d \cdot f(x) \in R[x]$ (比方說令 $d = b_n \cdots b_0$). 因此利用 Lemma 8.4.5 知存在 $c \in R$ 以及 $f^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomial 使得 $d \cdot f(x) = c \cdot f^*(x)$. 由於 $d \neq 0$, 我們可將 $f(x)$ 寫成

$$f(x) = \frac{c}{d} \cdot f^*(x).$$

換句話說任意 $F[x]$ 中非 0 的 polynomial $f(x)$ 皆可寫成 $f(x) = r \cdot f^*(x)$, 其中 $r \in F$ 且 $f^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomial. 我們依然稱此 r 是 $f(x)$ 的 content 且仍記作 $c(f)$.

Corollary 8.4.7. 假設 R 是一個 *unique factorization domain,* 且 F 是 R 的 *quotient field.* 則對任意 $f(x) \in F[x]$ 且 $f(x) \neq 0$, 都可找到 $c \in F$ 且 $f^*(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomial* 滿足

$$f(x) = c \cdot f^*(x).$$

又假設

$$\begin{aligned} f(x) &= c \cdot f^*(x) \\ &= c' \cdot g(x) \end{aligned}$$

其中 $c, c' \in F$, 且 $f^*(x), g(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomials,* 則存在 $u \in R$ 是 R 的 *unit* 使得 $c = u \cdot c'$ 且 $u \cdot f^*(x) = g(x)$.

Proof. 前面已證存在性, 我們僅證唯一性. 我們將 c 和 c' 分別寫成 $c = a/b$ 且 $c' = a'/b'$, 其中 $a, a', b, b' \in R$ 且 $b \neq 0$, $b' \neq 0$. 將 $f(x)$ 乘上 $b \cdot b'$, 我們有 $(b \cdot b') \cdot f(x) \in R[x]$ 且

$$\begin{aligned} (b \cdot b') \cdot f(x) &= (a \cdot b') \cdot f^*(x) \\ &= (a' \cdot b) \cdot g(x). \end{aligned}$$

既然 $(b \cdot b') \cdot f(x) \in R[x]$ 我們可以將 Lemma 8.4.5 套用在 $(b \cdot b') \cdot f(x)$ 上, 故知存在 $u \in R$ 是 R 中的 unit 滿足 $a \cdot b' = u \cdot (a' \cdot b)$. 也就是說 $c = u \cdot c'$. 再利用 $c' \neq 0$ 及 $F[x]$ 是 integral domain 得 $u \cdot f^*(x) = g(x)$. □

和 $\mathbb{Z}[x]$ 一樣的狀況, 我們有以下的 Gauss Lemma 來幫助我們計算兩個 polynomials 相乘後之 content.

Lemma 8.4.8 (Gauss)**.** 假設 R 是一個 *unique factorization domain.* 若 $f(x), g(x) \in R[x]$ 是 $R[x]$ 中的 *primitive polynomials,* 則 $f(x) \cdot g(x)$ 依然是 $R[x]$ 中的 *primitive polynomial.*

Proof. 我們利用和 Lemma 7.3.5 相同的証明, 所以只給大略的証明. 假設 $f(x) \cdot g(x)$ 不是 primitive polynomial, 表示 $f(x) \cdot g(x)$ 所有係數的 greatest common divisor 不是 R 中的 unit. 因此利用 R 是 unique factorization domain 知存在 $p \in R$ 是 R 中的一個 irreducible (也是 prime) element 是 $f(x) \cdot g(x)$ 所有係數的 common

divisor. 然而 $f(x)$ 和 $g(x)$ 皆是 primitive polynomials, p 不可能整除所有 $f(x)$ 的係數也不可能整除所有 $g(x)$ 的係數. 所以若 i 是最小的數使得 $f(x)$ 的 x^i 項係數不能被 p 整除, 而 j 是最小的數使得 $g(x)$ 的 x^j 項係數不能被 p 整除, 則很容易看出 $f(x)\cdot g(x)$ 的 x^{i+j} 項係數不可能被 p 整除. 這和 p 是 $f(x)\cdot g(x)$ 各項係數的 common divisor 矛盾, 故得證 $f(x)\cdot g(x)$ 是 $R[x]$ 的 primitive polynomial. □

Primitive polynomial 在 $R[x]$ 中是和 $F[x]$ 溝通的橋樑, 事實上在 $R[x]$ 中不是常數的 irreducible element 都是 primitive polynomial.

Lemma 8.4.9. 假設 R 是一個 *unique factorization domain.* 若 $f(x)\in R[x]$ 是 $R[x]$ 的 *irreducible element* 且 $\deg(f(x))\geq 1$, 則 $f(x)$ 是 $R[x]$ 中的 *primitive polynomial.*

Proof. 若 $f(x)$ 是 $R[x]$ 中的 irreducible element, 由於 $f(x)$ 可寫成 $f(x)=c(f)\cdot f^*(x)$ 其中 $c(f)\in R\subseteq R[x]$ 且 $f^*(x)\in R[x]$, 故知 $c(f)$ 是 $f(x)$ 的一個 divisor. 由 $f(x)$ 是 irreducible element 的假設知 $c(f)$ 是 R 中的 unit ($f(x)$ 不可能和 $c(f)$ associates 因 $\deg(f(x))\geq 1$ 但 $\deg(c(f))=0$), 故知 $f(x)$ 是 primitive polynomial. □

若 $f(x),g(x)\in R[x]$, 由於 $R\subseteq F$, $f(x)$ 和 $g(x)$ 可同時看成是 $R[x]$ 的 polynomials 也可以看成是 $F[x]$ 的 polynomials. 因此這兩個 polynomials 間關係看成是 $R[x]$ 或 $F[x]$ 中的情況就會不同. 例如若 $g(x)=f(x)\cdot h(x)$, 其中 $h(x)\in R[x]$ 我們就說 $f(x)\mid g(x)$ in $R[x]$. 然而若 $h(x)\in F[x]$, 我們就說 $f(x)\mid g(x)$ in $F[x]$. 由於 $R[x]\subseteq F[x]$, 很自然的我們知道若 $f(x)\mid g(x)$ in $R[x]$ 則 $f(x)\mid g(x)$ in $F[x]$. 然而一般來說 $f(x)\mid g(x)$ in $F[x]$ 不見得會有 $f(x)\mid g(x)$ in $R[x]$. 不過當 $f(x)$ 是 $R[x]$ 的 primitive polynomial 時, 就對了.

Lemma 8.4.10. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field.* 假設 $f(x),g(x)\in R[x]$ 且 $f(x)$ 是 $R[x]$ 的一個 *primitive polynomial,* 則 $f(x)\mid g(x)$ *in* $F[x]$ 若且唯若 $f(x)\mid g(x)$ *in* $R[x]$.

Proof. 我們只要證明: 若 $f(x)\mid g(x)$ in $F[x]$ 則 $f(x)\mid g(x)$ in $R[x]$. 由假設知存在 $h(x)\in F[x]$ 使得 $g(x)=f(x)\cdot h(x)$. 利用 content, 我們得

$$c(g)\cdot g^*(x)=(c(f)\cdot c(h))\cdot(f^*(x)\cdot h^*(x)).$$

其中 $c(g),c(f)\in R$ 是 $g(x),f(x)$ 的 content, 而 $c(h)\in F$ 是 $h(x)$ 的 content, 且 $g^*(x)$, $f^*(x)$ 以及 $h^*(x)$ 都是 $R[x]$ 的 primitive polynomials. 利用 Lemma 8.4.8 知 $f^*(x)\cdot h^*(x)$ 是 $R[x]$ 的 primitive polynomial. 再利用 Corollary 8.4.7 知存在 $u\in R$ 是 R 的 unit 滿足 $u\cdot c(g)=c(f)\cdot c(h)$. 然而由 $f(x)$ 是 $R[x]$ 的 primitive polynomial, 知 $c(f)$ 是 R 的 unit. 又由假設 $g(x)\in R[x]$ 知 $c(g)\in R$. 故得

$$c(h)=c(f)^{-1}\cdot u\cdot c(g)\in R.$$

然而 $h(x)=c(h)\cdot h^*(x)$, 故由 $c(h)\in R$ 以及 $h^*(x)\in R[x]$ 可得 $h(x)\in R[x]$. 換句話說 $f(x)\mid g(x)$ in $R[x]$. □

利用 Lemma 8.4.10 我們可以得到 $R[x]$ 和 $F[x]$ 中 prime element 的關係.

Corollary 8.4.11. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field* 且假設 $p(x) \in R[x]$ 是 $R[x]$ 的 *primitive polynomial.* 若 $p(x)$ 是 $F[x]$ 中的 *prime element* 則 $p(x)$ 是 $R[x]$ 中的 *prime element.*

Proof. 假設 $p(x)$ 是 $F[x]$ 中的 prime element. 要證明 $p(x)$ 是 $R[x]$ 中的 prime element, 我們必須證明若 $p(x) \mid f(x) \cdot g(x)$ in $R[x]$, 其中 $f(x), g(x) \in R[x]$, 則 $p(x) \mid f(x)$ in $R[x]$ 或 $p(x) \mid g(x)$ in $R[x]$. 因 $p(x)$ 是 $R[x]$ 中的 primitive polynomial, 由 Lemma 8.4.10 我們有 $p(x) \mid f(x) \cdot g(x)$ in $F[x]$. 故利用 $p(x)$ 是 $F[x]$ 的 prime element, 我們知 $p(x) \mid f(x)$ in $F[x]$ 或 $p(x) \mid g(x)$ in $F[x]$. 再一次利用 Lemma 8.4.10, 我們知 $p(x) \mid f(x)$ in $R[x]$ 或 $p(x) \mid g(x)$ in $R[x]$, 故得證 $p(x)$ 是 $R[x]$ 的 prime element. □

另外在 $R[x]$ 和 $F[x]$ 中要區分清楚的是一個 $R[x]$ 中的 polynomial 在 $R[x]$ 和 $F[x]$ 中可否分解 (即是否 irreducible) 的關聯性.

Lemma 8.4.12. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field* 且假設 $f(x) \in R[x]$ 及 $\deg(f(x)) \geq 1$. 若存在 $g(x), h(x) \in F[x]$ 滿足 $\deg(g(x)) \geq 1$ 且 $\deg(h(x)) \geq 1$, 使得 $f(x) = g(x) \cdot h(x)$, 則存在 $m(x), n(x) \in R[x]$ 滿足 $\deg(g(x)) = \deg(m(x))$ 且 $\deg(h(x)) = \deg(n(x))$ 使得 $f(x) = m(x) \cdot n(x)$.

Proof. 利用 content 我們將 $f(x) = g(x) \cdot h(x)$ 寫成:

$$c(f) \cdot f^*(x) = (c(g) \cdot c(h)) \cdot (g^*(x) \cdot h^*(x)),$$

其中 $c(f) \in R$, $c(g), c(h) \in F$, 而 $f^*(x), g^*(x)$ 和 $h^*(x)$ 都是 $R[x]$ 的 primitive polynomial. 利用 Lemma 8.4.8 知 $g^*(x) \cdot h^*(x)$ 是 $R[x]$ 的 primitive polynomial, 故由 Lemma 8.4.5 知存在 $u \in R$ 是 R 的 unit 使得 $c(g) \cdot c(h) = c(f) \cdot u$. 換言之, $c(g) \cdot c(h) \in R$. 故若令 $m(x) = (c(g) \cdot c(h)) \cdot g^*(x) \in R[x]$, $n(x) = h^*(x)$, 則 $m(x)$, $n(x)$ 符合定理所要求. □

由 Lemma 8.4.12 我們可得 $R[x]$ 和 $F[x]$ 間 irreducible element 的關係.

Corollary 8.4.13. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field.* 若 $p(x) \in R[x]$ 滿足 $\deg(p(x)) \geq 1$ 是 $R[x]$ 的 *primitive polynomial,* 則 $p(x)$ 是 $R[x]$ 的 *irreducible element* 若且唯若 $p(x)$ 是 $F[x]$ 的 *irreducible element.*

Proof. 首先假設 $p(x)$ 是 $R[x]$ 的 irreducible element, 要證明 $p(x)$ 也是 $F[x]$ 的 irreducible element. 假如 $p(x)$ 在 $F[x]$ 不是 irreducible element, 則存在 $g(x), h(x) \in F[x]$ 滿足 $\deg(g(x)) \geq 1$ 且 $\deg(h(x)) \geq 1$ 使得 $p(x) = g(x) \cdot h(x)$. 故由 Lemma 8.4.12 知存在 $m(x), n(x) \in R[x]$ 滿足 $\deg(m(x)) \geq 1$ 且 $\deg(n(x)) \geq 1$ 使得 $p(x) = m(x) \cdot n(x)$. 換句話說由 $1 \leq \deg(m(x)) < \deg(p(x))$ 知, $m(x)$ 是 $p(x)$ 在

$R[x]$ 的一個 divisor 且既不是 unit 也不和 $p(x)$ associates. 故知 $p(x)$ 不是 $R[x]$ 的 irreducible element. 此和假設矛盾, 故知 $p(x)$ 是 $F[x]$ 的 irreducible element.

反之, 假設 $p(x)$ 是 $F(x)$ 的 irreducible element. 如果 $p(x)$ 在 $R[x]$ 中不是 irreducible, 即存在 $l(x), m(x) \in R[x]$ 滿足 $p(x) = l(x) \cdot m(x)$, 其中 $l(x)$ 和 $m(x)$ 都不是 $R[x]$ 中的 unit. 但 $l(x), m(x) \in R[x] \subseteq F[x]$, 故利用 $p(x)$ 是 $F[x]$ 中的 irreducible element 知 $l(x)$ 和 $m(x)$ 中必有一個是 $F[x]$ 中的 unit (即常數多項式). 就假設是 $l(x) = a \in R$ 吧! 由假設 a 不能是 R 的 unit, 否則 $l(x) = a$ 是 $R[x]$ 的 unit (Lemma 8.4.3). 然而由 $f(x) = l(x) \cdot m(x) = a \cdot m(x)$ 且 $m(x) \in R[x]$ 知 a 是 $f(x)$ 各項係數之 common divisor, 即 $a \mid c(f)$ in R. 但由假設 $f(x)$ 是 primitive polynomial 知 $c(f)$ 是 R 中的 unit, 故由 $a \mid c(f)$ in R 知 a 是 R 的 unit; 此和 a 不是 R 的 unit 相矛盾. 故知 $f(x)$ 在 $R[x]$ 中是 irreducible. □

接著我們來看證明 $R[x]$ 是 unique factorization domain 最關鍵的性質.

Proposition 8.4.14. 假設 R 是一個 *unique factorization domain,* 則 $R[x]$ 中的 *irreducible element* 和 *prime element* 是相同的.

Proof. 由於 $R[x]$ 是 integral domain, 我們知 $R[x]$ 的 prime element 就是 irreducible element (Lemma 8.1.8). 因此只要證明若 $f(x) \in R[x]$ 是一個 irreducible element, 則 $f(x)$ 是一個 prime element. 我們想藉由 $F[x]$ (這裡 F 是 R 的 quotient field) 中的 irreducible element 是 prime element (Proposition 7.2.11) 來證明.

首先考慮 $\deg(f(x)) = 0$ (即 $f(x) = a \in R$ 是常數) 的情形. 因 $a \in R$ 是 irreducible 且 R 是 unique factorization domain, 由 Proposition 8.4.2 知 a 是 R 的 prime element. 我們要證明 a 也是 $R[x]$ 中的 prime element. 假設 $g(x), h(x) \in R[x]$ 滿足 $a \mid g(x) \cdot h(x)$ in $R[x]$, 即存在 $l(x) \in R[x]$ 使得 $a \cdot l(x) = g(x) \cdot h(x)$. 利用 content 得

$$(a \cdot c(l)) \cdot l^*(x) = (c(g) \cdot c(h)) \cdot (g^*(x) \cdot h^*(x)),$$

其中 $c(l), c(g), c(h) \in R$ 且 $l^*(x), g^*(x), h^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomials. 由 Lemma 8.4.8 知 $g^*(x) \cdot h^*(x)$ 依然是 primitive polynomial, 故由 Lemma 8.4.5 知存在 $u \in R$ 是 R 的 unit 滿足

$$u \cdot a \cdot c(l) = c(g) \cdot c(h),$$

換句話說 $a \mid c(g) \cdot c(h)$ in R. 利用 a 是 R 的 prime element 之假設得 $a \mid c(g)$ 或 $a \mid c(h)$. 然而 $g(x) = c(g) \cdot g^*(x)$, 故若 $a \mid c(g)$ 則 $a \mid g(x)$. 同理若 $a \mid c(h)$, 則 $a \mid h(x)$. 故知 $a = f(x)$ 是 $R[x]$ 中的 prime element.

現考慮 $\deg(f(x)) \geq 1$ 的情形. 令 F 是 R 的 quotient field. 因為 $f(x)$ 是 $R[x]$ 的 irreducible element 由 Corollary 8.4.13 知 $f(x)$ 是 $F[x]$ 的 irreducible element. 然而 Proposition 7.2.11 告訴我們此時 $f(x)$ 也是 $F[x]$ 中的 prime element. 由於 Lemma 8.4.9 告訴我們 $f(x)$ 是 $R[x]$ 的 primitive polynomial, 故可套用 Corollary 8.4.11 得證 $f(x)$ 也是 $R[x]$ 中的 prime element. □

現在我們有足夠的性質來幫助我們證明 $R[x]$ 也是一個 unique factorization domain. 大家可以沿用證明 $\mathbb{Z}[x]$ 是 unique factorization domain (Theorem 7.3.13) 的方法來處理. 這裡我們想藉由 $F[x]$ 是 unique factorization domain (Theorem 7.2.14) 這個事實來推導. 這個證明不見的比較簡明, 不過可以幫助我們多了解 $R[x]$ 和 $F[x]$ 間的關聯.

Theorem 8.4.15. 假設 R 是一個 *unique factorization domain,* 則 $R[x]$ 也是一個 *unique factorization domain.*

Proof. 令 F 是 R 的 quotient field.

首先證明存在性: 即任一 $R[x]$ 中非 0 且不是 unit 的元素 $f(x)$ 可寫成有限多個 $R[x]$ 的 irreducible elements 的乘積. 首先將 $f(x)$ 寫成 $f(x) = c(f) \cdot f^*(x)$, 其中 $c(f) \in R$ 且 $f^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomial. 若 $c(f)$ 不是 unit, 則利用 R 是 unique factorization domain 我們可以將 $c(f)$ 寫成有限多個 R 中的 irreducible elements 的乘積. 利用 Lemma 8.4.3 (3) 知道 $c(f)$ 可以寫成有限多個 $R[x]$ 中的 irreducible elements 的乘積. 所以我們只要證明 $f^*(x)$ 可以寫成有限多個 irreducible elements 的乘積. 現將 $f^*(x)$ 看成是 $F[x]$ 中的元素, 則利用 $F[x]$ 是 unique factorization domain, 知道 $f^*(x) = p_1(x) \cdots p_m(x)$, 其中 $p_1(x), \ldots, p_m(x) \in F[x]$ 是 $F[x]$ 中的 irreducible elements. 再利用 content, 知每個 $p_i(x)$ 都可寫成 $p_i(x) = c(p_i) \cdot p_i^*(x)$, 其中 $p_i^*(x) \in R[x]$ 是 $R[x]$ 的 primitive polynomial. 換句話說

$$f^*(x) = (c(p_1) \cdots c(p_m)) \cdot p_1^*(x) \cdots p_m^*(x).$$

利用 Lemma 8.4.8 知 $p_1^*(x) \cdots p_m^*(x)$ 是 $R[x]$ 的 primitive polynomial, 故由 $f^*(x)$ 是 $R[x]$ 的 primitive polynomial 以及 Lemma 8.4.5 知 $c(p_1) \cdots c(p_m) = u$ 是 R 中的 unit, 由 Lemma 8.4.3 知 u 也是 $R[x]$ 的 unit. 因此我們只要證明 $p_1^*(x), \ldots p_m^*(x)$ 是 $R[x]$ 中的 irreducible elements 就可. 如此一來

$$f^*(x) = (u \cdot p_1^*(x)) \cdot p_2^*(x) \cdots p_m^*(x),$$

所以 $f^*(x)$ 可以寫成有限多個 irreducible elements 的乘積 (注意 $u \cdot p_1^*(x)$ 和 $p_1^*(x)$ associates, 所以也是 $R[x]$ 中的 irreducible element). 然而因 $p_i(x) = c(p_i) \cdot p_i^*(x)$, 由 $p_i(x)$ 在 $F[x]$ 中 irreducible 知 $p_i^*(x)$ 也是 $F[x]$ 的 irreducible element. 由於 $p_i^*(x)$ 是 $R[x]$ 的 primitive polynomial, 套用 Corollary 8.4.13 知 $p_i^*(x)$ 也是 $R[x]$ 的 irreducible element.

接著證明分解的唯一性: 其實我們可以利用 Proposition 8.4.14 直接證明唯一性, 不過這裡我們依然利用 $F[x]$ 和 R 是 unique factorization domain 來證明. 首先假設

$$\begin{aligned} f(x) &= (a_1^{n_1} \cdots a_r^{n_r}) \cdot p_1^{n_{r+1}}(x) \cdots p_v^{n_{r+v}}(x) \\ &= (b_1^{m_1} \cdots b_s^{m_s}) \cdot q_1^{m_{s+1}}(x) \cdots q_w^{m_{s+w}}(x), \end{aligned}$$

其中 $a_1, \dots a_r \in R$ (即 $\deg(a_i) = 0$) 是 $R[x]$ 中兩兩不 associates 的 irreducible elements 而 $p_1(x), \dots, p_v(x) \in R[x]$ 是 $R[x]$ 中兩兩不 associates 且 degree 大於 0 的 irreducible elements, 對於 $b_1, \dots, b_s \in R$ 以及 $q_1(x), \dots, q_w(x) \in R[x]$ 也是同樣的假設. 首先注意由於這些 $p_i(x)$ 和 $q_j(x)$ 都是 $R[x]$ 中的 irreducible elements 且 $\deg(p_i(x)) \geq 1$ 以及 $\deg(q_j(x)) \geq 1$, 由 Lemma 8.4.9 知這些 $p_i(x)$ 和 $q_j(x)$ 都是 primitive polynomial, 故由 Lemma 8.4.8 以及 Lemma 8.4.5 知存在 R 中的 unit u 滿足

$$a_1^{n_1} \cdots a_r^{n_r} = u \cdot b_1^{m_1} \cdots b_s^{m_s},$$

故利用 R 是 unique factorization domain 的性質知經過適當順序掉換我們有 $r = s$, $a_i \sim b_i$ 且 $n_i = m_i, \forall\, i = 1, \dots, r$. 所以最後我們只要考慮

$$\begin{aligned} f_0(x) &= u \cdot p_1^{n_{r+1}}(x) \cdots p_v^{n_{r+v}}(x) \\ &= q_1^{m_{s+1}}(x) \cdots q_w^{m_{s+w}}(x) \end{aligned}$$

這一部分的唯一性. 由於 $f_0(x) \in R[x] \subseteq F[x]$, 且 $p_i(x), q_i(x)$ 是 $R[x]$ 中的 irreducible elements 所以也是 $F[x]$ 中的 irreducible elements (Corollary 8.4.13), 故利用 $F[x]$ 是 unique factorization domain 知經過重排後 $v = w$, $p_i(x) = k_i \cdot q_i(x)$ 且 $n_i = m_i$, $\forall\, i = r+1, \dots r+v$, 其中 $k_i \in F$. 然而 $p_i(x)$ 和 $q_i(x)$ 都是 $R[x]$ 的 primitive polynomial, 故知 k_i 是 R 的 unit. 換言之, 對所有的 $i = r+1, \dots, r+v$, 皆有 $p_i(x) \sim q_i(x)$. 故得證唯一性. □

最後我們來看 Theorem 8.4.15 一個重要的應用. 若 R 是一個 unique factorization domain, 由 Theorem 8.4.15 知 $R' = R[x]$ 也是一個 unique factorization domain. 現考慮 $R'[y]$ 這一個以 y 為變數 R' 的元素為係數的 polynomial ring, 也就是 $R'[y]$ 的元素都是

$$f_n(x)y^n + f_{n-1}(x)y^{n-1} + \cdots + f_1(x)y + f_0(x),$$

其中對所有的 $i = 0, 1, \dots, n$, $f_i(x) \in R' = R[x]$ 是係數在 R 的 x 的多項式. 很容易看出 $R'[y] = R[x][y] = R[x, y]$ 就是以 R 的元素為係數 x, y 為變數的兩個變數的多項式所成的集合, 故再次由 Theorem 8.4.15 知 $R[x, y]$ 是 unique factorization domain. 我們可以將以上的論述推廣到 $R[x_1, \dots, x_n]$ 這個以 R 的元素為係數 $x_1, \dots, x_n$ 為變數的 n 個變數的 polynomial ring:

Theorem 8.4.16. 假設 R 是一個 *unique factorization domain,* 則 $R[x_1, \dots, x_n]$ 這個 n 個變數的 *polynomial ring* 也是一個 *unique factorization domain.*

Proof. 利用數學歸納法, 當 $n = 1$ 時 Theorem 8.4.15 告訴我們 $R[x_1]$ 是一個 integral domain. 假設 $n-1$ 時, $R' = R[x_1, \dots, x_{n-1}]$ 是 unique factorization domain. 再由 Theorem 8.4.15 知 $R'[x_n] = R[x_1, \dots, x_n]$ 也是 unique factorization domain. □

Theorem 8.4.16 是一個代數上很重要的定理, 最常見的狀況是當 F 是一個 field 時因 $F[x_1]$ 是一個 unique factorization domain, 故知 $F[x_1, \ldots, x_n]$ 也是一個 unique factorization domain.

Part III

FIELD

Chapter 9

初級 Field 的性質

這一章中我們介紹一些 field 的基本性質. 由於很多有關於 field 的性質可以用線性代數的觀點得到, 所以我們也會簡單的複習一下線性代數的基本概念.

9.1. Field 的基本性質

這一節中我們首先介紹一些直接由定義得到的 field 的性質.

回顧一下一個 field 是一個 commutative ring with 1 而且其中非 0 的元素都是 unit. 也就是若 F 是一個 field, 則 F 中的 $+$ 和 $\cdot$ 需滿足 Definition 5.1.1 中 (R1) 到 (R8) 的性質, 另外需有:

- 對任意 $a, b \in F$ 皆滿足 $a \cdot b = b \cdot a$.
- 存在 $1 \in F$ 使得對任意 $a \in F$ 皆滿足 $a \cdot 1 = 1 \cdot a = a$.
- 對任意 $a \in F$ 且 $a \neq 0$, 皆存在 $a^{-1} \in F$ 使得 $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

前兩項是要求 F 是一個 commutative ring with 1; 最後一項是要求 F 中不為 0 的元素都是 unit.

很快的利用以上的定義我們可以得到以下有關 field 簡單但重要的性質.

Lemma 9.1.1. 若 F 是一個 *field,* 則 F 是一個 *integral domain.*

Proof. 由 field 的定義已知 F 是一個 commutative ring with 1, 所以我們只要證明 F 中沒有 zero-divisor 即可. 這可有由 Lemma 5.3.7 馬上得知, 不過為了完整性我們再給一次證明.

若 $a \in F$ 是 F 中的一個 zero-divisor, 即 $a \neq 0$ 且存在 $b \neq 0$ 滿足 $a \cdot b = 0$. 然而由 $b \neq 0$ 知 b 是 F 中的 unit, 故知存在 $b^{-1} \in F$ 滿足 $b \cdot b^{-1} = 1$. 因此可得

$$0 = (a \cdot b) \cdot b^{-1} = a \cdot (b \cdot b^{-1}) = a \cdot 1 = a.$$

此和 $a \neq 0$ 的假設相矛盾, 故 a 不可能是 F 中的 zero-divisor. □

以後我們會看到 Lemma 9.1.1 在有關 field 的性質的推導過程中很多地方占了關鍵性的地位. 首先看一個簡單的例子:

Corollary 9.1.2. *假設 F 是一個 field, 令 $F^* = F \setminus \{0\}$ 表示 F 中不為 0 的元素所成的集合, 則 F^* 在乘法的運算之下是一個 abelian group.*

Proof. 利用 F 是一個 ring with 1, 我們知道 F^* 滿足 Definition 1.1.1 中 (GP2) 和 (GP3) 的條件. 再來若 $a \in F^*$ 我們知存在 $a^{-1} \in F$ 滿足 $a \cdot a^{-1} = 1$, 然而 a^{-1} 不可能是 0, 否則會造成 $a \cdot a^{-1} = a \cdot 0 = 0$. 故知 $a^{-1} \in F^*$, 也就是說 F^* 也滿足 Definition 1.1.1 中 (GP4) 的性質. 因此要證明 F^* 在乘法的運算之下是一個 group 我們僅要檢查 (GP1). 也就是說若 $a, b \in F^*$, 則 $a \cdot b \in F^*$. 然而 $a, b \in F^*$ 表示 $a, b \in F$ 且 $a \neq 0, b \neq 0$, 故由 Lemma 9.1.1 知 $a \cdot b \neq 0$, 即 $a \cdot b \in F^*$. 至於 F^* 是 abelian, 則由 F 是 commutative ring 馬上得知. □

Example 9.1.3. 考慮

$$\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

這一個 ring. 由於 5 是 $\mathbb{Z}$ 中的 irreducible element 且 $\mathbb{Z}$ 是 principle ideal domain 利用 Lemma 8.3.2 知 $5\mathbb{Z} = \big(5\big)$ 是 $\mathbb{Z}$ 中的 maximal ideal. 所以知 $\mathbb{Z}/5\mathbb{Z}$ 是一個 field (Theorem 6.5.11). 我們可以驗證

$$(\mathbb{Z}/5\mathbb{Z})^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

在乘法之下是一個 abelian group. 事實上由

$$\overline{2}^2 = \overline{4}, \quad \overline{2}^3 = \overline{3}, \quad \overline{2}^4 = \overline{1},$$

可知 $(\mathbb{Z}/5\mathbb{Z})^*$ 在乘法之下是一個 cyclic group (因 $|(\mathbb{Z}/5\mathbb{Z})^*| = 4$ 且 $\mathrm{ord}(\overline{2}) = 4$).

假設 F 是一個 field 且 $S \subseteq F$. 如果將 F 的加法與乘法運算限制在 S 中來看, S 也是一個 field, 則稱 S 是 F 的*subfield*. 因此如果 S 在 F 的加法之下是 F 的 subgroup 且 $S^* = S \setminus \{0\}$ 在 F^* 的乘法之下是 F^* 的 subgroup, 則 S 就會是 F 的 subfield. 因此利用 Lemma 1.3.4 我們有以下的檢查 subfield 的方法.

Lemma 9.1.4. *假設 F 是一個 field 且 $S \subseteq F$. 如果對任意 $a, b \in S$, 其中 $b \neq 0$ 皆有 $a - b \in S$ 且 $a \cdot b^{-1} \in S$, 則 S 是 F 的 subfield.*

接下來我們來看 field 之間 homomorphism 的性質. 若 R 和 R' 是兩個 ring 且 $\psi : R \to R'$, 其中對任意的 $a \in R$ 皆有 $\psi(a) = 0$, 則依定義 ψ 當然是 R 到 R' 的一個 ring homomorphism. 不過這種 ring homomorphism 對我們來說是無用的, 一般我們稱之為*trivial homomorphism*.

Proposition 9.1.5. *假設 F 和 F' 都是 field 且 1_F 和 $1_{F'}$ 分別是 F 和 F' 中乘法的 identity. 如果 $\psi : F \to F'$ 是一個 nontrivial 的 ring homomorphism, 則*

(1) $\psi(1_F) = 1_{F'}$.

(2) ψ 是一對一的 *homomorphism.*

Proof. (1) 我們要證明 $\psi(1_F)$ 是 F' 的乘法 identity. 由於 ψ 不是 trivial, 故存在 $a \in F$ 使得 $\psi(a) \neq 0$. 然而 $\psi(a) = \psi(a \cdot 1_F)$, 利用 ψ 是 ring homomorphism 我們得 $\psi(a) = \psi(a) \cdot \psi(1_F)$. 然而在 F' 中我們仍然有 $\psi(a) \cdot 1_{F'} = \psi(a)$, 故得 $\psi(a) \cdot \psi(1_F) = \psi(a) \cdot 1_{F'}$, 也就是說

$$\psi(a) \cdot \big(\psi(1_F) - 1_{F'}\big) = 0.$$

利用 F' 是一個 integral domain (Lemma 9.1.1) 且 $\psi(a) \neq 0$, 我們得證 $\psi(1_F) = 1_{F'}$.

(2) 要證明 ψ 是一對一的等價於要證明 $\ker(\psi) = \big(0\big)$ (Lemma 6.3.4). 然而因 $\ker(\psi)$ 一定是 F 的一個 ideal (Lemma 6.3.3) 且 F 中僅有 F 和 $\big(0\big)$ 這兩個 trivial ideals (Lemma 6.2.4) 所以可知 $\ker(\psi) = F$ 或 $\ker(\psi) = \big(0\big)$. 但如果 $\ker(\psi) = F$, 表示對任意 $a \in F$ 皆使得 $\psi(a) = 0$, 此與 ψ 不是 trivial 的 ring homomorphism 相矛盾. 故知 $\ker(\psi) = \big(0\big)$, 也就是說 ψ 是一對一的 ring homomorphism. □

9.2. Field 的 Characteristic

對一般的 field F, 若 $a \in F$, 由於 $1 \in F$, 故對任意的 $n \in \mathbb{N}$ 我們有

$$\underbrace{a + \cdots + a}_{n \text{ 次}} = \underbrace{(1 + \cdots + 1)}_{n \text{ 次}} \cdot a. \tag{9.1}$$

要注意在這裡 1 加 n 次並不等於 n, 這是由於這裡的 1 是 F 中的 1 並不是自然數 $\mathbb{N}$ 中的 1. 例如上例中 $\overline{1}$ 是 $\mathbb{Z}/5\mathbb{Z}$ 中的 1, 但

$$\overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{0},$$

而在 $\mathbb{N}$ 中 5 是不等於 0 的. 所以我們不能把式子 (9.1) 寫成

$$\underbrace{a + \cdots + a}_{n \text{ 次}} = n \cdot a.$$

不過為了方便, 對任意 $a \in F$ 且 $n \in \mathbb{N}$ 我們用 na 來表示 a 自己加自己 n 次, 也就是說

$$\underbrace{a + \cdots + a}_{n \text{ 次}} = na.$$

希望不會造成大家的困擾. 因此我們可以將式子 (9.1) 寫成

$$na = \underbrace{a + \cdots + a}_{n \text{ 次}} = \underbrace{(1 + \cdots + 1)}_{n \text{ 次}} \cdot a = (n1) \cdot a.$$

Lemma 9.2.1. 假設 F 是一個 *field,* 則對 F 下面兩種情況之一會發生*:*

(1) 對任意 $n \in \mathbb{N}$ 且 $a \in F \setminus \{0\}$ 皆有 $na \neq 0$.

(2) 存在一個 *prime* $p \in \mathbb{N}$ 使得對任意的 $a \in F$ 皆有 $pa = 0$.

Proof. 考慮 $\phi : \mathbb{Z} \to F$ 其中 $\phi(0) = 0$, 且對任意 $n \in \mathbb{N}$, $\phi(n) = n1$, $\phi(-n) = n(-1)$. 即

$$\phi(n) = \underbrace{1 + \cdots + 1}_{n \text{ 次}} \quad \text{且} \quad \phi(-n) = \underbrace{(-1) + \cdots + (-1)}_{n \text{ 次}}.$$

注意這裡的 1 是 F 中的 1, 而 -1 是 F 中 1 的加法 inverse. 很容易檢查 ϕ 是一個從 $\mathbb{Z}$ 到 F 的 ring homomorphism.

現考慮 ϕ 的 kernel. 由 ring 的 1st isomorphism theorem (Theorem 6.4.2) 我們有

$$\mathbb{Z}/\ker(\phi) \simeq \mathrm{im}(\phi).$$

然而 $\mathrm{im}(\phi)$ 會是 F 的一個 subring (Lemma 6.3.3), 故由 F 是 integral domain (Lemma 9.1.1) 知 $\mathrm{im}(\phi)$ 也是一個 integral domain. 換句話說 $\mathbb{Z}/\ker(\phi)$ 是一個 integral domain. 另一方面 $\ker(\phi)$ 會是 $\mathbb{Z}$ 的一個 ideal (Lemma 6.3.3) 故利用 Theorem 6.5.7 知 $\ker(\phi)$ 是 $\mathbb{Z}$ 的一個 prime ideal. 因 $\mathbb{Z}$ 是一個 principle ideal domain, 故存在 $a \in \mathbb{N}$ 滿足 $\ker(\phi) = \big(a\big)$. 利用 Lemma 8.1.9 我們知 $a = 0$ 或 $a = p$, 其中 p 是 $\mathbb{Z}$ 中的一個 prime.

(1) $\ker(\phi) = \big(0\big)$ 的情形: 此時因對任意的 $n \in \mathbb{N}$, 皆有 $n1 \neq 0$ (因 $n \notin \ker(\phi)$), 故知對任意的 $a \in F$ 且 $a \neq 0$, 因 F 是 integral domain, 皆有

$$na = (n1) \cdot a \neq 0.$$

(2) $\ker(\phi) = \big(p\big)$ 的情形: 此時因 $p \in \ker(\phi)$, 我們有 $p1 = 0$. 故得對任意的 $a \in F$ 皆有

$$pa = (p1) \cdot a = 0.$$

□

在 Lemma 9.2.1 中的 0 或 p 對 field 的分類上是很重要的, 因此我們有以下之定義.

Definition 9.2.2. 假設 F 是一個 field. 若對任意的 $n \in \mathbb{N}$ 且 $a \in F \setminus \{0\}$ 皆有 $na \neq 0$, 則稱 F 的 *characteristic* 是 0. 記為 $\mathrm{char}(F) = 0$. 反之若存在 $p \in \mathbb{N}$ 是 $\mathbb{Z}$ 中的 prime 使得對任意的 $a \in F$ 皆有 $pa = 0$, 則稱 F 的 *characteristic* 是 p. 記為 $\mathrm{char}(F) = p$.

例如有理數所成的 field $\mathbb{Q}$ 的 characteristic 就是 0. 又例如在 Example 9.1.3 中的 $\mathbb{Z}/5\mathbb{Z}$ 就符合對任意的 $a \in \mathbb{Z}/5\mathbb{Z}$ 皆有 $5a = 0$, 所以我們有 $\mathrm{char}(\mathbb{Z}/5\mathbb{Z}) = 5$.

要注意由 Lemma 9.2.1 我們知若 F 是一個 field, 則 $\mathrm{char}(F)$ 要不是等於 0 就是等於一個 prime p. 如果 $\mathrm{char}(F) = p \neq 0$, 則此 p 是滿足 $pa = 0$ 其中 $a \in F \setminus \{0\}$ 的最小的正整數. 因為若 $n \in \mathbb{N}$ 且 $na = 0$, 則由 F 是 integral domain 以及

$$na = (n1) \cdot a = 0$$

知 $n1 = 0$. 也就是說 $n \in \ker(\phi) = \big(p\big)$. 這告訴我們 $n \geq p$.

若 F 是一個 field 且 F 只有有限多個元素, 則我們稱 F 為一個 *finite field*.

Lemma 9.2.3. 若 F 是一個 *finite field,* 則存在一 *prime* $p \in \mathbb{N}$ 使得 $\mathrm{char}(F) = p$.

Proof. 由 Lemma 9.2.1 我們知 $\mathrm{char}(F) = 0$ 或 $\mathrm{char}(F) = p$ 其中 p 是一個質數. 我們要說明 $\mathrm{char}(F)$ 不可能是 0. 其實如果 $\mathrm{char}(F) = 0$, 表示前面定的那個 ring homomorphism $\phi : \mathbb{Z} \to F$ 符合 $\ker(\phi) = \big(0\big)$, 也就是說 ϕ 是一對一的. 換言之 $\mathbb{Z} \simeq \mathrm{im}(\phi) \subseteq F$. 然而 $\mathbb{Z}$ 有無窮多個元素, 故得到 F 中有一個 subring 其元素有無窮多個. 此和 F 是 finite field 相矛盾, 故知 $\mathrm{char}(F) = p \neq 0$. □

利用 Proposition 9.1.5 我們可得以下有關於 characteristic 的性質. 它告訴我們當兩個 field 的 characteristic 不相同時, 它們之間不可能存在 nontrivial 的 ring homomorphism.

Proposition 9.2.4. 假設 F 和 F' 是 *fields* 且 F 和 F' 之間存在 *nontrivial* 的 *ring homomorphism,* 則 $\mathrm{char}(F) = \mathrm{char}(F')$.

Proof. 假設 $\psi : F \to F'$ 不是一個 trivial 的 ring homomorphism, 由 Proposition 9.1.5 (1) 知 $\psi(1_F) = 1_{F'}$. 因此若 $\mathrm{char}(F) = p \neq 0$, 利用

$$\psi(p1_F) = \psi(0) = 0$$

以及

$$\psi(p1_F) = \psi(\underbrace{1_F + \cdots 1_F}_{p \text{ 次}}) = p\psi(1_F) = p1_{F'},$$

我們得

$$p1_{F'} = 0.$$

故知 $\mathrm{char}(F') \neq 0$. 然而若 $\mathrm{char}(F') = q \neq p$, 則因 p 和 q 皆是質數所以互質, 故存在 $m, n \in \mathbb{Z}$ 使得 $mp + nq = 1$. 因此由 $p1_{F'} = q1_{F'} = 0$ 可得

$$1_{F'} = (mp + nq)1_{F'} = 0,$$

造成矛盾. 故知 $\mathrm{char}(F) = \mathrm{char}(F')$.

另外若 $\mathrm{char}(F) = 0$, 此時對任意 $n \in \mathbb{N}$ 皆有 $n1_F \neq 0$. 利用 Proposition 9.1.5 (2) 知 $\psi(n1_F) \neq 0$. 換句話說

$$\psi(n1_F) = n\psi(1_F) = n1_{F'} \neq 0,$$

這表示 $\mathrm{char}(F') = 0$. □

最後我們來看當 $\mathrm{char}(F) = p \neq 0$ 時, 在運算上的一個特殊性質.

Lemma 9.2.5. 假設 F 是一個 *field* 且 $\mathrm{char}(F) = p \neq 0$, 則對任意 $a, b \in F$, 我們有

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \quad \text{and} \quad (a - b)^{p^n} = a^{p^n} - b^{p^n}, \quad \forall\, n \in \mathbb{N}.$$

Proof. 我們先用 induction 證明 $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. 首先考慮 $n = 1$ 的情況. 我們先檢查 $(a+b)^2$ 為何? 由於 $(a+b)^2 = a^2 + a\cdot b + b\cdot a + b^2$, 利用 F 是一個 field 知 $a\cdot b = b\cdot a$, 因此我們得 $(a+b)^2 = a^2 + 2(a\cdot b) + b^2$. 再次強調這裡 $2(a\cdot b)$ 是 $(a\cdot b) + (a\cdot b)$ 而不是 $2\cdot(a\cdot b)$. 所以繼續下去我們可以利用類似二項式定理得

$$(a+b)^p = a^p + p(a^{p-1}\cdot b) + \cdots + \binom{p}{i}(a^i\cdot b^{p-i}) + \cdots + b^p.$$

由於 $\mathrm{char}(F) = p$, 對任意 $\alpha \in F$, α 自己連加自己 p 次等於 0 (即 $p\alpha = 0$). 大家都知道當 p 是質數且當 $i = 1, \ldots, p-1$ 時, $\binom{p}{i}$ 是 p 的倍數, 故知此時 $\binom{p}{i}(a^i\cdot b^{p-i}) = 0$. 因此我們可得

$$(a+b)^p = a^p + b^p. \tag{9.2}$$

現利用歸納假設

$$(a+b)^{p^{n-1}} = a^{p^{n-1}} + b^{p^{n-1}}, \tag{9.3}$$

故利用式子 (9.2) 和 (9.3) 我們知

$$(a+b)^{p^n} = \big((a+b)^{p^{n-1}}\big)^p = (a^{p^{n-1}} + b^{p^{n-1}})^p = a^{p^n} + b^{p^n}.$$

接下來證明 $(a-b)^{p^n} = a^{p^n} - b^{p^n}$. 首先注意當 $\mathrm{char}(F) = 2$ 時, 對任意 $\alpha \in F$ 我們有 $\alpha + \alpha = 2\alpha = 0$, 故知 $\alpha = -\alpha$. 因此在 $p = 2$ 時我們自然有

$$(a-b)^{p^n} = (a+b)^{p^n} = a^{p^n} + b^{p^n} = a^{p^n} - b^{p^n}.$$

而當 p 是 odd prime number 時, 由於對任意 α 皆有 $(-\alpha)^{p^n} = -\alpha^{p^n}$ (Corollary 5.2.4), 我們得

$$(a-b)^{p^n} = \big(a + (-b)\big)^{p^n} = a^{p^n} + (-b)^{p^n} = a^{p^n} - b^{p^n}.$$

□

Lemma 9.2.5 也可以推廣到 $F[x]$ 上的運算. 注意 $F[x]$ 上的 polynomial 的係數都在 F 中, 而且 $F[x]$ 上的加法依定義是將同次項的係數都加起來. 因此若 $\mathrm{char}(F) = p$ 時, 對任意的 $f(x) = a_n x^n + \cdots + a_0 \in F[x]$ 我們都有

$$\underbrace{f(x) + \cdots + f(x)}_{p\text{ 次}} = \underbrace{(a_n + \cdots + a_n)}_{p\text{ 次}}x^n + \cdots + \underbrace{(a_0 + \cdots + a_0)}_{p\text{ 次}} = 0.$$

因此利用類似 Lemma 9.2.5 的證明我們有以下的性質:

Lemma 9.2.6. 假設 F 是一個 *field* 且 $\mathrm{char}(F) = p \neq 0$, 則對任意 $f(x) = a_m x^m + \cdots + a_0 \in F[x]$, 我們有

$$(f(x))^{p^n} = a_m^{p^n} x^{mp^n} + \cdots + a_0^{p^n}, \quad \forall\, n \in \mathbb{N}.$$

特別當 $a \in F$ 時, 我們有

$$(x-a)^{p^n} = x^{p^n} - a^{p^n}, \quad \forall\, n \in \mathbb{N}.$$

9.3. 線性代數的應用

這一節中我們先簡單的回顧一些線性代數的基本概念, 以便以後將這些概念應用在相關 field 的性質.

9.3.1. 線性代數基本性質. 在這裡我們僅簡單回顧什麼是 vector space, basis 以及 dimension. 我們不給這些基本性質的証明, 若不清楚的同學請參考一般有關線性代數的書籍.

Definition 9.3.1. 令 F 是一個 field. 我們說 V 是一個 *vector space over* F, 如果 V 本身元素間有加法 "+" 運算, 而且對任意 $c \in F$, $v \in V$ 皆有 $c \cdot v \in V$, 且滿足:

(VS1): V 在加法之下是一個 abelian group.

(VS2): 對所有的 $c \in F$ 以及 $v_1, v_2 \in V$ 皆有 $c \cdot (v_1 + v_2) = c \cdot v_1 + c \cdot v_2$.

(VS3): 對所有 $c_1, c_2 \in F$ 以及 $v \in V$ 皆有 $(c_1 + c_2) \cdot v = c_1 \cdot v + c_2 \cdot v$ 且 $c_1 \cdot (c_2 \cdot v) = (c_1 \cdot c_2) \cdot v$.

(VS4): 對任意 $v \in V$ 皆有 $1 \cdot v = v$, 其中 $1 \in F$ 是 F 乘法的 identity.

這裡要注意一般 vector space 的定義裡並沒有要求 $F \subseteq V$, 也沒有要求 V 的元素間有乘法運算. 不過將來我們討論 field 的性質時所碰到的 vector space 都會額外有 $F \subseteq V$ 以及 V 的元素間有乘法運算這兩種特性. 也就是這兩種特性使得 field 的性質比一般的 vector space 強得多.

Definition 9.3.2. 假設 F 是一個 field 且 V 是一個 vector space over F, 如果 $v_1, \ldots, v_n \in V$ 滿足對任意 $v \in F$ 皆存在 $c_1, \ldots, c_n \in F$ 使得

$$v = c_1 \cdot v_1 + \cdots + c_n \cdot v_n,$$

則稱 $v_1, \ldots, v_n$ *span* V over F.

如果一個 vector space 存在一組 $v_1, \ldots, v_n \in V$ span V over F, 則我們稱 V 是一個 *finite dimensional vector space* over F.

如果 $v_1, \ldots, v_n$ span V over F, 當然也有可能有另一組 $w_1, \ldots, w_m \in V$ 也 span V over F. 我們當然希望能找到一組元素最少的 $v_1, \ldots, v_n$ 可以 span V over F. 要達到這一點 $v_1, \ldots, v_n$ 之間至少要沒有線性關係, 要不然其中的某個 v_i 可以被其他的 v_j 展成, 我們就可以找到更少的元素 span V 了. 因此我們有以下的定義.

Definition 9.3.3. 假設 F 是一個 field 且 V 是一個 vector space over F, 如果對於 V 中的一組元素 $v_1, \ldots, v_n \in V$ 我們都找不到不全為 0 的 $c_1, \ldots, c_n \in F$ 使得

$$c_1 \cdot v_1 + \cdots + c_n \cdot v_n = 0,$$

則稱這組 $v_1, \ldots, v_n$ 是 *linearly independent* over F.

如果 $v_1, \ldots, v_n \in F$ span V 且是 linearly independent over F, 則稱 $v_1, \ldots, v_n$ 是一組 *basis* of V over F.

線性代數中最基本的性質就是當 V 是 finite dimensional vector space over F 時, 一定可以找到 V over F 的一組 basis. 雖然 basis 並不是唯一的, 不過任一組 basis 其元素個數都是相同的. 這個 basis 的個數稱之為 V over F 的 *dimension*, 我們記為 $\dim_F(V)$. 也就是說若 $\dim_F(V) = n$, 則可以找到一組 $v_1, \ldots, v_n \in V$ 是 linearly independent over F 且 span V over F.

如果 $W \subseteq V$ 且利用 V 和 F 間的運算 W 也是一個 vector space over F, 則稱 W 是 V 的一個 *subspace* over F. 以下是 dimension 一些基本的性質, 我們略去證明.

Lemma 9.3.4. 假設 F 是一個 *field* 且 V 是一個 *finite dimensional vector space over* F.

(1) 若 $v_1, \ldots, v_n$ *span* V *over* F, 則 $\dim_F(V) \leq n$.

(2) 若 $w_1, \ldots, w_m \in F$ 是 *linearly independent over* F, 則 $\dim_F(V) \geq m$.

(3) 若 W 是 V 的一個 *subspace over* F, 則 $\dim_F(V) \geq \dim_F(W)$.

9.3.2. 將 ring 看成是 vector space. 我們首先來看一些例子, 且計算其 dimension.

假設 F 是一個 field, 我們考慮 $F[x]$ 這一個 polynomial ring. 很容易看出來 $F[x]$ 和 F 滿足 Definition 9.3.1 中 (VS1) 到 (VS4) 性質, 故知 $F[x]$ 是一個 vector space over F. 至於 $F[x]$ 會不會是 finite dimensional vector space over F 呢?

Proposition 9.3.5. 假設 F 是一個 *field*, 若將 $F[x]$ 看成是一個 *vector space over* F, 則 $F[x]$ 不是 *finite dimensional vector space over* F.

Proof. 我們利用反證法. 假設 $F[x]$ 是 finite dimensional over F 且 $\dim_F(F[x]) = n$, 則考慮 $1, x, x^2, \ldots, x^n \in F[x]$, 我們要驗證 $1, x, x^2, \ldots, x^n$ 是 linearly independent over F. 這是因為對任意不全為 0 的 $c_0, c_1, \ldots, c_n$ 我們知

$$c_0 \cdot 1 + c_1 \cdot x + \cdots + c_n \cdot x^n \neq 0.$$

注意 $1, x, x^2, \ldots, x^n$ 共有 $n+1$ 個元素, 故利用 Lemma 9.3.4 (2) 知

$$n + 1 \leq \dim_F(F[x]) = n,$$

因而得到矛盾. 所以 $F[x]$ 不可能是 finite dimensional over F. □

接著我們考慮另一個 ring. 假設 $f(x) \in F[x]$ 且 $\deg(f(x)) \geq 1$, 我們考慮 $R = F[x]/\big(f(x)\big)$ 這一個 quotient ring. 回顧一下 R 中的元素都是 $\overline{g(x)}$ 的形式, 其中 $g(x) \in F[x]$. 對任意的 $c \in F$, $\overline{g(x)} \in R$, 我們定義

$$c \cdot \overline{g(x)} = \overline{c \cdot g(x)}.$$

這個運算是 well-defined. 因為若 $\overline{g(x)} = \overline{h(x)}$ 表示, $g(x) - h(x) \in \big(f(x)\big)$. 又因為 $c \in F \subseteq F[x]$ 且 $\big(f(x)\big)$ 是 $F[x]$ 的一個 ideal, 我們當然有 $c \cdot (g(x) - h(x)) \in \big(f(x)\big)$,

故知 $c\cdot\overline{g(x)}=c\cdot\overline{h(x)}$. 利用這個 F 對 R 的運算我們很容易驗證 R 是一個 vector space over F. 那麼 R 會不會是 finite dimensional vector space over F 呢?

Lemma 9.3.6. 假設 F 是一個 *field,* 若 $f(x)\in F[x]$ 且 $\deg(f(x))\geq 1$, 則 $R=F[x]/\big(f(x)\big)$ 這一個 *quotient ring* 是一個 *finite dimensional vector space over* F 而且 $\dim_F(R)=\deg(f(x))$.

Proof. 假設 $\deg(f(x))=n$, 我們要證明 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}\in R$ 是 R over F 的一組 basis.

首先證明 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}$ span R over F. 任取 $\overline{g(x)}\in R$, 其中 $g(x)\in F[x]$, 我們要找到 $c_0,c_1,\ldots,c_{n-1}\in F$ 使得

$$\overline{g(x)}=c_0\cdot\overline{1}+c_1\cdot\overline{x}+\cdots+c_{n-1}\cdot\overline{x}^{n-1}.$$

由 Theorem 7.2.4, 我們知道存在 $h(x),r(x)\in F[x]$ 滿足 $g(x)=f(x)\cdot h(x)+r(x)$, 其中 $r(x)=0$ 或 $\deg(r(x))<\deg(f(x))$. 因為 $g(x)-r(x)=f(x)\cdot h(x)\in\big(f(x)\big)$, 由 quotient ring 的定義知 $\overline{g(x)}=\overline{r(x)}$. 現若 $r(x)=0$, 知 $\overline{g(x)}=\overline{0}$, 故取 $c_0=c_1=\cdots=c_{n-1}=0$ 時可得

$$\overline{g(x)}=\overline{0}=c_0\cdot\overline{1}+c_1\cdot\overline{x}+\cdots+c_{n-1}\cdot\overline{x}^{n-1}.$$

另一方面若 $r(x)\neq 0$, 則由 $\deg(r(x))\leq n-1$ 知存在 $a_0,a_1,\ldots,a_{n-1}\in F$ 使得 $r(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$, 故令 $c_0=a_0,\ldots,c_{n-1}=a_{n-1}$ 時我們有

$$\overline{g(x)}=\overline{r(x)}=c_0\cdot\overline{1}+c_1\cdot\overline{x}+\cdots+c_{n-1}\cdot\overline{x}^{n-1}.$$

所以 R 中的元素都可由 $\overline{1},\ldots,\overline{x}^{n-1}$ span over F 得到.

接著證明 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}$ 是 linearly independent over F. 我們利用反證法. 假設存在不全為 0 的 $c_0,c_1,\cdots,c_{n-1}\in F$ 使得

$$c_0\cdot\overline{1}+c_1\cdot\overline{x}+\cdots+c_{n-1}\cdot\overline{x}^{n-1}=\overline{0},$$

表示 $g(x)=c_0+\cdots+c_{n-1}x^{n-1}$ 這個非 0 的多項式符合 $\overline{g(x)}=\overline{0}$. 換句話說 $g(x)\in\big(f(x)\big)$. 因 $g(x)\neq 0$, 故知存在 $h(x)\in F[x]$ 且 $h(x)\neq 0$ 使得 $g(x)=f(x)\cdot h(x)$. 觀察 degree 知

$$\deg(g(x))=\deg(f(x))+\deg(h(x))\geq\deg(f(x))=n,$$

不過由當初 $g(x)$ 的選取, 我們知道 $\deg(g(x))\leq n-1$, 因此得到矛盾. 故知 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}$ 是 linearly independent over F.

我們已證得 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}\in R$ 是 R over F 的一組 basis. 又因 $\overline{1},\overline{x},\ldots,\overline{x}^{n-1}$ 中共有 n 個元素, 故知 $\dim_F(R)=n=\deg(f(x))$. □

當 R 是一個 integral domain 且 F 是一個包含於 R 的 field 時, 我們也可以將 R 看成是一個 vector space over F. 事實上由 ring 的性質加上 $F\subseteq R$, Definition 9.3.1 中的 (VS1), (VS2) 以及 (VS3) 自然都符合, 我們唯一要檢查的是 (VS4). 假

設 $1_F, 1_R$ 分別是 F 和 R 乘法的 identity, 我們只要檢察 $1_F = 1_R$ 即可. 這是因為 (VS4) 是說對任意的 $a \in R$ 要符合 $1_F \cdot a = a$. 因此若能證得 $1_F = 1_R$, 那麼上式自然成立. 要注意我們曾經看過例子一個 subring 的 identity 不一定會是原來的 ring 的 identity. 不過由於現在 R 是 integral domain, 事情就沒有那麼複雜了. 我們只要任取 F 中的一個非 0 元素 c, 將它考慮成是 F 的元素, 我們有 $1_F \cdot c = c$; 另一方面將它看成是 R 的元素, 我們有 $1_R \cdot c = c$. 結合上面兩個等式得: $(1_F - 1_R) \cdot c = 0$. 由於 R 是 integral domain 且 $c \neq 0$, 所以我們有 $1_F = 1_R$.

既然 R 是一個 over F 的 vector space, 我們來看當 R 是 finite dimensional over F 時它有什麼重要特性.

Theorem 9.3.7. 假設 R 是一個 *integral domain*, F 是一個 *field* 且 $F \subseteq R$. 又假設 R 看成是一個 *vector space over* F 時是 *finite dimensional over* F, 則

(1) 對任意 $a \in R$, 皆存在一個非 0 的 $f(x) \in F[x]$ 使得 $f(a) = 0$.

(2) R 是一個 *field*.

Proof. 我們假設 $\dim_F(R) = n$.

(1) 考慮 $1, a, a^2, \ldots, a^n$ 這 $n+1$ 個 R 中的元素. 如果它們是 linearly independent over F, 則由 Lemma 9.3.4 (2) 得

$$n = \dim_F(R) \geq n + 1,$$

造成矛盾, 故知 $1, a, a^2, \ldots, a^n$ 不是 linearly independent over F. 換句話說存在不全為 0 的 $c_0, c_1, \ldots, c_n \in F$, 滿足

$$c_0 \cdot 1 + c_1 \cdot a + \cdots + c_n \cdot a^n = 0.$$

故令 $f(x) = c_0 + c_1 x + \cdots + c_n x^n$, 我們得 $f(x) \neq 0$ 且 $f(a) = 0$.

(2) 因 R 已知是 integral domain, 要證明 R 是一個 field, 我們只要證明 R 中不為 0 的元素都是 unit. 換句話說要證明對任意 $a \in R$ 且 $a \neq 0$, 皆存在 $b \in R$ 滿足 $a \cdot b = 1$. 由 (1) 知存在非 0 的多項式 $f(x)$ 滿足 $f(a) = 0$. 我們假設

$$f(x) = c_0 + c_1 x + \cdots + c_m x^m \in F[x]$$

是 $F[x]$ 中非 0 且滿足 $f(a) = 0$ 的 degree 最小的 polynomial. 由 degree 最小的假設, 我們可得 $c_0 \neq 0$. 這是因為若 $c_0 = 0$, 則由

$$f(a) = c_1 \cdot a + \cdots + c_m \cdot a^m = (c_1 + c_2 \cdot a + \cdots + c_m \cdot a^{m-1}) \cdot a = 0$$

以及 R 是 integral domain 得 $g(a) = 0$, 其中 $g(x) = c_1 + c_2 x + \cdots + c_m x^{m-1} \in F[x]$ 不為 0 且 $\deg(g(x)) < \deg(f(x))$. 此和 $f(x)$ 是 degree 最小的找法相矛盾, 故得 $c_0 \neq 0$. 現將 $f(a) = 0$ 的 c_0 移至等式的另一邊, 我們得

$$(c_1 + c_2 \cdot a + \cdots + c_m \cdot a^{m-1}) \cdot a = -c_0.$$

因此若令

$$b = (-c_0)^{-1} \cdot (c_1 + c_2 \cdot a + \cdots + c_m \cdot a^{m-1}),$$

則我們有 $a \cdot b = 1$. 注意由於 $-c_0 \in F$ 且 $-c_0 \neq 0$ 以及 F 是一個 field, 我們有 $(-c_0)^{-1} \in F \subseteq R$, 再加上 $c_1 + c_2 \cdot a + \cdots + c_m \cdot a^{m-1} \in R$ 我們得 $b \in R$, 故知 a 是 R 的一個 unit. □

利用 Theorem 9.3.7 我們可以很快的給 Proposition 9.3.5 另一個證明: 假如 $F[x]$ 是 finite dimensional over F, 由於 $F[x]$ 是 integral domain 利用 Theorem 9.3.7 我們得 $F[x]$ 會是一個 field. 但這是不可能的, 因為 $F[x]$ 中只有 degree 為 0 的元素才是 unit.

9.4. Extension Field

給定一個 field F, 我們當然可以討論其 subfield, 不過因一般 field 的理論關心的是給定 $f(x) \in F[x]$ 如果在 F 中 $f(x)$ 沒有根, 那麼如何在比 F 大的 field 找到根. 所以我們比較關心的就是所謂 F 的 extension field.

Definition 9.4.1. 給定 F 是一個 field, 若 $L \supseteq F$ 也是一個 field 而且 L 的運算限制在 F 中就是原本 F 的運算, 則我們稱 L 是 F 的一個 *extension* (或稱 *extension field*). 當然了我們也可以稱 F 是 L 的一個 *subfield*.

假設 F 是一個 field 且 L 是 F 的一個 extension field, 由 Lemma 9.1.1 知 L 是一個 integral domain, 故由前一節的討論我們知 L 是一個 vector space over F. 我們當然可以討論 L over F 的 dimension.

Definition 9.4.2. 假設 F 是一個 field 且 L 是 F 的一個 extension field. 如果將 L 看成是 over F 的一個 vector space 是一個 finite dimensional vector space over F, 則稱 L 是 F 的一個 *finite extension*. 通常我們會將 $\dim_F(L)$ 用 $[L : F]$ 來表示, 稱之為 the *degree* of L over F (而不是說 the dimension of L over F).

我們可以利用 Theorem 9.3.7 得到以下有趣的結果:

Proposition 9.4.3. 假設 F 是一個 *field* 且 L 是 F 的一個 *finite extension*. 如果 R 是 L 的一個 *subring* 且符合 $F \subseteq R \subseteq L$, 則 R 是一個 *field*.

Proof. 我們不打算用定義直接證明 R 是一個 field, 而是想套用 Theorem 9.3.7 來得到. 要套用 Theorem 9.3.7, 我們必須說明 R 是一個 integral domain 且 $\dim_F(R)$ 是有限的.

因為 L 已經是一個 integral domain (Lemma 9.1.1), 而 R 是 L 的 subring, 所以 R 當然是 integral domain. 另一方面, 我們可以把 R 看成是 L 的一個 subspace over F. 故利用 L 是 F 的一個 finite extension 的假設以及 Lemma 9.3.4 知 $\dim_F(R) \leq \dim_F(L)$, 換句話說 R 是一個 finite dimensional vector space over F. 因此利用 Theorem 9.3.7 (2) 得證 R 是一個 field. □

若 L 是 F 的一個 finite extension, 則直接將 Theorem 9.3.7 (1) 套用在 L 上, 我們馬上知對任意的 $a \in L$ 皆存在一個 $F[x]$ 中的 polynomial $f(x) \neq 0$ 滿足 $f(a) = 0$. 這樣的元素我們給它一個特殊的名字.

Definition 9.4.4. 假設 F 是一個 field 且 L 是 F 的一個 extension field. 假設 $a \in L$, 如果存在 $F[x]$ 中的一個非 0 的 polynomial $f(x)$ 滿足 $f(a) = 0$, 則稱 a 是 *algebraic* over F.

所以 Theorem 9.3.7 告訴我們以下結果:

Lemma 9.4.5. 假設 F 是一個 *field* 且 L 是 F 的一個 *finite extension,* 則 L 中的元素都是 *algebraic over* F.

當一個 extensional field of F 中的元素都是 algebraic over F 時, 我們稱這個 extension 是一個 *algebraic extension*. Lemma 9.4.5 告訴我們任何的 finite extension of F 也都是 algebraic extension of F. 不過要注意的是一個 algebraic extension of F 不一定是 finite extension of F.

最後我們再看一個有關 finite extension 重要的性質. 如果 F 是一個 field, K 是 F 的 一個 extension field, 而又 L 是 K 的一個 extension field. 也就是我們有 $F \subseteq K \subseteq L$ 這一個關係. 當然了 L 也可看成是 F 的一個 extension. 現若假設 K over F 和 L over K 都是 finite extension, 我們自然會問那麼 L 看成是 F 的 extension 時是否也是 finite extension?

Theorem 9.4.6. 假設 F 是一個 *field,* L 和 K 都是 F 的 *extensions* 且符合 $F \subseteq K \subseteq L$. 若已知 K 是 F 的一個 *finite extension* 且 L 是 K 的一個 *finite extension,* 則 L 也是 F 的一個 *finite extension,* 而且

$$[L : F] = [L : K][K : F].$$

Proof. 假設 $[K : F] = m$ 以及 $[L : K] = n$, 我們想證明 L 是一個 finite extension of F 且其 degree 為 $m \cdot n$. 由 $[K : F] = m$ 的假設知 $\dim_F(K) = m$, 即存在 $a_1, \ldots, a_m \in K$ 是 K over F 的一組 basis. 同樣的存在 $b_1, \ldots, b_n \in L$ 是 L over K 的一組 basis. 我們想證明

$$\{a_i \cdot b_j\}, \quad i = 1, \ldots, m \text{ 且 } j = 1, \ldots, n$$

是 L over F 的一組 basis. 如此自然得證本定理. 首先要注意的是因為 $K \subseteq L$ 所以由 $a_i \in K$, $b_j \in L$ 自然可得 $a_i \cdot b_j \in L$. 我們要證明這些 $a_i \cdot b_j$ span L over F 且是 linearly independent over F.

首先證明 $\{a_i \cdot b_j\}$ span L over F: 任取 $\alpha \in L$, 我們要找到 $c_{i,j} \in F$ 使得

$$\alpha = \sum_{j=1}^{n} \sum_{i=1}^{m} c_{i,j} \cdot (a_i \cdot b_j).$$

然而因 $b_1, \ldots, b_n$ span L over K, 我們可以找到 $d_1, \ldots, d_n \in K$ 使得

$$\alpha = d_1 \cdot b_1 + \cdots + d_n \cdot b_n. \tag{9.4}$$

再利用 $a_1, \ldots, a_m$ span K over F, 對任一 $d_j \in K$, 我們都可以找到 $c_{1,j}, \ldots, c_{m,j} \in F$ 使得

$$d_j = c_{1,j} \cdot a_1 + c_{2,j} \cdot a_2 + \cdots + c_{m,j} \cdot a_m.$$

將這些 d_j 帶入式子 (9.4), 得證$\{a_i \cdot b_j\}$ span L over F.

接著證明 $\{a_i \cdot b_j\}$ 是 linearly independent over F. 利用反證法, 假設存在一組不全為 0 的 $c_{i,j} \in F$ 使得 $\sum c_{i,j} \cdot (a_i \cdot b_j) = 0$. 這表示

$$\begin{aligned} 0 \;=\; & (c_{1,1} \cdot a_1 + c_{2,1} \cdot a_2 + \cdots + c_{m,1} \cdot a_m) \cdot b_1 \\ & + \cdots + (c_{1,n} \cdot a_1 + c_{2,n} \cdot a_2 + \cdots + c_{m,n} \cdot a_m) \cdot b_n \end{aligned}$$

注意對任意的 $j = 1, \ldots, n$, 若令

$$d_j = c_{1,j} \cdot a_1 + c_{2,j} \cdot a_2 + \cdots + c_{m,j} \cdot a_m,$$

因為 $c_{i,j} \in F$, $a_i \in K$ 且 $F \subseteq K$, 我們有 $d_j \in K$ 且

$$0 = d_1 \cdot b_1 + d_2 \cdot b_2 + \cdots + d_n \cdot b_n.$$

因為 $b_1, \ldots, b_n$ 是 linearly independent over K, 故得 $d_1 = d_2 = \cdots = d_n = 0$. 換句話說對任意的 $j = 1, \ldots, n$, 皆有

$$0 = d_j = c_{1,j} \cdot a_1 + c_{2,j} \cdot a_2 + \cdots + c_{m,j} \cdot a_m.$$

再利用 $a_1, \ldots, a_m$ 是 linearly independent over F 以及這些 $c_{i,j}$ 皆屬於 F, 我們得這些 $c_{i,j}$ 皆等於 0. 此和當初假設 $c_{i,j}$ 不全為 0 相矛盾, 故得證 $\{a_i \cdot b_j\}$ 是 linearly independent over F. □

要注意 Theorem 9.4.6 中的條件是要求 K 是 F 的 finite extension 且 L 是 K 的 finite extension 才能推得 L 是 F 的 finite extension. 我們自然會問反過來對嗎? 也就是說但如果已知 L 是 F 的 finite extension, 我們是否可得 K 是 F 的 finite extension 且 L 是 K 的 finite extension 呢? 答案是肯定的, 事實上我們有以下的結果:

Corollary 9.4.7. 假設 F 是一個 *field,* L 和 K 都是 F 的 *extensions* 且符合 $F \subseteq K \subseteq L$. 若已知 L 是 F 的一個 *finite extension,* 則 K 是 F 的一個 *finite extension* 且 L 是 K 的一個 *finite extension,* 而且

$$[L : F] = [L : K][K : F].$$

Proof. 由 $F \subseteq K \subseteq L$ 這個關係式, 我們可將 K 看成是 L over F 的 subspace, 所以由 Lemma 9.3.4 (3) 知 $\dim_F(L) \geq \dim_F(K)$, 換句話說若 L over F 是一個 finite extension 那麼 K over F 當然也是 finite extension. 另一方面若假設 $[L : F] = \dim_F(L) = n$, 也就說存在 $a_1, \ldots, a_n \in L$ 是一組 L over F 的 basis, 由於

$a_1, \ldots, a_n$ span L over F 再加上 $F \subseteq K$, 我們當然知 $a_1, \ldots, a_n$ 也 span L over K. 所以利用 Lemma 9.3.4 (1) 知 $\dim_K(L) \leq n = \dim_F(L)$. 因此得 L 是 K 的一個 finite extension.

上面已證若 L 是 F 的一個 finite extension, 則 K 是 F 的一個 finite extension 且 L 是 K 的一個 finite extension. 因此可套用 Theorem 9.4.6 得證

$$[L : F] = [L : K][K : F].$$

□

Chapter 10

中級 Field 的性質

在這一章中我們要更進一步探討 algebraic element 以及 algebraic extension 的性質. 另外我們也會利用所得的性質來探討一些有關 finite field 的基本性質.

10.1. Algebraic Elements

假設 F 是一個 field, L 是 F 的一個 extension. 要知道 F 中的一個元素 a 是否 algebraic over F, 依定義就必須驗證是否存在一個不為 0 的 $f(x) \in F[x]$ 使得 $f(a) = 0$. 一般來說用這種方法來驗證一個元素是否是 algebraic over F, 技術上是相當困難的. 這一節中我們將討論幾種和原先 algebraic element 的定義等價的性質, 這樣以後我們要驗證一個元素是否是 algebraic over F 就有多一點的方法來處理.

首先注意當 $a \in L$ 是 algebraic over F 時, 事實上滿足 $f(x) \in F[x]$ 且 $f(a) = 0$ 的多項式有無窮多個. 不過這其中有一個相當特別. 我們首先可以考慮滿足 $f(a) = 0$ 的 $f(x) \in F[x]$ 中 degree 最小的 polynomials. 這樣的 polynomials 有以下兩個重要的性質.

Lemma 10.1.1. 假設 F 是一個 *field,* L 是 F 的一個 *extension.* 若 $a \in L$ 是 *algebraic over* F 且 $f(x) \in F[x]$ 是 $F[x]$ 中滿足 $f(a) = 0$ 的非 0 多項式中 *degree* 最小的一個 *polynomial,* 則 $f(x)$ 有以下兩個性質*:*

(1) 若 $g(x) \in F[x]$ 且 $g(a) = 0$, 則存在 $h(x) \in F[x]$ 滿足 $g(x) = f(x) \cdot h(x)$.

(2) $f(x)$ 是 $F[x]$ 中的 *irreducible element.*

Proof. (1) 由於 F 是一個 field, 利用 Euclid's Algorithm (Theorem 7.2.4) 知存在 $h(x), r(x) \in F[x]$ 使得

$$g(x) = f(x) \cdot h(x) + r(x) \tag{10.1}$$

其中 $r(x) = 0$ 或 $\deg(r(x)) < \deg(f(x))$. 將 a 代入式子 (10.1) 得

$$g(a) = f(a) \cdot h(a) + r(a).$$

由於 $f(a) = g(a) = 0$, 我們得 $r(a) = 0$. 如果 $r(x) \neq 0$, 則得到 $r(x) \in F[x]$ 滿足 $\deg(r(x)) < \deg(f(x))$ 且 $r(a) = 0$. 這和 $f(x)$ 當初的選取相矛盾, 故知 $r(x) = 0$. 也就是說 $g(x) = f(x) \cdot h(x)$.

(2) 假設 $f(x)$ 在 $F[x]$ 中不是 irreducible, 即存在 $h(x), l(x) \in F[x]$ 滿足 $\deg(h(x)) < \deg(f(x))$, $\deg(l(x)) < \deg(f(x))$ 且 $f(x) = h(x) \cdot l(x)$. 將 a 代入上式, 由 $f(a) = 0$ 知 $h(a) \cdot l(a) = 0$. 由於 $h(x), l(x) \in F[x]$ 且 $a \in L$, 我們知 $h(a), l(a) \in L$. 故由 L 是 integral domain (Lemma 9.1.1) 得 $h(a) = 0$ 或 $l(a) = 0$. 這再次和 $f(x)$ 的選取相矛盾, 故知 $f(x)$ 是 $F[x]$ 中的 irreducible element. □

若 $f(x) \in F[x]$ 是 $F[x]$ 中符合 $f(a) = 0$ degree 最小的 polynomial 且 $g(x) \in F[x]$ 滿足 $g(a) = 0$, 則由 Lemma 10.1.1 (1) 知 $g(x) \in \big(f(x)\big)$. 現在如果 $g(x)$ 也是 $F[x]$ 中符合 $g(a) = 0$ degree 最小的 polynomial, 則可得 $\big(f(x)\big) = \big(g(x)\big)$. 由於 $F[x]$ 中的 unit 都是 F 中的非 0 元素 (Proposition 7.2.3) 利用 Lemma 8.1.3 知存在 $c \in F$ 使得 $f(x) = c \cdot g(x)$. 所以如果我們將這些次數最低而滿足 $f(a) = 0$ 的 polynomial 除以它們的最高次項係數所得的 monic polynomial 就唯一了. 因此我們有以下之定義.

Definition 10.1.2. 假設 F 是一個 field, L 是 F 的一個 extension field 且 $a \in L$ 是 algebraic over F. 若 $p(x) \in F[x]$ 是 $F[x]$ 的非 0 polynomial 中滿足 $p(a) = 0$ degree 最小的 monic polynomial, 則稱 $p(x)$ 是 a over F 的 *minimal polynomial.* 又如果 $\deg(p(x)) = n$, 則稱 a 是 algebraic over F of *degree* n.

我們知道當 $[L : F]$ 是有限的時候, L 中的元素都是 algebraic over F. 若 $[L : F] = n$ 且 $a \in L$, 則由於 $1, a, \ldots, a^n$ 一定 linearly independent over F, 故知存在 $f(x) \in F[x]$ 且 $\deg(f(x)) \leq n$ 使得 $f(a) = 0$ (詳見 Theorem 9.3.7 的証明) 故由 minimal polynomial 的定義知: 若 $p(x)$ 是 a 的 minimal polynomial, 則 $\deg(p(x)) \leq \deg(f(x)) \leq n$. 換言之我們得 a 的 degree 小於或等於 $[L : F]$. 我們將這個結果寫成以下之 Lemma.

Lemma 10.1.3. 假設 F 是一個 *field,* L 是 F 的一個 *finite extension,* 則 L 中任意的元素都是 *algebraic over* F 且其 *degree* 小於或等於 $[L : F]$.

當 L 不是 finite extension over F 時, L 中當然有可能存在元素是 algebraic over F. 如果 $a \in L$ 是 algebraic over F, 我們想知道 F 和 L 之間是否可以找到一個 field K 是 F 的一個 finite extension 滿足 $a \in K$?

Definition 10.1.4. 假設 F 是一個 field, L 是 F 的一個 extension field. 若 K 是 L 的一個 extension field 且 $F \subseteq K \subseteq L$, 則稱 K 是 L over F 的一個 *subextension* 或是 *intermediate field.*

Proposition 10.1.5. 假設 F 是一個 *field*, L 是 F 的一個 *extension field*. 若 $a \in L$ 是 *algebraic over* F 且其 *degree* 為 n, 則存在 L *over* F 的一個 *subextension* K 滿足 $a \in K$ 且 $[K : F] = n$.

Proof. 考慮 $\phi : F[x] \to L$ 其中對任意的 $f(x) \in F[x]$, $\phi(f(x)) = f(a)$. 由於 $a \in L$, 所以自然有 $\phi(f(x)) = f(a) \in L$, 因此 ϕ 確實是一個從 $F[x]$ 映射到 L 的函數. 很容易驗證 ϕ 是一個 ring homomorphism.

什麼是 $\ker(\phi)$ 呢? 由於 $F[x]$ 是一個 principle ideal domain 且 $\ker(\phi)$ 是 $F[x]$ 的一個 ideal, 我們知存在 $p(x) \in f[x]$ 使得 $\ker(\phi) = \big(p(x)\big)$. 事實上 我們可以有 $\ker(\phi) = \big(p(x)\big)$ 其中 $p(x)$ 是 a 的 minimal polynomial. 這是因為若 $f(x) \in \ker(\phi)$, 則知 $\phi(f(x)) = f(a) = 0$. 故由 Lemma 10.1.1 知 $f(x) \in \big(p(x)\big)$. 反之, 對任意 $f(x) \in \big(p(x)\big)$, 存在 $h(x) \in F[x]$ 使得 $f(x) = p(x) \cdot h(x)$, 因此由 $p(a) = 0$ 得 $f(a) = p(a) \cdot h(a) = 0$. 故得證 $\ker(\phi) = \big(p(x)\big)$, 其中 $p(x)$ 是 a 的 minimal polynomial.

現由 First Isomorphism Theorem (6.4.2) 知

$$F[x]/\big(p(x)\big) \simeq \mathrm{im}(\phi).$$

然而 $p(x)$ 是 $F[x]$ 的一個 irreducible element (Lemma 10.1.1), 故由 $\big(p(x)\big)$ 是 $F[x]$ 的一個 maximal ideal (Lemma 8.3.2), 得知 $F[x]/\big(p(x)\big)$ 是一個 field (Theorem 6.5.11). 換言之 $\mathrm{im}(\phi)$ 是一個 field.

至於什麼是 $\mathrm{im}(\phi)$ 呢? 由定義知

$$\mathrm{im}(\phi) = \{f(a) \mid f(x) \in F[x]\}.$$

換言之, $\mathrm{im}(\phi)$ 裡的元素都是由某個 $F[x]$ 裡的 polynomial 代入 a 所得. 所以若 $c \in F$, 我們自然有 $\phi(c) = c \in \mathrm{im}(\phi)$, 故得 $F \subseteq \mathrm{im}(\phi) \subseteq L$. 另一方面將 a 代入 x 這一個 polynomial 得到 a: 也就是說 ϕ 將 x 送到 a (即 $\phi(x) = a$), 故知 $a \in \mathrm{im}(\phi)$. 所以若令 $K = \mathrm{im}(\phi)$, 則知 K 是 L over F 的一個 subextension 且 $a \in K$. 最後由假設 a over F 的 degree 是 n, 也就是說 a 的 minimal polynomial $p(x)$ 的 degree 是 n, 因此由 Lemma 9.3.6 知 $\dim_F(F[x]/\big(p(x)\big)) = \deg(p(x)) = n$. 故由 $K \simeq F[x]/\big(p(x)\big)$ 知 $[K : F] = n$. □

若僅由定義來看 Proposition 10.1.5 中的 $\mathrm{im}(\phi) = \{f(a) \mid f(x) \in F[x]\}$ 只是一個 ring, 那為何它會是 field 呢? 若你記得 Theorem 9.3.7 這就一點都不奇怪了. 因為 $\mathrm{im}(\phi) \subseteq L$ 自然是 integral domain, 而由 Proposition 10.1.5 的證明也知 $\dim_F(\mathrm{im}(\phi)) = n$.

我們也很容易檢查 $\{f(a) \mid f(x) \in F[x]\}$ 會是 L 中包含 F 以及 a 最小的 ring, 這是因為若 R 是一個 ring 且包含 F 以及 a, 則對任意的 $f(x) \in F[x]$, 由於 $f(a)$ 僅牽涉到 a 和 F 中的元素間的加法以及乘法, 別忘了這些都是 R 中元素的運算所以當然

得 $f(a) \in R$. 換言之我們得 $\{f(a) \mid f(x) \in F[x]\} \subseteq R$, 再加上 $\{f(a) \mid f(x) \in F[x]\}$ 本身是一個 ring 所以它自然是包含 F 以及 a 最小的 ring 了!

為了方便我們定以下之符號, 在一般的代數書上這個定義是標準的且常被使用的定義.

Definition 10.1.6. 假設 F 是一個 field, L 是 F 的一個 extension field 且 $a \in L$. 我們令 $F[a]$ 表示 L 中包含 F 以及 a 最小的 ring; 我們也令 $F(a)$ 表示 L 中包含 F 以及 a 最小的 field.

前面已知 $F[a]$ 就是 $\mathrm{im}(\phi) = \{f(a) \mid f(x) \in F[x]\}$. 那麼 $F(a)$ 中的元素又是怎樣呢? 利用 quotient field 的性質 (Proposition 7.4.2) 很容易驗證

$$F(a) = \{f(a)/g(a) \mid f(x), g(x) \in F[x] \text{ 且 } g(a) \neq 0\}.$$

由這裡可看出: 一般來說 $F[a]$ 和 $F(a)$ 是不相同的; 不過前面提過若 a 是 algebraic over F, 則 $F[a]$ 會是一個 field, 所以 $F[a]$ 自然是包含 F 以及 a 最小的 field. 換句話說當 a 是 algebraic over F 時, 我們有 $F[a] = F(a)$. 因此 $F(a)$ 就是 Proposition 10.1.5 中所要找的 K, 所以我們將 Proposition 10.1.5 重整以後可以得:

Corollary 10.1.7. 假設 F 是一個 *field,* L 是 F 的一個 *extension field. 若* $a \in L$ 是 *algebraic over* F 且 $p(x) \in F[x]$ 為 a *over* F 的 *minimal polynomial,* 則

$$F(a) \simeq F[x]/\big(p(x)\big) \quad \text{and} \quad [F(a) : F] = \deg(p(x)).$$

Remark 10.1.8. 同學或許會奇怪 $F[a]$ 裡的元素長的是 $f(a)$ 其中 $f(x) \in F[x]$ 這種樣子, 而 $F(a)$ 裡的元素長的是 $f(a)/g(a)$ 其中 $f(x), g(x) \in F[x]$ 這種樣子: 兩個樣子差這麼多, 怎麼可能會 $F[a] = F(a)$ 呢? 這是因為當 a 是 algebraic over F 時, $F[a]$ (或 $F(a)$) 裡的元素其表示法是不唯一的. 例如若 $p(x) \in F[x]$ 是 a 的 minimal polynomial, 如果令 $g(x) = f(x) + p(x)$, 則 $g(a) = f(a)$. 所以當然有可能用不同的形式寫下來的元素它們的值是相同的.

接下來我們就來看和 a 是 algebraic over F 等價的條件是什麼?

Theorem 10.1.9. 假設 F 是一個 *field,* L 是 F 的一個 *extension field* 且 $a \in L$, 則下面有關於 a 的敘述是等價的.

(1) a 是 *algebraic over* F.

(2) 存在 K 是 L *over* F 的 *subextension* 滿足 $a \in K$ 且 $[K : F]$ 是有限的.

(3) $F[a] = F(a)$.

Proof. 由前面 Proposition 10.1.5 可知 (1) $\Rightarrow$ (2), 所以我們僅要驗證 (2) $\Rightarrow$ (3) 以及 (3) $\Rightarrow$ (1).

(2) ⇒ (3): 若 K 是 L over F 的 subextension (即 $F \subseteq K \subseteq L$), 則由假設 $a \in K$ 知 $F[a] \subseteq K$. 再由假設 K 是 F 的一個 finite extension, 套用 Proposition 9.4.3 可得 $F[a]$ 是一個 field. 故知 $F[a] = F(a)$.

(3) ⇒ (1): 假設 $F[a] = F(a)$, 也就是說 $F[a]$ 是一個 field. 如果 $a = 0 \in F$, 那當然 a 是 algebraic over F (注意 F 中的元素當然是 algebraic over F). 如果 $a \neq 0$, 則由 $a \in F[a]$ 且 $F[a]$ 是一個 field 知 $a^{-1} \in F[a]$. 別忘了 $F[a]$ 裡的元素都是 $f(a)$, 其中 $f(x) \in F[x]$ 這種形式, 所以我們有 $a^{-1} = f(a)$, 其中

$$f(x) = c_n x^n + \cdots + c_1 x + c_0, \quad c_i \in F.$$

故由

$$a^{-1} = c_n \cdot a^n + \cdots + c_1 \cdot a + c_0$$

得

$$1 = c_n \cdot a^{n+1} + \cdots + c_1 \cdot a^2 + c_0 \cdot a.$$

因此若令

$$g(x) = c_n x^{n+1} + \cdots + c_1 x^2 + c_0 x - 1,$$

則 $g(a) = 0$. 由於 $g(x) \in F[x]$ 且 $g(x) \neq 0$, 故知 a 是 algebraic over F. □

Theorem 10.1.9 給了我們一個很好的方法來驗證 a 是否是 algebraic over F. 也就是說今後要檢查 a 是 algebraic over F 我們可以不必真的去找一個 $f(x) \in F[x]$ 使得 $f(a) = 0$. 當然了要用什們方法會因問題而有所差別. 比方說若 $a^2 \in L$ 且我們知 a^2 是 algebraic over F, 如果 $f(x) \in F[x]$ 滿足 $f(a^2) = 0$, 則令 $g(x) = f(x^2)$, 我們可得 $g(a) = f(a^2) = 0$. 因此知 a 也是 algebraic over F. 也就是當 a^2 是 algebraic over F 時, a 也會是 algebraic over F. 但是反過來, 如果已知 a 是 algebraic over F, 我們就無法利用滿足 a 的 polynomial 來製造一個滿足 a^2 的 polynomial 了. 同學或許會想若 $f(a) = 0$, 我們可以令 $g(x) = f(x^{1/2})$, 則 $g(a^2) = f(a) = 0$ 呀! 這是不對的, 因為 $f(x)$ 若有奇數次項, 則 $g(x) = f(x^{1/2})$ 就不再是一個 polynomial 了. 所以在這種狀況下就不可能利用找 polynomial 的方法來證明 a^2 是 algebraic over F. 其實當 a 是 algebraic over F 時利用 Theorem 10.1.9 知存在一個 field K 是 F 的 finite extension 且 $a \in K$. 然而 K 是一個 field 且 $a \in K$, 所以當然 $a^2 \in K$, 所以再用一次 Theorem 10.1.9 (或是利用 Lemma 10.1.3) 我們得證 a^2 也是 algebraic over F. 以後我們常會用類似的方法來處理相關的問題.

10.2. Algebraic Closure

當 F 是一個 field, L 是 F 的一個 extension 時, 我們可以將 L 中的元素分成 algebraic over F 和不是 algebraic over F 的兩種. 在這一節中我們將探討 L 中所有 algebraic over F 的元素所成之集合.

Definition 10.2.1. 假設 F 是一個 field 且 L 是 F 的一個 extension. 我們令

$$\overline{L_F} = \{a \in L \mid a \text{ 是 algebraic over } F\},$$

稱之為 F 在 L 的 *algebraic closure*.

F 中的元素當然是 algebraic over F, 所以由定義知 $F \subseteq \overline{L_F} \subseteq L$. 另外如果 L 是 F 的一個 finite extension, 則由 Lemma 9.4.5 知 L 中的元素都 algebraic over F, 所以在這個假設之下 $\overline{L_F} = L$.

接下來我們要證明 $\overline{L_F}$ 的一個重要性質, 即 $\overline{L_F}$ 是一個 field. 換言之, 我們要證明若 $a, b \in \overline{L_F}$, 其中 $b \neq 0$, 則 $a - b$ 以及 $a \cdot b^{-1}$ 皆在 $\overline{L_F}$ 中 (Lemma 9.1.4). 要如何證明這些元素都是 algebraic over F 呢? 當然不可能用找 polynomial 的方法, 我們必須藉助 Theorem 10.1.9. 在這之前我們先推廣一下 Definition 10.1.6.

Definition 10.2.2. 假設 F 是一個 field 且 L 是 F 的一個 extension. 若 $a_1, \ldots, a_n \in L$, 則定 $F(a_1, \ldots, a_n)$ 表示為 L 中包含 F 以及 $a_1, \ldots, a_n$ 最小的 field.

Lemma 10.2.3. 假設 F 是一個 *field* 且 L 是 F 的一個 *extension.* 若 $a_1, \ldots, a_n \in L$ 皆為 *algebraic over* F, 則 $F(a_1, \ldots, a_n)$ 是 F 的一個 *finite extension.* 事實上, 如果已知 $a_1, \ldots, a_n$ *over* F 的 *degree* 分別為 $m_1, \ldots, m_n$, 則

$$[F(a_1, \ldots, a_n) : F] \leq m_1 \cdots m_n.$$

Proof. 為了方便, 我們令

$$K_1 = F(a_1), K_2 = K_1(a_2) = F(a_1, a_2), \ldots, K_n = K_{n-1}(a_n) = F(a_1, \ldots, a_n).$$

對任意的 i, 我們有 $[K_i : K_{i-1}] = [K_{i-1}(a_i) : K_i] \leq m_i$. 這裡 $[K_{i-1}(a_i) : K_{i-1}]$ 會小於或等於 m_i 的原因是: 由 Corollary 10.1.7 知 $[K_{i-1}(a_i) : K_{i-1}]$ 的值剛好是 a_i over K_{i-1} 的 minimal polynomial $q_i(x) \in K_{i-1}[x]$ 的 degree. 然而由假設 a_i over F 的 minimal polynomial $p_i(x) \in F[x]$ 的 degree 為 m_i. 由於 $p_i(x) \in F[x] \subseteq K_{i-1}[x]$ 且 $p_i(a_i) = 0$, 故由 $q_i(x)$ 是 a_i over K_{i-1} 的 minimal polynomial 的假設知 $\deg(q_i(x)) \leq \deg(p_i(x)) = m_i$. 故知

$$[K_i : K_{i-1}] = [K_{i-1}(a_i) : K_{i-1}] = \deg(q_i(x)) \leq m_i.$$

現在由於每一段 $[K_i : K_{i-1}]$ 都是有限的, 所以我們可以連續套用 Theorem 9.4.6 得:

$$\begin{aligned} [F(a_1, \ldots, a_n) : F] &= [K_n : K_{n-1}][K_{n-1} : F] \\ &= [K_n : K_{n-1}][K_{n-1} : K_{n-2}][K_{n-2} : F] \\ &\vdots \\ &= [K_n : K_{n-1}] \cdots [K_1 : F] \leq m_n \cdots m_1. \end{aligned}$$

故得證 $F(a_1, \ldots, a_n)$ 是 F 的一個 finite extension. □

利用 Lemma 10.2.3 我們馬上可得知 $\overline{L_F}$ 是一個 field.

Theorem 10.2.4. 假設 F 是一個 *field* 且 L 是 F 的一個 *extension.* 若 $a, b \in L$, 其中 $b \neq 0$, 皆為 *algebraic over* F, 則 $a+b$, $a-b$, $a \cdot b$ 以及 $a \cdot b^{-1}$ 皆為 *algebraic over* F. 由此我們可得 $\overline{L_F}$ 是一個 *field.*

Proof. 由 Lemma 10.2.3 我們知 $F(a,b)$ 是 F 的一個 finite extension. 由於 $a, b \in F(a,b)$, $b \neq 0$ 且 $F(a,b)$ 是一個 field, 我們自然有 $a+b$, $a-b$, $a \cdot b$ 以及 $a \cdot b^{-1}$ 皆為 $F(a,b)$ 的元素. 故由 Theorem 10.1.9 (或 Lemma 10.1.3) 知這四個元素皆為 algebraic over F.

今若 $a, b \in \overline{L_F}$, 其中 $b \neq 0$, 則由定義知 a, b 皆為 algebraic over F. 故由前知 $a+b$, $a-b$, $a \cdot b$ 以及 $a \cdot b^{-1}$ 皆為 algebraic over F. 故知這四個元素皆在 $\overline{L_F}$ 中, 因此得證 $\overline{L_F}$ 是一個 field. □

假設 L 是 F 的一個 extension, 且 K 是 L over F 的 subextension (即 $F \subseteq K \subseteq L$). L 中是 algebraic over K 的元素未必是 algebraic over F. 不過 L 中是 algebraic over F 的元素就一定是 algebraic over K. 這是因為若 $a \in \overline{L_F}$ (即 $a \in L$ 是 algebraic over F), 表示在 $F[x]$ 中存在 $f(x) \neq 0$ 使得 $f(a) = 0$. 由於 $f(x) \in F[x] \subseteq K[x]$, 我們自然得 a 也是 algebraic over K. 故得 $a \in \overline{L_K}$, 換句話說我們總是有

$$\overline{L_F} \subseteq \overline{L_K}.$$

我們有興趣知道什麼時候 $\overline{L_F}$ 會等於 $\overline{L_K}$. 以下是一個例子.

Lemma 10.2.5. 假設 F 是一個 *field,* L 是 F 的一個 *extension,* 且 K 是 L *over* F 的 *subextension.* 若 K 是 F 的一個 *finite extension,* 則 $\overline{L_F} = \overline{L_K}$

Proof. 我們已知 $\overline{L_F} \subseteq \overline{L_K}$, 所以只要證明 $\overline{L_K} \subseteq \overline{L_F}$. 也就是要證明: 若 $a \in L$ 是 algebraic over K, 則 a 是 algebraic over F. 我們考慮 $K(a)$ 這一個 field. 由假設 a 是 algebraic over K, 故利用 Corollary 10.1.7 知 $K(a)$ 是 K 的一個 finite extension. 再加上 K 是 F 的一個 finite extension, 套用 Theorem 9.4.6 可得

$$[K(a) : F] = [K(a) : K][K : F],$$

因此 $K(a)$ 是 F 的一個 finite extension. 故利用 $a \in K(a)$ 以及 Theorem 10.1.9 (或 Lemma 10.1.3) 知 a 是 algebraic over F. □

我們可以將 Lemma 10.2.5 推廣到更一般的狀況. 回顧一下若 K 是 F 的一個 algebraic extension 表示 K 中的元素皆為 algebraic over F. 在 Lemma 10.2.5 中的假設 K 是 F 的 finite extension, 所以自然是 F 的一個 algebraic extension. 我們要將 Lemma 10.2.5 推廣到 K 是 F 的 algebraic extension 這個狀況.

Theorem 10.2.6. 假設 F 是一個 *field,* L 是 F 的一個 *extension,* 且 K 是 L *over* F 的 *subextension.* 若 K 是 F 的一個 *algebraic extension,* 則 $\overline{L_F} = \overline{L_K}$

Proof. 和 Lemma 10.2.5 相同的情形, 我們只要證明: 若 $a \in L$ 是 algebraic over K, 則 a 是 algebraic over F. 不過這裡碰到的狀況是 K 可能不是 finite extension over F, 所以我們不能直接套用 Lemma 10.2.5. 要克服這個困難, 我們必須想辦法找到一個 F 的 finite extension K' 且滿足 a 是 algebraic over K'. 如此再套用 Lemma 10.2.5 得證 a 是 algebraic over F.

由假設 a 是 algebraic over K, 知存在 $f(x) \neq 0$ 且 $f(x) \in K[x]$ 使得 $f(a) = 0$. 假設 $f(x) = a_n x^n + \cdots + a_0$. 由於 $a_n, \ldots, a_0 \in K$ 且 K 是 F 的一個 algebraic extension, 故知 $a_n, \ldots, a_0$ 皆為 algebraic over F. 令 $K' = F(a_n, \ldots, a_0)$, 由 Lemma 10.2.3 知 K' 是 F 的一個 finite extension. 故利用 Lemma 10.2.5 知 $\overline{L_{K'}} = \overline{L_F}$. 另外由於 $a_n, \ldots, a_0 \in F(a_n, \ldots, a_0) = K'$, 我們知 $f(x) \in K'[x]$. 故由 $f(a) = 0$ 知 a 是 algebraic over K'. 換言之, 我們有 $a \in \overline{L_{K'}}$, 故由 $\overline{L_{K'}} = \overline{L_F}$ 得知 $a \in \overline{L_F}$. 因此得證 a 是 algebraic over F. □

我們已知 $\overline{L_F}$ 是一個 filed (Theorem 10.2.4) 且 $F \subseteq \overline{L_F} \subseteq L$. 如果我們再收集 L 中是 algebraic over $\overline{L_F}$ 的元素會不會得到更大的 field 的呢? 換句話來說, 我們想知道 $\overline{L_{\overline{L_F}}}$ (不要被這符號嚇著了) 是什麼? 事實上所謂的 algebraic closure 就是說 L 中 algebraic over $\overline{L_F}$ 的元素所成的集合就是 $\overline{L_F}$ 自己.

Corollary 10.2.7. 假設 F 是一個 *field* 且 L 是 F 的一個 *extension,* 若 $a \in L$ 且 a 是 *algebraic over* $\overline{L_F}$, 則 a 是 *algebraic over* F. 也就是說, 我們有

$$\overline{L_{\overline{L_F}}} = \overline{L_F}.$$

Proof. 首先注意由定義 $\overline{L_F}$ 中的元素都是 algebraic over F, 故知 $\overline{L_F}$ 是 F 的一個 algebraic extension. 因此若令 $K = \overline{L_F}$, 則 K 符合 Theorem 10.2.6 的條件, 故知 $\overline{L_K} = \overline{L_F}$. 也因此若 $a \in L$ 是 algebraic over $\overline{L_F} = K$, 表示 $a \in \overline{L_K}$. 故由 $\overline{L_K} = \overline{L_F}$ 得知 $a \in \overline{L_F}$, 也就是說 a 是 algebraic over F. □

10.3. Roots of Polynomials

這一節中我們將討論一個 polynomial 在一個 field 中它的根的性質.

首先我們還是來看大家最熟悉的餘式定理.

Lemma 10.3.1. 假設 F 是一個 *field.* 若 $f(x) \in F[x]$, 其中 $\deg(f(x)) = n$, 且 $a \in F$ 滿足 $f(a) = 0$, 則存在 $h(x) \in F[x]$, 其中 $\deg(h(x)) = n - 1$, 使得 $f(x) = (x - a) \cdot h(x)$.

Proof. 由於 F 是一個 field, 考慮 $f(x) \in F[x]$ 以及 $(x - a) \in F[x]$, 利用 Euclid's Algorithm (Theorem 7.2.4) 知存在 $h(x), r(x) \in F[x]$ 滿足 $f(x) = (x-a) \cdot h(x) + r(x)$, 其中 $r(x) = 0$ 或 $\deg(r(x)) < \deg(x - a) = 1$. 如果 $r(x) \neq 0$ 由 $\deg(r(x)) < 1$ 知 $r(x) = c \in F$ 是一個常數. 但由於 $f(a) = 0$ 故將 a 代入 $f(x) = (x - a) \cdot h(x) + c$

得 $c = 0$, 此和 $r(x) \neq 0$ 相矛盾故知 $r(x) = 0$. 也就是 $f(x) = (x - a) \cdot h(x)$. 至於 $\deg(h(x)) = n - 1$, 可由 Lemma 7.2.2 直接得知. □

由於 $\deg(x - a) = 1$, 我們知道 $x - a$ 是 $F[x]$ 中的 irreducible element. 因此 Lemma 10.3.1 告訴我們若 $f(a) = 0$, 則 $x - a$ 會是 $f(x)$ 的一個 irreducible divisor. 利用 $F[x]$ 是 unique factorization domain (Theorem 7.2.14), 我們知存在 $k \in \mathbb{N}$ 以及 $q(x) \in F[x]$ 使得 $f(x) = (x - a)^k \cdot q(x)$, 其中 $q(a) \neq 0$ (即 $x - a$ 不是 $q(x)$ 的 divisor). 我們依此來定義 a 在 $f(x)$ 的重根數.

Definition 10.3.2. 假設 F 是一個 field. 若 $f(x) \in F[x]$ 且 $a \in F$ 滿足 $f(a) = 0$, 則稱 a 是一個 *root* of $f(x)$. 又如果 $f(x) = (x - a)^k \cdot q(x)$, 其中 $q(a) \neq 0$, 則稱 a 是一個 *root* of *multiplicity* k of $f(x)$.

接下來也是大家熟悉的定理: 一個 n 次多項式在一個 field 中計算重根在內至多有 n 個根. 這裡指的計算重根在內是說如果 a 是 k 重根, 則要算成是 k 個根.

Theorem 10.3.3. 假設 F 是一個 *field.* 若 $f(x) \in F[x]$ 且 $\deg(f(x)) = n \geq 1$, 則在 F 中將 *multiplicity* 計算在內, $f(x)$ 至多有 n 個 *roots.*

Proof. 我們利用 induction. 如果 $\deg(f(x)) = 1$, 則 $f(x)$ 當然僅有 1 個根. 假設 degree 小於 n 的 polynomial 定理皆成立. 現考慮 $f(x) \in F[x]$ 且 $\deg(f(x)) = n$ 的情形. 如果 $f(x)$ 在 F 中沒有 root, 則定理當然成立. 如果 $a \in F$ 是 $f(x)$ 的一個 root of multiplicity k, 即表示存在 $q(x) \in F[x]$ 使得 $f(x) = (x - a)^k \cdot q(x)$, 其中 $q(a) \neq 0$. 利用 degree 的性質 (Lemma 7.2.2) 我們有 $\deg(q(x)) = n - k < n$, 故利用 induction 的假設知在 F 中將 multiplicity 計算在內, $q(x)$ 至多有 $n - k$ 個 roots. 然而若 $b \in F$ 是 $f(x)$ 的一個 root, 我們有

$$0 = f(b) = (b - a)^k \cdot q(b).$$

利用 F 是 integral domain, 我們知 $f(x)$ 的 roots 要不是 a 就是 $q(x)$ 的 roots. 因此在 F 中 $f(x)$ roots 的個數就是 k 加上 $q(x)$ 的 roots 的個數, 所以至多有 $k + (n - k) = n$ 個. □

我們要看一個元素 a 是否是 $f(x)$ 的一個根, 大家直覺的想法就是將 a 代入 $f(x)$ 看是否為 0. 事實上這是不對的, 要將 a 代入 $f(x)$ 牽扯上 a 和 $f(x)$ 的係數間的加法和乘法. 換言之如果 a 座落在一個包含 F 和 a 的 field L (至少要是 ring) 中, 這樣我們才可以將 a 和 $f(x)$ 的係數考慮成是 L 的元素而加以運算. 這樣 $f(a)$ (看成是 L 的元素) 才有意義. 這就是為甚麼我們前面的討論都會先給 F 的一個 extension L, 然後再談論 $a \in L$ 與 $F[x]$ 中的 polynomials 的關係. 所以我們自然會問: 給定任一非常數的 $f(x) \in F[x]$ 是否可以找到 F 的一個 extension L 使得 $f(x)$ 在 L 中有根? 答案是肯定的. 以下的定理就是回答這個問題. 我們將會建構一個 F 的 extension field 然後說明在其中可找到一個根. 這個定理的證明同學或許會覺得"虛

虛"的, 因為好像沒有真的在找根的感覺. 不過這就是數學在談存在性所關心的重點, 我們只要知道東西存在而不必真正告訴你東西是什麼.

Theorem 10.3.4. 假設 F 是一個 *field* 且 $p(x) \in F[x]$ 是 $F[x]$ 中的 *irreducible element,* 則存在一個 *field* L 是 F 的 *finite extension,* 其中 $[L:F] = \deg(p(x))$ 且 L 中存在 $a \in L$ 滿足 $p(a) = 0$.

Proof. 令 $L = F[x]/\big(p(x)\big)$. 由於 $p(x)$ 是 irreducible, 我們知 $\big(p(x)\big)$ 是 $F[x]$ 中的 maximal ideal, 故知 L 是一個 field.

首先我們要驗證 L 中存在一個 subfield 和 F 是 isomorphic 的, 因此我們可以將 L 看成是 F 的一個 extension. 事實上考慮 $\pi : F \to F[x]/\big(p(x)\big)$, 定義成 $\pi(c) = \overline{c}$, 很容易驗證 π 是一個 ring homomorphism. 也很容易驗證 π 是一對一的: 這是因為如果 $c \in \ker(\pi)$, 表示 $\overline{c} = \overline{0}$, 即 $c \in \big(p(x)\big)$. 但是 $\big(p(x)\big)$ 中除了 0 以外沒有其他的常數, 故得 $c = 0$ (也可套用 Proposition 9.1.5 (2) 得到 π 是一對一). 因此得證 $\mathrm{im}(\pi)$ 是 L 的 subfield 且和 F 是 isomorphic 的.

現在要證明 L 中存在一元素是 $p(x)$ 的根. 考慮 $a = \overline{x} \in L$, 我們要說明 $p(\overline{x}) = \overline{0}$ (注意 $\overline{0}$ 是 $L = F[x]/\big(p(x)\big)$ 的 0). 假設 $p(x) = a_n x^n + \cdots + a_1 x + a_0$, 其中 $a_i \in F$. 那麼 $p(a)$ 會是什麼呢? 別忘了我們提過這裡代入 a 必須用到的是 L 中的運算, 而在 L 中 $c \in F$ 是需經過 π 送到 L 的, 換句話說我們必須考慮的是 $\overline{c}$. 因此有

$$\begin{aligned} p(a) &= p(\overline{x}) \\ &= a_n \cdot \overline{x}^n + \cdots + a_1 \cdot \overline{x} + a_0 \\ &= \overline{a_n} \cdot \overline{x}^n + \cdots + \overline{a_1} \cdot \overline{x} + \overline{a_0} \quad (\text{依 } L \text{ 的運算定義}) \\ &= \overline{a_n x^n + \cdots + a_1 x + a_0} \\ &= \overline{p(x)} = \overline{0} \end{aligned}$$

所以 L 中真的存在一個元素代入 $p(x)$ 等於 L 中的 0.

最後由 Lemma 9.3.6 知 $[L:F] = \dim_F(L) = \dim_F(F[x]/\big(p(x)\big)) = \deg(p(x))$. □

由 Theorem 10.3.4 我們很容易得到以下一般的狀況.

Corollary 10.3.5. 假設 F 是一個 *field* 且 $f(x) \in F[x]$, 其中 $\deg(f(x)) = n \geq 1$, 則存在一個 *field* L 是 F 的 *finite extension,* 其中 $[L:F] \leq n$ 且 L 中存在 $a \in L$ 滿足 $f(a) = 0$.

Proof. 由於 $f(x) \in F[x]$ 而且 $\deg(f(x)) \geq 1$, 所以 $f(x)$ 不是 $F[x]$ 中的 unit. 利用 $F[x]$ 是 unique factorization domain, 我們知存在 $p(x) \in F[x]$ 是 $F[x]$ 中的 irreducible element 滿足 $p(x) \mid f(x)$. 注意如果 $p(a) = 0$, 則當然得 $f(a) = 0$. 因此由 Theorem 10.3.4 知存在 L, 其中 $[L:F] = \deg(p(x)) \leq \deg(f(x))$ 且 $a \in L$, 滿足 $f(a) = p(a) = 0$. □

我們可以一直套用 Corollary 10.3.5 找到一個 F 的 finite extension L' 使得 $f(x)$ 在 L' 中可以完全分解. 這裡所謂的 $f(x)$ 在 L' 完全分解就是說: 如果 $\deg(f(x)) = n$, 則 $f(x)$ 在 $L'[x]$ 中可以寫成 $f(x) = c \cdot (x - a_1) \cdots (x - a_n)$, 其中 $a_i \in L'$. 此時我們通常稱 $f(x)$ *splits into linear factors* in L'.

Theorem 10.3.6. 假設 F 是一個 *field* 且 $f(x) \in F[x]$, 其中 $\deg(f(x)) = n \geq 1$, 則存在一個 *field* L' 是 F 的 *finite extension,* 其中 $[L' : F] \leq n!$, 使得 $f(x)$ *splits into linear factors in* L'.

Proof. 利用 Corollary 10.3.5 知存在 L_1 是 F 的一個 extension 滿足 $[L_1 : F] \leq n$ 且 $a_1 \in L_1$ 使得 $f(a_1) = 0$. 故由 Lemma 10.3.1 知存在 $f_1(x) \in L_1[x]$ 且 $\deg(f_1(x)) = n - 1$ 使得 $f(x) = (x - a_1) \cdot f_1(x)$. 對 $f_1(x)$ 再套用一次 Corollary 10.3.5 知存在 L_2 是 L_1 的一個 extension 滿足 $[L_2 : L_1] \leq n - 1$ 且 $a_2 \in L_2$ 使得 $f_1(a_2) = 0$. 注意此時

$$[L_2 : F] = [L_2 : L_1][L_1 : F] \leq n(n - 1),$$

且存在 $f_2(x) \in L_2[x]$ 使得

$$f(x) = (x - a_1) \cdot (x - a_2) \cdot f_2(x).$$

所以這樣一直作下去 (或是對 degree 作 induction) 我們得證本定理. □

最後我們強調一下 Theorem 10.3.6 裡的 L' 當然會因 $f(x)$ 不同而不同, 不過事實上我們可以找到一個 F 的 extension $\tilde{F}$ 使得 $F[x]$ 中的所有 polynomial 在 $\tilde{F}$ 中都可以 splits into linear factors (當然此時 $\tilde{F}$ 有可能不是 F 的 finite extension). 不過由於這個定理的證明需用到所謂的 *Zorn's Lemma*, 我們就略去不證了.

10.4. Finite Fields

在這個講義的最後一節, 我們要簡單的介紹 finite field 的一些簡單的性質.

回顧一下所謂 F 是一個 finite field 就是說 F 是一個 field 且 F 的元素個數 (通常我們用 $|F|$ 來表示) 是有限多個. 由這個定義我們馬上知若 F 是 finite field, 則 F 的 characteristic 一定是一個質數 p (Lemma 9.2.3). 當初我們定 characteristic 是利用一個 ring homomorphism $\phi : \mathbb{Z} \to F$, 其中對任意 $n \in \mathbb{N}$ 我們定 $\phi(n) = n1$, 而 $\phi(-n) = n(-1)$. F 的 characteristic 是 p 表示 $\ker(\phi) = \big(p\big)$. 因此由 ring 的 1st Isomorphism Theorem 我們知 $\mathbb{Z}/\big(p\big) \simeq \mathrm{im}(\phi) \subseteq F$. 別忘了 p 是質數, 故知 $\big(p\big)$ 會是 $\mathbb{Z}$ 的一個 maximal ideal, 因此 $\mathbb{Z}/\big(p\big)$ 是一個 field. 又因 $\big|\mathbb{Z}/\big(p\big)\big| = p$, 我們得 F 中存在一個 subfield 和 $\mathbb{Z}/\big(p\big)$ 這個 p 個元素的 finite field 是 isomorphic 的. 為了方便我們將這個 p 個元素的 finite field 記為: $\mathbb{F}_p$.

既然 F 是 $\mathbb{F}_p$ 的一個 extension, 我們當然就可以把 F 看成是一個 vector space over $\mathbb{F}_p$. 那麼 F 會不會是 finite dimensional over $\mathbb{F}_p$ 呢? 大家可能都會猜想會, 但是怎麼證呢? 一般來說我們要證明一個 vector space V 是 finite dimensional over 一

個 field K, 我們只要證明 V 中可以找到有限多個元素 span V over K. 現在由於 F 是 finite field, 就假設 $|F| = n$ 吧, 那麼 F 中所有的元素當然 span F over $\mathbb{F}_p$ 了 (因為每個 $a \in F$ 都可以看成是 $a = 1 \cdot a$). 所以由 Lemma 9.3.4 (1) 知 $\dim_{\mathbb{F}_p}(F) \leq n$. 當然我們這個估計的 dimension 是非常粗略, 不過我們目前的目的只是要知道 F 是 $\mathbb{F}_p$ 的一個 finite extension. 綜合以上的結果我們可以得到以下 finite field 第一個重要的性質.

Theorem 10.4.1. 假設 F 是一個 *finite field* 且 $\mathrm{char}(F) = p$, 則 F 中存在一個 *subfield* $\mathbb{F}_p$, 其中 $|\mathbb{F}_p| = p$ 且和 $\mathbb{Z}/(p)$ *isomorphic,* 而且 F 是 $\mathbb{F}_p$ 的一個 *finite extension.* 若 $[F : \mathbb{F}_p] = k$, 則 $|F| = p^k$.

Proof. 我們前面已知 F 中存在一個 subfield $\mathbb{F}_p$ 滿足 $\mathbb{F}_p \simeq \mathbb{Z}/(p)$, 而且 F 是 $\mathbb{F}_p$ 的 finite extension. 所以我們僅剩下要證: 若 $[F : \mathbb{F}_p] = k$, 則 $|F| = p^k$.

這完全是一個線性代數的問題. 由 $\dim_{\mathbb{F}_p}(F) = [F : \mathbb{F}_p] = k$ 的假設知存在 $a_1, \ldots, a_k \in F$ 是一組 F over $\mathbb{F}_p$ 的 basis. 由 basis 的定義知對任意的 $\alpha \in F$, 存在一組唯一的 $c_1, \ldots, c_k \in \mathbb{F}_p$ 使得 $\alpha = c_1 \cdot a_1 + \cdots + c_k \cdot a_k$. (這裡的存在是因為 $a_1, \ldots, a_k$ span F over $\mathbb{F}_p$, 而唯一是因為 $a_1, \ldots, a_k$ 是 linearly independent over $\mathbb{F}_p$.) 注意這裡的 $a_1, \ldots, a_k$ 是固定的一組 basis, 而 $c_1, \ldots, c_k \in \mathbb{F}_p$ 會隨著 $\alpha \in F$ 的改變而改變. 換言之 F 中的任一個元素都由唯一的一組 $c_1, \cdots, c_k$ 所決定. 但由於這些 c_i 皆在 $\mathbb{F}_p$ 中而 $|\mathbb{F}_p| = p$, 因此對每個 $i \in \{1, \ldots, k\}$, c_i 都有 p 個選擇, 故知這些 $c_1, \ldots, c_k$ 共有 p^k 個選擇. 也就是說 F 中共有 p^k 個元素. □

Theorem 10.4.1 簡單來說就是告訴我們每一個 finite field 其元素的個數應該是 p^k 個這種形式. 所以不可能有 finite field 有 6 個元素; 不過 Theorem 10.4.1 也沒有告訴我們到底有沒有 finite field 有 9 個元素或 16 個元素等等. 馬上我們就要回答這個問題, 不過在此之前我們先談談 finite field 的乘法結構.

假設 F 是一個 finite field, 因為 F 是 field, 由 Corollary 9.1.2 知 $F^* = F \setminus \{0\}$ 在乘法之下是一個 abelian group. 又因為 F 只有有限個元素, 所以我們知道 F^* 是一個 finite abelian group. 既然 F^* 是一個 finite group, 利用 Lagrange's Theorem 我們有以下之結果.

Proposition 10.4.2. 假設 F 是一個 *finite field* 且 $|F| = p^k$. 令 $f(x) = x^{p^k} - x$, 則對任意 $a \in F$ 皆符合 $f(a) = 0$ 且 $f(x)$ *splits linear factors in* F. 事實上我們有

$$x^{p^k} - x = \prod_{a \in F} (x - a).$$

Proof. 首先我們考慮 F^* 這個 order 為 $p^k - 1$ 的 finite group. 利用 Lagrange's Theorem (Corollary 2.3.4), 我們知對任意 $a \in F^*$, 皆有 $a^{p^k - 1} = 1$ (注意 1 是 F^* 的 identity). 等式兩邊乘上 a 得 $a^{p^k} = a$, 故知 $f(a) = 0$. 另外當 $a = 0$ 時自然有 $f(a) = 0$, 所以我們得到對任意的 $a \in F$ 皆符合 $f(a) = 0$. 然而由 Theorem 10.3.3

我們知道 $f(x)$ 在 F 中最多只能有 $\deg(f(x)) = p^k$ 個根. 所以 F 中的元素剛好就是 $f(x)$ 所有的根. 因此 $f(x)$ 可以完全分解成

$$f(x) = \prod_{a \in F} (x - a),$$

也就是說 $f(x)$ splits linear factors in F. □

要注意 Lagrange's Theorem 是對一般的 finite group 都對的, 所以 Proposition 10.4.2 並沒有用到 F^* 是 abelian 的性質. 接下來我們要用到 finite abelian group 的重要性質來證明事實上 F^* 是一個 cyclic group. 回顧一下 finite abelian group 的 fundamental theorem (Theorem 3.3.11) 是說任意的 finite abelian group 都可寫成一些 cyclic groups 的 direct product. 另外要注意的是若 C_n 表示是一個 cyclic group of order n, 則 $C_n \times C_m$ 不見得會 isomorphic to C_{nm}, 除非 n 和 m 是互質的 (Proposition 3.2.2).

Theorem 10.4.3. 假設 F 是一個 *finite field,* 則 $F^* = F \setminus \{0\}$ 看成是一個乘法的 *group* 時是一個 *cyclic group.*

Proof. 由 Theorem 3.3.11 知存在 $n_1, \ldots, n_r \in \mathbb{N}$ 使得

$$F^* \simeq C_{n_1} \times \cdots \times C_{n_r},$$

其中 C_{n_i} 是一個 cyclic group of order n_i. 若我們能證明這些 n_i 都是兩兩互質的, 則重複運用 Proposition 3.2.2 可得

$$C_{n_1} \times \cdots \times C_{n_r} \simeq C_{n_1 \cdots n_r},$$

換言之 F^* 是 cyclic group.

我們利用反證法, 為了方便就假設 n_1 和 n_2 不互質好了 (其他的狀況都是用相同的證明). 這表示存在一質數 q 是 n_1 和 n_2 的公因數. 因為 $q \mid n_1$ 且 q 是質數, Cauchy's 定理 (Theorem 3.3.2 或 Theorem 4.2.1) 告訴我們存在 $a \in C_{n_1}$ 滿足 $\mathrm{ord}(a) = q$. 也就是說 $a, a^2, \ldots, a^{q-1}, a^q = e_1$ 是 C_{n_1} 中 q 個相異的元素 (這裡我們用 e_i 來表示 C_{n_i} 的 identity). 同理我們知在 C_{n_2} 中存在 $b \in C_{n_2}$ 滿足 $\mathrm{ord}(b) = q$. 現考慮

$$\alpha = (a, e_2, \ldots, e_r), \beta = (e_1, b, \ldots, e_r) \in C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}.$$

當 $i, j \in \{1, \ldots, q\}$ 且 $i \neq j$ 時, 我們知

$$\alpha^i = (a^i, e_2, \ldots, e_r) \quad \text{and} \quad \alpha^j = (a^j, e_2, \ldots, e_r),$$

故由於 $a^i \neq a^j$, 我們知 $\alpha^i \neq \alpha^j$. 同理 $\beta^i \neq \beta^j$. 另外對任意的 $i, j \in \{1, \ldots, q-1\}$, 由於 $a^i \neq e_1$ 且 $b^j \neq e_2$, 我們也知

$$\alpha^i = (a^i, e_2, \ldots, e_r) \neq (e_1, b^j, \ldots, e_r) = \beta^j.$$

換句話說

$$\alpha, \alpha^2, \ldots, \alpha^{q-1}, \beta, \beta^2, \ldots, \beta^{q-1}$$

以及

$$\alpha^q = \beta^q = (e_1, e_2, \ldots, e_r)$$

是 $C_{n_1} \times \cdots \times C_{n_r}$ 中相異的 $2q-1$ 個元素. 由於 $a^q = e_1$ 且 $b^q = e_2$, 這 $2q-1$ 個元素 α^i 以及 β^j 都符合

$$(\alpha^i)^q = (\beta^j)^q = (e_1, e_2, \ldots, e_r). \tag{10.2}$$

別忘了 $(e_1, \ldots, e_r)$ 是 $C_{n_1} \times \cdots \times C_{n_r}$ 中的 identity, 所以 $C_{n_1} \times \cdots \times C_{n_r}$ 和 F^* 間的 isomorphism 會將 $(e_1, \ldots, e_r)$ 送到 F^* 的 identity 1. 而且這個 isomorphism (因為是一對一) 也會將 α^i 和 β^j 這 $2q-1$ 個相異的元素送到 F^* 中 $2q-1$ 個相異的元素. 由式子 (10.2) 我們知這 $2q-1$ 個 F^* 中的元素都符合 $x^q - 1 = 0$. 但是 Theorem 10.3.3 告訴我們 $x^q - 1$ 在 F 中至多只能有 q 個根, 因此得到矛盾. 也就是說 $F^* \simeq C_{n_1} \times \cdots \times C_{n_r}$ 中的 $n_1, \ldots, n_r$ 都兩兩互質, 故得證 F^* 是一個 cyclic group. □

F^* 是 cyclic 表示存在 $a \in F^*$ 使得所有 F^* 中的元素都是 a^i 這種形式, 所以我們有以下這個重要的性質.

Corollary 10.4.4. 假設 F 是一個 *finite field* 且 $|F| = p^k$, 則存在 $a \in F$ 滿足 $\mathbb{F}_p(a) = F$ 且 a *over* $\mathbb{F}_p$ 的 *degree* 為 k.

Proof. 令 $a \in F^* \subseteq F$ 產生 F^* 這一個 cyclic group. 回顧一下 $\mathbb{F}_p(a)$ 是 F 中包含 a 和 $\mathbb{F}_p$ 最小的 filed, 因此我們自然有 $\mathbb{F}_p(a) \subseteq F$. 另一方面任取 $b \in F$, 如果 $b = 0$, 則自然 $b \in \mathbb{F}_p(a)$; 如果 $b \neq 0$, 表示 $b \in F^*$, 故存在 $i \in \mathbb{N}$ 使得 $b = a^i$. 由於 $\mathbb{F}_p(a)$ 是一個 field, 故此時 $b = a^i \in \mathbb{F}_p(a)$. 因此證得 $F \subseteq \mathbb{F}_p(a)$, 故知 $F = \mathbb{F}_p(a)$.

由於已知 $|F| = p^k$, 故利用 Theorem 10.4.1 知 $[\mathbb{F}_p(a) : \mathbb{F}_p] = [F : \mathbb{F}_p] = k$. 因此由 Corollary 10.1.7 知 a over $\mathbb{F}_p$ 的 minimal polynomial 的 degree 為 k, 故由定義知 a over $\mathbb{F}_p$ 的 degree 為 k. □

接下來我們要證 finite field 的存在性, 即給定任一質數 p 以及 $k \in \mathbb{N}$, 我們要找到一個 finite field F 其元素個數剛好是 p^k. 首先注意當 $k = 1$ 時 $\mathbb{Z}/(p)$ 就是一個元素個數為 p 的 finite filed, 為了方便我們將此 filed 記為 $\mathbb{F}_p$. Theorem 10.4.1 告訴我們一個元素個數為 p^k 的 finite filed F 若存在, 則 F 一定會是 $\mathbb{F}_p$ 的一個 extension. 另外 Proposition 10.4.2 告訴我們在此情形 $x^{p^k} - x$ 在 F 中必定 splits into linear factors. 因此要尋找 F 必須從這兩個觀點出發.

Theorem 10.4.5. 給定任一質數 p 以及 $k \in \mathbb{N}$, 一定存在一個 *finite field* F 滿足 $|F| = p^k$.

Proof. 考慮 $x^{p^k} - x \in \mathbb{F}_p[x]$, Theorem 10.3.6 告訴我們存在一個 filed L 是 $\mathbb{F}_p$ 的一個 finite extension 使得 $x^{p^k} - x$ 在 L 中 splits into linear factors. 現在考慮

$$F = \{a \in L \mid a^{p^k} = a\},$$

也就是說 F 是 L 中 $x^{p^k}-x$ 所有的根所成的集合.

我們首先證明 F 是一個 filed. 利用 Lemma 9.1.4, 我們只要檢查對任意 $a,b\in F$ 且 $b\neq 0$ 皆有 $a-b\in F$ 以及 $a/b\in F$ 即可. $a-b$ 以及 a/b 當然都是 L 的元素, 再加上由 Lemma 9.2.5 我們有

$$(a-b)^{p^k}=a^{p^k}-b^{p^k}\quad\text{and}\quad(a/b)^{p^k}=a^{p^k}/b^{p^k},$$

故因 $a,b\in F$ (即 $a^{p^k}=a$ 且 $b^{p^k}=b$) 得知 $(a-b)^{p^k}=a-b$ 以及 $(a/b)^{p^k}=a/b$. 也就是說 $a-b$ 以及 a/b 都是 F 的元素.

接下來要證明 $|F|=p^k$. 要注意由假設 $x^{p^k}-x$ splits into linear factors in L, 我們只能知 F 的元素個數至多有 p^k 個, 除非能證得 $x^{p^k}-x$ 沒有重根. 要證明 $x^{p^k}-x$ 沒有重根, 我們先任取 $a\in L$ 是 $x^{p^k}-x$ 的一個根, 由 Lemma 10.3.1 知存在 $h(x)\in L[x]$ 使得 $x^{p^k}-x=(x-a)\cdot h(x)$. 若得 $h(a)\neq 0$, 則知 a 不是重根. 然而利用 Lemma 9.2.6, 我們知道 $(x-a)^{p^k}-(x-a)=x^{p^k}-a^{p^k}-x+a$. 由於 $a^{p^k}=a$ (因假設 a 是 $x^{p^k}-x$ 的一個根), 故得

$$x^{p^k}-x=(x-a)^{p^k}-(x-a)=(x-a)\cdot h(x),$$

其中 $h(x)=(x-a)^{p^k-1}-1$. 因為 $h(a)=-1\neq 0$, 故知任意 $x^{p^k}-x$ 的根都不是重根. 因此得證 F 是一個有 p^k 個元素的 finite field. □

利用 finite field 的存在性以及Corollary 10.4.4, 我們馬上有以下的應用.

Corollary 10.4.6. 假設 $\mathbb{F}_p$ 是一個有 p 個元素的 *finite field,* 則對任意 $k\in\mathbb{N}$, 皆存在 $g(x)\in\mathbb{F}_p[x]$ 在 $\mathbb{F}_p[x]$ 中是 *irreducible* 且 $\deg(g(x))=k$.

Proof. 利用 Theorem 10.4.5 知存在一個 finite field F 滿足 $[F:\mathbb{F}_p]=k$. 故由 Corollary 10.4.4 知存在 $a\in F$ 使得 $F=\mathbb{F}_p(a)$, 且由於 $[\mathbb{F}_p(a):\mathbb{F}_p]=k$ 知 a over $\mathbb{F}_p$ 的 minimal polynomial 的 degree 為 k. 由於 minimal polynomial 一定是 irreducible (Lemma 10.1.1), 故得證本定理. □

接下來我們來看在 $\mathbb{F}_p[x]$ 中的 irreducible element 的特性.

Lemma 10.4.7. 假設 $\mathbb{F}_p$ 是一個有 p 個元素的 *finite field* 且 $g(x)\in\mathbb{F}_p[x]$ 在 $\mathbb{F}_p[x]$ 中是 *irreducible.* 若 $\deg(g(x))=k$, 則在 $\mathbb{F}_p[x]$ 中 $g(x)\mid x^{p^k}-x$.

Proof. 由於 $\deg(g(x))=k$, 利用 Theorem 10.3.4 知存在一個 $\mathbb{F}_p$ 的 extension L 滿足 $[L:\mathbb{F}_p]=k$ 且 $a\in L$ 滿足 $g(a)=0$. 換言之, L 是一個 finite field 且 $|L|=p^k$. 然而 Proposition 10.4.2 告訴我們 L 中的元素都會是 $f(x)=x^{p^k}-x$ 的根, 因此由 $a\in L$ 知 $f(a)=0$. 要注意事實上 $g(x)$ 會和 a over $\mathbb{F}_p$ 的 minimal polynomial $h(x)$ associates. 這是因為 $g(a)=0$ 故利用 Lemma 10.1.1 (1) 知 $h(x)\mid g(x)$, 但 $g(x)$ 又假設是 irreducible, 故得 $h(x)$ 和 $g(x)$ associates (注意 $h(x)$ 不可能是 unit). 又由於 $f(a)=0$, 再利用一次 Lemma 10.1.1 (1) 知 $h(x)\mid f(x)$ (即 $f(x)\in\big(h(x)\big)$). 故由 $g(x)$ 和 $h(x)$ associates 知 $\big(g(x)\big)=\big(h(x)\big)$, 因此得證 $f(x)\in\big(g(x)\big)$ 即 $g(x)\mid f(x)$. □

最後我們來看有關 finite field 的唯一性. 我們將證明若 K 和 L 都是 finite field 且 $|K| = |L|$ 則 $K \simeq L$. 首先要強調的是這裡的 isomorphic 指的是 ring 的 isomorphism. 大家或許還記得在線性代數中兩個 vector space 若 dimension 相同, 則它們之間是 isomorphic. 不過這裡的 isomorphic 是指 vector space 間的 isomorphism, 要求的函數是 linear transformation, 僅保持加法的結構. 另外 K^* 和 L^* 是元素個數相同的 cyclic group, 從 Theorem 3.1.1 知 K^* 和 L^* 也是 isomorphic. 不過這裡的 isomorphic 指的是 group 的 isomorphism, 僅保持乘法的結構. 這兩種 isomorphic 都不能保證 K 和 L 間存在著 ring isomorphism. 我們的證明不是真的找到 K 的 L 的 ring isomorphism. 而是想找到一個 field F 滿足 $K \simeq F$ 且 $F \simeq L$, 則利用 isomorphism 的 transitivity 性質得證 $K \simeq L$.

Theorem 10.4.8. 假設 K 和 L 都是 *finite field* 且 $|K| = |L|$, 則 K 和 L 之間存在一個 *ring isomorphism.* 也就是說 $K \simeq L$ *as rings.*

Proof. 首先觀察當 $|K| = |L| = p$ 時, 由 Theorem 10.4.1 知 K 存在一個 subfield 和 $\mathbb{Z}/\big(p\big)$ isomorphic. 不過由於 $|K| = \big|\mathbb{Z}/\big(p\big)\big| = p$, 故得知 $K \simeq \mathbb{Z}/\big(p\big)$. 同理得 $L \simeq \mathbb{Z}/\big(p\big)$, 故知 $K \simeq L$.

現在看一般 $|K| = |L| = p^k$ 的情形. 由於所有元素個數為 p 的 finite field 皆 isomorphic, 所以我們可以假設 K 和 L 都是 $\mathbb{F}_p$ 的 extension, 其中 $\mathbb{F}_p$ 就是元素個數為 p 的 finite field. 由於 $|K| = p^k$, 利用 Corollary 10.4.4 知存在 $a \in K$ 使得 $\mathbb{F}_p(a) = K$ 且 a over $\mathbb{F}_p$ 的 minimal polynomial $g(x)$ 的 degree 是 k. 因此由 Corollary 10.1.7 得

$$K = \mathbb{F}_p(a) \simeq \mathbb{F}_p[x]/\big(g(x)\big).$$

或許同學們會想對 L 如法泡製得到 $L \simeq \mathbb{F}_p[x]/\big(g(x)\big)$. 事實上這是不行的, 因為雖然 Corollary 10.4.4 告訴我們存在 $a' \in L$ 使得 $L = \mathbb{F}_p(a')$, 不過 a' over $\mathbb{F}_p$ 的 minimal polynomial 不見得就是 $g(x)$. 要克服這個困難我們得利用 Lemma 10.4.7. 首先, 由於 $|L| = p^k$, Proposition 10.4.2 告訴我們 $x^{p^k} - x$ splits into linear factors in L. 不過由於 $g(x)$ 在 $\mathbb{F}_p[x]$ 中是 irreducible (Lemma 10.1.1), 因此由 Lemma 10.4.7 得知 $g(x) \mid x^{p^k} - x$. 所以 $g(x)$ 也 splits into linear factors in L. 換言之在 L 中存在 $b \in L$ 滿足 $g(b) = 0$. 當然了 $g(x)$ 是 b over $\mathbb{F}_p$ 的 minimal polynomial. 原因是 b over $\mathbb{F}_p$ 的 minimal polynomial 一定是 $g(x)$ 的 divisor (Lemma 10.1.1) 但 $g(x)$ 是 irreducible 且兩者皆為 monic polynomial, 故得證 $g(x)$ 是 b over $\mathbb{F}_p$ 的 minimal polynomial. 因此由 Corollary 10.1.7 知

$$\mathbb{F}_p[x]/\big(g(x)\big) \simeq \mathbb{F}_p(b).$$

不過由於 $\mathbb{F}_p(b) \subseteq L$ 且 $[L : \mathbb{F}_p] = [\mathbb{F}_p(b) : \mathbb{F}_p] = k$, 我們得證 $L = \mathbb{F}_p(b)$. 故知

$$L \simeq \mathbb{F}_p[x]/\big(g(x)\big) \simeq K.$$

□

關於大學基礎代數中 field 的性質, 我們就介紹至此. 我們並沒有觸及所謂的 Galois Theory, 不過已有足夠的預備知識. 若同學們對本講義中的 field 理論很清楚了, 應該可以更進一步的去了解 Galois Theory.