Solutions Manual for Gallian's Contemporary Abstract Algebra 8/e

張世杰
bfhaha@gmail.com

January 12, 2017

Contents

0 Chapter 0

0.1 For $n = 5, 8, 12, 20$, and 25, find all positive integers less than n and relatively prime to n.

補充. relatively prime 就是“互質”的意思, 所以題目是要找小於 n 且與 n 互質的所有正整數。例如 $n = 12$ 時, 我們可以先算出 $12 = 2^2 \cdot 3$, 我們要找跟 12 互質且小於 12 的正整數時, 我們只要找 “不含有”因數 2 跟因數 3 的正整數就好。

0.2 Determine

$$\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2 \quad , \quad 2 \cdot 3^3 \cdot 7 \cdot 11)$$

and

$$\operatorname{lcm}(2^3 \cdot 3^2 \cdot 5 \quad , \quad 2 \cdot 3^3 \cdot 7 \cdot 11).$$

0.3 Determine $51 \mod 13$,
$342 \mod 85$,
$62 \mod 15$,
$10 \mod 15$,
$(82 \cdot 73) \mod 7$,
$(51 + 68) \mod 7$,
$(35 \cdot 24) \mod 11$,
and $(47 \cdot 68) \mod 11$.

補充. $a \mod n$ 的意思就是 a 被 n 除之後的餘數, 例如 17 被 5 除餘 2, 所以 $17 \mod 5 = 2$。

你可能對這個 mod 運算感到彆扭, 但事實上, 你平常就已經在使用它了, 例如我們的時鐘就是 mod 12, 所以 14 點也可以說是下午 $14 \mod 12 = 2$ 點; 又或者是星期就是 mod 7。

0.4 Find integers s and t such that $1 = 7 \cdot s + 11 \cdot t$. Show that s and t are not unique.

補充. 我作一題更複雜的給你看: Find integers s and t such that $1 = 69 \cdot s + 31 \cdot t$.

$$\begin{aligned} 69 &= 31 \cdot 2 + 7, && (1) \\ 31 &= 7 \cdot 4 + 3, && (2) \\ 7 &= 3 \cdot 2 + 1. && (3) \end{aligned}$$

$$\begin{aligned} (18) \Rightarrow 1 &= 7 - 3 \cdot 2 \\ &\overset{(17)}{\overset{\downarrow}{=}} 7 - (31 - 7 \cdot 4) \cdot 2 \\ &= 7 - 31 \cdot 2 + 7 \cdot 8 \\ &= 7 \cdot 9 - 31 \cdot 2 \\ &\overset{(16)}{\overset{\downarrow}{=}} (69 - 31 \cdot 2) \cdot 9 - 31 \cdot 2 \\ &= 69 \cdot 9 - 31 \cdot 18 - 31 \cdot 2 \\ &= 69 \cdot 9 - 31 \cdot 20 \\ &\Rightarrow s = 9, \quad t = -20. \end{aligned}$$

注意到 $\gcd(7, 11)$ 及 $\gcd(69, 31)$ 都是1。一般來說, 我們有

$$\gcd(a, b) = 1 \Leftrightarrow \exists s, t \in \mathbb{Z} \text{ such that } as + bt = 1. \qquad (4)$$

這超級重要的, 你以後看到 a, b 互質 (relatively prime) 或是 $\gcd(a, b) = 1$, 你就要馬上想到他, 這不是很好證, 你不妨就先把他記下來。

另外, 我們其實還有

$$\gcd(a, b) = d \Rightarrow \exists s, t \in \mathbb{Z} \text{ such that } as + bt = d. \qquad (5)$$

0.6 Suppose a and b are integers that divide the integer c. If a and b are relatively prime, show that ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

補充. Since $a \mid c$ and $b \mid c$, suppose that

$$c = aq_1, \quad c = bq_2, \quad q_1, q_2 \in \mathbb{Z}. \qquad (6)$$

$$\begin{aligned} & \text{Since } \gcd(a, b) = 1 \\ \overset{(4)}{\overset{\downarrow}{\Rightarrow}} \quad & \exists s, t \in \mathbb{Z} \text{ such that } as + bt = 1 \\ \overset{\text{multiplying } c}{\overset{\downarrow}{\Rightarrow}} \quad & asc + \underline{\qquad} = c \\ \overset{(6)}{\overset{\downarrow}{\Rightarrow}} \quad & as(bq_2) + \underline{\qquad\qquad} = c \\ \Rightarrow \quad & ab(sq_2) + \underline{\qquad\qquad} = c \\ \Rightarrow \quad & ab(sq_2 + \underline{\qquad}) = c \\ \Rightarrow \quad & ab \mid c. \end{aligned}$$

如果 $\gcd(a, b) \neq 1$ 時的反例自己想想。

0.7 If a and b are integers and n is a positive integer, prove that $a \mod n = b \mod n$ if and only if n divides $a - b$.

補充. 關於 $a \mod n$ 這東西, 如果你沒有學過基礎數論, 請務必花一些時間把它弄熟, 我實在無法過分強調它在數論及代數中的重要性。

先複習一下高中學的“整除(divide)”, a 整除 b 的意思就是 a 是 b 的因數, 或是說 b 是 a 的倍數, 也就是存在整數 q, 使得 $b = aq$, 我們記作 $a \mid b$, 其中 $a \neq 0$。

我們剛剛講過, $a \mod n$ 代表一個數字, 這個數字就是 a 被 n 除之後的餘數, 所以 $a \mod n = b \mod n$ 的意思就是 a 跟 b 被 n 除之後的餘數會是一樣的, 我們稱 “a 跟 b 對模 n 同餘”, 用符號來記的話, 就是 $a \equiv b \pmod{n}$。所以Exercise 0.7的意思就是

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b) \tag{7}$$

我們證明如下。

$$\begin{aligned}
& a \equiv b \pmod{n} \leftarrow \text{慣用的符號} \\
\Leftrightarrow \quad & a \mod n = b \mod n \leftarrow \text{課本用的符號} \\
\Leftrightarrow \quad & a \div n = q_1 \ldots r, \quad b \div n = q_2 \ldots r \leftarrow \text{國小用的符號, 好懷念啊\textasciitilde} \\
\Leftrightarrow \quad & a = nq_1 + r, \quad b = nq_2 + r, \quad q_1, q_2 \in \mathbb{Z} \leftarrow \text{高中用的符號} \\
\Leftrightarrow \quad & (a - b) = (nq_1 + \cancel{r}) - (nq_2 + \cancel{r}) = nq_1 - nq_2 = n(q_1 - q_2) \\
\Leftrightarrow \quad & (a - b) = n(q_1 - q_2) \\
\Leftrightarrow \quad & n \mid a - b.
\end{aligned}$$

另外, 這個 $\equiv$ 其實就是一個 equivalence relation 這個我們之後會談。

0.8 Let $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

補充. 用反證法。

$$\begin{aligned}
& \text{Suppose} \gcd(a', b') = k > 1 \qquad (8) \\
\Rightarrow \quad & k \mid a', \quad k \mid b' \\
\Rightarrow \quad & a' = kq_1, \quad b' = kq_2, \quad q_1, q_2 \in \mathbb{Z} \\
\Rightarrow \quad & a = da' = dkq_1, \quad b = \underline{\qquad} = \underline{\qquad} \\
\Rightarrow \quad & dk \mid a \text{ and } \underline{\qquad} \\
\overset{\substack{\text{第10題} \\ \downarrow}}{\Rightarrow} \quad & dk \mid \gcd(a, b) = d \\
\Rightarrow \quad & dk \mid d \\
\Rightarrow \quad & dk \leq d, \text{ contrary to (8).}
\end{aligned}$$

這題的另一種表示就是

$$\gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1. \tag{9}$$

你可以試試看證明

$$a \mid bc \Rightarrow \frac{a}{\gcd(a, b)} \mid \frac{b}{\gcd(a, b)} \cdot c.$$

由此再配合 Exercise 0.19及(9), 可以得到

$$a \mid bc \Rightarrow \frac{a}{\gcd(a,b)} \mid c.$$

這幾個結果我們在後面學 cyclic group 的時候會用到。

0.9 Let n be a fixed positive integer greater than 1. If $a \mod n = a'$ and $b \mod n = b'$, prove that $(a+b) \mod n = (a'+b') \mod n$ and $(ab) \mod n = (a'b') \mod n$. (This exercise is referred to in Chapter 6, 8, 10, and 15.)

補充.

$$\begin{aligned}
& a \mod n = a', \quad b \mod n = b' \\
\overset{(7)}{\overset{\downarrow}{\Rightarrow}} \quad & n \mid (a-a'), \quad n \mid (b-b') \\
\Rightarrow \quad & a - a' = nq_1, \quad b - b' = nq_2, \quad q_1, q_2 \in \mathbb{Z} \\
\Rightarrow \quad & a = a' + nq_1, \quad b = \underline{\hspace{2cm}} \\
\Rightarrow \quad & a + b = (a' + nq_1) + (\underline{\hspace{2cm}}) \\
& = (a'+b') + (nq_1 + \underline{\hspace{1cm}}) = (a'+b') + n(q_1 + \underline{\hspace{1cm}}) \\
\Rightarrow \quad & (a+b) - (a'+b') = n(q_1 + \underline{\hspace{1cm}}) \\
\Rightarrow \quad & n \mid (a+b) - (a'+b') \\
\Rightarrow \quad & (a+b) \equiv (a'+b') \pmod n
\end{aligned}$$

$(a \cdot b) \equiv (a' \cdot b') \pmod n$ 也是類似的方法。

利用這題的結果, 你應該想想Exercise 0.3有沒有更快的算法。

0.10 Let a and b be positive integers and let $d = \gcd(a,b)$ and $m = \operatorname{lcm}(a,b)$. If t divides both a and b, prove that t divides d. If s is a multiple of both a and b, prove that s is a multiple of m.

補充. 前半部比較重要, 後半部不妨先跳過。

我們先來證一個 Lemma: If $t \mid a$ and $t \mid b$, then $t \mid as + bu$ for any $s, u \in \mathbb{Z}$. 事實上, 這是非常基本的技巧,

$$\begin{aligned}
& \text{If } t \mid a \text{ and } t \mid b \\
\Rightarrow \quad & a = tq_1, \quad b = \underline{\hspace{1cm}}, \quad q_1, q_2 \in \mathbb{Z} \\
\Rightarrow \quad & as = t(q_1 s), \quad bu = t(q_2 u), \quad q_1, q_2, s, u \in \mathbb{Z} \\
\Rightarrow \quad & as + bu = t(q_1 s) + t(q_2 u) = t(\underline{\hspace{2cm}}) \\
\Rightarrow \quad & t \mid as + bu. \qquad (10)
\end{aligned}$$

來證原題目:

$$\begin{aligned}
& \gcd(a,b) = d \\
\overset{(5)}{\overset{\downarrow}{\Rightarrow}} \quad & \exists s, u \in \mathbb{Z} \text{ such that } as + bu = d. \qquad (11) \\
& \text{If } t \mid a \text{ and } t \mid b \\
\overset{(10)}{\overset{\downarrow}{\Rightarrow}} \quad & t \mid as + bu \overset{(11)}{\overset{\downarrow}{=}} d.
\end{aligned}$$

你要想一想這題背後的意義, 這題說明了, 任何公因數都是最大公因數的因數, 聽起來眞繞口。

0.11 Let n and a be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax \pmod{n} = 1$ has a solution if and only if $d = 1$.

補充. 想一想這題跟 $U(n)$ 的定義有何關係? $U(n)$ 就是你們在 Elmentary Number Theory 中學的 $\mathbb{Z}_n^*$。

Proof. We need a lemma:

$$\gcd(a, b) = 1 \Leftrightarrow \exists s, t \in \mathbb{Z} \text{ such that } as + bt = 1.$$

($\Leftarrow$) It follows immediately from p.4, thm.0.2.

($\Rightarrow$) If there exists $s, t \in \mathbb{Z}$ such that $as + bt = 1$, then since $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, we have $\gcd(a, b) \mid (as + bt) = 1$. Which implies that $\gcd(a, b) = 1$.

$$\begin{aligned}
&\gcd(a, n) = 1 \\
\overset{\text{Lemma}}{\underset{}{\overset{\downarrow}{\Leftrightarrow}}}\quad &\exists s, t \in \mathbb{Z}, \text{ such that } as + nt = 1 \\
\Leftrightarrow\quad &as - 1 = n(-t) \\
\Leftrightarrow\quad &n \mid (as - 1) \\
\Leftrightarrow\quad &as \equiv 1 \pmod{n} \\
\Leftrightarrow\quad &ax \equiv 1 \pmod{n} \text{ has a solution} \\
\Leftrightarrow\quad &a \text{ has a multiplicative inverse modulo } n \\
\Leftrightarrow\quad &a \in U(n)
\end{aligned}$$

■

類似 0.11 Solve the congruence equation $69x \equiv 1 \pmod{31}$.

補充. 由 Exercise 0.4的提示,

$$\begin{aligned}
&69 \cdot 9 + 31 \cdot (-20) = 1 \\
\Rightarrow\quad &69 \cdot 9 - 1 = 31 \cdot 20 \\
\Rightarrow\quad &31 \mid 69 \cdot 9 - 1 \\
\Rightarrow\quad &69 \cdot 9 \equiv 1 \pmod{31}
\end{aligned} \tag{12}$$

利用(12)及 Exercise 0.9的結果, 將 $69x \equiv 1 \pmod{31}$ 左右同乘以 9, 得到

$$\begin{aligned}
&9 \cdot 69x \equiv 9 \cdot 1 \pmod{31} \\
\overset{(12)}{\overset{\downarrow}{\Rightarrow}}\quad &1 \cdot x \equiv x \equiv 9 \pmod{31}
\end{aligned}$$

這個我們在後面求一些 group 中的元素的 inverse 時會用到。

0.13 Suppose that m and n are relatively prime and r is any integer. Show that there are integers x and y such that $mx + ny = r$.

補充. 這題就是(4), 證明有點難度, 你可以先跳過, 但如果你想要挑戰看看的話, 下面是提示。

你學期末學完 ring 之後, 你會發現如果用 ring 的觀點來看, 這個定理就會變得很簡單。

- Consider the set $S = \{ms + nt \mid s, t \in \mathbb{Z}\}$.
- Consider the subset $S^+ = \{a \in S \mid a > 0\}$ of S.
- Prove that $S^+ \neq \varnothing$.
- Apply the Well-Ordering Principle on S^+, there is a smallest positive integer d in S^+.
- Suppose that $d = mp + nq$.
- If $c \mid m$ and $c \mid n$, by (10), $c \mid mp + nq = d$.
- That is, $d = \gcd(m, n)$.
- If $\gcd(m, n) = 1$, then there exist $p, q \in \mathbb{Z}$ such that $mp + nq = 1$. Thus, $r = m(pr) + n(qr)$. Let $x = pr$ and $y = qr$.

0.16 Determine $7^{1000} \mod 6$ and $6^{1001} \mod 7$.

補充. 注意到 $7 \equiv 1 \pmod 6$ and $6 \equiv -1 \pmod 7$, 利用Exercise 0.9的結果。例如

$$6^{1001} \equiv (-1)^{1001} \equiv -1 \equiv 6 \pmod 7.$$

0.17 Let a, b, s, and t be integers. If $a \pmod{st} = b \pmod{st}$, show that $a \pmod s = b \pmod s$ and $a \pmod t = b \pmod t$. What condition on s and t is needed to make the converse true?

0.18 Determine $8^{402} \mod 5$.

補充. 注意到 $8^2 \equiv -1 \pmod 5$, 利用第9題的結果。例如

$$8^{402} \equiv (8^2)^{201} \equiv 64^{201} \equiv (-1)^{201} \equiv \cdots \pmod 5.$$

0.19 Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

Proof. $\gcd(a, c)$ divides $\gcd(a, bc)$ is obviously. We show that $\gcd(a, bc)$ divides $\gcd(a, c)$. Since $\gcd(a, b) = 1$, by p.4, thm.0.2, there exists $s, t \in \mathbb{Z}$ such that $as + bt = 1$.

$$\begin{aligned}
\text{Let} \quad & d = \gcd(a, bc) \\
\Rightarrow \quad & d \mid a \text{ and } d \mid bc \\
\Rightarrow \quad & d \mid [a(cs) + (bc)t] = (as + bt)c = c \\
\Rightarrow \quad & d \mid \gcd(a, c).
\end{aligned}$$

■

類似 0.19 If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

補充. Since $a \mid bc$, suppose that

$$bc = aq, \quad q \in \mathbb{Z}. \tag{13}$$

$$\begin{aligned}
& && \text{Since } \gcd(a,b) = 1 \\
& \overset{\overset{(4)}{\downarrow}}{\Rightarrow} && \exists s,t \in \mathbb{Z} \text{ such that } as + bt = 1 \\
& \overset{\overset{\text{multiplying } c}{\downarrow}}{\Rightarrow} && \underline{\qquad} + (bt)c = c \\
& \Rightarrow && \underline{\qquad} + (bc)t = c \\
& \overset{\overset{(13)}{\downarrow}}{\Rightarrow} && asc + (aq)t = c \\
& \Rightarrow && a(\underline{\qquad\qquad}) = c \\
& \Rightarrow && a \mid c.
\end{aligned}$$

0.22 Express $(-7-3i)^{-1}$ in standard form.

補充.

$$\frac{1}{-7-3i} = \frac{(-7+3i)}{(-7-3i)(-7+3i)}.$$

0.23 Express $\frac{-5+2i}{4-5i}$ in standard form.

0.27 For every positive integer n, prove that a set with exactly n elements has exactly 2^n subsets (counting the empty set and the entire set).

補充. 這是高中的排列組合問題。

0.30 (Generalized Euclid's Lemma) If p is a prime and p divides $a_1 a_2 \cdots a_n$, prove that p divides a_i for some i.

0.31 Use the Generalized Euclid's Lemma (see Exercise 0.30) to establish the uniqueness portion of the Fundamental Theorem of Arithmetic.

提示. Use mathematical induction on n.

0.33 Prove that the First Principle of Mathematical Induction isa consequence of the Well Ordering Principle.

0.37 In the cut "As" from *Songs in the Key of Life.* Stevie Wonder mentions the equation $8 \times 8 \times 8 = 4$. Find all integers n for which this statement is true, modulo n.

補充. 其實就是找 n 使得 $8 \times 8 \times 8 \equiv 4 \pmod{n}$.

關於 Stevie Wonder, 我想我必須要多講一點, 你可能不認識他, 但你一定聽過他的*I Just Called To Say I Love You.* (`http://goo.gl/ADsXte`) 他可以算是美國的蕭煌奇, (恩... 應該說蕭煌奇是台灣的 Stevie Wonder,) 布魯斯威利在終極警探 裡說過一句玩笑話: "Who's driving this car, Stevie Wonder?" Stevie Wonder 膾炙人口的當然不只這首歌, 還有

- You Are The Sunshine Of My Life. `http://goo.gl/BbrnI1`

- Part Time Lover. `http://goo.gl/YiLfRe`
- Sir Duke. `http://goo.gl/ZxyFeG`
- Superstition. `http://goo.gl/W12uEp`
- Master Blaster (Jammin'). `http://goo.gl/tm1xFp`.
- Uptight (Everything's Alright). `http://goo.gl/TxRU5p`

0.39 If it is $2:00$ A.M. now, what time will it be 3736 hours from now?

補充. mod 24

0.50 The 10-digit International Standard Book Number (ISBN-10) $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ has the property $(a_1, a_2, ..., a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1) \mod 11 = 0$. The digit a_{10} is the check digit. When a_{10} is required to be 10 to make the dot product 0, the character X is used as the check digit. Suppose that an ISBN-10 has a smudged entry where the question mark appears in the number 0-716?-2841-9. Determine the missing digit.

補充. $(a_1, a_2, ..., a_{10}) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$ 是內積的意思, 就是

$$10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + \cdots + 2 \cdot a_9 + 1 \cdot a_{10}.$$

這題就是 mod 的一個經典應用, 就在你手上拿的這本書背面。

英國大數學家 Hardy 在1940寫的“一個數學家的辯白”裡面, 提到數論是個沒什麼應用的科目, 他萬萬想不到今天數論在密碼學上的重要性。

在解這題的過程中, 你可能需要解 $6x \equiv 9 \pmod{11}$, 你可以將兩邊同乘以 2, 爲什麼知道要乘以2, 做完 Exercise 0.11你就知道了。

0.58 Let S be the set of real numbers. If $a, b \in S$, define $a \sim b$ if $a - b$ is an integer. Show that $\sim$ is an equivalence relation on S. Describe the equivalence classes of S.

Proof. For all $a \in S$, $a - a = 0 \in \mathbb{Z}$, so $a \sim a$, or says $(a, a) \in \sim$.

If $a \sim b$, then $a - b \in \mathbb{Z}$ and $b - a = -(a - b) \in \mathbb{Z}$. Thus, $b \sim a$.

If $a \sim b$ and $b \sim c$, then $a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$ and $a - c = (a - b) + (b - c) \in \mathbb{Z}$. Therefore, $a \sim c$. ■

補充. 我們先任意選定一個數字, 例如 3.4 好了, 我們知道 $3.4 \sim 3.4$, $4.4 \sim 3.4$, $5.4 \sim 3.4$, ... 我們可以考慮這個集合 $[3.4] = \{a \in \mathbb{R} \mid a \sim 3.4\}$, 所以 $3.4 \in [3.4]$, $4.4 \in [3.4]$, $5.4 \in [3.4]$, ... 這個集合 $[3.4]$ 就叫做一個 equivalence class。

equivalence relation 是比較抽象的內容, 其實你在學同餘“≡”及 $\mathbb{Z}_n$ 的時候就遇過了, 未來我們在學 coset 及代數拓樸時都還會再遇到他。雖然你不知道 equvalence relation 的話也可以往後學, 但是如果你瞭解它的話, 你會看到一番截然不同的數學面貌。

這是比較進階的內容, 你不知道的話也可以往後學, 但是如果你瞭解它的話, 你會看到一番截然不同的數學面貌, 我覺得這也是你讀數學系眞正該學的東西。

我們先來講講 relation, 助教我高中的時候, 數學課本的第一章就是“邏輯、集合、函數”, 這說明了這三個觀念是數學中最根本的東西, 我猜你早就聽過這句話了, 但你應該對這句話不是很有感覺, 我現在要展現這句話的深刻意涵給你看。

先講一下 direct product, 兩個集合 A 跟 B 的 direct product 就是一個新的集合, 記作 $A \times B$, 這個集合收集由 A 跟 B 分別取元素出來構成的有序對 (ordered pair), 簡單來說就是

$$A \times B \overset{\text{def.}}{=} \{(a,b) \mid a \in A, b \in B\}.$$

當然, 我們也可以由一個集合 S 自己跟自己做 direct product, 你以前學的 $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x,y) \mid x,y \in \mathbb{R}\}$ 就是一個典型的例子。

你回想一下國小學的小於關係, 例如

$$13 < 25, \quad \sqrt{2} < 2, \quad \frac{3}{4} < 1, \quad 21 \not< 10, \quad \pi \not< 2, \ldots$$

現在我們要用抽象、嚴謹的語言來描述這個“<”。

“<”在本質上是一個集合, 它是一個 $\mathbb{R} \times \mathbb{R}$ 的子集合(subset), 這個 subset “<”包含了下面這些元素

$$(13,25), \quad (\sqrt{2},2), \quad (\frac{3}{4},1), \ldots$$

但是不包含

$$(21,10), \quad (\pi,2), \ldots.$$

也就是

$$< = \{(13,25),(\sqrt{2},2),(\frac{3}{4},1),\ldots\} \subseteq \mathbb{R} \times \mathbb{R}.$$

但是

$$(21,10),(\pi,2) \notin < .$$

很抽象吧, 所以你看這個跟集合看似一點關係都沒有的觀念, 竟然可以用集合來定義它。

我們現在來定義什麼是 relation,

$$\text{a relation “} \sim \text{” on a set } S \overset{\text{def.}}{=} \text{ a subset } \sim \text{ of } S \times S.$$

這實在太抽象了, 所以通常如果 $(a,b) \in \sim$, 我們就記作 $a \sim b$, 所以剛剛的 $(13,25) \in <$, 我們就記作 $13 < 25$。數學家們眞是無聊嗎? 其實如果你瞭解這個 relation 的本質, 你在看數學上的很多事情時都會變得很淸楚。

有了 relation, 我們要定義 equivalence relation,

$$\text{a relation } \sim \text{ on a set } S \text{ is called an equivalence relation}$$
$$\text{if and only if the following statements hold:}$$
$$\text{(i) } \forall s \in S, (s,s) \in \sim .$$
$$\text{(ii) If } (s,t) \in \sim \text{, then } (t,s) \in \sim .$$
$$\text{(iii) If } (s,t) \in \sim \text{ and } (t,u) \in \sim \text{, then } (s,u) \in \sim .$$

或是也可以記作

$$\text{(i) } \forall s \in S, s \sim s.$$
$$\text{(ii) If } s \sim t \text{, then } t \sim s.$$
$$\text{(iii) If } s \sim t \text{ and } t \sim u \text{, then } s \sim u.$$

關於 equivalence relation 的基本練習就是驗證一個 relation是不是 equivalence relation, 假設 $S = \{a,b,c,d\}$, 請問下面哪一個 relation on S 是 equivalence relation?

- $\sim_1 = \{(a,b),(b,c),(c,d),(a,c),(b,d),(a,d)\}$
- $\sim_2 = \{(a,b),(b,c),(a,c)\}$
- $\sim_3 = \{(a,b),(b,c),(a,c),(a,a),(b,b),(c,c)\}$
- $\sim_4 = \{(a,b),(b,c),(a,c),(a,a),(b,b),(c,c),(d,d)\}$
- $\sim_5 = \{(a,b),(b,c),(a,c),(a,a),(b,b),(c,c),(d,d),(b,a),(c,b),(c,a)\}$

驗證一下 the relation $<$ on $\mathbb{R}$ 不是一個equivalence relation。

驗證一下 the relation $\equiv$ on $\mathbb{Z}$ 是一個equivalence relation。這個 equivalence relation 尤其重要, 我們後面會花很長的篇幅來討論它。

equivalence relation 跟 partition 是有密切關係的, 應該說他們算是同一件事。

你應該想想, equivalence relation 感覺上就是一種弱化的相等, 例如13跟9本來是不相等的, 可是在 mod 4 之下, 它們就是相等的, 也就是 $13 \equiv 9 \pmod 4$。

如果你覺得類似這種探討數學本質的活動很有趣, 想要知道更多的話, 你可以想想你以前國小學的整數乘法, 其實就是一個從 $\mathbb{Z}\times\mathbb{Z}$ 打到 $\mathbb{Z}$ 的函數, 也就是 $\times : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$, 例如 $\times(3,7) = 21$。

0.59 Let S be the set of integers. If $a, b \in S$, define aRb if $ab \geq 0$. Is R an equivalence relation on S?

補充.

0.60 Let S be the set of integers. If $a, b \in S$, define aRb if $a + b$ is even. Prove that R is an equivalence relation and determine the equivalence classes of S.

0.63 What is the last digit of 3^{100}? What is the last digit of 2^{100}?

補充. 一個數字 a 的個位數其實就是 $a \mod 10$, 這在高中就學過了 (?) 助教我離高中很遠很遠了...

0.65 (Cancellation Property) Suppose α, β, and γ are functions. If $\alpha\gamma = \beta\gamma$ and γ is one-to-one and onto, prove that $\alpha = \beta$.

Proof.

$$\begin{aligned}
\alpha(x) &= \Big(\alpha(\gamma\gamma^{-1})\Big)(x) \\
&= \Big((\alpha\gamma)\gamma^{-1}\Big)(x) \\
&= \Big((\beta\gamma)\gamma^{-1}\Big)(x) \\
&= \Big(\beta(\gamma\gamma^{-1})\Big)(x) \\
&= \beta(x)
\end{aligned}$$

■

1 Chapter 1

1.1 With pictures and words, describe each symmetry in D_3 (the set of symmetries of an equilateral triangle).

1.2 Write out a complete Cayley table for D_3. Is D_3 Abelian?

補充. 你先想想, abelian在 Cayley table 上如何表現?

這裡提供你一個記下 dihedral group D_n 的 Cayley Table 的好方法, 其中

$$D_n = \{1, a, a^2, ..., a^{n-1}, b, ba, ba^2, ..., ba^{n-1} \mid |a| = n, |b| = 2, ab = ba^{-1}\}.$$

在這裡以 D_3 爲例, 但這個規律對於一般的 D_n 都是成立的。

- 按照 $1, a, a^2, b, ba, ba^2$ 的順序, 將表頭塡上。
- 先寫出第一列。
- 將表格對半分成四等份, 然後畫交叉線, 把第一列的內容交叉塡下來。
- 接著分別利用四個部分的第一列來塡滿四個部分, 左半邊依序往左輪轉一格; 右半邊依序往右輪轉一格。

如下圖所示。

D_3	1	a	a^2	b	ba	ba^2
1	1	a	a^2	b	ba	ba^2
a		←			→	
a^2	←					→
b	b	ba	ba^2	1	a	a^2
ba		←			→	
ba^2	←					→

得到

D_3	1	a	a^2	b	ba	ba^2
1	1	a	a^2	b	ba	ba^2
a	a	a^2	1	ba^2	b	ba
a^2	a^2	1	a	ba	ba^2	b
b	b	ba	ba^2	1	a	a^2
ba	ba	ba^2	b	a^2	1	a
ba^2	ba^2	b	ba	a	a^2	1

1.3 In D_4, find all elements X such that
a. $X^3 = V$;
b. $X^3 = R_{90}$;
c. $X^3 = R_0$;
d. $X^3 = R_0$;
e. $X^3 = H$.

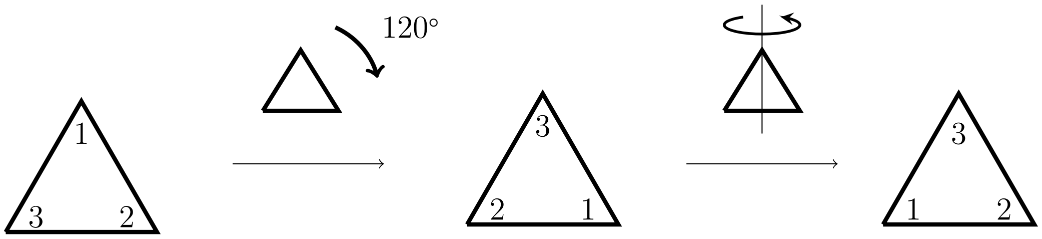
1.4 Describe in pictures or words the elements of D_5 (symmetries of a regular pentagon).

1.5 For $n \geq 3$, describe the elements of D_n. (Hint: You will need to consider two cases—n even and n odd.) How many elements does D_n have?

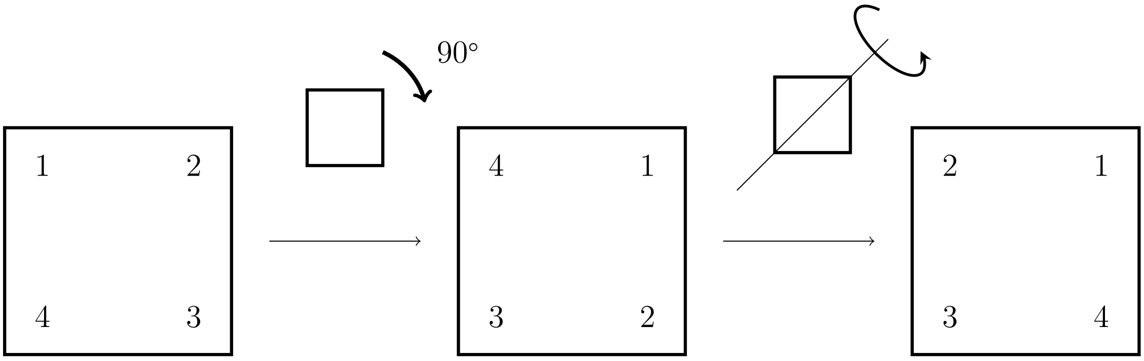
補充.

1.6 In D_n, explain geometrically why a reflection followed by a reflection must be a rotation.

提示. 將正 n 邊形的頂點按順時針依序標號, 觀察 rotation 或是 reflection 如何影響頂點標號的順逆。例如



或是



1.7 In D_n, explain geometrically why a rotation followed by a rotation must be a rotation.

補充.

1.8 In D_n, explain geometrically why a rotation and a reflection taken together in either order must be a reflection.

補充.

1.10 If r_1, r_2, and r_3 represent rotations from D_n and f_1, f_2, and f_3 represent reflections from D_n, determine whether $r_1 r_2 f_1 r_3 f_2 f_3 r_3$ is a rotation or a reflection.

1.11 Find elements A, B, and C in D_4 such that $AB = BC$ but $A \neq C$. (Thus, "cross cancellation" is not valid.)

1.12 Explain what the following diagram proves about the group D_n.

補充.

1.13 Describe the symmetries of a nonsquare rectangle. Construct the corresponding Cayley table.

1.14 Describe the symmetries of a parallelogram that is neither a rectangle nor a rhombus. Describe the symmetries of a rhombus that is not a rectangle.

1.15 Describe the symmetries of a noncircular ellipse. Do the same for a hyperbola.

1.17 For each of the snowflakes in the figure, find the symmetry group and locate the axes of reflective symmetry (disregard imperfections).

補充. 關於雪花的美我就不多說了, 仔細看這些美麗的結構, 你很難不相信神的存在。

- 你可以參考這個網站 `https://www.youtube.com/watch?v=fd-hb2xzvZI`,
- 助教上課給你們看的書在這裡, `http://goo.gl/uRFJba`, 博客來有賣, 700元而已, `http://goo.gl/CjZGqz`,
- 台灣很可惜看不到雪, 如果你企圖在家裡製造雪的話, 這個網站有教學, `http://goo.gl/h7pw3`, 不過我想買這些製作器材的錢可以出國好幾趟了。

1.19 Does a fan blade have a cyclic symmetry group or a dihedral symmetry group?

補充.

1.20 Bottle caps that are pried off typically have 22 ridges around the rim. Find the symmetry group of such a cap.

補充.

2 Chapter 2

常用結果

Gallian	Burton	Theorem
exe.0.13	p.21, thm.2.3	$\gcd(a,b)=d \Rightarrow \exists s,t$ such that $as+bt=d$
	p.23, thm.2.4	$\gcd(a,b)=1 \Leftrightarrow \exists s,t$ such that $as+bt=1$
exe.0.6	p.23, cor.2	$\gcd(a,b)=1, a \mid c, b \mid c \Rightarrow ab \mid c$
	p.24, thm.2.5	$\gcd(a,b)=1, a \mid bc \Rightarrow a \mid c$
p.79, cor.2		$\lvert a\rvert = n, a^s = e \Rightarrow n \mid s$
exe.3.4		$\lvert x\rvert = \lvert x^{-1}\rvert$
p.80, thm.4.2		$\lvert a^r\rvert = \frac{n}{\gcd(r,n)}$

2.1 Which of the following binary operations are closed?

(a) subtraction of positive integers

(b) division of nonzero integers

(c) function composition of polynomials with real coefficients

(d) multiplication of 2×2 matrices with integer entries

2.2 Which of the following binary operations are associative?

(a) multiplication $\mod n$

(b) division of nonzero rationals

(c) function composition of polynomials with real coefficients

(d) multiplication of 2×2 matrices with integer entries

2.3 Which of the following binary operations are commutative?

(a) subtraction of integers

(b) division of nonzero real numbers

(c) function composition of polynomials with real coefficients

(d) multiplication of 2×2 matrices with integer entries

2.4 Which of the following sets are closed under the given operation?

(a) $\{0, 4, 8, 12\}$ addition $\mod 16$

(b) $\{0, 4, 8, 12\}$ addition $\mod 15$

(c) $\{1, 4, 7, 13\}$ multiplication $\mod 15$

(d) $\{1, 4, 5, 7\}$ multiplication $\mod 9$

2.5 In each case, find the inverse of the element under the given operation.

(a) 13 in $\mathbb{Z}_{20}$

(b) 13 in $U(14)$

(c) $n - 1$ in $U(n)$ $(n > 2)$

(d) $3 - 2i$ in $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication

2.6 In each case, perform the indicated operation.

(a) In $\mathbb{C}^*$, $(7 + 5i)(-3 + 2i)$

(b) In $GL(2, \mathbb{Z}_{13})$, $\det \begin{bmatrix} 7 & 4 \\ 1 & 5 \end{bmatrix}$

(c) In $GL(2, \mathbb{R})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$

(d) In $GL(2, \mathbb{Z}_{13})$, $\begin{bmatrix} 6 & 3 \\ 8 & 2 \end{bmatrix}^{-1}$

2.8 Referring to Example 13, verify the assertion that subtraction is not associative.

2.9 Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

2.10 Show that the group $GL(2, \mathbb{R})$ of Example 9 is non-Abelian by exhibiting a pair of matrices A and B in $GL(2, \mathbb{R})$ such that $AB \neq BA$.

2.12 Given an example of group elements a and b with the property that $a^{-1}ba \neq b$.

2.15 Let G be a group and let $H = \{x^{-1} \mid x \in G\}$. Show that $G = H$ as sets.

2.20 For any integer $n > 2$, show that there are at least two elements in $U(n)$ that satisfy $x^2 = 1$.

提示. 這裡教各位一個解題技巧, 我相信, 這也是數學家們發現新結果的常用手段: 就是列出大量的例子, 然後再從中觀察並且大膽假設、小心求證。我們列出 $U(3) \sim U(9)$, 然後把滿足 $x^2 = 1$ 的元素圈起來, 你發現了什麼事情嗎?

$$\begin{array}{rcl} U(3) & = & \{\textcircled{1}, \textcircled{2}\} \\ U(4) & = & \{\textcircled{1}, \textcircled{3}\} \\ U(5) & = & \{\textcircled{1}, 2, 3, \textcircled{4}\} \\ & \downarrow & \text{剩下的自己圈} \\ U(6) & = & \{1, 5\} \\ U(7) & = & \{1, 2, 3, 4, 5, 6\} \\ U(8) & = & \{1, 3, 5, 7\} \\ U(9) & = & \{1, 2, 4, 5, 7, 8\} \\ & \vdots & \end{array}$$

你發現了什麼事情嗎?

Proof. When $n > 2$, $n - 1 \neq 1 \in U(n)$ and $1^2 = (n-1)^2 = 1$. ■

補充. 這題跟 Exercise 3.59有什麼關係?

2.22 Let G be a group with the property that for any x, y, z in the group, $xy = zx$ implies $y = z$. Prove that G is Abelian. ("Left-right cancellation" implies commutativity.)

Proof.

$$\underline{ab}_{y} = \underline{ba}_{z} \Leftarrow \underline{b}_{x}(\underline{ab}_{y}) = (\underline{ba}_{z})\underline{b}_{x}$$

■

2.23 (Law of Exponents for Abelian Groups) Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-Abelian groups?

2.24 (Socks-Shoes Property) Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your socks and shoes. Find distinct nonidentity elements a and b from a non-Abelian group such that $(ab)^{-1} = a^{-1}b^{-1}$. Find an example that shows that in a group, it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. What would be an appropriate name for the group property $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$?

補充. 我解釋一下爲什麼 $(sw)^{-1} = w^{-1}s^{-1}$ 叫做Socks-Shoes Property,

- 假設 s 表示穿鞋子,w 表示穿襪子。
- 那 sw 表示先穿襪子再穿鞋子, (注意, 我們看 $\underleftarrow{sw}$ 時是從右到左, 跟函數一樣。)
- 則 $(sw)^{-1}$ 表示要全部脫掉, 光脚丫。
- 脫掉時當然要先脫鞋子 s^{-1} 再拖襪子 w^{-1}, 也就是 $\underleftarrow{w^{-1}s^{-1}}$。
- 所以 $(sw)^{-1} = w^{-1}s^{-1}$。

2.25 Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.

Proof. $(\Rightarrow)$ For any $a, b \in G$,

$$(ab)^{-1} = b^{-1}a^{-1} \overset{\text{abelian}}{\overset{\downarrow}{=}} a^{-1}b^{-1}.$$

$(\Leftarrow)$ For any $a, b \in G$,

$$ab = (a^{-1})^{-1}(b^{-1})^{-1} \overset{\text{hypothesis}}{\overset{\downarrow}{=}} (a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba.$$

■

2.27 For any elements a and b from a group and any integer n, prove that $(a^{-1}ba)^n = a^{-1}b^na$.

補充. 這其實我們以前在 linear algebra 中, 講矩陣對角化的應用時就遇過了。例如 $A = P^{-1}DP$,$A^{100} = P^{-1}D^{100}P$。

Proof. If $n = 0$, then

$$(a^{-1}ba)^0 = e = a^{-1}a = aea^{-1} = ab^0a^{-1}.$$

If $n > 0$, then

$$(a^{-1}ba)^n = \underbrace{(a^{-1}b\cancel{a})(\cancel{a^{-1}}b\cancel{a})\cdots(\cancel{a^{-1}}ba)}_{n\text{ times}} = a^{-1}b^na.$$

If $n < 0$, then

$$\begin{aligned}(a^{-1}ba)^n &= ((a^{-1}ba)^{-1})^{-n}\\ &= (a^{-1}b^{-1}a)^{-n}\\ &= \underbrace{(a^{-1}b^{-1}\cancel{a})(\cancel{a^{-1}}b^{-1}\cancel{a})\cdots(\cancel{a^{-1}}b^{-1}a)}_{-n\text{ times}}\\ &= a^{-1}(b^{-1})^{-n}a\\ &= a^{-1}b^na.\end{aligned}$$

■

2.30 Give an example of a group with 105 elements. Give two examples of groups with 44 elements.

補充. Consider cyclic groups and dihedral groups.

2.31 Prove that every group table is a *Latin square*; that is, each element of the group appears exactly once in each row and each column.

補充. 這題隱含了一個很重要的訊息, 就是 group table 的每一行, 恰好都是這個 group 的元素的一個重新排列, 這我們在 Section 5還會再詳細討論。這個發現引出了一個重要的定理: Cayley Theorem.

2.34 Prove that if $(ab)^2 = a^2b^2$ in a group G, then $ab = ba$.

Proof.

$$\begin{aligned} & (ab)^2 = a^2b^2 \\ \Rightarrow \quad & abab = aabb \\ \overset{\substack{\text{left multiplying } a^{-1} \\ \downarrow}}{\Rightarrow} \quad & bab = abb \\ \overset{\substack{\text{right multiplying } b^{-1} \\ \downarrow}}{\Rightarrow} \quad & ba = ab. \end{aligned}$$

■

2.36 Let a and b belong to a group G. Find an x in G such that $xabx^{-1} = ba$.

2.37 Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.

Proof. Note that

$$x \neq e,\ x^3 = e \Rightarrow x^2 \neq e \Leftrightarrow x \neq x^{-1}.$$

Let $S = \{x \in G \mid x^3 = e\}$. Pick $x_1 \neq e \in S$. Then $x_1 \neq x_1^{-1}$ and $x_1^{-1} \in S$. Remove these two elements x_1 and x_1^{-1} from S. Pick x_2 from the remaining elements, do the same process as above. We can always remove two elements because $x_i^{-1} \neq x_j^{-1} \in S$ if $i \neq j$. Since G is finite, we can't do the process infinitely. Finally, there is only one element remain in S. That is, the identity element e. Thus, $S = \{e, x_1, x_1^{-1}, x_2, x_2^{-1}, , , , , x_n, x_n^{-1}\}$ and $\#S$ is odd.

Note that

$$x^2 \neq e \Leftrightarrow x \neq x^{-1}.$$

Let $S = \{x \in G \mid x^2 \neq e\}$. Pick $x_1 \neq e \in S$. Then $x_1 \neq x_1^{-1}$ and $x_1^{-1} \in S$ (why?). Remove these two elements x_1 and x_1^{-1} from S. Pick x_2 from the remaining elements, do the same process as above. We can always remove two elements because $x_i^{-1} \neq x_j^{-1} \in S$ if $i \neq j$. Since G is finite, we can't do the process infinitely. Finally, there is no element remain in S. Thus, $S = \{x_1, x_1^{-1}, x_2, x_2^{-1}, , , , , x_n, x_n^{-1}\}$ and $\#S$ is even. ■

補充. c.f. Exercise 3.59.

2.38 Given an example of a group with elements a, b, c, d and x such that $axb = cxd$ but $ab \neq cd$. (Hence "middle cancellation" is not valid in groups.)

2.39 Suppose that G is a group with the property that for every choice of elements in G, $axb = cxd$ implies $ab = cd$. Prove that G is Abelian. ("Middle cancellation" implies commutativity.)

補充. 1 □ $ab = ba$ □ 1

2.40 Find an element X in D_4 such that $R_{90}VXH = D'$.

補充. 想一想, 有沒有一眼就可以看出答案的方法。

2.41 Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n. Prove that $F_1F_2 \neq R_0$.

補充. Since $F_1^2 = F_2^2 = R_0$ and by Theorem 2.3, $F_1^{-1} = F_1 \neq F_2^{-1} = F_2$. If $F_1F_2 = R_0$, then $F_2 = F_1^{-1}$.

2.42 Suppose F_1 and F_2 are distinct reflections in a dihedral group D_n such that $F_1F_2 = F_2F_1$. Prove that $F_1F_2 = R_{180}$.

補充. See Section 1 Exercise 6 (p.37). Note that

$$(F_1F_2)^2 = (F_1F_2)(F_1F_2) = F_1(F_2F_1)F_2 = F_1(F_1F_2)F_2 = F_1^2F_2^2 = R_0.$$

2.43 Let R be any fixed rotation and F any fixed reflection in a dihedral group. Prove that $R^kFR^k = F$.

補充. It is sufficient to show that $R_{360/n}FR_{360/n} = F$. Note that $R = R_{360/n}^m$ for some m.

2.44 Let R be any fixed rotation and F any fixed reflection in a dihedral group. Prove that $FR^kF = R^{-k}$. Why does this imply that D_n is non-Abelian?

補充. It immediately follows by Exercise 2.43.

2.45 In the dihedral group D_n, let $R = R_{360/n}$ and let F be any reflection. Write each of the following products in the form R^i or R^iF, where $0 \leq i < n$.
a. In D_4, $FR^{-2}FR^5$
b. In D_5, $R^{-3}FR^4FR^{-2}$
c. In D_6, $FR^5FR^{-2}F$

補充.

2.46 Prove that the set of all rational numbers of the form 3^m6^n, where m and n are integers, is a group under multiplication.

提示. 記住 group test 的口訣: 閉結單反。

Proof. Let $S = \{3^m6^n \in \mathbb{Q} \mid m, n \in \mathbb{Z}\}$. We show that S is a group under multiplication.

- **Closed:** For any $3^{m_1}6^{n_1}, 3^{m_2}6^{n_2} \in S$, where $m_1, m_2, n_1, n_2 \in \mathbb{Z}$, since $m_1 + m_2, n_1 + n_2 \in \mathbb{Z}$, we have

$$3^{m_1}6^{n_1} \cdot 3^{m_2}6^{n_2} = 3^{m_1+m_2}6^{n_1+n_2} \in S.$$

- **Associative:** For any $3^{m_1}6^{n_1}, 3^{m_2}6^{n_2}, 3^{m_3}6^{n_3} \in S$, where $m_1, m_2, m_3, n_1, n_2, n_3 \in \mathbb{Z}$,

$$\begin{aligned}(3^{m_1}6^{n_1} \cdot 3^{m_2}6^{n_2}) \cdot 3^{m_3}6^{n_3} &= 3^{m_1+m_2}6^{n_1+n_2} \cdot 3^{m_3}6^{n_3} \\ &= 3^{(m_1+m_2)+m_3}6^{(n_1+n_2)+n_3} \\ &= 3^{m_1+(m_2+m_3)}6^{n_1+(n_2+n_3)} \\ &= 3^{m_1}6^{n_1} \cdot 3^{m_2+m_3}6^{n_2+n_3} \\ &= 3^{m_1}6^{n_1} \cdot (3^{m_2}6^{n_2} \cdot 3^{m_3}6^{n_3})\end{aligned}$$

- **Identity:** Since $0 \in \mathbb{Z}$, we have $1 = 3^0 6^0 \in S$ and 1 is the multiplicative identity in S.
- **Inverse:** For any $3^m 6^n \in S$, where $m, n \in \mathbb{Z}$, since $-m, -n \in \mathbb{Z}$, we have $3^{-m}6^{-n} \in S$ and $3^m 6^n \cdot 3^{-m} 6^{-n} = 1 \in S$. That is, $3^m 6^n$ has a multiplicative inverse in S.

■

補充. 其實也可以視爲 $S \subseteq \mathbb{Q} - \{0\}$, 用subgroup test 就好, 這樣可以少證一個 associative。

2.47* Prove that if G is a group with the property that the square of every element is the identity, then G is abelian.

Proof. For any $a, b \in G$, since $a^2 = b^2 = e$, we have

$$a = a^{-1} \text{ and } b = b^{-1}. \tag{14}$$

$$\begin{aligned} & e = (ab)^2 = abab \\ \overset{\substack{\text{left multiplying } a^{-1} \\ \downarrow}}{\Rightarrow} \quad & a^{-1} = bab \\ \overset{\substack{\text{left multiplying } b^{-1} \\ \downarrow}}{\Rightarrow} \quad & b^{-1}a^{-1} = ab \\ \overset{\substack{(14) \\ \downarrow}}{\Rightarrow} \quad & ba = ab \end{aligned}$$

■

2.49 Prove the assertion made in Example 20 that the set $\{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is prime.

補充. 這我們之前講過了,

$$\gcd(a, n) = 1 \Leftrightarrow ax \equiv 1 \pmod{n} \text{ has a solution} \Leftrightarrow a \text{ has an inverse in } \mathbb{Z}_n.$$

或是說,

$$\begin{aligned} & \gcd(a, n) = 1 \\ \Leftrightarrow \quad & \exists x, y \in \mathbb{Z}, \text{ such that } ax + ny = 1 \\ \Leftrightarrow \quad & 1 = ax + ny = ax \in U(n) \\ \Leftrightarrow \quad & a \text{ has an inverse in } \mathbb{Z}_n. \end{aligned}$$

2.50 In a finite group, show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 5. If the stipulation that the group be finite is omitted, what can you say about the number of nonidentity elements that satisfy the equation $x^5 = e$?

補充. Note that if x_0 is a solutaion of the equation $x^5 = e$, then $x_0, x_0^2, x_0^3, x_0^4, x_0^5$ all are and $x_0^i \neq x_0^j$ for any $i \neq j \in \{1, 2, 3, 4, 5\}$.

2.52 Let $G = \{[\begin{smallmatrix} a & a \\ a & a \end{smallmatrix}] \mid a \in \mathbb{R},\ a \neq 0\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinants. (Compare with Example 10.)

2.53 Suppose that in the definition of a group G, the condition that there exists an element e with the property $ae = ea = a$ for all a in G is replaced by $ae = a$ for all a in G. Show that $ea = a$ for all a in G. (Thus, a one-sided identity is a two-sided identity.)

2.54 Suppose that in the definition of a group G, the condition that for each element a in G there exists an element b in G with the property $ab = ba = e$ is replaced by the condition $ab = e$. Show that $ba = e$. (Thus, a one-sided inverse is a two-sided inverse.)

補充 2.A Let G be a set with an operation $*$ such that:
1. G is closed under $*$.
2. $*$ is associative.
3. There exists an element $e \in G$ such that $e * x = x$ for all $x \in G$.
4. Given $x \in G$, there exists a $y \in G$ such that $y * x = e$.

Prove that G is a group. (Thus you must show that $x * e = x$ and $x * y = e$ for e, y as above.) (Abstract Algebra, Herstein, Section 2.2, Exercise 28)

補充. 這題比上面兩題更強, 所以你可以發現 group axiom 中的某些條件是多餘的, 也就是說可以由其他條件得到。這是比較進階的題目, 有興趣再做就好。

3 Chapter 3

3.1 For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the order of the group?

$$\mathbb{Z}_{12},\quad U(10),\quad U(12),\quad U(20),\quad D_4$$

補充. C.f. p.148, Corollary 2.

3.4 Prove that in any group, an element and its inverse have the same order.

提示. $x^n = e \Leftrightarrow x^{-n} = e$.

Proof. Note that $x^n = e \Leftrightarrow (x^{-1})^n = x^{-n} = (x^n)^{-1} = e$. If $|x| < |x^{-1}|$, since $x^{|x|} = e$, then $(x^{-1})^{|x|} = e$, a contradiction. ■

補充. 簡單來說, 這題就是 $|x| = |x^{-1}|$, 這個定理很重要, 直觀來看, 如果 $|x| \geq 2$, 那麼 x 跟 x^{-1} 就是成雙成對的。這題的應用包括Exercise 2.20, 2.37, 3.5, 3.59。

3.5 Without actually computing the orders, explain why the two elements in each of the following pairs of elements from $\mathbb{Z}_{30}$ must have the same order: $\{2, 28\}$, $\{8, 22\}$. Do the same for the following pairs of elements from $U(15)$: $\{2, 8\}$, $\{7, 13\}$.

3.6 In the group $\mathbb{Z}_{12}$, find $|a|, |b|$, and $|a+b|$ for each case.
a. $a = 6, b = 2$
b. $a = 3, b = 8$
c. $a = 5, b = 4$
Do you see any relationship between $|a|, |b|$, and $|a+b|$?

3.8 What can you say about a subgroup of D_3 that contains R_{240} and a reflection F? What can you say about a subgroup of D_3 that contains two reflections?

3.9 What can you say about a subgroup of D_4 that contains R_{270} and a reflection? What can you say about a subgroup of D_4 that contains H and D? What can you say about a subgroup of D_4 that contains H and V?

3.10 How many subgroups of order 4 does D_4 have?

提示. 如果一個 group G 的 order 是 4, 那麼他必定是由一個 order 是 4 的 element 所生成, 例如 $\mathbb{Z}_4$; 或是由 3 個 order 2 的元素及一個 order 1 的元素 (identity) 構成, 其中任兩個 order 爲 2 的元素相乘 (或相加) 會等於第三個 order 爲 2 的元素, 例如 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$。

3.11 Determine all elements of finite order in $\mathbb{R}^*$, the group of nonzero real numbers under multiplication.

Proof. ± 1. ■

3.12 If a and b are group elements and $ab \neq ba$, prove that $aba \neq e$.

補充. $aba = e \Rightarrow ba \overset{\text{left}}{\overset{\downarrow}{=}} a^{-1} \overset{\text{right}}{\overset{\downarrow}{=}} ab$

3.13 Suppose that H is a nonempty subset of a group G that is closed under the group operation and has the property that if a is not in H then a^{-1} is not in H. Is H a subgroup?

3.14 Let G be the group of polynomials under addition with coefficients from $\mathbb{Z}_{10}$. Find the orders of $f(x) = 7x^5+5x+4$, $g(x) = 4x^2+8x+6$, and $f(x)+g(x) = x^2+3x$. If $h(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ belongs to G, determine $|h(x)|$ given that $\gcd(a_1, a_2, \ldots, a_n) = 1$; $\gcd(a_1, a_2, \ldots, a_n) = 2$; $\gcd(a_1, a_2, \ldots, a_n) = 5$; and $\gcd(a_1, a_2, \ldots, a_n) = 10$.

Proof.

$$\begin{array}{rcl} |f(x)| & = & 10, \\ |g(x)| & = & 5, \\ |f(x)+g(x)| & = & 10. \end{array}$$

$$|h(x)| = \begin{cases} 5 & \text{if } \gcd(a_1, a_2, \ldots, a_n) = 2, \\ 2 & \text{if } \gcd(a_1, a_2, \ldots, a_n) = 5, \\ 1 & \text{if } \gcd(a_1, a_2, \ldots, a_n) = 10. \end{cases}$$

■

3.15 If a is an element of a group G and $|a| = 7$, show that a is the cube of some element of G.

補充. $a^7 = 1, b^3 = a$, consider in $\langle a \rangle$. $|a| = 7, b = a^r, a^7 = 1, (a^7)^r = a^{7r} = 1 \Rightarrow a^{7r+1} = a \Rightarrow 3 \mid (7r+1) \Rightarrow r = 2$

3.16 Suppose that H is a nonempty subset of a group G with the property that if a and b belongs to H then $a^{-1}b^{-1}$ belongs to H. Prove or disprove that this is enough to guarantee that H is a subgroup of G.

3.17 Prove that if an Abelian group has more than three elements of order 2, then it has at least 7 elements of order 2. Find an example that shows this is not true for non-Abelian groups.

3.18* Suppose that a is a group element and $a^6 = e$. What are the possibilities for $|a|$? Provide reasons for your answer.

提示. Division Algorithm.

Proof. By division algorithm,

$$6 = |a| \cdot q + r \quad \text{for some } q, r \in \mathbb{Z}, \quad \text{where} \quad 0 \le r < |a|.$$

If $r \neq 0$, then $0 < r < |a|$ and

$$e = a^6 = a^{|a| \cdot q + r} = (a^{|a|})^q \cdot a^r = a^r,$$

a contradiction. Thus, $r = 0$ and $|a|$ divide 6. That is, $|a| \in \{1, 2, 3, 6\}$. ■

3.19 If a is a group element and a has infinite order, prove that $a^m \neq a^n$ when $m \neq n$.

3.20 Let x belong to a group. If $x^2 \neq e$ and $x^6 = e$, prove that $x^4 \neq e$ and $x^5 \neq e$. What can we say about the order of x?

Proof. It immediately follows by Problem 3, $|x| = 3$ or 6. ■

3.21 Show that if a is an element of a group G, then $|a| \le |G|$.

3.23 Show that $U(20) \neq \langle k \rangle$ for any k in $U(20)$. [Hence, $U(20)$ is not cyclic.]

3.24 Suppose n is an even positive integer and H is a subgroup of $\mathbb{Z}_n$. Prove that either every member of H is even or exactly half of the members of H are even.

補充. $2 \in H, 2 \in H$

3.25 Prove that for every subgroup of D_n, either every member of the subgroup is a rotation or exactly half of the members are rotations.

3.26 Prove that a group with two elements of order 2 that commute must have a subgroup of order 4.

3.27 For every even integer n, show that D_n has a subgroup of order 4.

補充. $\{1, a^{n/2}, b, ba^{n/2}\}$.

3.28 Suppose that H is a proper subgroup of Z under addition and H contains $18, 30$, and 40. Determine H.

Proof. $\langle \gcd(18, 30, 40) \rangle = \langle 2 \rangle$. ■

3.29 Suppose that H is a proper subgroup of Z under addition and that H contains $12, 30$, and 54. What are the possibilities for H?

補充. 線性代數中的 span

3.30 Prove that the dihedral group of order 6 does not have a subgroup of order 4.

補充. There is no element in D_3 which is of order 4. Hence if there is a subgroup H of D_3 which is of order 4, then H must be a Klein four group. The elements in D_3 which is of order 2 are b, ba, ba^2. But $\{1, b, ba, ba^2\}$ is not a subgroup of D_3.

C.f. p.148, Corollary 2.

補充. 學完 Lagrange's Theorem, 這題就很簡單了。

3.31 For each divisor $k > 1$ of n, let $U_k(n) = \{x \in U(n) \mid x \mod k = 1\}$. [For example, $U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and $U_7(21) = \{1, 8\}$.] List the elements of $U_4(20), U_5(29), U_5(30)$, and $U_{10}(30)$. Prove that $U_k(n)$ is a subgroup of $U(n)$. Let $H = \{x \in U(10) \mid x \mod 3 = 1\}$. Is H a subgroup of $U(10)$? (This exercise is referred to in Chapter 8.)

Proof.

$$\begin{aligned} U_4(20) &= \{1, 9, 13, 17\}, \\ U_5(20) &= \{1, 11\}, \\ U_5(30) &= \{1, 11\}, \\ U_{10}(30) &= \{1, 11\}. \end{aligned}$$

We show that $U_k(n)$ is a subgoup of $U(n)$.

- **Closed:**

$$\begin{aligned} & a, b \in U_k(n) \\ \Rightarrow\ & a \equiv 1 \pmod{k},\ b \equiv 1 \pmod{k} \\ \Rightarrow\ & ab \equiv 1 \cdot 1 = 1 \pmod{k} \\ \Rightarrow\ & ab \in U_k(n). \end{aligned}$$

- **Identity:**

$$1 \mod k = 1 \Rightarrow 1_{U(n)} \in U_k(n).$$

- **Inverse*:**

$$a \in U_k(n) \subseteq U(n) \Rightarrow \exists a^{-1} \in U(n) \Rightarrow \gcd(a^{-1}, n) = 1 \overset{\overset{k|n}{\downarrow}}{\Rightarrow} \gcd(a^{-1}, k) = 1 \Rightarrow a^{-1} \in U_k(n).$$

H is not a subgroup of $U(10)$ because $H = \{1, 7\}$ and $7 \cdot 7 = 49 = 9 \notin H$. ■

3.32 If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroup of G, finite or infinite, is again a subgroup of G?)

提示. 記住 subgroup test 的口訣: 閉單反

Proof.

- **Closed:**

$$x, y \in H \cap K \Rightarrow x, y \in H, x, y \in K \overset{H,K\leq G}{\overset{\downarrow}{\Rightarrow}} xy \in H, xy \in K \Rightarrow xy \in H \cap K.$$

- **Identity:**

$$H, K \leq G \Rightarrow e_G \in H, e_G \in K \Rightarrow e_G \in H \cap K.$$

- **Inverse:**

$$x \in H \cap K \Rightarrow x \in H, x \in K \overset{H,K\leq G}{\overset{\downarrow}{\Rightarrow}} x^{-1} \in H, x^{-1} \in K \Rightarrow x^{-1} \in H \cap K.$$

■

3.33 Show that $Z(G) = \cap_{a\in G} C_G(a)$. [This means the intersection of all subgroups of the form $C_G(a)$.]

Proof.

$$\begin{aligned} & g \in Z(G) \\ \Leftrightarrow\ & ga = ag \text{ for all } a \in G \\ \Leftrightarrow\ & g \in \cap_{a\in G} C_G(a). \end{aligned}$$

■

3.34 Let G be a group, and let $a \in G$. Prove that $C(a) = C(a^{-1})$.

Proof.

$$\begin{aligned} & b \in C_G(a) \\ \Leftrightarrow\ & ba = ab \\ \Leftrightarrow\ & a^{-1}(ba) = a^{-1}(ab) \\ \Leftrightarrow\ & a^{-1}(ba) = b \\ \Leftrightarrow\ & a^{-1}(ba)a^{-1} = ba^{-1} \\ \Leftrightarrow\ & a^{-1}b = ba^{-1} \\ \Leftrightarrow\ & b \in C_G(a^{-1}). \end{aligned}$$

■

補充. If $g \in C(a)$, then $ga^{-1} = (ag^{-1})^{-1} \overset{g^{-1}\in C(a)}{\overset{\downarrow}{=}} (g^{-1}a)^{-1} = a^{-1}g$ and $g \in C(a^{-1})$

3.36 Complete the partial Cayley group table given below.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1			
6	6	5	7	8		1		
7	7	8	5	6			1	
8	8	7	6	5				1

補充. $6 = 5 \cdot 2, 5 \cdot 6 = 5 \cdot 5 \cdot 2$.

3.37 Suppose G is the group defined by the following Cayley table.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	8	7	6	5	4	3
3	3	4	5	6	7	8	1	2
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	4	3	2	1	8	7
7	7	8	1	2	3	4	5	6
8	8	7	6	5	4	3	2	1

a. Find the centralizer of each member of G.
b. Find $Z(G)$.
c. Find the order of each element of G. How are these orders arithmetically related to the order of the group?

補充. $C(a), Z(G)$ 在 Cayley Table 上如何表現?

3.38 If a and b are distinct group elements, prove that either $a^2 \neq b^2$ or $a^3 \neq b^3$.

補充. 這裡教各位一個很常用的證明技巧, 當你要證明

$$A \Rightarrow (B \text{ or } C)$$

時, 可以證明

$$A \text{ and } (\sim B) \Rightarrow C.$$

在這題就是證明

$$a \neq b, a^2 = b^2 \Rightarrow a^3 \neq b^3.$$

3.40 In the group $\mathbb{Z}$, find
a. $\langle 8, 14 \rangle$;
b. $\langle 8, 13 \rangle$;
c. $\langle 6, 15 \rangle$;
d. $\langle m, n \rangle$;
e. $\langle 12, 18, 45 \rangle$;
In each part, find an integer k such that the subgroup is $\langle k \rangle$.

3.41 For each a in a group G, the centralizer of a is a subgroup of G.

Proof. Since $ea = a = ae$, we get $e \in C_G(a)$.
If $b, c \in C_G(a)$, then

$$(bc)a = b(ca) \overset{c \in C_G(a)}{\overset{\downarrow}{=}} b(ac) = (ba)c \overset{c \in C_G(a)}{\overset{\downarrow}{=}} (ab)c = a(bc).$$

Hecnce, $bc \in C_G(a)$.
If $b \in C_G(a)$, then

$$\begin{aligned} & ab = ba \\ \overset{\text{right multiplying } b^{-1}}{\overset{\downarrow}{\Rightarrow}} \quad & (ab)b^{-1} = (ba)b^{-1} \\ \Rightarrow \quad & ae = a = bab^{-1} \\ \overset{\text{left multiplying } b^{-1}}{\overset{\downarrow}{\Rightarrow}} \quad & b^{-1}a = ab^{-1} \\ \Rightarrow \quad & b^{-1} \in C_G(a). \end{aligned}$$

■

3.42 If H is a subgroup of G, then by the centralizer $C(H)$ of H we mean the set $\{x \in G \mid xh = hx \text{ for all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

Proof.

- **Closed:**

$$\begin{aligned} & x, y \in C(H) \\ \Rightarrow \quad & \forall h \in H, (xy)h = x(yh) \overset{y \in C(H)}{\overset{\downarrow}{=}} x(hy) = (xh)y \overset{x \in C(H)}{\overset{\downarrow}{=}} (hx)y = h(xy) \\ \Rightarrow \quad & xy \in C(H). \end{aligned}$$

- **Identity:**

$$\forall h \in H, e_G h = h = he_G \Rightarrow e_G \in C(H).$$

- **Inverse*:**

$$x \in C(H) \overset{H \leq G, \forall h \in H, h^{-1} \in H}{\overset{\downarrow}{\Rightarrow}} x^{-1}h = (h^{-1}x)^{-1} \overset{x \in C(H)}{\overset{\downarrow}{=}} (xh^{-1})^{-1} = hx^{-1} \Rightarrow x^{-1} \in C(H).$$

■

3.43 Must the centralizer of an element of a group be Abelian?

3.44 Must the center of a group be Abelian?

3.45 Let G be an abelian group with identity e and let n be some fixed integer. Prove that the set of all elements of G that satisfy the equation $x^n = e$ is a subgroup of G. Give an example of a group G in which the set of all elements of G that satisfy the equation $x^2 = e$ does not form a subgroup of G.

Proof. Let $S = \{x \in G \mid x^n = e\}$. We claim that S is a subgroup of G.

- **Closed:**

$$a, b \in S \Rightarrow a^n = e = b^n \Rightarrow (ab)^n \overset{\overset{G\text{ abelian}}{\downarrow}}{=} a^n b^n = ee = e \Rightarrow ab \in S.$$

- **Identity:**

$$e_G^n = e \Rightarrow e_G \in S.$$

- **Inverse*:**

$$a \in S \Rightarrow (a^{-1})^n = (a^n)^{-1} = e^{-1} = e \Rightarrow a^{-1} \in S.$$

In the case $G = D_3 = \{\langle a, b\rangle \mid |a| = 3, |b| = 2, ab = ba^{-1}\}$, $S = \{x \in G \mid x^2 = e\} = \{e, b, ba, ba^2\}$. S is not a subgroup of G because $b \cdot ba = a \notin S$. ■

3.46 Suppose a belongs to a group and $|a| = 5$. Prove that $C(a) = C(a^3)$. Find an element a from some group such that $|a| = 6$ and $C(a) \neq C(a^3)$.

補充. See p.67, Example 14.

3.47 Let G be the set of all polynomials with coefficients from the set $\{0, 1, 2, 3\}$. We can make G a group under addition by adding the polynomials in the usual way, except that we use modulo 4 to combine the coefficients. With this group operation, determine the orders of the elements of G. Determine a necessary and sufficient condition for an element of G to have order 2.

3.48 In each case, find elements a and b from a group such that $|a| = |b| = 2$.
a. $|ab| = 3$ b. $|ab| = 4$ c. $|ab| = 5$

3.49 Suppose a group contains elements a and b such that $|a| = 4$, $|b| = 2$, and $a^3 b = ba$. Find $|ab|$.

3.50* Suppose a and b are group elements such that $|a| = 2$, $b \neq e$, and $aba = b^2$. Determine $|b|$.

Proof. We show that $b^2 \neq e$.

$$\begin{aligned}
& \text{If } b^2 = e \\
\Rightarrow\quad & aba = b^2 = e \\
\overset{\overset{\text{left multiplying } a}{\downarrow}}{\Rightarrow}\quad & aaba = a \\
\overset{\overset{\text{right multiplying } a}{\downarrow}}{\Rightarrow}\quad & aabaa = aa \\
\overset{\overset{aa=e}{\downarrow}}{\Rightarrow}\quad & b = e, \text{ a contradiction.}
\end{aligned}$$

蔡○諭, 沈○慧的解法:

$$
\begin{aligned}
b^4 &= (b^2)(b^2) \\
&= (aba)(aba) \\
&= ab(aa)ba \\
&\overset{aa=e}{\overset{\downarrow}{=}} ab^2a \\
&\overset{aba=b^2}{\overset{\downarrow}{=}} a(aba)a \\
&= (aa)b(aa) \\
&\overset{aa=e}{\overset{\downarrow}{=}} b.
\end{aligned}
$$

Therefore, $b^4 = b$ and $b^3 = e$ and $|b| = 3$.

袁○隆的解法:

$$
\begin{aligned}
& && aba = b^2 \\
&\overset{\text{left multiplying } a}{\overset{\downarrow}{\Rightarrow}} && aaba = ab^2 \\
&\overset{\text{right multiplying } a}{\overset{\downarrow}{\Rightarrow}} && aabaa = ab^2a \\
&\overset{aa=e}{\overset{\downarrow}{\Rightarrow}} && b = ab^2a \\
&\Rightarrow && b^2 = (ab^2a)^2 = (ab^2a)(ab^2a) = ab^2(aa)b^2a \overset{aa=e}{\overset{\downarrow}{=}} ab^4a \\
&\Rightarrow && aba = b^2 = ab^4a \\
&\overset{\text{left multiplying } a}{\overset{\downarrow}{\Rightarrow}} && aaba = aab^4a \\
&\overset{\text{right multiplying } a}{\overset{\downarrow}{\Rightarrow}} && aabaa = aab^4aa \\
&\overset{aa=e}{\overset{\downarrow}{\Rightarrow}} && b = b^4.
\end{aligned}
$$

Therefore, $b^4 = b$ and $b^3 = e$ and $|b| = 3$.

■

3.51 Let a be a group element of order n, and suppose that d is a positive divisor of n. Prove that $|a^d| = n/d$.

補充. 建議你直接背 p.80, thm.4.2的公式: If $|a| = n$, then $|a^r| = \frac{n}{\gcd(r,d)}$, 這是更強的版本, 不用要求 $r \mid n$。證明也很簡單, 類似國小的兩個人跑操場, 不同起點, 同時抵達終點的問題。

下面是助教我以前大學時記下這個公式的方法, 注意到 r 跟 n 分別都有一個在上一個在下。

$$|g^r| = \frac{r}{\gcd(r,n)}$$

3.52 Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2,\mathbb{R})$. Find $|A|, |B|$, and $|AB|$. Does your answer surprise you?

Proof. $|A| = 4$, $|B| = 3$, $|AB| = \infty$. ∎

3.53 Consider the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $SL(2,\mathbb{R})$. What is the order of A? If we view $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ as a member of $SL(2,\mathbb{Z}_p)$ (p is a prime), what is the order of A?

Proof.

$$|A| = \begin{cases} \infty & \text{if } A \in SL(2,\mathbb{R}), \\ p & \text{if } A \in SL(2,\mathbb{Z}_p). \end{cases}$$

∎

3.54 For any positive integer n and any angle θ, show that in the group $SL(2,\mathbb{R})$,

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}.$$

Use this formula to find the order of

$$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix} \text{ and } \begin{bmatrix} \cos \sqrt{2}^\circ & -\sin \sqrt{2}^\circ \\ \sin \sqrt{2}^\circ & \cos \sqrt{2}^\circ \end{bmatrix}.$$

(Geometricall, $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ represents a rotation of the plane θ degree.)

3.56 Let x belong to a group and $|x| = 6$. Find $|x^2|, |x^3|, |x^4|$, and $|x^5|$. Let y belong to a group and $|y| = 9$. Find $|y^i|$ for $i = 2, 3, ..., 8$. Do these examples suggest and relationship between the order of the power of an element and the order of the element?

補充. 事實上, 我們有

$$|a^r| = \frac{n}{\gcd(n,r)}.$$

這蠻難證的, 有興趣的同學可以挑戰看看。

3.57 D_4 has seven cyclic subgroups. List them.

3.58 $U(15)$ has six cyclic subgroups. List them.

Proof.

$$\begin{aligned} \langle 1 \rangle &= \{1\}, \\ \langle 2 \rangle &= \{1, 2, 4, 8\}, \\ \langle 4 \rangle &= \{1, 4\}, \\ \langle 7 \rangle &= \{1, 7, 7^2 = 4, 7^3 = 13\}, \\ \langle 11 \rangle &= \{1, 11\}, \\ \langle 14 \rangle &= \{1, 14\}. \end{aligned}$$

∎

3.59* Prove that a group of even order must have an element of order 2.

Proof. Consider the set $S = \{x \in G \mid x^2 = e\}$. Since $|x| = |x^{-1}|$, if $|x| \geq 3$, then x and x^{-1} are two distinct elements that they have the same order. Thus, there are even number of elements in $G \backslash S$ and the number of elements in S are even. Since $e \in S$, there is an element $x_0 \in S$ such that $x_0 \neq e$ and $x_0^2 = e$.

胡○瑋的解法: Define a relation "$\sim$" on the group G of even order by

$$a \sim b \Leftrightarrow a = b \text{ or } a = b^{-1}.$$

Then show that "$\sim$" is an equivalence relation. In addition, show that the number of elements in each equivalence class is either 1 or 2 and the equivalence class which contains the identity is $\{e\}$.

其他 idea(未證明): Let $G = \{g_1, g_2, ..., g_n\}$ be a group, where n is an even number. Let Perm G be the set of all permutation on the set G. Show that the mapping $\sigma : G \to G$ defined by $\sigma(g) = g^{-1}$ is a permutation. That is, $\sigma \in \text{Perm } G$.

Define a mapping $\theta : \text{Perm } G \to S_n$.

$$\begin{array}{rl} \text{If } \tau \in \text{Perm } G \text{ and} & \tau(g_i) = g_j, \\ \text{then} & \theta(\tau)(i) = j. \end{array}$$

Show that θ is well-define and $\theta(\sigma)$ is a product of disjoint tranpositions.

If $g_1 = e$, then $\theta(\sigma)(1) = 1$. Since n is even and $\theta(\sigma)$ is a product of disjoint tranpositions, there must exists $j \neq 1$ such that $\theta(\sigma)(j) = j$. That is, $\sigma(g_j) = g_j$ and $g_j^{-1} = g_j$ and $|g_j| = 2$. ■

Proof. Note that

$$x^2 \neq e \Leftrightarrow x \neq x^{-1}.$$

Let $S = \{x \in G \mid x^2 \neq e\}$. Pick $x_1 \neq e \in S$. Then $x_1 \neq x_1^{-1}$ and $x_1^{-1} \in S$ (why?[1]). Remove these two elements x_1 and x_1^{-1} from S. Pick x_2 from the remaining elements, do the same process as above. We can always remove two elements because $x_i^{-1} \neq x_j^{-1} \in S$ if $i \neq j$. Since G is finite, we can't do the process infinitely. Finally, there is no element remain in S. Thus, $S = \{x_1, x_1^{-1}, x_2, x_2^{-1}, , , , , x_n, x_n^{-1}\}$ and $\#S$ is even. Since $|G|$ is even, we get $\#(G - S)$ is even and there exists $g \neq e \in G - S$ and $|g| = 2$. ■

補充.

- 這題跟2.20有什麼關係?
- 之後學到 group action 會知道這題只是 Cauchy's Theorem 的一個特例。

3.60 Suppose G is a group that has exactly eight elements of order 3. How many subgroups of order 3 does G have?

[1] 可以直接證也可以用 $|x| = |x^{-1}|$。

Proof. Suppose that a_1 is an element of order 3 in G. Then $|a_1^2| = 3$ and $a_1^2 \neq a_1$. By a similar argument, $\{a_1, a_1^2, a_2, a_2^2, a_3, a_3^2, a_4, a_4^2\}$ are all the eight elements of order 3. There are 4 subgroups of order 3. They are

$$\begin{aligned} H_1 &= \{e, a_1, a_1^2\}, \\ H_2 &= \{e, a_2, a_2^2\}, \\ H_3 &= \{e, a_3, a_3^2\}, \\ H_4 &= \{e, a_4, a_4^2\}. \end{aligned}$$

■

3.61 Let H be a subgroup of a finite group G. Suppose that g belongs to G and n is the smallest positive integer such that $g^n \in H$. Prove that n divides $|g|$.

補充. By Division Algorithm, suppose that $|g| = n \cdot q + r$ for some integer q and $0 \leq r < n$. If $r \neq 0$, then $e = g^{|g|} = g^{n \cdot q + r} = (g^n)^q \cdot g^r$ and $g^r = (g^n)^{-q} \in H$. Contrary to the minimality of n. Therefore, $r = 0$ and n divides $|g|$.

3.62 Compute the orders of the following groups.
a. $U(3), U(4), U(12)$
b. $U(5), U(7), U(35)$
c. $U(4), U(5), U(20)$
d. $U(3), U(5), U(15)$
On the basis of your answers, make a conjecture about the relationship among $|U(r)|, |U(s)|$, and $|U(rs)|$.

補充. 這個以後再講, 在這裡先算就好, 要證明的話要用到一些進階的工具。

3.63 Let $\mathbb{R}^*$ be the group of nonzero real numbers under multiplication and let $H = \{x \in \mathbb{R}^* \mid x^2 \text{ is rational}\}$. Prove that H is a subgroup of $\mathbb{R}^*$. Can the exponent of 2 be replaced by any positive integer and still have H be a subgroup?

3.64 Compute $|U(4)|, |U(10)|$, and $|U(40)|$. Do these groups provide a counterexample to your answer to Exercise 62? If so, revise your conjecture.

3.65 Find a cyclic subgroup of order 4 in $U(40)$.

3.66 Find a noncyclic subgroup of order 4 in $U(40)$.

補充. $\{1, 9, 11, 19\}$.

3.70 Let G be a group of functions from $\mathbb{R}$ to $\mathbb{R}^*$, where the operation of G is multiplication of functions. Let $H = \{f \in G \mid f(2) = 1\}$. Prove that H is a subgroup of G. Can 2 be replaced by any real number?

Proof.

- **Closed:**

$$x, y \in H \Rightarrow (xy)(2) = x(2) \cdot y(2) \overset{\substack{x,y \in H \\ \downarrow}}{=} 1 \cdot 1 = 1 \Rightarrow xy \in H.$$

- **Identity:**

$$1_G(2) = 1 \Rightarrow 1_G \in H.$$

- **Inverse:**

$$x \in H \Rightarrow x^{-1}(2) \overset{\overset{x(2)>0}{\downarrow}}{=} [x(2)]^{-1} = 1^{-1} = 1 \Rightarrow x^{-1} \in H.$$

■

3.71 Let $G = GL(2,\mathbb{R})$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a \text{ and } b \text{ are nonzero integers} \right\}$ under the operation of matrix multiplication. Prove or disprove that H is a subgroup of $GL(2,\mathbb{R})$.

Proof.

- **Closed:**

$$\begin{aligned} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in H \quad &\Rightarrow \quad a,b,c,d \text{ all are not } 0 \\ &\Rightarrow \quad ac \neq 0, bd \neq 0 \\ &\Rightarrow \quad \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in H. \end{aligned}$$

- **Identity:**

$$1 \neq 0 \Rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e_G \in H.$$

- **Inverse:**

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in H \Rightarrow a \neq 0, b \neq 0 \Rightarrow \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix} \in H.$$

■

3.73 Let $H = \{a + bi \mid a,b \in \mathbb{R}, a^2 + b^2 = 1\}$. Prove or disprove that H is a subgroup of $\mathbb{C}^*$ under multiplication. Describe the elements of H geometrically.

Proof.

- **Closed:**

$$\begin{aligned} a + bi, c + di \in H \quad &\Rightarrow \quad a^2 + b^2 = 1 = c^2 + d^2 \\ &\Rightarrow \quad (a^2 + b^2)(c^2 + d^2) = a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 = 1 \cdot 1 = 1 \\ &\Rightarrow \quad (ac - bd)^2 + (bc + ad)^2 = 1 \\ &\Rightarrow \quad (a + bi)(c + di) = (ac - bd) + (bc + ad)i \in H. \end{aligned}$$

- **Identity:**

$$1 = 1 + 0i,\ 1^2 + 0^2 = 1 \Rightarrow 1 \in H.$$

- **Inverse:**

$$\begin{aligned} a+bi \in H &\Rightarrow a^2+b^2=1 \\ &\Rightarrow \left(\frac{a}{a^2+b^2}\right)^2 + \left(\frac{-b}{a^2+b^2}\right)^2 = 1 \\ &\Rightarrow (a+bi)^{-1} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} \in H. \end{aligned}$$

The geometric interpretation of H is the unit circle in the complex plane. ■

類似 3.73 Let $H = \{a+bi \mid a,b \in \mathbb{R}, a^2+b^2=1\}$. Prove or disprove that H is a subgroup of $\mathbb{C}^*$ under multiplication. Describe the elements of H geometrically.

Proof. Since $1 = 1+0i$ and $1^2+0^2=1$, we get $1 \in H$.

If $a+bi, c+di \in H$, then $a^2+b^2 = 1 = c^2+d^2$ and

$$(a^2+b^2)(c^2+d^2) = a^2c^2+b^2c^2+a^2d^2+b^2d^2 = 1 \cdot 1 = 1.$$

Therefore, $(ac-bd)^2+(bc+ad)^2=1$ and

$$(a+bi)(c+di) = (ac-bd)+(bc+ad)i \in H.$$

■

3.74 Let G be a finite Abelian group and let a and b belong to G. Prove that the set $\langle a,b\rangle = \{a^ib^j \mid i,j \in \mathbb{Z}\}$ is a subgroup of G. What can you say about $|\langle a,b\rangle|$ in terms of $|a|$ and $|b|$?

3.77 Let a belong to a group and $|a|=m$. If n is relatively prime to m, show that a can be written as the nth power of some element in the group.

補充. $a = a^1 = a^{\gcd(m,n)} = a^{mx+ny} = (a^m)^x + (a^y)^n = (a^y)^n$.

Compare to Section 4, Exercise 73.

3.78 Let F be a reflection in the dihedral group D_n and R a rotation in D_n. Determine $C(F)$ when n is odd. Determine $C(F)$ when n is even. Determine $C(R)$.

3.79 Let $G = GL(2,\mathbb{R})$.

a. Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

b. Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

c. Find $Z(G)$.

Proof. Let

$$B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

$$\begin{aligned} C_G(B) &= \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}, ad-bc \neq 0\right\} \\ &= \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R} \mid b=c, a=d, ad-bc \neq 0\right\} \\ &= \left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} \in GL(2,\mathbb{R}) \mid a^2-b^2 \neq 0\right\} \end{aligned}$$

Let

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

By a similar argument,

$$C_G(A) = \left\{\begin{bmatrix} a & b \\ b & a-b \end{bmatrix} \in GL(2,\mathbb{R}) \mid a^2-ab-b^2 \neq 0\right\}$$

Therefore,

$$\begin{aligned} Z(G) &\subseteq C_G(A) \cap C_G(B) \\ &= \left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in GL(2,\mathbb{R}) \mid a^2 \neq 0\right\} \\ &= S. \end{aligned}$$

It is easy to show that $S \subseteq Z(G)$. Hence, $Z(G) = S$. ■

補充. See Exercise 33. $Z(G) \subseteq C(a) \cap C(b)$.

3.80 Let G be a finite group with more than one element. Show that G has an element of prime order.

補充. Show that $|a| < \infty$. Suppose $|a| = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$. Then consider $a^{p_1^{r_1-1} \cdot p_2^{r_2} \cdots p_n^{r_n}}$.

補充 3.A Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

(a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).

Proof. For any $z_1, z_2 \in G$, suppose that $z_1^{n_1} = z_2^{n_2} = 1$ for some $n_1, n_2 \in \mathbb{Z}^+$. Then $(z_1 z_2)^{n_1 n_2} = (z_1^{n_1})^{n_2}(z_2^{n_2})^{n_1} = 1 \cdot 1 = 1$. That is, $z_1 z_2 \in G$. Obviously, $1^1 = 1$ so $1 \in G$. In addition, $\left(\frac{1}{z_1}\right)^{n_1} = \frac{1}{z_1^{n_1}} = 1$. Thus, $z_1^{-1} \in G$. The associative of the multiplication on G inherited from the multiplication on $\mathbb{C}$. Therefore, G is a group under multiplcation. ■

(b) Prove that G is not a gorup under addition.

Proof. Note that $1 \in G$ but $1 + 1 = 2$ is not in G because $2^n \neq 1$ for any $n \in \mathbb{Z}^+$. Hence, G is not closed under addition. ■

4 Chapter 4

4.4 List the elements of the subgroups $\langle 3\rangle$ and $\langle 15\rangle$ in Z_{18}. Let a be a group element of order 18. List the elements of the subgroups $\langle a^3\rangle$ and $\langle a^{15}\rangle$.

Proof. By Exercise 4.11,

$$\langle 3\rangle = \langle -3\rangle = \langle 15\rangle = \{0,3,6,9,12,15\}.$$

$$\langle a^3\rangle = \langle a^{-3}\rangle = \langle a^{15}\rangle = \{1,a^3,a^6,a^9,a^{12},a^{15}\}.$$

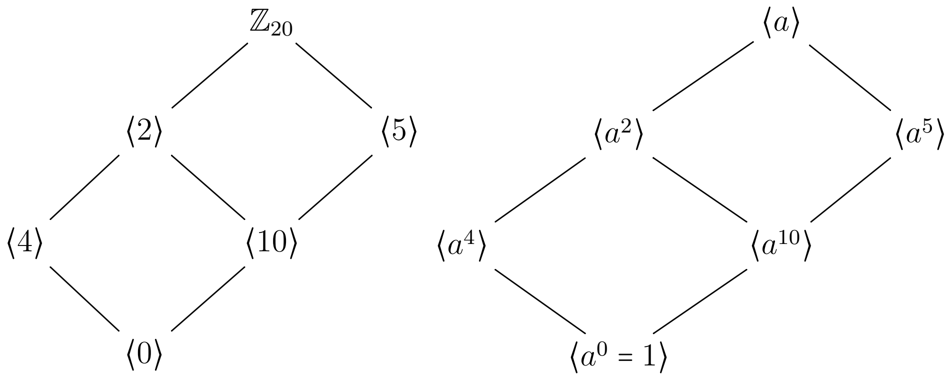
■

4.5 List the elements of the subgroups $\langle 3\rangle$ and $\langle 7\rangle$ in $U(20)$.

Proof. $\langle 3\rangle = \langle 7\rangle = \{1,3,9,7\}$. ■

4.9 How many subgroups does $\mathbb{Z}_{20}$ have? List a generator for each of these subgroups. Suppose that $G = \langle a\rangle$ and $|a| = 20$. How many subgroups does G have? List a generator for each of these subgroups.

Proof.



■

4.10 Let $G = \langle a\rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.

Proof. By the formula of the order of the element in a finite cyclic group, we know that $|a^m| = \frac{24}{\gcd(m,24)}$. It is sufficient to find m such that $\gcd(m,24) = 3$. Then $|\langle a^m\rangle| = \frac{24}{\gcd(m,24)} = 8$. By some computation, $m \in \{3,9,15,21\}$. That is, the generators for the subgroup of order 8 are a^3, a^9, a^{15} and a^{21}. ■

4.11 Let G be a group and let $a \in G$. Prove that $\langle a^{-1}\rangle = \langle a\rangle$.

4.13 In $\mathbb{Z}_{24}$ find a generator for $\langle 21\rangle \cap \langle 10\rangle$. Suppose that $|a| = 24$. Find a generator for $\langle a^{21}\rangle \cap \langle a^{10}\rangle$. In general, what is a generator for the subgroup $\langle a^m\rangle \cap \langle a^n\rangle$?

Proof. 你當然可以直接算 $\langle 21\rangle$ 跟 $\langle 10\rangle$, 但這裡我教你一些技巧。

- $\langle 21\rangle = \langle -3\rangle \overset{\text{Exercise 4.11}}{\overset{\downarrow}{=}} \langle 3\rangle = \{0,3,6,9,12,15,18,21\}$.
- Since $|\langle 10\rangle| = |10| \overset{\text{p.80, thm.4.2}}{\overset{\downarrow}{=}} \frac{24}{\gcd(10,24)} = 12$, by the Fundamental Theorem of Cyclic Groups, there is only one subgroup of order 12. Thus,

$$\langle 10\rangle = \langle 2\rangle = \{0,2,4,6,8,10,12,14,16,18,20,22\}.$$

- Then $\langle 21\rangle \cap \langle 10\rangle = \langle 3\rangle \cap \langle 2\rangle = \langle 6\rangle$.

Similarly,

$$\langle a^{21}\rangle \cap \langle a^{10}\rangle = \langle a^{3}\rangle \cap \langle a^{2}\rangle = \langle a^{6}\rangle.$$

In general, $\langle a^m\rangle \cap \langle a^n\rangle = \langle a^r\rangle$, where $r = \text{l.c.m.}(\underline{\gcd(m,24)}, \underline{\gcd(n,24)})$. ■

補充. 解答有誤。

4.14 Suppose that a cyclic group G has exactly three subgroups: G itself, $\{e\}$, and a subgroup of order 7. What is $|G|$? What can you say if 7 is replaced with p where p is a prime?

提示. Fundamental Theorem of Cyclic Groups.

Proof. By the Fundamental Theorem of Cyclic Groups, $G = \mathbb{Z}_{49}$. $\mathbb{Z}_{49}$ has exactly three subgroup: $\mathbb{Z}_{49}, \langle 7\rangle$ and $\{0\}$. $|G| = 49$. If 7 is replaced with a prime p, then $G = \mathbb{Z}_{p^2}$. ■

Proof. 這題如果要嚴謹證明的話, 要用到一些還沒教過的觀念。

- At first, we need to prove that $|G|$ is finite. See Hungerford, p.37, exe.I.4.8.
- Recall that the Fundamental Theorem of Cyclic Groups states that: If G is a cyclic group of finite order, then the order of every subgroup of G divides $|G|$ and for each divisor k of $|G|$, there is only one subgroup H of G such that $|H| = k$.
- If G has exactly three subgroups G, H and $\{0\}$, where $|H| = 7$, then by the Fundamental Theorem of Cyclic Groups, $|G| = 49$.
- If G is cyclic and $|G| = 49$, then $G \cong \mathbb{Z}_{49}$.
- If 7 is replaced with a prime p, then $G = \mathbb{Z}_{p^2}$.

■

4.16 Find a collection of distinct subgroups $\langle a_1\rangle, \langle a_2\rangle, \ldots, \langle a_n\rangle$ of $\mathbb{Z}_{240}$ with the property that $\langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle$ with n as large as possible.

Proof. $\langle 0\rangle \subset \langle 120\rangle \subset \langle 60\rangle \subset \langle 30\rangle \subset \langle 15\rangle \subset \langle 5\rangle \subset \langle 1\rangle$. ■

4.19 List the cyclic subgroups of $U(30)$.

Proof.

$$\begin{array}{rcl}
\langle 1\rangle & = & \{1\}, \\
\langle 7\rangle & = & \{1,7,19,13\}, \\
\langle 17\rangle & = & \{1,17,19,23\}, \\
\langle 11\rangle & = & \{1,11\}, \\
\langle 19\rangle & = & \{1,19\}, \\
\langle 29\rangle & = & \{1,29\}.
\end{array}$$

■

4.21 Let G be a cyclic group with $|G| = 24$, and let $a \in G$. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\langle a\rangle = G$. (Hint: consider $|a|$ and $|G|$.)

Proof. By the Lagrangle's Theorem, $|a|$ divide $|G| = 24$. Recall that if $|a|$ divide n, then $a^n = e$. Equivalently, if $a^n \neq e$, then $|a| \nmid n$. Hence, $a^8 \neq e$ and $a^{12} \neq e$ implies that $|a| \notin \{1,2,3,4,6,8,12\}$. Therefore, $|a| = 24$ and G is a cyclic group generated by a. That is, $G = \langle a\rangle$. ■

4.24 For any element a in any group G, prove that $\langle a\rangle$ is a subgroup of $C_G(a)$.

Proof. $\langle a\rangle$ is already a subgroup of G. It is sufficient to show that $\langle a\rangle \subseteq C_G(a)$. If $a^m \in \langle a\rangle$, then $a^m \cdot a = a^{m+1} = a \cdot a^m$. That is, $a^m \in C_G(a)$. ■

4.26 Find all generators of $\mathbb{Z}$. Let a be a group element that has infinite order. Find all generators of $\langle a\rangle$.

Proof. ± 1, $a^{\pm 1}$. ■

4.27 Prove that $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication, has a cyclic subgroup of order n for every positive integer n.

提示. 回想高中學的 $z^n = 1$。

Proof. $\langle \omega_n\rangle$, where $\omega_n = e^{\frac{2\pi}{n}i} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. ■

4.28 Let a be a group element that has infinite order. Prove that $\langle a^i\rangle = \langle a^j\rangle$ if and only if $i = \pm j$.

Proof. ($\Leftarrow$) By Exercise 4.11.

(⇒)

$$\begin{array}{cl}
 & \langle a^i \rangle = \langle a^j \rangle \\
\Rightarrow & a^i \in \langle a^j \rangle \\
\Rightarrow & a^i = (a^j)^{q_1} \text{ for some } q_1 \in \mathbb{Z} \\
\Rightarrow & a^{i-jq_1} = e \\
\overset{\overset{|a|=\infty}{\downarrow}}{\Rightarrow} & i - jq_1 = 0 \\
\Rightarrow & i = jq_1 \\
\text{Similar} & j = iq_2 \text{ for some } q_2 \in \mathbb{Z} \\
\Rightarrow & i = jq_1 = iq_1q_2 \\
\Rightarrow & i(q_1q_2 - 1) = 0 \\
\text{If} & i = 0 \\
\Rightarrow & j = 0 = -i \\
\text{If} & q_1q_2 - 1 = 0 \\
\Rightarrow & q_1q_2 = 1 \\
\Rightarrow & q_1 = \pm 1 \\
\Rightarrow & i = \pm j
\end{array}$$

■

4.30* Suppose a and b belong to a group, a has odd order, and $aba^{-1} = b^{-1}$. Show that $b^2 = e$.

提示. $aba^{-1} = b^{-1} \Rightarrow bab = a$. Let $x = ba = ab^{-1}$. Then $x^2 = \cdots = a^2$.

Suppose $|a| = 2n + 1$. Then $x^{2n+1} = \cdots = b$.

Therefore, $b^2 = x^{4n+2} = \cdots$.

Proof. $aba^{-1} = b^{-1}$ implies that $ba = ab^{-1}$. Let $x = ba = ab^{-1}$. Then $x^2 = (ab^{-1})(ba) = a^2$.

Suppose that $|a| = 2n + 1$. Then

$$x^{2n+1} = x \cdot (x^2)^n = x \cdot (a^2)^n = (ba) \cdot (a^2)^n = b \cdot a^{2n+1} = b.$$

Therefore, $b^2 = (x^{2n+1})^2 = (x^2)^{2n+1} = (a^2)^{2n+1} = (a^{2n+1})^2 = e$. ■

4.31 Let G be a finite group. Show that there exists a fixed positive integer n such that $a^n = e$ for all a in G. (Note that n is independent of a.)

提示. Consider $\langle a \rangle = \{a, a^2, a^3, \ldots\}$.

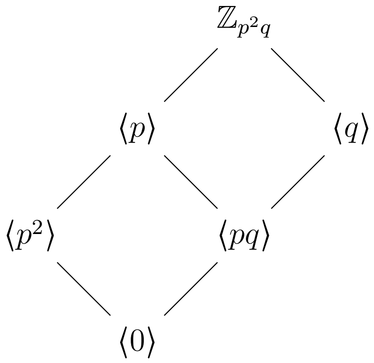
補充. 學過 Lagrange's Theorem 之後, 這題會變得很簡單。

Proof. Let $G = \{a_1, a_2, \ldots, a_s\}$. Since G is finite, for $i = 1, 2, \ldots, s$, $\langle a_i \rangle = \{a_i, a_i^2, a_i^3, \ldots\}$ is finite. Hence, $a^{j_i} = a^{k_i}$ for some $j_i > k_i$ and $a^{j_i - k_i} = e$. Let $n = \text{l.c.m.}(j_1 - k_1, j_2 - k_2, \ldots, j_s - k_s)$. ■

4.33 Determine the subgroup lattice for Z_{p^2q}, where p and q are distinct primes.

提示. List some concrete examples. Then you will discover something.

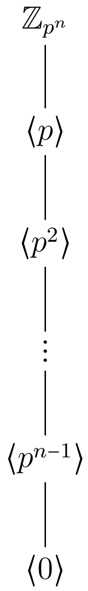
Proof.



■

4.35 Determine the subgroup lattice for $\mathbb{Z}_{p^n}$, where p is a prime and n is some positive integer.

Proof.



■

4.36* Prove that a finite group is the union of proper subgroups if and only if the group is not cyclic.

提示. Fundamental Theorem of Cyclic Groups.

Proof. ($\Rightarrow$) Suppose that $G = \langle a\rangle$ is a cyclic group and which is the union of its proper subgroups. If H is a proper subgroup of G, then $a \notin H$. Therefore,

$$a \notin \bigcup_{H \subsetneq G} H = G,$$

a contradiction.

($\Leftarrow$) Let $G = \{a_1, a_2, ..., a_n\}$ be a finite group which is not cyclic. Then there does not exist an element $a \in G$ such that $\langle a \rangle = G$. That is, $\langle a_i \rangle$ is a proper subgroup for every $i = 1, 2, ..., n$. Therefore,

$$G = \bigcup_{i=1}^{n} \langle a_i \rangle.$$

G is the union of its proper subgroups. ■

4.40 Let m and n be elements of the group $\mathbb{Z}$. Find a generator for the group $\langle m \rangle \cap \langle n \rangle$.

Proof. $\langle \text{l.c.m.}(m, n) \rangle$. ■

4.41 Suppose that a and b are group elements that commute and have order m and n. If $\langle a \rangle \cap \langle b \rangle = \{e\}$, prove that the group contains an element whose order is the least common multiple of m and n. (Hint: the idea of the proof is similar to the one we prove the order of two disjoint cycles.)

Proof. We show that ab is an element whose order is l.c.m.(m, n). Note that

$$\begin{aligned}
& \text{If } (ab)^r = e \\
\Rightarrow\ & e = (ab)^r \overset{\substack{ab \text{ commute} \\ \downarrow}}{=} a^r b^r \\
\Rightarrow\ & a^r = b^{-r} \in \langle a \rangle \cap \langle b \rangle = \{e\} \\
\Rightarrow\ & a^r = b^{-r} = e \\
\Rightarrow\ & a^r = b^r = e \\
\Rightarrow\ & m = |a| \text{ divide } r \text{ and } n = |b| \text{ divide } r \\
\Rightarrow\ & r \text{ is a common multiple of } m \text{ and } n \\
\Rightarrow\ & \text{the least common multiple of } m \text{ and } n \text{ is the order of } ab.
\end{aligned}$$

■

補充. 如果沒有 $\langle a \rangle \cap \langle b \rangle = \{e\}$ 這個條件的話就不成立, 例如 $a = 2, b = 4 \in \mathbb{Z}_{12}$, 這是常犯的錯誤。

4.49 For each positive integer n, prove that $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication, has exactly $\phi(n)$ element of order n.

提示. 1 的所有 n 次方根中, 有幾個是"恰好" 自乘 n 次後回到 1 的? 例如 1 的 4 個 4 次方根 $1, -1, i, -i$ 中, (-1) 在 2 次方的時候就提早回到 1 了, 只有 i 跟 $-i$ "恰好"在自乘 4 次後回到 1。

Proof. Let $\omega_n = e^{\frac{2\pi}{n} i} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. Then $|\omega_n^k| \overset{\substack{\text{p.80, thm.4.2} \\ \downarrow}}{=} \frac{n}{\gcd(n,k)}$. Thus,

$$|\omega_n^k| = n \Leftrightarrow \gcd(n, k) = 1$$

and

$$\#\{\omega_n^k \in \langle \omega_n \rangle \mid \gcd(n,k) = 1\} = \#\{1 \le k < n \mid \gcd(n,k) = 1\} = \phi(n).$$

■

補充. 比較一下這題跟 p.81, cor.4。事實上, $\mathbb{Z}_n \cong \langle \omega_n \rangle$.

4.51 Suppose that G is a finite group with the property that every nonidentity element has prime order (for example, D_3 and D_5). If $Z(G)$ is not trivial, prove that every nonidentity element of G has the same order.

Proof.

Lemma: If $ab = ba$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$, then $|ab| = \text{l.c.m.}(|a|, |b|)$.

Proof of Lemma:

$$\begin{aligned}
& \text{If } (ab)^r = e \\
\Rightarrow\quad & e = (ab)^r \overset{\overset{ab=ba}{\downarrow}}{=} a^r b^r \\
\Rightarrow\quad & a^r = b^{-r} \in \langle a \rangle \cap \langle b \rangle = \{e\} \\
\Rightarrow\quad & a^r = b^{-r} = e \\
\Rightarrow\quad & a^r = b^r = e \\
\overset{\overset{\text{p.79, cor.2}}{\downarrow}}{\Rightarrow}\quad & |a| \text{ divide } r \text{ and } |b| \text{ divide } r \\
\Rightarrow\quad & r \text{ is a common multiple of } |a| \text{ and } |b| \\
\Rightarrow\quad & \text{the least common multiple of } |a| \text{ and } |b| \text{ is the order of } ab.
\end{aligned}$$

Proof of the Problem: Suppose that $e \neq c \in Z(G)$. For any $e \neq g \in G$, we show that $|g| = |c|$.

$$\begin{aligned}
& \text{If } |g| = p \neq q = |c| \text{ for some primes } p \text{ and } q \\
\Rightarrow\quad & \gcd(|g|, |c|) = 1 \\
\overset{\overset{\text{Exercise 4.64}}{\downarrow}}{\Rightarrow}\quad & \langle c \rangle \cap \langle g \rangle = \{e\} \\
\overset{\overset{\text{Lemma and } c\in Z(G)}{\downarrow}}{\Rightarrow}\quad & |cg| = \text{l.c.m.}(|c|, |g|) = pq. \\
& \text{But } |gc| \text{ is also a prime, a contradiction.}
\end{aligned}$$

課本的解法: Suppose that $e \neq c \in Z(G)$ and $|c| = p$ for some prime p. Pick a fixed $g \neq e \in G$, suppose that $|g| = q$ for some prime q.

$$\begin{aligned}
& \text{Since } c \in Z(G) \\
\Rightarrow\quad & cg = gc \\
\Rightarrow\quad & (cg)^{pq} = (c^p)^q (g^q)^p = e \\
\overset{\overset{\text{p.79, cor.2}}{\downarrow}}{\Rightarrow}\quad & |cg| \text{ divide } pq \\
\overset{\overset{cg=e \text{ or } |cg| \text{ is a prime}}{\downarrow}}{\Rightarrow}\quad & |cg| \in \{1, p, q\}
\end{aligned}$$

If $|cg| = 1$, then $cg = e$ and $g = c^{-1}$ and $q = |g| = |c^{-1}| = |c| = p$.

If $|cg| = p$, then $e = (cg)^p = c^p g^p = g^p$ and $q = |g|$ divide p. Which implies that $q = p$.

If $|cg| = q$, then $e = (cg)^q = c^q g^q = c^q$ and $p = |c|$ divide q. Which implies that $q = p$. ■

補充. 注意, 並沒有 $ab = ba \neq e \Rightarrow |ab| = \operatorname{lcm}(|a|,|b|)$, 例如在 D_{24} 中, $|a^3| = 8 = |a^9|$, $a^3 \cdot a^9 = a^9 \cdot a^3 \neq e$, 但是 $|a^3 \cdot a^9| = |a^{12}| = 2 \neq \text{l.c.m.}(|a^3|,|a^9|)$.

4.53 Let p be a prime. If a group has more than $p-1$ elements of order p, why can't the group be cyclic?

Proof. Let G be a such group. If G is infinite, then G is $\mathbb{Z}$. But $\mathbb{Z}$ has no element with finite order except the identity. So let's assume that G is finite and cyclic. Let $a \in G$ and $|a| = p$. Then for any $e \neq b \in \langle a \rangle$, by p.81, cor.1, $|b|$ divides p and $|b| = p$. Hence, $\langle a \rangle$ contains $p-1$ elements of order p. By the hypothesis, there exists $c \notin \langle a \rangle$ such that $|c| = p$. Then $\langle c \rangle$ is another subgroup of G with order p. But by the Fundamental Theorem of Cyclic Groups, G can have only one subgroup of order p, we have a contradiction. Thus, G can't be cyclic. ■

4.64 Let a and b belong to a group. If $|a|$ and $|b|$ are relatively prime, show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Proof.

$$\begin{array}{cl}
 & c \in \langle a \rangle \cap \langle b \rangle \\
\Rightarrow & c = a^s = b^t \\
\Rightarrow & c^{|a|} = (a^s)^{|a|} = (a^{|a|})^s = e \\
\Rightarrow & e = c^{|a|} = (b^t)^{|a|} = b^{t|a|} \\
\overset{\text{p.79, cor.2}}{\overset{\downarrow}{\Rightarrow}} & |b| \text{ divide } t|a| \\
\overset{\gcd(|a|,|b|)=1,(??)}{\overset{\downarrow}{\Rightarrow}} & |b| \text{ divide } t \\
\text{Suppose} & t = |b| \cdot q \text{ for some } q \in \mathbb{Z} \\
\Rightarrow & c = b^t = (b^{|b|})^q = e \\
\Rightarrow & \langle a \rangle \cap \langle b \rangle = \{e\}.
\end{array}$$

另解: If $x \in \langle a \rangle \cap \langle b \rangle$, then $x = a^s = b^t$. By p.80, thm.4.2,

$$|x| = \frac{|a|}{\gcd(|a|,s)} = \frac{|b|}{\gcd(|b|,t)}.$$

Which is a divisor of $|a|$ and $|b|$. But $|a|$ and $|b|$ are relatively prime, the only possible is $|x| = 1$. That is, $x = e$. ■

補充. 學完 Lagrange's Theorem, 這題會變得很簡單。

4.66 Prove that $U(2^n)$ $(n \geq 3)$ is not cyclic.

提示. Use induction on n to prove that if $\gcd(a, 2^n) = 1$, then $a^{2^{n-2}} \equiv 1 \pmod{2^n}$, where $n \geq 3$. Therefore, for any $a \in U(2^n)$, by p.79, cor.2, $|a|$ divides 2^{n-2} and $|a| \neq 2^{n-1} = \phi(2^n)$. That is, $U(2^n)$ can't be generated by any element.

4.68 Prove that $\mathbb{Z}_n$ has an even number of generators if $n > 2$. What does this tell you about $\phi(n)$?

Proof. If x is a generator of $\mathbb{Z}_n$, by Exercise 4.11, then $\mathbb{Z}_n = \langle x \rangle = \langle -x \rangle$. In $\mathbb{Z}_n$, $1 = -1$ if and only if $n \in \{1, 2\}$. Thus, if $n > 2$, then $x \neq -x \in \mathbb{Z}_n$. Therefore, there are even number of generators of $\mathbb{Z}_n$ if $n > 2$.

In addition, by p.81, cor.4,

$$\underline{\text{the number of generator of } \mathbb{Z}_n} = \underline{\#\{1 \leq k < n \mid \gcd(k, n) = 1\}} = |U(n)| = \phi(n).$$

■

補充. 跟 Exercise 3.59比較一下。

你也可以想想反過來要怎麼證, 也就是先證明 $\phi(n)$ is even when $n > 2$, 然後得到 $\mathbb{Z}_n$ has an even number of generators if $n > 2$。

Suppose that $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$, where $p_1, p_2, \ldots, p_s$ are distinct primes.

- **Case I:** there exists p_i is odd.

$$\begin{aligned}
\phi(n) &= n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right) \\
&= n\left(\frac{p_1 - 1}{p_1}\right) \cdots \left(\frac{p_2 - 1}{p_2}\right) \cdots \left(\frac{p_s - 1}{p_s}\right) \\
&= \frac{n}{p_1 p_2 \cdots p_s}(p_1 - 1)(p_2 - 1) \cdots (p_s - 1) \text{ is even because } p_i - 1 \text{ is even}
\end{aligned}$$

- **Case II:** $n = 2^r$. Since $n > 2$, we have $r > 1$ and $\phi(n) = 2^r\left(1 - \frac{1}{2}\right) = 2^{r-1}$ is even.

學完 Lagrange's Theorem 之後, 可以很簡單地就證明 $\phi(n)$ is even when $n > 2$。

4.70 Suppose that $|x| = n$. Find a necessary and sufficient condition on r and s such that $\langle x^r \rangle \subseteq \langle x^s \rangle$.

Proof.

$$\begin{aligned}
& \langle x^r \rangle \subseteq \langle x^s \rangle \\
\Leftrightarrow \quad & x^r = (x^s)^q \text{ for some } q \in \mathbb{Z} \\
\Leftrightarrow \quad & x^{r - sq} = e \\
\overset{\substack{\text{p.79, cor.2} \\ \downarrow}}{\Leftrightarrow} \quad & n \mid (r - sq) \\
\Leftrightarrow \quad & r \equiv sq \pmod{n} \\
\Leftrightarrow \quad & sq \equiv r \pmod{n} \\
\overset{\substack{\text{Exercise 0.11} \\ \downarrow}}{\Leftrightarrow} \quad & \gcd(s, n) \mid r.
\end{aligned}$$

■

4.73* Let p be a prime. Show that in a cyclic group of order $p^n - 1$, every element is a pth power (that is , every element can be written in the form a^p for some a).

Proof. **課本的解法**:

$$
\begin{aligned}
\text{Suppose}\quad & G=\langle a\rangle, |G|=p^n-1 \\
\overset{\overset{\text{gcd}\,(p,p^n-1)=1}{\downarrow}}{\Rightarrow}\quad & |a^p| \overset{\overset{\text{p.80, thm.4.2}}{\downarrow}}{=} \frac{p^n-1}{\gcd(p,p^n-1)}=p^n-1 \\
\Rightarrow\quad & G=\langle a^p\rangle \\
\Rightarrow\quad & \forall g\in G, g=(a^p)^s=(a^s)^p.
\end{aligned}
$$

另解一:

$$
\begin{aligned}
\text{Suppose}\quad & G=\langle a\rangle, |G|=p^n-1 \\
\Rightarrow\quad & a^{p^n-1}=e \\
\Rightarrow\quad & a^{p^n}=a \\
\Rightarrow\quad & G=\langle a\rangle=\langle a^{p^n}\rangle \\
\Rightarrow\quad & \forall g\in G, g=(a^{p^n})^s=a^{sp^n}=(a^{sp^{n-1}})^p.
\end{aligned}
$$

另解二:

$$
\begin{aligned}
\text{Suppose}\quad & G=\langle a\rangle, |G|=p^n-1 \\
\text{Consider}\quad & f:G\to G, f(g)=g^p \\
\text{If}\quad & f(a^s)=f(a^t) \\
\Rightarrow\quad & a^{sp}=a^{tp} \\
\Rightarrow\quad & a^{p(s-t)}=e \\
\overset{\overset{\text{p.79, cor.2}}{\downarrow}}{\Rightarrow}\quad & |a|=(p^n-1)\mid p(s-t) \\
\overset{\overset{\text{gcd}\,(p^n-1,p)=1,(??)}{\downarrow}}{\Rightarrow}\quad & (p^n-1)\mid(s-t) \\
\Rightarrow\quad & a^{s-t}=e \\
\Rightarrow\quad & a^s=a^t \\
\Rightarrow\quad & f \text{ is one-to-one} \\
\overset{\overset{|G|=|G|<\infty}{\downarrow}}{\Rightarrow}\quad & f \text{ is onto} \\
\Rightarrow\quad & \forall g\in G, \exists h\in G \text{ such that } h^p=f(h)=g
\end{aligned}
$$

■

補充. 細心的同學可能會發現我們並沒有用到“p是質數”這個條件, 這個定理的確在 p 不是質數的時候也成立, 但爲什麼還要要求“p是質數”這個條件呢? 是因爲發現這個定理的動機, 是來自於 finite field 裡面的一種 Frobenius automorphism, 參考15.44。

4.78 If n is odd, prove that D_n has no subgroup of order 4.

Proof. Recall that there are only two kind of group of order 4, one is $\langle x\rangle=\{1,x,x^2,x^3\}$, $|x|=4$. For example, $\mathbb{Z}_4$. Another one is $\{1,x,y,z\}$, $xy=z, yz=x, xz=y$ and $|x|=|y|=|z|=2$. For example, $\mathbb{Z}_2\oplus\mathbb{Z}_2$. These two kind of group both are abelian.

Suppose that $D_n = \{1, a, a^2, ..., a^{n-1}, b, ba, ba^2, ..., ba^{n-1}\}$, where $|a| = n$, $|b| = 2$ and $ab = ba^{-1}$.

If $x \in \langle a \rangle$, by p.81, cor.1, $|x|$ divides $|\langle a \rangle| = |a| = n$. Since n is odd, we get $|x| \neq 4$. If $x = ba^i$, then $|x| = 2 \neq 4$. There are no element with order 4 and D_n has no cyclic subgroup of order 4.

If $x \in \langle a \rangle$, by p.81, cor.1, $|x|$ divides $|\langle a \rangle| = |a| = n$. Since n is odd, we get $|x| \neq 2$. Thus, there are no element in $\langle a \rangle$ with order 2. If D_n has a subgroup which is of the form $\{1, x, y, z\}$, where $xy = z$, $|x| = |y| = |z| = 2$, then it must be $x = ba^i, y = ba^j$ for some $n - 1 \leq i > j \leq 0$ and $ba^{i-j} = xy = yx = ba^{j-i}$. Which implies that $a^{i-j} = a^{j-i}$ and $(a^{i-j})^2 = e$ and $|a^{i-j}| = 2$, a contradiction because $a^{i-j} \in \langle a \rangle$. ■

補充. 學完 Lagrange's Theorem 之後, 這個定理會變得更簡單。

4.79 If $n \geq 4$ and is even, show that D_n has exactly $n/2$ noncyclic subgroups of order 4.

Proof. $\langle a^{n/2}, b \rangle, \langle a^{n/2}, ba \rangle, \langle a^{n/2}, ba^2 \rangle, ..., \langle a^{n/2}, ba^{n/2-1} \rangle$. ■

4.80 If $n \geq 4$ and n is divisible by 2 but not by 4, prove that D_n has exactly $n/2$ subgroups of order 4.

Proof. $\langle a^{n/2}, b \rangle, \langle a^{n/2}, ba \rangle, \langle a^{n/2}, ba^2 \rangle, ..., \langle a^{n/2}, ba^{n/2-1} \rangle$. ■

4.81 How many subgroups of order n does D_n have?

Proof.

$$\{H \leq D_n \mid |H| = n\} = \begin{cases} \{\langle a \rangle\}, & n \text{ is odd;} \\ \{\langle a \rangle, \langle a^2, b \rangle, \langle a^2, ba \rangle\}, & n \text{ is even.} \end{cases}$$

■

↓4.63, 4.83* Let a and b belong to some group. Suppose that $|a| = m$ and $|b| = n$ and m and n are relatively prime. If $a^k = b^k$ for some integer k, prove that mn divides k.

提示. Division Algorithm.

Proof. By Exercise 4.64, $a^k = b^k \in \langle a \rangle \cap \langle b \rangle = \{e\}$. Then $|a| = m \mid k$ and $|b| = n \mid k$. Since $\gcd(m, n) = 1$, we have $mn \mid k$.

曾〇傑的解法:

$$\begin{array}{ll} & e = (a^m)^k = (a^k)^m = (b^k)^m = b^{km} \Rightarrow n \mid km \overset{\gcd(r,s)=1, r|st \Rightarrow r|t}{\overset{\downarrow}{\Rightarrow}} n \mid k \\ \text{and} & e = (b^n)^k = (b^k)^n = (a^k)^n = a^{kn} \Rightarrow m \mid kn \overset{\gcd(r,s)=1, r|st \Rightarrow r|t}{\overset{\downarrow}{\Rightarrow}} m \mid k \\ \overset{\gcd(r,s)=1, r|t, s|t \Rightarrow rs|t}{\overset{\downarrow}{\Rightarrow}} & mn \mid k. \end{array}$$

課本的解法:

$$
\begin{array}{cl}
 & \langle a\rangle \cap \langle b\rangle \le \langle a\rangle \text{ and } \langle a\rangle \cap \langle b\rangle \le \langle b\rangle \\
\overset{\overset{\text{Lagrange's Theorem}}{\downarrow}}{\Rightarrow} & |\langle a\rangle \cap \langle b\rangle| \text{ divide } |\langle a\rangle| = |a| = m \text{ and } |\langle b\rangle| = |b| = n \\
\overset{\overset{\gcd(m,n)=1}{\downarrow}}{\Rightarrow} & |\langle a\rangle \cap \langle b\rangle| = 1 \\
\Rightarrow & \langle a\rangle \cap \langle b\rangle = \{e\} \\
\Rightarrow & a^k = b^k \in \langle a\rangle \cap \langle b\rangle = \{e\} \\
\Rightarrow & a^k = b^k = e \\
\Rightarrow & |a| = m \mid k \text{ and } |b| = n \mid k \\
\overset{\overset{\gcd(r,s)=1,\, r|t,\, s|t \Rightarrow rs|t}{\downarrow}}{\Rightarrow} & mn \mid k.
\end{array}
$$

■

4.84 For every integer n greater that 2, prove that the group $U(n^2-1)$ is not cyclic.

提示. Note that $\gcd(\pm 1, n^2-1) = \gcd(\pm n, n^2-1) = 1$ because $(\pm n)^2 - (n^2-1) = 1$. $S = \{1, -1, n, -n\}$ form a noncyclic group of $U(n^2-1)$. $(S \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.)$ So $U(n^2-1)$ can't be a cyclic group because any subgroup of a cyclic group must be a cyclic as well.

4.85 Prove that for any prime p and positive integer n, $\phi(p^n) = p^n - p^{n-1}$.

Proof.

$$
\begin{aligned}
\phi(p^n) &= \#\{a \in \{1,2,\ldots,p^n\} \mid \gcd(a,p^n) = 1\} \\
&= \#\{a \in \{1,2,\ldots,p^n\} \mid \gcd(a,p) = 1\} \\
&= \#\{a \in \{1,2,\ldots,p^n\} \mid p \nmid a\} \\
&= p^n - \#\{a \in \{1,2,\ldots,p^n\} \mid p \text{ divides } a\} \\
&= p^n - \#\{\underline{1}p, \underline{2}p, \underline{3}p, \underline{4}p, \underline{5}p, \ldots, \underline{p^{n-1}} \cdot p\} \\
&= p^n - p^{n-1}.
\end{aligned}
$$

■

5 Chapter 5

5.1 Let

$$
\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix} \text{ and } \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}.
$$

Compute each of the following.

(a) α^{-1}

(b) $\beta\alpha$

(c) $\alpha\beta$

5.2 Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix}$$

and

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}.$$

Write α, β, and $\alpha\beta$ as

(a) products of disjoint cycles,

Proof.

$$\begin{aligned} \alpha &= (12345)(678), \\ \beta &= (23847)(56). \end{aligned}$$

■

(b) products of 2-cycles.

Proof.

$$\begin{aligned} \alpha &= (15)(14)(13)(12)(68)(67), \\ \beta &= (23)(38)(84)(47)(56). \end{aligned}$$

■

類似 5.2 Let

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 9 & 5 & 7 & 6 & 8 & 1 & 2 \end{bmatrix}$$

and

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 8 & 2 & 6 & 9 & 7 & 1 & 5 \end{bmatrix}.$$

Write α, β, and $\alpha\beta$ as

(a) products of disjoint cycles and determine the order of α, β and $\alpha\beta$.

Proof.

$$\begin{aligned} \alpha &= (14578)(239), \\ \beta &= (138)(24)(569), \\ \alpha\beta &= (197843)(256). \end{aligned}$$

$$\begin{aligned} |\alpha| &= 15, \\ |\beta| &= 6, \\ |\alpha\beta| &= 6. \end{aligned}$$

■

(b) products of 2-cycles (transpositions), and determine α, β and $\alpha\beta$ are even or odd.

Proof.

$$\begin{aligned}
\alpha &= (18)(17)(15)(14)(29)(23), \text{ even permutation,}\\
\beta &= (13)(38)(24)(56)(69), \text{ odd permutation,}\\
\alpha\beta &= (13)(14)(18)(17)(19)(26)(25), \text{ odd permutation.}
\end{aligned}$$

■

5.3 Write each of the following permutations as a product of disjoint cycles.

(a) (1235)(413)

(b) (13256)(23)(46512)

(c) (12)(13)(23)(142)

5.5 What is the order of each of the following permutations?

(a) (124)(357)

(b) (124)(3567)

(c) (124)(35)

(d) (124)(357869)

(e) (1235)(24567)

(f) (345)(245)

5.9 What are the possible orders for the elements of S_6 and A_6? What about A_7?

提示. If two permutations have the same cycle structure, then they have the same order.

$$\begin{aligned}
|(1234)(56)| &= 4.\\
|(123)(45)| &= 6.\\
|(123)(456)| &= 3.\\
|(12)(34)| &= 2.\\
|(12)(34)(56)| &= 2.
\end{aligned}$$

Proof. If two permutations have the same cycle structure, then they have the same order. Note that the elements in S_6 has the following type.

$$\begin{aligned}
&(123456),\\
&(12345),\\
&(1234),\\
&(123),\\
&(12),\\
&(1234)(56),\\
&(123)(45),\\
&(123)(456),\\
&(12)(34),\\
&(12)(34)(56),\\
&e.
\end{aligned}$$

The order of the elements in each type is

$$\begin{aligned}
|(123456)| &= 6,\\
|(12345)| &= 5,\\
|(1234)| &= 4,\\
|(123)| &= 3,\\
|(12)| &= 2,\\
|(1234)(56)| &= 4,\\
|(123)(45)| &= 6,\\
|(123)(456)| &= 3,\\
|(12)(34)| &= 2,\\
|(12)(34)(56)| &= 2,\\
|e| &= 1.
\end{aligned}$$

The possible orders for the elements of S_6 are $1, 2, 3, 4, 5, 6$.

Note that the elements in A_6 has the following type.

$$\begin{aligned}
&(12345),\\
&(123),\\
&(1234)(56),\\
&(123)(456),\\
&(12)(34),\\
&e.
\end{aligned}$$

The order of the elements in each type is

$$\begin{aligned}
|(12345)| &= 5,\\
|(123)| &= 3,\\
|(1234)(56)| &= 4,\\
|(123)(456)| &= 3,\\
|(12)(34)| &= 2,\\
|e| &= 1.
\end{aligned}$$

The possible orders for the elements of A_6 are $1, 2, 3, 4, 5$.

The elements in S_7 has the following type.

$$\begin{array}{r}
(1234567), \\
(123456), \\
(12345), \\
(1234), \\
(123), \\
(12), \\
(12345)(67), \\
(1234)(567), \\
(1234)(56), \\
(123)(456), \\
(123)(45), \\
(123)(45)(67), \\
(12)(34)(56), \\
(12)(34), \\
e.
\end{array}$$

The elements in A_7 has the following type.

$$\begin{array}{r}
(1234567), \\
(12345), \\
(123), \\
(1234)(56), \\
(123)(456), \\
(123)(45)(67), \\
(12)(34), \\
e.
\end{array}$$

The order of the elements in each type is

$$\begin{array}{rcl}
|(1234567)| & = & 7, \\
|(12345)| & = & 5, \\
|(123)| & = & 3, \\
|(1234)(56)| & = & 4, \\
|(123)(456)| & = & 3, \\
|(123)(45)(67)| & = & 6, \\
|(12)(34)| & = & 2, \\
|e| & = & 1.
\end{array}$$

The possible orders for the elements of A_7 are $1, 2, 3, 4, 5, 6, 7$. ■

5.13 Suppose that α is a mapping from a set S to itself and $\alpha(\alpha(x)) = x$ for all x in S. Prove that α is one-to-one and onto.

Proof. **One-to-one:** $\alpha(x_1) = \alpha(x_2) \Rightarrow \alpha(\alpha(x_1)) = \alpha(\alpha(x_2)) = x_2$.

Onto: For any $y \in S$, there exists $\alpha(y) \in S$ such that $\alpha(\alpha(y)) = y$. ■

5.19 Let α and β belong to S_n. Prove that $\alpha\beta$ is even if and only if α and β are both even or both odd.

Proof. If α is even and β is odd, then $\alpha\beta$ is odd. ■

5.23* Show that if H is a subgroup of S_n, then either every member of H is an even permutation or exactly half of the members are even.

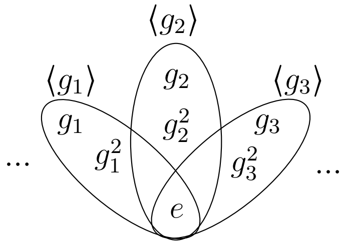
提示. Suppose that $\sigma_1, \sigma_2, ..., \sigma_n$ are all the even permutation in H. If τ_0 is an odd permutation in H, show that $\tau_0\sigma_1, \tau_0\sigma_2, ..., \tau_0\sigma_n$ are all the odd permutation in H.

Proof. Suppose that $\sigma_1, \sigma_2, ..., \sigma_n$ are all the even permutation in H. If τ_0 is an odd permutation in H, then for any odd permutation τ in H,

$$\tau = (\tau_0\tau_0^{-1})\tau = \tau_0(\tau_0^{-1}\tau)$$

and $\tau_0^{-1}\tau$ is an even permutation because it is a product of two odd permutations. That is, every odd permutation in H is of the form $\tau_0\sigma$ for some even permutation σ in H. Thus, $\tau_0\sigma_1, \tau_0\sigma_2, ..., \tau_0\sigma_n$ are all the odd permutation in H. ■

Proof. Let G be a group of order 12. For any $e \neq g \in G$, by Lagrange's Theorem, $|g| \in \{2, 3, 4, 6, 12\}$. If $|g| = 2n$ for some $n \in \mathbb{Z}$, then $|g^n| = 2$. If for all $e \neq g \in G$, we have $|g| = 3$, then $|g^2| = 3$ and there are $2k$ elements of order 3 for some $k \in \mathbb{Z}$, as the following figure indicates.



■

5.24 Suppose that H is a subgroup of S_n of odd order. Prove that H is a subgroup of A_n.

提示. Tricky. Consider HA_n.

Proof.

$$\begin{aligned}
&\text{If} && H \nsubseteq A_n \\
&\Rightarrow && \exists h \in H, h \text{ is an odd permutation} \\
&\Rightarrow && HA_n = S_n \\
&\Rightarrow && |S_n| = |HA_n| = \frac{|H|\cdot|A_n|}{|H\cap A_n|} \\
&\Rightarrow && 2 = \frac{|S_n|}{|A_n|} = \frac{|H|}{|H\cap A_n|} \\
&\Rightarrow && |H| = 2\cdot|H\cap A_n|.
\end{aligned}$$

Thus, $H \nsubseteq A_n$ implies that 2 divides $|H|$. Equivalently, $|H|$ is odd implies that $H \subseteq A_n$. ■

5.26 Let α and β belong to S_n. Prove that $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation.

提示. Consider a mapping $s: S_n \to U(3) = \{1,2\} = \{1,-1\}$ defined by

$$s(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is even;} \\ -1, & \text{if } \sigma \text{ is odd.} \end{cases}$$

Show that $s(\sigma\tau) = s(\sigma)s(\tau)$ and $s(\sigma) = s(\sigma^{-1})$ for all $\sigma, \tau \in S_n$.

Proof. [方法一] g and g^{-1} in S_n both are even or odd. g and aga^{-1} both are even or odd. So $\alpha^{-1}\beta^{-1}\alpha$ and β both are even or odd.

[方法二] Consider a mapping $s: S_n \to U(3) = \{1,2\} = \{1,-1\}$ defined by

$$s(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

For any $\sigma, \tau \in S_n$, you can prove that $s(\sigma\tau) = s(\sigma)s(\tau)$ and $s(\sigma) = s(\sigma^{-1})$ case by case. Then whatever α and β is either even or odd, we have

$$s(\alpha^{-1}\beta^{-1}\alpha\beta) = s(\alpha^{-1})s(\beta^{-1})s(\alpha)s(\beta) = s(\alpha)^2 s(\beta)^2 = 1$$

and $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation. ■

5.29 How many elements of order 4 does S_6 have? How many elements of order 2 does S_6 have?

提示. 180, 75. (why?)

Proof. By Problem 5, the element of order 4 in S_6 must be of the type (1234) or (1234)(56). There are $\binom{6}{4}\frac{4!}{4} = 90$ elements of type (1234) and $\binom{6}{4}\frac{4!}{4} = 90$ elements of type (1234)(56). Thus, there are 180 elements of order 4 in S_6.

By Problem 5, the element of order 2 in S_6 must be of the type (12) or (12)(34) or (12)(34)(56). There are $\binom{6}{2} = 15$ elements of type (12) and $\frac{\binom{6}{2}\binom{4}{2}}{2} = 45$ elements of type (12)(34) and $\frac{\binom{6}{2}\binom{4}{2}}{3!} = 15$ elements of type (12)(34)(56) Thus, there are 75 elements of order 2 in S_6.

Something good: `http://goo.gl/BjYQhN` ■

5.30 Prove that (1234) is not the product of 3-cycles.

Proof. (1234) is odd and a product of 3-cycles is even. ■

5.31* Let $\beta \in S_7$ and suppose $\beta^4 = (2143567)$. Find β.

提示.

Proof. Note that $(x_1x_2x_3x_4x_5x_6x_7)^4 = (x_1x_5x_2x_6x_3x_7x_4)$. That is, the quartic of a 7-cycle is a rearrangement of the number in the order

$$1 \to 5 \to 2 \to 6 \to 3 \to 7 \to 4.$$

Since

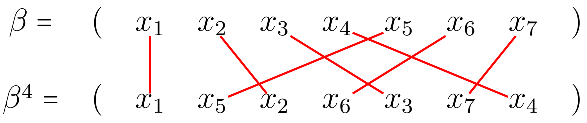
$$\beta^4 = (x_1x_5x_2x_6x_3x_7x_4) = (2143567),$$

we get $\beta = (x_1x_2x_3x_4x_5x_6x_7) = (2457136)$.

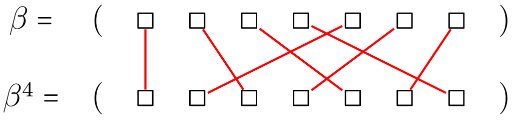
Furthermore, since $(\beta^4)^7 = e$, the order of β must be a divisor of $4 \times 7 = 2^2 \times 7$. If $|\beta| \in \{1, 2, 2^2\}$, then $\beta^4 = e \neq (2143567)$. In addition, there are no element in S_7 whose order is 2×7 or $2^2 \times 7$, hence, the order of β must be 7. The element of order 7 in S_7 must be a 7-cycle. Thus, $\beta = (2457136)$ is the only possible answer.

丁丁的解法:

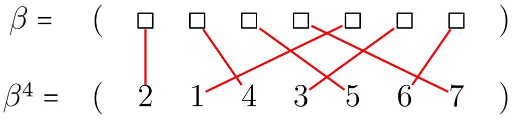
Step 1: Connect the corresponding number between β and β^4.



Step 2: Ease the number.



Step 3: Fill the number into β^4.



Step 4: The answer is clearly. ■

5.32 Let $\beta = (1, 2, 3)(1, 4, 5)$ (β is not a product of disjoint cycles). Write β^{99} in disjoint cycle form.

Proof. Note that $\beta = (123)(145) = (14523)$ and $\beta^5 = e$. Thus,

$$\beta^{99} = \beta^{100}\beta^{-1} = (\beta^5)^{20}\beta^{-1} = \beta^{-1} = (32541).$$

■

5.33* Find three elements σ in S_9 with the property that $\sigma^3 = (157)(283)(469)$.

提示. Observe that $(123456789)^3$.

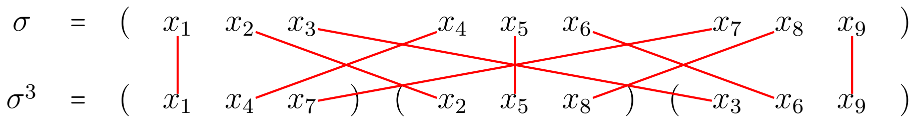
Proof. Observe that $(123456789)^3 = (147)(258)(369)$.

$$\begin{aligned} a &= (\underline{1}24\underline{5}86\underline{7}39), \\ b &= (\underline{7}24\underline{1}86\underline{5}39), \\ c &= (\underline{5}24\underline{7}86\underline{1}39) \end{aligned}$$

are three desired elements.

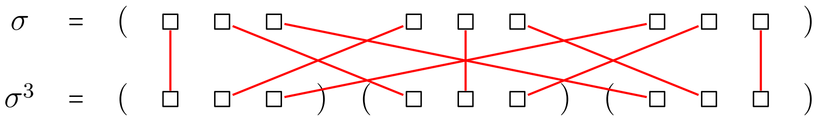
丁丁的解法:

Step 1: Connect the corresponding number between σ and σ^4.



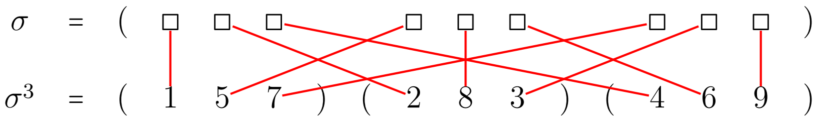
σ = (x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9)
σ^3 = (x_1 x_4 x_7) (x_2 x_5 x_8) (x_3 x_6 x_9)

Step 2: Ease the number.



σ = (□ □ □ □ □ □ □ □ □)
σ^3 = (□ □ □) (□ □ □) (□ □ □)

Step 3: Fill the number into σ^3.



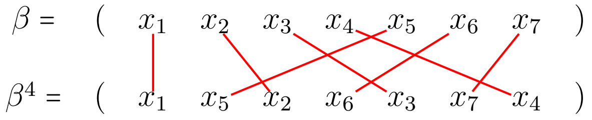
σ = (□ □ □ □ □ □ □ □ □)
σ^3 = (1 5 7) (2 8 3) (4 6 9)

Step 4: The answer is clearly. ■

Proof. Note that $(x_1x_2x_3x_4x_5x_6x_7)^4 = (x_1x_5x_2x_6x_3x_7x_4)$. That is, the quartic of a 7-cycle is a rearrangement of the number in the order

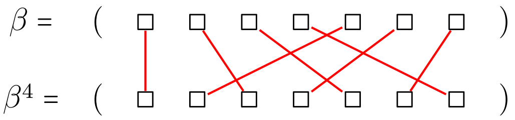
$$1 \to 5 \to 2 \to 6 \to 3 \to 7 \to 4.$$

Since $\beta^4 = (x_1x_5x_2x_6x_3x_7x_4) = (2143567)$, we get $\beta = (x_1x_2x_3x_4x_5x_6x_7) = (2457136)$. At first, you can connect the corresponding number between σ and σ^4.

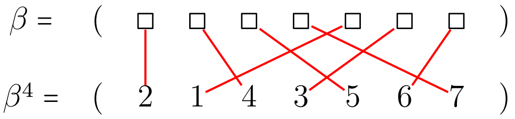


β = (x_1 x_2 x_3 x_4 x_5 x_6 x_7)
β^4 = (x_1 x_5 x_2 x_6 x_3 x_7 x_4)

Then erase the number.



Finally, fill the number in β^4.



Then the answer is obviously. ■

5.34 What cycle is $(a_1 a_2 \cdots a_n)^{-1}$?

Proof. $(a_n \cdots a_2 a_1)$. ■

5.35 Let G be a group of permutations on a set X. Let $a \in X$ and define $\operatorname{stab}(a) = \{\alpha \in G \mid \alpha(a) = a\}$. We call $\operatorname{stab}(a)$ the *stabilizer* of a in G. Prove that $\operatorname{stab}(a)$ is a subgroup of G.

提示. Note that $\alpha(a) = a = \alpha(\alpha^{-1}(a))$ and α is one-to-one.

Proof. The identity of G is the identity mapping i_X defined by $i_X(x) = x$ for all $x \in X$. In particular, $i_X(a) = a$. Thus, $i_X \in \operatorname{stab}(a)$.

If $\alpha, \beta \in \operatorname{stab}(a)$, then

$$(\alpha\beta)(a) = \alpha(\beta(a)) = \alpha(a) = a.$$

Thus, $\alpha\beta \in \operatorname{stab}(a)$.

Since $\alpha(\underline{a}) = a = \alpha(\underline{\alpha^{-1}(a)})$ and α is one-to-one, we have $a = \alpha^{-1}(a)$. That is, $\alpha^{-1} \in \operatorname{stab}(a)$. ■

5.37 Let $\alpha = (1,3,5,7,9)(2,4,6)(8,10)$. If α^m is a 5-cycle, what can you say about m?

Proof. $6 \mid m$ but $5 \nmid m$. ■

5.45 Prove that S_n is non-Abelian for all $n \geq 3$.

Proof. $(12)(123) \neq (123)(12)$. ■

5.46 Prove that A_n is non-Abelian for all $n \geq 4$.

Proof. $(123)(234) \neq (234)(123)$. ■

5.48 Show that in S_7, the equation $x^2 = (1234)$ has no solutions but the equation $x^3 = (1234)$ has at least two.

Proof. x^2 is even and (1234) is odd. ■

5.50 Let α be a 2-cycle and β be a t-cycle in S_n. Prove that $\alpha\beta\alpha$ is a t-cycle.

提示. Since α is a 2-cycle, we have $\alpha = \alpha^{-1}$. Suppose that $\beta = (c_1c_2\cdots c_t)$. Then

$$\alpha\beta\alpha = \alpha\beta\alpha^{-1} = (\alpha(c_1)\alpha(c_2)\cdots\alpha(c_t)).$$

5.51 Use the previous exercise to prove that, if α and β belong to S_n and β is the product of k cycles of lengths $n_1, n_2, \ldots, n_k$, then $\alpha\beta\alpha^{-1}$ is the product of k cycles of lengths $n_1, n_2, \ldots, n_k$.

提示. Note that if $C = (c_1c_2\cdots c_t)$, then $\alpha C\alpha^{-1} = (\alpha(c_1)\alpha(c_2)\cdots\alpha(c_t))$, as the following figure indicates.

$$\begin{tikzcd}
\alpha(c_i) \arrow[r, "\alpha^{-1}"] \arrow[d, "?"'] & c_i \arrow[d, "C"] \\
\alpha(c_{i+1}) & c_{i+1} \arrow[l, "\alpha"]
\end{tikzcd}$$

Suppose that $\beta = C_1C_2\cdots C_k = (c_{11}c_{12}\cdots c_{1n_1})(c_{21}c_{22}\cdots c_{2n_2})\cdots(c_{k1}c_{k2}\cdots c_{kn_k})$ is a product of k disjoint cycles of lengths $n_1, n_2, \ldots, n_k$, respectively. Then

$$\begin{aligned}
\alpha\beta\alpha^{-1} &= \alpha C_1C_2\cdots C_k\alpha^{-1} \\
&= \underline{\alpha C_1\alpha^{-1}}\cdot\underline{\alpha C_2\alpha^{-1}}\cdots\underline{\alpha C_k\alpha^{-1}} \\
&= \underline{\alpha(c_{11}c_{12}\cdots c_{1n_1})\alpha^{-1}}\cdot\underline{\alpha(c_{21}c_{22}\cdots c_{2n_2})\alpha^{-1}}\cdots\underline{\alpha(c_{k1}c_{k2}\cdots c_{kn_k})\alpha^{-1}} \\
&= \underline{(\alpha(c_{11})\alpha(c_{12})\cdots\alpha(c_{1n_1}))}\cdot\underline{(\alpha(c_{21})\alpha(c_{22})\cdots\alpha(c_{2n_2}))}\cdots\underline{(\alpha(c_{k1})\alpha(c_{k2})\cdots\alpha(c_{kn_k}))} \\
&\ \text{is also a product of } k \text{ cycles of lengths } n_1, n_2, \ldots, n_k
\end{aligned}$$

補充. 這題很重要, 這說明了在 S_n 裡面, β 跟 $\alpha\beta\alpha^{-1}$ 有相同的cycle structure (雖然只證明了一半), 而這個事實在我們以後學 conjugate 及 group action 的時候非常重要。

5.52 Let α and β belong to S_n. Prove that $\beta\alpha\beta^{-1}$ and α are both even or both odd.

提示. 你可以用 Exercise 5.51, 也可以討論 even-odd。

5.59 Let n be an odd integer greater than 1. Viewing D_n as a group of permutations of a regular n-gon with consecutive vertices labeled $1, 2, \ldots, n$, explain why the rotation subgroup of D_n is a subgroup of A_n.

提示. $\langle(12\cdots n)\rangle = \langle(1n)(1\ n-1)\cdots(12)\rangle \leq A_n$ because n is odd.

補充. 你要記住兩個常用的分解,

- 頭尾法:$(1234) = (14)(13)(12)$,
- 相鄰法:$(1234) = (12)(23)(34)$,

這可以讓你在計算上省下很多功夫。

5.60 Let n be an integer greater than 1. Viewing D_n as a group of permutations of a regular n-gon with consecutive vertices labeled $1, 2, \ldots, n$, determine for which n all the permutations corresponding to reflections in D_n are even permutations. Hint: Consider the fours cases for $n \mod 4$.

提示. Write down some easy cases $n = 3, 4, 5, 6, 7, 8$. Then you will discovery something.

Proof. $n = 2k + 1$, k is even. ■

5.61 Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2.

Proof. There are $\frac{5!}{5} = 24$ elements are of type (12345).

There are $\binom{5}{3}\frac{3!}{3} = 20$ elements are of type (123).

There are $\frac{\binom{5}{2}\binom{3}{2}}{2!} = 15$ elements are of type $(12)(34)$. ■

5.65* Show that every element in A_n for $n \geq 3$ can be expressed as a 3-cycle or a product of three cycles.

提示.

- **Lemma:** Any permutation could be express as a product of transpositions (2-cycle). For instance, $(12345) = (15)(14)(13)(12)$ or $(12345) = (12)(23)(34)(45)$.
- If $n \geq 4$, without loss of generality, $(12)(34) = (123)(234)$ and $(12)(23) = (123)$.

Proof. If $n = 3$, then $A_3 = \{e = (123)^3, (123), (132)\}$. Every element in A_3 is a 3-cycle or a product of three cycles.

From now on, we suppose that $n \geq 4$. Recall that any permutation could be express as a product of transpositions (2-cycle). Thus, any element in A_n could be express as a product of even number of transpositions. Since $n \geq 4$, there are three possibilities of a product of two transpositions.

$$\begin{aligned}(12)(34) &= (123)(234),\\ (12)(23) &= (123),\\ (12)(12) &= e.\end{aligned}$$

Therefore, every element in A_n is a 3-cycle of a product of three cycles.

■

5.66* Show that for $n \geq 3$, $Z(S_n) = \{e\}$.

提示.

- **Lemma:** Every permutation can be written as a product of disjoint cycles
- Suppose that $e \neq \sigma \in S_n$. By Lemma, $\sigma = \gamma_1\gamma_2\cdots\gamma_m$. W.L.O.G., if $\gamma_1 = (123\cdots)$, then $\sigma(12) \neq (12)\sigma$, a contradiction.
  If $\gamma_1\gamma_2 = (12)(34)$, then $\sigma(23) \neq (23)\sigma$.
  If $\sigma = (12)$, then ...

Proof. Suppose that $e \neq \sigma \in S_n$. Decomposite σ into a product of disjoint cycles, write $\sigma = \gamma_1\gamma_2\cdots\gamma_m$.

Case I: $\gamma_1 = (123\cdots)$. Then $\sigma(12) \neq (12)\sigma$ and $\sigma \notin Z(S_n)$.

Case II: $\gamma_1\gamma_2 = (12)(34)$. Then $\sigma(23) \neq (23)\sigma$ and $\sigma \notin Z(S_n)$.

Case III: $\sigma = (12)$. Then $\sigma(123) \neq (123)\sigma$ and $\sigma \notin Z(S_n)$. ■

5.69 Prove that every element of S_n $(n > 1)$ can be written as a product of elements of the form $(1k)$.

提示. Note that if $C = (c_1c_2\cdots c_t)$, then

$$\begin{aligned} C &= (c_1c_2\cdots c_t) \\ &= (1c_1)(1c_1)(c_1c_2\cdots c_t) \\ &= (1c_1)(1c_1c_2\ldots c_t) \\ &= (1c_1)(1c_t)(1c_{t-1})\cdots(1c_2)(1c_1) \end{aligned}$$

Suppose that $\beta \in S_n$. By Theorem 5.1, we can write β as a product of k disjoint cycles of lengths $n_1, n_2, \ldots, n_k$, respectively. That is,

$$\beta = C_1C_2\cdots C_k = (c_{11}c_{12}\cdots c_{1n_1})(c_{21}c_{22}\cdots c_{2n_2})\cdots(c_{k1}c_{k2}\cdots c_{kn_k}).$$

Then

$$\beta = (1c_{11})(1c_{1n_1})\cdots(1c_{12})(1c_{11})\cdots(1c_{k1})(1c_{kn_k})\cdots(1c_{k2})(1c_{k1}).$$

5.77* Why does the fact that the orders of the elements of A_4 are 1, 2, and 3 imply that $|Z(A_4)| = 1$?

提示. ~~If $ab = ba \neq e$, then $|ab| = \text{l.c.m.}(|a|, |b|)$.~~ Suppose that $e \neq a \in Z(A_4)$ and $|a| = 3$. Then pick $b \in A_4$ such that $ab \neq e$ and $|b| = 2$. We have $|ab| = \text{l.c.m.}(|a|, |b|) = 6$, a contradiction.

Proof.

Lemma 1: If $|a|$ and $|b|$ are two distinct prime, then $\langle a\rangle \cap \langle b\rangle = \{e\}$.

Proof of Lemma 1: Suppose that $c \in \langle a\rangle \cap \langle b\rangle$. By Lagrange's Theorem, $|c|$ divide $|a|$ and $|b|$. Since $|a|$ and $|b|$ are relatively prime, we have $|c| = 1$ and $c = e$.

Lemma 2: If $ab = ba$ and $\langle a\rangle \cap \langle b\rangle = \{e\}$, then $|ab| = \text{l.c.m.}(|a|, |b|)$.

Proof of Lemma 2:

$$\begin{aligned} & \text{If } (ab)^r = e \\ \Rightarrow\ & e = (ab)^r \overset{\overset{ab=ba}{\downarrow}}{=} a^rb^r \\ \Rightarrow\ & a^r = b^{-r} \in \langle a\rangle \cap \langle b\rangle = \{e\} \\ \Rightarrow\ & a^r = b^{-r} = e \\ \Rightarrow\ & a^r = b^r = e \\ \Rightarrow\ & |a| \text{ divide } r \text{ and } |b| \text{ divide } r \\ \Rightarrow\ & r \text{ is a common multiple of } |a| \text{ and } |b| \\ \Rightarrow\ & \text{the least common multiple of } |a| \text{ and } |b| \text{ is the order of } ab. \end{aligned}$$

Proof of the Problem: If $e \neq c \in Z(A_4)$, pick an element $g \in Z(A_4)$ such that $g \neq e$ and $|g| \neq |c|$. One can write down all the elements of A_4. Then conclude that such element g must exists. Since $|g| \neq |c| \in \{2, 3\}$, by Lemma 1, we have $\langle g\rangle \cap \langle c\rangle = \{e\}$. Since $c \in Z(A_4)$, by Lemma 2, we have $|gc| = \text{l.c.m.}(|g|, |c|) = 6 \notin \{1, 2, 3\}$, a contradiction.

原解法有誤: ~~If $ab = ba \neq e$, then $|ab| = \text{l.c.m.}(|a|, |b|)$.~~ Suppose that $e \neq a \in Z(A_4)$ and $|a| = 3$. Then pick $b \in A_4$ such that $ab \neq e$ and $|b| = 2$. We have $|ab| = \text{l.c.m.}(|a|, |b|) = 6$, a contradiction. ■

補充 5.A 加法與乘法的陷阱

- $3 \in \mathbb{Z}_7,\ 3 \cdot 5 = 15 = 1,$ so $3^{-1} = 5$.
- $2^3 = 8 = 0 \in \mathbb{Z}_8$, $|2| = 3$?
- In $U(9)$, $\langle 2 \rangle =$?
- In $\mathbb{Z}_9$, $\langle 2 \rangle =$?
- $3 \in \mathbb{Z}_7,\ 3 = \underline{3},\ 3^2 = 9 = \underline{2},\ 3^3 = \underline{6},\ 3^4 = \underline{4},\ 3^5 = \underline{5},\ 3^6 = \underline{1},$ so $|3| = 6$.

補充 5.B Calculate all conjugacy classes for the groups S_3, S_4, D_4, D_5, A_4 and Q_8.

Proof.

- In S_3,

$$\begin{aligned} \text{orbit}(e) &= \{e\}, \\ \text{orbit}((12)) &= \{(12),(13),(23)\}, \\ \text{orbit}((123)) &= \{(123),(132)\}. \end{aligned}$$

In S_4,

$$\begin{aligned} \text{orbit}(e) &= \{e\}, \\ \text{orbit}((12)) &= \{(12),(13),(14),(23),(24),(34)\}, \\ \text{orbit}((123)) &= \{(123),(132),(124),(142),(134),(143),(234),(243)\}, \\ \text{orbit}((1234)) &= \{(1234),(1243),(1324),(1342),(1423),(1432)\}, \\ \text{orbit}((12)(34)) &= \{(12)(34),(13)(24),(14)(23)\}. \end{aligned}$$

Lemma: In S_n, two permutations are conjugate if and only they have the same cyclic structure.

Proof of Lemma: $(\Rightarrow)$ By cycle decomposition theorem, any permutation σ can be writed as a product of some disjoint cycles. That is, $\sigma = \gamma_1\gamma_2\cdots\gamma_m$ for some cycles γ_1, γ_2, ..., γ_m. Consider a conjugate $g\sigma g^{-1}$ of σ. Then

$$g\sigma g^{-1} = g\gamma_1\gamma_2\cdots\gamma_m g^{-1} = g\gamma_1 g^{-1} \cdot g\gamma_2 g^{-1} \cdots g\gamma_m g^{-1}.$$

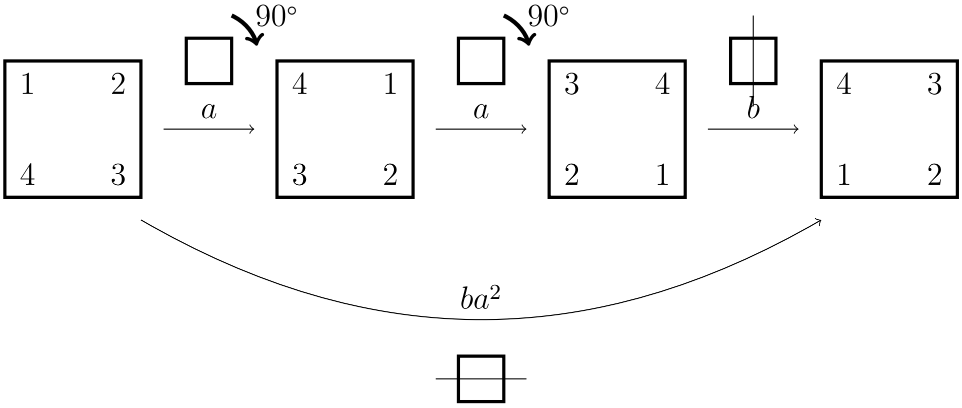
W.L.O.G., suppose that $\gamma_1 = (ij\cdots)$. Then $g\gamma_1 g^{-1} = g(ij\cdots)g^{-1} = (g(i)\ g(j)\cdots)$. You can verify the last identity directly by compute $g(ij\cdots)g^{-1}(g(i))$.

$(\Leftarrow)$ If two cycles $\gamma = (ij\cdots)$ and $\gamma' = (kl\cdots)$ have the same cycle structure, then let σ be the permutation such that $\sigma(i) = k$, $\sigma(j) = k$, ... Then $\sigma\gamma\sigma^{-1} = (\sigma(i)\ \sigma(j)\cdots) = (kl\cdots) = \gamma'$. That is, γ and γ' are conjugate.

- In $D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3 \mid |a| = 4, |b| = 2, aba = b\}$,

$$\begin{aligned} \text{orbit}(1) &= \{1\}, \\ \\ \text{orbit}(a) &= \{a,\quad a^3\}, \\ \\ \text{orbit}(a^2) &= \{a^2\}, \\ \\ \text{orbit}(b) &= \{b,\quad ba^2\}, \\ \\ \text{orbit}(ba) &= \{ba,\quad ba^3\}. \end{aligned}$$

This is an example which shows that how to know the geometric interpretation of an element in D_n.



注意, 函數的計算是從右到左。

In $D_5 = \{1, a, a^2, a^3, a^4, b, ba, ba^2, ba^3, ba^4 \mid |a| = 5, |b| = 2, aba = b\}$,

$$\begin{aligned}
\text{orbit}(1) &= \{1\}, \\
\text{orbit}(a) &= \{a,\ \ a^4\}, \\
\text{orbit}(a^2) &= \{a^2,\ \ a^3\}, \\
\text{orbit}(b) &= \{b,\ \ ba,\ \ ba^2,\ \ ba^3,\ \ ba^4\}.
\end{aligned}$$

Note that in D_n, two elements in the same conjugacy class if and only if they are the same type of symmetry.
助教強烈建議您將 D_n 中的每個conjugacy class 中的每一個元素所代表的幾何變換標示在它旁邊, 並觀察同一個conjugacy class 中的元素的幾何變換有何關係。

- In A_4,

$$\begin{aligned}
\text{orbit}(e) &= \{e\}, \\
\text{orbit}((123)) &= \{(123), (134), (142), (243)\}, \\
\text{orbit}((132)) &= \{(132), (124), (143), (234)\}, \\
\text{orbit}((12)(34)) &= \{(12)(34), (13)(24), (14)(23)\}.
\end{aligned}$$

Note that in A_n, two permutations have the same cycle structure are not necessarily in the same conjugacy class.

- The conjugacy classes of Q_8 see the next Exercise.

■

補充. 助教提醒您, 要會算, 不要只是強記, 小考也會考一點計算。

補充 5.C Let G be any group. Prove that the map from G to itself defined by $g \to g^2$ is a group homomorphism if and only if G is abelian.

Proof. Let θ be the mapping from G to itself defined by $g \to g^2$. For any $a, b \in G$,

$$\begin{aligned} & \theta(ab) = \theta(a)\theta(b) \\ \Leftrightarrow\ & (ab)^2 = a^2b^2 \\ \Leftrightarrow\ & abab = aabb \\ \Leftrightarrow\ & ba = ab. \end{aligned}$$

■

6 Chapter 6

6.2 Find $\mathrm{Aut}(\mathbb{Z})$.

提示. Suppose that $\theta \in \mathrm{Aut}(\mathbb{Z})$. Since θ is onto, suppose that $\theta(n) = 1$. Then

$$1 = \theta(n) \overset{\overset{\theta \text{ is a homomorphism}}{\downarrow}}{=} n\theta(1)$$

and $\theta(1) \in \{1, -1\}$.

6.3 Let $\mathbb{R}^+$ be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbb{R}^+$.

6.4 Show that $U(8)$ is not isomorphic to $U(10)$.

提示. Observe the order of each element.

Proof. $U(10) = \{1, 3, 7, 9\}$ has an element of order 4, but $U(8) = \{1, 3, 5, 7\}$ doesn't have such element. ■

6.5 Show that $U(8)$ is isomorphic to $U(12)$, where $U(n)$ is a group under multiplication modulo n.

Proof. You can construct a mapping $\theta : U(8) \to U(12)$ defined by $\theta(3) = 5$ and $\theta(5) = 7$. Then verify θ is an isomorphism.

Another way is note that there are only two groups of order 4 up to isomorphism. That is, the cyclic group of order 4 and the Klein four group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. $U(8)$ and $U(12)$ both have no element of order 4, That is, they are not cyclic group. Therefore, $U(8) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong U(12)$. ■

6.7 Prove that S_4 (symmetric group of degree 4) is not isomorphic to D_{24} (dihedral group of order 24).

Proof. 姜〇珽同學的解法: Since $Z(S_4) = \{e\}$ and $Z(D_{24}) = \{1, a^6\}$, we get $|Z(S_4)| = 1 \neq 2 = |Z(D_{24})|$ and $S_4 \ncong D_{24}$.

There are exactly 9 elements of order 2 in S_4. They are

$$\begin{array}{ll} (12), & (12)(34), \\ (13), & (13)(24), \\ (14), & (14)(23). \\ (23), & \\ (24), & \\ (34), & \end{array}$$

But there are exactly 13 elements of order 2 in $D_{24} = \{\langle a, b\rangle \mid |a| = 12, |b| = 2, ab = ba^{-1}\}$. They are a^6 and ba^i, where $i = 0, 1, 2, ..., 11$. ■

6.8 Show that the mapping $a \to \log_{10} a$ is an isomorphism from $\mathbb{R}^+$ under multiplication to $\mathbb{R}$ under addition.

6.9 In the notation of Theorem 6.1, prove that T_e is the identity and that $(T_g)^{-1} = T_{g^{-1}}$.

提示. $T_{g^{-1}} T_g = T_{g^{-1}g} = T_e$ and by p.51, thm.2.3.

6.10 Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is abelian.

6.15 If G is a group, prove that $\text{Aut}(G)$ and $\text{Inn}(G)$ are groups.

6.18 Let H be the subgroup of all rotations in D_n and let ϕ be an automorphism of D_n. Prove that $\phi(H) = H$. (In words, an automorphism of D_n carries rotations to rotations.)

提示. For any automorphism of D_n, we show that $\phi(a) \in \langle a\rangle$. If $\phi(a) = ba^i$ for some $i \in \mathbb{Z}$, then $\phi(a^2) = [\phi(a)]^2 = (ba^i)^2 = 1 = \phi(1)$. Since ϕ is one-to-one, we get $a^2 = 1$. Which is impossible because $|a| = n \geq 3$ (c.f. p.34, the definition of the dihedral group).

6.25 Identify a group G that has subgroups isomorphic to $\mathbb{Z}_n$ for all positive integers n.

提示. $\{z \in \mathbb{C} \mid |z| = 1\}$.

6.27 Let $r \in U(n)$. Prove that the mapping $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\alpha(s) = sr \pmod n$ for all s in $\mathbb{Z}_n$ is an automorphism of $\mathbb{Z}_n$.

6.31 Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Show that ϕ^{-1} is an isomorphism from $\overline{G}$ onto G.

6.32 Prove property 4 of Theorem 6.3. Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then if K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

Proof.

- **Closed:**

$$\phi(k_1), \phi(k_2) \in \phi(K), k_1, k_2 \in K \overset{\overset{K \leq G}{\downarrow}}{\Rightarrow} k_1 k_2 \in K \Rightarrow \phi(k_1)\phi(k_2) \overset{\overset{\phi \text{ is a homomorphism}}{\downarrow}}{=} \phi(k_1 k_2) \in \phi(K).$$

- **Identity:** For any $\overline{x} \in \overline{G}$, since ϕ is onto, there exists $x \in G$ such that $\phi(x) = \overline{x}$. Thus, $\overline{x}\phi(e_G) = \phi(x)\phi(e_G) = \phi(xe_G) = \phi(x) = \overline{x}$. Similarly, $\phi(e_G)\overline{x} = \overline{x}$. That is, $\phi(e_G) = e_{\overline{G}}$.
$$K \leq G \Rightarrow e_G \in K \Rightarrow e_{\overline{G}} = \phi(e_G) \in \phi(K).$$
- **Inverse:** Since $\phi(k)\phi(k^{-1}) = \phi(kk^{-1}) = \phi(e_G) = e_{\overline{G}} = \phi(k^{-1})\phi(k)$, by the uniqueness of inverse in a group (p.51, thm.2.3), $\phi(k^{-1}) = \phi(k)^{-1}$.

$$\phi(k) \in \phi(K), k \in K \Rightarrow \phi(k)^{-1} = \phi(k^{-1}) \overset{K \leq G,\ k^{-1} \in K}{\overset{\downarrow}{\in}} \phi(K).$$

■

6.33 Referring to Theorem 6.1, prove that T_g is indeed a permutation on the set G.

提示. Show that T_g is one-to-one and onto.

6.35 Show that the mapping $\phi(a+bi) = a-bi$ is an automorphism of the group of complex numbers under addition. Show that ϕ preserves complex multiplication as well (i.e. $\phi(xy) = \phi(x)\phi(y)$ for all x and y in $\mathbb{C}$).

6.39 Let $\mathbb{C}$ be the complex numbers and

$$M = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}.$$

Prove that $\mathbb{C}$ and M are isomorphic under addition and that $\mathbb{C}^*$ and M^*, the nonzero elements of M, are isomorphic under multiplication.

6.42 Suppose that G is a finite abelian group and G has no element of order 2. Show that the mapping $g \to g^2$ is an automorphism of G. Show, by example, that if G is infinite the mapping need not be an automorphism.

Proof. Let ϕ be the mapping on G defined by $\phi(g) = g^2$. Since G has no element of order 2, the kernel of ϕ is

$$\ker \phi = \{g \in G \mid \phi(g) = e\} = \{e\}.$$

Thus, ϕ is one-to-one. Since ϕ is a one-to-one mapping on G and G is finite, we have ϕ is onto. We show that ϕ is a homomorphism. For any $g_1, g_2 \in G$,

$$\phi(g_1g_2) = (g_1g_2)^2 \overset{G \text{ abelian}}{\overset{\downarrow}{=}} g_1^2g_2^2 = \phi(g_1)\phi(g_2).$$

In the case $G = \mathbb{Z}$, ϕ is defined by $\phi(m) = 2m$. ϕ is not onto because an odd number 1 in $\mathbb{Z}$ has no preimage in $\mathbb{Z}$ under ϕ. ■

6.43 Let G be a group and let $g \in G$. If $z \in Z(G)$, show that the inner automorphism induced by g is the same as the inner automorphism induced by zg (that is, that the mappings ϕ_g and ϕ_{zg} are equal).

Proof. For all $a \in G$,

$$\phi_{zg}(a) = (zg)a(zg)^{-1} = zgag^{-1}z^{-1} \overset{z \in Z(G)}{\overset{\downarrow}{=}} gag^{-1}zz^{-1} = gag^{-1} = \phi_g(a).$$

■

6.45 Suppose that g and h induce the same inner automorphism of a group G. Prove that $h^{-1}g \in Z(G)$.

Proof. For all $a \in G$,

$$\begin{aligned}(h^{-1}g)a &= (h^{-1}g)a \cdot e \\ &= h^{-1}ga(g^{-1}g) \\ &= h^{-1}(gag^{-1})g \\ &= h^{-1}\phi_g(a)g \\ &= h^{-1}\phi_h(a)g \\ &= h^{-1}(hah^{-1})g \\ &= (h^{-1}h)ah^{-1}g \\ &= a(h^{-1}g).\end{aligned}$$

■

6.48 let ϕ be an isomorphism from a group G to a group $\overline{G}$ and let a belong to G. Prove that $\phi(C(a)) = C(\phi(a))$.

Proof. ($\subseteq$)

$$\begin{aligned} & y \in \phi(C(a)) \\ \Rightarrow\ & y = \phi(x), x \in C(a) \\ \Rightarrow\ & y = \phi(x), xa = ax \\ \Rightarrow\ & y\phi(a) = \phi(x)\phi(a) \overset{\phi \text{ is a homomorphism}}{\overset{\downarrow}{=}} \phi(xa) = \phi(ax) = \phi(a)\phi(x) = \phi(a)y \\ \Rightarrow\ & y \in C(\phi(a))\end{aligned}$$

($\supseteq$) Suppose that $y \in C(\phi(a))$. Then $y\phi(a) = \phi(a)y$. On the other hand, since ϕ is onto, assume that $\phi(x) = y$. Then

$$\begin{aligned} & \phi(x)\phi(a) = y\phi(a) = \phi(a)y = \phi(a)\phi(x) \\ \Rightarrow\ & \phi(xa) = \phi(x)\phi(a) = \phi(a)\phi(x) = \phi(ax) \\ \overset{\phi \text{ is one-to-one}}{\overset{\downarrow}{\Rightarrow}}\ & xa = ax \\ \Rightarrow\ & x \in C(a) \\ \Rightarrow\ & y = \phi(x) \in \phi(C(a))\end{aligned}$$

■

6.53 Let a belong to a group G and let $|a|$ be finite. Let ϕ_a be the automorphism of G given by $\phi_a(x) = axa^{-1}$. Show that $|\phi_a|$ divides $|a|$. Exhibit an element a from a group for which $1 < |\phi_a| < |a|$.

提示. P.79, cor.2. D_4.

Proof. $(\phi_a)^{|a|} = \phi_{a^{|a|}} = \phi_e$, note that ϕ_e is the identity map on G, or says, the identity in the group $\overline{G} = \{\phi_g \mid g \in G\}$. Thus, $|\phi_a|$ divides $|a|$ by p.79, cor.2.

Cosider $a \in D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3 \mid |a| = 4, |b| = 2, ab = ba^{-1}\}$ and $\phi_a(a) = aaa^{-1} = a \neq 1$. Thus, $\phi_a \neq \phi_1$. For any $x \in D_4$,

$$(\phi_a)^2(x) = \phi_{a^2}(x) = \begin{cases} a^2a^i(a^2)^{-1} = a^i = x & \text{if } x = a^i; \\ a^2(ba^i)(a^2)^{-1} = (a^2b)a^ia^{-2} = (ba^{-2})a^ia^{-2} = ba^i = x & \text{if } x = ba^i. \end{cases}$$

Therefore, $(\phi_a)^2 = \phi_1$ and $1 < |\phi_a| = 2 < 4 = |a|$. ■

補充. 這些部分有點難, 我們以後學 group action 的時候會再詳細討論。

p.183,37 Prove or disprove that $D_{12} \cong \mathbb{Z}_3 \oplus D_4$.

Proof. D_{12} has 13 elements of order 2, but $\mathbb{Z}_3 \oplus D_4$ only has 5 elements of order 2. Thus, $D_{12} \ncong \mathbb{Z}_3 \oplus D_4$. ■

補充 6.A If a and g are elements of a group, prove that $C_G(a)$ is isomorphic to $C_G(gag^{-1})$.

提示. If you want to construct a function $f : C_G(a) \to C_G(gag^{-1})$, then you should prove that f is well-defind. That is, for all $b \in C_G(a)$, $f(b) \in C_G(gag^{-1})$.

Proof. We define a function $f : C_G(a) \to C_G(gag^{-1})$ by $f(h) = ghg^{-1}$.

$$\begin{aligned} & h \in C_G(a) \\ \Rightarrow\ & ha = ah \\ \Rightarrow\ & f(h)(gag^{-1}) = (ghg^{-1})(gag^{-1}) = gh(g^{-1}g)ag^{-1} \\ & = g(ha)g^{-1} = g(ah)g^{-1} = (gag^{-1})(ghg^{-1}) = (gag^{-1})f(h) \\ \Rightarrow\ & f(h) \in C_G(gag^{-1}). \end{aligned}$$

Thus, f is well-define. ■

7 Chapter 7

7.1 Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4 (see Table 5.1 on page 111).

Proof.

$$\begin{aligned} H &= \{e, (12)(34), (13)(24), (14)(23)\}, \\ (123)H &= \{(123), (134), (243), (142)\}, \\ (132)H &= \{(132), (143), (234), (124)\}. \end{aligned}$$

■

7.2 Let H be as in Exercise 7.1. How many left cosets of H in S_4 are there? (Determine this without listing them.)

Proof. $[S_4 : H] = |S_4|/|H| = 24/4 = 6$. ■

7.6 Let n be a positive integer. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$. Find all left cosets of H in $\mathbb{Z}$. How many are there?

Proof. $H, 1 + H, 2 + H, \ldots, (n-1) + H$. ■

7.7 Find all of the left cosets of $\{1, 11\}$ in $U(30)$.

Proof. $\{1, 11\}, \{7, 17\}, \{13, 23\}, \{19, 29\}$. ■

7.10 Give an example of a group G and subgroups H and K such that $HK = \{h \in H, k \in K\}$ is not a subgroup of G.

提示. S_3.

Proof. Let $H = \langle(123)\rangle$, $K = \langle(12)\rangle \le S_3$. Then $HK = \{e, (123), (12), (13)\}$ and $(123)^2 \notin HK$. ■

7.11 If H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$.

提示. ($\supseteq$) If $gh = gk \in gH \cap gK$, then $h = k$.

7.12 Lt a and b be nonidentity elements of different orders in a group G of order 155. Prove that the only subgroup of G that contains a and b is G itself.

Proof. Suppse that $\{a, b\} \subseteq H \le G$. If $|a| = 155$ or $|b| = 155$, then $H = G$. So we assume $|a| = 5$ and $|b| = 31$. Then by Lagrange's Theorem, $|a|$ divides $|H|$ and $|b|$ divides $|G|$. Since $\gcd(|a|, |b|)$, by Exercise 0.6, $155 = 5 \cdot 31 = |a| \cdot |b|$ divides $|H|$ and $H = G$. ■

7.13 Let H be a subgroup of $\mathbb{R}^*$, the group of nonzero real numbers under multiplication. If $\mathbb{R}^+ \subseteq H \subseteq \mathbb{R}^*$, prove that $H = \mathbb{R}^+$ or $H = \mathbb{R}^*$.

提示.

$$\overbrace{\mathbb{R}^+ \underbrace{\le}_{?} H \underbrace{\le}_{?} \mathbb{R}^*}^{?}.$$

7.14 Let $\mathbb{C}^*$ be the group of nonzero complex numbers under multiplication and let $H = \{a + bi \in \mathbb{C}^* \mid a^2 + b^2 = 1\}$. Give a geometric description of the coset $(3 + 4i)H$. Give a geometric description of the coset $(c + di)H$.

Proof. The circle with radius $\sqrt{3^2 + 4^2} = 5$ on the complex plane. ■

7.18 Recall that, for any integer n greater than 1, $\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)} \pmod{n} = 1$.

提示. Apply Lagrange's Theorem on $U(n)$.

7.20 Use Corollary 2 of Lagrange's Theorem (Theorem 7.1) to prove that the order of $U(n)$ is even when $n > 2$.

提示. $(-1) \neq 1 \in U(n)$ when $n > 2$.

Proof. By Lagrange's Theorem, $|-1| = 2$ divides $U(n)$. ■

7.23* Suppose that H is a subgroup of S_4 and that H contains (12) and (234). Prove that $H = S_4$.

提示.

(a) Note that $(234) \in H$ and $3 = |(234)|$, by Lagrange's Theorem, 3 divide ____

(b) Note that $(1234) = (12)(234) \in H$ and $4 = |(12)(234)| = |(1234)|$, by Lagrange's Theorem, 4 divide ____

(c) Recall that if $a \mid c$ and $b \mid c$ and $\gcd(a,b) = 1$, then $ab \mid c$. Thus, ____ divide $|H|$.

(d) In addition, by Lagrange's Theorem, $|H|$ divide $|G|$. Thus, $|H| \in \{$____$, 24\}$.

(e) If $|H| = 12$, then $H =$ ____. But $(12) \in H$, a contradiction.

(f) Therefore, $|H| = 24$ and $H =$ ____.

Proof. Note that $3 = |(234)|$ divide $|H|$ and $4 = |(12)(234)| = |(1234)|$ divide $|H|$. Recall that if $a \mid c$ and $b \mid c$ and $\gcd(a,b) = 1$, then $ab \mid c$. Thus, 12 divide $|H|$. But $(12) \in H$ implies that $H \neq A_4$. Therefore, $H = S_4$. ■

7.24* Suppose that H and K are subgroups of G and there are elements a and b in G such that $aH \subseteq bK$. Prove that $H \subseteq K$.

提示.

(a) 我們想要證明 $H \subseteq K$。也就是對於所有的 $h \in H$, 我們要證明 ________.

(b) 但是我們只有這個條件 $aH \subseteq bK$, 爲了讓這個條件派上用場, 我們要想辦法湊出具有 ah 這個形式的元素, 這樣一來就可以得到 $ah = bk$ for some $k \in K$。所以

$$h = (a^{-1}a)h = a^{-1}(ah) = a^{-1}(b\underline{\hspace{2em}})$$

(c) 我們的目標是證明 $h = a^{-1}(b\underline{\hspace{2em}}) \in K$, 我們已經知道 ____ $\in K$ 了, 但是我們不知道 $a^{-1}b$ 是不是也屬於 K。

(d) 讓我們想想, (這有點 tricky,) 我們取 $1 \in H$, 則 $a \cdot 1 \in aH \subseteq$ ____, 所以 $a =$ ____, 且 $a^{-1}b =$ ____ $\in K$。

Proof. Note that $a{\cdot}1 \in bK$ and $a{\cdot}1 = bk$ for some $k \in K$. It follows that $a^{-1}b = k^{-1} \in K$. For all $h \in H$,

$$h = (a^{-1}a)h = a^{-1}(ah) \overset{aH\subseteq bK}{\overset{\downarrow}{=}} a^{-1}(bk') = (a^{-1}b)k' = kk' \in K.$$

That is, $H \subseteq K$. ■

7.26 Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)

提示. Let $g \neq e \in G$. Consider $\langle g \rangle$.

Proof. Let $g \neq e \in G$. Then $\langle g \rangle = G$. That is, G is cyclic. By the Fundamental Theorem of Cyclic Group, for each divisor d of $|G|$, there exists a unique subgroup of order d. But there are only two subgroups of G, $\{e\}$ and G. Hence, $|G|$ is prime. ■

7.27 Let $|G| = 15$. If G has only one subgroup of order 3 and only one of order 5, prove that G is cyclic. Generalize to $|G| = pq$, where p and q are prime.

提示.

(a) Let H and K be the only one subgroup of G which is of order 3 and 5, respectively.

(b) By the Corollary of The Lagrange's Theorem, $H \cap K = \_\_\_\_$. Hence, $|H \cup K| = \_\_\_\_$.

(c) Pick an element $e \neq g \in G$, $g \notin H \cup K$. By Lagrange's Theorem, $|g|$ divide $|G| = \_\_\_\_$. Thus, $|g| \in \{3, \_\_\_\_, \_\_\_\_\}$.

(d) If $|g| = 3$, then $\langle g \rangle$ is another subgroup of order ____ distinct from H, contrary to the uniqueness of ____.

(e) If $|g| = 5$, then ...

(f) Therefore, $|g| = \_\_\_\_$ and $G = \langle \_\_\_\_ \rangle$.

Proof. Let H and K be the only one subgroup of G which is of order 3 and 5, respectively. By Lagrange's Theorem, $|H \cap K| = 1$ and $H \cap K = \{e\}$. Hence $|H \cup K| = 7$. Since $|G| = 15 > 7$, we can pick an element $g \in G$ such that $e \neq g \notin H \cup K$. By the Lagrange's Theorem, $|g| \in \{3, 5, 15\}$. If $|g| = 3$, then $\langle g \rangle$ is another subgroup of order 3 distinct from H, contrary to the uniqueness of H. Similarly, $|g| \neq 5$. Therefore, $|g| = 15$ and G is a cyclic group generated by g. ■

7.28 Let G be a group of order 25. Prove that G is cyclic or $g^5 = e$ for all g in G. Generalize to any group of order p^2 where p is prime. Does your proof work for this generalization?

Proof. By Lagrange's Theorem, any nonidentity element in G is of order 5 or 25. If there exists $g \in G$ such that $|g| = 25$, then G is cyclic. If G is not cyclic, then for any nonidentity element g in G, we have $|g| = 5$. ■

7.31* Can a group of order 55 have exactly 20 elements of order 11? Give a reason for your answer.

提示.

(a) If there are exactly 20 elements of order 11, then suppose that $a \in G$ and $|a| = 11$.

(b) By Lagrange's Theorem, the element in $\langle a \rangle$ except e is of order ____.

(c) Pick $b \notin \langle a \rangle$ and $|b| = 11$.

(d) If $c \in \langle a \rangle \cap \langle b \rangle$, then by Lagrange's Theorem, $|c| \in \{1, \underline{\quad\quad}\}$.

(e) If $|c| = 11$, then $\langle a \rangle = \langle \underline{\quad\quad} \rangle = \langle b \rangle$, a contradiction.

(f) Thus, $\langle a \rangle \cap \langle b \rangle =$ ____.

(g) The number of elements of order 11 in $\langle a \rangle \cup \langle b \rangle$ is ____.

Proof. No such group exists. We prove the assertion by contradiction. Suppose that G is a group of order 55 and have exactly 20 elements of order 11.

By Lagrange's Theorem, If $g \in G$, then $|g|$ divide $|G| = 55$ and $|g| \in \{1, 5, 11, 55\}$.

If there exists an element g of order 55, then G is a cyclic group. In this case, $G = \langle g \rangle$. Then $g^5, g^{10}, g^{15}, g^{20}, \ldots, g^{50}$, these 10 elements are all the element in G which is of order 11, a contradiction.

Suppose that there is no element in G with order 55. Then for all $g \in G$, $|g| \in \{1, 5, 11\}$. Suppose that $a \in G$ and $|a| = 11$. All the elements in $\langle a \rangle$ except e is of order 11. Pick $b \notin \langle a \rangle$ and $|b| = 11$. If $e \neq c \in \langle a \rangle \cap \langle b \rangle$, then by Lagrange's Theorem, $|c| = 11$ and $\langle a \rangle = \langle c \rangle = \langle b \rangle$, a contradiction. Thus, $\langle a \rangle \cap \langle b \rangle = \{e\}$ and $\langle a \rangle \cup \langle b \rangle - \{e\}$ exhaust all the 20 elements of order 11.

Then there are $|G| - |\langle a \rangle \cup \langle b \rangle| = 55 - 21 = 34$ elements whose ordre is 5. Note that if $g_1 \neq g_2$ are two distinct elements of order 5, then $\langle g_1 \rangle$ contains 4 elements of order 5 and $\langle g_1 \rangle \cap \langle g_2 \rangle = \{e\}$. But 4 does not divide 34. Thus, it is impossible that there are 34 elements of order 5. ■

7.33 Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $[G : H] = [G : K] \cdot [K : H]$.

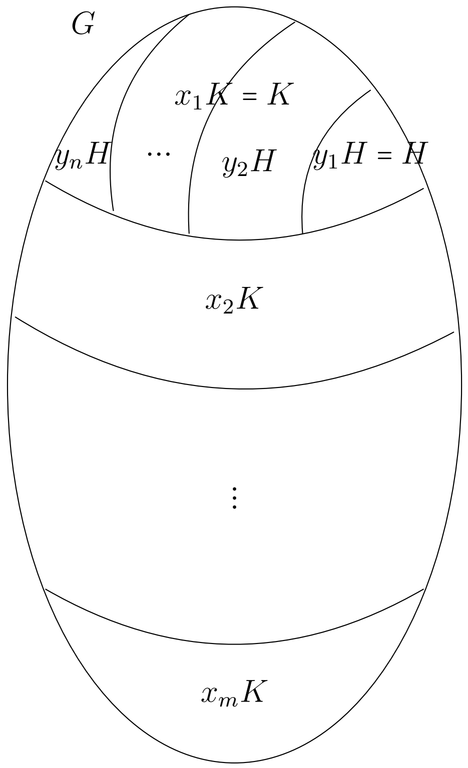
補充. 這個定理太重要了, 重要到無法言喻。簡單來說, 就是如果我們有一個 subgroup tower, $H \le K \le G$, 那麼中間的兩個 index 相乘會等於頭尾的 index, 也就是

$$\overbrace{H \underbrace{\le}_{n} K \underbrace{\le}_{m} G}^{nm}.$$

這個定理不一定要求要 finite group, 只要 index 是 finite 就好, 也就是說,

$$[G : H] < \infty \Leftrightarrow [G : K] < \infty \text{ and } [K : H] < \infty.$$

Proof. ($\Leftarrow$) Suppose that $[G : K] = m$ and $[K : H] = n$. Let $G = \bigcup_{i=1}^{m} x_i K$ and $x_k K \cap x_l K = \varnothing$ when $k \neq l$. Let $K = \bigcup_{j=1}^{n} y_j H$ and $y_s H \cap y_t H = \varnothing$ when $s \neq t$. We show that $G = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} x_i y_j H$ and $x_i y_j H \neq x_u y_v H$ if $i \neq u$ or $j \neq v$, as the following figure indicates.



$$G = \bigcup_{i=1}^{m} x_iK = \bigcup_{i=1}^{m} x_i \left(\bigcup_{j=1}^{n} y_jH \right) = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} x_iy_jH.$$

$$\begin{array}{cl}
\text{If} & x_iy_jH = x_uy_vH \\
\Rightarrow & y_v^{-1}x_u^{-1}x_iy_j \in H \le K \\
\Rightarrow & x_u^{-1}x_i \in K \\
\Rightarrow & x_uK = x_iK \\
\overset{G=\bigcup_{i=1}^{m} x_iK}{\overset{\downarrow}{\Rightarrow}} & x_u = x_i \text{ and } i = u \\
\overset{x_iy_jH=x_uy_vH}{\overset{\downarrow}{\Rightarrow}} & y_jH = y_vH \\
\overset{K=\bigcup_{j=1}^{n} y_jH}{\overset{\downarrow}{\Rightarrow}} & y_j = y_v \text{ and } j = v
\end{array}$$

■

7.38 Prove that if G is a finite group, the index of $Z(G)$ cannot be prime.

提示. P.194, thm.9.3.

Proof. **Lemma:** If $[G : Z(G)]$ is prime, then G is abelian.

Proof of Lemma: If $[G : Z(G)] = p$ and G is not abelian, then there exists $a, b \in G$ such that $ab \neq ba$. Consider the tower of groups

$$\overbrace{Z(G) \le C(a,b) \le C(a) \le G}^{p},$$

where $C(S) = \{g \in G \mid gs = sg \text{ for all } s \in S\}$ is the centralizer of S. If $S = \{a_1, a_2, ..., a_n\}$, then we write $C(S)$ as $C(a_1, a_2, ..., a_n)$ instead of $C(\{a_1, a_2, ..., a_n\})$. Since there exists $b \in G$, $ba \neq ab$, we have $C(a) \neq G$ and $[G : C(a)] \neq 1$. Since $a \in C(a)$, $a \notin C(a, b)$, we have $C(a, b) \neq C(a)$ and $[C(a) : C(a, b)] \neq 1$. Contrary to that $[G : C(a)] \cdot [C(a) : C(a, b)]$ divides $[G : Z(G)] = p$

Proof of Exercise: If $[G : Z(G)]$ is a prime, by Lemma, G is abelian. It follows that $Z(G) = G$ and $[G : Z(G)] = 1$, a contradiction.

Advanced Method: If $[G : Z(G)]$ is prime, then by p.194, thm.9.3, G is abelian and $Z(G) = G$ and $[G : Z(G)] = 1$, a contradiction. ■

7.42 Let G be a finite abelian group and let n be a positive integer that is relatively prime to $|G|$. Show that the mapping $a \to a^n$ is an automorphism of G.

提示.

(a) Let θ be the mapping defined by $\theta : a \to a^n$.

(b) We show that θ is onto.

(c) Since $\gcd(n, |G|) = 1$, there exist $x, y \in \mathbb{Z}$ such that ________.

(d) Then

$$a = a^1 = a^{\underline{\qquad\qquad}} = a^{xn} \cdot \underline{\qquad} = \cdots$$

Proof. Let $\theta : G \to G$ be the mapping defined by $\theta(g) = g^n$. Then

$$\theta(ab) = (ab)^n \overset{G \text{ abelian}}{\overset{\downarrow}{=}} a^n b^n = \theta(a)\theta(b).$$

That is, θ is a homomorphism.

Since $\gcd(n, |G|) = 1$, suppose that $nx + |G|y = 1$. Then by Lagrange's Theorem, $a^{|G|} = e$ and

$$a = a^{nx+|G|y} = (a^x)^n \cdot (a^{|G|})^y = (a^x)^n.$$

That is, θ is onto. Which implies that θ is one-to-one. (Suppose that a function $f : A \to B$ and $|A| = |B| < \infty$. Then f is one-to-one if and only if f is onto.) ■

7.43 Let G be a group of permutations of a set S. Prove that the orbits of the members of S constitute a partition of S.

提示. $s_1 \sim s_2 \overset{\text{def.}}{\Leftrightarrow} s_1 = g(s_2)$ for some $g \in G$. Prove that "$\sim$" is an equivalence relation on S.

↓ 5.23, 7.46 Prove that a group of order 12 must have an element of order 2.

提示. Recall that a group of even order must have an element of order 2.

Proof. Recall that a group of even order must have an element of order 2. See Assignment 1 Problem 5(b). ■

7.47 Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.

Proof. Define a mapping $\theta : G \to G$ by $\theta(g) = g^2$. Then for all $a \in G$, since G is of odd order, we ave $|a^{-1}| = 2s + 1$ for some $s \in \mathbb{Z}$ and $e = (a^{-1})^{2s+1} = (a^{-s})^2 a^{-1}$ and $a = (a^{-s})^2$. Thus, θ is onto. It follows that θ is also one-to-one because its domain and its codomain are finite and has the same cardinality. (If $f : A \to B$ and $|A| = |B| < \infty$, then f is one-to-one $\Leftrightarrow$ f is onto.) ∎

7.57 Let $G = GL(2, \mathbb{R})$ and $H = SL(2, \mathbb{R})$. Let $A \in G$ and suppose that $\det A = 2$. Prove that AH is the set of all 2×2 matrices in G that have determinant 2.

8 Chapter 8

8.3 Let G be a group with identity e_G and let H be a group with identity e_H. Prove that G is isomorphic to $G \oplus \{e_H\}$ and that H is isomorphic to $\{e_H\} \oplus H$.

Proof. Define $\theta : G \to \{e_H\}$ by $\theta(g) = (g, e_H)$. Show that θ is an one-to-one and onto homomorphism (an isomorphism). ∎

8.10 How many elements of order 9 does $Z_3 \oplus Z_9$ have?

提示. 18.

Proof. There are 6 elements of order 9 in $\mathbb{Z}_9$. They are $\{1, 2, 4, 5, 7, 8\}$. Since every elements in $\mathbb{Z}_3$ is of order 1 or 3, both divide 9. Therefore, there are 18 elements of order 9 in $\mathbb{Z}_3 \oplus \mathbb{Z}_9$. They are

$$\begin{gathered}(0,1),(0,2),(0,4),(0,5),(0,7),(0,8),\\(1,1),(1,2),(1,4),(1,5),(1,7),(1,8),\\(2,1),(2,2),(2,4),(2,5),(2,7),(2,8).\end{gathered}$$

∎

8.17 If $G \oplus H$ is cyclic, prove that G and H are cyclic. State the general case.

Proof. [方法一] Suppose that $G \oplus H = \langle (g, h) \rangle$. Then for any $a \in G$, $(a, e_H) = (g, h)^m = (g^m, h^m)$ for some $m \in \mathbb{Z}$ and $a = g^m$. Hence, $G = \langle g \rangle$.

[方法二, 感謝王O鈞同學提供] Note that there is a subgroup A of $G \oplus H$ such that $G \oplus \{e_H\} \cong A \subseteq G \oplus H$. Recall that a subgroup of a cyclic is also a cyclic group. Thus, by Exercise 8.3, $G \cong G \oplus \{e_H\} \cong A$ is a cyclic group. ∎

8.22 Determine the number of elements of order 15 and the number of cyclic subgroups of order 15 in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$.

Proof. There are 48 elements in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$ whose order is 15.

$\lvert a\rvert = 3, \lvert b\rvert = 5$	$a \in \{10, 20\}, b \in \{4, 8, 12, 16\}$
$\lvert a\rvert = 15, \lvert b\rvert = 1$	$a \in \{2, 4, 8, 14, 16, 22, 26, 28\}, b \in \{0\}$
$\lvert a\rvert = 15, \lvert b\rvert = 5$	$a \in \{2, 4, 8, 14, 16, 22, 26, 28\}, b \in \{3, 6, 9, 12\}$

In a cyclic subgroup H of order 15, there are $\varphi(15) = 8$ elements of order 15 in H. (If $H = \langle h \rangle$, then $|h^r| = \frac{15}{\gcd(15,r)}$ and $\{h^r \in H \mid \gcd(15,r) = 1\} = \{h^1, h^2, h^4, h^7, h^8, h^{11}, h^{13}, h^{14}\}$ is the set of the element of order 15 in H.) Thus, there are $\frac{48}{8} = 6$ cyclic subgroups of order 15. ■

8.27 Let G be a group, and let $H = \{(g,g) \mid g \in G\}$. Show that H is a subgroup of $G \oplus G$. (This subgroup is called the diagonal of $G \oplus G$.) When G is the set of real numbers under addition, describe $G \oplus G$ and H geometrically.

Proof. Obviously, $(e_G, e_G) \in H$.

If $(a,a), (b,b) \in H$, then $(a,a) \cdot (b,b) = (ab, ab) \in H$.

If $(a,a) \in H$, the inverse of (a,a) in $G \oplus G$ is (a^{-1}, a^{-1}), which is also in H. ■

8.41 Prove that $D_3 \oplus D_4 \not\cong D_{12} \oplus Z_2$.

提示. 一般來說, 要證明兩個 group G_1 跟 G_2 是 isomorphic, 是蠻困難的, 因爲要在兩個 group G_1 跟 G_2 之間定義一個函數, 這個函數必須是 one-to-one and onto, 還必須是 homomorphism, 這樣的函數要怎麼找, 通常就是靠題目提供的線索或是一些嘗試, 當然也需要一點經驗。

我再次強調, 沒有人是一開始就知道答案的, 我們有一個想法, 就試試看, 成功了, 我幸; 失敗了, 再試。

例如作業二的最後一小題, 要證明 $C(a)$ 跟 $C(gag^{-1})$ 是isomorphic, 或許你可以造一個從 $C(a)$ 送到 $C(gag^{-1})$ 的函數, 把 h 送到 ghg^{-1}, 試試看吧。

另外, 我們要造一個 G_1 到 G_2 的 isomorphism f 時, 如果我們已經知道 G_1 的 generator 了, 我們就只要先決定這些 generator 在 f 之下的函數值就好。例如 $D_6 = \langle a, b \rangle$, 我們要證明 $D_6 \cong G_2$ 的話, 我們可以定義一個函數 f, 並且先決定 $f(a)$ 及 $f(b)$。因爲 f 必須要是一個 homomorphism, 所以 D_6 裡面的所有元素的函數值都被 generator 的函數值決定了, 例如 $f(ba^2) = f(b)f(a^2) = f(b)f(a)^2$。

另一方面, 要證明 G_1 跟 G_2 不是 isomorphic 就相對簡單了, 有同學用比較元素個數的方法來證明 G_1 跟 G_2 不是 isomorphic, 當然, 這是一個方法, 不過這個方法很弱, 你可以上這個網站看看 `http://hobbes.la.asu.edu/groups/groups.html`, 光是 order 16的 group 就有14個, 這14個 group 之間就是彼此不 isomorphic 的, 所以一般來說, 我們不會由元素個數來判斷不是 isomorphic。事實上, 你遇到的題目通常都是給你兩個 order 一樣的 group, 要你判斷他們不是 isomorphic。

那我們該怎麼證明兩個 group G_1 跟 G_2 不是 isomorphic 呢, 方法沒有固定, 但下面是一些常用的手段:

- G_1 是 abelian, 但 G_2 不是 abelian, 由此就可以知道 $G_1 \not\cong G_2$。
  例如 $\mathbb{Z}_6$ 跟 S_3。
- G_1 有一個 order 爲6的元素, 但 G_2 沒有 order 爲6的元素, 由此就可以知道 $G_1 \not\cong G_2$。
  例如 D_6 跟 A_4。
- G_1 有7個 order 爲2的元素, 但 G_2 只有3個 order 爲2的元素, 由此就可以知道 $G_1 \not\cong G_2$。
  例如 D_6 跟 A_4。

- G_1 跟 G_3 isomorphic, G_2 跟 G_4 isomorphic, 而且我們已知 G_3 跟 G_4 不是 isomorphic, 由此就可以知道 $G_1 \ncong G_2$, 簡單來說, 就是

$$G_1 \cong G_3 \ncong G_4 \cong G_2 \Rightarrow G_1 \ncong G_2.$$

例如 $U(10) \cong \mathbb{Z}_4$, $U(12) \cong K \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, 我們已知 $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, 所以 $U(10) \ncong U(12)$。

- G_1 跟 G_2 的 center 的大小不同, 由此就可以知道 $G_1 \ncong G_2$。
例如 $|Z(A_4)| = 1$, $|Z(D_6)| = 2$. 所以 $A_4 \ncong D_6$。

當然還有更多更多手段, 只要是 isomorphism 可以保持的性質, 而且 G_1 跟 G_2 在這個性質上是不同的, 那我們就可以說 G_1 跟 G_2 不是 isomorphic 了。

當然, 主要還是要依照 G_1 跟 G_2 本身具有的特性來選擇該用哪一種性質, 相信上面幾個已經夠你應付你所遇到的題目了, 老話一句, 試試看就知道了。

Proof. There are exactly 4 elements of order 12 in $D_3 \oplus D_4$. They are

$$(a,a), (a,a^3), (a^2,a) \text{ and } (a^2,a^3).$$

But there are exactly 8 elements of order 12 in $D_{12} \oplus \mathbb{Z}_2$. They are

$$(a,0), (a,1), (a^5,0), (a^5,1), (a^7,0), (a^7,1), (a^{11},0), (a^{11},1).$$

■

8.59 Let (a,b) belong to $\mathbb{Z}_m \oplus \mathbb{Z}_n$. Prove that $|(a,b)|$ divides $\operatorname{lcm}(m,n)$.

Proof. [**方法一**] By Lagrange's Theorem, $|a|$ divides $|\mathbb{Z}_m| = m$ and $|b|$ divides $|\mathbb{Z}_n| = n$. Note that m divides $\operatorname{lcm}(m,n)$ and n divides $\operatorname{lcm}(m,n)$. That is, $\operatorname{lcm}(m,n)$ is a common multiple of $|a|$ and $|b|$. Therefore,

$$|(a,b)| \overset{\text{Theorem 8.1}}{\overset{\downarrow}{=}} \operatorname{lcm}(|a|,|b|) \text{ divides } \operatorname{lcm}(m,n)$$

because the least common multiple divides every common multiple.

[**方法二, 感謝王O鈞同學提供**] By Lagrange's Theorem,

$$|a| \text{ divides } m \text{ divides } \operatorname{lcm}(m,n)$$

and

$$|b| \text{ divides } n \text{ divides } \operatorname{lcm}(m,n).$$

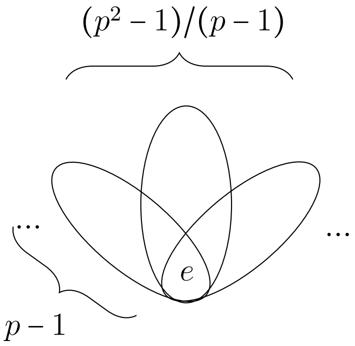
Thus, $\operatorname{lcm}(m,n) \cdot (a,b) = (\operatorname{lcm}(m,n) \cdot a,\ \operatorname{lcm}(m,n) \cdot b) = (0,0)$. Then by p.79, Corollary 2. ■

8.63* Let p be a prime. Prove that $Z_p \oplus Z_p$ has exactly $p+1$ subgroups of order p.

提示. Write down some concrete example. Observe the example and give a conjecture. Verify your conjecture.

Proof.

- If H is a subgroup of order p, then H must be a cyclic group.
- If H is a subgroup of order p, then every elements in H except identity is of order p.
- If H_1 and H_2 are any two distinct subgroups of order p, then $H_1 \cap H_2 = \{e\}$. (If $e \neq g \in H_1 \cap H_2$, by Lagrange's Theorem, $|g|$ divide $|H_1| = p$, then $|g| = p$ and $H_1 = \langle g \rangle = H_2$, a contradiction.)
- By Lagrange's Theorem and $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is not cyclc, every elements in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ except identity is of order p. Thus, there are $p^2 - 1$ elements of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$.
- Any subgroup of order p has exactly $p-1$ elements of order p. Therefore, there are $(p^2-1)/(p-1)$ subgroups of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$.



補充. 事實上, 這 $p+1$ 個 order 為 p 的 subgroup 為

$$\begin{aligned}
\langle(1,0)\rangle &= \{(0,0),(1,0),(2,0),(3,0),\ldots,(p-1,0)\},\\
\langle(1,1)\rangle &= \{(0,0),(1,1),(2,2),(3,3),\ldots,(p-1,p-1)\},\\
\langle(1,2)\rangle &= \{(0,0),(1,2),(2,4),(3,6),\ldots,(p-1,(p-1)2)\},\\
&\vdots\\
\langle(1,p-1)\rangle &= \{(0,0),(1,p-1),(2,2(p-1)),(3,3(p-1)),\ldots,(p-1,(p-1)(p-1))\},\\
\langle(0,1)\rangle &= \{(0,0),(0,1),(0,2),(0,3),\ldots,(0,p-1)\}.
\end{aligned}$$

■

8.83* Let $p_1, p_2, \ldots, p_k$ be distinct odd primes and $n_1, n_2, \ldots, n_k$ be positive integers. Determine the number of elements of order 2 in $U(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k})$. How many are there in $U(2^n p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k})$ where n is at least 3?

Proof. Recall that $U(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}) \cong U(p_1^{n_1}) \oplus U(p_2^{n_2}) \oplus \cdots \oplus U(p_k^{n_k})$. By the primitive root theorem, $U(p_i^{n_i})$ is cyclic for each $i = 1, 2, \ldots, k$. Since 2 divides $p_i^{n_i} - p_i^{n_i - 1} = |U(p_i^{n_i})|$, by the Fundamental Theorem of Finite Cyclic Groups (Theorem 4.3), there exists only one cyclic group of order 2. Thus, there is only one element $a_i \in U(p_i^{n_i})$ of order 2. Therefore, the set of all elements of order 2 in $U(p_1^{n_1}) \oplus U(p_2^{n_2}) \oplus \cdots \oplus U(p_k^{n_k})$ is

$$S = \{(b_1, b_2, \ldots, b_k) \mid b_i \in \{e_i, a_i\}\} - \{(e_1, e_2, \ldots, e_k)\}$$

and $|S| = 2^k - 1$, where e_i is the identity of $U(p_i^{n_i})$.

Recall that $U(2^n p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}) \cong U(2^n) \oplus U(p_1^{n_1}) \oplus U(p_2^{n_2}) \oplus \cdots \oplus U(p_k^{n_k})$. We show that there are three elements c_1, c_2 and c_3 of order 2 in $U(2^n)$ for any $n \geq 3$. Then the set of all elements of order 2 in $U(2^n) \oplus U(p_1^{n_1}) \oplus U(p_2^{n_2}) \oplus \cdots \oplus U(p_k^{n_k})$ is

$$S = \{(c, b_1, b_2, \ldots, b_k) \mid c \in \{c_0, c_1, c_2, c_3\},\ b_i \in \{e_i, a_i\}\} - \{(c_0, e_1, e_2, \ldots, e_k)\}$$

and $|S| = 4 \cdot 2^k - 1$, where c_0 is the identity of $U(2^n)$ and e_i is the identity of $U(p_i^{n_i})$. Note that

$$\begin{aligned} U(2^n) &= \{1, 3, 5, \ldots, 2^{n-1} - 3, 2^{n-1} - 1, \quad 2^{n-1} + 1, \quad 2^{n-1} + 3, \ldots, 2^n - 3, 2^n - 1\} \\ &= \{1, \underbrace{3, 5, \ldots, 2^{n-1} - 3}_{\substack{2k+1, \\ k \in \{1,2,3,\ldots,2^{n-2}-2\}}}, 2^{n-1} - 1, -(2^{n-1} - 1), \underbrace{-(2^{n-1} - 3), \ldots, -3}_{-(2k+1)}, \quad -1\} \pmod{2^n} \end{aligned}$$

$$\begin{aligned} \text{If} \quad & [\pm(2k+1)]^2 = 1 \\ \Rightarrow \quad & (2k+1)^2 = 1 \\ \Rightarrow \quad & 4k^2 + 4k + 1 = 1 \in U(2^n) \\ \Rightarrow \quad & 2^n \mid 4k^2 + 4k \\ \Rightarrow \quad & 2^{n-2} \mid (k^2 + k) = k(k+1) \end{aligned}$$

Note that k and $k+1$ are two consecutive integers, one of them is even and the other one is odd. It follows that $\gcd(2^{n-2}, k) = 1$ or $\gcd(2^{n-2}, k+1) = 1$. Hence, $2^{n-2} \mid k$ or $2^{n-2} \mid (k+1)$. Which is impossible because $k \in \{1, 2, 3, \ldots, 2^{n-2} - 2\}$.

In addition,

$$(2^{n-1} \pm 1)^2 = 2^{2n-2} \pm 2^n + 1 = 2^n \cdot 2^{n-2} \pm 2^n + 1 \overset{\substack{n \geq 2 \\ \downarrow}}{=} 1 \in U(2^n).$$

Note that when $n = 2$, $2^{n-1} - 1 = 1 \in U(2^2)$ and $|2^{n-1} - 1| = 1 \neq 2$. So the condition $n \geq 3$ is necessary.

Therefore, there are three elements $2^{n-1} + 1$, $2^{n-1} - 1$ and (-1) of order 2 in $U(2^n)$ for any $n \geq 3$.

補充. 我怎麼知道 $U(2^n)$ 中有 3 個 order 爲 2 的元素呢? 觀察幾個簡單的例子並大膽地猜測。當 $n = 4$ 時,

$$\begin{aligned} 1^2 &= 1 \in U(2^4), \\ 3^2 &= 9, \\ 5^2 &= 9, \\ 7^2 &= 1, \\ 9^2 &= 1, \\ 11^2 &= 9, \\ 13^2 &= 9, \\ 15^2 &= 1. \end{aligned}$$

當 $n=5$ 時,

$$\begin{aligned}
1^2 &= 1 \in U(2^5),\\
3^2 &= 9,\\
5^2 &= 25,\\
7^2 &= 17,\\
9^2 &= 17,\\
11^2 &= 25,\\
13^2 &= 9,\\
15^2 &= 1,\\
17^2 &= 1,\\
19^2 &= 9,\\
21^2 &= 25,\\
23^2 &= 17,\\
25^2 &= 17,\\
27^2 &= 25,\\
29^2 &= 9,\\
31^2 &= 1.
\end{aligned}$$

■

補充 8.A (A part of primitive root theorem.) For any odd prime p and any positive integer n, $U(p^n)$ is cyclic.

9 Chapter 9

9.2 Prove that A_n is normal in S_n.

Proof. $[S_n : A_n] = 2$ implies that $A_n \triangleleft S_n$. See Exercise 9.9. ■

提示. See Exercise 9.9.

9.6 Let $H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, b, d \in \mathbb{R}, ad \neq 0 \right\}$. Is H a normal subgroup of $GL(2, \mathbb{R})$?

9.7 Let $G = GL(2, \mathbb{R})$ and let K be a subgroup of $\mathbb{R}^*$. Prove that $H = \{A \in G \mid \det A \in K\}$ is a normal subgroup of G.

Proof. Since K is a subgroup of $\mathbb{R}^*$, we have $1 \in K$. Let I be the identity matrix in G. Then $\det I = 1 \in K$ and $I \in H$.

If $M_1, M_2 \in G$, then $\det M_1, \det M_2 \in K$ and $\det(M_1 M_2) = \det M_1 \cdot \det M_2 \in K$ because K is closed under multiplication. Thus, $M_1 M_2 \in H$.

For any $M \in G$, $\det(M^{-1}) = (\det M)^{-1} \in K$ because K contains the inverse of its element $\det M$. Therefore, $M^{-1} \in H$.

Finally, for any $A \in G$ and $M \in H$.

$$\begin{aligned}
\det AMA^{-1} &= \det A \cdot \det M \cdot \det(A^{-1}) \\
&= \det A \cdot \det M \cdot (\det A)^{-1} \\
&\overset{\mathbb{R}^* \text{ is abelian}}{\overset{\downarrow}{=}} \det A \cdot (\det A)^{-1} \cdot \det M \\
&= \det M \in K.
\end{aligned}$$

That is, $AMA^{-1} \in H$ and $H \triangleleft G$. ■

9.9 Prove that if H has index 2 in G, then H is normal in G

Proof. For any $g \in G$, if $g \in H$, then $gHg^{-1} \subseteq H$ and we are done.

If $g \notin H$, since $[G : H] = 2$, then there are exactly two left cosets of H in G. That is, g and gH. Recall that these cosets partition G. That is, for any $a \in G$, either $a \in H$ or $a \in gH$. For any $h \in H$, if $ghg^{-1} \in H$, then we are done. If $ghg^{-1} \notin H$, then $ghg^{-1} \in gH$ and $ghg^{-1} = gh_1$ for some $h_1 \in H$. It follows that $g = h_1^{-1}h \in H$, a contradiction. ■

提示. For any $g \in G$, if $g \in H$, then $gHg^{-1} \subseteq H$ and we are done.

If $g \notin H$, since $[G : H] = 2$, then there are exactly two left cosets of H in G. That is, H and gH. Recall that these cosets partition G. ...

補充. 這個定理非常非常非常重要, 這個定理的重要性在於, 他讓我們可以用簡單的計算 ($[G : H] = 2$), 取代複雜的驗證 ($gHg^{-1} \subseteq H$)。

9.12 Prove that a factor group of a cyclic group is cyclic.

Proof. If $G = \langle g \rangle$ is a cyclic group and $H \triangleleft G$, then $G/H = \langle gH \rangle$. ■

9.13 Prove that a factor group of an Abelian group is Abelian.

Proof. If G is an abelian group and $H \triangleleft G$, then $(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$. ■

9.14 What is the order of the element $14 + \langle 8 \rangle$ in the factor group $\mathbb{Z}_{24}/\langle 8 \rangle$?

Proof. Since $|\mathbb{Z}_{24}/\langle 8 \rangle| = 8$, by Lagrange's Theorem, the order of the element in $\mathbb{Z}_{24}/\langle 8 \rangle$ must be a divisor of 8. Compute $2(14 + \langle 8 \rangle) = 4 + \langle 8 \rangle$, $4(14 + \langle 8 \rangle) = 0 + \langle 8 \rangle$. Thus, $|14 + \langle 8 \rangle| = 4$. ■

9.15 What is the order of the element $4U_5(105)$ in the factor group $U(105)/U_5(105)$?

Proof. $(4U_5(105))^2 = 16U_5(105) = U_5(105)$ because $16 \in U_5(105)$. So $|4U_5(105)| = 2$. ■

9.16 Recal that $Z(D_6) = \{R_0, R_{180}\}$. What is the order of the element $R_{60}Z(D_6)$ in the factor group $D_6/Z(D_6)$?

Proof. Compute $(R_{60}Z(D_6))^2 = R_{120}Z(D_6)$, $(R_{60}Z(D_6))^3 = R_{180}Z(D_6) = Z(D_6)$. So $|R_{60}Z(D_6)| = 3$. ■

9.27 Let $G = U(16)$, $H = \{1, 15\}$, and $K = \{1, 9\}$. Are H and K isomorphic? Are G/H and G/K isomorphic?

Proof. $H \cong K \cong \mathbb{Z}_2$. But

$$G/H = \{H, 3H, 3^2H, 3^3H\} \cong \mathbb{Z}_4 \ncong G/K = \{K, 3K, 5K, 7K\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

■

9.28 Let $G = Z_4 \oplus Z_4$, $H = \{(0,0), (2,0), (0,2), (2,2)\}$, and $K = \langle(1,2)\rangle$. Is G/H isomorphic to Z_4 or $Z_2 \oplus Z_2$? Is G/K isomorphic to Z_4 or $Z_2 \oplus Z_2$?

Proof. Write down all the cosets of H in G.

$$\begin{aligned} H &= \{(0,0), (2,0), (0,2), (2,2)\}, \\ (1,0) + H &= \{(1,0), (3,0), (1,2), (3,2)\}, \\ (0,1) + H &= \{(0,1), (2,1), (0,3), (2,3)\}, \\ (1,1) + H &= \{(1,1), (3,1), (1,3), (3,3)\}. \end{aligned}$$

Recall that the operation (addition or multiplication) of two cosets is defined by

$$(a + H) + (b + H) = (a + b) + H.$$

Then we can write down that Cayley table of the quotient group G/H.

G/H	H	$(1,0)+H$	$(0,1)+H$	$(1,1)+H$
H	H	$(1,0)+H$	$(0,1)+H$	$(1,1)+H$
$(1,0)+H$	$(1,0)+H$	H	$(1,1)+H$	$(0,1)+H$
$(0,1)+H$	$(0,1)+H$	$(1,1)+H$	H	$(1,0)+H$
$(1,1)+H$	$(1,1)+H$	$(0,1)+H$	$(1,0)+H$	H

Note that the entries in the main diagonal all are H. Which implies that $G/H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Similarly, G/K is isomorphic to $\mathbb{Z}_4$. ■

提示. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

9.29 Prove that $A_4 \oplus Z_3$ has no subgroup of order 18.

Proof. Let $G = A_4 \oplus \mathbb{Z}_3$. If H is a subgroup of G which is of order 18, then since $|A_4 \oplus \mathbb{Z}_3| = 36$ and by Exercise 9.9, $H \triangleleft G$. Note that A_4 has only one normal subgroup $H = \langle(12)(34), (13)(24)\rangle$. But $|H \oplus \mathbb{Z}_3| = 12$ and $|H \oplus \{0\}| = 4$, both are not of order 18. Therefore, $A_4 \oplus \mathbb{Z}_3$ has no subgroup of order 18. ■

提示. Let $G = A_4 \oplus \mathbb{Z}_3$. If H is a subgroup of G which is of order 18 then by Exercise 9.9, $H \lhd G$. Note that A_4 has only one normal proper subgroup $H = \langle (12)(34), (13)(24) \rangle$. But $|H \oplus \mathbb{Z}_3| = 12$ and $|H \oplus \{0\}| = 4$.

Proof. Let $G = A_4 \oplus \mathbb{Z}_3$. If H is a subgroup of G which is of order 18, then since $[A_4 \oplus \mathbb{Z}_3 : H] = 2$ and $H \lhd G$. Note that A_4 has only one normal subgroup $K = \langle (12)(34), (13)(24) \rangle$. But $|K \oplus \mathbb{Z}_3| = 12$ and $|H \oplus \{0\}| = 4$, both are not of order 18. Therefore, $A_4 \oplus \mathbb{Z}_3$ has no subgroup of order 18. ■

9.33 Let H and K be subgroups of a group G. If $G = HK$ and $g = hk$, where $h \in H$ and $k \in K$, is there any relationship among $|g|$, $|h|$, and $|k|$? What if $G = H \times K$?

Proof. There is no relation between $|h|, |k|$ and $|hk|$. Let $G = D_n$, $H = \langle b \rangle \le G$ and $K = \langle a \rangle \le G$. Then $G = HK$. Let $h = b$, $k = a$. Then $|h| = 2, |k| = n, |hk| = 2$. $|k| = n$ could be arbitrarily large.

If $G = H \times K$, then $|g| = |(h,k)| = \text{l.c.m.}(|h|, |k|)$. ■

提示. No any relationship. See Exercise 3.48.

9.37 Let G be a finite group and let H be a normal subgroup of G. Prove that the order of the element gH in G/H must divide the order of g in G.

提示. p.79, cor.2.

想一想, 這題跟 p.210, thm.10.1.3有什麼關係。

9.39 If H is a normal subgroup of a group G, prove that $C_G(H)$, the centralizer of H in G, is a normal subgroup of G.

Proof. Recall that $C_G(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$. Since $1h = h = h1$ for all $h \in H$, we have $1 \in C_G(H)$.

If $g_1, g_2 \in C_G(H)$, then $g_1 h = h g_1$ and $g_2 h = h g_2$ for all $h \in H$. Thus,

$$(g_1g_2)h = g_1(g_2h) \overset{\substack{g_2h=hg_2 \\ \downarrow}}{=} g_1(hg_2) = (g_1h)g_2 \overset{\substack{g_1h=hg_1 \\ \downarrow}}{=} (hg_1)g_2 = h(g_1g_2) \text{ for all } h \in H$$

and $g_1g_2 \in C_G(H)$.

Suppose that $g \in C_G(H)$. For all $h \in H$, since H is a subgroup of G, h^{-1} is also in H. Hence, $gh^{-1} = h^{-1}g$. Therefore,

$$g^{-1}h = (h^{-1}g)^{-1} = (gh^{-1})^{-1} = hg^{-1}$$

and $g^{-1} \in C_G(H)$.

For any $a \in G$, $g \in C_G(H)$ and $h \in H$,

$$\begin{aligned}
aga^{-1} \cdot h &= aga^{-1}h(aa^{-1}) \\
&= ag(a^{-1})h(a^{-1})^{-1}a^{-1} \\
&\overset{\substack{H \lhd G,\ (a^{-1})h(a^{-1})^{-1} \in H \\ \downarrow}}{=} agh'a^{-1} \\
&\overset{\substack{g \in C_G(H),\ gh'=h'g \\ \downarrow}}{=} ah'ga^{-1} \\
&\overset{\substack{h'=a^{-1}h(a^{-1})^{-1} \\ \downarrow}}{=} a(a^{-1})h(a^{-1})^{-1}ga^{-1} \\
&= h \cdot aga^{-1}.
\end{aligned}$$

That is, $aga^{-1} \in C_G(H)$ and $C_G(H) \lhd G$. ■

9.40 Let ϕ be an isomorphism from a group G onto a group $\overline{G}$. Prove that if H is a normal subgroup of G, then $\phi(H)$ is a normal subgroup of $\overline{G}$.

9.45 Let p be a prime. Show that if H is a subgroup of a group of order $2p$ that is not normal, then H has order 2.

Proof. By Lagrange's Theorem, $|H| \in \{1, 2, p, 2p\}$. If $|H| = p$, then $[G : H] = 2p/p = 2$ and by Exercise 9.9, $H \lhd G$, a contradiction. If $|H| \in \{1, 2p\}$, then H is normal in G, it is impossible. Therefore, $|H| = 2$. ■

提示. By Lagrange's Theorem, $|H| \in \{1, 2, p, 2p\}$. If $|H| = p$, then by Exercise 9.9, ...

9.47* Suppose that N is a normal subgroup of a finite group G and H is a subgroup of G. If $|G/N|$ is prime, prove that H is contained in N or that $NH = G$.

Proof. [方法一] By Example 9.5, NH is a subgroup of G. Consider the subgroup tower and by Exercise 7.33,

$$\overbrace{N \underbrace{\le}_{\in\{1,p\}} NH \underbrace{\le}_{\in\{1,p\}} G}^{p}.$$

[方法二] If $H \nleq N$, then there exists $h \in H$ and $h \notin N$. Suppose that $|G/N| = p$. Then the factor group G/N is of order prime and G/N must be a cyclic group. By Lagrange's Theorem, the order of any one element in G/N except the identity must be of order p. That is, any one element in G/N except the identity is a generator of G/N. In particular, $Nh \neq N$ and

$$G/N = \langle Nh \rangle = \{N, Nh, Nh^2, Nh^3, ..., Nh^{p-1}\}.$$

Recall that all the right cosets of N in G partition G. Therefore, $G = NH$. ■

提示. [方法一] By Example 9.5, NH is a subgroup of G. Consider the subgroup tower and by Exercise 7.33,

$$\overbrace{N \underbrace{\le}_{\in\{1,p\}} NH \underbrace{\le}_{\in\{1,p\}} G}^{p}.$$

[方法二] If $H \nleq N$, then there exists $h \in H$ and $h \notin N$. Suppose $|G/N| = p$. Then G/N is a cyclic group generated by Nh. That is,

$$G/N = \langle Nh \rangle = \{N, Nh, Nh^2, Nh^3, ..., Nh^{p-1}\}.$$

Therefore, $G = NH$.

9.49 Suppose that G is a non-abelian group of order p^3, where p is a prime, and $Z(G) \neq \{e\}$. Prove that $|Z(G)| = p$.

Proof. By Lagrange's Theorem, $|Z(G)|$ divide $|G| = p^3$ and $Z(G) \in \{1, p, p^2, p^3\}$. Since G is non-abelian, we have $|Z(G)| \neq p^3$. Since $Z(G) \neq e$, we have $|Z(G)| \neq 1$.

If $|Z(G)| = p^2$, then $[G : Z(G)] = p$ and $G/Z(G)$ is a cyclic group. By Theorem 9.3, it follows that G is abelian, a contradiciton. Therefore, $|Z(G)| = p$. ■

提示. By Lagrange's Theorem, $|Z(G)| \in \{1, p, p^2, p^3\}$. By Theorem 9.3.

9.50 If $|G| = pq$, where p and q are primes that are not necessarily distinct, prove that $|Z(G)| = 1$ or pq.

提示. By Theorem 9.3.

9.51 Let N be a normal subgroup of G and let H be a subgroup of G. If N is a subgroup of H, prove that H/N is a normal subgroup of G/N if and only if H is a normal subgroup of G.

補充. 跟 exe.10.51比較一下。

9.56 Show that the intersection of two normal subgroups of G is a normal subgroup of G. Generalize.

Proof. Let H and K be two normal subgroup of G. For any $a \in H \cap K$ and $g \in G$, since H is normal in G, we have $gag^{-1} \in H$. Similarly, $gag^{-1} \in K$. Thus, $gag^{-1} \in H \cap K$ and $H \cap K \lhd G$. ■

補充. 考試考出來的話你必須先證明 $H \cap K$ is a subgroup of G.

Exa.9.5, 9.57 Let N be a normal subgroup of G and let H be any subgroup of G. Prove that NH is a subgroup of G. Give an example to show that NH need not be a subgroup of G if neither N nor H is normal.

Proof. $e = e \cdot e \in NH$. If $n_1h_1, n_2h_2 \in NH$, then

$$(n_1h_1)(n_2h_2) = n_1h_1n_2\underline{h_1^{-1}h_1}h_2 = n_1(h_1n_2h_1^{-1})h_1h_2 \overset{N \lhd G,\ h_1n_2h_1^{-1} \in N}{\overset{\downarrow}{=}} n_1n_3h_1h_2 \in NH$$

and

$$(n_1h_1)^{-1} = h_1^{-1}n_1^{-1} = h_1^{-1}n_1^{-1}\underline{(h_1^{-1})^{-1}h_1^{-1}} \overset{N \lhd G,\ h_1^{-1}n_1^{-1}(h_1^{-1})^{-1} \in N}{\overset{\downarrow}{=}} n_4h_1^{-1} \in NH.$$

Therefore, NH is a subgroup of G.

Let $G = S_3$, $H = \langle(12)\rangle$, $K = \langle(13)\rangle$. Then $HK = \{e, (12), (13), (132)\}$ is not a subgroup of S_3. ■

提示. S_3.

9.58 If N and M are normal subgroups of G, prove that NM is also a normal subgroup of G.

Proof. By Example 9.5, NM is a subgroup of G. For any $nm \in NM$, $g \in G$,

$$gnmg^{-1} = gn(g^{-1}g)mg^{-1} = (gng^{-1})(gmg^{-1}) \overset{N\lhd G,\ M\lhd G}{\overset{\downarrow}{=}} n'm' \in NM.$$

That is, $NM \lhd G$. ■

9.59 Let N be a normal subgroup of a group G. If N is cyclic, prove that every subgroup of N is also normal in G.

Proof. Recall that every subgroup of a cyclic group is also cyclic. Suppose that $H = \langle a^m \rangle \le N = \langle a \rangle \lhd G$. Then for any $(a^m)^s \in H = \langle a^m \rangle$ and $g \in G$,

$$g(a^m)^s g^{-1} = (ga^s g^{-1})^m \overset{a^s\in N\lhd G,\ ga^s g^{-1}\in N}{\overset{\downarrow}{=}} (a^t)^m = (a^m)^t \in H.$$

Therefore, $gHg^{-1} \subseteq H$ and $H \lhd G$. ■

提示. Recall that every subgroup of a cyclic group is also cyclic. Suppose that $H = \langle a^m \rangle \le N = \langle a \rangle \lhd G$. Then

$$g(a^m)^s g^{-1} = (ga^s g^{-1})^m \overset{a^s\in N\lhd G,\ ga^s g^{-1}\in N}{\overset{\downarrow}{=}} (a^t)^m = (a^m)^t \in H.$$

補充. 這個定理的一個直接應用就是找 D_n 的某些 normal subgroup。因爲 $\langle a \rangle \lhd D_n$, 且 $\langle a \rangle$ is a cyclic group, 所以 $\langle a^m \rangle \lhd D_n$.

9.61 Let H be a normal subgroup of a finite group G and let $x \in G$. If $\gcd(|x|, |G/H|) = 1$, show that $x \in H$.

Proof. [**方法一**] By Exercise 10.46, $|xH|$ divides $|x|$. By Lagrange's Theorem, $|xH|$ divides $|G/H|$. Hence, $|xH|$ is a common divisor of $|x|$ and $|G/H|$. Therefore, $|xH| = 1$ and $xH = H$ and $x \in H$.

[**方法二**] Since $\gcd(|x|, |G/H|) = 1$, suppose that $|x| \cdot m + |G/H| \cdot n = 1$ for some $m, n \in \mathbb{Z}$. Then

$$xH = x^1 H = x^{|x|\cdot m + |G/H|\cdot n} H = x^{|G/H|\cdot n} H = (xH)^{|G/H|\cdot n} \overset{\text{Lagrange's Theorem}}{\overset{\downarrow}{=}} eH = H.$$

Therefore, $x \in H$. ■

9.62 Let G be a group and let G' be the subgroup of G generated by the set

$$S = \{x^{-1}y^{-1}xy \mid x, y \in G\}.$$

補充.

- 這題對你們來說眞的頗難。
- 這個 subgroup G' 叫做 commutator subgroup, 看似奇怪, 之後我們在做 group 的 classification 的時候還有討論 group series 時會用到, 到時候你就會見識到它的威力。

- 在這裡所謂的"generates"就是指

$$G' = \bigcap_{S\subseteq H} H.$$

如你所知道的, subgroup的交集仍然是 subgroup, 所以 G' 也是 subgroup。

- 直觀來看, G' 就是包含 S 的最小 subgroup, 也就是說, 如果 $S \subseteq H \leq G$, 則 $G' \subseteq H$。

- 另外, 我們要說明一下 G' 裡面的元素的長相, 有點醜, 不過其實也不難懂, 就是任意抓有限個 S 裡面的元素拿來隨便相乘, 可以重複抓, 也就是

$$G' = \{s_1^{r_1}s_2^{r_2}\cdots s_m^{r_m} \mid s_i \in S, r_i \in \mathbb{Z}, m \in \mathbb{Z}^+\}.$$

例如 $s_1^3s_2^{-2}s_3^8s_2^{-5} \in G'$ 或是 $s_4^2s_2^{-1}s_4^4 \in G'$, 注意, 這裡的 $s_4^2s_2^{-1}s_4^4$ 不一定等於 $s_4^6s_2^{-1}$, 因為 G 不一定是 abelian。

- 所以囉,

$$G' = \bigcap_{S\subseteq H} H = \{s_1^{r_1}s_2^{r_2}\cdots s_m^{r_m} \mid s_i \in S, r_i \in \mathbb{Z}, m \in \mathbb{Z}^+\}.$$

感覺起來, 第二個定義比較有"generate"的感覺, 有點像是你線性代數學的 span, 但第二個定義很難推廣, 而第一個定義則可以推廣到其他 algebraic structure 的 substructure generated by some subset, 這我們以後學 ring theory 的時候會比較有感覺。

- 你現在可能覺得莫名其妙, 越弄越複雜, group就好好的 group, 為什麼還弄個 genearte 的觀念呢? 這個問題其實你線性代數就遇過了, 或許你當時沒時間好好地想一想, 但相信你現在瞭解它的意義之後就會恍然大悟。我們在討論一個 over 在 field F 上的 vector space(向量空間) V 的時候, 我們會去找它的 basis(基底), 這樣的其中一個好處是, 我們不用把 V 裡面的 vector 全部寫出來, 因為 V 裡面的 vector 全部可以用 basis 裡面的 vector 作線性組合來表示; 另一個好處是, 我們在決定 linear transformation(線性變換) T 時, 我們只要決定 basis 在 T 之下的 image 就好。類似地, 我們在討論 group homomorphism θ 時, 我們只要決定這個 group 的 generator 在 θ 下的 image 就好。而在這裡呢, 因為 G' 是由 S 所 generate 的, 所以我們想要證明 G' 具有某些性質時, 我們只要證明 S 裡面的元素具有這些性質就好了, 因為 S 裡面的元素是 G' 的 generator。所以下面的論證中, 我們只證明 $x^{-1}y^{-1}xy \in S$ 具有某個性質, 就足以判斷對於所有的 $a \in G'$ 具有該性質。

(a) Prove that G' is normal in G.

Proof. Denote $x^{-1}y^{-1}xy$ by $[x, y]$. Then

$$\begin{aligned}
g[x,y]g^{-1} &= gx^{-1}y^{-1}xyg^{-1} \\
&= gx^{-1}\underline{g^{-1}g}y^{-1}\underline{g^{-1}g}x\underline{g^{-1}g}yg^{-1} \\
&= (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \\
&= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \\
&= [gxg^{-1}, gyg^{-1}] \in S \subseteq G'.
\end{aligned}$$

■

提示. Denote $x^{-1}y^{-1}xy$ by $[x, y]$. Show that $[gxg^{-1}, gyg^{-1}] = g[x, y]g^{-1}$.

(b) Prove that G/G' is abelian.

Proof. For any $g_1G', g_2G' \in G/G'$, since $g_1^{-1}g_2^{-1}g_1g_2 \in G'$, we have $g_1^{-1}g_2^{-1}g_1g_2G' = G'$ and $g_1g_2G' = g_2g_1G'$ and

$$g_1G' \cdot g_2G' = g_1g_2G' = g_2g_1G' = g_2G' \cdot g_1G'.$$

■

提示. Note that $g_1^{-1}g_2^{-1}g_1g_2G' = G'$.

(c) If G/N is abelian, prove that $G' \leq N$.

Proof. If G/N is abelian, then for any $x, y \in G$,

$$\begin{aligned} & (xN)(yN) = (yN)(xN) \\ \Rightarrow\ & xyN = yxN \\ \Rightarrow\ & x^{-1}y^{-1}xyN = N \\ \Rightarrow\ & x^{-1}y^{-1}xy \in N \\ \Rightarrow\ & G' \leq N. \end{aligned}$$

■

提示.

$$\begin{aligned} & (xN)(yN) = (yN)(xN) \\ \Rightarrow\ & \square N = yxN \\ \Rightarrow\ & \square y^{-1}xyN = N \\ \Rightarrow\ & x^{-1} \square\, xy \in N \\ \Rightarrow\ & G' \leq N. \end{aligned}$$

補充. 直觀來看,G' 是使得 $G/\square$ 是 abelian 的最小 normal subgroup。

(d) Prove that if H is a subgroup of G and $G' \leq H$, then H is normal in G.

Proof. For any $h \in H$ and $g \in G$,

$$ghg^{-1} = (g^{-1})^{-1}(h^{-1})^{-1}(g^{-1})\underline{(h^{-1})h} = [g^{-1}, h^{-1}]h \in H.$$

■

提示.

$$ghg^{-1} = (g^{-1})^{-1}(h^{-1})^{-1}(g^{-1})(h^{-1})h = [g^{-1}, h^{-1}]h \in H.$$

補充. 你不妨把 G' 想成舍利子, 如果有一個 subgroup H 把 G' 含在嘴裡, 就可以 normal。

9.64* Suppose that a group G has a subgroup of order n. Prove that the intersection of all subgroups of G of order n is a normal subgroup of G.

Proof. If H is a subgroup of order n, we show that gHg^{-1} is also a subgroup of order n.

$e \in gHg^{-1}$ is clearly because $e = geg^{-1}$. If $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$, then

$$(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in gHg^{-1}$$

and

$$(gh_1g^{-1})^{-1} = gh_1^{-1}g \in gHg^{-1}.$$

Thus, gHg^{-1} is a subgroup of G. Define a mapping $f : H \to gHg^{-1}$ by $f(h) = ghg^{-1}$. Then f is onto and one-to-one. Therefore, H and gHg^{-1} have the same cardinality (the number of element).

Furthermore, if $gH_1g^{-1} = gH_2g^{-1}$, then $H_1 = g^{-1}gH_1g^{-1}g = g^{-1}gH_2g^{-1}g = H_2$. Thus, for any $g \in G$, if $\{H_i \mid i \in I\}$ is the set of all subgroup of G whose order is n, then $\{gH_ig^{-1} \mid i \in I\}$ is also the set of all subgroup of G whose order is n. It follows that

$$\bigcap_{|H|=n} H = \bigcap_{|H|=n} gHg^{-1}.$$

For any $x \in \bigcap_{|H|=n} H$ and $g \in G$,

$$gxg^{-1} \in \bigcap_{|H|=n} gHg^{-1} = \bigcap_{|H|=n} H.$$

That is, $\bigcap_{|H|=n} H \triangleleft G$. ■

提示.

- Show that if H is a subgroup of order n, then gHg^{-1} is also a subgroup of order n.
- For any $g \in G$, show that if $gH_1g^{-1} = gH_2g^{-1}$, then $H_1 = g^{-1}gH_1g^{-1}g = g^{-1}gH_2g^{-1}g = H_2$.
- Thus, for any $g \in G$, if $\{H_i \mid i \in I\}$ is the set of all subgroup of G whose order is n, then $\{gH_ig^{-1} \mid i \in I\}$ is also the set of all subgroup of G whose order is n.
- Show that
$$\bigcap_{|H|=n} H = \bigcap_{|H|=n} gHg^{-1}.$$

9.65 If G is non-Abelian, show that $\operatorname{Aut}(G)$ is not cyclic.

Proof.

$$\begin{array}{cl} \text{If} & \operatorname{Aut}(G) \text{ is cyclic}\\ \Rightarrow & \operatorname{inn}(G) \le \operatorname{Aut}(G) \text{ is also cyclic}\\ \overset{\overset{\text{Theorem 9.4}}{\downarrow}}{\Rightarrow} & G/Z(G) \cong \operatorname{inn}(G) \text{ is cylic}\\ \overset{\overset{\text{Theorem 9.3}}{\downarrow}}{\Rightarrow} & G \text{ is abelian} \end{array}$$

■

9.66 Let $|G| = p^n m$, where p is prime and $\gcd(p, m) = 1$. Suppose that H is a normal subgroup of G of order p^n. If K is a subgroup of G of order p^k, show that $K \subseteq H$.

Proof. [**方法一**] It follows immediately from Exercise 9.61.

[**方法二**]

$$\begin{aligned}
& H \triangleleft G \\
\Rightarrow\quad & HK \le G \\
\Rightarrow\quad & \frac{\cancel{p^n}\cdot p^k}{|H\cap K|} = \frac{|H|\cdot|K|}{|H\cap K|} = |HK| \text{ divides } |G| = \cancel{p^n} m \\
\Rightarrow\quad & \frac{p^k}{|H\cap K|} \mid m \\
\overset{\overset{\gcd(p,m)=1}{\downarrow}}{\Rightarrow}\quad & |H\cap K| = p^k \\
\overset{\overset{H\cap K\le K}{\downarrow}}{\Rightarrow}\quad & H\cap K = K \\
\Rightarrow\quad & K \le H.
\end{aligned}$$

與 Exercise 24.56比較一下。

[**方法三**] Consider the canonical homomorphism $\theta : G \to G/H$. That is, $\theta(g) = gH$. For any $l \in K$,

$$|\theta(l)| = |lH| \quad \overset{\overset{\text{Lagrange's Theorem}}{\downarrow}}{\text{divides}} \quad |G/H| = m.$$

On the other hand,

$$|\theta(l)| \quad \overset{\overset{[\theta(l)]^{|l|}=\theta(l^{|l|})=\theta(e)=e}{\downarrow}}{\text{divides}} \quad |l| \text{ and } |l| \quad \overset{\overset{\text{Lagrange's Theorem}}{\downarrow}}{\text{divides}} \quad |K| = p^k.$$

Therefore, $|\theta(l)| = 1$ because $\gcd(m, p) = \gcd(m, p^k) = 1$. It follows that $\theta(l) = e_{G/H}$ and $K \subseteq \ker\theta = H$.

[**方法四**] It follows immediately from Sylow 1st and 2nd Theorems. ■

9.68 A subgroup N of a group G is called *characteristic* if $\phi(N) = N$ for all automorphisms ϕ of G. If N is a characteristic subgroup of G, show that N is a normal subgroup of G.

Proof. For any $g \in G$, consider the inner automorphism $\sigma_g : G \to G$ defined by $\sigma_g(a) = gag^{-1}$. Then $\sigma_g(N) = N = gNg^{-1}$. Which implies that $N \triangleleft G$. ■

提示. For any $g \in G$, define $\sigma_g : G \to G$ by $\sigma_g(a) = gag^{-1}$. Show that σ_g is an automorphism.

補充. 跟你們講講 characteristic subgroup 的動機。一般來說 $H \triangleleft N \triangleleft G$ 並沒有 imply $H \triangleleft G$, 你能舉一個反例嗎?

所以這迫使數學家們尋找更強的條件, 來讓 normal 具有“遞移性”, 這個 characteristic subgroup 就是我們要找的。也就是

$$H \quad \overset{\overset{\text{characteristic}}{\downarrow}}{\le} \quad N \triangleleft G \Rightarrow H \triangleleft G.$$

注意一下, 剛剛在 Exercise 9.59, 我們也有類似的定理,

$$H \le \overset{\overset{\text{cyclic}}{\downarrow}}{N} \lhd G \Rightarrow H \lhd G.$$

事實上, 每一個 cyclic group 的 subgroup 都是 characteristic 的。

9.73 Prove that A_5 cannot have a normal subgroup of order 2.

Proof. You ought to know that a group of order 2 must be generated by an element of order 2. The element in A_5 must be of the form $(123), (12)(34), (12345)$. Among these elements, the element of the type $(12)(34)$ is the element of order 2. Thus, a normal subgroup of order 2 in A_5 must be of the form $\langle (12)(34) \rangle$. But $(123)(12)(34)(123)^{-1} = (14)(23) \notin \langle (12)(34) \rangle$, a contradiction. ∎

提示. A group of order 2 must be generated by an element of order 2. The element in A_5 must be of the form $(123), (12)(34), (12345)$. Among these elements, the element of the type $(12)(34)$ is the element of order 2. But $(123)(12)(34)(123)^{-1} \notin \langle (12)(34) \rangle$.

9.74* Let G be a finite group and let H be an odd-order subgroup of G of index 2. Show that the product of all the elements of G (taken in any order) cannot belong to H.

Proof. Since $[G : H] = 2$, we have $|G|$ is even. Consider the set $S = \{g \in G \mid g^2 = e\}$. Recall that $|x| = |x^{-1}|$. If $g \in G$ and $|g| \ge 3$, then $g \ne g^{-1}$ and $g \notin S$ and $g^{-1} \notin S$. Hence, $|G - S|$ is even and $|S|$ is even. Thus, $|S - \{e\}|$ is odd and there are odd number of element of order 2 in G.

Since $[G : H] = 2$, by Exercise 9.9, we have $H \lhd G$ and $|G/H| = 2$. Thus, G/H is an abelian group. That is, $(xH)(yH) = (yH)(xH)$ in G/H.

Let π be the product of all the elements of G. Note that if $y \in G$ and $|y| \ge 3$, then $y \ne y^{-1}$ and

$$\begin{aligned}
\pi H &= \left(\prod_{g \in G} g \right) H \\
&= \prod_{g \in G} (gH) \\
&\overset{\overset{G/H \text{ is abelian}}{\downarrow}}{=} \left(\prod_{g \in G - \{y, y^{-1}\}} (gH) \right) (yH)(y^{-1}H) \\
&= \cdots \\
&= x_1 x_2 \cdots x_{2s+1} H,
\end{aligned}$$

where $x_1, x_2, \ldots, x_{2s+1}$ are all the elements of order 2 in G.

Since $[G : H] = 2$, there are exactly two left cosets H and $g_0 H$ for some $g_0 \notin H$. Since $|H|$ is odd, by Lagrange's Theorem, $x_1, x_2, \ldots, x_{2s+1}$ all are not in H. Then $x_1 H \ne H$, $x_2 H \ne H$, ..., $x_{2s+1} H \ne H$ and $x_1 H = x_2 H = \cdots = x_{2s+1} H = g_0 H$.

Therefore,

$$\pi H = \left(\prod_{i=1}^{2s+1} x_i \right) H = \prod_{i=1}^{2s+1} (x_i H) = x_1^{2s+1} H = ((x_1)^2)^s \cdot x_1 H = e^s x_1 H = x_1 H \ne H.$$

That is, $\pi \notin H$. ∎

提示.

- Show that there are odd number of element of order 2 in G. ($|G|$ is even and $|x| = |x^{-1}|$)
- Show that G/H is an abelian group.
- Let π be the product of all the elements of G. Show that
$$\pi H = x_1 x_2 \cdots x_{2s+1} H,$$
where $x_1, x_2, \ldots, x_{2s+1}$ are all the elements of order 2 in G.
- Show that $x_1, x_2, \ldots, x_{2s+1}$ all are not in H.
- Show that $x_1 H = x_2 H = \cdots = x_{2s+1} H$.
- Then
$$\pi H = \left(\prod_{i=1}^{2s+1} x_i \right) H = \prod_{i=1}^{2s+1} (x_i H) = x_1^{2s+1} H = x_1 H \neq H.$$
That is, $\pi \notin H$.

9.77* Let G be a group and H a subgroup of G of index 2. Show that H contains every element of G of odd order.

Proof. Since $[G : H] = 2$, by Exercise 9.9, we have $H \triangleleft G$ and $G/H \cong \mathbb{Z}_2$. That is, any element in G/H except the identity is of order 2. Hence, for all $g \in G$, $g^2 H = (gH)^2 = H$. That is, $g^2 \in H$.

If $|a| = 2s + 1$, then $e = a^{2s+1} = (a^2)^s \cdot a$ and $a = (a^2)^{-s} \in H$. ■

提示. Note that for any $gH \in G/H$, we have $(gH)^2 = H$. That is, $g^2 \in H$.

If $|a| = 2s + 1$, then $e = a^{2s+1} = (a^2)^s \cdot a$ and $a = (a^2)^{-s} \in H$.

9.78 A proper subgroup H of a group G is called maximal if there is no subgroup K such that $H \subset K \subset G$ (that is, there is no subgroup K properly contained between H and G). Show that $Z(G)$ is never a maximal subgroup of a group G.

Proof. [方法一]

$$\begin{array}{cl}
\text{If} & Z(G) \text{ is a maximal subgroup of } G \\
\overset{\substack{\text{Correspondence Theorem for Groups} \\ \downarrow}}{\Rightarrow} & G/Z(G) \text{ has no nontrivial proper subgroups} \\
\overset{\substack{\forall g \in G/Z(G),\ \langle g \rangle \leq G/Z(G) \\ \downarrow}}{\Rightarrow} & G/Z(G) = \langle a \rangle, \text{ for arbitrary } a \neq e \\
\Rightarrow & G/Z(G) \cong \mathbb{Z}_n, \text{ where } n = |G/Z(G)| \\
\overset{\substack{G/Z(G) \text{ has no nontrivial proper subgroups and} \\ \text{by Fundamental Theorem of Finite Cyclic Groups} \\ \downarrow}}{\Rightarrow} & G/Z(G) \cong \mathbb{Z}_p \\
\overset{\substack{\text{Theorem 9.3} \\ \downarrow}}{\Rightarrow} & G \text{ is abelian} \\
\Rightarrow & G = Z(G), \text{ a contradiction}
\end{array}$$

[**方法二**] If G is abelian, then $Z(G) = G$ and $Z(G)$ is not maximal. (Note that a maximal subgroup is a **proper** subgroup.)

If G is not abelian,

$$\begin{aligned} & G \text{ is not abelian} \\ \Rightarrow\ & \exists g \notin Z(G) \\ \Rightarrow\ & g \notin Z(G) \text{ and } C(g) \neq G \\ \Rightarrow\ & g \in C(G) \neq Z(G) \text{ and } C(g) \neq G \\ \Rightarrow\ & Z(G) \subset C(g) \subseteq G \\ \Rightarrow\ & Z(G) \text{ is not maximal.} \end{aligned}$$

■

補充. 想想這題跟 G/Z Theorem 的關係。

補充 9.A Let H be a normal subgroup of G. If H and G/H are abelian, must G be abelian?

Proof. A counterexample is $D_3 = \{\langle a, b\rangle \mid |a| = 3, |b| = 2, ab = ba^{-1}\}$. $\langle a\rangle$ is a cyclic (abelian) normal subgroup of D_3 because $[D_3 : \langle a\rangle] = 2$. In addition, $D_3/\langle a\rangle \cong \mathbb{Z}_2$ is also abelian. But D_3 is not abliean. ■

提示. D_3.

補充 9.B Let G be a group of order p^n where p is prime. Prove that the center of G cannot have order p^{n-1}.

Proof. If $|Z(G)| = p^{n-1}$, then $|G/Z(G)| = p$. By Lagrange's Theorem, $G/Z(G)$ is a cyclic group. By Theorem 9.3, G is abelian and $Z(G) = G$ and $p^{n-1} = |Z(G)| = |G| = p^n$, a contradiction. ■

提示. By Theorem 9.3.

Thm.9.3* $G/Z(G)$ cyclic $\Rightarrow$ G abelian

Proof. Suppose that $G/Z(G)$ is cyclic and $G/Z(G) = \langle gZ(G)\rangle$. For all $a, b \in G$, since all the left cosets $g^iZ(G)$ is a partition of G, where $i \in \mathbb{Z}$, we have $a \in g^mZ(G)$ and $b \in g^nZ(G)$ for some $m, n \in \mathbb{Z}$. Suppose that $a = g^mz_1$ and $b = g^nz_2$ for some

$z_1, z_2 \in Z(G)$. Then

$$\begin{array}{rcl} ab & = & (g^m z_1)(g^n z_2) \\ & = & g^m[z_1(g^n z_2)] \\ & \overset{z_1 \in Z(G)}{\overset{\downarrow}{=}} & g^m[(g^n z_2)z_1] \\ & = & [g^m(g^n z_2)]z_1 \\ & = & [(g^m g^n)z_2]z_1 \\ & = & [g^{m+n}z_2]z_1 \\ & = & [g^{n+m}z_2]z_1 \\ & = & [(g^n g^m)z_2]z_1 \\ & = & [g^n(g^m z_2)]z_1 \\ & \overset{z_2 \in Z(G)}{\overset{\downarrow}{=}} & [g^n(z_2 g^m)]z_1 \\ & = & [(g^n z_2)g^m]z_1 \\ & = & (g^n z_2)(g^m z_1) \\ & = & ba. \end{array}$$

■

thm.9.6 Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $hk = kh$ for all $h \in H$ and $k \in K$.

Proof. For any $h \in H$, $k \in K$,

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \overset{K \triangleleft G}{\overset{\downarrow}{\in}} K$$

and

$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \overset{H \triangleleft G}{\overset{\downarrow}{\in}} H.$$

Thus, $hkh^{-1}k^{-1} \in H \cap K = \{e\}$ and $hkh^{-1}k^{-1} = e$ and $hk = kh$. ■

exa.9.7 Let H be a subgroup of G and fix some element $g \in G$.

(a) Prove that gHg^{-1} is a subgroup of G and that $|gHg^{-1}| = |H|$.

Proof. Since H is a subgroup of G, we have $e \in H$ and $e = geg^{-1} \in gHg^{-1}$. Since H is a subgroup of G, for any $h_1, h_2 \in H$, we have $h_1h_2 \in H$ and $h_1^{-1} \in H$. Then for any $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$,

$$(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in gHg^{-1}$$

and

$$(gh_1g^{-1})^{-1} = gh_1^{-1}g^{-1} \in gHg^{-1}.$$

Consider the mapping $f : H \to gHg^{-1}$ defined by $f(h) = ghg^{-1}$. Then f is a bijection. In fact, f is the inner automorphism σ_g of G restricted to H. ■

(b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \lhd G$.

Proof. Recall that gHg^{-1} is also a subgroup of G whose order is also n. By the uniqueness, $H = gHg^{-1}$ for all $g \in G$. Which means that H is normal in G. ∎

10 Chapter 10

10.8 Let G be a group of permutations. For each σ in G, define

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is an even permutation,} \\ -1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Prove that sgn is a homomorphism from G to the multiplicative group $\{+1, -1\}$. What is the kernel? Why does this homomorphism allow you to conclude that A_n is a normal subgroup of S_n of index 2?

Proof. If $\sigma, \tau \in G$ both are even or odd permutation, then $\sigma\tau$ is an even permutation and

$$1 = \operatorname{sgn}(\sigma\tau) = \begin{cases} 1 \cdot 1 = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau), & \text{if } \sigma \text{ and } \tau \text{ both are even;} \\ (-1) \cdot (-1) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau), & \text{if } \sigma \text{ and } \tau \text{ both are odd.} \end{cases}$$

If one of σ and τ is even and another one is odd, then $\sigma\tau$ is an odd permutation and $-1 = \operatorname{sgn}(\sigma\tau) = (-1) \cdot 1 = 1 \cdot (-1) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. ∎

10.10 Let G be a subgroup of some dihedral group. For each x in G, define

$$\phi(x) = \begin{cases} +1 & \text{if } x \text{ is a rotation,} \\ -1 & \text{if } x \text{ is a reflection.} \end{cases}$$

Prove that ϕ is a homomorphism from G to the multiplicative group $\{+1, -1\}$. What is the kernel? Why does this prove Exercise 25 of Chapter 3?

10.12 Suppose that k is a divisor of n. Prove that $\mathbb{Z}_n / \langle k \rangle \cong \mathbb{Z}_k$.

Proof. By First Isomorphism Theorem. ∎

10.24 Suppose that $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ is a group homomorphism with $\phi(7) = 6$.

(a) Determine $\phi(x)$.

(b) Determine the image of ϕ.

(c) Determine the kernel of ϕ.

(d) Determine $\phi^{-1}(3)$. That is, determine the set of all element that map to 3.

Proof. Observe that $7\cdot 7 = 49 = -1 \in \mathbb{Z}_{50}$. So $\phi(-1) = \phi(49) = \phi(7\cdot 7) = 7\phi(7) = 7\cdot 6 = 42 = 12 \in \mathbb{Z}_{15}$. Thus, $\phi(1) = \phi(-1\cdot -1) = -1\cdot\phi(-1) = -1\cdot 12 = -12 = 3 \in \mathbb{Z}_{15}$. Hence, $\phi(x) = \phi(x\cdot 1) = x\phi(1) = 3x$.

$$\mathrm{Im}(\phi) = \langle 3\rangle.$$

$$\begin{aligned}\ker\phi &= \{x \in \mathbb{Z}_{50} \mid \phi(x) = 3x = 0 \in \mathbb{Z}_{15}\}\\ &= \{x \in \mathbb{Z}_{50} \mid 15 \mid 3x\}\\ &= \{x \in \mathbb{Z}_{50} \mid 5 \mid x\}\\ &= \langle 5\rangle.\end{aligned}$$

$$\begin{aligned}\phi^{-1}(3) &= \{x \in \mathbb{Z}_{50} \mid \phi(x) = 3x = 3 \in \mathbb{Z}_{15}\}\\ &= \{x \in \mathbb{Z}_{50} \mid 15 \mid (3x-3)\}\\ &= \{x \in \mathbb{Z}_{50} \mid 5 \mid (x-1)\}\\ &= 1 + \langle 5\rangle.\end{aligned}$$

■

Proof. 另解: Since $\mathbb{Z}_{50} = \langle 7\rangle$. $\phi(c\cdot 7) = c\phi(7) = c\cdot 6$.

$$\begin{aligned}\mathrm{Im}(\phi) &= \{\phi(c\cdot 7) \mid c\cdot 7 \in \mathbb{Z}_{50}\}\\ &= \{c\cdot 6 \mid c \in \mathbb{Z}\}\\ &= \langle 6\rangle.\end{aligned}$$

$$\begin{aligned}\ker\phi &= \{c\cdot 7 \in \mathbb{Z}_{50} \mid \phi(c\cdot 7) = 0\}\\ &= \{c\cdot 7 \in \mathbb{Z}_{50} \mid 15 \mid (c\cdot 6)\}\\ &= \{c\cdot 7 \in \mathbb{Z}_{50} \mid 5 \mid (c\cdot 2)\}\\ &\overset{\substack{\gcd(5,2)=1\\ \downarrow}}{=} \{c\cdot 7 \in \mathbb{Z}_{50} \mid 5 \mid c\}\\ &\overset{\substack{\langle 7\rangle=\mathbb{Z}_{50}\\ \downarrow}}{=} \{c \in \mathbb{Z}_{50} \mid 5 \mid c\}\\ &= \langle 5\rangle.\end{aligned}$$

We use a lemma to find $\phi^{-1}(3)$: if $f : G \to G'$ is a group homomorphism and $H = \ker f$, then $xH = Hx = f^{-1}(f(x))$ for any $x \in G'$.

$$\phi^{-1}(3) = \phi^{-1}(18) = \phi^{-1}(3\cdot 6) = \phi^{-1}(3\cdot\phi(7)) = \phi^{-1}(\phi(3\cdot 7)) = 3\cdot 7 + \ker\phi = 21 + \langle 5\rangle.$$

■

補充. 上面求 $\phi^{-1}(3)$ 所用的 lemma 是比較 tricky 的, 所以你硬算 $\phi^{-1}(3)$ 也無妨, 不過你要注意到, 上面的 lemma 的另一個應用是, 證明 the kernel of a group homomorphism is normal.

給定 homomorphism $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$, $\phi(s) = t$. 如果 $\mathbb{Z}_m = \langle s\rangle$, 則 $\mathrm{Im}(\phi) = \langle t\rangle$。如果要求 $\ker\phi$, 則先求出 $\phi(1)$。

10.25* How many homomorphisms are there from Z_{20} onto Z_{10}? How many are there to Z_{10}?

Proof. To determine a homomorphism, it is sufficient to determine the image $\varphi(1)$ of $1 \in \mathbb{Z}_{20}$ because 1 is a generator of $\mathbb{Z}_{20}$.

If φ is an onto homomorphism from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{10}$, then $\varphi(1)$ must be a generator of $\mathbb{Z}_{10}$. Thus, $\varphi(1) \in \{1, 3, 7, 9\}$ because $1, 3, 7$ and 9 are all the generators of $\mathbb{Z}_{20}$. Thus, there are 4 onto homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{10}$.

If φ is a homomorphism from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{10}$, then $\varphi(1) \in \mathbb{Z}_{10}$ and there are 10 possibilities of $\varphi(1)$. ■

提示. 4, 10.

To determine a homomorphism φ from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{10}$, it is sufficient to determine the image $\varphi(1)$ of $1 \in \mathbb{Z}_{20}$ because 1 is a generator of $\mathbb{Z}_{20}$.

If φ is an onto homomorphism from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{10}$, then $\varphi(1)$ must be a generator of $\mathbb{Z}_{10}$.

If φ is a homomorphism from $\mathbb{Z}_{20}$ to $\mathbb{Z}_{10}$, then $\varphi(1) \in \mathbb{Z}_{10}$.

10.27 Determine all homomorphisms from $\mathbb{Z}_n$ to itself.

Proof. For each $k \in \mathbb{Z}_n$, $\theta_k(1) = k$ is a homomorphism from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. ■

10.41 (Second Isomorphism Theorem) If K is a subgroup of G and N is a normal subgroup of G, prove that $K/(K \cap N)$ is isomorphic to KN/N.

Proof. Define a mapping $f : KN \to K/(K \cap N)$ by $f(kn) = k(K \cap N)$. Then

$$\begin{aligned}
f((k_1 n_1)(k_2 n_2)) &= f(k_1 \underline{k_2 k_2^{-1}} n_1 (k_2^{-1})^{-1} n_2) \\
&= f(k_1 k_2 \underline{k_2^{-1} n_1 (k_2^{-1})^{-1}} n_2) \\
&\overset{N \lhd G,\ k_2^{-1} n_1 (k_2^{-1})^{-1} \in N}{\overset{\downarrow}{=}} f(k_1 k_2 n_3 n_2) \\
&= k_1 k_2 (N \cap K) \\
&= k_1 (N \cap K) \cdot k_2 (N \cap K) \\
&= f(k_1 n_1) \cdot f(k_2 n_2).
\end{aligned}$$

That is, f is a homomorphism. For any $k(K \cap N) \in K/(K \cap N)$, there exists $k \cdot 1 \in KN$ such that $f(k1) = k(K \cap N)$. That is, f is onto. We show that the kernel of f is N.

$$\begin{aligned}
\ker f &= \{kn \in KN \mid f(kn) = e_{K/K \cap N}\} \\
&= \{kn \in KN \mid k(K \cap N) = K \cap N\} \\
&= \{kn \in KN \mid k \in K \cap N\} \\
&= \{kn \in KN \mid k \in N\} \\
&\subseteq N.
\end{aligned}$$

On the other hand, if $n \in N$, then $f(n) = f(1 \cdot n) = 1(K \cap N) = K \cap N$ and $n \in \ker f$ and $N \subseteq \ker f$. Thus, $\ker f = N$. Finally, by the First Isomorphism Theorem,

$$KN/N = KN/\ker f \cong \operatorname{Im} f \overset{\overset{f \text{ is onto}}{\downarrow}}{=} K/(K \cap N).$$

■

提示. Define $f : KN \to K/K \cap N$ by.... Show that f is an onto homomorphism with kernel N. Then by the First Isomorphism Theorem.

補充. 注意到這個定理跟 p.150, thm.7.2的相似性。

10.42 (Third Isomorphism Theorem) If M and N are normal subgroups of G and $N \le M$, prove that $(G/N)/(M/N) \cong G/M$.

10.43 Let $\phi(d)$ denote the Euler phi function of d (see page 85). Show that the number of homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_k$ is $\sum \phi(d)$, where the sum runs over all common divisors d of n and k. [It follows from number theory that this sum is actually $\gcd(n,k)$.]

10.44 Let K be a divisor of n. Consider the homomorphism from $U(n)$ to $U(k)$ given by $x \to x \mod k$. What is the relationship between this homomorphism and the subgroup $U_k(n)$ of $U(n)$?

10.45* Determine all homomorphic images of D_4 (up to isomorphism).

Proof. If φ is a homomorphism from G_1 to another group G_2, then by The First Isomorphism Theorem, $\varphi(G_1) \cong G_1/\ker\varphi$. Recall that $\ker\varphi$ is a normal subgroup of G_1. On the other hand, for any normal subgroup N of G_1, there is a homomorphism φ whose kernel is N. In fact, it is $\varphi : G_1 \to G_1/N$ defined by $\varphi(g) = gN$.

Since $[D_4 : \langle a \rangle] = 2$, $\langle a \rangle$ is a normal subgroup of order 4 in D_4. There is a homomorphism φ with kernel $\langle a \rangle$. In this case, $D_4/\ker\varphi \cong \mathbb{Z}_2$.

If H is another normal subgroup of D_4 which is of order 4 and φ is a homomophism with kernel H, then we still have $D_4/\ker\varphi \cong \mathbb{Z}_2$ because there is only one group of order 2 (up to isomorphism).

There is only one normal subgroup of order 2 in D_4, it is $Z(D_4) = \langle a^2 \rangle$. (One cau apply the Theorem "$K \le \overset{\text{cyclic}}{H} \lhd G \Rightarrow K \lhd G$" on $\langle a^2 \rangle \le \overset{\text{cyclic}}{\langle a \rangle} \lhd D_4$ to get that $\langle a^2 \rangle \lhd D_4$.) Suppose that φ is a homomorphism from D_4 to another group and $\ker\varphi = \langle a^2 \rangle$. Then in the factor group $D_4/\langle a^2 \rangle = \{\langle a^2 \rangle, a\langle a^2 \rangle, b\langle a^2 \rangle, ba\langle a^2 \rangle\}$,

$$(a\langle a^2 \rangle)^2 = (b\langle a^2 \rangle)^2 = (ba\langle a^2 \rangle)^2 = \langle a^2 \rangle.$$

Thus, $\varphi(D_4) \cong D_4/\langle a^2 \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

If $\ker\varphi = D_4$, that is, the homomorphism φ assign every element of D_4 to the identity, then $\varphi(D_4) \cong D_4/\ker\varphi = D_4/D_4 \cong \{e\}$.

If $\ker\varphi = \{e\}$, that is, the homomorphism φ is one-to-one, then $\varphi(D_4) \cong D_4/\ker\varphi = D_4/\{e\} \cong D_4$. ■

提示.

- If φ is a homomorphism from D_4 to another group G, then show that $\ker\varphi$ is a normal subgroup of D_4.
- By The First Isomorphism Theorem, $\varphi(D_4) \cong$ ________.
- For any normal subgroup N of D_4, show that the mapping $\varphi : D_4 \to D_4/N$ defined by $\varphi(g) = gN$ is a homomorphism.
- For any normal subgroup N of D_4, what is the kenel of the homomorphism $\varphi : D_4 \to D_4/N$ defined by $\varphi(g) = gN$.
- For any normal subgroup N of D_4, there is a homomorphism from D_4 to another group whose kernel is N.
- $\langle a \rangle$ is a normal subgroup of order 4 in D_4. There is a homomorphism φ with kernel $\langle a \rangle$. In this case, $D_4/\ker\varphi \cong$ ________.
- If H is another subgroup of order 4 in D_4 and φ is a homomophism with kernel H, then we still have $D_4/\ker\varphi \cong$ ________ because there is only one group of order 2 (up to isomorphism).
- Show that $Z(D_4) = \langle a^2 \rangle$.
- Show that $\langle a^2 \rangle \lhd D_4$.
- Show that there is only one normal subgroup of order 2 in D_4.
- Show that $D_4/\langle a^2 \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- There is a homomorphism φ from D_4 to another group whose kernel is $\langle a^2 \rangle$. By The First Isomorphism Theore, $\varphi(D_4) \cong D_4/\ker\varphi =$ ________.
- You should consider the cases $\ker\varphi = D_4$ and $\ker\varphi = \{e\}$.

10.46 Let G be a finite group and let H be a normal subgroup of G. Prove that the order of the element gH in G/H must divide the order of g in G.

Proof. $(gH)^{|g|} = g^{|g|}H = eH = H$ implies that $|gH|$ divide $|g|$. ■

補充. 更一般地, 如果 $|g| < \infty$ 且 θ 是一個 homomorphism, 那我們有 $|\theta(g)|$ 整除 $|g|$。在這個觀點之下, 這題就只是這個定理的一個特例。

Correspondence Theorem

10.51* Let N be a normal subgroup of a group G. Prove that every subgroup of G/N has the form H/N, where H is a subgroup of G.

Proof. Suppose that S is a subgroup of G/N. Let $H = \{h \in G \mid hN \in S\}$. We claim that H is a subgroup of G.

Since S is a subgroup of G/N, we have $1N \in S$. It follows that $1 \in H$. If $h_1, h_2 \in H$, then $h_1N, h_2N \in S$ and $(h_1N)(h_2N) = (h_1h_2)N \in S$ because that S is closed under its operation. Thus, $h_1h_2 \in H$. Note that $h_1^{-1}N = (h_1N)^{-1} \in S$ because S is a subgroup of G/N. Therefore, $h_1^{-1} \in H$ and H is a subgroup of G. $S = H/N$ follows immediately from the definition of H. ■

提示. If S is a subgroup of G/N, then show that $H = \{h \in G \mid hN \in S\}$ is a subgroup of G and $S = H/N$.

補充. 這個定理叫correspondence theorem, 它刻劃了G跟G/N之間的對應關係。要注意到, G/N跟G比起來是相對小 (且簡單) 的, 這個定理可以幫助我們透過分析G/N來獲取G的資訊。

跟exe 9.51比較一下。

10.59* Suppose that H and K are distinct subgroups of G of index 2. Prove that $H \cap K$ is a normal subgroup of G of index 4 and that $G/(H \cap K)$ is not cyclic.

Proof. If $K = HK$, then $H \le K$. Hence,

$$\overbrace{H \le K \underbrace{\le}_{2} G}^{2}.$$

By Exercise 7.33, we get $[K : H] = 1$ and $H = K$, a contradiction. Thus, $HK \ne K$ and $[HK : K] \ne 1$. Then we have

$$\overbrace{K \underbrace{\le}_{\ne 1} HK \le G}^{2}.$$

By Exercise 7.33 again, we have $[G : HK] = 1$ and $G = HK$.

Since $[G : K] = 2$, we have $K \lhd G$. By Exercise 10.41, $[H : H \cap K] = [HK : K]$. Therefore,

$$\begin{aligned}
& [G : H \cap K] \\
\overset{\overset{H\cap K\le H\le G,\ \text{Exercise 7.33}}{\downarrow}}{=} \quad & [G : H] \cdot [H : H \cap K] \\
= \quad & [G : H] \cdot [HK : K] \\
\overset{\overset{K\le HK\le G,\ \text{Exercise 7.33}}{\downarrow}}{=} \quad & [G : H] \cdot \frac{[G : K]}{[G : HK]} \\
\overset{\overset{[G:HK]=1}{\downarrow}}{=} \quad & [G : H] \cdot [G : K] = 4.
\end{aligned}$$

Finally,

$$\begin{aligned}
& |G/H| = 2 = |G/K| \\
\Rightarrow \quad & \forall g \in G, (gH)^2 = H \in G/H \text{ and } (gK)^2 = K \in G/K \\
\Rightarrow \quad & g^2 \in H \text{ and } g^2 \in K \\
\Rightarrow \quad & g^2 \in H \cap K \\
\Rightarrow \quad & [g(H \cap K)]^2 = g^2(H \cap K) = H \cap K \\
\Rightarrow \quad & G/(H \cap K) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \text{ and it is not cyclic.}
\end{aligned}$$

■

提示.

- If $K = HK$, then $H \le K$. We have

$$\overbrace{H \le K \underbrace{\le}_{2} G}^{2}.$$

By Exercise 7.33, and $H = \underline{\qquad\qquad}$, a contradiction. Thus, $HK \ne K$.

- Then

$$\overbrace{K \underbrace{\le}_{\neq 1} HK \le G}^{2}.$$

By Exercise 7.33 again, we have $G = \underline{\qquad\qquad}$ and $[G : HK] = \underline{\qquad\qquad}$.

- By Exercise 10.41, $[H : H \cap K] = \underline{\qquad\qquad}$. Therefore,

$$\begin{aligned}
& [G : H \cap K] \\
\overset{H\cap K \le H \le G,\ \text{Exercise 7.33}}{\overset{\downarrow}{=}} \quad & [G : H] \cdot \underline{\qquad\qquad} \\
= \quad & [G : H] \cdot [HK : K] \\
\overset{K \le HK \le G,\ \text{Exercise 7.33}}{\overset{\downarrow}{=}} \quad & [G : H] \cdot \frac{[G : K]}{[G : HK]} \\
\overset{[G:HK]=1}{\overset{\downarrow}{=}} \quad & [G : H] \cdot \underline{\qquad\qquad} = 4.
\end{aligned}$$

- Finally,

$$\begin{aligned}
& |G/H| = 2 = |G/K| \\
\Rightarrow \quad & \forall g \in G, (gH)^2 = H \in G/H \text{ and } \underline{\qquad\qquad} \\
\Rightarrow \quad & g^2 \in H \text{ and } \underline{\qquad\qquad} \\
\Rightarrow \quad & g^2 \in H \cap K \\
\Rightarrow \quad & [g(H \cap K)]^2 = g^2(H \cap K) = H \cap K \\
\Rightarrow \quad & G/(H \cap K) \cong \underline{\qquad\qquad} \\
\Rightarrow \quad & G/H \cap K \text{ is not cyclic.}
\end{aligned}$$

補充. 下面是另外一種解法, 首先, 我們需要一個 Lemma。

Lemma.[2] In a group G, show that the intersection of a left coset of $H \le G$ and a left coset of $K \le G$ is either empty or a left coset of $H \cap K$.

By this Lemma, we show that $H \cap K, (g_1H) \cap K, H \cap (g_2K), (g_1H) \cap (g_2K)$ all are distinct and nonempty. Then $H \cap K, (g_1H) \cap K, H \cap (g_2K), (g_1H) \cap (g_2K)$ are all the cosets of $H \cap K$ and $[G : H \cap K] = 4$.

10.61 Prove that every group of order 77 is cyclic. (Hint: the proof is similar to the one for the group of order 35)

Proof. By Lagrange's Theorem, for any $e \neq g \in G$, $|g| \in \{7, 11, 77\}$. If there is an element $g \in G$, $|g| = 77$, then $G = \langle g \rangle$ is a cyclic group. Thus, we suppose that for any $e \neq g \in G$, $|g| \neq 77$.

If for all nonidentity element g in G, $|g| = 7$, then G is consists of $6k$ elements of order 7 and the identity e. But $|G| = 77$ is not of the form $6k + 1$. Hence, there is at least an element a of order 11. Let $H = \langle a \rangle$. By a similar argument, there is an element b which is of order 7.

We claim that H is the only one subgroup of order 11 in G. If K is another subgroup of G whose order is 11, then $|HK| = \frac{|H|\cdot|K|}{|H\cap K|} = 121 > |G|$, which is impossible.

[2] Grillet's Abstract Algebra

Recall that for any $g \in G$, gHg^{-1} is also a subgroup of G with order $|H|$. By the uniqueness of H, $gHg^{-1} = H$ for all $g \in G$. It follows that $H \triangleleft G$ and $N(H) = G$.

In addition, H is of order 11, so H is a cyclic group and is abelian. Thus, $H \le C(H) \le G$ and

$$\overbrace{H \le C(H) \le G}^{11}.$$

Therefore, $[C(H) : H]$ divide 11.

If $[C(H) : H] = 11$, then $[G : C(H)] = 1$ and $C(H) = G$. Thus, $ba = ab$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$ and $|ab| = \text{l.c.m.}(|a|, |b|) = 77$, a contradiction.

If $[C(H) : H] = 1$, then $C(H) = H$ and

$$|N(H)/C(H)| = \frac{|N(H)|}{|C(H)|} = \frac{|G|}{|H|} = 7.$$

But $N(H)/C(H)$ is isomorphic to a subgroup of $\text{Aut } H \cong \text{Aut } \mathbb{Z}_7 \cong U(7)$, which is impossible because $7 = |N(H)/C(H)|$ does not divide $6 = |U(7)|$.

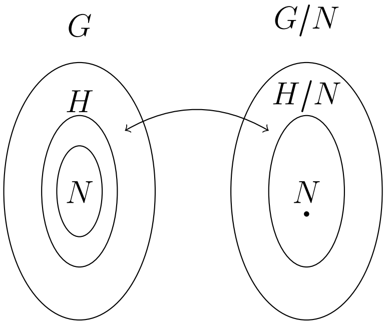
■

補充. 注意到, N/C theorem (p.217, exa.15) 跟 $G/Z(G) \cong \text{inn } G$ (p.194, thm.9.4) 兩者的證明方法是一樣的。

Correspondence Theorem

Let G be a group and $N \triangleleft G$. If H is a subgroup of G which contains N, then $H/N = \{hN \mid h \in H\}$ is a subgroup of G/N. On the other hand, for any subgroup $\mathcal{H}$ of G/N, there exists $H \le G$ such that $N \le H$ and $H/N = \mathcal{H}$.

補充.



Correspondence* Theorem

Let N be a normal subgroup of G and let H be a subgroup of G. If N is a subgroup of H, prove that H/N is a normal subgroup of G/N if and only if H is a normal subgroup of G.

Proof. ($\Leftarrow$) Suppose that H is a normal group of G. Note that

$$G/N = \{gN \mid g \in G\} \quad \text{and} \quad H/N = \{hN \mid h \in H\}.$$

Since $1 \in H \le G$, we have $1N \in H/N$. Note that $1N$ is the identity of the factor group G/N.

If $h_1N, h_2N \in H/N$, where $h_1, h_2 \in H$, then $h_1h_2 \in H$ and $(h_1N)(h_2N) = (h_1h_2)N \in H/N$. That is, H/N is closed under its operation.

If $hN \in H/N$, where $h \in H$, then $h^{-1} \in H$ and $(hN)^{-1} = h^{-1}N \in H/N$. Therefore, H/N is a subgroup of G/N.

For any $hN \in H/N$ and $gN \in G/N$,

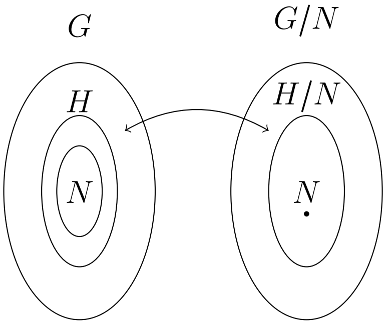
$$gN \cdot hN \cdot (gN)^{-1} = ghg^{-1}N \overset{H \lhd G,\ ghg^{-1} \in H}{\overset{\downarrow}{\in}} H/N.$$

That is, $H/N \lhd G/N$.

($\Rightarrow$) If $H/N = \{hN \mid h \in H\} \lhd G/N$, then for all $g \in G$ and $h \in H$, the coset $ghg^{-1}N = (gN)(hN)(g^{-1}N) \in H/N$. Which implies that $ghg^{-1}N = h_1N$ and $h_1^{-1}ghg^{-1} \in N \subseteq H$ for some $h_1 \in H$. Suppose that $h_1^{-1}ghg^{-1} = h_2$ for some $h_2 \in H$. Then $ghg^{-1} = h_1h_2 \in H$. Therefore, $gHg^{-1} \subseteq H$ and $H \lhd G$. ■

提示. $H/N = \{hN \mid h \in H\}$.

補充. 這個定理很重要, 叫做 Correspondence Theorem。如果 $N \lhd G$, 這個定理刻劃了 G 跟 G/N 之間的關係。也就是說, 在 G 裡面, 包含 N 的 normal subgroup 跟 G/N 的 normal subgroup 會有一一對應的關係, 事實上, 包含 N 的 subgroup 跟 G/N 的 subgroup 會是一一對應的, 如下圖所示, 參考 Exercise 10.51.



補充 10.A If $\phi : G \to H$ is an isomorphism, prove that $|\phi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$.

Proof. At first, we need to show that $\phi(e_G) = e_H$. For any $h \in H$, since ϕ is onto, there is an element $g \in G$ such that $\phi(g) = h$. Then

$$\phi(e_G) \cdot h = \phi(e_G) \cdot \phi(g) = \phi(e_G \cdot g) = \phi(g) = h.$$

Similarly, $h \cdot \phi(e_G) = h$. Thus, $\phi(e_G)$ is the identity of H and $\phi(e_G) = e_H$.

Now, we have

$$x^n = e_G \Rightarrow (\phi(x))^n = \phi(x^n) = \phi(e_G) = e_H$$

and

$$x^n = e_G \overset{\phi \text{ one-to-one and } \ker\phi = \{e_G\}}{\overset{\downarrow}{\Leftarrow}} (\phi(x))^n = \phi(x^n) = e_H.$$

That is,

$$x^n = e \Leftrightarrow (\phi(x))^n = e.$$

If $|x| < |\phi(x)|$, then $e = x^{|x|}$ and $(\phi(x))^{|x|} = e$, contrary to the minimality of $|\phi(x)|$. Thus, $|x| \geq |\phi(x)|$. By a similar argument, we can get $|x| \leq |\phi(x)|$. Therefore, $|x| = |\phi(x)|$.

For any fixed $n \in \mathbb{Z}^+$, let $X_n = \{x \in G \mid |x| = n\} \subseteq G$ and $Y_n = \{y \in H \mid |y| = n\} \subseteq H$. By the above discussion, $\phi(X_n) = \{\phi(x) \mid x \in X_n\} \subseteq Y_n$. On the other hand, for any $y \in Y_n$, since ϕ is onto, there exists an element $x \in G$ such that $\phi(x) = y$. Once again by the above discussion, $|x| = |\phi(x)| = |y| = n$. That is, $x \in X_n$ and $y = \phi(x) \in \phi(X_n)$. Therefore, $\phi(X_n) = Y_n$. Since ϕ is one-to-one, we have $|X_n| = |\phi(X_n)| = |Y_n|$.

■

11 Chapter 11

11.6 Show that there are two abelian groups of order 108 that have exactly four subgroups of order 3.

Proof. By the fundamental theorem of finite abelian groups, there are 6 abelian groups of order 108. They are

$$\begin{array}{rcl}
\mathbb{Z}_2 \oplus \mathbb{Z}_2 & \oplus & \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, \\
\mathbb{Z}_2 \oplus \mathbb{Z}_2 & \oplus & \mathbb{Z}_9 \oplus \mathbb{Z}_3, \\
\mathbb{Z}_2 \oplus \mathbb{Z}_2 & \oplus & \mathbb{Z}_{27}, \\
\mathbb{Z}_4 & \oplus & \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, \\
\mathbb{Z}_4 & \oplus & \mathbb{Z}_9 \oplus \mathbb{Z}_3, \\
\mathbb{Z}_4 & \oplus & \mathbb{Z}_{27}.
\end{array}$$

A group of order 3 must be isomorphic to the cyclic group of order 3. If a group has exactly four subgroups of order 3, then it must be has exactly 8 elements of order 3. The group which has exactly 8 elements of order in the above list are $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$. ■

提示.

- Show that a group of order 3 must be isomorphic to the cyclic group of order 3.
- Show that if a group has exactly four subgroups of order 3, then it must be has exactly 8 elements of order 3.
- In $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$, the four subgroups of order 3 are

$$\begin{array}{rcl}
\langle(0,0,1)\rangle & = & \{(0,0,0),(0,0,1),(0,0,2)\}, \\
\langle(0,3,0)\rangle & = & \{(0,0,0),(0,3,0),(0,6,0)\}, \\
\langle(0,3,1)\rangle & = & \{(0,0,0),(0,3,1),(0,6,2)\}, \\
\langle(0,3,2)\rangle & = & \{(0,0,0),(0,3,2),(0,6,1)\}.
\end{array}$$

- The answer is $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3$.

11.10 Find all abelian groups (up to isomorphism) of order 1800.

Proof. $1800 = 2^3 \cdot 3^2 \cdot 5^2$.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$	$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$	$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$	$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}$	$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}$

■

11.11 Prove that every finite Abelian group can be expressed as the (external) direct product of cyclic groups of orders $n_1, n_2, ..., n_t$, where n_{i+1} divides n_i for $i = 1, 2, ..., t-1$.

Proof. By the Fundamental Theorem of Finite Abelian Groups, write

$G \cong \underline{\mathbb{Z}_{p_1^{r11}} \oplus \mathbb{Z}_{p_1^{r12}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{r1s_1}}} \oplus \underline{\mathbb{Z}_{p_2^{r21}} \oplus \mathbb{Z}_{p_2^{r22}} \oplus \cdots \oplus \mathbb{Z}_{p_2^{r2s_2}}} \oplus \cdots \oplus \underline{\mathbb{Z}_{p_t^{rt1}} \oplus \mathbb{Z}_{p_t^{rt2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{rts_t}}},$

where $r_{ij} \le r_{i(j+1)}$ for $1 \le i \le t$ and $1 \le j \le s_u - 1$. We can rewrite G as

$$\begin{aligned} G \;\; &\cong \;\; \left(\mathbb{Z}_{p_1^{r11}} \oplus \mathbb{Z}_{p_2^{r21}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{rt1}}\right) \\ &\oplus \;\; \left(\mathbb{Z}_{p_1^{r12}} \oplus \mathbb{Z}_{p_2^{r22}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{rt2}}\right) \\ &\oplus \;\; \cdots \\ &\oplus \;\; \left(\mathbb{Z}_{p_1^{r1s_1}} \oplus \mathbb{Z}_{p_2^{r2s_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{rts_t}}\right). \end{aligned}$$

Then set

$$\begin{aligned} n_1 &= p_1^{r11} p_2^{r21} \cdots p_t^{rt1}, \\ n_2 &= p_1^{r12} p_2^{r22} \cdots p_t^{rt2}, \\ &\vdots \\ n_t &= p_1^{r1s_1} p_2^{r2s_2} \cdots p_t^{rts_t}. \end{aligned}$$

■

11.22* Suppose that G is a finite abelian group that has exactly one subgroup for each divisor of $|G|$. Show that G is cyclic.

Proof. By The Fundamental Theorem of Finite Abelian Groups, we can write G as

$$G \cong \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{r_s}},$$

where $p_1, p_2, ..., p_s$ are prime but not necessarily all distinct and $r_1, r_2, ..., r_s$ are positive integers.

If $p_i = p_j$ for some $i \neq j$, then

$$\mathbb{Z}_{p_i^{r_i}} \oplus \mathbb{Z}_{p_j^{r_j}} = \mathbb{Z}_{p_i^{r_i}} \oplus \mathbb{Z}_{p_i^{r_j}} \cong H \le G.$$

In this case, there are two distnct subgroups of order p_i generated by $(p_i^{r_i-1}, 0)$ and $(0, p_i^{r_i-1})$ in $\mathbb{Z}_{p_i^{r_i}} \oplus \mathbb{Z}_{p_i^{r_j}}$, respectively. So is H and G, a contradiction. Therefore, $p_1, p_2, ..., p_s$ all are distinct and G is cyclic. ■

提示. By The Fundamental Theorem of Finite Abelian Groups, we can write G as

$$G \cong \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{r_s}},$$

where $p_1, p_2, \ldots, p_s$ are prime but not necessarily all distinct and $r_1, r_2, \ldots, r_s$ are positive integers. If $p_i = p_j$ for some $i \neq j$, then

$$\mathbb{Z}_{p_i^{r_i}} \oplus \mathbb{Z}_{p_j^{r_j}} = \mathbb{Z}_{p_i^{r_i}} \oplus \mathbb{Z}_{p_i^{r_j}} \cong H \leq G.$$

In this case, show that there are two distnct subgroups of order p_i in $\mathbb{Z}_{p_i^{r_i}} \oplus \mathbb{Z}_{p_i^{r_j}}$

11.23 Characterize those integers n such that the only Abelian groups of order n are cyclic.

Proof. Let G be a finite abelian group of order $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$, where $p_1, p_2, \ldots, p_s$ are distinct primes. If $r_i \geq 2$ for some $i \in \{1, 2, \ldots, s\}$, then by the Fundamental Theorem of Finite Abelian Groups, G maybe isomorphic to $\mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_i} \oplus \mathbb{Z}_{p_i^{r_i-1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{r_s}}$. Which is not cyclic by p.166, Corollay 2. Thus, $r_1 = r_2 = \cdots = r_s = 1$. By the Fundamental Theorem of Finite Abelian Groups and p.166, Corollay 2 again, $G \cong \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \cdots \oplus \mathbb{Z}_{p_s} \cong \mathbb{Z}_{p_1 p_2 \cdots p_s}$ is a cyclic. ∎

11.29 Suppose that G is an abelian group of order 9. What is the maximum number of elements (excluding the identity) of which one needs to compute the order to determine the isomorphism class of G? What if G has order 18? What about 16?

Proof. The answer is 3, 6 and 12.

我解釋一下題目的意思。以 $|G| = 16$ 爲例, 題目的意思是說, 我們手上有一個 abelian group G, 我們目前只知道 G 的 order 是 16, Fundamental Theorem of Finite Abelian Groups 告訴我們, G 有五種可能,

$$\begin{gathered}\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4,\\ \mathbb{Z}_2 \oplus \mathbb{Z}_8,\\ \mathbb{Z}_4 \oplus \mathbb{Z}_4,\\ \mathbb{Z}_{16}.\end{gathered}$$

我們可以藉由去計算 G 裡面全部元素的 order, 來決定 G 到底跟列表中的哪一個 abelian group 是 isomorphic 的。但我們其實不用把 G 裡面的每一個元素的 order 都計算完才能決定他跟哪一個 abelian group 是 isomorphic, 因爲啊, 我們來看下表,

$d\backslash G$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$	$\mathbb{Z}_4 \oplus \mathbb{Z}_4$	$\mathbb{Z}_2 \oplus \mathbb{Z}_8$	$\mathbb{Z}_{16}$
16	0	0	0	0	8
8	0	0	0	8	4
4	0	8	12	4	2
2	16	7	3	3	1

這個表格分別列出了五個 abelian group 裡面, order爲 d 的元素的個數。所以, 我們任意地一個一個抓 G 中的元素, 不抓 identity, 然後去看這個元素的 order, 譬如說, 我抓到 1 個元素, 並算出這個元素的 order 是16, 那我就可以確定 $G \cong \mathbb{Z}_{16}$; 如果我抓了 9 個元素, 其中 5 個元素的 order 都是 4, 另外 4 個元素的 order 都是 2, 那麼我就可以知道 $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$; 如果我抓到 2 個 order 是 2 的元素, 5 個 order 是 4 的元素, 那我還不能確定 G, 我只能知道 $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$ 或是 $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$。

照著上面討論的方法, 我們最多只要抓 12 個元素就能決定 G 到底跟哪一個 abelian 是 isomorphic 的, 而這個情況就是抓到 8 個 order 爲 4 的元素及 3 個 order 爲 2 的元素, 這個時候我們就可以知道 $G \cong G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$ 或是 $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$, 此時再多抓一個元素就能決定它跟哪一個 abelian group 是 isomorphic。

$|G| = 9$

$d\backslash G$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_9$
9	0	6
3	8	2

$|G| = 18$

$d\backslash G$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$	$\mathbb{Z}_9 \oplus \mathbb{Z}_2$
18	0	6
9	0	6
6	8	2
3	8	2
2	1	1

■

提示. 我解釋一下題目的意思。以 $|G| = 16$ 爲例, 題目的意思是說, 我們手上有一個 abelian group G, 我們目前只知道 G 的 order 是 16, Fundamental Theorem of Finite Abelian Groups 告訴我們, G 有五種可能,

$$\begin{gathered}\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4,\\ \mathbb{Z}_2 \oplus \mathbb{Z}_8,\\ \mathbb{Z}_4 \oplus \mathbb{Z}_4,\\ \mathbb{Z}_{16}.\end{gathered}$$

我們可以藉由去計算 G 裡面全部元素的 order, 來決定 G 到底跟列表中的哪一個 abelian group 是 isomorphic 的。但我們其實不用把 G 裡面的每一個元素的 order 都計算完才能決定他跟哪一個 abelian group 是 isomorphic, 因爲啊, 我們來看下表,

$d\backslash G$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$	$\mathbb{Z}_4 \oplus \mathbb{Z}_4$	$\mathbb{Z}_2 \oplus \mathbb{Z}_8$	$\mathbb{Z}_{16}$
16	0	0	0	0	8
8	0	0	0	8	4
4	0	8	12	4	2
2	16	7	3	3	1

這個表格分別列出了五個 abelian group 裡面, order爲 d 的元素的個數。所以, 我們任意地一個一個抓 G 中的元素, 不抓 identity, 然後去看這個元素的 order, 譬如說, 我抓到 1 個元素, 並算出這個元素的 order 是16, 那我就可以確定 $G \cong \mathbb{Z}_{16}$; 如果我抓了 9 個元素, 其中 5 個元素的 order 都是 4, 另外 4 個元素的 order 都是 2, 那麼我就可以知道 $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$; 如果我抓到 2 個 order 是 2 的元素, 5 個 order 是 4 的元素, 那我還不能確定 G, 我只能知道 $G \cong G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$ 或是 $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$。

照著上面討論的方法, 我們最多只要抓 12 個元素就能決定 G 到底跟哪一個 abelian 是 isomorphic 的, 而這個情況就是抓到 8 個 order 爲 4 的元素及 3 個 order 爲 2 的元素, 這個時候我們就可以知道 $G \cong G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$ 或是 $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, 此時再多抓一個元素就能決定它跟哪一個 abelian group 是 isomorphic。

11.36 Suppose that G is a finite Abelian group. Prove that G has order p^n, where p is prime, if and only if the order of every element of G is a power of p.

Proof. ($\Rightarrow$) It follows immediately from Lagrange's Theorem.

($\Leftarrow$) If $p \neq q$ divides $|G|$, since G is a finite abelian, by the Fundamental Theorem of Finite Abelian Group, there exists a subgroup H of G such that $\mathbb{Z}_{q^{r_1}} \oplus \mathbb{Z}_{q^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{q^{r_t}} \cong H \leq G$. Hence, there is an element of order q^{r_1} in $\mathbb{Z}_{q^{r_1}} \oplus \mathbb{Z}_{q^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{q^{r_t}}$, so is in G, contrary to the hypothesis. ■

補充. 事實上, 這題的 abelian 這個條件可以拿掉, 並用 Cauchy Theorem 證明。order爲 prime p power 的 group 稱爲 p-group。

12 Chapter 12

12.7 Show that the three properties listed in Exercise 6 are valid for $\mathbb{Z}_p$, where p is prime.

Proof. Because $\mathbb{Z}_p$ is a finite field, so $\mathbb{Z}_p$ is also an integral domain. ■

12.9 Prove that the intersection of any collection of subrings of a ring R is a subring of R.

12.12 Let a, b, and c be elements of a commutative ring, and suppose that a is a unit. Prove that b divides c if and only if ab divide c.

Proof. Let R be a commutative ring and $a, b, c \in R$.

$$\begin{aligned} & b \mid c \\ \Rightarrow\ & c = bq \text{ for some } q \in R \\ \Rightarrow\ & c = 1 \cdot bq = (a^{-1}a)bq \overset{R \text{ is commutative}}{\overset{\downarrow}{=}} ab(a^{-1}q) \\ \Rightarrow\ & ab \mid c. \end{aligned}$$

■

12.13 describe all the subrings of the ring of integers.

Proof. Note that $\mathbb{Z}$ is a cyclic group under addition. Recall that a subgroup group of a cyclic group must be also a cyclic group. Thus, a subgroup of $(\mathbb{Z}, +)$ is of the form $\langle m\rangle = \{n \cdot m \mid n \in \mathbb{Z}\}$. It is easy to verify that $\langle m\rangle = m\mathbb{Z}$ is also a subring of $\mathbb{Z}$. ■

12.14 Let a and b belong to a ring R and let m be an integer. Prove that $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$.

12.15 Show that if m and n are integers and a and b are elements from a ring, then $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$.

12.16 Show that if n is an integer and a is an element from a ring, then $n \cdot (-a) = -(n \cdot a)$.

Proof. Show that $n \cdot a + n \cdot (-a) = 0$. Then by the uniqueness of the additive inverse. ■

12.19 Let R be a ring. The center of R is the set $\{x \in R \mid ax = xa \text{ for all } a \text{ in } R\}$. Prove that the center of a ring is a subring.

12.22 Let R be a commutative ring with unity and let $U(R)$ denote the set of units of R. Prove that $U(R)$ is a group under the multiplication of R. (This group is called the group of units of R.)

12.23 Determine $U(\mathbb{Z}[i])$.

提示. $|a + bi| = a^2 + b^2$.

Proof. Let $|a + bi| = a^2 + b^2$ be the norm of the complex number. Suppose that $a + bi, c + di \in \mathbb{Z}[i]$ and $(a + bi)(c + di) = 1$. Then

$$1 = |1| = |(a + bi)(c + di)| = |a + bi| \cdot |c + di| = (a^2 + b^2)(c^2 + d^2).$$

Since $a, b \in \mathbb{Z}$, we get $a + bi \in \{1, -1, i, -i\}$. ■

補充. 下面是較基本但暴力的做法。

Suppose that $a + bi, c + di \in \mathbb{Z}[i]$ and

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i = 1.$$

Then

$$\begin{cases} ac - bd = 1 \\ ad + bc = 0 \end{cases} \tag{15}$$

If $a = 0$, then $-bd = 1$ and $bc = 0$. It follows that $c = 0$ and $d = -b$ and $b \in \{1, -1\}$. That is, $(c + di) = -(a + bi)$ and $a + bi \in \{i, -i\}$.

If $b = 0$, then $ac = 1$ and $ad = 0$. It follows that $d = 0$ and $c = a \in \{1, -1\}$. That is, $c + di = a + bi \in \{1, -1\}$.

The cases $c = 0$ and $d = 0$ are similar.

Suppose that a, b, c and d are all nonzero. Solve the equations (15).

$$\begin{cases} acd - bd^2 = d \\ acd + bc^2 = 0 \end{cases}$$

We get $bd^2 + d + bc^2 = 0$ and $d = \frac{-1\pm\sqrt{1-4b^2c^2}}{2b}$. Since $d \in \mathbb{Z}$, the discriminant $1 - 4b^2c^2$ must be 0 or 1. If $1 - 4b^2c^2 = 0$, then $bc = \frac{1}{2}$, a contradiction. If $1 - 4b^2c^2 = 1$, then $b = 0$ or $c = 0$, contrary to the assumption.

12.24 If $R_1, R_2, ..., R_n$ are commutative rings with unity, show that $U(R_1 \oplus R_2 \oplus \cdots \oplus R_n) = U(R_1) \oplus U(R_2) \oplus \cdots \oplus U(R_n)$.

Proof. ($\subseteq$) If $(r_1, r_2, ..., r_n)$ is a unit of $R_1 \oplus R_2 \oplus \cdots \oplus R_n$, then there exists $(s_1, s_2, ..., s_n) \in R_1 \oplus R_2 \oplus \cdots \oplus R_n)$ such that $(r_1, r_2, ..., r_n) \cdot (s_1, s_2, ..., s_n) = (1_{R_1}, 1_{R_2}, ..., 1_{R_n})$. Thus, $s_i = r_i^{-1}$ and $r_i \in U(R_i)$ for all $i = 1, 2, ..., n$. ■

12.25 Determine $U(\mathbb{Z}[x])$.

Proof. ±1. ■

12.26 Determine $U(\mathbb{R}[x])$.

Proof. $U(\mathbb{R}[x]) = \{f(x) = r \in \mathbb{R}[x] \mid r \neq 0 \in \mathbb{R}\}$. [Hint: If $f(x)g(x) = 1$, then $0 = \deg 1 = \deg f(x) + \deg g(x)$. ■

12.27 Show that a unit of a ring divides every element of the ring.

Proof. Let u be a unit in a ring R. Then for any $r \in R$, $r = 1 \cdot r = (uu^{-1})r = u(u^{-1}r)$. ■

12.31 Give an example of ring elements a and b with the properties that $ab = 0$ but $ba \neq 0$.

Proof. $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ ■

12.35 Find an integer $n > 1$ such that $a^n = a$ for all a in $\mathbb{Z}_6$. Do the same for $\mathbb{Z}_{10}$. Show that no such n exists for $\mathbb{Z}_m$ when m is divisible by the square of some prime.

Proof. 觀察最小的例子, 也就是 $p = 2, m = 2^2 \cdot 3$, $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, ..., 11\}$, 注意到 $2^r \neq 2$ for all $r \in \mathbb{N}^+$。所以我們大膽地猜測: 如果 $m = p^2 \cdot s$, 則 $p \in \mathbb{Z}_m$, $p^r \neq p$ for all $r \in \mathbb{N}^+$。到這裡你不妨自己證明看看。

If $m = p^2 \cdot s$ and $p \in \mathbb{Z}_m$ and $p^n = p$ for some $n \in \mathbb{Z}$, then $p^n = p \in \mathbb{Z}_m$ and $p^n \equiv p \pmod{m = p^2 s}$. Therefore, $p^2 s \mid p^n - p$ and $ps \mid (p^{n-1} - 1)$ and $p \mid (p^{n-1} - 1)$, a contradiction. ■

12.36 Let m and n be positive integers and let k be the least common multiple of m and n. Show that $m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$.

12.37 Explain why every subgroup of $\mathbb{Z}_n$ under addition is also a subring of $\mathbb{Z}_n$.

12.38 Is $\mathbb{Z}_6$ a subring of $\mathbb{Z}_{12}$?

Proof. No. But there is a subring $\langle 2 \rangle$ of $\mathbb{Z}_{12}$ isomorphic to $\mathbb{Z}_6$. ■

12.40 Let $M_2(\mathbb{Z})$ be the ring of all 2×2 matrices over the integers and let

$$R = \left\{ \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

Prove or disprove that R is a subring of $M_2(\mathbb{Z})$.

12.41 Let $M_2(\mathbb{Z})$ be the ring of all 2×2 matrices over the integers and let

$$R = \left\{ \begin{pmatrix} a & a-b \\ a-b & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

Prove or disprove that R is a subring of $M_2(\mathbb{Z})$.

Proof. **Additive Identity:**

$$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1-0 \\ 1-0 & 1 \end{smallmatrix}\right) \in R.$$

Additive and Multiplicative Closed: For $\left(\begin{smallmatrix} a & a-b \\ a-b & b \end{smallmatrix}\right), \left(\begin{smallmatrix} c & c-d \\ c-d & d \end{smallmatrix}\right) \in R$,

$$\left(\begin{smallmatrix} a & a-b \\ a-b & b \end{smallmatrix}\right) + \left(\begin{smallmatrix} c & c-d \\ c-d & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+c & a-b+c-d \\ a-b+c-d & b+d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+c & (a+c)-(b+d) \\ (a+c)-(b+d) & b+d \end{smallmatrix}\right) \in R$$

and

$$\left(\begin{smallmatrix} a & a-b \\ a-b & b \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} c & c-d \\ c-d & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2ac\underline{-bc-ad}+bd & ac-bd \\ ac-bd & ac\underline{-bc-ad}+2bd \end{smallmatrix}\right) \in R.$$

Additive Inverse: For $\left(\begin{smallmatrix} a & a-b \\ a-b & b \end{smallmatrix}\right) \in R$,

$$-\left(\begin{smallmatrix} a & a-b \\ a-b & b \end{smallmatrix}\right) = \left(\begin{smallmatrix} -a & -a+b \\ -a+b & -b \end{smallmatrix}\right) \in R.$$

Therefore, R is a subring of $M_2(\mathbb{Z})$. ■

12.45 Let R be a ring with unity 1. Show that $S = \{n \cdot 1 \mid n \in \mathbb{Z}\}$ is a subring of R.

12.47 Determine the smallest subring of $\mathbb{Q}$ that contains 1/2. (That is, find the subring S with the property that S contains 1/2 and, if T is any subring containing 1/2, then T contains S.)

Proof. 不妨先觀察一下, 如果 S 是 $\mathbb{Q}$ 中含有 1/2 的最小 subring, 那麼因爲 S 是 subring, 所以有加法封閉, 加法反元素, 所以 $1/2 + 1/2 = 1 \in S$, 這麼一來, $\mathbb{Z} \subseteq S$。類似地, 因爲 S 有乘法封閉, 所以 $1/2 \cdot 1/2 = 1/4 \in S$。

事實上,

$$S = \bigcap_{1/2 \in A \leq \mathbb{Q}} A = \left\{ \frac{n_1}{2} + \frac{n_2}{2^2} + \cdots + \frac{n_s}{2^s} \mid n_i \in \mathbb{Z}, s \in \mathbb{N}^+ \right\}.$$

S 的最小性就留給你驗證。 ■

12.48 Determine the smallest subring of $\mathbb{Q}$ that contains 2/3.

Proof. 類似 Exercise 12.47。 ■

12.52 If a, b, and c are elements of a ring, does the equation $ax + b = c$ always have a solution x? If it does, must the solution be unique? Answer the same questions given that a is a unit.

Proof. No. No. Yes. Yes.

In $\mathbb{Z}_6$, $2x + 1 = 2$ has no solution. $2x + 3 = 3$ has two solutions.

If a is a unit, then $x = a^{-1}(c - b)$. ■

13 Chapter 13

13.4 List all zero-divisors in $\mathbb{Z}_{20}$. Can you see a relationship between the zero-divisors of $\mathbb{Z}_{20}$ and the units of $\mathbb{Z}_{20}$?

Proof.

$$\begin{aligned} & \gcd(a, 20) = 1 \\ \Leftrightarrow\ & \text{there exists } x, y \text{ such that } ax + 20y = 1 \\ \Leftrightarrow\ & ax - 1 = -20y \\ \Leftrightarrow\ & ax \equiv 1 \pmod{20} \\ \Leftrightarrow\ & ax = 1 \in \mathbb{Z}_{20} \\ \Leftrightarrow\ & a \text{ is a unit} \end{aligned}$$

If $a \neq 0 \in \mathbb{Z}_{20}$ and $\gcd(a, 20) = d \neq 1$, suppose that $a = ds$ and $20 = dt$ for some $s, t \in \mathbb{Z}$, then $at = (ds)t = (dt)s = 20s = 0 \in \mathbb{Z}_{20}$. Since $d \neq 1$, we have $20 \nmid t$ and $t \neq 0 \in \mathbb{Z}_{20}$. Thuse, a is a zero-divisor in $\mathbb{Z}_{20}$.

The unit in $\mathbb{Z}_{20}$ are $1, 3, 7, 9, 11, 13, 17, 19$.

The zero-divisor in $\mathbb{Z}_{20}$ are $2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18$.

Note that 0 is neither unit nor zero-divisor. ■

補充. zero-divisor跟 unit 在 multiplication table 上會有什麼特性?

考考你, 會不會有元素同時又是 unit 又是 zero-divisor?

13.5 Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.

提示. In general, if R is a finite commutative ring with unity, then every nonzero element in R is a unit or a zero-divisor.

Let $R = \{r_1, r_2, \ldots, r_n\}$ be a finite commutative ring with unity. If $0 \neq a \in R$ is not a zero-divisor, show that $aR = \{ar_1, ar_2, \ldots, ar_n\} = R$.

補充. 這個定理還可以更強, 不需要 commutative 這個條件, 不過證明就難多了。

13.7* Let R be a finite commutative ring with unity. Prove that every nonzero element of R is either a zero-divisor or a unit. What happens if we drop the "finite" condition on R?

提示. 這個 hint 要修改一下, 有很多學生看不懂。If $u \neq 0$ is not a zero divisor, then show that $uR = \{ur \mid r \in R\} = R$. Hence, $1 \in R = uR$ and $1 = ur$ for some $r \in R$.

13.9 Find elements a, b, and c in the ring $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ such that ab, ac, and bc are zero-divisors but abc is not a zero-divisor.

Proof. $a = (0,0,1), b = (0,1,0), c = (0,0,1)$. ■

13.10 Describe all zero-divisors and units of $\mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}$.

Proof. The set of all zero-divisor of $\mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}$ are $\{(a,b,c) \mid a, b$ and c at least one is 0 and not all $0\}$
$U(\mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}) = \{(\pm 1, r, \pm 1) \mid 0 \neq r \in \mathbb{Q}\}$. ■

13.11 * Let d be an integer. Prove that $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

補充. 你可以用定義證明, 但更聰明的方法, 是利用定理: a subring of a field which contains the unity is an integral domain.

13.12 In $\mathbb{Z}_7$, give a reasonable interpretation for the expressions $1/2$, $-2/3$, $\sqrt{-3}$, and $-1/6$.

Proof. 4, 4, 2, 1. ■

13.15 Let a belong to a ring R with unity and suppose that $a^n = 0$ for some positive integer n. (Such an element is called nilpotent.) Prove that $1 - a$ has a multiplicative inverse in R. [Hint: Consider $(1-a)(1+a+a^2+\cdots+a^{n-1})$.]

13.17 Show that 0 is the only nilpotent element in an integral domain.

13.18 A ring element a is called an idempotent if $a^2 = a$. Prove that the only idempotents in an integral domain are 0 and 1.

13.20 Show that $\mathbb{Z}_n$ has a nonzero nilpotent element if and only if n is divisible by the square of some prime.

提示. 類似 Exercise 12.35。一樣先觀察 $\mathbb{Z}_{12}$, $12 = 2^2 \cdot 3$, 觀察到 $\mathbb{Z}_{12}$ 中有一個 nonzero nilpotent element 6, 而這個 6 恰好是 $2 \cdot 3$, 所以我們大膽地猜測, 如果 $n = p^2 \cdot s$, 那麼 $ps \in \mathbb{Z}_n$ 是一個nonzero nilpotent element。

Proof. $(\Leftarrow)$ Suppose that $n = p^2 \cdot s$. Then $(ps)^2 = (p^2 s) \cdot s = 0 \in \mathbb{Z}_n$.

$(\Rightarrow)$ We prove that by contradiction. Suppose that $n = p_1 p_2 \cdots p_s$, where $p_1, p_2, \ldots, p_s$ are distinct prime. If $0 \neq a \in \mathbb{Z}_n$ and $a^r = 0$, then $p_1 p_2 \cdots p_s = n \mid a^r$ and $p_1 p_2 \cdots p_s = n \mid a$ and $a = 0$, a contradiction. ■

13.26 Find all units, zero-divisors, idempotents, and nilpotent elements in $\mathbb{Z}_3 \oplus \mathbb{Z}_6$.

Proof. 自己找。

nil這個字根有消滅的意思, 例如籃下消滅者—俠客-歐尼爾 (Shark O'Nil), 其實是 (Shaquille O'Neal), potent這個字有次方的意思, 所以 nilpotent 就是某次方之後會消失 (變成 0) 的元素。

而 idem 有相等的意思, 所以 idempotent 就是次方之後會等於自己的元素。 ■

13.29 (Subfield Test) Let F be a field and let K be a subsetof F with at least two elements. Prove that K is a subfield of F if, for any a, b $(b \neq 0)$ in K, $a - b$ and ab^{-1} belong to K.

Proof. 我講過, group裡面的 group 就是 subgroup, ring裡面的 ring 就是 subring。而 field 裡面的 field 就是 subfield, 你知道, field要滿足那 12 個條件,

for any $a, b, c \in F$	$+$	$\cdot$
closed	$a + b \in F$	$a \cdot b \in F$
associative	$(a+b)+c = a+(b+c)$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
identity	$\exists 0 \in F$ s.t. $a + 0 = 0 + a = a$	$\exists 1 \in F$ s.t. $a \cdot 1 = 1 \cdot a = a$
inverse	$\exists (-a) \in F$ s.t. $-a + a = a + (-a) = 0$	$\forall a \neq 0$, $\exists a^{-1} \in F$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1$
commutative	$a + b = b + a$	$a \cdot b = b \cdot a$
left distribution	$a \cdot (b + c) = a \cdot b + a \cdot c$	
right distribution	$(a + b) \cdot c = a \cdot c + b \cdot c$	

所以對於一個 field 的 subset, 我們要知道這個 subset 是不是 subfield, 我們就是要測試這個 subset 是不是也是一個 field, 所以同樣要對這個 subset 去驗證這 12 個條件。你一定要自己找一題來做, 你才會知道有哪些條件根本不用驗證, 因爲某些條件會繼承大的集合而來。

在這題中, 你要自己想想爲什麼課本說只要驗證 $a - b \in K$, $ab^{-1} \in K$ 就好, 這是因爲這兩個條件就蘊含了那 12 個條件。 ■

13.30 Let d be a positive integer. Prove that $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is a field.

Proof. $0 \in \mathbb{Q}[\sqrt{d}]$ is obviously. If $a + b\sqrt{d}, c + e\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, then

$$(a + b\sqrt{d}) + (c + e\sqrt{d}) = (a + c) + (b + e)\sqrt{d} \overset{\overset{a+c,b+e\in\mathbb{Q}}{\downarrow}}{\in} \mathbb{Q}[\sqrt{d}]$$

and

$$-(a + b\sqrt{d}) = (-a) + (-b)\sqrt{d} \overset{\overset{-a,-b\in\mathbb{Q}}{\downarrow}}{\in} \mathbb{Q}[\sqrt{d}].$$

Thus, $\mathbb{Q}[\sqrt{d}]$ is a subring of $\mathbb{R}$.

If $a^2 - b^2 d = 0$, then $\sqrt{d} = \frac{a}{b} \in \mathbb{Q}$ and $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}$ is a field. Thus, we suppose that $a^2 - b^2 d \neq 0$. If $a + b\sqrt{d} \neq 0$, then

$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{(a + b\sqrt{d})(a - b\sqrt{d})} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = \frac{a}{a^2 - b^2 d} + \frac{-b}{a^2 - b^2 d}\sqrt{d} \in \mathbb{Q}[\sqrt{d}].$$

Therefore, $a + b\sqrt{d} \neq 0$ has a multiplicative inverse in $\mathbb{Q}[\sqrt{d}]$ and $\mathbb{Q}[\sqrt{d}]$ is a field. ■

補充. 我們之後會學到其他方法, If $\sqrt{d} \in \mathbb{Q}$, then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ is a field. If $\sqrt{d} \notin \mathbb{Q}$, then $x^2 - d$ is always irreducible over $\mathbb{Q}$. It follows that $\langle x^2 - d \rangle$ is a maximal ideal in $\mathbb{Q}[x]$ and $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[x]/\langle x^2 - d \rangle$ is a field.

13.33 Formulate the appropriate definition of a subdomain (that is, a "sub" integral domain). Let D be an integral domain with unity 1. Show tat $P = \{n \cdot 1 \mid n \in \mathbb{Z}\}$ (that is all integral multiples of 1) is a subdomain of D. Show that P is contained in every subdomain of D. What can we say about the order of P?

Proof. Show that P is a subring of D. If $n \cdot 1, m \cdot 1 \in P$ and $(n \cdot 1) \cdot (m \cdot 1) = 0$, then $nm \cdot 1 = 0$. But the characteristic of $\mathbb{Z}$ is 0. Hence, $nm = 0$. Since $n, m \in \mathbb{Z}$ and $\mathbb{Z}$ is an integral domain, it follows that $m = 0$ or $n = 0$. That is $(n \cdot 1) = 0$ or $(m \cdot 1) = 0$ and P is an integral domain. ■

13.34 Prove that there is no integral domain with exacty six elements. Can your argument be adapted to show that there is no integral doman with exactly four elements? What about 15 elements? Use these observations to guess a general result about the number of elements in a finite integral domain.

Proof. 要用到 Exercise 13.51, 先看 Exercise 13.51。

The number of elements of a finite field must be a power of a prime. Since a finite integral domain must be a finite field, we have that the number of elements of a finite integral must be a power of a prime. ■

13.35 Let F be a field of order 2^n. Prove that char $F = 2$.

提示. Show that char F divide 2^n and by theorem: The characteristic of a field is a prime.

Proof. Since $(F, +)$ is an additive abelian group, by Lagrange's Theorem, $|F| \cdot 1 = 0$. Thus, the additive order of 1 divide $|F| = 2^n$. That is, the characteristic of F divide 2^n. The characteristic of a field is a prime. Hence, char $F = 2$. ■

13.36* Determine all elements of an integral domain that are their own inverses under multiplication.

Proof. Let D be an integral domain. If $a \in D$ and $a = a^{-1}$, then $a^2 = aa^{-1} = 1$ and $a^2 - 1 = 0$. Thus, $(a-1)(a+1) = 0$. Since D is an integral domain, it follows that $(a-1) = 0$ or $(a+1) = 0$. That is, $a \in \{1, -1\}$. On the other hand, the multiplicative inverse of 1 and -1 are themselves, The only possible are 1 and -1. ■

13.38* Determine all integers $n > 1$ for which $(n-1)!$ is a zero-divisor in $\mathbb{Z}_n$.

Proof. Since $\mathbb{Z}_n$ is a commutative ring with unity, by Exercise 13.7, every nonzero element of R is either a zero-divisor or a unit. Thus, $(n-1)!$ is a zero-divisor in $\mathbb{Z}_n$ if and only if $(n-1)!$ is not a unit and $(n-1)! \neq 0 \in \mathbb{Z}_n$.

$$\begin{aligned}
& (n-1)! \text{ is not a unit} \\
\Leftrightarrow\ & (n-1)!s \neq 1 \in \mathbb{Z}_n \text{ for all } s \in \mathbb{Z} \\
\Leftrightarrow\ & (n-1)!s - 1 \neq 0 \in \mathbb{Z}_n \text{ for all } s \in \mathbb{Z} \\
\Leftrightarrow\ & n \nmid (n-1)!s - 1 \text{ for all } s \in \mathbb{Z} \\
\Leftrightarrow\ & (n-1)!s - 1 \neq nq \text{ for all } s, q \in \mathbb{Z} \\
\Leftrightarrow\ & (n-1)!s - nq \neq 1 \text{ for all } s, q \in \mathbb{Z} \\
\Leftrightarrow\ & \gcd((n-1)!, n) \neq 1 \\
\Leftrightarrow\ & n \text{ is not a prime.}
\end{aligned}$$

$$\begin{aligned} & (n-1)! \neq 0 \in \mathbb{Z}_n \\ \Leftrightarrow\ & n \nmid (n-1)! \\ \Leftrightarrow\ & n \text{ is a prime or } n = 4. \\ & (\text{If } n = st \text{ and } 1 < s \neq t < n,\ \text{then } n = st \mid (n-1)! \\ & \text{If } n = p^2 \text{ for some prime } p \text{ and } p > 2,\ \text{then } p, 2p \leq p^2 - 1 \text{ and } n = p^2 \mid (p^2-1)!). \end{aligned}$$

Therefore, only when $n = 4$, $(n-1)!$ is a zero-divisor in $\mathbb{Z}_n$. ■

13.41 If a is an idempotent in a commutative ring, show that $1 - a$ is also an idempotent.

13.45* Show that a finite commutative ring with no zero-divisors and at least two elements has a unity.

Proof. 類似於 Exercise 13.7。

Let $0 \neq r \in R$. Suppose that $R = \{r_1, r_2, ..., r_n\}$. If $rr_i = rr_j$, then $r(r_i - r_j) = 0$ and $r_i = r_j$. Thus, $rR = \{rr_1, rr_2, ..., rr_n\} = R$.

Since $r \in R = rR$, there exists $s \in R$ such that $r = rs \overset{R \text{ is commutative}}{\overset{\downarrow}{=}} sr$. We show that s is the unity.

For all $t \in R = rR$, write $t = ru$. Then

$$ts \overset{R \text{ is commutative}}{\overset{\downarrow}{=}} st = s(ru) = (sr)u \overset{r=sr}{\overset{\downarrow}{=}} ru = t.$$

That is, s is the unity. ■

13.47* Suppose that R is a commutative ring without zero-divisors. Show that all the nonzero elements of R have the same additive order.

Proof. Let a and b are two nonzero elements in R. If n is a positive integer such that $na = 0$, then $0 = (na)b = (nb)a$. Since R has no zero-divisor and $a \neq 0$, we have $nb = 0$. Therefore, all the nonzero elements in R have the same additive order. ■

13.48 Suppose that R is a commutative ring without zero-divisors. Show that the characteristic of R is 0 or prime.

Proof. If char $R = n$, then we show that n is a prime.

Since char $R = n$, there exists an element $0 \neq a \in R$ such that $na = 0$ and $ma \neq 0$ for $1 \leq m < n$. If $n = st$ and $1 < s, t < n$, then $0 = na^2 = (st)a^2 = (sa)(ta)$. Since R has no zero-divisor, we have $sa = 0$ or $ta = 0$, both cases contrary to the minimality of n. Thus, n is a prime.

注意到這題的證明中, 說明了如果要證明 integral domain 的 characteristic 是 prime, unity這個條件是多餘的。 ■

13.49 Let x and y belong to a commutative ring R with prime characteristic p.

(a) Show that $(x+y)^p = x^p + y^p$.

提示. If p is a prime, then $p \mid \binom{p}{i}$ for $i = 1, 2, ..., p-1$.

補充. 這個定理很重要, 之後在學 field theory 還會再遇到。

(b) Show that, for all positive integers n, $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.

(c) Find elements x and y in a ring of characteristic 4 such that $(x+y)^4 \neq x^4 + y^4$.

提示. $\mathbb{Z}_4$.

Proof. $x = 1, y = 4 \in \mathbb{Z}_4$. ∎

13.51* Show that any finite field has order p^n, where p is a prime. [Hint: Use facts about finite Abelian groups.]

Proof. Let F be a finite field. Define a mapping $\theta : \mathbb{Z} \to F$ by $\theta(m) = m \cdot 1$. Show that θ is an one-to-one homomorphism. Suppose that char $F = p$. Then $\ker\theta = p\mathbb{Z}$. By the First Isomorphism Theorem for Ring, we have $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/\ker\theta \cong \mathrm{Im}\theta \leq F$. That is, F contains a subfield $\mathbb{Z}_p$ (up to isomorphism). Let F be a vector space over its subfield $\mathbb{Z}_p$. The scalar multiplication is the same as the multiplication in F. Suppose that $\dim_{\mathbb{Z}_p} F = n$ and $\{v_1, v_2, \ldots, v_n\}$ is a basis for ${}_{\mathbb{Z}_p}F$. Then $F = \{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \mid \lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{Z}_p\}$ and $|F| = p^n$ because there are p choices for each λ_i. ∎

13.53 Let R be a ring and let $M_2(R)$ be the ring of 2×2 matrices with entries from R. Explain why these two rings have the same characteristic.

13.54 Let R be a ring with m elements. Show that the characteristic of R divides m.

Proof. Recall that $(R, +)$ is a group. If the characteristic of R is n, then there exists an elememt $r \in R$ whose additive order is n. By Lagrange's Theorem, the order of an element must divide the order of the group. Thus, char $R = n = |r|$ divide $|R| = m$. ∎

13.56 Find all solutions of $x^2 - x + 2 = 0$ over $\mathbb{Z}_3[i]$.

提示. $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$.

Proof. Suppose that $a + bi$ is a solution of $x^2 - x + 2 = 0$, where $a, b \in \mathbb{Z}_3$. Then $(a+bi)^2 - (a+bi) + 2 = 0$ and

$$\begin{cases} a^2 - b^2 - a + 2 = 0 \\ 2ab - b = 0 \end{cases}$$

If $b = 0$, then $a^2 - a + 2 = 0$. But there are no element in $\mathbb{Z}_3$ satisfying $a^2 - a + 2 = 0$. Thus, $b \neq 0$. Multiplying b^{-1} to the equation $2ab - b = 0$. We get $a = 2$. Substitute to $a = 2$ to $a^2 - b^2 - a + 2 = 0$, we get $b \in \{1, 2\}$. Therefore, the solutions of $x^2 - x + 2$ in $\mathbb{Z}_3[i]$ are $2 + i$ and $2 + 2i$. ∎

13.57 Consider the equation $x^2 - 5x + 6 = 0$.

(a) How many solutions does this equation have in $\mathbb{Z}_7$?

(b) Find all solutions of this equation in $\mathbb{Z}_8$.

(c) Find all solutions of this equation in $\mathbb{Z}_{12}$.

(d) Find all solutions of this equation in $\mathbb{Z}_{14}$.

Proof.

(a) Observe that $x^2 - 5x + 6 = (x-2)(x-3)$. Note that $\mathbb{Z}_7$ is a field and an integral domain. That is, if $ab = 0 \in \mathbb{Z}_7$, then $a = 0$ or $b = 0$. Therefore, if $x^2 - 5x + 6 = (x-2)(x-3) = 0$, then $(x-2) = 0$ or $(x-3) = 0$. That is, $x = 2$ or $x = 3$.

補充. 課本解答有誤。

(b) Observe that $x^2 - 5x + 6 = (x-2)(x-3)$. The set of all zero divisor in $\mathbb{Z}_8$ is $\{2, 4, 6\}$. There are three factorizations of 0 with nonzero factor. They are

$$\begin{aligned} 2 \cdot 4, \\ 4 \cdot 4, \\ 4 \cdot 6. \end{aligned}$$

There are no x satisfying $(x-2)(x-3) = 4 \cdot 2$ or $(x-2)(x-3) = 4 \cdot 4$ or $(x-2)(x-3) = 6 \cdot 4$. Therefore, $x^2 - 5x + 6 = (x-2)(x-3) = 0$ has only two solutions $2, 3$ in $\mathbb{Z}_8$.

(c) Observe that $x^2 - 5x + 6 = (x-2)(x-3)$. The set of all zero divisor in $\mathbb{Z}_{12}$ is $\{2, 3, 4, 6, 8, 9, 10\}$. There are nine factorizations of 0 with nonzero factor. They are

$$\begin{aligned} 2 \cdot 6, \\ 3 \cdot 4, \\ 3 \cdot 8, \\ 4 \cdot 6, \\ 4 \cdot 9, \\ 6 \cdot 6, \\ 6 \cdot 8, \\ 6 \cdot 10, \\ 8 \cdot 9. \end{aligned}$$

Note that $x^2 - 5x + 6 = (x-2)(x-3) = ((x-3)+1)(x-3)$. Thus, if $((x-3)+1)(x-3) = 0$ and $((x-3)+1) \neq 0$ and $(x-3) \neq 0$, then

$$((x-3)+1) = 4 \text{ and } (x-3) = 3 \text{ and } x = 6$$

or

$$((x-3)+1) = 9 \text{ and } (x-3) = 8 \text{ and } x = 11.$$

Therefore, $x^2 - 5x + 6 = (x-2)(x-3) = 0$ has four solutions $6, 11, 2, 3$ in $\mathbb{Z}_{12}$.

(d) Observe that $x^2 - 5x + 6 = (x-2)(x-3)$. The set of all zero divisor in $\mathbb{Z}_{14}$ is $\{2, 4, 6, 7, 8, 10, 12\}$. There are nine factorizations of 0 with nonzero factor.

They are

$$\begin{gathered}7\cdot 2,\\ 7\cdot 4,\\ 7\cdot 6,\\ 7\cdot 7,\\ 7\cdot 8,\\ 7\cdot 10,\\ 7\cdot 12.\end{gathered}$$

Note that $x^2 - 5x + 6 = (x-2)(x-3) = ((x-3)+1)(x-3)$. Thus, if $((x-3)+1)(x-3) = 0$ and $((x-3)+1) \neq 0$ and $(x-3) \neq 0$, then

$$((x-3)+1) = 7 \text{ and } (x-3) = 6 \text{ and } x = 9$$

or

$$((x-3)+1) = 8 \text{ and } (x-3) = 7 \text{ and } x = 10.$$

Therefore, $x^2 - 5x + 6 = (x-2)(x-3) = 0$ has four solutions $9, 10, 2, 3$ in $\mathbb{Z}_{14}$.

■

13.59 Suppose that R is an integral domain in which $20\cdot 1 = 0$ and $12 \cdot 1 = 0$. (Recall that $n\cdot 1$ means the sum $1 + 1 + \cdots + 1$ with n terms.) What is the characteristic of R?

Proof. Recall that the characteristic of an integral domain must be a prime. If $20\cdot 1 = 0$ and $12\cdot 1 = 0$, then $\operatorname{char} R \mid 20$ and $\operatorname{char} R \mid 12$. Thus, $\operatorname{char} R = 2$. ■

13.60 In a commutative ring of characteristic 2, prove that the idempotents form a subring.

Proof. Let S be the set of all idempotent in R and $a, b \in S$. $0 \in S$ is obviously.

$$(a+b)^2 = a^2 + ab + ba + b^2 \overset{R \text{ is commutative}}{\overset{\downarrow}{=}} a^2 + 2ab + b^2 \overset{\text{char } R=2}{\overset{\downarrow}{=}} a^2 + b^2 = a + b.$$

Thus, $(a+b)$ is also an idempotent.

$(-a)^2 = a^2 = a \overset{\text{char } R=2}{\overset{\downarrow}{=}} -a$, $(-a)$ is also an idempotent.

$(ab)^2 = abab \overset{R \text{ is commutative}}{\overset{\downarrow}{=}} a^2b^2 = ab$, ab is also an idempotent. ■

13.61 Describe the smallest subfield of the field of real numbers that contains $\sqrt{2}$. (That is, describe the subfield K with the property that K contains $\sqrt{2}$ and if F is any subfield containing $\sqrt{2}$, then F contains K.)

提示. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Proof. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Verify directly. ■

補充. 下面提供一個不一樣的證法, 但要用到一些進階的知識。回憶一下在 Exercise 13.51 時, 我們作了類似的推論。

Let F be a subfield of $\mathbb{R}$. Define a mapping $\theta : \mathbb{Z} \to F$ by $\theta(m) = m \cdot 1$. Show that θ is an one-to-one homomorphism. Since $F \le \mathbb{R}$, we have char $F = 0$. Then $\ker \theta = \{0\}$. By the First Isomorphism Theorem for Ring, we have $\mathbb{Z} \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}/\ker\theta \cong \text{Im}(\theta) \le F$. That is, F contains an integral domain $\mathbb{Z}$ (up to isomorphism).

The field of quotient of $\mathbb{Z}$ is $\mathbb{Q}$ and the field of quotient of $\mathbb{Z}$ is the smallest field which contains $\mathbb{Z}$. Thus, $\mathbb{Q} \le F$.

If $\sqrt{2} \in F$ and F is the smallest subfield of $\mathbb{R}$ which contains $\sqrt{2}$, then $F = \mathbb{Q}(\sqrt{2})$.

13.62 Let F be a finite field with n elements. Prove that $x^{n-1} = 1$ for all nonzero x in F.

Proof. $F - \{0\}$ is a group under multiplication. By Lagrange's Theorem. ■

13.64* Suppose that a and b belong to a field of order 8 and that $a^2 + ab + b^2 = 0$. Prove that $a = 0$ and $b = 0$. Do the same when the field has order 2^n with n odd.

提示.

- Show that $a^3 = b^3$.
- By Exercise 13.35, char $F = ?$
- Show that $3 \nmid 2^n - 1$ for any odd integer n. (Hint: Suppose that $n = 2k+1$ and compute $2^n \equiv ? \pmod 3$.)
- If $a \neq 0$, then consider the multiplicative order of $a^{-1}b$ in the multiplicative group $F - \{0\}$.

Proof. By Exercise 13.35, char $F = 2$. Note that $a^3 - b^3 = (a-b)(a^2 + ab + b^2) = 0$. Hence, $a^3 = b^3$.

If $a \neq 0$, then $(a^{-1}b)^3 = 1$ and the multiplicative order of $a^{-1}b$ in the multiplicative group $F - \{0\}$ is 1 because $3 \nmid |F - \{0\}| = 2^n - 1$ for any odd integer n. Hence, $a^{-1}b = 1$ and $a = b$, Then

$$0 = a^2 + ab + b^2 = 3a^2 \overset{\overset{\text{char } F=2}{\downarrow}}{=} a^2$$

and $a = 0$, a contradiction. Therefore, $a = 0$. ■

13.65 Let F be a field of characteristic 2 with more than two elements. Show that $(x+y)^3 \neq x^3 + y^3$ for some x and y in F.

提示. Observe that

$$\begin{aligned} & (x+y)^3 = x^3 + y^3 \\ \overset{\overset{\text{char } F=2}{\downarrow}}{\Leftrightarrow} \quad & \underline{\hspace{6cm}} \\ \Leftrightarrow \quad & xy(x+y) = 0. \end{aligned}$$

That is, $(x+y)^3 \neq x^3 + y^3 \Leftrightarrow$ ____________. Since $|F| > 2$, let $x, y \in F$ satisfying $x \neq 0, y \neq 0$ and $x \neq y$. Show that $xy(x+y) \neq 0$.

Proof. Observe that

$$\begin{aligned} & (x+y)^3 = x^3 + y^3 \\ \overset{\text{char } F=2}{\overset{\downarrow}{\Leftrightarrow}} \quad & x^3 + xy^2 + x^2y + y^3 = x^3 + y^3 \\ \Leftrightarrow \quad & xy(x+y) = 0. \end{aligned}$$

Since $|F| > 2$, let $x, y \in F$ satisfying $x \neq 0, y \neq 0$ and $x \neq y$. Then $x+y \neq 0$ (if $x+y=0$, then $x = -y \overset{\text{char } F=2}{\overset{\downarrow}{=}} y$) and $xy(x+y) \neq 0$ and $(x+y)^3 \neq x^3 + y^3$. ■

13.66* Suppose that F is a field with characteristic not 2, and that the non-zero elements of F form a cyclic group under multiplication. Prove that F is finite.

Proof. Suppose that $F - \{0\} = \{a, a^2, a^3, \ldots\}$. Since there is a multiplicative identity 1 in $F - \{0\}$, we have $a^m = 1$ for some $m \in \mathbb{N}^+$. Thus, $F = \{0, a, a^2, a^3, \ldots, a^{m-1}\}$ and F is finite. ■

補充. 似乎沒用到 char $F = 2$ 這個條件, 去看一下 `http://math.stackexchange.com/questions/753437/` 及 `http://math.stackexchange.com/questions/856975/`

13.68* Let F be a field of order 32. Show that the only subfields of F are F itself and $\{0, 1\}$.

Proof. $F - \{0\}$ is an abelian group under multiplication. If S is a subfield of F, then $S - \{0\}$ is a subgroup of $F - \{0\}$ under multiplication. By Lagrange's Theorem, $|S - \{0\}|$ divide $|F - \{0\}| = 31$. Thus, $|S - \{0\}| = 1$ or $|S - \{0\}| = 31$. That is, $S = \{0, 1\}$ or $S = F$. ■

14 Chapter 14

題組 14.15, 14.17, 14.27

!!! Theorem 14.3, Theorem 14.4 及 p.274 line 11: In a commutative ring with unity, a maximal ideal is also a prime ideal. 並稱爲基礎環論中的三大定理, 我們之後會不斷地用到他們, 請務必記下來。

14.4 Find a subring of $\mathbb{Z} \oplus \mathbb{Z}$ that is not an ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

Proof. $\{(m, m) \mid m \in \mathbb{Z}\} \leq \mathbb{Z} \oplus \mathbb{Z}$. ■

14.5 Let $S = \{a + bi \mid a, b \in \mathbb{Z}, b \text{ is even}\}$. Show that S is a subring of $\mathbb{Z}[i]$, but not an ideal of $\mathbb{Z}[i]$.

14.6 Fina all maimal ideals in

(a) $\mathbb{Z}_8$.

(b) $\mathbb{Z}_{10}$.

(c) $\mathbb{Z}_{12}$.

(d) $\mathbb{Z}_n$.

Proof. 你可以先找 $(\mathbb{Z}_n, +)$ 的 subgroup, 這以前就找過了, 很簡單, 就是 cyclic group 的 subgroup, 畫出 subgroup lattice diagram。並且確認這些 subgroup 也會是 ideal。由互相包含的關係中, 猜測 maximal ideal, 並利用 ring 的三大定理證明。

(a) $\langle 2\rangle$.

(b) $\langle 2\rangle$, $\langle 5\rangle$.

(c) $\langle 2\rangle$, $\langle 3\rangle$.

(d) Suppose that $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$. Then all the maxiaml ideal of $\mathbb{Z}_n$ are $\langle p_1\rangle$, $\langle p_2\rangle$,..., $\langle p_s\rangle$ because $\mathbb{Z}_n$ is a commutative ring with unity and $\mathbb{Z}_n/\langle p_i\rangle \cong \mathbb{Z}_{p_i}$ is a field. (You can construct a ring homomorphism from $\mathbb{Z}_n$ to $\mathbb{Z}_{p_i}$ and show that whose kernel is $\langle p_i\rangle$. Then by the First Isomorphism Theorem for Ring.)

■

14.8 Prove that the intersection of any set of ideals of a ring is an ideal.

14.10 If A and B are ideals of a ring, show that the sum of A and B, $A + B = \{a + b \mid a \in A, b \in B\}$, is an ideal.

14.11 In the ring of integers, find a positive integer a such that

(a) $\langle a\rangle = \langle 2\rangle + \langle 3\rangle$.

(b) $\langle a\rangle = \langle 6\rangle + \langle 8\rangle$.

(c) $\langle a\rangle = \langle m\rangle + \langle n\rangle$.

Proof. $\langle m\rangle + \langle n\rangle = \langle \gcd(m, n)\rangle$. ■

14.12 If A and B are ideals of a ring, show that the product of A and B, $AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_i \in A, b_i \in B, n$ a positive integer$\}$, is an ideal.

補充. 注意,n 不是固定的, 例如 $a_1b_1 + a_2b_2 \in AB$, $a_3b_3 + a_4b_4 + a_5b_5 \in AB$.

14.13 Find a positive integer a such that

(a) $\langle a\rangle = \langle 3\rangle\langle 4\rangle$.

(b) $\langle a\rangle = \langle 6\rangle\langle 8\rangle$.

(c) $\langle a\rangle = \langle m\rangle\langle n\rangle$.

Proof. $\langle m\rangle\langle n\rangle = \langle mn\rangle$. ■

補充. 注意, 不是 $\langle m\rangle\langle n\rangle = \langle \text{l.c.m.}(m, n)\rangle$, 例如 $\langle 6\rangle\langle 8\rangle = \langle 48\rangle \neq \langle 24\rangle = \langle \text{l.c.m.}(6, 8)\rangle$. 注意, $AB = \{\sum_{i=1}^n a_ib_i \mid n \in \mathbb{N} \cup \{0\}, a_i \in A, b_i \in B\}$, (注意, 其中的 n 並不是固定的。) 不是 $AB = \{ab \mid a \in A, b \in B\}$.

14.14 Let A and B be ideals of a ring. Prove that $AB \subseteq A \cap B$.

Proof. If $ab \in AB$, then $ab \in A$ because $A \lhd R$. ■

14.15 If A is an ideal of a ring R and 1 belongs to A, prove that $A = R$.

補充. 這定理非常重要, 簡單來說, 你以後只要看到 ideal 含有 unity 或是 unit, 你就要意識到這個 ideal 一定就是整個 ring。我們可以很直覺地用 multiplication table 來解釋這個定理。

Consider the multiplication table of R.

	r_1	r_2	r_3	$\cdots$
r	rr_1	rr_2	rr_3	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	r_1	r_2	r_3	$\cdots$

If I is an ideal in R and $r \in I$, then $rr_1, rr_2, rr_3, \ldots$ all are contained in I. Thus, if $1 \in I$, then $r_1, r_2, r_3, \ldots$, all the elements in R are contained in I and $I = R$.

14.16 If A and B are ideals of a commutative ring R with unity and $A + B = R$, show that $A \cap B = AB$.

提示. ($\subseteq$) Since $1 \in R = A + B$, let $1 = a_0 + b_0$, where $a_0 \in A, b_0 \in B$. If $x \in A \cap B$, then

$$x = x \cdot 1 = x(a_0 + b_0) = xa_0 + xb_0 = a_0x + xb_0 \in AB.$$

14.17 If an ideal I of a ring R contains a unit, show that $I = R$.

14.18 Suppose that in the ring $\mathbb{Z}$, the ideal $\langle 35 \rangle$ is a proper ideal of J and J is a proper ideal of I. What are the possibilities for J? What are the possibilities for I?

Proof. $J = \langle 5 \rangle$ or $J = \langle 7 \rangle$. $I = \mathbb{Z}$. ■

14.20 Suppose that R is a commutative ring and $|R| = 30$. If I is an ideal of R and $|I| = 10$, prove that I is a maximal ideal.

Proof. If $I \leq A \lhd R$, then $(I, +) \leq (A, +) \leq (R, +)$ as additive group. By Lagrange's Theorem, $|I| = 10$ divide $|A|$ and $|A|$ divide $|R| = 30$. Hence, $|A| = 10$ or $|A| = 30$. That is, $A = I$ or $A = R$ and I is a maximal ideal.

注意, 不能用三大定理, 因爲不確定 R 有沒有 unity。 ■

14.22 Let $I = \langle 2 \rangle$. Prove that $I[x]$ is not a maximal ideal of $\mathbb{Z}[x]$ even though I is a maximal ideal of $\mathbb{Z}$.

提示. 三大定理。

Proof. Note that $\mathbb{Z}[x]$ is a commutative ring with unity. Since $\mathbb{Z}[x]/I[x] \cong \mathbb{Z}_2[x]$ is not a field, we have $I[x]$ is not a maximal ideal in $\mathbb{Z}[x]$.

Why $\mathbb{Z}[x]/I[x] \cong \mathbb{Z}_2[x]$**?** Consider $(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0) + I[x] \in \mathbb{Z}[x]/I[x]$, where $a_i \in \mathbb{Z}$.

$$\begin{aligned} & (a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0) + I[x] \\ = & \Big((2b_n + r_n)x^n + (2b_{n-1} + r_{n-1})x^{n-1} + \cdots(2b_1 + r_1)x + (2b_0 + r_0)\Big) + I[x], \text{ where } r_i \in \{0,1\} \\ = & \Big((2b_nx^n + 2b_{n-1}x^{n-1} + \cdots 2b_1x + 2b_0) + I[x]\Big) + \Big((r_nx^n + r_{n-1}x^{n-1}\cdots + r_1x + r_0) + I[x]\Big) \\ = & \Big(0 + I[x]\Big) + \Big((r_nx^n + r_{n-1}x^{n-1}\cdots + r_1x + r_0) + I[x]\Big) \leftarrow (2b_nx^n + \cdots + 2b_0) \in I[x] \\ = & (r_nx^n + r_{n-1}x^{n-1}\cdots + r_1x + r_0) + I[x] \end{aligned}$$

■

14.24 Give an example of a commutative ring that has a maximal ideal that is not a prime ideal.

提示. 三大定理。

Proof. $4\mathbb{Z} \lhd 2\mathbb{Z}$. ■

補充. 注意到三大定理中的“a maximal ideal must be a prime ideal”必須在一個 commutative ring with unity 當中才會成立, 所以在 $2\mathbb{Z}$ 中, 因爲沒有unity, 所以 maximal ideal 不一定是一個 prime ideal。

14.26 If R is a commutative ring with unity and A is a proper ideal of R, show that R/A is a commutative ring with unity.

14.27 Prove that the only ideals of a field F are $\{0\}$ and F itself.

補充. 注意到, 這個定理跟 Theorem 15.2跟 Theorem 15.1.7三者透露了一件很重要的事情, 就是 domain 爲 field 的 ring homomorphism 一定是 one-to-one 的。

14.28 Show that $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field.

提示. See Theorem 17.1, Theorem 17.5, 三大定理。

Proof. x^2+1 has no root in $\mathbb{R}$ and $\deg x^2+1 = 2$. x^2+1 is irreducible over $\mathbb{R}$. By Theorem 17.5, $\langle x^2+1\rangle$ is a maximal ideal in $\mathbb{R}[x]$. By Theorem 14.4, $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field. ■

14.29 In $\mathbb{Z}[x]$, the ring of polynomials with integer coefficiens, let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$. Prove that $I = \langle x\rangle$.

Proof. ($\subseteq$) If $f(x) = a_nx^n + \cdots + a_1x + a_0 \in I$, then $0 = f(0) = a_0$ and $f(x) = a_nx^n + \cdots + a_1x = x(a_nx^{n-1} + \cdots + a_1) \in \langle x\rangle = \{xg(x) \mid g(x) \in \mathbb{Z}[x]\}$.

($\supseteq$) If $f(x) = xg(x) \in \langle x\rangle$, then $f(0) = 0 \cdot g(0) = 0$ and $f(x) \in I$. ■

補充. 較囉嗦的解法。

$x \in I$ is obviously. Thus, $\langle x\rangle \subseteq I$. ($\langle x\rangle$ is the smallest ideal which contains x.) On the other hand, suppose that $f(x) = a_nx^n + \cdots + a_1x \in I$. Then $f(x) = x(a_nx^{n-1} + \cdots + a_1) \in \langle x\rangle$. Therefore, $I \subseteq \langle x\rangle$ and $I = \langle x\rangle$.

14.30 Show that $A = \{(3x, y) \mid x, y \in \mathbb{Z}\}$ is a maximal ideal of $\mathbb{Z} \oplus \mathbb{Z}$. Generalize. What happens if $3x$ is replaced by $4x$? Generalize.

Proof. 由三大定理。

Note that $A \cong 3\mathbb{Z} \oplus \mathbb{Z}$. Since $\mathbb{Z} \oplus \mathbb{Z}$ is a commutative ring with unity and $(\mathbb{Z} \oplus \mathbb{Z})/A = (\mathbb{Z} \oplus \mathbb{Z})/(3\mathbb{Z} \oplus \mathbb{Z}) \cong \mathbb{Z}_3$ is a field, we get that A is a maximal ideal in $\mathbb{Z} \oplus \mathbb{Z}$.

$p\mathbb{Z} \oplus \mathbb{Z}$ is a maximal ideal in $\mathbb{Z} \oplus \mathbb{Z}$ for any prime p.

$(\mathbb{Z} \oplus \mathbb{Z})/(4\mathbb{Z} \oplus \mathbb{Z}) \cong \mathbb{Z}_4$ is not an integral domain. $4\mathbb{Z} \oplus \mathbb{Z}$ is not a maximal ideal in $\mathbb{Z} \oplus \mathbb{Z}$. ■

14.31 Let R be the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Show that $A = \{f \in R \mid f(0) = 0\}$ is a maximal ideal of R.

提示. 三大定理。

.274, exa.17, 14.34 In $\mathbb{Z}[x]$, the ring of polynomials with integer coefficiens, let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$. Prove that I is a prime ideal in $\mathbb{Z}[x]$ but not a maximal ideal in $\mathbb{Z}[x]$.

提示. 三大定理。

Proof. By Exercise 14.29, $I = \langle x \rangle$.

Note that

$$
\begin{aligned}
& \mathbb{Z}[x]/I \\
= \quad & \mathbb{Z}[x]/\langle x \rangle \\
= \quad & \{f(x) + \langle x \rangle \mid f(x) \in \mathbb{Z}[x]\} \\
= \quad & \{(f_n x^n + \cdots + f_1 x + f_0) + \langle x \rangle \mid f_i \in \mathbb{Z}\} \\
= \quad & \{\Big(x(f_n x^{n-1} + \cdots + f_1) + f_0\Big) + \langle x \rangle \mid f_i \in \mathbb{Z}\} \\
= \quad & \Big\{\Big(x(f_n x^{n-1} + \cdots + f_1) + \langle x \rangle\Big) + \Big(f_0 + \langle x \rangle\Big) \mid f_i \in \mathbb{Z}\Big\} \\
= \quad & \Big\{\Big(x + \langle x \rangle\Big) \cdot \Big(f_n x^{n-1} + \cdots + f_1 + \langle x \rangle\Big) + \Big(f_0 + \langle x \rangle\Big) \mid f_i \in \mathbb{Z}\Big\} \\
\overset{x \in \langle x \rangle,\ x + \langle x \rangle = 0 + \langle x \rangle}{\overset{\downarrow}{=}} \quad & \Big\{\Big(0 + \langle x \rangle\Big) \cdot \Big(f_n x^{n-1} + \cdots + f_1 + \langle x \rangle\Big) + \Big(f_0 + \langle x \rangle\Big) \mid f_i \in \mathbb{Z}\Big\} \\
= \quad & \{f_0 + \langle x \rangle \mid f_0 \in \mathbb{Z}\} \\
\cong \quad & \mathbb{Z}.
\end{aligned}
$$

Since $\mathbb{Z}[x]$ is a commutative ring with unity, by p.273, thm.14.3 and $\mathbb{Z}[x]/I \cong \mathbb{Z}$ is an integral domain, I is a prime ideal. By p.273, thm.14.4 and $\mathbb{Z}[x]/I \cong \mathbb{Z}$ is not a field, I is not a maximal ideal of $\mathbb{Z}[x]$.

There is another way to prove that I is not a maximal ideal by the definition. We show that $I \subseteq \langle x, 2 \rangle \subseteq \mathbb{Z}[x]$ and $I \neq \langle x, 2 \rangle$ and $\langle x, 2 \rangle \neq \mathbb{Z}[x]$. $I \subseteq \langle x, 2 \rangle = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ is obviously. Since $2 \notin I$, we have $I \neq \langle x, 2 \rangle$. Since $1 \notin \langle x, 2 \rangle$, we have $\langle x, 2 \rangle \neq \mathbb{Z}[x]$. ■

14.35 In $\mathbb{Z} \oplus \mathbb{Z}$, let $I = \{(a, 0) \mid a \in \mathbb{Z}\}$. Show that I is a prime ideal but not a maximal ideal.

提示. 三大定理。p.273, Theorem 14.3, 14.4 and that in a commutative ring with unity, a maximal ideal must be a prime ideal. (p.274)

14.36 Let R be a ring and let I be an ideal of R. Prove that the factor ring R/I is commutative if and only if $rs - sr \in I$ for all r and s in R.

提示. For all $r, s \in R$,

$$\begin{aligned} & (r+I)(s+I) = (s+I)(r+I) \\ \Leftrightarrow\ & rs + I = sr + I \\ \Leftrightarrow\ & (rs - sr) + I = I \\ \Leftrightarrow\ & rs - sr \in I \end{aligned}$$

14.37 In $\mathbb{Z}[x]$, let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is an even integer}\}$. Prove that $I = \langle x, 2\rangle$. Is I a prime ideal of $\mathbb{Z}[x]$? Is I a maximal ideal? How many elements does $\mathbb{Z}[x]/I$ have?

提示. 三大定理。

Proof. $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$. ■

14.39 In $\mathbb{Z}_5[x]$, let $I = \langle x^2+x+2\rangle$. Find the multiplicative inverse of $(2x+3)+I$ in $\mathbb{Z}_5[x]/I$.

提示. Method 1 (Euclidean Algorithm 輾轉相除法): We want to find that $s(x), t(x) \in \mathbb{Z}_5[x]$ such that

$$(2x+3)\cdot s(x) + (x^2+x+2)\cdot t(x) = 1.$$

Then $s(x)$ is the multiplicative inverse of $(2x+3)$ in $\mathbb{Z}_5[x]/I$. Applies the division algorithm on x^2+x+2 and $2x+3$.

$$\begin{array}{rlll} & 3x & +1 & \\ \cline{2-4} 2x+3 \;\big) & x^2 & +x & +2 \\ & x^2 & +4x & \\ \cline{2-3} & & 2x & +2 \\ & & 2x & +3 \\ \cline{3-4} & & & -1 \end{array}$$

$$\underline{(x^2+x+2)}_{f(x)} = \underline{(2x+3)}_{g(x)} \cdot \underline{(3x+1)}_{q(x)} + \underline{-1}_{r(x)}$$

Then

$$-1 = (x^2+x+2) - (2x+3)\cdot(3x+1).$$

Multiplying (-1) on both sides, we get

$$1 = -(x^2+x+2) + (2x+3)\cdot(3x+1).$$

Therefore, $(3x+1)$ is the multiplicative inverse of $(2x+3)$ in $\mathbb{Z}_5[x]/I$.

這個方法我們在之前就有看過了, 參考 Exercise 0.4: Find integers s and t such that $1 = 7\cdot s + 11\cdot t$. Show that s and t are not unique.

當時我演示了一題更複雜的題目。Find integers s and t such that $1 = 69 \cdot s + 31 \cdot t$.

$$\begin{aligned} 69 &= 31 \cdot 2 + 7, & (16)\\ 31 &= 7 \cdot 4 + 3, & (17)\\ 7 &= 3 \cdot 2 + 1. & (18) \end{aligned}$$

$$\begin{aligned} \text{by (18)},\ 1 &= 7 - 3 \cdot 2 \\ &\overset{\substack{(17)\\ \downarrow}}{=} 7 - (31 - 7 \cdot 4) \cdot 2 \\ &= 7 - 31 \cdot 2 + 7 \cdot 8 \\ &= 7 \cdot 9 - 31 \cdot 2 \\ &\overset{\substack{(16)\\ \downarrow}}{=} (69 - 31 \cdot 2) \cdot 9 - 31 \cdot 2 \\ &= 69 \cdot 9 - 31 \cdot 18 - 31 \cdot 2 \\ &= 69 \cdot 9 - 31 \cdot 20 \\ &\Rightarrow s = 9, \quad t = -20. \end{aligned}$$

Method 2 ($F - \{0\}$ is a multiplicative group): Let $F = \mathbb{Z}_5[x]/I$. Note that F is a finite field[3] and $F - \{0\}$ is a multiplicative group with order $5^2 - 1 = 24$. By Lagrange's Theorem, the multiplicative order of $(2x + 3)$ is a divisor of 24.

Note that $x^2 + x + 2 = 0$ in $\mathbb{Z}_5[x]/I$. Hence $x^2 = -x - 2 = 4x + 3$ in $\mathbb{Z}_5[x]/I$. Then compute that

$$\begin{aligned} (2x+3)^2 &= 4x^2 + 12x + 9 = 4(4x+3) + 12x + 9 = 28x + 21 = 3x + 1 \neq 1 \\ (2x+3)^3 &= (2x+3) \cdot (2x+3)^2 = (2x+3)(3x+1) = 35x + 21 = 1. \end{aligned}$$

Therefore, $(2x+3)^2 = 3x + 1$ is the multiplicative inverse of $(2x+3)$ in $\mathbb{Z}_5[x]/I$.

Method 3 (Undetermined Coefficients Method): Suppse that

$$(2x+3)(ax+b) = (x^2 + x + 2)q(x) + 1 \in \mathbb{Z}_5[x]/I.$$

Then $(ax + b)$ is the multiplicative inver of $(2x+3)$ in $\mathbb{Z}_5[x]/I$.

$$\begin{array}{r|lll} & 3x & +1 & \\ \cline{2-4} 2x+3 & x^2 & +x & +2 \\ & x^2 & +4x & \\ \cline{2-3} & & 2x & +2 \\ & & 2x & +3 \\ \cline{3-4} & & & -1 \end{array}$$

Therefore, $(x^2+x+2) = (2x+3) \cdot (3x+1) + (-1)$ and $(2x+3)(3x+1) = (x^2+x+2) + 1$.

14.41 An integral domain D is called a principal ideal domain if every ideal of D has the form $\langle a \rangle = \{ad \mid d \in D\}$ for some a in D. Show that $\mathbb{Z}$ is a principal ideal domain.

[3] $\deg(x^2 + x + 2) \in \{2, 3\}$ and $x^2 + x + 2$ has no root in $\mathbb{Z}_5$, by p.312, thm.17.1, $x^2 + x + 2$ is irreducible over $\mathbb{Z}_5$. By p.317, thm.17.5, $I = \langle x^2 + x + 2 \rangle$ is a maximal ideal in $\mathbb{Z}_5[x]$. Since $\mathbb{Z}_5[x]$ is a commutative ring with unity, by p.274, thm.14.4, $\mathbb{Z}_5[x]/I$ is a field.

提示. See Exercise 12.13. If $I \triangleleft \mathbb{Z}$, then $I = m\mathbb{Z} = \langle m \rangle$ for some $m \in \mathbb{Z}$.

14.45 Let R be a commutative ring and let A be any subset of R. Show that the annihilator of A, $\mathrm{Ann}(A) = \{r \in R \mid ra = 0 \text{ for all } a \text{ in } A\}$, is an ideal.

14.46 Let R be a commutative ring and let A be any ideal of R. Show that the nil radical of A, $N(A) = \{r \in R \mid r^n \in A \text{ for some positive integer } n \ (n \text{ depends on } r)\}$, is an ideal of R. [$N(\langle 0 \rangle)$ is called the nil radical of R.]

14.49 Let R be a commutative ring. Show that $R/N(\langle 0 \rangle)$ has no nonzero nilpotent elements.

補充. 注意到, R 原本可能有 nonzero nilpotent element, 但是我們把 nilpotent element 蒐集起來, 構成一個 ideal $N(\langle 0 \rangle)$, 並且將 R quotient 掉這個由 nilpotent element 構成的 ideal, 得到的新的 quotient ring $R/N(\langle 0 \rangle)$ 就沒有 nonzero nilpotent element 了, 所以, 感覺上來說, “quotient”這個動作, 具有把具有某些性質的元素 消滅的功能。

其實我們在group theory 裡面也遇過類似的想法了, 例如 commutator subgroup G', 我們在 G 裡面蒐集形如 $a^{-1}b^{-1}ab$ 的元素及由其生成的元素, 當我們 quotient 掉 G' 的時候, 感覺上就是消滅形如 $a^{-1}b^{-1}ab$ 的元素, 事實上, 這裡的“消滅”是指將其視爲 identity, 也就是 $a^{-1}b^{-1}ab = 1$。(嚴謹來說, 應該是 $(a^{-1}b^{-1}ab)G' = G'$。) 如此一來, 就有 $ab = ba$, 這就是爲什麼 G/G' is abelian 的原因。

14.50 Let A be an ideal of a commutative ring. Prove that $N(N(A)) = N(A)$.

14.51 Let $\mathbb{Z}_2[x]$ be the ring of all polynomials with coefficients in $\mathbb{Z}_2$ (that is, coefficients are 0 or 1, and addition and multiplication of coefficients are done modulo 2). Show that $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ is a field.

提示. See Theorem 17.1, Theorem 17.5, 三大定理。

14.52 List the elements of the field given in Exercise 51, and make an addition and multiplication table for the field.

14.53 Show that $\mathbb{Z}_3[x]/\langle x^2 + x + 1 \rangle$ is not a field.

提示. See Theorem 17.1, Theorem 17.5, 三大定理。

Proof. $x^2 + x + 1$ has a root 1 in $\mathbb{Z}_3$. ■

14.54 Let R be a commutative ring without unity, and let $a \in R$. Describe the smallest ideal I of R that contains a (that is, if J is any ideal that contains a, then $I \subseteq J$).

提示. $\langle a \rangle = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$.

14.60 Let R be a commutative ring with unity, and let I be a proper ideal with the property that every element of R that is not in I is a unit of R. Prove that I is the unique maximal ideal of R.

提示. Let $I \leq J \triangleleft R$ and $J \neq I$. Then there exists $j \in J$ such that $j \notin I$. By the hypothesis, j must be a ...

Proof. Let $I \leq J \lhd R$ and $J \neq I$. Then there exists $j \in J$ such that $j \notin I$. By the hypothesis, j must be a unit. Then $J = R$. Thus, I is a maximal ideal in R.

If I' is another maximal ideal has the same property. That is, if $u \notin I'$, then u is a unit. If $I \neq I'$, then there exists $i' \in I'$ and $i' \notin I$. By the hypothesis, i' is a unit and $I' = R$, contrary to the maximality of I'. (A maximal ideal is proper.) ■

14.63 Let R be a commutative ring with unity and let $a, b \in R$. Show that $\langle a, b\rangle$, the smallest ideal of R containing a and b, is $I = \{ra + sb \mid r, s \in R\}$. That is, show that I contains a and b and that any ideal that contains a and b also contains I.

p.268, exa.6 In $\mathbb{Z}[x]$, the ring of polynomials with integer coefficiens, let $I = \{f(x) \in \mathbb{Z}[x] \mid f(x)$ has even constant term$\}$. Prove that $I = \langle x, 2\rangle$.

Proof. ($\subseteq$) If $f(x) = a_nx^n + \cdots + a_1x + a_0 \in I$, then $f(0) = a_0 = 2k$ is an even integer and $f(x) = a_nx^n + \cdots + a_1x + 2k = x(a_nx^{n-1} + \cdots + a_1) + 2k \in \langle x, 2\rangle = \{xg(x) + 2h(x) \mid g(x), h(x) \in \mathbb{Z}[x]\}$.

($\supseteq$) If $f(x) = xg(x) + 2h(x) \in \langle x, 2\rangle$, then $f(0) = 0 \cdot g(0) + 2h(0) = 2h(0)$ is an even integer and $f(x) \in I$. ■

補充. 較囉嗦的解法。

Since $\mathbb{Z}[x]$ is a commutative ring with unity, we have $\langle x, 2\rangle = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ (c.f. p.268, exa.5).

If $h(x) = xf(x) + 2g(x) \in \langle x, 2\rangle$, suppose that $f(x) = f_nx^n + \cdots + f_1x + f_0$ and $g(x) = g_mx^m + \cdots + g_1x + g_0$, then $h(x) = x(f_nx^n + \cdots + f_1x + f_0) + 2(g_mx^m + \cdots + g_1x) + 2g_0 \in I$. Hence, $\langle x, 2\rangle \subseteq I$.

If $h(x) = h_sx^s + \cdots + h_1x + 2h_0 \in I$, then $h(x) = x(h_sx^{s-1} + \cdots + h_1) + 2(h_0) \in \langle x, 2\rangle$ and $I \subseteq \langle x, 2\rangle$.

補充 14.A Find the multiplicative inverse of $(2x + 1)$ in $\mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle$.

提示. Method 1 (Euclidean Algorithm 輾轉相除法): We want to find that $s(x), t(x) \in \mathbb{Z}_3[x]$ such that

$$(2x + 1) \cdot s(x) + (x^2 + 2x + 2) \cdot t(x) = 1.$$

Then $s(x)$ is the multiplicative inverse of $(2x + 1)$ in $\mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle$. Applies the division algorithm on $x^2 + 2x + 2$ and $2x + 1$.

$$\begin{array}{r|lll} & 2x & & \\ \cline{2-4} 2x+1 & x^2 & +2x & +2 \\ & x^2 & +2x & \\ \cline{2-4} & & & +2 \end{array}$$

$$\underline{(x^2 + 2x + 2)}_{f(x)} = \underline{(2x + 1)}_{g(x)} \cdot \underline{(2x)}_{q(x)} + \underline{2}_{r(x)}$$

Then

$$2 = (x^2 + 2x + 2) - (2x + 1) \cdot (2x).$$

Multiplying 2 on both sides, we get

$$1 = 2(x^2 + x + 2) - 2(2x + 1) \cdot (2x).$$

Therefore, $(-2)(2x) = 2x$ is the multiplicative inverse of $(2x+1)$ in $\mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$.

Method 2 ($F-\{0\}$ is a multiplicative group): Let $F = \mathbb{Z}_3[x]/\langle x^2+2x+2\rangle$. Note that F is a finite field and $F - \{0\}$ is a multiplicative group with order $3^2 - 1 = 8$. By Lagrange's Theorem, the multiplicative order of $(2x + 1)$ is a divisor of 8.

Note that $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle$. Hence

$$\begin{array}{rcl} x^2 & = & -2x - 2 = x + 1, \\ x^3 & = & x \cdot x^2 = x(x + 1) = x^2 + x = 2x + 1, \\ x^4 & = & (x^2)^2 = (x + 1)^2 = x^2 + 2x + 1 = 2. \end{array}$$

Then compute that

$$\begin{array}{rcl} (2x + 1)^2 & = & 4x^2 + 4x + 1 = x^2 + x + 1 = 2x + 2 \neq 1 \\ (2x + 1)^4 & = & (2x + 2)^2 = 4x^2 + 8x + 4 = x^2 + 2x + 1 = 2 \neq 1. \end{array}$$

Therefore, $(2x + 1)^8 = 1$ and $(2x + 1)^7 = (2x + 1)^4 \cdot (2x + 1)^2 \cdot (2x + 1) = 2x$ is the multiplicative inverse of $(2x + 1)$ in $\mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle$.

補充 14.B Find the multiplicative inverse of $(x^2 + x + 1)$ in $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$.

提示. **Method 1 (Euclidean Algorithm 輾轉相除法):** We want to find that $s(x), t(x) \in \mathbb{Z}_2[x]$ such that

$$(x^2 + x + 1) \cdot s(x) + (x^3 + x + 1) \cdot t(x) = 1.$$

Then $s(x)$ is the multiplicative inverse of $(x^2 + x + 1)$ in $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$. Applies the division algorithm on $x^3 + x + 1$ and $x^2 + x + 1$.

$$\begin{array}{r|rrrr} & x & +1 & & \\ \cline{2-5} x^2+x+1 & x^3 & & +x & +1 \\ & x^3 & +x^2 & +x & \\ \cline{2-4} & & x^2 & & +1 \\ & & x^2 & +x & +1 \\ \cline{3-5} & & & +x & \end{array}$$

$$\underline{(x^3 + x + 1)}_{f(x)} = \underline{(x^2 + x + 1)}_{g(x)} \cdot \underline{(x + 1)}_{q_1(x)} + \underline{\ x\ }_{r_1(x)} \tag{19}$$

Again, applies the division algorithm on $g(x)$ and $r_1(x)$.

$$\begin{array}{r|rrr} & x & +1 & \\ \cline{2-4} x & x^2 & +x & +1 \\ & x^2 & & \\ \cline{2-4} & & x & \\ & & x & \\ \cline{3-4} & & & +1 \end{array}$$

$$\underline{(x^2+x+1)}_{g(x)} = \underline{(x)}_{r_1(x)} \cdot \underline{(x+1)}_{q_2(x)} + \underline{1}_{r_2(x)}$$

Therefore,

$$\begin{aligned}
\underline{1}_{r_2(x)} &= \underline{(x^2+x+1)}_{g(x)} - \underline{(x)}_{r_1(x)} \cdot \underline{(x+1)}_{q_2(x)} \\
&= g - r_1 q_2 \\
&\overset{\overset{(19)}{\downarrow}}{=} g - (f - gq_1)q_2 \\
&= g - fq_2 + gq_1q_2 \\
&= g(1 + q_1q_2) - fq_2
\end{aligned}$$

Therefore, $1+q_1q_2 = 1+(x+1)(x+1) = x^2$ is the multiplicative inverse of (x^2+x+1) in $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$.

Method 2 ($F-\{0\}$ is a multiplicative group): Let $F = \mathbb{Z}_2[x]/\langle x^3+x+1\rangle$. Note that F is a finite field and $F-\{0\}$ is a multiplicative group with order $2^3-1=7$. By Lagrange's Theorem, the multiplicative order of (x^2+x+1) is a divisor of 7. It follows that $(x^2+x+1)^7 = 1$ and $(x^2+x+1)^6$ is the multiplicative inverse of (x^2+x+1) in $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$.

Note that $x^3+x+1=0$ in $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$. Hence

$$\begin{aligned}
x^3 &= -x-1 = x+1, \\
x^4 &= x\cdot x^3 = x(x+1) = x^2+x.
\end{aligned}$$

Then compute that

$$\begin{aligned}
(x^2+x+1)^2 &= x^4+x^2+1 = x+1 \\
(x^2+x+1)^4 &= (x+1)^2 = x^2+1 \\
(x^2+x+1)^6 &= (x^2+x+1)^2\cdot(x^2+x+1)^4 = (x+1)(x^2+1) = x^3+x^2+x+1 = x^2.
\end{aligned}$$

Method 3 (Undetermined Coefficients Method): Suppse that

$$(x^2+x+1)(ax^2+bx+1) = (x^3+x+1)(dx+e)+1 \in \mathbb{Z}_2[x]/\langle x^3+x+1\rangle.$$

Note that ax^2+bx+c is the general form of the element in $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$. Then (ax^2+bx+c) is the multiplicative inver of (x^2+x+1) in $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$. Expand the equation and get the coefficients a, b and c.

補充 14.C Find the multiplicative inverse of $(2x^2+x+3)$ in $\mathbb{Z}_5[x]/\langle x^3+3x+2\rangle$.

提示. We want to find that $s(x), t(x) \in \mathbb{Z}_5[x]$ such that

$$(2x^2+x+3)\cdot s(x) + (x^3+3x+2)\cdot t(x) = 1.$$

Then $s(x)$ is the multiplicative inverse of $(2x^2+x+3)$ in $\mathbb{Z}_5[x]/\langle x^3+3x+2\rangle$.

$$\begin{array}{rcllll}
 & & 3x & +1 & & \\ \cline{3-6}
2x^2+x+3 & \Big) & x^3 & & +3x & +2 \\
 & & x^3 & +3x^2 & +4x & \\ \cline{3-5}
 & & & 2x^2 & +4x & +2 \\
 & & & 2x^2 & +x & +3 \\ \cline{4-6}
 & & & & 3x & +4
\end{array}$$

$$\underline{(x^3+3x+2)}_{f(x)} = \underline{(2x^2+x+3)}_{g(x)} \cdot \underline{(3x+1)}_{q_1(x)} + \underline{(3x+4)}_{r_1(x)} \tag{20}$$

Again, applies the division algorithm on $g(x)$ and $r_1(x)$.

$$\begin{array}{r|lll} & \multicolumn{3}{l}{4x} \\ \cline{2-4} 3x+4 & 2x^2 & +x & +3 \\ & 2x^2 & +x & \\ \cline{2-4} & & & +3 \end{array}$$

$$\underline{(2x^2+x+3)}_{g(x)} = \underline{(3x+4)}_{r_1(x)} \cdot \underline{(4x)}_{q_2(x)} + \underline{3}_{r_2(x)}$$

Therefore,

$$\begin{aligned} \underline{3}_{r_2(x)} &= \underline{(2x^2+x+3)}_{g(x)} - \underline{(3x+4)}_{r_1(x)} \cdot \underline{(4x)}_{q_2(x)} \\ &= g - r_1 q_2 \\ &\overset{\overset{(20)}{\downarrow}}{=} g - (f - gq_1)q_2 \\ &= g - fq_2 + gq_1q_2 \\ &= g(1+q_1q_2) - fq_2 \end{aligned}$$

Multiplying 2 on both sides, we get

$$1 = g(2+2q_1q_2) - 2fq_2.$$

Therefore, $2+2q_1q_2 = 2+2(3x+1)(4x) = 4x^2+3x+2$ is the multiplicative inverse of $(2x^2+x+3)$ in $\mathbb{Z}_5[x]/\langle x^3+3x+2\rangle$.

15 Chapter 15

題組 15.13, 15.12, 15.14, 15.44

題組 15.11, 15.19, 15.47

題組 15.22, 15.23, 15.42, 15.52, 15.53, 15.51

題組 15.57, 15.58, 15.59, 15.61

15.11 Prove that the intersection of any collection of subfields of a field F is a subfield of F.

15.12 Let $\mathbb{Z}_3[i] = \{a+bi \mid a,b \in \mathbb{Z}_3\}$. Show that the field $\mathbb{Z}_3[i]$ is ring-isomorphic to the field $\mathbb{Z}_3[x]/\langle x^2+1\rangle$.

Proof. Define a mapping ϕ from $\mathbb{Z}_3[x]$ to $\mathbb{Z}_3[i]$ by

$$\phi(f(x)) = f(i).$$

It is easy to verify that ϕ is a ring homomorphism. For any $a+bi \in \mathbb{Z}_3[i]$, there exists $f(x) = a+bx \in \mathbb{Z}_3[x]$ such that $\phi(f(x)) = a+bi$. Thus, ϕ is onto.

Since $F[x]$ is a P.I.D. and the kernel of ϕ is an ideal of $F[x]$, $\ker\phi = \langle g(x)\rangle$ for some $g(x) \in F[x]$. Note that $x^2+1 \in \ker\phi = \langle g(x)\rangle$. We assume that $x^2+1 = g(x)h(x)$ for some $h(x) \in F[x]$. Since x^2+1 is irreducible over $\mathbb{Z}_3$, we have $g(x)$ or $h(x)$ is a unit. If $g(x)$ is a unit, then $\ker\phi = \langle g(x)\rangle = F[x]$, a contradiction. ($\phi(1) = 1 \neq 0$) If $h(x)$ is a unit, then $g(x) = (x^2+1)h(x)^{-1}$ and $\langle g(x)\rangle = \langle x^2+1\rangle$. Thus, $\ker\phi = \langle x^2+1\rangle$.

By the First Isomorphism Theorem for Ring,

$$\mathbb{Z}_3[x]/\langle x^2+1\rangle = \mathbb{Z}_3[x]/\ker\phi \cong \mathrm{Im}\phi = \mathbb{Z}_3[i].$$

■

提示. Define a mapping ϕ from $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ to $\mathbb{Z}_3[i]$ by

$$\phi\Big((bx+a)+\langle x^2+1\rangle\Big) = a+bi, \text{ where } a,b \in \mathbb{Z}_3.$$

We show that ϕ is a ring isomorphism.

Homomorphism:

$$\begin{aligned}
&\phi\Big(\underline{(bx+a)+\langle x^2+1\rangle}+\underline{(dx+c)+\langle x^2+1\rangle}\Big)\\
=\ &\phi\Big([(b+d)x+(a+c)]+\langle x^2+1\rangle\Big)\\
=\ &(a+c)+(b+d)i = (a+bi)+(c+d)i\\
=\ &\phi\Big((bx+a)+\langle x^2+1\rangle\Big)+\phi\Big((dx+c)+\langle x^2+1\rangle\Big).
\end{aligned}$$

$$\begin{aligned}
&\phi\Big(\underline{(bx+a)+\langle x^2+1\rangle}\cdot\underline{(dx+c)+\langle x^2+1\rangle}\Big)\\
=\ &\phi\Big(bdx^2+(ad+bc)x+ac+\langle x^2+1\rangle\Big)\\
\overset{\overset{x^2+\langle x^2+1\rangle=-1+\langle x^2+1\rangle}{\downarrow}}{=}\ &\phi\Big((ad+bc)x+(ac-bd)+\langle x^2+1\rangle\Big)\\
=\ &(ac-bd)+(ad+bc)i\\
=\ &(a+bi)\cdot(c+di)\\
=\ &\phi\Big(bx+a+\langle x^2+1\rangle\Big)\cdot\phi\Big(dx+c+\langle x^2+1\rangle\Big).
\end{aligned}$$

One-to-One and Onto: It is easy to verify. You can prove that ϕ is onto. Then since $|\mathbb{Z}_3[x]/\langle x^2+1\rangle| = 9 = |\mathbb{Z}_3[i]|$, we have that ϕ is one-to-one.

15.13 Let

$$S = \left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \,\middle|\, a,b \in \mathbb{R}\right\}.$$

Show that $\phi : \mathbb{C} \to S$ given by

$$\phi(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

is a ring isomorphism.

15.14 Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

Show that $\mathbb{Z}[\sqrt{2}]$ and H are isomorphic as rings.

15.19 Describe the kernel of the homomorphism given in Example 3.

15.22 Determine all ring isomorphisms from $\mathbb{Z}_n$ to itself.

提示. If θ is a ring automorphism on $\mathbb{Z}_n$, then $\theta(1) = \ldots$

Proof. If θ is a ring automorphism on $\mathbb{Z}_n$, then $\theta(1) = 1$. Thus, there is only one ring automorphism on $\mathbb{Z}_n$. Which is the identity mapping. ■

15.23 Determine all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

提示. $\theta(1) = \theta(1 \cdot 1) = \theta(1) \cdot \theta(1) = \theta(1)^2$. So $\theta(1) \in \{0, 1\}$.

15.23 Determine all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

提示. $\theta(1) = \theta(1 \cdot 1) = \theta(1) \cdot \theta(1) = \theta(1)^2$. $\theta(1) \in \{0, 1\}$.

15.25* Determine all ring homomorphisms from $\mathbb{Z} \oplus \mathbb{Z}$ into $\mathbb{Z} \oplus \mathbb{Z}$.

提示. $\theta(0,1) = \theta(0,1)^2$, $\theta(1,0) = \theta(1,0)^2$, $\theta(0,0) = \theta((0,1)(1,0)) = \theta(0,1)\theta(1,0)$.

$\theta(0,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\theta(1,0)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

15.29 Determine all ring homomorphisms from $\mathbb{Z} \oplus \mathbb{Z}$ to $\mathbb{Z}$.

提示.

$\theta(0,1)$	0	1
$\theta(1,0)$	1	0

15.42 Determine all ring homomorphisms from $\mathbb{Q}$ to $\mathbb{Q}$.

提示. $\theta(1) = \theta(1 \cdot 1) = \theta(1) \cdot \theta(1) = \theta(1)^2$. So $\theta(1) \in \{0, 1\}$.

15.44 Let R be a commutative ring of prime characteristic p. Show that the Frobenius map $x \to x^p$ is a ring homomorphism from R to R.

提示. See Exercise 13.49.

補充. 參考4.73及 Lidl's Finite Field, exe.2.12。另一個更重要的應用是 Frobenis homomorphism 是 $\mathrm{Gal}_{\mathbb{Z}_p}\mathbb{Z}_{p^n} \cong \mathbb{Z}_n$ 的 generator, 參考 Foote, p.585, sec.14.3。

15.47 Suppose that R and S are commutative rings with unities. Let ϕ be a ring homomorphism from R onto S and let A be an ideal of S.

(a) If A is prime in S, show that $\phi^{-1}(A)=\{x\in R\mid\phi(x)\in A\}$ is prime in R.

(b) If A is maximal in S, show that $\phi^{-1}(A)$ is maximal in R.

提示. 三大定理

Proof. We show that $R/\phi^{-1}(A)$ is a field.

$$\begin{array}{ll}
\text{If} & x+\phi^{-1}(A)\neq 0+\phi^{-1}(A)\in R/\phi^{-1}(A)\\
\Rightarrow & x\notin\phi^{-1}(A)\\
\Rightarrow & \phi(x)\notin A\\
\Rightarrow & \phi(x)+A\neq 0+A\in S/A\\
\overset{\substack{S/A\text{ is a field}\\ \downarrow}}{\Rightarrow} & \text{there exists } s+A \text{ such that } (s+A)(\phi(x)+A)=1+A\in S/A\\
\Rightarrow & s\phi(x)+A=1+A\\
\Rightarrow & 1-s\phi(x)\in A\\
\overset{\substack{\phi\text{ is onto}\\ \downarrow}}{\Rightarrow} & \phi(1-r_sx)\in A\\
\Rightarrow & 1-r_sx\in\phi^{-1}(A)\\
\Rightarrow & (x+\phi^{-1}(A))(r_s+\phi^{-1}(A))=1+\phi^{-1}(A).
\end{array}$$

■

15.51 Prove or disprove that the field of real numbers is ring-isomorphic to the field of complex numbers.

提示. If $\theta:\mathbb{R}\to\mathbb{C}$ is an isomorphism and $\theta(r)=i$, then ...

Proof. If $\theta:\mathbb{R}\to\mathbb{C}$ is an isomorphism and $\theta(r)=i$, then

$$\theta(r^2)=\theta(r)^2=i^2=-1=\theta(-1)$$

and $r^2=-1$. Which is impossible. ■

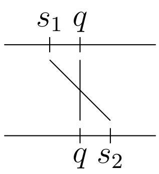
15.52 Show that the only ring automorphism of the real numbers is the identity mapping.

提示. If θ is a ring automoprhism of $\mathbb{R}$, then $\theta(1)=\theta(1\cdot1)=\theta(1)\cdot\theta(1)=\theta(1)^2$. So $\theta(1)\in\{0,1\}$.

Prove that if $r>0\in\mathbb{R}$, then $\theta(r)>0$. Suppose that there exists $s_1\in\mathbb{R}-\mathbb{Q}$ such that $\theta(s_1)=s_2\neq s_1$.

Proof. If θ is a ring automoprhism of $\mathbb{R}$, then $\theta(1)=\theta(1\cdot1)=\theta(1)\cdot\theta(1)=\theta(1)^2$. So $\theta(1)\in\{0,1\}$. But since $\theta(0)=0$ and θ is one-to-one, we have $\theta(1)\neq0$ and $\theta(1)=1$. It follows that $\theta(q)=q$ for all $q\in\mathbb{Q}\subseteq\mathbb{R}$.

If $r>0\in\mathbb{R}$, then $\theta(r)=\theta((\sqrt{r})^2)=\theta(\sqrt{r})^2>0$. If there exists $s_1\in\mathbb{R}-\mathbb{Q}$ such that $\theta(s_1)=s_2\neq s_1$. W.L.O.G., suppose that $s_2>s_1$. Then select a rational number $q\in(s_1,s_2)$. As the following figure indicates.



We have

$$0 \overset{q>s_1}{\overset{\downarrow}{<}} \theta(q-s_1) = \theta(q) - \theta(s_1) = q - s_2 < 0,$$

a contradiction. ■

15.53 Determine all ring homomorphisms from $\mathbb{R}$ to $\mathbb{R}$

15.57 Let $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$. Show that the field of quotients of $\mathbb{Z}[i]$ is ring-isomorphic to $\mathbb{Q}[i] = \{r+si \mid r,s \in \mathbb{Q}\}$.

Proof. Let F be the field of quotients of $\mathbb{Z}[i]$. Then

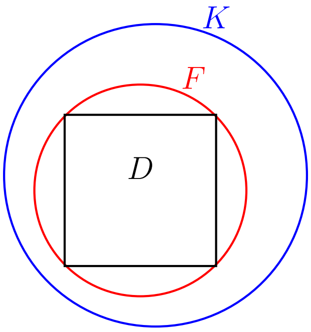
$$F = \left\{ \frac{a+bi}{c+di} \mid a+bi, c+di \in \mathbb{Z}[i], c+di \neq 0 \right\}.$$

Define a mapping θ from F to $\mathbb{Q}[i]$ and show that θ is a ring isomorphism. ■

15.58 Let F be a field. Show that the field of quotients of F is ring-isomorphic to F.

15.59 Let D be an integral domain and let F be the field of quotients of D. Show that if E is any field that contains D, then E contains a subfield that is ring-isomorphic to F. (Thus, the field of quotients of an integral domain D is the smallest field containing D.)

補充. 用圖形來記的話, 就是



以下是關於這個 field of quotient 的三個應用。

- $F[x] \leq F(x)$,
- char $F = p \Rightarrow \mathbb{Z}_p \leq F$, char $F = 0 \Rightarrow \mathbb{Q} \leq F$,
- $\theta_\pi : \mathbb{Q}[x] \to \mathbb{R}$, $\theta_\pi(f(x)) = f(\pi)$, $\ker\theta_\pi = 0$,

$$\mathbb{Q}[x] \cong \mathbb{Q}[x]/\ker\theta_\pi \cong \operatorname{Im}(\theta_\pi) = \mathbb{Q}[\pi],$$

$\mathbb{Q}[\pi] \leq \mathbb{Q}(\pi)$.

15.61 Show that the relation $\equiv$ defined in the proof of Theorem 15.6 is an equivalence relation.

15.65 Let $f(x) \in \mathbb{R}[x]$. If $a + bi$ is a complex zero of $f(x)$ (here $i = \sqrt{-1}$), show that $a - bi$ is a zero of $f(x)$.

提示. If $z = a + bi \in \mathbb{C}$, then denote the conjugate of z by $\bar{z} = a - bi$. Note that if $r \in \mathbb{R}$, then $\bar{r} = r$.

Proof. Denote the complex conjugate of $z = a + bi \in \mathbb{C}$ by $\overline{z} = a - bi$. Recall that $\overline{z_1 + z_1} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$. If $z \in \mathbb{R}$, then $\overline{z} = z$. Suppose that $f(x) = a_n x^n + \cdots a_1 x + a_0 \in \mathbb{R}[x]$. If z is a root of $f(x)$, then $0 = f(z) = a_n z^n + \cdots a_1 z + a_0$. It follows that

$$\begin{array}{rl} & f(\overline{z}) \\ = & a_n \overline{z}^n + \cdots a_1 \overline{z} + a_0 \\ = & a_n \overline{z^n} + \cdots + a_1 \overline{z} + a_0 \\ = & \overline{a_n}\,\overline{z^n} + \cdots + \overline{a_1 z} + \overline{a_0} \\ = & \overline{a_n z^n + \cdots a_1 z + a_0} \\ = & \overline{f(z)} \\ = & \overline{0} \\ = & 0. \end{array}$$

Therefore, $\overline{z}$ is also a root of $f(x)$.

■

補充. 這就是高中的虛根成雙定理。

16 Chapter 16

16.2 In $\mathbb{Z}_3[x]$, show that the distinct polynomials $x^4 + x$ and $x^2 + x$ determine the same function from $\mathbb{Z}_3$ to $\mathbb{Z}_3$.

16.3 Show that $x^2 + 3x + 2$ has four zeros in $\mathbb{Z}_6$.

16.4 If R is a commutative ring, show that the characteristic of $R[x]$ is the same as the characteristic of R.

16.5 Prove Corollary 1 of Theorem 16.2. (Remainder Theorem) Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

16.11 If $\phi : R \to S$ is a ring homomorphism, define $\overline{\phi} : R[x] \to S[x]$ by $(a_n x^n + \cdots + a_0) \to \phi(a_n)x^n + \cdots + \phi(a_0)$. Show that $\overline{\phi}$ is a ring homomorphism.

16.16 Are there any nonconstant polynomials in $\mathbb{Z}[x]$ that have multiplicative inverses? Explain your answer.

提示. See Exercise 12.25.

16.17 Let p be a prime. Are there any nonconstant polynomials in $\mathbb{Z}_p[x]$ that have multiplicative inverses? Explain your answer.

提示. See Exercise 12.26.

16.19 (Degree Rule) Let D be an integral domain and $f(x), g(x) \in D[x]$. Prove that $\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x)$. Show, by exampe, that for commutative ring R it is possible that $\deg f(x)g(x) < \deg f(x) + \deg g(x)$, where $f(x)$ and $g(x)$ are nonzero elements in $R[x]$.

16.20 Prove that the ideal $\langle x\rangle$ in $\mathbb{Q}[x]$ is maximal.

提示. 三大定理。

16.21 Let $f(x)$ belong to $F[x]$, where F is a field. Let a be a zero of $f(x)$ of multiplicity n, and write $f(x) = (x-a)^n q(x)$. If $b \neq a$ is a zero of $q(x)$, show that b has the same multiplicity as a zero of $q(x)$ as it does for $f(x)$.

16.23 Let F be an infinite field and let $f(x) \in F[x]$. If $f(a) = 0$ for infinitely many elements a of F, show that $f(x) = 0$.

16.24 Let F be an infinite field and let $f(x), g(x) \in F[x]$. If $f(a) = g(a)$ for infinitely many elements a of F, show that $f(x) = g(x)$.

16.25 Let F be a field and let $p(x) \in F[x]$. If $f(x), g(x) \in F[x]$ and $\deg f(x) < \deg p(x)$ and $\deg g(x) < \deg p(x)$, show that $f(x)+\langle p(x)\rangle = g(x)+\langle p(x)\rangle$ implies $f(x) = g(x)$.

提示.

$$\begin{aligned}
& f(x)+\langle p(x)\rangle = g(x)+\langle p(x)\rangle\\
\Rightarrow\quad & f(x)-g(x) \in \langle p(x)\rangle\\
\Rightarrow\quad & p(x) \mid f(x)-g(x)\\
\Rightarrow\quad & f(x)-g(x) = p(x)q(x) \text{ for some } q(x) \in \mathbb{Z}[x]\\
\overset{\substack{\text{if } f(x)-g(x)\neq 0\\ \downarrow}}{\Rightarrow}\quad & \deg(f(x)-g(x)) \geq \deg p(x)
\end{aligned}$$

On the other hand, if $f(x)-g(x) \neq 0$, then $\deg(f(x)-g(x)) \leq \max(\deg f(x), \deg g(x)) < \deg p(x)$, a contradiction.

16.26* Prove that $\mathbb{Z}[x]$ is not a principal ideal domain.

提示. Show that $\langle 2, x\rangle$ is not principal.

Proof. If $\langle 2, x\rangle$ is principal, then $\langle 2, x\rangle = \langle f(x)\rangle$ for some $f(x) \in \mathbb{Z}[x]$. It follows that $x = f(x)\cdot g(x)$ and $2 = f(x)\cdot h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$.

$$\begin{aligned}
& 2 = f(x)\cdot h(x)\\
\overset{\substack{\text{Exercise 16.19}\\ \downarrow}}{\Rightarrow}\quad & 0 = \deg 2 = \deg f(x) + \deg h(x)\\
\Rightarrow\quad & \deg f(x) = 0\\
\overset{\substack{2=f(x)\cdot h(x)\\ \downarrow}}{\Rightarrow}\quad & f(x) \in \{\pm 1, \pm 2\}\\
\overset{\substack{\langle f(x)\rangle=\langle 2,x\rangle\neq\mathbb{Z}[x]\\ \text{Exercise 14.15}\\ \text{Exercise 12.25}\\ \downarrow}}{\Rightarrow}\quad & f(x) \in \{\pm 2\}, \text{ contrary to that } x = f(x)\cdot g(x).
\end{aligned}$$

■

16.28 Let $f(x) \in \mathbb{R}[x]$. Suppose that $f(a) = 0$ but $f'(a) \neq 0$, where $f'(x)$ is the derivative of $f(x)$. Show that a is a zero of $f(x)$ of multiplicity 1.

16.31 Let F be a field and let

$$\begin{aligned} I &= \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \mid a_n, a_{n-1}, \ldots, a_0 \in F \text{ and} \\ &\quad a_n + a_{n-1} + \cdots + a_0 = 0\}. \end{aligned}$$

Show that I is an ideal of $F[x]$ and find a generator for I.

提示. Note that if $f(x) \in I$, then $f(1) = 0$ and $(x-1) \mid f(x)$.

Proof. Suppose that $f(x) = a_n x^n + \cdots + a_0 \in I$, where $a_n + \cdots + a_0 = 0$. Then $f(1) = 0$. By p.303, cor.2, $f(x) = (x-1)q(x)$ for some $q(x) \in F[x]$. Thus, $(x-1)$ is a generator of I and $I = \langle x-1 \rangle$ as a set. We already know that $\langle x-1 \rangle$ is an ideal of $F[x]$. Therefore, $I = \langle x-1 \rangle$ is an ideal of $F[x]$. ■

補充. In fact, $F[x]$ is a principal ideal domain.

16.33 Let m be a fixed positive integer. For any integer a, let $\overline{a}$ denote $a \pmod m$. Show that the mapping of $\phi : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ given by

$$\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = \overline{a}_n x^n + \overline{a}_{n-1}x^{n-1} + \cdots + \overline{a}_0$$

is a ring homomorphism.

Proof. Suppose that $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i \in \mathbb{Z}[x]$. Suppose that $f(x)g(x) = h(x) = \sum_{i=0}^{m+n} c_i x^i$, where $c_i = \sum_{j+k=i} a_j b_k$. Then

$$\begin{aligned} \phi(f(x)\cdot g(x)) &= \phi\left(\sum_{i=0}^{m+n} c_i x^i\right) \\ &= \sum_{i=0}^{m+n} \overline{c_i} x^i \\ &= \sum_{i=0}^{m+n} \left(\overline{\sum_{j+k=i} a_j b_k}\right) x^i \\ &= \sum_{i=0}^{m+n} \left(\sum_{j+k=i} \overline{a_j} \cdot \overline{b_k}\right) x^i \\ &= \sum_{i=0}^{n} \overline{a_i} x^i \cdot \sum_{i=0}^{m} \overline{b_i} x^i \\ &= \phi\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \phi\left(\sum_{i=0}^{m} b_i x^i\right) \end{aligned}$$

Without loss of generality, we suppose that $n = \deg f(x) \geq \deg g(x) = m$. Then we can write $g(x)$ as $\sum_{i=0}^{n} b_i x^i = b_n x^n + \cdots + b_m x^m + \cdots + b_1 x + b_0$, where $b_n = b_{n-1} = \cdots = b_{m+1} = 0$.

Then

$$\begin{aligned}
\phi(f(x)+g(x)) &= \phi\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i\right) \\
&= \phi\left(\sum_{i=0}^{n}(a_i+b_i)x^i\right) \\
&= \sum_{i=0}^{n}(\overline{a_i+b_i})x^i \\
&= \sum_{i=0}^{n}\overline{a_i}x^i + \sum_{i=0}^{n}\overline{b_i}x^i \\
&= \phi\left(\sum_{i=0}^{n} a_i x^i\right) + \phi\left(\sum_{i=0}^{n} b_i x^i\right)
\end{aligned}$$

■

16.35 For every prime p, show that

$$x^{p-1} - 1 = (x-1)(x-2)\cdots[x-(p-1)]$$

in $\mathbb{Z}_p[x]$.

提示. Note that $\mathbb{Z}_p - \{0\}$ is a group under multiplication. By Lagrange's Theorem, for any $a \in \mathbb{Z}_p - \{0\}$, $|a|$ divides $|\mathbb{Z}_p - \{0\}| = p - 1$.

16.44 Let R be a commutative ring with unity. If I is a prime ideal of R, prove that $I[x]$ is a prime ideal of $R[x]$.

提示. 由三大定理及 $R[x]/I[x] \cong (R/I)[x]$ 及 D is an integral domain implies that $D[x]$ is also an integral domain.

Proof.

$$\begin{aligned}
& I \text{ is a prime ideal of } R \\
\Rightarrow\ & R/I \text{ is an integral domain} \\
\Rightarrow\ & R[x]/I[x] \cong (R/I)[x] \text{ is an integral domain} \\
\Rightarrow\ & I[x] \lhd R[x] \text{ is a prime ideal of } R[x].
\end{aligned}$$

■

16.46 Prove that $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is ring-isomorphic to $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

提示. Consider $\theta_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}$, $\theta_{\sqrt{2}}(f(x)) = f(\sqrt{2})$. By First Isomorphism Theorem for Rings.

16.49* Let $g(x)$ and $h(x)$ belong to $\mathbb{Z}[x]$ and let $h(x)$ be monic. If $h(x)$ divides $g(x)$ in $\mathbb{Q}[x]$, show that $h(x)$ divides $g(x)$ in $\mathbb{Z}[x]$.

Proof. Suppose that $g(x) = h(x)q(x) \in \mathbb{Z}[x]$, where

$$h(x) = h_m x^m + h_{m-1}x^{m-1} + \cdots + h_1 x + h_0 \in \mathbb{Z}[x]$$

and

$$q(x) = q_n x^n + q_{n-1}x^{n-1} + \cdots + q_1 x + q_0 \in \mathbb{Q}[x].$$

We show that $q_n \in \mathbb{Z}$ and if $q_n, q_{n-1}, \ldots, q_{n-k} \in \mathbb{Z}$ for $k = 0, 1, 2, \ldots, n-1$, then $q_{n-k-1} \in \mathbb{Z}$. Since $h(x)$ is monic, we have $h_m = 1$ and $g_{m+n} = \sum_{i+j=m+n} h_i q_j = h_m q_n = q_n \in \mathbb{Z}$. Note that

$$\begin{array}{rcl}
g_{m+n-1} & = & \displaystyle\sum_{i+j=m+n-1} h_i q_j = h_m q_{n-1} + h_{m-1}q_n, \\
g_{m+n-2} & = & \displaystyle\sum_{i+j=m+n-2} h_i q_j = h_m q_{n-2} + h_{m-1}q_{n-1} + h_{m-2}q_n, \\
 & \vdots & \\
g_{m+n-k} & = & \displaystyle\sum_{i+j=m+n-k} h_i q_j = h_m q_{n-k} + h_{m-1}q_{n-k+1} + \cdots + h_{m-k}q_n, \\
g_{m+n-k-1} & = & \displaystyle\sum_{i+j=m+n-k-1} h_i q_j = h_m q_{n-k-1} + h_{m-1}q_{n-k} + \cdots + h_{m-k}q_{n-1} + h_{m-k-1}q_n \\
 & \overset{h_m=1}{\overset{\downarrow}{=}} & q_{n-k-1} + (h_{m-1}q_{n-k} + \cdots + h_{m-k}q_{n-1} + h_{m-k-1}q_n).
\end{array}$$

Thus,

$$q_{n-k-1} = g_{m+n-k-1} - (h_{m-1}q_{n-k} + \cdots + h_{m-k}q_{n-1} + h_{m-k-1}q_n).$$

If $q_n, q_{n-1}, \ldots, q_{n-k} \in \mathbb{Z}$, then

$$q_{n-k-1} = g_{m+n-k-1} - (h_{m-1}q_{n-k} + \cdots + h_{m-k}q_{n-1} + h_{m-k-1}q_n) \in \mathbb{Z}.$$

■

提示. Suppose that $g(x) = h(x)q(x) \in \mathbb{Z}[x]$, where

$$h(x) = h_m x^m + h_{m-1}x^{m-1} + \cdots + h_1 x + h_0 \in \mathbb{Z}[x]$$

and

$$q(x) = q_n x^n + q_{n-1}x^{n-1} + \cdots + q_1 x + q_0 \in \mathbb{Q}[x].$$

We show that $q_n \in \mathbb{Z}$ and if $q_n, q_{n-1}, \ldots, q_{n-k} \in \mathbb{Z}$ for $k = 0, 1, 2, \ldots, n-1$, then $q_{n-k-1} \in \mathbb{Z}$. Since $h(x)$ is monic, we have $h_m = 1$ and $g_{m+n} = \sum_{i+j=m+n} h_i q_j = h_m q_n = q_n \in \mathbb{Z}$. Note that

$$\begin{array}{rcl}
g_{m+n-1} & = & \displaystyle\sum_{i+j=m+n-1} h_i q_j = h_m q_{n-1} + h_{m-1}q_n, \\
g_{m+n-2} & = & \displaystyle\sum_{i+j=m+n-2} h_i q_j = h_m q_{n-2} + h_{m-1}q_{n-1} + h_{m-2}q_n, \\
 & \vdots & \\
g_{m+n-k} & = & \displaystyle\sum_{i+j=m+n-k} h_i q_j = h_m q_{n-k} + h_{m-1}q_{n-k+1} + \cdots + h_{m-k}q_n, \\
g_{m+n-k-1} & = & \displaystyle\sum_{i+j=m+n-k-1} h_i q_j = h_m q_{n-k-1} + h_{m-1}q_{n-k} + \cdots + h_{m-k}q_{n-1} + h_{m-k-1}q_n \\
 & \overset{h_m=1}{\overset{\downarrow}{=}} & q_{n-k-1} + (h_{m-1}q_{n-k} + \cdots + h_{m-k}q_{n-1} + h_{m-k-1}q_n).
\end{array}$$

Thus,

$$q_{n-k-1} = g_{m+n-k-1} - (h_{m-1}q_{n-k} + \cdots + h_{m-k}q_{n-1} + h_{m-k-1}q_n).$$

If $q_n, q_{n-1}, \ldots, q_{n-k} \in \mathbb{Z}$, then

$$q_{n-k-1} = g_{m+n-k-1} - (h_{m-1}q_{n-k} + \cdots + h_{m-k}q_{n-1} + h_{m-k-1}q_n) \in \mathbb{Z}.$$

16.59* Let $f(x)$ belong to $\mathbb{Z}[x]$. If $a \pmod m = b \pmod m$, prove that $f(a) \pmod m = f(b) \pmod m$. Prove that if both $f(0)$ and $f(1)$ are odd, then f has no zero in $\mathbb{Z}$.

Proof. Suppose that r is a root of f in $\mathbb{Z}$. If r is even, then $r \equiv 0 \pmod 2$ and $0 = f(r) \equiv f(0) \pmod 2$ and $f(0)$ is even, a contradiction. If r is odd, then $r \equiv 1 \pmod 2$ and $0 = f(r) \equiv f(1) \pmod 2$ and $f(1)$ is even, a contradiction. ■

提示. If r is a root of f in $\mathbb{Z}$. If r is even, then $r \equiv 0 \pmod 2$ and $0 = f(r) \equiv f(0) \pmod 2$ and $f(0)$ is even, a contradiction. If r is odd, then ...

17 Chapter 17

17.3 Show that a nonconstant polynomial from $\mathbb{Z}[x]$ that is irreducible over $\mathbb{Z}$ is primitive.

提示. By definition.

17.4* Suppose that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If r is rational and $x - r$ divides $f(x)$, show that r is an integer.

Proof. Suppose that $f(x) = (x - r)q(x)$ and $r = \frac{s}{t}$, where $\gcd(s,t) = 1$. Then $f(r) = (r - r)q(r) = 0$ and

$$0 = f(r) = f\left(\frac{s}{t}\right) = \left(\frac{s}{t}\right)^n + a_{n-1}\left(\frac{s}{t}\right)^{n-1} + \cdots + a_1\left(\frac{s}{t}\right) + a_0.$$

Multiplying both sides by t^n, we get

$$0 = s^n + a_{n-1}s^{n-1}t + \cdots + a_1st^{n-1} + a_0t^n$$

and

$$-s^n = t(a_{n-1}s^{n-1} + \cdot a_1st^{n-2} + a_0t^{n-1}).$$

Then $t \mid s^n$ and $t \mid s$ because $\gcd(s,t) = 1$. ■

提示. Suppose that $f(x) = (x - r)q(x)$ and $r = \frac{s}{t}$, where $\gcd(s,t) = 1$. Then $f(r) = (r - r)q(r) = 0$ and

$$0 = f(r) = f\left(\frac{s}{t}\right) = \left(\frac{s}{t}\right)^n + a_{n-1}\left(\frac{s}{t}\right)^{n-1} + \cdots + a_1\left(\frac{s}{t}\right) + a_0.$$

Multiplying both sides by t^n, we get

$$\underline{\hspace{5cm}}$$

and

$$-s^n = t(\underline{\hspace{5cm}}).$$

Then $t \mid s^n$ and $t \mid \underline{\hspace{1cm}}$ because $\gcd(s,t) = 1$.

17.5 Let F be a field and let a be a nonzero element of F.

(a) If $f(x+a)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

Proof. If $f(x+a)$ is irreducible over F and suppose that $f(x)=g(x)h(x)$, then $f(x+a)=g(x+a)h(x+a)$ and $g(x+a)$ is a unit or $h(x+a)$ is a unit. Without loss of generality, suppose that $g(x+a)$ is a unit. Then $g(x+a)=c\neq 0\in F$ and $g(x)=c\neq 0\in F$. That is, $g(x)$ is also a unit. Therefore, $f(x)$ is irreducible over F. ■

(b) Use part 0a to prove that $8x^3-6x+1$ is irreducible over $\mathbb{Q}$.

Proof. Let $f(x)=8x^3-6x+1\in\mathbb{Q}[x]$. Then $f(x+1)=8x^3+24x^2+18x+3$. Which is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion with $p=3$. Therefore, $f(x)$ is irreducible over $\mathbb{Q}$. ■

17.8 Suppose that $f(x)\in\mathbb{Z}_p[x]$ and $f(x)$ is irreducible over $\mathbb{Z}_p$, where p is a prime. If $\deg f(x)=n$, prove that $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field with p^n elements.

補充. 這個定理非常重要, 這是三大定理的一個應用, 這也是 finite field 構造方法的理論依據。If $f(x)\in F[x]$ is irreducible over F, then $\langle f(x)\rangle$ is a maximal ideal in $F[x]$ and $F[x]/\langle f(x)\rangle$ is a field.

17.9 Construct a field of order 25.

Proof. List all monic polynomials of degree 2 in $\mathbb{Z}_5[x]$. They are

$$\begin{array}{lll} x^2 & & \text{has root } 0 \\ x^2 & +1 & \text{has root } 2 \\ x^2 & +2 & \text{has no root in } \mathbb{Z}_5 \\ & \vdots & \end{array}$$

By Theorem 17.1, x^2+2 is **an** irreducible polynomial of degree 2 over $\mathbb{Z}_5$. By Corolloary 1 of Theorem 17.5, $\mathbb{Z}_5[x]/\langle x^2+2\rangle$ is a field. Furthermore,

$$\begin{aligned}
&\mathbb{Z}_5[x]/\langle x^2+2\rangle\\
=\;&\{f(x)+\langle x^2+2\rangle \mid f(x)\in\mathbb{Z}_5[x]\}\\
\overset{\substack{\text{by division algorithm,}\\ f(x)=(x^2+2)\cdot q(x)+r(x),\\ r(x)=0\text{ or }\deg r(x)<\deg(x^2+2)\\ \downarrow}}{=}\;&\{[(x^2+2)\cdot q(x)+r(x)]+\langle x^2+2\rangle\\
&\mid \text{for some } q(x),r(x)\in\mathbb{Z}_5[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+2)\}\\
=\;&\{\big(\underline{(x^2+2)+\langle x^2+2\rangle}\big)\cdot\big(\underline{q(x)+\langle x^2+2\rangle}\big)+\big(\underline{r(x)+\langle x^2+2\rangle}\big)\\
&\mid \text{for some } q(x),r(x)\in\mathbb{Z}_5[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+2)\}\\
=\;&\{\cancel{\big(\underline{0+\langle x^2+2\rangle}\big)\cdot\big(\underline{q(x)+\langle x^2+2\rangle}\big)}+\big(\underline{r(x)+\langle x^2+2\rangle}\big)\\
&\mid \text{for some } q(x),r(x)\in\mathbb{Z}_5[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+2)\}\\
=\;&\{r(x)+\langle x^2+2\rangle \mid r(x)=0 \text{ or } \deg r(x)<2\}\\
=\;&\{(ax+b)+\langle x^2+2\rangle \mid a,b\in\mathbb{Z}_5\}.
\end{aligned}$$

Therefore, $\mathbb{Z}_5[x]/\langle x^2+2\rangle$ is a finite field of order $5^2 = 25$.

Remark. All the monic irreducible polynomials of degree 2 in $\mathbb{Z}_5[x]$ are

$$\begin{gathered} x^2+2, \\ x^2+3, \\ x^2+x+1, \\ x^2+x+2, \\ x^2+2x+3, \\ x^2+2x+4, \\ x^2+3x+3, \\ x^2+3x+4, \\ x^2+4x+1, \\ x^2+4x+2. \end{gathered}$$

You can choose any one of them to construct a finite field of order 25. ■

17.10 Construct a field of order 27.

Proof. List all monic polynomials of degree 3 in $\mathbb{Z}_3[x]$. They are

x^3			has root 0
x^3		$+1$	has root 2
x^3		$+2$	has root 1
x^3	$+x$		has root 0
x^3	$+x$	$+1$	has root 1
x^3	$+x$	$+2$	has root 2
x^3	$+2x$	$+1$	has no root in $\mathbb{Z}_3$
	$\vdots$		

By Theorem 17.1, x^3+2x+1 is **an** irreducible polynomial of degree 3 over $\mathbb{Z}_3$. By Corolloary 1 of Theorem 17.5, $\mathbb{Z}_3[x]/\langle x^3+2x+1\rangle$ is a field. Furthermore,

$$\begin{aligned}
& \mathbb{Z}_3[x]/\langle x^3+2x+1\rangle \\
= \ & \{f(x)+\langle x^3+2x+1\rangle \mid f(x)\in\mathbb{Z}_3[x]\} \\
= \ & \{[(x^3+2x+1)\cdot q(x)+r(x)]+\langle x^3+2x+1\rangle \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_3[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^3+2x+1)\} \\
= \ & \{\big(\underline{(x^3+2x+1)+\langle x^3+2x+1\rangle}\big)\cdot\big(\underline{q(x)+\langle x^3+2x+1\rangle}\big)+\big(\underline{r(x)+\langle x^3+2x+1\rangle}\big) \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_3[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^3+2x+1)\} \\
= \ & \{\cancel{\big(\underline{0+\langle x^3+2x+1\rangle}\big)\cdot\big(\underline{q(x)+\langle x^3+2x+1\rangle}\big)}+\big(\underline{r(x)+\langle x^3+2x+1\rangle}\big) \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_3[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^3+2x+1)\} \\
= \ & \{r(x)+\langle x^3+2x+1\rangle \mid r(x)=0 \text{ or } \deg r(x)<3\} \\
= \ & \{(ax^2+bx+c)+\langle x^3+2x+1\rangle \mid a,b,c\in\mathbb{Z}_3\}.
\end{aligned}$$

Therefore, $\mathbb{Z}_3[x]/\langle x^3+2x+1\rangle$ is a finite field of order $3^3 = 27$.

Remark. All the monic irreducible polynomials of degree 3 in $\mathbb{Z}_3[x]$ are

$$\begin{gathered}
x^3 + 2x + 1,\\
x^3 + 2x + 2,\\
x^3 + x^2 + 2,\\
x^3 + x^2 + x + 2,\\
x^3 + x^2 + 2x + 1,\\
x^3 + 2x^2 + 1,\\
x^3 + 2x^2 + x + 1,\\
x^3 + 2x^2 + 2x + 2.
\end{gathered}$$

You can choose any one of them to construct a finite field of order 27. ■

17.11 Show that $x^3 + x^2 + x + 1$ is reducible over $\mathbb{Q}$. Does this fact contradict the corollary to Theorem 17.4?

Proof. Observe that $x^3+x^2+x+1 = (x^3+x^2)+(x+1) = x^2(x+1)+(x+1) = (x^2+1)(x+1)$ or

$$\begin{aligned}
x^3 + x^2 + x + 1 &= \frac{(x-1)(x^3 + x^2 + x + 1)}{(x-1)}\\
&= \frac{(x^4 - 1)}{(x-1)}\\
&= \frac{(x^2+1)(x^2-1)}{(x-1)}\\
&= \frac{(x^2+1)(x+1)\cancel{(x-1)}}{\cancel{(x-1)}}\\
&= (x^2+1)(x+1).
\end{aligned}$$

■

17.12 Determine which of the polynomials below is (are) irreducible over $\mathbb{Q}$.

(a) $x^5 + 9x^4 + 12x^2 + 6$

(b) $x^4 + x + 1$

(c) $x^4 + 3x^2 + 3$

(d) $x^5 + 5x^2 + 1$

(e) $(5/2)x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + 3/14$

Proof.

(a) Let $f(x) = x^5 + 9x^4 + 12x^2 + 6$. Choose prime $p = 3$.

- p divides all the coefficients of $f(x)$ except the leading coefficient.
- p doesn't divide the leading coefficient 1 of $f(x)$ and
- $p^2 = 9$ doesn't divide the constant term 6 of $f(x)$.

By Eisenstein's criterion, $f(x)$ is irreducible over $\mathbb{Q}$.

(b) **補充:** 這題你應該先試試 $f(x+1), f(x+2), f(x-1), f(x-2)$ 能否用 Eisenstein's criterion。

這題有點難, 不妨先跳過, 做完助教補充的題目之後, 再回來看這題。

Let $f(x) = x^4 + x + 1$. Consider $\bar{f}(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$. We want to show that $\bar{f}(x)$ is irreducible over $\mathbb{Z}_2$. Then by Mod p Irreducibility Test, $f(x)$ is irreducible over $\mathbb{Q}$.

$\bar{f}(x)$ has no root in $\mathbb{Z}_2$, so $\bar{f}(x)$ has no linear factor in $\mathbb{Z}_2[x]$ by Factor Theorem. But $\deg \bar{f}(x) \notin \{2,3\}$, we can't apply Theorem 17.1 on it.

List all monic polynomials of degree 2 in $\mathbb{Z}_2[x]$. They are

$$\begin{array}{llll} x^2 & & & \text{has root } 0 \\ x^2 & & +1 & \text{has root } 1 \\ x^2 & +x & & \text{has root } 0 \\ x^2 & +x & +1 & \text{has no root in } \mathbb{Z}_2 \end{array}$$

By Theorem 17.1, $x^2 + x + 1$ is the only one irreducible polynomial of degree 2 over $\mathbb{Z}_2$. If $\bar{f}(x) = x^4 + x + 1$ is not irreducible over $\mathbb{Z}_2$, then it must be $\bar{f}(x) = (x^2 + x + 1)^2$ because $\bar{f}(x)$ has no linear factor. But $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq \bar{f}(x)$. Hence, $\bar{f}(x)$ is irreducible over $\mathbb{Z}_2$.

(c) Let $f(x) = x^4 + 3x^2 + 3$. Choose prime $p = 3$.

- p divides all the coefficients of $f(x)$ except the leading coefficient.
- p doesn't divide the leading coefficient 1 of $f(x)$ and
- $p^2 = 9$ doesn't divide the constant term 3 of $f(x)$.

By Eisenstein's criterion, $f(x)$ is irreducible over $\mathbb{Q}$.

(d) Let $f(x) = x^5 + 5x^2 + 1$. Note that $f(x-1) = x^5 - 5x^4 + 10x^3 - 5x^2 - 5x + 5$. Choose prime $p = 5$.

- p divides all the coefficients of $f(x-1)$ except the leading coefficient.
- p doesn't divide the leading coefficient 1 of $f(x-1)$ and
- $p^2 = 25$ doesn't divide the constant term 5 of $f(x-1)$.

By Eisenstein's criterion, $f(x-1)$ is irreducible over $\mathbb{Q}$, so is $f(x)$ by Exercise 17.5.

補充: 你或許會困惑說, 我怎麼知道考慮 $f(x+1), f(x+2), f(x-1)$ 還是 $f(x-2)$, 一般來說, 我們就是用 trial and error, 試試看就知道了, 可以! 你幸, 不行, 你命, 就趕快換個方法吧。

(e) Let $f(x) = (5/2)x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + 3/14$. Consider $14f(x) = 35x^5 + 63x^4 + 210x^3 + 6x^2 + 84x + 3$. Choose prime $p = 3$.

- p divides all the coefficients of $14f(x)$ except the leading coefficient.
- p doesn't divide the leading coefficient 35 of $14f(x)$ and
- $p^2 = 9$ doesn't divide the constant term 3 of $14f(x)$.

By Eisenstein's criterion, $14f(x)$ is irreducible over $\mathbb{Q}$, so is $f(x)$ by Exercise 17.5.

■

17.13 Show that $x^4 + 1$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.

提示. Show that x^4+1 is irreducibe over $\mathbb{Z}$. Then by p.313, Theorem 17.2. You can assume that $x^4+1=(ax^2+bx+c)(dx^2+ex+f)$, where $a,b,c,d,e,f\in\mathbb{Z}$.
$x^4+1=(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$.

Proof. Let $f(x)=x^4+1$. Note that $f(x+1)=x^4+4x^3+6x^2+4x+2$. Choose prime $p=2$.

- p divides all the coefficients of $f(x+1)$ except the leading coefficient.
- p doesn't divide the leading coefficient 1 of $f(x+1)$ and
- $p^2=4$ doesn't divide the constant term 2 of $f(x+1)$.

By Eisenstein's criterion, $f(x+1)$ is irreducible over $\mathbb{Q}$, so is $f(x)$ by Exercise 17.5.

$$x^4+1=(x^2)^2+1=(x^2+1)^2-2x^2=(x^2+1)^2-(\sqrt{2}x)^2=(x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)\in\mathbb{R}[x].$$

■

補充. 你可以先將 x^4+1 在 $\mathbb{C}$ 中分解, 並且將以相互共軛的複數爲根的兩個一次多項式乘在一起並乘開。

$$\begin{aligned}
x^4+1 &= (x^2)^2-(-1)\\
&= (x^2)^2-i^2\\
&= (x^2-i)(x^2+i)\\
&= (x^2-i)[x^2-(-i)]\\
&= \left[x^2-\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right)^2\right]\cdot\left[x^2-\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i\right)^2\right]\\
&= \left[x-\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right)\right]\underbrace{\left[x+\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right)\right]\left[x-\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i\right)\right]}_{\text{exchange}}\left[x+\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i\right)\right]\\
&= \left[x-\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right)\right]\left[x-\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i\right)\right]\left[x+\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right)\right]\left[x+\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i\right)\right]\\
&= (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1).
\end{aligned}$$

17.14 Show that x^2+x+4 is irreducible over $\mathbb{Z}_{11}$.

x^2+x+4 has no root in $\mathbb{Z}_{11}$ and $\deg(x^2+x+4)=2$. By Theorem 17.1.

17.15 Let $f(x)=x^3+6\in\mathbb{Z}_7[x]$. Write $f(x)$ as a product of irreducible polynomials over $\mathbb{Z}_7$.

Proof. Note that $f(1)=1^3+6=7=0$. By Factor Theorem, $(x-1)$ is a factor of $f(x)$.

$$\begin{array}{r|rrrr}
 & x^2 & +x & +1 & \\ \hline
x-1 & x^3 & & & +6 \\
 & x^3 & -x^2 & & \\ \cline{2-4}
 & & x^2 & & \\
 & & x^2 & -x & \\ \cline{3-5}
 & & & x & +6 \\
 & & & x & -1 \\ \cline{4-5}
 & & & & 0
\end{array}$$

Thus, $f(x) = (x-1)(x^2+x+1)$. Let $g(x) = x^2+x+1$. Note that $g(2) = 0$. By Factor Theorem, $(x-2)$ is a factor of $g(x)$.

$$\begin{array}{r|lll} & x & +3 & \\ \hline x-2 & x^2 & +x & +1 \\ & x^2 & -2x & \\ \hline & & 3x & +1 \\ & & 3x & -6 \\ \hline & & & 0 \end{array}$$

Therefore, $g(x) = (x-2)(x+3)$ and $f(x) = (x-1)(x-2)(x+3)$. ■

17.16 Let $f(x) = x^3+x^2+x+1 \in \mathbb{Z}_2[x]$. Write $f(x)$ as a product of irreducible polynomial over $\mathbb{Z}_2$.

Proof. Note that $f(1) = 0$. By Factor Theorem, $(x-1)$ is a factor of $f(x)$.

$$\begin{array}{r|llll} & x^2 & & +1 & \\ \hline x-1 & x^3 & +x^2 & +x & +1 \\ & x^3 & -x^2 & & \\ \hline & & & +x & +1 \\ & & & +x & -1 \\ \hline & & & & 0 \end{array}$$

Thus, $f(x) = (x-1)(x^2+1)$. Let $g(x) = x^2+1$. Note that $g(1) = 0$. By Factor Theorem, $(x-1)$ is a factor of $g(x)$.

$$\begin{array}{r|lll} & x & +1 & \\ \hline x-1 & x^2 & & +1 \\ & x^2 & -x & \\ \hline & & x & +1 \\ & & x & -1 \\ \hline & & & 0 \end{array}$$

Therefore, $g(x) = (x-1)(x+1)$ and $f(x) = (x-1)(x-1)(x+1) = (x+1)^3$. ■

17.17* Let p be a prime.

(a) Show that the number of reducible polynomials over $\mathbb{Z}_p$ of the form x^2+ax+b is $p(p+1)/2$.

Proof. [方法一]

$$\begin{aligned} & \#\{\text{reducible polynomial } x^2+ax+b\} \\ = \; & \#\{(x-\alpha)(x-\beta) \mid \alpha, \beta \in \mathbb{Z}_p\} \\ = \; & \#\{(x-\alpha)^2 \mid \alpha \in \mathbb{Z}_p\} + \#\{(x-\alpha)(x-\beta) \mid \alpha \neq \beta \in \mathbb{Z}_p\} \\ = \; & p + \binom{p}{2} = p + \frac{p(p-1)}{2} = \frac{p(p+1)}{2}. \end{aligned}$$

[方法二]

- Recall that if $f(x) \in F[x]$ and $f(x) \in \{2,3\}$, then $f(x)$ is irreducible over F if and only if $f(x)$ has no root in F.
- If $p = 2$, then there are $3 = \frac{2(2+1)}{2}$ reducible polynomials over $\mathbb{Z}_p$. They are x^2, x^2+1 and x^2+x. We suppose that $p \geq 3$.
- Given a fixed $a \in \mathbb{Z}_p$. For any $f \in \mathbb{Z}_p$, let $b = -f^2 - af$. Then f is a root of the polynomial $x^2 + ax + b$.
- It may seem that there are p choices for f and p possiblities of b. But this is not the case. If $f_1 \neq f_2$, then

  $$-f_1^2 - af_1 = -f_2^2 - af_2 \Leftrightarrow (f_1 - f_2)(f_1 + f_2 + a) = 0 \Leftrightarrow f_1 + f_2 + a = 0.$$

  That is, when $f_2 = -a - f_1$, we get the same b.
- Note that

  $$f_1 = f_2 = -a - f_1 \Leftrightarrow 2f_1 = -a \overset{p\geq 3}{\overset{\downarrow}{\Leftrightarrow}} f_1 = (-a)\cdot 2^{-1}.$$

  That is, we have $f_1 = f_2$ when $f_1 = (-a)\cdot 2^{-1}$.
- Therefore, there are $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ choices for f.

■

(b) Determine the number of reducible quadratic polynomials over $\mathbb{Z}_p$.

提示. $(p-1)\cdot p(p+1)/2$. Note that $f(x) \in F[x]$ has a root in F if and only if $rf(x)$ has a root in F, where $r \neq 0 \in F$.

17.20 Prove that, for every positive integer n, there are infinitely many polynomials of degree n in $\mathbb{Z}[x]$ that are irreducible over $\mathbb{Q}$.

提示. Eisenstein Criterion.

17.27 (Rational Root Theorem) Let

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

and $a_n \neq 0$. Prove that if r and s are relatively prime integers and $f(r/s) = 0$, then $r \mid a_0$ and $s \mid a_n$.

17.29* Show that $x^4 + 1$ is reducible over $\mathbb{Z}_p$ for every prime p.

Proof. 助教在這裡給出我曾經試過的幾個方法, 希望你們可以用正確的心態看待錯誤的嘗試, 因爲, 失敗正是成功之母。

- 方法一 (失敗): 觀察簡單的情形。

$$\begin{array}{rcl} \text{in } \mathbb{Z}_2[x],\ (x^4+1) & = & (x^2+1)(x^2+1) \\ \text{in } \mathbb{Z}_3[x],\ (x^4+1) & = & (x^2+x+2)(x^2+2x+2) \\ \text{in } \mathbb{Z}_5[x],\ (x^4+1) & = & (x^2+2)(x^2+3) \\ & \vdots & \end{array}$$

觀察不出規律, 更重要的是, 或許根本沒有規律, 也就是說, 或許根本不存在一個用 p 來表述的公式, 可以給出 $(x^4+1) = (x^2+ax+b)(x^2+cx+d)$。

- 方法二 (失敗): 嘗試用 Mod-p Irreducibility Test。如果存在 p, 使得 x^4+1 是 irreducible over $\mathbb{Z}_p$, 則對於任意的 $s_4, s_3, ..., s_1, s_0 \in \mathbb{Z}$, $(ps_4+1)x^4+ps_3x^3+ps_2x^2+ps_1x+(ps_0+1)$ 是 irreducible over $\mathbb{Q}$。我們希望找到一組 $s_4, s_3, ..., s_1, s_0$ 使得這件事不成立, 如此就可以證得矛盾, 但是我失敗了。王 O 鈞同學找了 $x^4+1=(x^2+px+1)^2$, 但是是不行的。
- 方法三 (成功): 要用到一個 finite field 的定理, 也就是你課本的 p.389, thm.22.2。如果存在 p 使得 x^4+1 是 irreducible over $\mathbb{Z}_p$, 則 $\mathbb{Z}_p[x]/\langle x^4+1\rangle$ 是一個 finite field, 令 $E=\mathbb{Z}_p[x]/\langle x^4+1\rangle$。

  觀察 $x^4+1=0\in E$, 所以 $x^4=-1$ 且 $x^8=1$ 且 $x\in E$ 的 multiplicative order 是 8。因爲 $E-\{0\}$ 在乘法下是一個group, 由 Lagrange's Theorem, 8 整除 $|E-\{0\}|=p^4-1$, 所以我們想要證明 $8\nmid p^4-1$ 得到矛盾。試了 $p=2$, 的確有 $8\nmid p^4-1$, 感覺有機會, 但是稍微試了 $p=3$, $p=5$, ..., 可惡, 馬上被打臉。但仔細想一想, 如果 p 是奇數, 則 $8\mid(p^4-1)=\underline{(p^2+1)}_{2s}\underline{(p+1)}_{2t}\underline{(p-1)}_{2u}$, 所以這條路是證不出矛盾的。

  換個方式, 再來一次, 注意到 $(-x)$ 的 multiplicative order 也是 8。但是 $x=(-x)^2$, 所以感覺上 $(-x)$ 的 multiplicative order 應該是 16 才對, 這個觀察提供了一些想法。

  由 p.389, thm.22.2, $E-\{0\}$ 在乘法下是一個cyclic group。假設 $E-\{0\}=\langle g\rangle$, 且 $-x=g^d$, 則 $x=g^{2d}$, 令 $|g^r|$ 表示 g^r 的 multiplicative order,

$$\frac{p^4-1}{\gcd(2d,p^4-1)}=|g^{2d}|=|x|=8=|-x|=|g^d|=\frac{p^4-1}{\gcd(d,p^4-1)}.$$

  於是 $\gcd(2d,p^4-1)=\gcd(d,p^4-1)$, 假設

$$\begin{aligned} d &= 2^s\cdot a,\ 2\nmid a,\\ p^4-1 &= 2^t\cdot b,\ 2\nmid b,\\ & s\le t. \end{aligned}$$

  如果 $s<t$, 則

$$\gcd(d,p^4-1)=2^s\gcd(a,b)\ne 2^{s+1}\gcd(a,b)=\gcd(2d,p^4-1).$$

  所以必有 $s=t$, 接著又走不下去了。

  再觀察一下, $0=x+(-x)=g^{2d}+g^d=g^d(g^d+1)$, 因爲 E 是一個 integral domain 且 $g^d\ne 0$, 所以 $g^d+1=0$ 且 $g^d=-1$ 且 $x=g^{2d}=1$, 矛盾。

■

17.31 Let F be a field and let $p(x)$ be irreducible over F. If E is a field that contains F and there is an element a in E such that $p(a)=0$, show that the mapping $\phi: F[x]\to E$ given by $f(x)\to f(a)$ is a ring homomorphism with kernel $\langle p(x)\rangle$.

補充. 非常重要。

17.32 Prove that the ideal $\langle x^2+1\rangle$ is prime in $\mathbb{Z}[x]$ but not maximal in $\mathbb{Z}[x]$.

Proof. Define $\theta:\mathbb{Z}[x]\to\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}\le\mathbb{C}$ by $\theta(f(x))=f(i)$. Show that θ is an onto ring homomorphism. Obviously, $x^2+1\in\ker\theta$, so $\langle x^2+1\rangle\subseteq\ker\theta$. By the following Lemma, we have $\langle x^2+1\rangle=\ker\theta$. By the First Isomorphism Theorem,

$$\mathbb{Z}[x]/\langle x^2+1\rangle=\mathbb{Z}[x]/\ker\theta\cong\text{Im }\theta\overset{\overset{\theta\text{ is onto}}{\downarrow}}{=}\mathbb{Z}[i]\le\mathbb{C}.$$

Since $\mathbb{Z}[i]$ is a subring of the field $\mathbb{C}$, $\mathbb{Z}[i]$ is an integral domain and $\langle x^2+1\rangle$ is a prime ideal in $\mathbb{Z}[x]$. Since $1+i$ has no multiplicative inverse in $\mathbb{Z}[i]$, $\mathbb{Z}[i]$ is not a field and $\langle x^2+1\rangle$ is not a maximal ideal in $\mathbb{Z}[x]$.

Lemma. $\langle x^2+1\rangle = \ker\theta$**:** Define $\overline{\theta}:\mathbb{Q}[x]\to\mathbb{Q}[i]=\{a+bi \mid a,b\in\mathbb{Q}\}$ by $\overline{\theta}(f(x))=f(i)$. Show that θ is an onto ring homomorphism and $\langle x^2+1\rangle = \ker\overline{\theta}$.

If $f(x)\in\ker\theta$, then $f(x)\in\ker\overline{\theta}=\langle x^2+1\rangle$. Assume $f(x)=(x^2+1)\left(\frac{a_n}{b_n}x^n+\cdots+\frac{a_1}{b_1}x+\frac{a_0}{b_0}\right)$. Let $\pi=b_n\cdot b_{n-1}\cdots b_1\cdot b_0$. Then

$$\begin{aligned}
f(x) &= (x^2+1)\cdot\frac{1}{\pi}\cdot\left(a_n\frac{\pi}{b_n}x^n+\cdots+a_1\frac{\pi}{b_1}x+a_0\frac{\pi}{b_0}\right)\\
&= (x^2+1)\cdot\frac{\gcd\left(a_n\frac{\pi}{b_n},\cdots,a_1\frac{\pi}{b_1},a_0\frac{\pi}{b_0}\right)}{\pi}\cdot(c_nx^n+\cdots+c_1x+c_0)\\
&= (x^2+1)\cdot\frac{v}{w}\cdot(c_nx^n+\cdots+c_1x+c_0)\\
\Rightarrow wf(x) &= (x^2+1)\cdot v\cdot(c_nx^n+\cdots+c_1x+c_0).
\end{aligned}$$

where $v,w,c_n,\dots,c_1,c_0\in\mathbb{Z}$ and $\gcd(c_n,\dots,c_1,c_0)=1$ and $\gcd(v,w)=1$ by canceling out the common factor of $\gcd\left(a_n\frac{\pi}{b_n},\cdots,a_1\frac{\pi}{b_1},a_0\frac{\pi}{b_0}\right)$ and π. We show that $w=1$. Then we have $f(x)\in\langle x^2+1\rangle$ and $\langle x^2+1\rangle=\ker\theta$.

If $w\neq1$, then there exists a prime p divides w. Since $\gcd(v,w)=1$, we have $p\nmid v$. Since $\gcd(c_n,\dots,c_1,c_0)=1$, we have $p\nmid c_i$ for some $i\in\{n,\dots,1,0\}$. Consider $\overline{wf(x)}\in\mathbb{Z}_p[x]$. We have

$$\begin{aligned}
\overline{0} &= \overline{0}\cdot\overline{f(x)}\\
&\overset{\overset{p|w}{\downarrow}}{=} \overline{w}\cdot\overline{f(x)}\\
&= \overline{wf(x)}\\
&= \overline{(x^2+1)\cdot v\cdot(c_nx^n+\cdots+c_1x+c_0)}\\
&= \overline{(x^2+1)}\cdot\overline{v}\cdot\overline{(c_nx^n+\cdots+c_1x+c_0)}\\
&\overset{\overset{p\nmid v,\ p\nmid c_i}{\downarrow}}{=} \overline{(x^2+1)}_{\neq0}\cdot\overline{v}_{\neq0}\cdot\overline{(c_nx^n+\cdots+c_1x+c_0)}_{\neq0}\\
&\overset{\overset{\mathbb{Z}_p[x]\text{ is an I.D.}}{\downarrow}}{\neq} \overline{0}\in\mathbb{Z}_p[x].
\end{aligned}$$

Which is a contradiction. ■

補充. 注意, 課本的 Division Algorithm 只能用在 $F[x]$ 上, 所以我們不能用課本提供的 Division Algorithm 來證明 $\langle x^2+1\rangle=\ker\theta\subseteq\mathbb{Z}[x]$。但事實上, F 是一個 field 這個條件太強了, 下面是廣義的 Division Algorithm。

Let R be a ring with unity and let $f(x),g(x)\in R[x]$. If $g(x)\neq0$ and the leading coefficient of g is a unit in R, then there exists uniquely $q(x),r(x)\in R[x]$ such that $f(x)=g(x)q(x)+r(x)$, where $r(x)=0$ or $\deg r(x)<\deg f(x)$.

類似地, 更廣義的 Factor Theorem 敍述如下。

Let R be a commutative ring with unity. Let $a\in R$ and let $f(x)\in R[x]$. Then $f(a)=0$ if and only if $f(x)=(x-a)q(x)$ for some $q(x)\in R[x]$.

於是, 我們可以用下面另一個解法,

If $f(x)\in\ker\theta$, then $f(i)=\theta(f(x))=0$. By the Complex Conjugate Root Theorem, $f(-i)=0$. By Factor Theorem, $(x-i)(x+i)=(x^2+1)\mid f(x)$. That is, $f(x)\in\langle x^2+1\rangle$.

17.33 Let F be a field and let $p(x)$ be irreducible over F. Show that $\{a + \langle p(x)\rangle \mid a \in F\}$ is a subfield of $F[x]/\langle p(x)\rangle$ isomorphic to F.

17.34 Let F be a field and let $f(x)$ be a polynomial in $F[x]$ that is reducible over F. Prove that $\langle f(x)\rangle$ is not a prime ideal in $F[x]$.

提示. By definition.

17.36* Suppose there is a real number r with the property that $r + 1/r$ is an odd integer. Prove that r is irrational.

Proof. If $r \in \mathbb{R}$ satisfying

$$r + \frac{1}{r} = 2k + 1, \text{ for some } k \in \mathbb{Z},$$

then $r = \frac{(2k+1)\pm\sqrt{4k^2+4k-3}}{2}$. That is, given any integer k, there exists a real number r such that $r + \frac{1}{r} = 2k + 1$. We show that this real number r is irrational.

If $r \in \mathbb{Q}$, suppose that $r = \frac{a}{b}$, where $\gcd(a, b) = 1$, then

$$r + \frac{1}{r} = \frac{a}{b} + \frac{b}{a} = 2k + 1.$$

By some simple computation, we get $a^2 + b^2 = (2k+1)a^2b^2$. If a and b are odd, then $a^2 + b^2$ is even but $(2k + 1)a^2b^2$ is odd, a contradiction. If a is odd and b is even, then $a^2 + b^2$ is odd but $(2k + 1)a^2b^2$ is even, a contradiction. If a and b both are even, then $\gcd(a, b) \neq 1$, a contradiction. ■

提示. If $r \in \mathbb{R}$ satisfying

$$r + \frac{1}{r} = 2k + 1, \text{ for some } k \in \mathbb{Z},$$

then $r = \frac{(2k+1)\pm\sqrt{4k^2+4k-3}}{2}$. That is, given any integer k, there exists a real number r such that $r + \frac{1}{r} = 2k + 1$. We show that this real number r is irrational.

If $r \in \mathbb{Q}$, suppose that $r = \frac{a}{b}$, where $\gcd(a, b) = 1$, then

$$r + \frac{1}{r} = \frac{a}{b} + \frac{b}{a} = 2k + 1.$$

By some simple computation, we get $a^2 + b^2 = (2k+1)a^2b^2$. If a and b are odd, then $a^2 + b^2$ is even but $(2k + 1)a^2b^2$ is odd, a contradiction. If a is odd...

p.317, thm.17.5 Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x)\rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F.

Proof. ($\Rightarrow$) If $\langle p(x)\rangle$ is a maximal ideal in $F[x]$, then $\langle p(x)\rangle \neq \{0\}$ and

$$p(x) \neq 0, \tag{21}$$

otherwise, $\{0\} = \langle p(x)\rangle \subsetneq \langle x\rangle \subsetneq F[x]$, contrary to the maximality of $\langle p(x)\rangle$.

$$\begin{aligned} & \text{Suppose that } p(x) = a(x)b(x) \qquad (22) \\ \Rightarrow\quad & \langle p(x)\rangle \subseteq \langle a(x)\rangle \subseteq F[x] \\ \overset{\substack{\langle p(x)\rangle \text{ is a maximal ideal in } F[x] \\ \downarrow}}{\Rightarrow}\quad & \langle a(x)\rangle = \langle p(x)\rangle \text{ or } \langle a(x)\rangle = F[x]. \end{aligned}$$

$$\begin{aligned} \text{If } \langle a(x)\rangle = F[x] \quad & \Rightarrow \quad 1 \in F[x] = \langle a(x)\rangle \\ & \Rightarrow \quad 1 = a(x)q(x) \text{ for some } q(x) \in F[x] \\ & \Rightarrow \quad a(x) \text{ is a unit.} \end{aligned}$$

$$\begin{aligned} \text{If } \langle a(x)\rangle = \langle p(x)\rangle \quad & \Rightarrow \quad a(x) \in \langle p(x)\rangle \\ & \Rightarrow \quad a(x) = p(x)q(x) \text{ for some } q(x) \in F[x] \\ & \overset{\substack{(22) \\ \downarrow}}{\Rightarrow} \quad p(x) = p(x)q(x)b(x) \\ & \Rightarrow \quad p(x)(q(x)b(x) - 1) = 0 \\ & \overset{\substack{F[x] \text{ is an I.D. and by (21)} \\ \downarrow}}{\Rightarrow} \quad q(x)b(x) - 1 = 0 \\ & \Rightarrow \quad b(x) \text{ is a unit in } F[x]. \end{aligned}$$

Therefore, $p(x)$ is irreducible over F.

($\Leftarrow$) Suppose $p(x)$ is irreducible over F and $\langle p(x)\rangle \subseteq I \subseteq F[x]$. Since $F[x]$ is a P.I.D., we can assume $I = \langle q(x)\rangle$ for some $q(x) \in F[x]$. Then $\langle p(x)\rangle \subseteq \langle q(x)\rangle \subseteq F[x]$ and $p(x) \in \langle q(x)\rangle$ and $p(x) = q(x)r(x)$ for some $r(x) \in F[x]$. Since $p(x)$ is irreducible over F, either $q(x)$ or $r(x)$ is a unit. If $q(x)$ is a unit, then $\langle q(x)\rangle = F[x]$. If $r(x)$ is a unit, then $q(x) = p(x)r(x)^{-1}$ and $q(x) \in \langle p(x)\rangle$ and $\langle p(x)\rangle = \langle q(x)\rangle$. ■

p.317, cor.1 Let F be a field and $p(x)$ be an irreducible polynomial over F. Then $F[x]/\langle p(x)\rangle$ is a field.

Proof. If $p(x)$ is irreducible over F, then $\langle p(x)\rangle$ is a maximal ideal in $F[x]$. By p.274, thm.14.4, $F[x]/\langle p(x)\rangle$ is a field. ■

補充 17.A Construct a field of order 4.

Proof. List all monic polynomials of degree 2 in $\mathbb{Z}_2[x]$. They are

x^2			has root 0
x^2		$+1$	has root 1
x^2	$+x$		has root 0
x^2	$+x$	$+1$	has no root in $\mathbb{Z}_2$

By Theorem 17.1, x^2+x+1 is the only one irreducible polynomial of degree 2 over $\mathbb{Z}_2$. By Corolloary 1 of Theorem 17.5, $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is a field. Furthermore,

$$\begin{aligned}
& \mathbb{Z}_2[x]/\langle x^2+x+1\rangle \\
= \; & \{f(x)+\langle x^2+x+1\rangle \mid f(x)\in\mathbb{Z}_2[x]\} \\
= \; & \{[(x^2+x+1)\cdot q(x)+r(x)]+\langle x^2+x+1\rangle \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_2[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+x+1)\} \\
= \; & \{\big(\underline{(x^2+x+1)+\langle x^2+x+1\rangle}\big)\cdot\big(\underline{q(x)+\langle x^2+x+1\rangle}\big)+\big(\underline{r(x)+\langle x^2+x+1\rangle}\big) \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_2[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+x+1)\} \\
= \; & \{\cancel{\big(\underline{0+\langle x^2+x+1\rangle}\big)\cdot\big(\underline{q(x)+\langle x^2+x+1\rangle}\big)+}\big(\underline{r(x)+\langle x^2+x+1\rangle}\big) \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_2[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+x+1)\} \\
= \; & \{r(x)+\langle x^2+x+1\rangle \mid r(x)=0 \text{ or } \deg r(x)<2\} \\
= \; & \{(ax+b)+\langle x^2+x+1\rangle \mid a,b\in\mathbb{Z}_2\}.
\end{aligned}$$

Therefore, $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ is a finite field of order $2^2=4$. ■

補充 17.B Construct a field of order 9.

Proof. List all monic polynomials of degree 2 in $\mathbb{Z}_3[x]$. They are

$$\begin{array}{lll}
x^2 & & \text{has root } 0 \\
x^2 & +1 & \text{has no root in } \mathbb{Z}_3 \\
\vdots & &
\end{array}$$

By Theorem 17.1, x^2+1 is **an** irreducible polynomial of degree 2 over $\mathbb{Z}_3$. By Corolloary 1 of Theorem 17.5, $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field. Furthermore,

$$\begin{aligned}
& \mathbb{Z}_3[x]/\langle x^2+1\rangle \\
= \; & \{f(x)+\langle x^2+1\rangle \mid f(x)\in\mathbb{Z}_3[x]\} \\
= \; & \{[(x^2+1)\cdot q(x)+r(x)]+\langle x^2+1\rangle \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_3[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+1)\} \\
= \; & \{\big(\underline{(x^2+1)+\langle x^2+1\rangle}\big)\cdot\big(\underline{q(x)+\langle x^2+1\rangle}\big)+\big(\underline{r(x)+\langle x^2+1\rangle}\big) \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_3[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+1)\} \\
= \; & \{\cancel{\big(\underline{0+\langle x^2+1\rangle}\big)\cdot\big(\underline{q(x)+\langle x^2+1\rangle}\big)+}\big(\underline{r(x)+\langle x^2+1\rangle}\big) \\
& \mid \text{for some } q(x),r(x)\in\mathbb{Z}_3[x], r(x)=0 \text{ or } \deg r(x)<\deg(x^2+1)\} \\
= \; & \{r(x)+\langle x^2+1\rangle \mid r(x)=0 \text{ or } \deg r(x)<2\} \\
= \; & \{(ax+b)+\langle x^2+1\rangle \mid a,b\in\mathbb{Z}_3\}.
\end{aligned}$$

Therefore, $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a finite field of order $3^2=9$.

Remark. All the monic irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$ are

$$\begin{gathered}
x^2+1, \\
x^2+x+2, \\
x^2+2x+2.
\end{gathered}$$

You can choose any one of them to construct a finite field of order 9. ■

18 Chapter 18

18.1 For the ring $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$, where $d \neq 1$ and d is not divisible by the square of a prime, prove that the norm $N(a + b\sqrt{d}) = |a^2 - db^2|$ satisfies the four assertions made preceding Example 1.

Proof.

$$N(a + b\sqrt{d}) = |a^2 - db^2| = 0 \Leftrightarrow a^2 - db^2 = 0 \Leftrightarrow a^2 = db^2.$$

If $b \neq 0$, then $d = \left(\frac{a}{b}\right)^2$, a contradiction. Thus, $b = 0 = a$.

$$\begin{aligned}
& a + b\sqrt{d} \text{ is a unit} \\
\Rightarrow\ & \text{there exists } c + e\sqrt{d} \text{ such that } (a + b\sqrt{d})(c + e\sqrt{d}) = 1 \\
\Rightarrow\ & N(a + b\sqrt{d}) \cdot N(c + e\sqrt{d}) = N((a + b\sqrt{d}) \cdot (c + e\sqrt{d})) = N(1) = 1 \\
\Rightarrow\ & N(a + b\sqrt{d}) = 1
\end{aligned}$$

$$\begin{aligned}
& N(a + b\sqrt{d}) = 1 \\
\Rightarrow\ & |a^2 - db^2| = N(a + b\sqrt{d}) = 1 \\
\Rightarrow\ & a^2 - db^2 = \pm 1 \\
\text{If}\ & a^2 - db^2 = 1 \\
\Rightarrow\ & (a + b\sqrt{d}) \cdot (a - b\sqrt{d}) = a^2 - db^2 = 1 \\
\Rightarrow\ & a + b\sqrt{d} \text{ is a unit} \\
\text{If}\ & a^2 - db^2 = -1 \\
\Rightarrow\ & (a + b\sqrt{d}) \cdot (a - b\sqrt{d}) = a^2 - db^2 = -1 \\
\Rightarrow\ & a + b\sqrt{d} \text{ is a unit with inverse } (-1)(a - b\sqrt{d})
\end{aligned}$$

■

補充.

- 注意,d 可能為負數, 也就是 $d < 0$。
- 取 norm 有點類似像高中學的在複數平面上取複數與原點的距離。
- 注意到這題在後面是多麼重度地被使用上。

18.2 In an integral domain, show that a and b are associates if and only if $\langle a \rangle = \langle b \rangle$.

Proof. ($\Rightarrow$) If $b = ac$, then $b \in \langle a \rangle$ and $\langle b \rangle \subseteq \langle a \rangle$.

($\Leftarrow$) Suppose that $\langle a \rangle = \langle b \rangle$. If $a = 0$, then $b = 0 = a$. Suppose that $a \neq 0$. Then $a \in \langle b \rangle$ and $a = bq_1$ for some $q_1 \in R$. On the other hand, $b \in \langle a \rangle$ implies that $b = aq_2$ for some $q_2 \in R$. Therefore, $a = bq_1 = abq_2$ and $a(1 - bq_2) = 0$. ■

補充. 注意到, 這題用兩種不同的語言來描述同一件事。

18.8 Let D be a Euclidean domain with measure d. Prove that u is a unit in D if and only if $d(u) = d(1)$.

Proof. (⇒)

$$u = 1 \cdot u \Rightarrow d(u) = d(1)d(u) \Rightarrow d(1) \leq d(u).$$

On the other hand,

$$\begin{aligned} & u \text{ is a unit} \\ \Rightarrow\ & \text{there exists } u^{-1} \in D \text{ such that } uu^{-1} = 1 \\ \Rightarrow\ & d(u)d(u^{-1}) = d(uu^{-1}) = d(1) \\ \Rightarrow\ & d(u) \leq d(1). \end{aligned}$$

Therefore, $d(u) = d(1)$.

(⇐) By Division Algorithm,

$$1 = uq + r \text{ for some } q, r \in D, \text{ where } r = 0 \text{ or } d(r) < d(u) = d(1).$$

On the other hand, $d(r) = d(1 \cdot r) = d(1) \cdot d(r)$ implies that $d(1) \leq d(r)$. Thus, r must be 0 and $1 = uq$ and u is a unit. ■

18.9 Let D be a Euclidean domain with measure d. Show that if a and b are associates in D, then $d(a) = d(b)$.

Proof.

$$\begin{aligned} & a \text{ and } b \text{ are associates in } D \\ \Rightarrow\ & \langle a \rangle = \langle b \rangle \\ \Rightarrow\ & a = bq_1 \text{ and } b = aq_2 \text{ for some } q_1, q_2 \in D \\ \Rightarrow\ & d(a) = d(bq_1) = d(b)d(q_1) \text{ and } d(b) = d(a)d(q_2) \\ \Rightarrow\ & d(b) \leq d(a) \text{ and } d(a) \leq d(b) \\ \Rightarrow\ & d(a) = d(b). \end{aligned}$$

■

補充. 與 Exercise 18.2比較一下。

18.10 Let D be a principal ideal domain and let $p \in D$. Prove that $\langle p \rangle$ is a maximal ideal in D if and only if p is irreducible.

Proof.

$$\begin{array}{cl}
 & \text{Suppose that } 0 \neq \langle p\rangle \text{ is a maximal ideal and } p = ab \\
\Rightarrow & \langle p\rangle \subseteq \langle a\rangle \subseteq D \\
\overset{\overset{\langle p\rangle \text{ is maximal}}{\downarrow}}{\Rightarrow} & \langle a\rangle = \langle p\rangle \text{ or } \langle a\rangle = D \\
\text{If} & \langle a\rangle = \langle p\rangle \\
\Rightarrow & a = ps \text{ for some } s \in D \\
\Rightarrow & p = ab = psb \\
\Rightarrow & p(sb-1) = 0 \\
\overset{\overset{D \text{ is an I.D. and } p\neq 0}{\downarrow}}{\Rightarrow} & sb = 1 \\
\Rightarrow & b \text{ is a unit.} \\
\text{If} & \langle a\rangle = D \\
\Rightarrow & 1 \in D = \langle a\rangle \\
\Rightarrow & 1 = at \text{ for some } t \in D \\
\Rightarrow & a \text{ is a unit.}
\end{array}$$

Therefore, p is irreducible in D.

$$\begin{array}{cl}
 & \text{Suppose that } p \text{ is irreducible and } \langle p\rangle \subseteq I \lhd D \\
\overset{\overset{D \text{ is a P.I.D.}}{\downarrow}}{\Rightarrow} & I = \langle q\rangle \text{ and } \langle p\rangle \subseteq \langle q\rangle \subseteq D \\
\Rightarrow & p \in \langle q\rangle \text{ and } p = qr \text{ for some } r \in D \\
\overset{\overset{p \text{ is irreducible}}{\downarrow}}{\Rightarrow} & q \text{ is a unit or } r \text{ is a unit} \\
\text{If} & q \text{ is a unit} \\
\Rightarrow & \langle q\rangle = D \\
\text{If} & r \text{ is a unit} \\
\Rightarrow & q = pr^{-1} \\
\Rightarrow & q \in \langle p\rangle \\
\Rightarrow & \langle q\rangle = \langle p\rangle.
\end{array}$$

Therefore, $\langle p\rangle$ is a maximal ideal. ■

補充. 這題也要多加一個 $\langle p\rangle \neq 0$ 的條件。

18.12 Let D be a principal ideal domain. Show that every proper ideal of D is contained in a maximal ideal of D.

Proof. Suppose that D is a P.I.D. and $I = \langle a\rangle$ is a proper ideal of D. Since D is also a U.F.D., suppose that $a = ur_1r_2\cdots r_n$ for some irreducible elements $r_1, r_2, \ldots, r_n$ and a unit u. Then $I = \langle a\rangle \subseteq \langle r_1\rangle$ and $\langle r_1\rangle$ is a maximal ideal by Exercise 18.10. ■

補充. In fact, if R is a commutative with unity, then every proper ideal of R is contained in a maximal ideal of R, c.f. p.128, Theorem 2.18 in Hungerford's "Algebra". 這個定理不好證明, 要用到 Zorn's lemma。

18.13 In $\mathbb{Z}[\sqrt{-5}]$, show that 21 does not factor uniquely as a product of irreducibles.

Proof. $21 = (4+\sqrt{-5})(4-\sqrt{-5}) = 3\cdot 7$.

Suppose that $(4+\sqrt{-5}) = (a+b\sqrt{-5})(c+d\sqrt{-5})$. Then $21 = N(4+\sqrt{-5}) = N(a+b\sqrt{-5})N(c+d\sqrt{-5})$. If $N(a+b\sqrt{-5}) = 1$, then $a+b\sqrt{-5}$ is a unit by Exercise 18.1. If $N(a+b\sqrt{-5}) = 3$, then $a^2+5b^2 = 3$, which is impossible. If $N(a+b\sqrt{-5}) = 7$, then $a^2+5b^2 = 7$, which is impossible.

Suppose that $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$. Then $9 = N(3) = N(a+b\sqrt{-5})N(c+d\sqrt{-5})$. If $N(a+b\sqrt{-5}) = 1$, then $a+b\sqrt{-5}$ is a unit by Exercise 18.1. If $N(a+b\sqrt{-5}) = 3$, then $a^2+5b^2 = 3$, which is impossible.

Suppose that $7 = (a+b\sqrt{-5})(c+d\sqrt{-5})$. Then $49 = N(7) = N(a+b\sqrt{-5})N(c+d\sqrt{-5})$. If $N(a+b\sqrt{-5}) = 1$, then $a+b\sqrt{-5}$ is a unit by Exercise 18.1. If $N(a+b\sqrt{-5}) = 7$, then $a^2+5b^2 = 7$, which is impossible. ■

18.14 Show that $1-i$ is an irreducible in $\mathbb{Z}[i]$.

Proof. $N(1-i) = 2$ is a prime number and by Exercise 18.1. ■

重複 18.15 Show that $\mathbb{Z}[\sqrt{-6}]$ is not a unique factorization domain. (Hint: Factor 10 in two ways.) Why does this show that $\mathbb{Z}[\sqrt{-6}]$ is not a principal ideal domain?

Proof. $10 = (2+\sqrt{-6})(2-\sqrt{-6}) = 2\cdot 5$. You should show that $(2+\sqrt{-6}), (2-\sqrt{-6}), 2$ and 5 all are irreducibles as you did in Exercise 18.13. If $\mathbb{Z}[\sqrt{-6}]$ is a P.I.D., then $\mathbb{Z}[\sqrt{-6}]$ is a U.F.D.. ■

18.17 In $\mathbb{Z}[i]$, show that 3 is irreducible but 2 and 5 are not.

Proof. Suppose that $3 = xy$ and $x = a+bi$. Then $9 = N(3) = N(xy) = N(x)N(y)$. Without loss of generality, if $N(x) = 1$, then x is a unit by Exercise 18.1. If $N(x) = 3$, then $a^2+b^2 = 3$, which is impossible. Therefore, 3 is irreducible.

$2 = (1+i)(1-i)$ and $5 = (2+i)(2-i)$. $(1+i), (1-i), (2+i)$ and $(2-i)$ all are not unit in $\mathbb{Z}[i]$ by Exercise 18.32. ■

18.18* Prove that 7 is irreducible in $\mathbb{Z}[\sqrt{6}]$, even though $N(7)$ is not prime.

Proof. Suppose that $7 = (a-b\sqrt{6})(c-d\sqrt{6})$. Then $49 = N(7) = N(a+b\sqrt{6})N(c+d\sqrt{6})$. If $N(a+b\sqrt{6}) = 1$, then $a+b\sqrt{6}$ is a unit by Exercise 18.1.

$$\begin{array}{cl}
\text{If} & N(a+b\sqrt{6}) = 7 \\
\overset{\overset{49=N(a+b\sqrt{6})N(c+d\sqrt{6})}{\downarrow}}{\Rightarrow} & N(c+d\sqrt{6}) = 7 \\
\Rightarrow & |a^2-6b^2| = |c^2-6d^2| = 7 \\
\Rightarrow & a^2-6b^2, c^2-6d^2 \in \{7,-7\} \\
\Rightarrow & a^2+b^2 = 0 = c^2+d^2 \in \mathbb{Z}_7 \\
\overset{\overset{\forall x\in\mathbb{Z}_7,\ x^2\in\{0,1,2,4\}}{\downarrow}}{\Rightarrow} & a = b = c = d = 0 \in \mathbb{Z}_7 \\
\Rightarrow & 7 \mid (a-b\sqrt{6}) \text{ and } 7 \mid (c-d\sqrt{6}) \\
\Rightarrow & 49 \mid (a-b\sqrt{6})(c-d\sqrt{6}) = 7,\ \text{a contradiction.}
\end{array}$$

■

補充. 我們剛剛在 Exercise 18.1看過: If $N(x)$ is a prime, then x is irreducible. 反過來不一定成立, 這題就是一個例子。

重複 18.20 Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a principal ideal domain.

Proof. A P.I.D. must be a U.F.D.. So we show that $\mathbb{Z}[\sqrt{-3}]$ is not a U.F.D..

Consider $4 = (1+\sqrt{-3})(1-\sqrt{-3}) = 2 \cdot 2$. we show that $(1+\sqrt{-3}), (1-\sqrt{-3})$ and 2 all are irreducible. Then $\mathbb{Z}[\sqrt{-3}]$ is not a U.F.D..

Suppose that $1+\sqrt{-3} = (a+b\sqrt{-3})(c+d\sqrt{-3})$. Then $10 = N(1+\sqrt{-3}) = N(a+b\sqrt{-3})N(c+d\sqrt{-3})$.

If $N(a+b\sqrt{-3}) = 1$, then $a+b\sqrt{-3}$ is a unit by Exercise 18.1.

If $N(a+b\sqrt{-3}) = 2$, then $a^2+3b^2 = 2$, which is impossible.

If $N(a+b\sqrt{-3}) = 5$, then $N(c+d\sqrt{-3}) = 2$, which is impossible.

If $N(a+b\sqrt{-3}) = 10$, then $N(c+d\sqrt{-3}) = 1$ and $c+d\sqrt{-3}$ is a unit by Exercise 18.1.

Therefore, $1+\sqrt{-3}$ is irreducible. The proof of the irreducibility of $(1-\sqrt{-3})$ and 2 are similarly. ■

18.21 In $\mathbb{Z}[\sqrt{-5}]$, prove that $1+3\sqrt{-5}$ is irreducible but not prime.

Proof. **Irreducible:** Suppose that $1+3\sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5})$. Then $46 = N(1+3\sqrt{-5}) = N(a+b\sqrt{-5})N(c+d\sqrt{-5})$.

If $N(a+b\sqrt{-5}) = 1$, then $a+b\sqrt{-5}$ is a unit by Exercise 18.1.

If $N(a+b\sqrt{-5}) = 2$, then $a^2+5b^2 = 2$, which is impossible.

If $N(a+b\sqrt{-5}) = 23$, then $N(c+d\sqrt{-5}) = 2$, which is impossible.

If $N(a+b\sqrt{-5}) = 46$, then $N(c+d\sqrt{-5}) = 1$ and $c+d\sqrt{-5}$ is a unit by Exercise 18.1.

Therefore, $1+3\sqrt{-5}$ is irreducible.

Not Prime: We know that $46 = (1+3\sqrt{-5})(1-3\sqrt{-5})$ and $(1+3\sqrt{-5}) \mid 46 = 2 \cdot 23$.

If $(1+3\sqrt{-5}) \mid 2$, then $46 = N(1+3\sqrt{-5}) \mid N(2) = 4$, which is impossible.

If $(1+3\sqrt{-5}) \mid 23$, then $46 = N(1+3\sqrt{-5}) \mid N(23) = 23^2$, which is impossible.

Therefore, $1+3\sqrt{-5}$ is not a prime. ■

18.22 In $\mathbb{Z}[\sqrt{5}]$, prove that both 2 and $1+\sqrt{5}$ are irreducible but not prime.

Proof. **2 is irreducible:** Suppose that $2 = (a+b\sqrt{5})(c+d\sqrt{5})$. Then $4 = N(2) = N(a+b\sqrt{5})N(c+d\sqrt{5})$.

If $N(a+b\sqrt{5}) = 1$, then $a+b\sqrt{5}$ is a unit by Exercise 18.1.

If $N(a+b\sqrt{5}) = 2$, then $a^2-5b^2 = 2$. If such a and b exist, then $a^2 = 2 \in \mathbb{Z}_5$, which is impossible.

If $N(a+b\sqrt{5}) = 4$, then $N(c+d\sqrt{5}) = 1$ and $c+d\sqrt{5}$ is a unit by Exercise 18.1.

Therefore, 2 is irreducible.

$1+\sqrt{5}$ **is irreducible:** Similar to the above case because 2 and $1+\sqrt{5}$ have the same norm.

2 **is not prime:** Note that $2|4=(1+\sqrt{5})(1-\sqrt{5})$, but $2\nmid(1+\sqrt{5})$ and $2\nmid(1-\sqrt{5})$. For if $2\mid(1+\sqrt{5})$, then $(1+\sqrt{5})\in\langle 2\rangle=\{2s+2t\sqrt{5}\mid s,t\in\mathbb{Z}\}$, which is impossible.

$1+\sqrt{5}$ **is not prime:** Note that $(1+\sqrt{5})\mid 4=2\cdot 2$, but $(1+\sqrt{5})\nmid 2$. For if $(1+\sqrt{5})\mid 2$, then $2=(1+\sqrt{5})y$ and $4=N(2)=N(1+\sqrt{5})N(y)=4N(y)$. It follows that $N(y)=1$ and y is a unit by Exercise 18.1. Thus, $1+\sqrt{5}=2y^{-1}$ and $2\mid(1+\sqrt{5})$. Which is impossible. ■

18.23 Prove that $\mathbb{Z}[\sqrt{5}]$ is not a unique factorization domain.

Proof. [**方法一**] Consider $4=2\cdot 2=(-1)(1+\sqrt{5})(1-\sqrt{5})$. 2 and $1\pm\sqrt{5}$ all are irreducible by Exercise 18.22. Thus, $\mathbb{Z}[\sqrt{5}]$ is not a U.F.D..

[**方法二**] If $\mathbb{Z}[\sqrt{5}]$ is a U.F.D., then an irreducible element must be a prime element by Exercise 18.43. But by Exercise 18.22, 2 is an example which is an irreducible element but not prime. ■

18.24 Let F be a field. Show that in $F[x]$ a prime ideal is a maximal ideal.

Proof. Let $P\neq 0$ be a prime ideal. Since $F[x]$ is a P.I.D., we can write $P=\langle p\rangle$ for some $0\neq p\in F[x]$.

Claim: p **is a prime.**

$$\begin{aligned}
&\text{If} && p\mid ab\\
&\Rightarrow && ab\in\langle p\rangle=P\\
&\Rightarrow && a\in P=\langle p\rangle \text{ or } b\in P=\langle p\rangle\\
&\Rightarrow && p\mid a \text{ or } p\mid b\\
&\Rightarrow && p \text{ is a prime element.}
\end{aligned}$$

Claim: p is a prime.

$$\begin{array}{cl}
\text{Suppose} & P \subseteq I \lhd F[x] \\
\overset{\substack{F[x] \text{ is a P.I.D.} \\ \downarrow}}{\Rightarrow} & \langle p\rangle \subseteq \langle i\rangle \lhd F[x] \\
\Rightarrow & p \in \langle i\rangle \\
\Rightarrow & p = ij \text{ for some } j \in F[x] \\
\Rightarrow & p \mid ij \\
\overset{\substack{p \text{ is prime} \\ \downarrow}}{\Rightarrow} & p \mid i \text{ or } p \mid j. \\
\text{If} & p \mid i \\
\Rightarrow & i \in \langle p\rangle \\
\Rightarrow & I = \langle i\rangle \subseteq \langle p\rangle = P \\
\Rightarrow & I = P. \\
\text{If} & p \mid j \\
\Rightarrow & j = ps \\
\Rightarrow & p = ij = ips \\
\Rightarrow & p(is-1) = 0 \\
\overset{\substack{p\neq 0 \\ \downarrow}}{\Rightarrow} & is - 1 = 0 \\
\Rightarrow & i \text{ is a unit} \\
\Rightarrow & I = \langle i\rangle = F[x].
\end{array}$$

■

補充. 這題題目應該要多加一個“nonzeor”的條件。例如在 P.I.D. $\mathbb{Z}$ 當中, 0 是一個 prime ideal, 但不是一個 maximal ideal。

18.31 Prove or disprove that if D is a principal ideal domain, then $D[x]$ is a principal ideal domain.

Proof. $\mathbb{Z}$ is a P.I.D., but $\mathbb{Z}[x]$ is not a P.I.D.. ■

18.32 Determine the units in $\mathbb{Z}[i]$.

Proof. If $a+bi \in \mathbb{Z}[i]$ and $a+bi$ is a unit, then by Exercise 18.1, $N(a+bi) = a^2+b^2 = 1$ and $a+bi \in \{1,-1,i,-i\}$. On the other hand, $1,-1,i$ and $-i$ all are units. ■

18.34 Show that $3x^2+4x+3 \in \mathbb{Z}_5[x]$ factors as $(3x+2)(x+4)$ and $(4x+1)(2x+3)$. Explain why this does not contradict the corollary of Theorem 18.3.

Proof. $2(x+4) = (2x+3)$ and 2 is a unit in $\mathbb{Z}_5$. $3(3x+2) = (4x+1)$ and 3 is a unit in $\mathbb{Z}_5$. $(x+4)$ and $(2x+3)$ are associates. $(3x+2)$ and $(4x+1)$ are associates. Which does not contrary to the uniqueness of the factorization in the U.F.D. $\mathbb{Z}_5[x]$.

Proof directly. Note that $4 = 2\cdot 2 = (1+\sqrt{5})(-1+\sqrt{5})$. We show that $2, 1+\sqrt{5}$ and $-1+\sqrt{5}$ all are irreducible. Then the factorization of 4 is not unique and we are done.

Suppose that $1+\sqrt{5} = (a+b\sqrt{5})(c+d\sqrt{5})$. Then $4 = N(1+\sqrt{5}) = N(a+b\sqrt{5})\cdot N(c+d\sqrt{5})$. If $N(a+b\sqrt{5}) = 1$, then $a+b\sqrt{5}$ is a unit. If $N(a+b\sqrt{5}) = 2$, then $a^2-5b^2 = 2$. If such a and b exist, then $a^2 = 2 \in \mathbb{Z}_5$, which is impossible because for all $c \in \mathbb{Z}_5$, $c^2 \neq 2$.

Similarly, 2 and $-1+\sqrt{5}$ both are irreducible by the same disscusion as above. ∎

18.35 Let D be a principal ideal domain and p an irreducible element of D. Prove that $D/\langle p\rangle$ is a field.

Proof. Since p is irreducible in the P.I.D. D, by Exercise 18.10, $\langle p\rangle$ is a maximal ideal. It follows that $D/\langle p\rangle$ is a field. ∎

18.36 Show that an integral domain with the property that every strictly decreasing chain of ideals $I_1 \supset I_2 \supset \cdots$ must be finite in length is a field.

Proof. For any $0 \neq r \in R$, consider the chain of ideals $\langle r\rangle \supseteq \langle r^2\rangle \supseteq \cdots$. Since this chain of ideals is finite length, we have

$$\langle r\rangle \supseteq \langle r^2\rangle \supseteq \cdots \supseteq \langle r^n\rangle = \langle r^{n+1}\rangle = \cdots$$

for some $n \in \mathbb{N}^+$. It follows that

$$\begin{aligned}
& \langle r^n\rangle \subseteq \langle r^{n+1}\rangle \\
\Rightarrow\ & r^n \in \langle r^{n+1}\rangle \\
\Rightarrow\ & r^n = r^{n+1}s \text{ for some } s \in R \\
\Rightarrow\ & r^n(rs-1) = 0 \\
\overset{\overset{r\neq 0}{\downarrow}}{\Rightarrow}\ & rs-1 = 0 \\
\Rightarrow\ & r \text{ is a unit.}
\end{aligned}$$

∎

補充. 你不妨先想想反例, 也就是不滿足 descending chain condition 且不是 field 的例子。$\mathbb{Z}$ 就是一個最好的例子, $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \cdots$, 而且這個例子也給了我們證明這題的靈感。

18.37 An ideal A of a commutative ring R with unity is said to be finitely generated if there exist elements $a_1, a_2, \dots, a_n$ of A such that $A = \langle a_1, a_2, \dots, a_n\rangle$. An integral domain R is said to satisfy the ascending chain condition if every strictly incerasing chain of ideals $I_1 \subset I_2 \subset \cdots$ must be finite in length. Show that an integral domain R satisfies the ascending chain condition if and only if every ideal of R is finitely generated.

Proof. ($\Rightarrow$) If I is an ideal in R which is not finitely generated. Pick $a_1 \in I$. Then $\langle a_1\rangle \neq I$ because I is not finitely generated. We pick $a_2 \in I$ but $a_2 \notin \langle a_1\rangle$. Then we have $\langle a_1\rangle \subset \langle a_1, a_2\rangle$ but $\langle a_1\rangle \neq \langle a_1, a_2\rangle \neq I$. Continuing this process, we get a infinite strictly ascending chain of ideals

$$\langle a_1\rangle \subset \langle a_1, a_2\rangle \subset \langle a_1, a_2, a_3\rangle \subset \cdots.$$

Contrary to the hypothesis.

($\Leftarrow$) For any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, consider the ideal $\langle \bigcup_{j=1}^{\infty} I_j \rangle$. Since $\langle \bigcup_{j=1}^{\infty} I_j \rangle$ is finitely generated, suppose $\langle \bigcup_{j=1}^{\infty} I_j \rangle = \langle a_1, a_2, ..., a_n \rangle$. Suppose that $a_1 \in I_{k_1}$, $a_2 \in I_{k_2}$, ..., $a_n \in I_{k_n}$. Take $k = \max(k_1, k_2, ..., k_n)$. Then $I_s = I_{s+1}$ for all $s \geq k$ and the chain of ideal $I_1 \subseteq I_2 \subseteq \cdots$ is finite length

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_k = I_{k+1} = \cdots.$$

■

18.42 Let $R = \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$ (the collection of all sequences of integers under componentwise addition and multiplication). Show that R has ideals $I_1, I_2, I_3, ...$ with the property that $I_1 \subset I_2 \subset I_3 \subset \cdots$. (Thus R does not have the ascending chain condition.)

Proof. $I_n = \langle \{e_1, e_2, ..., e_n\} \rangle$, where $e_i \in R$ has 1 in the ith position and 0 elsewhere. ■

18.43 Prove that in a unique factorization domain, an element is irreducible if and only if it is prime.

Proof. ($\Leftarrow$) Theorem 18.1.

($\Rightarrow$) Let c be an irreducible element in a U.F.D. D. Suppose $c \mid ab$. Since D is a U.F.D., we factor a and b into the product of irreducible elements.

$$\begin{aligned} a &= ur_1r_2\cdots r_n. \\ b &= vr_{n+1}r_{n+2}\cdots r_{n+m}. \end{aligned}$$

Then

$$c = ab = uvr_1r_2\cdots r_{n+m}.$$

Since the factorization is unique and c is an irreducible element, c must be associates to r_i for some $i \in \{1, 2, ..., n+m\}$. If $i \in \{1, 2, ..., n\}$, then $c = r_iw$ for some unit w and $a = w^{-1}ur_1r_2\cdots(wr_i)\cdots r_n$ and $c \mid a$. Similarly, If $i \in \{n+1, n+2, ..., n+m\}$, then $c \mid b$. Therefore, c is a prime element. ■

補充. 與 p.330, Theorem 18.2比較一下, 在 Theorem 18.2是 P.I.D., 在這題是 U.F.D.。

18.61 Let $I_0 = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$. For any positive integer n, show that there exists a sequence of strictly increasing ideals such that $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n \subset \mathbb{Z}[x]$.

Proof.

$$I_0 = \langle x \rangle \subset \langle x, 2^n \rangle \subset \langle x, 2^{n-1} \rangle \subset \langle \cdots \rangle \subset \langle x, 2 \rangle.$$

■

19 Chapter 19

19.22 If V is a vector space of dimension n over the field $\mathbb{Z}_p$, how many elements are in V?

Proof. Suppose that $\{v_1, v_2, ..., v_n\}$ is a basis for V over $\mathbb{Z}_p$. Then $V = \{a_1v_1 + a_2v_2 + \cdots + a_nv_n \mid a_i \in \mathbb{Z}_p\}$. ■

補充 19.A Let F be a field, $F[x]$ the polynomial ring in x over F, and $f(x) \neq 0$ in $F[x]$. Consider $V = F[x]/J$ as a vector space over F, where J is the ideal of $F[x]$ generated by $f(x)$. Prove that

$$\dim_F V = \deg f(x).$$

Proof. View $F[x]/J$ as an abelian group under addition. Define a scalar multipliation $\cdot : F \times F[x]/J \to F[x]/J$ by

$$\lambda \cdot (f(x) + J) = (\lambda f(x)) + J.$$

Then $F[x]/J$ is a vector space over F. If $f(x) = a_nx^n + \cdots + a_1x + a_0$, then $\{1 + J, x + J, x^2 + J, ..., x^{n-1} + J\}$ is a basis for $F[x]/J$ over F. ■

20 Chapter 20

題組 Let $f(x) \in F[x]$ be the minimal polynomial of α over F and $\deg f(x) = n$. Then $F(\alpha) = \{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \mid a_i \in F\}$

20.7, 20.1, 20.8, 20.9, 20.10, 20.37

題組 If $F \leq L \leq E$ and $\alpha \in L$, then $F(\alpha) \leq L$

20.2, 補充,20.6, 20.19

題組 Splitting field

20.29, 20.25, 20.34, 20.16

下面是一些解決這類題目的技巧:

- 利用 Theorem 20.7, 20.8確認 $f(x)$ has no multiple zeros 這麼一來找 root 時, 找過的就不用再找兩次。
- 列出 $\alpha^2, \alpha^3, \alpha^4, \alpha^5, ...$, 之後計算時方便查閱。
- 在 $\mathbb{Z}_p$ 中, $(a+b)^p = a^p + b^p$。
- 如果是 2 次 polynomial 而且已經知道其中一個 root, 就用長除法, 例如 Exercise 20.29; 如果是 3 次或 3 次以上, 就一個一個元素代進去算, 看看是不是 root, 只差最後一個 root 時, 再用長除法。

題組 Criterion for Multiple Zeros

20.30, 20.31, 20.32, 20.33, 20.40

題組 Splitting field

20.13, 20.26, 20.3, 20.4, 20.5, 20.38

20.1 Describe the elements of $\mathbb{Q}(\sqrt[3]{5})$.

Proof. $\{a(\sqrt[3]{5})^2 + b\sqrt[3]{5} + c \mid a, b, c \in \mathbb{Q}\}$. ■

20.2 Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Proof. $\sqrt{3} - \sqrt{2} = \frac{1}{\sqrt{2}+\sqrt{3}} = (\sqrt{2} + \sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

$\sqrt{3} = \frac{(\frac{1}{\sqrt{2}+\sqrt{3}})+(\sqrt{3}+\sqrt{2})}{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

$\sqrt{2} = \frac{(\sqrt{3}+\sqrt{2})-(\frac{1}{\sqrt{2}+\sqrt{3}})}{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Therefore, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. ■

20.3 Find the splitting field of $x^3 - 1$ over $\mathbb{Q}$. Express your answer in the form $\mathbb{Q}(a)$.

Proof. $\mathbb{Q}(\xi_3)$, where $\xi_3 = e^{\frac{2\pi}{3}i} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$. $(x^3 - 1) = (x - 1)(x - \xi_3)(x - \xi_3^2)$.
Another expression is $\mathbb{Q}(\sqrt{3}i)$,

$$x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)\left(x - (\frac{-1 + \sqrt{3}i}{2})\right)\left(x - (\frac{-1 - \sqrt{3}i}{2})\right).$$

■

20.4 Find the splitting field of $x^4 + 1$ over $\mathbb{Q}$.

Proof.

$$\begin{aligned} x^4 + 1 \quad &= \quad (x^2 - i)(x^2 + i) \\ &= \quad \left(x + (\frac{\sqrt{2} + \sqrt{2}i}{2})\right)\left(x - (\frac{\sqrt{2} + \sqrt{2}i}{2})\right)\left(x + (\frac{\sqrt{2} - \sqrt{2}i}{2})\right)\left(x - (\frac{\sqrt{2} - \sqrt{2}i}{2})\right) \\ &\overset{\overset{\alpha=\frac{\sqrt{2}+\sqrt{2}i}{2}}{\downarrow}}{=} \quad (x + \alpha)(x - \alpha)(x + \overline{\alpha})(x - \overline{\alpha}). \end{aligned}$$

Note that $\alpha^2 = i$ and $2(\alpha + \overline{\alpha}) = \sqrt{2}$. So the splitting field of $x^4 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, -\alpha, \overline{\alpha}, -\overline{\alpha}) = \mathbb{Q}(\sqrt{2}, i)$. ■

20.5 Find the splitting field of $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ over $\mathbb{Q}$.

Proof. $\mathbb{Q}(\sqrt{3}i)$. ■

20.6 Let $a, b \in \mathbb{R}$ with $b \neq 0$. Show that $\mathbb{R}(a + bi) = \mathbb{C}$.

Proof. ■

20.7 Find a polynomial $p(x)$ in $\mathbb{Q}[x]$ such that $\mathbb{Q}(\sqrt{1 + \sqrt{5}})$ is ring-isomorphic to $\mathbb{Q}[x]/\langle p(x)\rangle$.

Proof. Let $\alpha = \sqrt{1+\sqrt{5}}$.

$$\begin{array}{rcl} \alpha &=& \sqrt{1+\sqrt{5}} \\ \alpha^2 &=& 1+\sqrt{5} \\ \alpha^2 - 1 &=& \sqrt{5} \\ (\alpha^2-1)^2 &=& 5 \\ \alpha^4 - 2\alpha^2 + 1 &=& 5 \\ \alpha^4 - 2\alpha^2 - 4 &=& 0. \end{array}$$

Let $p(x) = x^4 - 2x^2 - 4$. Then $p(\sqrt{1+\sqrt{5}}) = 0$. We show that $p(x)$ is monic and irreducible over $\mathbb{Q}$. Then $p(x)$ is the minimal polynomial of $\sqrt{1+\sqrt{5}}$ over $\mathbb{Q}$ and $\mathbb{Q}[x]/\langle p(x)\rangle \cong \mathbb{Q}(\sqrt{1+\sqrt{5}})$.

There are four methods that you can try.
(i) Eisenstein's Criterion.
(ii) If $f(x+a)$ is irreducible over $\mathbb{Q}$, then $f(x)$ is irreducible over $\mathbb{Q}$.
(iii) Mod p Irreducibility Test.
(iv) Reducibility over $\mathbb{Q}$ Implies Reducibility over $\mathbb{Z}$.

I use the method (iv). Since $p(x)$ has no roots in $\mathbb{Q}$, $p(x)$ has no linear factor in $\mathbb{Q}[x]$.

If $p(x)$ is reducible in $\mathbb{Q}[x]$, then by (iv), $p(x)$ is reducible over $\mathbb{Z}$. Since $p(x)$ is monic, suppose that $p(x) = (x^2+ax+b)(x^2+cx+d)$, where $a, b, c, d \in \mathbb{Z}$. Then

$$p(x) = x^4 - 2x^2 - 4 = x^4 + (a+c)x^3 + (b+ac+d)x^2 + (bc+ad)x + bd.$$

Compare the coefficients,

$$\begin{array}{ccccc} x^4 & +(a+c)x^3 & +(b+ac+d)x^2 & +(bc+ad)x & +bd \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ x^4 & +0x^3 & -2x^2 & +0x & -4 \end{array}$$

We have

$$\begin{array}{rcl} a+c &=& 0 \\ b+ac+d &=& -2 \\ bc+ad &=& 0 \\ bd &=& -4. \end{array}$$

By $a+c=0$, we have $c=-a$. Then $0 = bc+ad = -ab+ad = a(d-b)$. If $b-d=0$, then $bd = b^2 = -4$, it is impossible. Hence, $a=0$. Then $c=0$ and $b+ac+d = b+d = -2$ and $bd=-4$. It follows that $b(-2-b) = -4$ and $b = -1 \pm \sqrt{5}$, it is impossible. There are no such a, b, c and d in $\mathbb{Z}$ satisfy these equations and $p(x)$ is irreducible over $\mathbb{Z}$ and $\mathbb{Q}$. ■

20.8 Let $F = \mathbb{Z}_2$ and let $f(x) = x^3 + x + 1 \in F[x]$. Suppose that a is a zero of $f(x)$ in some extension of F. How many elements does $F(a)$ have? Express each member of $F(a)$ in terms of a. Write out a complete multiplication table or $F(a)$.

Proof. **Lemma.** Let $f(x) \in F[x]$ and $\deg f(x) \in \{2,3\}$. Then $f(x)$ is irreducible over F if and only if $f(x)$ has no roots in F.

Since $f(x)$ has no root in $\mathbb{Z}_2$ and $\deg f(x) = 3$, $f(x)$ is irreducible over $\mathbb{Z}_2$. Then $\mathbb{Z}_2[x]/\langle f(x)\rangle \cong \mathbb{Z}_2(a) = \{a_2a^2 + a_1a + a_0 \mid a_2, a_1, a_0 \in \mathbb{Z}_2\}$ and $\mathbb{Z}_2(a)$ is a finite field of order $2^3 = 8$. Note that $a^3 = -a - 1 = a + 1$. The multiplication table of $\mathbb{Z}_2(a)$ is

	0	1	a	$a+1$	a^2	a^2+1	a^2+a	a^2+a+1
0	0	0	0	0	0	0	0	0
1	0	1	a	$a+1$	a^2	a^2+1	a^2+a	a^2+a+1
a	0	a	a^2	a^2+a	$a+1$	1	a^2+a+1	a^2+1
$a+1$	0	$a+1$	a^2+a	a^2+1	a^2+a+1	a^2	1	a
a^2	0	a^2	$a+1$	a^2+a+1	a^2+a	a	a^2+1	1
a^2+1	0	a^2+1	1	a^2	a	a^2+a+1	$a+1$	a^2+a
a^2+a	0	a^2+a	a^2+a+1	1	a^2+1	$a+1$	a	a^2
a^2+a+1	0	a^2+a+1	a^2+1	a	1	a^2+a	a^2	$a+1$

■

20.9 Let $F(a)$ be the field described in Exercise 8. Express each of a^5, a^{-2}, and a^{100} in the form $c_2a^2 + c_1a + c_0$.

Proof. $a^5 = a^3 \cdot a^2 = (a+1)\cdot a^2 = a^3 + a^2 = (a+1) + a^2 = a^2 + a + 1$.

Since $\mathbb{Z}_2(a)$ is a finite field of order 8, $\mathbb{Z}_2(a) - \{0\}$ is a finite multiplicative group of order 7. By Lagrange's Theorem, the multiplicative order of a nonidentity element in $\mathbb{Z}_2(a) - \{0\}$ is 7. Therefore, $a^7 = 1$.

Then $a^{-2} = a^{-2}\cdot 1 = a^{-2}\cdot a^7 = a^5$ and $a^{100} = (a^7)^{14}\cdot a^2 = a^2$. ■

20.10 Let $F(a)$ be the field described in Exercise 8. Show that a^2 and $a^2 + a$ are zeros of $x^3 + x + 1$.

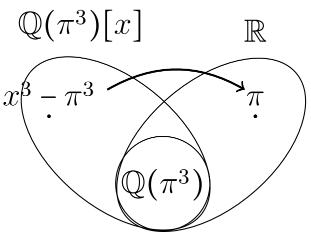
Proof. ■

20.11 Describe the elements in $\mathbb{Q}(\pi)$.

Proof. $\left\{\frac{f(\pi)}{g(\pi)} \mid f(x) \in \mathbb{Q}[x], g(x) \neq 0 \in \mathbb{Q}[x]\right\}$. ■

20.12 Let $F = \mathbb{Q}(\pi^3)$. Find a basis for $F(\pi)$ over F.

Proof. Note that π is algebraic over $\mathbb{Q}(\pi^3)$ with minimal polynomial $x^3 - \pi^3$ (why?). Thus, $\mathbb{Q}(\pi^3)[x]/\langle x^3 - \pi^3\rangle \cong \mathbb{Q}(\pi^3)(\pi)$ and $\{1, \pi, \pi^2\}$ is a basis for $\mathbb{Q}(\pi^3)(\pi)$ over $\mathbb{Q}(\pi^3)$.



■

20.13 Write $x^7 - x$ as a product of linear factors over $\mathbb{Z}_3$. Do the same for $x^{10} - x$.

Proof.

$$\begin{aligned}
x^7 - x &= x(x^6 - 1) \\
&= x(x^3 - 1)(x^3 + 1) \\
&= x(x - 1)(x^2 - x + 1)(x - 1)(x^2 + x + 1) \\
&= x(x - 1)(x^2 + 2x + 1)(x - 1)(x^2 - 2x + 1) \\
&= x(x - 1)(x + 1)^2(x - 1)(x - 1)^2 \\
&= x(x - 1)^4(x + 1)^2.
\end{aligned}$$

$$\begin{aligned}
x^{10} - x &= x(x^9 - 1) \\
&= x(x^3 - 1)(x^6 + x^3 + 1) \\
&= x(x^3 - 1)(x^6 - 2x^3 + 1) \\
&= x(x^3 - 1)^3 \\
&= x[(x - 1)(x^2 + x + 1)]^3 \\
&= x[(x - 1)(x^2 - 2x + 1)]^3 \\
&= x[(x - 1)(x - 1)^2]^3 \\
&= x(x - 1)^9.
\end{aligned}$$

■

20.14 Find all ring automorphisms of $\mathbb{Q}(\sqrt[3]{5})$.

Proof. The minimal polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$ is $f(x) = x^3 - 5$. Let E be the splitting field for $f(x)$ over $\mathbb{Q}$. Then $f(x) = (x^3 - 5) = (x - \sqrt[3]{5})(x - \sqrt[3]{5}\xi_3)(x - \sqrt[3]{5}\xi_3^2) \in E[x]$, where $\xi_3 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$.

If θ is an automorhphism on $\mathbb{Q}(\sqrt[3]{5})$ and $r \in \mathbb{Q}$, then $\theta(r) = r$.

Note that $f(\theta(\sqrt[3]{5})) = \theta(f(\sqrt[3]{5})) = \theta(0) = 0$. That is, $\theta(\sqrt[3]{5})$ is also a root of $f(x)$. Thus, $\theta(\sqrt[3]{5}) \in \{\sqrt[3]{5}, \sqrt[3]{5}\xi_3, \sqrt[3]{5}\xi_3^2\}$. But $\sqrt[3]{5}\xi_3$ and $\sqrt[3]{5}\xi_3^2$ are not in $\mathbb{Q}(\sqrt[3]{5})$. Therefore, $\theta(\sqrt[3]{5}) = \sqrt[3]{5}$. θ must be the identity mapping. ■

20.15* Let F be a field of characteristic p and let $f(x) = x^p - a \in F[x]$. Show that $f(x)$ is irreducible over F or $f(x)$ splits in F.

Proof. [**方法一**] Let E be the splitting field of $f(x)$ over F and let r be a root of $f(x)$ in E. Then $f(r) = r^p - a = 0$ and $r^p = a$ and $f(x) = x^p - a = x^p - r^p = (x - r)^p$ by char $F = p$ and Freshman's Dream.

Case I: If $r \in F$, then $f(x) = (x - r)^p$ splits in $F[x]$.

Case II: If $r \notin F$. Since $F[x]$ is a UFD and $f(x)$ is monic, suppose that $f(x) = g_1(x)g_2(x)\cdots g_n(x)$, where $g_i(x)$ is irreducible and monic in $F[x]$ for each $i = 1, 2, ..., n$.

In addition, $\deg g_i(x) \geq 2$ for each $i = 1, 2, ..., n$. For if $\deg g_i(x) = 1$, then $g_i(x) = (x - s) \in F[x]$ and $s \in F$ is a root of $f(x)$. Which is the Case I.

Then we have $f(x) = g_1(x)g_2(x)\cdots g_n(x) = (x - r)^p$. For each $i = 1, 2, ..., n$, since $\deg g_i(x) \geq 2$, it follows that $g_i(x)$ has multiple root in E. Recall that $g_i(x)$ is irreducible over F, by Theorem 20.6, $g_i(x) = h_i(x^p)$ for some $h_i(x) \in F[x]$. Then $f(x) = x^p - a = h_1(x^p)h_2(x^p)\cdots h_n(x^p)$. Compare the degree of this equation, it must be $\deg h_1(x) = 1$ and $h_2(x), h_3(x), ..., h_n(x)$ all are constant. It follows that $g_2(x) = g_3(x) = \cdots = g_n(x) = 1$ and $g_1(x) = f(x)$. Therefore, $f(x) = g_1(x)$ is irreducible over F.

[方法二] Consider the splitting field E for $f(x)$ over F. By Theorem 20.9, there are three possible factorizations of $f(x)$ in $E[x]$.
(i) $f(x) = (x - r_1)(x - r_2)\cdots(x - r_p)$, where $r_i \neq r_j$ if $i \neq j$.
(ii) $f(x) = (x - r_1)^s(x - r_2)^s\cdots(x - r_t)^s$, where $s \geq 2$, $t \geq 2$.
(iii) $f(x) = (x - r)^p$.
Since $f'(x) = 0$, we have $\gcd(f(x), f'(x)) = f(x) \neq 1$, the case (i) is impossible by Theorem 20.5. Since p is a prime, the case (ii) is impossible because $p = \deg f(x) = s \cdot t$. The remaining possible is $f(x) = (x - r)^p \in E[x]$.

Since r is a root of $f(x)$ over F, the minimal polynomial $m_r(x)$ of r over F divides $f(x) = x^p - a$.

$$\begin{array}{ll}
 & m_r(x) \mid f(x) = (x^p - a) \text{ in } F[x] \\
\Rightarrow & m_r(x) \mid f(x) = (x - r)^p \text{ in } E[x] \\
\Rightarrow & m_r(x) = (x - r)^q \text{ in } E[x] \text{ for some } q \leq p \\
\text{If} & q = p \\
\Rightarrow & f(x) = m_r(x) \in F[x] \text{ is irreducible over } F \\
\text{If} & q < p \\
\Rightarrow & m_r(x) = (x - r)^q = \binom{q}{0}x^q + \underline{\binom{q}{1}(-r)}x^{q-1} + \binom{q}{2}(-r)^2x^{q-2}\cdots + \binom{q}{q-1}(-r)^{q-1}x + \binom{q}{q}(-r)^q \in F[x \\
\Rightarrow & r \in F \\
\Rightarrow & f(x) = (x - r)^p \text{ splits in } F[x].
\end{array}$$

■

補充. http://math.stackexchange.com/questions/760538/let-f-be-a-field-of-characte

20.16* Suppose that β is a zero of $f(x) = x^4 + x + 1$ in some extension field E of $\mathbb{Z}_2$. Write $f(x)$ as a product of linear factors in $E[x]$.

Proof. $f(x) = (x - \beta)[x - (\beta + 1)](x - \beta^2)[x - (\beta^2 + 1)]$. ■

補充. If $f(x)$ is irreducible over $\mathbb{Z}_p$ and a is a root of $f(x)$ in the extension field $\mathbb{Z}_p(a) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$ of $\mathbb{Z}_p$, then a^p, a^{p^2}, a^{p^3}, ... are also roots of $f(x)$.

Proof. Since $\mathbb{Z}_p - \{0\}$ is a finite group under multiplication, by Lagrange's Theorem, for all $g \in \mathbb{Z}_p - \{0\}$, $g^{p-1} = 1$. Thus, $g^p = g$ and $g^{p^s} = \overbrace{((g^p)^p)^{\cdots})^p}^{s \text{ times}} = g$.

In addition, recall that if $\operatorname{char} K = p$, then $(u + v)^p = u^p + v^p$ for every $u, v \in K$.

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $f(a) = 0$, then

$$\begin{aligned}
f(a^{p^s}) &= a_n(a^{p^s})^n + a_{n-1}(a^{p^s})^{n-1} + \cdots + a_1 a^{p^s} + a_0 \\
&\overset{\overset{a_i\in\mathbb{Z}_p}{\downarrow}}{=} a_n^{p^s}(a^{p^s})^n + a_{n-1}^{p^s}(a^{p^s})^{n-1} + \cdots + a_1^{p^s} a^{p^s} + a_0^{p^s} \\
&= a_n^{p^s}(a^n)^{p^s} + a_{n-1}^{p^s}(a^{n-1})^{p^s} + \cdots + a_1^{p^s} a^{p^s} + a_0^{p^s} \\
&\overset{\overset{a_i,\ a\in K\supseteq\mathbb{Z}_p}{\downarrow}}{=} (a_n a^n + a_{n-1}a^{n-1} + \cdots + a_1 a + a_0)^{p^s} \\
&= 0
\end{aligned}$$

20.17 Find a, b, c in $\mathbb{Q}$ such that $(1 + \sqrt[3]{4})/(2 - \sqrt[3]{2}) = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Note that such a, b, c exist, since $(1 + \sqrt[3]{4})/(2 - \sqrt[3]{2}) \in \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.

20.18 Express $(3 + 4\sqrt{2})^{-1}$ in the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$.

Proof. $\frac{1}{3+4\sqrt{2}} = \frac{(4\sqrt{2}-3)}{(4\sqrt{2}+3)(4\sqrt{2}-3)} = \frac{4\sqrt{2}-3}{32-9} = \frac{-3}{23} + \frac{4}{23}\sqrt{2}$. ■

20.19 Show that $\mathbb{Q}(4 - i) = \mathbb{Q}(1 + i)$, where $i = \sqrt{-1}$.

20.20 Let F be a field, and let a and b belong to F with $a \neq 0$. If c belongs to some extension of F, prove th $F(c) = F(ac + b)$. (F "absorbs" its own elements.)

20.21 Let $f(x) \in F[x]$ and let $a \in F$. Show that $f(x)$ and $f(x+a)$ have the same splitting field over F.

Proof. Suppose that $f(x) = (x-c_1)^{r_1}(x-c_2)^{r_2}\cdots(x-c_s)^{r_s}$ in $E[x]$ for some extension field E of F. Then $f(x+a) = (x+a-c_1)^{r_1}(x+a-c_2)^{r_2}\cdots(x+a-c_s)^{r_s}$ splits in $E[x]$. Conversely, suppose that $f(x+a) = (x-c_1)^{r_1}(x-c_2)^{r_2}\cdots(x-c_s)^{r_s}$ in $E[x]$ for some extension field E of F. Then $f(x) = (x-a-c_1)^{r_1}(x-a-c_2)^{r_2}\cdots(x-a-c_s)^{r_s}$ splits in $E[x]$. ■

20.22 Recall that two polynomial $f(x)$ and $g(x)$ from $F[x]$ are said to be relatively prime if there is no polynomial of positive degree in $F[x]$ that divides both $f(x)$ and $g(x)$. Show that if $f(x)$ and $g(x)$ are relatively prime in $F[x]$, they are relatively prime in $K[x]$, where K is any extension of F.

Proof. Consider the principal ideals $\langle f(x)\rangle$ and $\langle g(x)\rangle$ generated by $f(x)$ and $g(x)$, respectively. Recall that the sum of two ideals I and J is defined by

$$I + J = \{i + j \mid i \in I, j \in J\}.$$

Which is also an ideal. Since $F[x]$ is a P.I.D., $\langle f(x)\rangle + \langle g(x)\rangle = \langle h(x)\rangle$. We have that

$$\gcd(f(x), g(x)) = h(x) \Leftrightarrow \langle f(x)\rangle + \langle g(x)\rangle = \langle h(x)\rangle, \text{ where } h(x) \text{ is monic.}$$

Therefore,

$$\begin{array}{cl}
 & \gcd(f(x), g(x)) = 1 \text{ in } F[x] \\
\Rightarrow & \langle f(x)\rangle + \langle g(x)\rangle = \langle 1\rangle \text{ in } F[x] \\
\Rightarrow & \text{there exists } a(x), b(x) \in F[x] \text{ such that } f(x)a(x) + g(x)b(x) = 1 \in F[x] \\
\overset{\overset{F\leq K}{\downarrow}}{\Rightarrow} & \text{there exists } a(x), b(x) \in K[x] \text{ such that } f(x)a(x) + g(x)b(x) = 1 \in K[x] \\
\Rightarrow & \langle f(x)\rangle + \langle g(x)\rangle = \langle 1\rangle \text{ in } K[x] \\
\Rightarrow & \gcd(f(x), g(x)) = 1 \text{ in } K[x]
\end{array}$$

Another method see p.225 in Herstein's Algebra. ■

20.23 Determine all of the subfields of $\mathbb{Q}(\sqrt{2})$.

Proof. Suppose that F is a subfield of $\mathbb{Q}(\sqrt{2})$. Consider the tower of fields

$$\overbrace{\mathbb{Q} \leq F \leq \mathbb{Q}(\sqrt{2})}^{2}.$$

$[F : \mathbb{Q}]$ divides $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. If $[F : \mathbb{Q}] = 1$, then $F = \mathbb{Q}$. If $[F : \mathbb{Q}] = 2$, then $[\mathbb{Q}(\sqrt{2}) : F] = 1$ and $F = \mathbb{Q}(\sqrt{2})$. All the subfields of $\mathbb{Q}(\sqrt{2})$ are $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$. ■

20.24 Let E be an extension of F and let a and b belong to E. Prove that $F(a, b) = F(a)(b) = F(b)(a)$.

20.25 Write $x^3 + 2x + 1$ as a product of linear polynomials over some extension field of $\mathbb{Z}_3$.

Proof. Since $x^3 + 2x + 1$ has no root in $\mathbb{Z}_3$ and $\deg(x^3 + 2x + 1) = 3$, $x^3 + 2x + 1$ is irreducible over $\mathbb{Z}_3$. Let α be the root of $x^3 + 2x + 1$ in the extension field $\mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle \cong \mathbb{Z}_3(\alpha)$ of $\mathbb{Z}_3$.

$$\begin{array}{r|lllll}
 & x^2 & +\alpha x & +(2+\alpha^2) & & \\
\hline
x - \alpha & x^3 & & +2x & +1 & \\
 & x^3 & -\alpha x^2 & & & \\
\cline{2-3}
 & & \alpha x^2 & +2x & & \\
 & & \alpha x^2 & -\alpha^2 x & & \\
\cline{3-4}
 & & & (2+\alpha^2)x & +1 & \\
 & & & (2+\alpha^2)x & -(2\alpha+\alpha^3) & \\
\cline{4-5}
 & & & & 1 + 2\alpha + \alpha^3 & = 0
\end{array}$$

$$\begin{array}{r|llll}
 & x & +(2\alpha+1) & & \\
\hline
x - (\alpha+1) & x^2 & +\alpha x & +(2+\alpha^2) & \\
 & x^2 & -(\alpha+1)x & & \\
\cline{2-3}
 & & (2\alpha+1)x & +(\alpha^2+2) & \\
 & & (2\alpha+1)x & -(\alpha+1)(2\alpha+1) & \\
\cline{3-4}
 & & & \alpha^2 + 2 + 2\alpha^2 + 2\alpha + \alpha + 1 & = 0
\end{array}$$

$x^3 + 2x + 1 = (x - \alpha)(x - (\alpha + 1))(x + (2\alpha + 1))$. ■

20.26 Express $x^8 - x$ as a product of irreducibles over $\mathbb{Z}_2$.

Proof. **Lemma.** Let $f(x) \in F[x]$ and $\deg f(x) \in \{2,3\}$. Then $f(x)$ is irreducible over F if and only if $f(x)$ has no roots in F.

Use the lemma. The monic irreducible polynomial of degree 2 in $\mathbb{Z}_2[x]$ is x^2+x+1. The monic irreducible polynomials of degree 3 in $\mathbb{Z}_3[x]$ are x^3+x+1 and x^3+x^2+1.

$$\begin{aligned} x^8 - x &= x(x^7-1) \\ &= x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1) \\ &= x(x-1)(x^3+x+1)(x^3+x^2+1). \end{aligned}$$

■

20.27 Prove or disprove that $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{-3})$ are ring-isomorphic.

Proof. Suppose $\theta : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{-3})$ is an isomorphism and $\theta(\sqrt{3}) = a + b\sqrt{-3}$, where $a, b \in \mathbb{Q}$.

Note that if $r \in \mathbb{Q}$, then $\theta(r) = r$. Therefore, if $b = 0$, then θ is not onto. Thus, $b \neq 0$.

$3 = \theta(3) = \theta((\sqrt{3})^2) = (\theta(\sqrt{3}))^2 = (a+b\sqrt{-3})^2 = a^2 - 3b^2 + 2ab\sqrt{-3}$, where $a, b \in \mathbb{Q}$. This equation has no solution. ■

20.28 For any prime p, find a field of characteristic p that is not perfect.

Proof. By Exercise 20.39. ■

20.29 If β is a zero of x^2+x+2 over $\mathbb{Z}_5$, find the other zero.

Proof.

$$\begin{array}{r|llll} & x & +(1+\beta) & & \\ \cline{2-4} x-\beta & x^2 & +x & +2 & \\ & x^2 & -\beta x & & \\ \cline{2-3} & & (1+\beta)x & +2 & \\ & & (1+\beta)x & -\beta(1+\beta) & \\ \cline{3-4} & & & 2+\beta+\beta^2 & = 0 \end{array}$$

$-(1+\beta)$ is another root of x^2+x+2 in the extension field $\mathbb{Z}_5[x]/\langle x^2+x+2\rangle \cong \mathbb{Z}_5(\beta)$ of $\mathbb{Z}_5$. ■

20.30 Show that x^4+x+1 over $\mathbb{Z}_2$ does not have any multiple zeros in any extension field of $\mathbb{Z}_2$.

20.31 Show that $x^{21}+2x^8+1$ does not have multiple zeros in any extension of $\mathbb{Z}_3$.

20.32 Show that $x^{21}+2x^9+1$ has multiple zeros in some extension of $\mathbb{Z}_3$.

20.33 Let F be a field of characteristic $p \neq 0$. Show that the polynomial $f(x) = x^{p^n} - x$ over F has distinct zeros.

Proof.

$$\gcd\left(f(x), f'(x)\right) = \gcd\left(x^{p^n} - x, p^n x^{p^n-1} - 1\right) \overset{\substack{\text{char } F=p\neq 0\\ \downarrow}}{=} \gcd\left(x^{p^n} - x, -1\right) = 1.$$

■

20.34* Find the splitting field for $f(x) = (x^2+x+2)(x^2+2x+2)$ over $\mathbb{Z}_3[x]$. Write $f(x)$ as product of linear factors.

Proof. (x^2+x+2) and (x^2+2x+2) both are irreducible over $\mathbb{Z}_3$. Let α be the root of x^2+x+2 in the extension field $\mathbb{Z}_3[x]/\langle x^2+x+2\rangle \cong \mathbb{Z}_3(\alpha)$ of $\mathbb{Z}_3$.

$$\begin{array}{r|llll} & x & +(1+\alpha) & & \\ \cline{2-4} x-\alpha & x^2 & +x & +2 & \\ & x^2 & -\alpha x & & \\ \cline{2-3} & & (1+\alpha)x & +2 & \\ & & (1+\alpha)x & -(\alpha+\alpha^2) & \\ \cline{3-4} & & & 2+\alpha+\alpha^2 & =0 \end{array}$$

Note that 2α is a root of (x^2+2x+2).

$$\begin{array}{r|llll} & x & +(2+2\alpha) & & \\ \cline{2-4} x-2\alpha & x^2 & +2x & +2 & \\ & x^2 & -2\alpha x & & \\ \cline{2-3} & & (2+2\alpha)x & +2 & \\ & & (2+2\alpha)x & -2\alpha(2+2\alpha) & \\ \cline{3-4} & & & 2+4\alpha+4\alpha^2 & =0 \end{array}$$

$f(x) = (x-\alpha)(x+(1+\alpha))(x-2\alpha)(x+(2+2\alpha))$. ■

20.35 Let F be a field and E an extension field of F that contains $a_1, a_2, \ldots, a_n$. Prove that $F(a_1, a_2, \ldots, a_n)$ is the intersection of all subfields of E that contain F and the set $\{a_1, a_2, \ldots, a_n\}$.

Proof. If $F \le K$ and $\{a_1, a_2, \ldots, a_n\} \subseteq K$, then $F(a_1, a_2, \ldots, a_n) \le K$ and

$$F(a_1, a_2, \ldots, a_n) \le \bigcap_{\substack{F\le L\\ \{a_1,a_2,\ldots,a_n\}\subseteq L}} L.$$

$\bigcap_{\substack{F\le L\\ \{a_1,a_2,\ldots,a_n\}\subseteq L}} L \le F(a_1, a_2, \ldots, a_n)$ is obviously because $F(a_1, a_2, \ldots, a_n)$ is one of such L. ■

20.37* Suppose that $f(x)$ is a fifth-degree polynomial that is irreducible over $\mathbb{Z}_2$. Prove that every nonidentity element is a generator of the cyclic group $(\mathbb{Z}_2[x]/\langle f(x)\rangle)^*$.

Proof. Note that $(\mathbb{Z}_2[x]/\langle f(x)\rangle)^* = \mathbb{Z}_2[x]/\langle f(x)\rangle - \{0\}$ is a finite group under multiplication. The order of this group is $2^5 - 1 = 31$. By Lagrange's Theorem, the order of every nonidentity element in this group is 31. That is, every nonidentity element is a generator of this cyclic group. ■

20.38 Show that $\mathbb{Q}(\sqrt{7}, i)$ is the splitting field for $x^4 - 6x^2 - 7$.

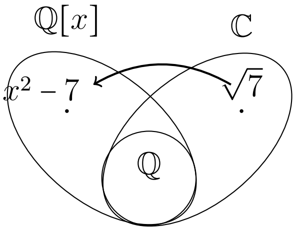
Proof.

$$\begin{aligned} x^4 - 6x^2 - 7 &= x^4 + x^2 - 7x^2 - 7 \\ &= x^2(x^2+1) - 7(x^2+1) \\ &= (x^2-7)(x^2+1) \\ &= (x-\sqrt{7})(x+\sqrt{7})(x+i)(x-i). \end{aligned}$$

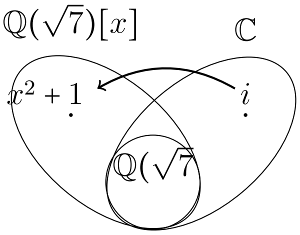
Hence, $\mathbb{Q}(\sqrt{7}, i)$ is the splitting field for $x^4 - 6x^2 - 7$ over $\mathbb{Q}$. ■

補充. 如果還要求 degree。

Since $x^2 - 7$ has no root in $\mathbb{Q}$ and $\deg x^2 - 7 = 2$, $x^2 - 7$ is irreducible over $\mathbb{Q}$ and it is the minimal of $\sqrt{7}$ over $\mathbb{Q}$. Thus, $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = \deg(x^2 - 7) = 2$.



Since $x^2 + 1$ has no root in $\mathbb{Q}(\sqrt{7})$ because the elements in $\mathbb{Q}(\sqrt{7})$ all are real numbers. $x^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt{7})$ and it is the minimal of i over $\mathbb{Q}(\sqrt{7})$. Thus, $[\mathbb{Q}(\sqrt{7})(i) : \mathbb{Q}(\sqrt{7})] = \deg(x^2 + 1) = 2$.



20.39 Let p be a prime, $F = \mathbb{Z}_p(t)$ (the field of quotients of the ring $\mathbb{Z}_p[x]$), and $f(x) = x^p - t$. Prove that $f(x)$ is irreducible over F and has a multiple zero in $K = F[x]/\langle x^p - t\rangle$.

Proof. By Exercise 20.15, $f(x)$ splits in $F[x]$ or irreducible over F.

$$\begin{aligned} &\text{If} && f(x) \text{ splits in } F[x] \\ &\Rightarrow && f(x) \text{ has a root } \frac{g(t)}{h(t)} \in F \\ &\Rightarrow && \left(\frac{g(t)}{h(t)}\right)^p - t = 0 \\ &\Rightarrow && [g(t)]^p = t \cdot [h(t)]^p \\ &\Rightarrow && p \mid \deg[g(t)]^p = \deg t[h(t)]^p = 1 + \deg[h(t)]^p, \\ &&& \text{which is a contradiction.} \\ &\Rightarrow && f(x) \text{ is irreducible over } F. \end{aligned}$$

Since $f'(x) = 0$, we have $\gcd(f(x), f'(x)) = f(x) \neq 1$ and $f(x)$ has multiple zero by Theorem 20.5.

Furthermore, consider $f(y) = y^p - t \in K[y] = (F[x]/\langle x^p - t\rangle)[y]$. Then

$$f(y) = y^p - t = y^p - x^p = (y - x)\sum_{i=0}^{p} y^i x^{p-i}.$$

Let $g(y) = \sum_{i=0}^{p} y^i x^{p-i}$. Then $g(x) = px^p = 0$ because the characteristic of K is p. Thus, $f(y)$ has multiple zero x in $K = F[x]/\langle x^p - t\rangle$. ■

補充. 題目中的 the field of quotients of the ring $\mathbb{Z}_p[x]$ 應該爲 the field of quotients of the ring $\mathbb{Z}_p[t]$。

20.40 Let $f(x)$ be an irreducible polynomial over a field F. Prove that the number of distinct zeros of $f(x)$ in a splitting field divides $\deg f(x)$.

Proof. It follows immediately from the Corollary in p.372. ■

補充 20.A Let $\alpha = \sqrt{2} + \sqrt{3}$. What is the minimal polynomial of α over $\mathbb{Q}$? Show further that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Proof.

$$\begin{aligned}
\alpha &= \sqrt{2} + \sqrt{3} \\
\alpha^2 &= 2 + 3 + 2\sqrt{6} \\
\alpha^2 - 5 &= 2\sqrt{6} \\
(\alpha^2 - 5)^2 &= 24 \\
\alpha^4 - 10\alpha^2 + 25 &= 24 \\
\alpha^4 - 10\alpha^2 + 1 &= 0.
\end{aligned}$$

Let $p(x) = x^4 - 10x^2 + 1$. Then $p(\sqrt{2} + \sqrt{3}) = 0$. We show that $p(x)$ is monic and irreducible over $\mathbb{Q}$. Then $p(x)$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

Since the roots of $p(x)$ all are not real numbers, $p(x)$ has no roots in $\mathbb{Q}$ and $p(x)$ has no linear factor in $\mathbb{Q}[x]$.

If $p(x)$ is reducible in $\mathbb{Q}[x]$, then $p(x)$ is reducible over $\mathbb{Z}$. Since $p(x)$ is monic, suppose that $p(x) = (x^2 + ax + b)(x^2 + cx + d)$, where $a, b, c, d \in \mathbb{Z}$. Then

$$p(x) = x^4 - 10x^2 + 1 = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (bc + ad)x + bd.$$

Compare the coefficients,

$$\begin{array}{ccccc}
x^4 & +(a+c)x^3 & +(b+ac+d)x^2 & +(bc+ad)x & +bd \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\
x^4 & +0x^3 & -10x^2 & +0x & +1
\end{array}$$

We have

$$\begin{aligned} a+c &= 0 \\ b+ac+d &= -10 \\ bc+ad &= 0 \\ bd &= 1. \end{aligned}$$

By $a+c=0$, we have $c=-a$. Then $0=bc+ad=-ab+ad=a(d-b)$. If $b-d=0$, then $bd=b^2=1$ and $b=d=\pm 1$. It follows that $b+ac+d=-a^2\pm 2=-10$ and $-a^2=-10\pm 2$. Which is impossible. Hence, $a=0$. Then $c=0$ and $b+ac+d=b+d=-10$ and $bd=1$. It follows that $b(-10-b)=1$ and $b=-5\pm 2\sqrt{6}$, it is impossible. There are no such a,b,c and d in $\mathbb{Z}$ satisfy these equations and $p(x)$ is irreducible over $\mathbb{Z}$ and $\mathbb{Q}$.

Furthermore, since $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$ is obviously. On the other hand, since $\sqrt{3}-\sqrt{2}=\frac{1}{\sqrt{2}+\sqrt{3}}=(\sqrt{2}+\sqrt{3})^{-1}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$, we have

$$\sqrt{3}=\frac{(\frac{1}{\sqrt{2}+\sqrt{3}})+(\sqrt{3}+\sqrt{2})}{2}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$$

and

$$\sqrt{2}=\frac{(\sqrt{3}+\sqrt{2})-(\frac{1}{\sqrt{2}+\sqrt{3}})}{2}\in\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Therefore, $\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$. ■

21 Chapter 21

題組 Minimal Polynomial

21.14, 21.16, 21.10, 21.13

題組 Finite Extension ⇒ Algebraic Extension

21.18, 21.22

題組 Computation in Field Extension

21.25, 21.24

題組 Algebraically Closed and Algebraic Closure

21.2, 21.5, thm.21.5, 21.4, Foote, p.541, exa, 21.17

重要 If $F\le L$ and $c\in L$ is algebraic over F. Let $m_F(x)$ be the minimal polynomial of c over F. Then $[F(c):F]=\deg m_F(x)$. Suppose that $K\le L$ is any extension of F. Note that $m_F(x)$ does not necessarily be the minimal polynomial of c over K. We can view $m_F(x)\in F[x]$ as a polynomial in $K[x]$ which has c as a root. So, c is algebraic over K. Let $m_K(x)$ be the minimal polynomial of c over K. Then

$$[K(c):K]=\deg m_K(x)\quad \overset{m_F(x)\in K[x],\ m_F(c)=0}{\overset{\downarrow}{\le}}\quad \deg m_F(x)=[F(c):F].$$

21.2 Let E be the algebraic closure of F. Show that every polynomial in $F[x]$ splits in E.

Proof. By the definition of the algebraic closure of F, E is algebraically closed. Thus, every polynomial in $E[x]$ splits in E. ■

21.3 Prove that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$ is an algebraic extension of $\mathbb{Q}$ but not a finite extension of $\mathbb{Q}$.

Proof. Let $\mathbb{A} = \{a \in \mathbb{C} \mid a \text{ is algebraic over } \mathbb{Q}\}$. Then $\mathbb{A}$ is an algebraic extension of $\mathbb{Q}$. Since $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots$ all are algebraic over $\mathbb{Q}$, we have $\mathbb{Q} \le \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots) \le \mathbb{A}$. Therefore, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$ is an algebraic extension of $\mathbb{Q}$.

If $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots) : \mathbb{Q}] = n$ is finite, then there exists $\sqrt[n+1]{2}$ such that

$$\overbrace{\mathbb{Q} \underbrace{\le}_{n+1} \mathbb{Q}(\sqrt[n+1]{2}) \le \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)}^{n},$$

a contradiction. ■

21.4 Let E be an algebraic extension of F. If every polynomial in $F[x]$ splits in E, show that E is algebraically closed.

Proof. Suppose that E is not algebraically closed. Then there exists a polynomial $f(x) \in E[x]$ which is irreducible over E and $\deg f(x) \ge 2$. Let $\alpha \notin E$ be a root of $f(x)$ in the extension field $E(\alpha) \cong E[x]/\langle f(x)\rangle$ of E.

Suppose that $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in E[x]$. Since E is an algebraic extension of F, $a_n, \dots, a_1, a_0$ all are algebraic over F. Then by Exercise 21.20, $F(a_n, \dots, a_1, a_0)$ is a finite extension of F. Now, $f(x) \in F(a_n, \dots, a_1, a_0)[x]$ and α is a root of $f(x)$, we have α is algebraic over $F(a_n, \dots, a_1, a_0)$ and $F(a_n, \dots, a_1, a_0)(\alpha)$ is an finite extension of $F(a_n, \dots, a_1, a_0)$ by Exercise 21.20 again. Then we have a tower of fields

$$F \underbrace{\le}_{<\infty} F(a_n, \dots, a_1, a_0) \underbrace{\le}_{<\infty} F(a_n, \dots, a_1, a_0)(\alpha).$$

It follows that $F(a_n, \dots, a_1, a_0)(\alpha)$ is a finite extension of F and α has the minimal polynomial $m(x) \in F[x]$ because a finite extension must be an algebraic extension.

By the hypothesis, $m(x)$ splits in $E[x]$. Suppose that $m(x) = (x - b_m)\cdots(x - b_2)(x - b_1) \in E[x]$. We know that α is a root of $m(x)$, so $\alpha = b_i$ for some $i \in \{1, 2, \dots, m\}$. But which implies that $\alpha = b_i \in E$, a contradiction. ■

21.5 Suppose that F is a field and every irreducible polynomial in $F[x]$ is linear. Show that F is algebraically closed.

補充. 不要把 algebraic closure of F 跟 algebraic closure of F in E 搞混了, 參考 moodle 上的講義。

補充. 關於 algebraically closed 的等價定義有下面四個, Gallian的書, 也就是你們的課本採用的是第四個。A field K is called algebraically closed.

(a) Every nonconstant polynomial in $K[x]$ has a root in K.

(b) Every nonconstant polynomial in $K[x]$ splits in $K[x]$.

(c) Every irreducible polynomial in $K[x]$ has degree 1.

(d) If K' is an algebraic extension of K, then $K' = K$.

21.6* Suppose that $f(x)$ and $g(x)$ are irreducible over F and that $\deg f(x)$ and $\deg g(x)$ are relatively prime. If a is a zero of $f(x)$ in some extension of F, show that $g(x)$ is irreducible over $F(a)$.

Proof. [**方法一**] Note that $f(x)$ is the minimal polynomial of a over F. Let b be a root of $g(x)$ in the extension field $F(b) \cong F[x]/\langle g(x)\rangle$ of F. Then $[F(a):F] = \deg f(x)$ and $[F(b):F] = \deg g(x)$ and $\gcd([F(a):F],[F(b):F]) = 1$. By Exercise 21.11,

$$\begin{aligned}
& [F(a,b):F] = [F(a):F]\cdot[F(b):F] \\
\Rightarrow\quad & [F(a,b):F(a)]\cdot\cancel{[F(a):F]} = \cancel{[F(a):F]}\cdot[F(b):F] \\
\Rightarrow\quad & [F(a,b):F(a)] = [F(b):F] = \deg g(x) \\
\Rightarrow\quad & g(x) \text{ is irreducible over } F(a).
\end{aligned}$$

[**方法二**] Let a be a root of $p(x)$ in some extension $E(a)$ of E. Although $p(x)$ is not necessarily the minimal polynomial of a over E, but we know that $[E(a):E] \le \deg p(x)$. Thus, we have the tower of fields

$$\overbrace{F \underbrace{\le}_{[E:F]} E \underbrace{\le}_{\le \deg p(x)} E(a)}^{[E(a):F]}$$

and $[E(a):F] \le \deg p(x)[E:F]$.

Consider the tower of fields

$$\begin{tikzcd}
 & E(a) \arrow[dl, dash, "\le \deg p(x)"'] \arrow[dd, dash] \arrow[dr, dash] & \\
E \arrow[dr, dash, "{[E:F]}"'] & & F(a) \arrow[dl, dash, "\deg p(x)"] \\
 & F &
\end{tikzcd}$$

We have

$$\begin{aligned}
& \deg p(x) = [F(a):F] \mid [E(a):F] \\
\text{and}\quad & [E:F] \mid [E(a):F] \\
\overset{\substack{\gcd(\deg p(x),[E:F])=1 \\ \downarrow}}{\Rightarrow}\quad & \deg p(x)[E:F] \mid [E(a):F] \\
\overset{\substack{[E(a):E]\le \deg p(x)[E:F] \\ \downarrow}}{\Rightarrow}\quad & [E(a):F] = \deg p(x)[E:F] \\
\Rightarrow\quad & [E(a):E] = \frac{[E(a):F]}{[E:F]} = \deg p(x) \\
\Rightarrow\quad & p(x) \text{ is irreducible over } E.
\end{aligned}$$

■

21.7 Let a and b belong to $\mathbb{Q}$ with $b \neq 0$. Show that $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ if and only if there exists some $c \in \mathbb{Q}$ such that $a = bc^2$.

Proof. ($\Leftarrow$) If $a = bc^2$ for some $c \in \mathbb{Q}$, then $\sqrt{a} = \sqrt{bc^2} = \sqrt{b}|c|$ and $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\sqrt{b})$. Since $c \neq 0$, we have $\sqrt{b} = \frac{\sqrt{a}}{|c|}$ and $\mathbb{Q}(\sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a})$.

($\Rightarrow$) If $\sqrt{a} \in \mathbb{Q}$, then $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{a}) = \mathbb{Q}$ and $\sqrt{b} \in \mathbb{Q}$. It follows that $\frac{\sqrt{a}}{\sqrt{b}} = c$ for some $c \in \mathbb{Q}$ and $a = bc^2$. We assume that $\sqrt{a}$ and $\sqrt{b}$ both are not in $\mathbb{Q}$.

$$\begin{aligned}
& \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b}) \\
\overset{\sqrt{a}\notin\mathbb{Q}}{\overset{\downarrow}{\Rightarrow}} \quad & \sqrt{a} = d + c\sqrt{b} \text{ for some } d, c \in \mathbb{Q}, c \neq 0 \\
\Rightarrow \quad & a = d^2 + c^2 b + 2bc\sqrt{b} \\
\text{if} \quad & d \neq 0 \\
\Rightarrow \quad & \sqrt{b} = \frac{a - d^2 - c^2 b}{2dc} \in \mathbb{Q}, \text{ a contradiction} \\
\Rightarrow \quad & d = 0 \\
\Rightarrow \quad & \sqrt{a} = c\sqrt{b} \\
\Rightarrow \quad & a = bc^2.
\end{aligned}$$

■

補充. 這題應該再多加 $c \neq 0$ 這個條件, 否則當 $c = 0$, $b = 2$ 時此題的 ($\Leftarrow$) 不成立。

21.8* Find the degree and a basis for $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ over $\mathbb{Q}(\sqrt{15})$. Find the degree and a basis for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2})$ over $\mathbb{Q}$.

Proof.

- Show that $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, see Exercise 20.2 and Exercise 21.35.
- Show that $\mathbb{Q}(\sqrt{3}, \sqrt{15}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$
- Show that $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$. Suppose that $\sqrt{5} = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ for some $a, b \in \mathbb{Q}$. If $a = 0$, then $b = \sqrt{\frac{5}{3}} \notin \mathbb{Q}$, a contradiction. If $b = 0$, then $\sqrt{5} = a \in \mathbb{Q}$, a contradiction. Thus, $a \neq 0$ and $b \neq 0$. Then $5 = a^2 + 2ab\sqrt{3} + 3b^2$ and $\sqrt{3} = \frac{5 - a^2 - 3b^2}{2ab} \in \mathbb{Q}$, a contradiction.

- Then we have

$$\begin{aligned}
& \sqrt{5}\notin\mathbb{Q}(\sqrt{3}) \\
\Rightarrow\quad & x^2-5 \text{ has no root in } \mathbb{Q}(\sqrt{3}) \\
\overset{\deg(x^2-5)=2}{\overset{\downarrow}{\Rightarrow}}\quad & x^2-5 \text{ is irreducible over } \mathbb{Q}(\sqrt{3}) \\
\Rightarrow\quad & x^2-5 \text{ is the minimal polynomial of } \sqrt{5} \text{ over } \mathbb{Q}(\sqrt{3}) \\
\Rightarrow\quad & [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{3})]=2 \\
\Rightarrow\quad & \overbrace{\mathbb{Q}\underbrace{\le}_{2}\mathbb{Q}(\sqrt{3})\underbrace{\le}_{2}\mathbb{Q}(\sqrt{3},\sqrt{5})}^{?} \\
\Rightarrow\quad & \overbrace{\mathbb{Q}\underbrace{\le}_{2}\mathbb{Q}(\sqrt{15})\underbrace{\le}_{?}\mathbb{Q}(\sqrt{15},\sqrt{3})=\mathbb{Q}(\sqrt{3},\sqrt{5})}^{4}.
\end{aligned}$$

- Therefore, $\{1,\sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{3}+\sqrt{5})=\mathbb{Q}(\sqrt{3},\sqrt{5})=\mathbb{Q}(\sqrt{15},\sqrt{3})$ over $\mathbb{Q}(\sqrt{15})$.

We prove the second part of the question. The method is the same as which we use in Exercise 21.34.

- Show that $\mathbb{Q}(\sqrt{2},\sqrt[3]{2},\sqrt[4]{2})=\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{2})$.
- Show that $\sqrt[3]{2}\notin\mathbb{Q}(\sqrt[4]{2})$. If $\sqrt[3]{2}\in\mathbb{Q}(\sqrt[4]{2})$, then

$$\overbrace{\mathbb{Q}\underbrace{\le}_{3}\mathbb{Q}(\sqrt[3]{2})\le\mathbb{Q}(\sqrt[4]{3})}^{4}.$$

- Show that x^3-2 has no root in $\mathbb{Q}(\sqrt[4]{2})$.

$$\begin{aligned}
& x^3-2 \text{ has no root in } \mathbb{Q}(\sqrt[4]{2}) \\
\overset{\deg(x^3-2)=3}{\overset{\downarrow}{\Rightarrow}}\quad & x^3-2 \text{ is irreducible over } \mathbb{Q}(\sqrt[4]{2}) \\
\Rightarrow\quad & [\mathbb{Q}(\sqrt[4]{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt[4]{2})]=\deg(x^3-2)=3
\end{aligned}$$

- Then we have

$$\mathbb{Q}\underbrace{\le}_{4}\mathbb{Q}(\sqrt[4]{2})\underbrace{\le}_{3}\mathbb{Q}(\sqrt[4]{2},\sqrt[3]{2}).$$

- $\{ab \mid a\in\{1,\sqrt[4]{2},\sqrt[4]{4},\sqrt[4]{8}\}, b\in\{1,\sqrt[3]{2},\sqrt[3]{4}\}\}$ is a basis for $\mathbb{Q}(\sqrt[4]{2},\sqrt[3]{2})$ over $\mathbb{Q}$.

■

21.9 Suppose that E is an extension of F of prime degree. Show that, for every a in E, $F(a)=F$ or $F(a)=E$.

Proof. Consider the tower of fields

$$\overbrace{F \leq F(a) \leq E}^{p}.$$

$[F(a):F]$ divides $[E:F]=p$. If $[F(a):F]=1$, then $F(a)=F$. If $[F(a):F]=p$, then $[E:F(a)]=1$ and $F(a)=E$. ■

21.10 Let a be a complex number that is algebraic over $\mathbb{Q}$. Show that $\sqrt{a}$ is algebraic over $\mathbb{Q}$. Why does this prove that $\sqrt[2n]{a}$ is algebraic over $\mathbb{Q}$.

Proof. Since a is algebraic over $\mathbb{Q}$, let $f(x)$ be a nonzero polynomial in $\mathbb{Q}[x]$ such that $f(a)=0$. Then $\sqrt{a}$ is a root of the polynomial $f(x^2)\in\mathbb{Q}[x]$ and $\sqrt[2n]{a}$ is a root of the polynomial $f(x^{2n})\in\mathbb{Q}[x]$. ■

21.11* Suppose that E is an extension of F and $a,b\in E$. If a is algebraic over F of degree m, and b is algebraic over F of degree n, where m and n are relatively prime, show that $[F(a,b):F]=mn$.

Proof. Consider the towers of fields

$$F \leq F(a) \leq F(a,b)$$

and

$$F \leq F(b) \leq F(a,b).$$

$$\begin{aligned}
& [F(a):F] \mid [F(a,b):F] = [F(a,b):F(b)]\cdot[F(b):F] \\
\overset{\substack{\gcd([F(a):F],[F(b):F])=1 \\ \downarrow}}{\Rightarrow} \quad & [F(a):F] \mid [F(a,b):F(b)] = [K(a):K], \text{ where } K=F(b) \\
\overset{\substack{[K(a):K]\leq[F(a):F] \\ \downarrow}}{\Rightarrow} \quad & [F(a):F] = [K(a):K] = [F(a,b):F(b)] \\
\overset{\substack{\text{multiplying } [F(b):F] \\ \downarrow}}{\Rightarrow} \quad & mn = [F(a):F][F(b):F] = [F(a,b):F(b)][F(b):F] = [F(a,b):F].
\end{aligned}$$

■

21.12* Find an example of a field F and elements a and b from some extension field such that $F(a,b)\neq F(a), F(a,b)\neq F(b)$, and $[F(a,b):F]<[F(a):F][F(b):F]$.

Proof. Since $\sqrt[6]{2}$ is a root of the polynomial $x^3-(\sqrt[4]{2})^2$ over $\mathbb{Q}(\sqrt[4]{2})$, let $m(x)$ be the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt[4]{2})$. Then we have $[\mathbb{Q}(\sqrt[4]{2},\sqrt[6]{2}):\mathbb{Q}(\sqrt[4]{2})] = \deg m(x) \leq \deg(x^3-(\sqrt[4]{2})^2)=3$. Consider the tower of fields

$$\mathbb{Q}\underbrace{\leq}_{4}\mathbb{Q}(\sqrt[4]{2}) \qquad \underbrace{\leq}_{\leq\deg(x^3-(\sqrt[4]{2})^2)=3} \qquad \mathbb{Q}(\sqrt[4]{2},\sqrt[6]{2}).$$

In this case, $[\mathbb{Q}(\sqrt[4]{2},\sqrt[6]{2}):\mathbb{Q}]\leq 4\cdot 3 < 4\cdot 6 = [\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]\cdot[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}]$. ■

21.13* Let K be a field extension of F and let $a\in K$. Show that $[F(a):F(a^3)]\leq 3$. Find examples to illustrate that $[F(a):F(a^3)]$ can be $1,2$, or 3.

Proof. Since a is a root of the polynomial $x^3 - a^3$ over $F(a^3)$, $[F(a) : F(a^3)] \leq \deg x^3 - a^3 = 3$.

Let $a \in F$. Then $[F(a) : F(a^3)] = 1$.

Let $F = \mathbb{Q}$, $a = \sqrt[3]{2}$. Then $[F(a) : F(a^3)] = 3$. A slightly complicate example is given by

$$\overbrace{\mathbb{Q} \underbrace{\leq}_{2} \mathbb{Q}(\sqrt{2}) \underbrace{\leq}_{?} \mathbb{Q}(\sqrt[6]{2})}^{6}$$

Let $F = \mathbb{Q}$ and $a = \xi_3$, where $= \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$. Then the minimal polynomial of a over $\mathbb{Q}$ is $x^2 + x + 1$ (not $x^3 - 1$) and we have

$$\mathbb{Q} \underbrace{\leq}_{1} \mathbb{Q}(a^3) \underbrace{\leq}_{2} \mathbb{Q}(a).$$

■

21.14 Find the minimal polynomial for $\sqrt{-3} + \sqrt{2}$ over $\mathbb{Q}$.

Proof.

$$\begin{aligned} x &= \sqrt{-3} + \sqrt{2} \\ x^2 &= (-3) + 2\sqrt{-6} + 2 \\ x^2 + 1 &= 2\sqrt{-6} \\ (x^2+1)^2 &= -24 \\ x^4 + 2x^2 + 1 &= -24 \\ x^4 + 2x^2 + 25 &= 0. \end{aligned}$$

Let $f(x) = x^4 + 2x^2 + 25$. Prove that $f(x)$ is irreducible over $\mathbb{Q}$. Then $f(x)$ is the minimal polynomial of $\sqrt{-3} + \sqrt{2}$ over $\mathbb{Q}$. ■

21.15 Let K be an extension of F. Suppose that E_1 and E_2 are contained in K and are extensions of F. If $[E_1 : F]$ and $[E_2 : F]$ are both prime, show that $E_1 = E_2$ or $E_1 \cap E_2 = F$.

Proof. Consider the tower of fields

$$\overbrace{F \leq E_1 \cap E_2 \leq E_1}^{p}.$$

$[E_1 \cap E_2 : F]$ divides $[E_1 : F] = p$. If $[E_1 \cap E_2 : F] = 1$, then $F = E_1 \cap E_2$.

If $[E_1 \cap E_2 : F] = p$, then $[E_1 : E_1 \cap E_2] = 1$ and $E_1 \cap E_2 = E_1$ and $E_1 \subseteq E_2$. In this case, consider the tower of fields

$$\overbrace{F \underbrace{\leq}_{p} E_1 \cap E_2 \leq E_2}^{p}.$$

We get $[E_2 : E_1 \cap E_2] = 1$ and $E_2 = E_1 \cap E_2$ and $E_2 \subseteq E_1$. Therefore, $E_1 = E_2$. ■

21.16 Find the minimal polynomial for $\sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$.

21.17 Let E be a finite extension of $\mathbb{R}$. Use the fact that $\mathbb{C}$ is algebraically closed to prove that $E = \mathbb{C}$ or $E = \mathbb{R}$.

21.18 Suppose that $[E : \mathbb{Q}] = 2$. Show that there is an integer d such that $E = \mathbb{Q}(\sqrt{d})$ where d is not divisible by the square of any prime.

Proof. [方法一]

$$\begin{array}{cl}
 & [E : \mathbb{Q}] = 2 \\
\Rightarrow & \mathbb{Q} \le E \text{ is finite extension} \\
\Rightarrow & \mathbb{Q} \le E \text{ is algebraic extension} \\
\overset{\substack{[E:\mathbb{Q}]=2,\ E\neq\mathbb{Q} \\ \downarrow}}{\Rightarrow} & \text{select } a \in E, a \notin \mathbb{Q}, a \text{ is algebraic over } \mathbb{Q} \\
\Rightarrow & \overbrace{\mathbb{Q} \underbrace{\le}_{\neq 1} \mathbb{Q}(a) \le E}^{2} \\
\Rightarrow & [\mathbb{Q}(a) : \mathbb{Q}] = 2 \text{ and } E = \mathbb{Q}(a) \\
\Rightarrow & \text{let } x^2 + bx + c \text{ be the minimal polynomial of } a \text{ over } \mathbb{Q} \\
\Rightarrow & a = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2} = \dfrac{-b \pm e\sqrt{d}}{2} \\
\Rightarrow & E = \mathbb{Q}(a) = \mathbb{Q}(\sqrt{d}).
\end{array}$$

[方法二]

$$\begin{array}{cl}
 & [E : \mathbb{Q}] = 2 < \infty \\
\overset{\substack{\text{Theorem 21.4} \\ \downarrow}}{\Rightarrow} & \mathbb{Q} \neq E \text{ is an algebraic extension of } \mathbb{Q} \\
\text{select} & a \in E \text{ and } a \notin \mathbb{Q} \\
\Rightarrow & a \text{ is algebraic over } \mathbb{Q} \\
\text{let} & m(x) \text{ be the minimal polynomial of } a \text{ over } \mathbb{Q} \\
\Rightarrow & [\mathbb{Q}(a) : \mathbb{Q}] = \deg m(x) \\
\text{since} & a \notin \mathbb{Q} \\
\Rightarrow & [\mathbb{Q}(a) : \mathbb{Q}] \neq 1 \\
\Rightarrow & \underbrace{\mathbb{Q} \overbrace{\le}^{\neq 1} \mathbb{Q}(a) \le E}_{2} \\
\Rightarrow & \deg m(x) = [\mathbb{Q}(a) : \mathbb{Q}] = 2 \text{ and } [E : \mathbb{Q}(a)] = 1 \\
\text{suppose} & m(x) = x^2 - d \in \mathbb{Q}[x] \\
\Rightarrow & m(a) = a^2 - d = 0 \\
\Rightarrow & a = \pm\sqrt{d} \\
\Rightarrow & E = \mathbb{Q}(a) = \mathbb{Q}(\sqrt{d}).
\end{array}$$

■

21.19 Suppose that $p(x) \in F[x]$ and E is a finite extension of F. If $p(x)$ is irreducible over F, and $\deg p(x)$ and $[E:F]$ are relatively prime, show that $p(x)$ is irreducible over E.

Proof. Since $F \le E$, we can view $p(x) \in F[x]$ as a polynomial in $E[x]$. By Kronecker's Theorem (Theorem 20.1), $p(x)$ has a root a in some extension field L of E. Let $m(x)$ be the minimal polynomial of a over E. Then $[E(a):E] = \deg m(x) \le \deg p(x)$. Then we have the tower of fields

$$\overbrace{F \underbrace{\le}_{[E:F]} E \qquad \underbrace{\le}_{[E(a):E]\le \deg p(x)} \qquad E(a)}^{[E(a):F]}.$$

On the other hand, note that $p(x)$ is the minimal polynomial of a over F. Hence, $[F(a):F] = \deg p(x)$. Consider the tower of fields

$$\overbrace{F \quad \underbrace{\le}_{\deg p(x)} \quad F(a) \le E(a)}^{[E(a):F]}.$$

Then

$$\begin{array}{cl}
 & \deg p(x) \mid [E(a):F] = [E:F] \cdot [E(a):E] \\
\overset{\gcd(\deg p(x),[E:F])=1}{\overset{\downarrow}{\Rightarrow}} & \deg p(x) \mid [E(a):E] \\
\overset{[E(a):E]\le \deg p(x)}{\overset{\downarrow}{\Rightarrow}} & \deg p(x) = [E(a):E] \\
\Rightarrow & p(x) \text{ is irreducible over } E.
\end{array}$$

■

21.20 Let E be an extension field of F. Show that $[E:F]$ is finite if and only if $E = F(a_1, a_2, ..., a_n)$, where $a_1, a_2, ..., a_n$ are algebraic over F.

Proof. ($\Rightarrow$) Suppose that $\dim_F E = [E:F] = n$. Let $\{a_1, a_2, ..., a_n\}$ be a basis for the vector space E over F. Then $E = F(a_1, a_2, ..., a_n)$. Since a finite extension of F must be a algebraice extension, E is an algebraic extension of F and $a_1, a_2, ..., a_n$ are algebraic over F.

($\Leftarrow$) Since a_i is algebraic over F, let $m_i(x)$ be the minimal polynomial of a_i over F. Recall that for each $i = 1, 2, ..., n$,

$$[F(a_1, a_2, ..., a_i) : F(a_1, a_2, ..., a_{i-1})] \le [F(a_i):F] = \deg m_i(x), \text{ where } a_0 = 0.$$

Then

$$\begin{array}{rcl}
[F(a_1, a_2, ..., a_n) : F] & = & [F(a_1, a_2, ..., a_n) : F(a_1, a_2, ..., a_{n-1})] \\
 & \times & [F(a_1, a_2, ..., a_{n-1}) : F(a_1, a_2, ..., a_{n-2})] \\
 & \times & \cdots \\
 & \times & [F(a_1, a_2) : F(a_1)] \times [F(a_1) : F] \\
 & \le & \deg m_n(x) \cdot \deg m_{n-1}(x) \cdots \deg m_1(x) < \infty
\end{array}$$

■

21.21 If α and β are real numbers and α and β are transcendental over $\mathbb{Q}$, show that either $\alpha\beta$ or $\alpha+\beta$ is also transcendental over $\mathbb{Q}$.

Proof. **Lemma:** If u and v both are algebraic over F, then $u+v$ and uv are also algebraic over F.

Proof of Lemma: Let $f(x)$ and $g(x)$ be the minimal polynomial of u and v over F, respectively. Then

$$\overbrace{F \underbrace{\le}_{\deg f(x)} F(u) \underbrace{\le}_{\le \deg g(x)} F(u,v)}^{\le \deg f(x)\cdot \deg g(x)}.$$

That is, $F(u,v)$ is a finite extension of F. (See Exercise 21.20.)

Consider two towers of fields,

$$\overbrace{F \le F(u+v) \le F(u,v)}^{<\infty}.$$

$$\overbrace{F \le F(uv) \le F(u,v)}^{<\infty}.$$

We have $F(u+v)$ and $F(uv)$ are finite extension of F. Hence, $F(u+v)$ and $F(uv)$ are algebraic extension of F. Therefore, $u+v$ and uv are algebraic over F.

We use the $\sim p \Leftarrow \sim q$ prove the original problem. If $\alpha\beta$ and $\alpha+\beta$ are algebraic over $\mathbb{Q}$, then by Lemma, $(\alpha-\beta)^2 = (\alpha+\beta)^2 - 4\alpha\beta$ is algebraic over $\mathbb{Q}$. By Exercise 21.10, $(\alpha-\beta)$ is also algebraic over F and $\alpha = \frac{(\alpha-\beta)+(\alpha+\beta)}{2}$ is algebraic over $\mathbb{Q}$. ■

21.22 Let $f(x)$ be a nonconstant elements of $F[x]$. If a belongs to some extension of F and $f(a)$ is algebraic over F, prove that a is algebraic over F.

Proof. Since a is a root of $f(x)-f(a)$ over $F(f(a))$, $[F(a):F(f(a))] \le \deg(f(x)-f(a))$. Then we have the tower of fields

$$F \underbrace{\le}_{\le\infty} F(f(a)) \underbrace{\le}_{\le \deg[f(x)-f(a)]} F(a).$$

Hence, $F(a)$ is a finite extension field of F and algebraic extension. It follows that a is algebraic over F. ■

補充. 這題也可以直接證。If $f(a)$ is algebraic over F and $g(f(a)) = 0$, then $(g\circ f)(a) = 0$.

21.23 Let $f(x) = ax^2+bx+c \in \mathbb{Q}[x]$. Find a primitive element for the splitting field for $f(x)$ over $\mathbb{Q}$.

Proof. $\sqrt{b^2-4ac}$. ■

21.24 Find the splitting field for x^4-x^2-2 over $\mathbb{Z}_3$.

Proof. $x^4 - x^2 - 2$ has no root in $\mathbb{Z}_3$, so $x^4 - x^2 - 2$ has no linear factor in $\mathbb{Z}_3[x]$.

Lemma. Suppose that $\deg f(x) \in \{2, 3\}$, $f(x)$ is irreducible over F if and only if $f(x)$ has no root in F.

You can list all monic polynomials of degree 2 in $\mathbb{Z}_3[x]$. They are

$$\begin{array}{llll}
x^2 & & & \text{has root } 0 \\
x^2 & & +1 & \leftarrow \\
x^2 & & +2 & \text{has root } 1 \\
x^2 & +x & & \text{has root } 0 \\
x^2 & +x & +1 & \text{has root } 1 \\
x^2 & +x & +2 & \leftarrow \\
x^2 & +2x & & \text{has root } 1 \\
x^2 & +2x & +1 & \text{has root } 2 \\
x^2 & +2x & +2 & \leftarrow
\end{array}$$

The only monic irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$ are $x^2 + 1, x^2 + x + 2$ and $x^2 + 2x + 2$.

Observe that $x^4 - x^2 - 2 = (x^2)^2 + 2x^2 + 1 = (x^2 + 1)^2$. Let a be a root of $x^2 + 1$ in the extension field $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$ of $\mathbb{Z}_3$. Then $(x^2 + 1) = (x - a)(x + a)$ and $x^4 - x^2 - 2 = [(x - a)(x + a)]^2$. ■

21.25 Let $f(x) \in F[x]$. If $\deg f(x) = 2$ and a is a zero of $f(x)$ in some extension of F, prove that $F(a)$ is the splitting field for $f(x)$ over F.

Proof. Suppose that $f(x) = a_2x^2 + a_1x + a_0$.

$$\begin{array}{r|llll}
 & a_2x & +(a_1 + a_2a) & & \\
\hline
x - a & a_2x^2 & +a_1x & +a_0 & \\
 & a_2x^2 & -a_2ax & & \\
\cline{2-3}
 & & (a_1 + a_2a)x & +a_0 & \\
 & & (a_1 + a_2a)x & -a(a_1 - a_2a) & \\
\cline{3-4}
 & & & a_0 + a_1a + a_2a^2 & = 0
\end{array}$$

The splitting field for $f(x)$ over F is $F(a, \frac{-a_1 - a_2a}{a_2}) = F(a)$.

■

21.26 Let a be a complex zero of $x^2 + x + 1$ over $\mathbb{Q}$. Prove that $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(a)$.

Proof. Note that $x^3 - 1 = (x - 1)(x^2 + x + 1)$. If $a = \xi_3 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, then, $\sqrt{a} = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{3}i) = \mathbb{Q}(\sqrt{a})$. If $a = \xi_3^2$, then $\sqrt{a} = \xi_3$. We also have the same result. ■

21.27 If F is a field and the multiplicative group of nonzero elements of F is cyclic, prove that F is finite.

Proof. Suppose that $F - \{0\} = \{a, a^2, a^3, ...\}$. Since $1 \in F - \{0\}$, we have $a^r = 1$ for some $r \in \mathbb{N}^+$. Thus, $F - \{0\}$ is finite. ■

補充. 這個定理的反方向是一個非常重要的定理, 敘述一遍: If F is a finite field, then the multiplicative group of nonzero elements of F is cyclic.

21.28 Let a be a complex number that is algebraic over $\mathbb{Q}$ and let r be a rational number. Show that a^r is algebraic over $\mathbb{Q}$.

Proof. Suppose that $r = \frac{s}{t}$, where $s, t \in \mathbb{Z}$ and $t > 0$. Since a is algebraic over $\mathbb{Q}$, suppose that there exists $f(x) = a_n x^n + \cdots + a_1 x + a_0$ such that $f(a) = 0$. Then $a^{\frac{1}{t}}$ is a root of $f(x^t) \in \mathbb{Q}[x]$. Hence, $a^{\frac{1}{t}}$ is algebraic over $\mathbb{Q}$. Therefore, $r = (a^{\frac{1}{t}})^s$ is algebraic over $\mathbb{Q}$. ■

21.29 Prove that, if K is an extension field of F, then $[K : F] = n$ if and only if K is isomorphic to F^n as vector spaces.

Proof. Let $\{k_1, k_2, \ldots, k_n\}$ be a basis for K over F. Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in F^n$ with 1 in the ith position and 0 elsewhere. Consider a mapping $T : K \to F^n$ which is defined by

$$T\left(\sum_{i=1}^{n} f_i k_i\right) = \sum_{i=1}^{n} f_i e_i.$$

Then T is a bijective linear transformation.

Recall that any two vector spaces are isomorphic if they have the same dimension.

■

21.30 Let a be a positive real number and let n be an integer greater that 1. Prove or disprove that $[\mathbb{Q}(a^{1/n}) : \mathbb{Q}] = n$.

Proof. Let $a = 4$, $n = 2$. Then $[\mathbb{Q}(4^{1/2}) : \mathbb{Q}] = 1 \neq 2 = n$. ■

21.31 Let a and b belong to some extension field of F and let b be algebraic over F. Prove that $[F(a,b) : F(a)] \leq [F(a,b) : F]$.

Proof. Consider the tower of fields

$$F \leq F(a) \leq F(a,b).$$

■

21.32* Let $f(x)$ and $g(x)$ be irreducible polynomials over a field F and let a and b belong to some extension E of F. If a is a zero of $f(x)$ and b is a zero of $g(x)$, show that $f(x)$ is irreducible over $F(b)$ if and only if $g(x)$ is irreducible over $F(a)$.

Proof. It is sufficient to prove one direction. See Exercise 21.6.

$$\begin{aligned}
\text{If } f(x) \text{ is irreducible over } F(b) \quad &\Rightarrow \quad F \underbrace{\leq}_{=\deg g(x)} F(b) \underbrace{\leq}_{=\deg f(x)} F(a,b) \\
&\Rightarrow \quad [F(a,b) : F] = \deg f(x) \cdot \deg g(x) \\
&\Rightarrow \quad \overbrace{F \underbrace{\leq}_{\deg f(x)} F(a) \leq F(a,b)}^{\deg f(x) \cdot \deg g(x)} \\
&\Rightarrow \quad [F(a,b) : F(a)] = \deg g(x)
\end{aligned}$$

■

21.33 Let β be a zero of $f(x) = x^5 + 2x + 4$ (see Example 8 in Chapter 17). Show that none of $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ belongs to $\mathbb{Q}(\beta)$.

Proof. If $\sqrt{2} \in \mathbb{Q}(\beta)$, then consider the tower of fields

$$\overbrace{\mathbb{Q} \underbrace{\le}_{2} \mathbb{Q}(\sqrt{2}) \le \mathbb{Q}(\beta)}^{5}.$$

Which implies that $2 \mid 5$, a contradiction. Thus, $\sqrt{2} \notin \mathbb{Q}(\beta)$. ■

21.34 Prove that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

Proof. [**方法一**]

$$\begin{aligned} & \sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \\ \Rightarrow \quad & x^3 - 2 \text{ has no root in } \mathbb{Q}(\sqrt{2}) \\ \overset{\deg(x^3-2)\in\{2,3\}}{\Rightarrow} \quad & x^3 - 2 \text{ is irreducible over } \mathbb{Q}(\sqrt{2}) \\ \Rightarrow \quad & x^3 - 2 \text{ is the minimal polynomial of } \sqrt[3]{2} \text{ over } \mathbb{Q}(\sqrt{2}) \\ \Rightarrow \quad & \mathbb{Q} \overbrace{\le}^{2} \mathbb{Q}(\sqrt{2}) \quad \overbrace{\le}^{\deg(x^3-2)=3} \quad \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \\ \Rightarrow \quad & [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6 \end{aligned}$$

On the other hand, since $\sqrt{2} = (\sqrt[6]{2})^3$ and $\sqrt[3]{2} = (\sqrt[6]{2})^2$, $\sqrt{2}$ and $\sqrt[3]{2}$ both are in $\mathbb{Q}(\sqrt[6]{2})$, we have a tower of fields and degree

$$\underbrace{\mathbb{Q} \overbrace{\le}^{6} \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \le \mathbb{Q}(\sqrt[6]{2})}_{6}.$$

Which implies that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})] = 1$ and $\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

[**方法二**]

- $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$ is obviously because $\sqrt{2} = (\sqrt[6]{2})^3$ and $\sqrt[3]{2} = (\sqrt[6]{2})^2$.
- We show that $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$. If $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2})$, then

$$\overbrace{\mathbb{Q} \underbrace{\le}_{3} \mathbb{Q}(\sqrt[3]{2}) \le \mathbb{Q}(\sqrt{2})}^{2}$$

  and $3 \mid 2$, a contradiction.
- All the root of $x^3 - 2$ in $\mathbb{C}$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\xi_3$ and $\sqrt[3]{2}\xi_3^2$, where $\xi_3 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$. We already know that $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$. $\sqrt[3]{2}\xi_3$ and $\sqrt[3]{2}\xi_3^2$ both are not real number. Thus, they are not in $\mathbb{Q}(\sqrt{2})$. Hence, $x^3 - 2$ has no root in $\mathbb{Q}(\sqrt{2})$.

- Then

$$\begin{aligned} & x^3-2 \text{ has no root in } \mathbb{Q}(\sqrt{2}) \\ \overset{\deg(x^3-2)=3}{\overset{\downarrow}{\Rightarrow}} \quad & x^3-2 \text{ is irreducible over } \mathbb{Q}(\sqrt{2}) \\ \Rightarrow \quad & [\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}(\sqrt{2})] = \deg(x^3-2) = 3 \end{aligned}$$

- Then we have the tower of field

$$\overbrace{\mathbb{Q} \underbrace{\le}_{2} \mathbb{Q}(\sqrt{2}) \underbrace{\le}_{3} \mathbb{Q}(\sqrt{2},\sqrt[3]{2}) \underbrace{\le}_{?} \mathbb{Q}(\sqrt[6]{2})}^{6}.$$

It follows that $[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}(\sqrt{2},\sqrt[3]{2})] = 1$ and $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

■

21.35 Let a and b be rational numbers. Show that $\mathbb{Q}(\sqrt{a},\sqrt{b}) = \mathbb{Q}(\sqrt{a}+\sqrt{b})$.

Proof. $\mathbb{Q}(\sqrt{a}+\sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a},\sqrt{b})$ is obviously because $\sqrt{a}+\sqrt{b} \in \mathbb{Q}(\sqrt{a},\sqrt{b})$. Conversely, if $a=b$, then the assertion is easy to verify. So we suppose that $a \ne b$. Then

$$\mathbb{Q}(\sqrt{a}+\sqrt{b}) \ni \frac{\sqrt{a}+\sqrt{b}}{a-b} + \frac{1}{\sqrt{a}+\sqrt{b}} = \frac{\sqrt{a}-\sqrt{b}}{a-b} + \frac{\sqrt{a}-\sqrt{b}}{a-b} = \frac{2\sqrt{a}}{a-b}$$

and $\sqrt{a} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$. Similary, $\sqrt{b} \in \mathbb{Q}(\sqrt{a}+\sqrt{b})$ and $\mathbb{Q}(\sqrt{a},\sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a}+\sqrt{b})$. ■

21.36 Let F, K, and L be fields with $F \subseteq K \subseteq L$. If L is a finite extension of F and $[L:F] = [L:K]$, prove that $F = K$.

Proof. Consider the tower of fields

$$\overbrace{F \underbrace{\le}_{1} K \underbrace{\le}_{r} L}^{r}.$$

Since $[L:F] = [L:K]$, it must be $[K:F] = 1$. That is, $K = F$. ■

21.37 Let F be a field and K a splitting field for some nonconstant polynomial over F. Show that K is a finite extension of F.

Proof. Let $f(x)$ be a nonconstant polynomial in $F[x]$ and $f(x)$ splits in its splitting field E. That is, $f(x) = u(x-r_1)^{s_1}(x-r_2)^{s_2}\cdots(x-r_t)^{s_t} \in E[x]$ and $E = F(r_1, r_2, ..., r_t)$. By Exercise 21.20, E is a finite extension of F. ■

21.38 Prove that $\mathbb{C}$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$.

Proof. ■

21.39 Prove that $\sqrt{2}$ is not an element of $\mathbb{Q}(\pi)$.

Proof. If $\sqrt{2} = \frac{f(\pi)}{g(\pi)}$, then π is a root of the polynomial $[f(x)]^2 - 2[g(x)]^2$ and π is algebraic over $\mathbb{Q}$, a contradiction. ■

21.40 Let $\alpha = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$ and $\beta = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Prove that β is not in $\mathbb{Q}(\alpha)$.

Proof.

$$\begin{aligned} & p \text{ is a prime} \\ \Rightarrow\ & x^{p-1} + \cdots + x + 1 \text{ is irreducible over } \mathbb{Q} \\ \Rightarrow\ & \text{the minimal polynomial of } \xi_p \text{ over } \mathbb{Q} \text{ is } x^{p-1} + \cdots + x + 1 \end{aligned}$$

If $\beta = \xi_5 \in \mathbb{Q}(\alpha) = \mathbb{Q}(\xi_7)$, then $\overbrace{\mathbb{Q} \underbrace{\le}_{4} \mathbb{Q}(\xi_5) \le \mathbb{Q}(\xi_7)}^{6}$. ■

補充. 這題在後面討論 cyclotomic polynomial 時很重要。這裡證明一下爲何 $x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.

$$f(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}.$$

$$\begin{aligned} f(x+1) &= (x+1)^{p-1} + \cdots + (x+1) + 1 \\ &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1} \\ &\Rightarrow f(x+1) \text{ is irreducible over } \mathbb{Q} \text{ by Eisenstein Criterion with prime } p \\ &\Rightarrow f(x) \text{ is irreducible over } \mathbb{Q}. \end{aligned}$$

20.36, 21.41 Suppose that a is algebraic over a field F. Show that a and $1 + a^{-1}$ have the same degree over F.

Proof. [**方法一**] $1 + a^{-1} \in F(a)$ and $F(1 + a^{-1}) \le F(a)$ is obviously. On the other hand, $a = [(1 + a^{-1}) - 1]^{-1} \in F(1 + a^{-1})$ implies that $F(a) \le F(1 + a^{-1})$. Therefore, $F(a) = F(1 + a^{-1})$ and a and $1 + a^{-1}$ have the same degree over F.

[**方法二**] Note that $F(a) = F(a^{-1})$. Let $m(x)$ be the minimal polynomial of a^{-1} over F. Then $m(x-1)$ is irreducible over F and $m(x-1)$ is the minimal polynomial of $1 + a^{-1}$ over F and $[F(1 + a^{-1}) : F] = \deg m(x-1) = \deg m(x) = [F(a^{-1}) : F] = [F(a) : F]$ ■

[**方法三**] Let $f(x)$ be the minimal polynomial of a. Since $f(x)$ is irreducible over F, the constant term of $f(x)$ is nonzero and the reciprocal polynomial $f^*(x) =$

$x^n f(1/x)$ of $f(x)$ is also irreducible over F (see here[4]) and $\deg f^*(x) = n$, where $n = \deg f(x)$. Note that $f^*(a^{-1}) = (a^{-1})^n f(a) = 0$. Hence, $g(x) = f^*(x)$ is the minimal polynomial of a^{-1}. Furthermore, $g(x-1)$ is irreducible over F and $g(x-1)$ is the minimal polynomial of $1 + a^{-1}$.

補充. 這題跟20.36重複了。

21.42 Suppose K is an extension of F of degree n. Prove that K can be written in the form $F(x_1, x_2, ..., x_n)$ for some $x_1, x_2, ..., x_n$ in K.

Proof. Select a basis $\{x_1, x_2, ..., x_n\}$ for K over F. ■

thm.21.5 Let K be a finite extension of the field F and let L be a finite extension of the field K. Prove that

$$[L : F] = [L : K][K : F].$$

Proof. Suppose that $\{v_1, v_2, ..., v_m\}$ is a basis for L over K and $\{w_1, w_2, ..., w_n\}$ is a basis for K over F. For any $v \in L$, suppose that $v = \sum_{i=1}^{m} k_i v_i$. For each k_i, suppose that $k_i = \sum_{j=1}^{n} f_{ij} w_j$, where $f_{ij} \in F$. Then

$$v = \sum_{i=1}^{m} k_i v_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} f_{ij} w_j \right) v_i = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} (w_j v_i) = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} (v_i w_j).$$

Thus, $S = \{v_i w_j \mid i = 1, 2, ..., m,\ j = 1, 2, ..., n\}$ generate L over F.

If $0 = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij}(v_i w_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij}(w_j v_i) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} f_{ij} w_j \right) v_i$, since $\{v_1, v_2, ..., v_m\}$ is linearly independent over K and $\sum_{j=1}^{n} f_{ij} w_j \in K$ for each i, we have $\sum_{j=1}^{n} f_{ij} w_j = 0$ for each $i = 1, 2, ..., m$. Since $\{w_1, w_2, ..., w_n\}$ is linearly independent over F and $f_{ij} \in F$, we have $f_{i1} = f_{i2} = \cdots = f_{in} = 0$ for each $i = 1, 2, ..., m$. Thus, $f_{ij} = 0$ for all $i = 1, 2, ..., m$ and $j = 1, 2, ..., n$. Therefore, S is linearly independent over F and S is a basis for L over F. It follows that $[L : F] = |S| = mn = [L : K][K : F]$. ■

Foote, p.541, exa.) Let p be a prime. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^p - 2$.

Proof. Since $x^p - 2 = (x - \sqrt[p]{2})(x - \sqrt[p]{2}\omega_p)(x - \sqrt[p]{2}\omega_p^2) \cdots (x - \sqrt[p]{2}\omega_p^{p-1})$. The splitting field for $x^p - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[p]{2}, \omega_p)$.

By Eisenstein's criterion with prime 2, $x^p - 2$ is irreducible over $\mathbb{Q}$. Hence, $[\mathbb{Q}(\sqrt[p]{2} : \mathbb{Q}] = \deg(x^p - 2) = p$.

We know that $\Phi_p(x)$ is the minimal polynomial of ω_p over $\mathbb{Q}$, so $[\mathbb{Q}(\omega_p) : \mathbb{Q}] = \deg \Phi_p(x) = p - 1$.

Since ω_p is a root of $\Phi_p(x)$ over $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[p]{2})$, we have $[\mathbb{Q}(\sqrt[p]{2}, \omega_p) : \mathbb{Q}(\sqrt[p]{2})] \leq \deg \Phi_p(x) = p - 1$. Thus,

$$[\mathbb{Q}(\sqrt[p]{2}, \omega_p) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[p]{2}, \omega_p) : \mathbb{Q}(\sqrt[p]{2})] \cdot [\mathbb{Q}(\sqrt[p]{2} : \mathbb{Q}] \leq p(p-1).$$

[4] `http://math.stackexchange.com/questions/1758745/prove-that-fx-is-irreducible-iff-its-reciprocal-`

On the other hand, since

$$p = [\mathbb{Q}(\sqrt[p]{2} : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}, \omega_p) : \mathbb{Q}]$$

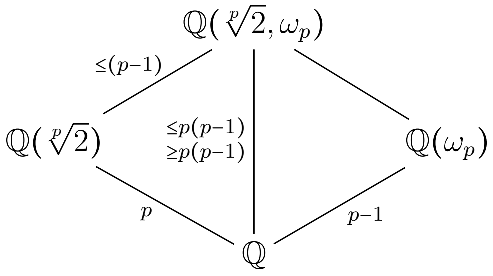
and

$$p - 1 = [\mathbb{Q}(\omega_p) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}, \omega_p) : \mathbb{Q}]$$

and $\gcd(p, p-1) = 1$, we have

$$p(p-1) \mid [\mathbb{Q}(\sqrt[p]{2}, \omega_p) : \mathbb{Q}].$$

Therefore, $[\mathbb{Q}(\sqrt[p]{2}, \omega_p) : \mathbb{Q}] = p(p-1)$.



■

22 Chapter 22

題組 $GF(p^n)^*$ is a cyclic group

22.4, 22.17, 22.19, 22.18, 22.15, 22.35, 22.8, 22.22, 22.41, 22.24, 22.7, 22.42, 22.43, 22.44

題組 Computational Exercises

22.23, 22.5, 22.6, 22.9, 22.20, 22.16

題組 Existence of Finite Field

22.27, 22.37, 22.25

題組 Uniqueness of Finite Field

22.10

題組 Advanced Exercises

22.11, 22.33, 22.39, 22.21, 22.32, 22.36

題組 Polynomial and Its Root

22.31, 補充 22.A

題組 $x^{p^n} - x$

補充 22.B, 補充 22.C, 補充 22.E, 22.26, 22.30, 22.40

22.1 Find $[GF(729) : GF(9)]$ and $[GF(64) : GF(8)]$.

Proof. By Exercise 22.2, $[GF(729):GF(9)]=3$, $[GF(64):GF(8)]=2$. ■

22.2 If m divides n, show that $[GF(p^n):GF(p^m)]=n/m$.

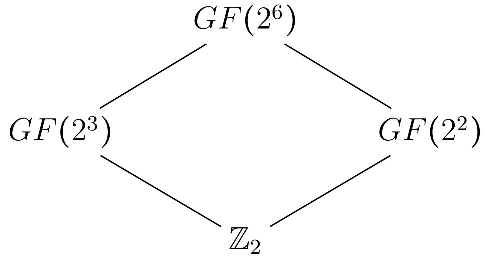
Proof. Consider the tower of fields

$$\overbrace{\mathbb{Z}_p \underbrace{\le}_{m} GF(p^m) \le GF(p^n)}^{n}.$$

■

22.3 Draw the lattice of subfields of $GF(64)$.

Proof.



■

22.4 Let α be a zero of x^3+x^2+1 in some extension field of $\mathbb{Z}_2$. Find the multiplicative inverse of $\alpha+1$ in $\mathbb{Z}_2[\alpha]$.

Proof. [方法一]

$$\begin{aligned}
& \alpha^3+\alpha^2+1=0 \\
\Rightarrow\ & \alpha^3+\alpha^2=-1=1 \\
\Rightarrow\ & \alpha^2(\alpha+1)=1 \\
\Rightarrow\ & (\alpha+1)^{-1}=\alpha^2
\end{aligned}$$

[方法二] Since $\mathbb{Z}_2(\alpha)\cong\mathbb{Z}[x]/\langle x^3+x^2+1\rangle$ and $|\mathbb{Z}_2(\alpha)^*|=2^3-1=7$. By Lagrange's Theorem, we have $(\alpha+1)^7=1$ and $(\alpha+1)^{-1}=(\alpha+1)^6$. Note that $\alpha^3=\alpha^2+1$ and $\alpha^4=\alpha^3\alpha=(\alpha^2+1)\alpha=\alpha^3+\alpha=(\alpha^2+1)+\alpha$.

$$\begin{aligned}
(\alpha+1)^6 &= (\alpha+1)^4(\alpha+1)^2 \\
&= (\alpha^4+1)(\alpha^2+1) \\
&= (\alpha^2+\alpha+1+1)(\alpha^2+1) \\
&= (\alpha^2+\alpha)(\alpha^2+1) \\
&= \alpha^4+\alpha^3+\alpha^2+\alpha \\
&= (\cancel{\alpha^2+\alpha}+\cancel{1})+(\alpha^2+\cancel{1})+\cancel{\alpha^2+\alpha} \\
&= \alpha^2.
\end{aligned}$$

■

22.5 Let α be a zero of $f(x) = x^2 + 2x + 2$ in some extension field of $\mathbb{Z}_3$. Find the other zero of $f(x)$ in $\mathbb{Z}_3[\alpha]$.

Proof. Let α be the root of x^2+2x+2 in the extension field $\mathbb{Z}_3[x]/\langle x^2+2x+2\rangle \cong \mathbb{Z}_3(\alpha)$ of $\mathbb{Z}_3$.

$$\begin{array}{r|llll}
 & x & +(2+\alpha) & & \\
\hline
x-\alpha & x^2 & +2x & +2 & \\
 & x^2 & -\alpha x & & \\
\cline{2-3}
 & & (2+\alpha)x & +2 & \\
 & & (2+\alpha)x & -(2\alpha+\alpha^2) & \\
\cline{3-4}
 & & & 2+2\alpha+\alpha^2 & = 0
\end{array}$$

The other zero of $f(x)$ in $\mathbb{Z}_3(\alpha)$ is $-(2+\alpha) = -2-\alpha = 1+2\alpha$. ■

22.6 Let α be a zero of $f(x) = x^3 + x + 1$ in some extension field of $\mathbb{Z}_2$. Find the other zero of $f(x)$ in $\mathbb{Z}_2[\alpha]$.

Proof. $\alpha, \alpha^{2^1} = \alpha^2$ and $\alpha^{2^2} = \alpha^4 = \alpha^3 \cdot \alpha = (\alpha+1)\alpha = \alpha^2 + \alpha$ are all the zero of $f(x)$ in $\mathbb{Z}_2(\alpha)$. ■

補充. 這在 Exercise 20.10遇過了。

補充. If $f(x)$ is irreducible over $\mathbb{Z}_p$ and a is a root of $f(x)$ in the extension field $\mathbb{Z}_p(a) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$ of $\mathbb{Z}_p$, then a^p, a^{p^2}, a^{p^3}, ... are also roots of $f(x)$.

Proof. Since $\mathbb{Z}_p - \{0\}$ is a finite group under multiplication, by Lagrange's Theorem, for all $g \in \mathbb{Z}_p - \{0\}$, $g^{p-1} = 1$. Thus, $g^p = g$ and $g^{p^s} = ((g^{\overbrace{p})^p)^{\cdots})^p}^{s\text{ times}} = g$.

In addition, recall that if char $K = p$, then $(u+v)^p = u^p + v^p$ for every $u, v \in K$.

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $f(a) = 0$, then

$$\begin{aligned}
f(a^{p^s}) &= a_n(a^{p^s})^n + a_{n-1}(a^{p^s})^{n-1} + \cdots + a_1 a^{p^s} + a_0 \\
&\overset{\overset{a_i\in\mathbb{Z}_p}{\downarrow}}{=} a_n^{p^s}(a^{p^s})^n + a_{n-1}^{p^s}(a^{p^s})^{n-1} + \cdots + a_1^{p^s} a^{p^s} + a_0^{p^s} \\
&= a_n^{p^s}(a^n)^{p^s} + a_{n-1}^{p^s}(a^{n-1})^{p^s} + \cdots + a_1^{p^s} a^{p^s} + a_0^{p^s} \\
&\overset{\overset{a_i,\ a\in K\supseteq\mathbb{Z}_p}{\downarrow}}{=} (a_n a^n + a_{n-1}a^{n-1} + \cdots + a_1 a + a_0)^{p^s} \\
&= 0
\end{aligned}$$

22.7* Let K be a finite extension field of a finite field F. Show that there is an element a in K such that $K = F(a)$.

22.8 How many elements of the cyclic group $GF(81)^*$ are generators?

Proof. Suppose that $GF(81)^* = \langle a\rangle$. The element in $GF(81)^*$ is of the form a^s. Since $|GF(81)^*| = |a| = 80$ and $|a^s| = \frac{|a|}{\gcd(|a|,s)} = \frac{80}{\gcd(80,s)}$, a^s is a generator of $GF(81)^*$ if and only if $|a^s| = \frac{80}{\gcd(80,s)} = 80$ if and only if $\gcd(80,s) = 1$. The number of such s is $\phi(80) = \phi(2^4\cdot 5) = 80\cdot(1-\frac{1}{2})\cdot(1-\frac{1}{5}) = 32$, where ϕ is the Euler phi function. ■

22.9 Let $f(x)$ be a cubic irreducible over $\mathbb{Z}_2$. Prove that the splitting field of $f(x)$ over $\mathbb{Z}_2$ has order 8.

Proof. **Lemma.** Suppose that $\deg f(x) \in \{2,3\}$, $f(x)$ is irreducible over F if and only if $f(x)$ has no root in F.

We use the Lemma to find all the monic irreducible cubic polynomials over $\mathbb{Z}_2$.

$$\begin{array}{lllll}
x^3 & & & & \text{has root } 0 \\
x^3 & & & +1 & \text{has root } 1 \\
x^3 & & +x & & \text{has root } 0 \\
x^3 & & +x & +1 & \leftarrow \\
x^3 & +x^2 & & & \text{has root } 0 \\
x^3 & +x^2 & & +1 & \leftarrow \\
x^3 & +x^2 & +x & & \text{has root } 0 \\
x^3 & +x^2 & +x & +1 & \text{has root } 1
\end{array}$$

Therefore, $f(x) = x^3 + x + 1$ or $f(x) = x^3 + x^2 + 1$.

Let a be a root of $x^3 + x + 1$ in the extension field $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ of $\mathbb{Z}_2$. Then $x^3 + x + 1 = (x - a)(x - a^{2^1})(x - a^{2^2}) = (x - a)(x - a^2)(x - (a^2 + a))$.

Similarly, let b be a root of $x^3 + x^2 + 1$ in the extension field $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$ of $\mathbb{Z}_2$. Then $x^3 + x^2 + 1 = (x - b)(x - b^{2^1})(x - b^{2^2}) = (x - b)(x - b^2)(x - (b^2 + b + 1))$. ∎

22.10 Prove that the rings $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$ and $\mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle$ are isomorphic.

Proof. The finite field $GF(p^n)$ is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. By the uniqueness of the splitting field, if two finite fields have the same order, then they are isomorphic.

Verify that x^2+x+2 and x^2+2x+2 have no root in $\mathbb{Z}_3$. Thus, x^2+x+2 and x^2+2x+2 are irreducible over $\mathbb{Z}_3$. Hence, $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$ and $\mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle$ both are field and $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle \cong GF(2^3) \cong \mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle$. ∎

22.11 Show that the Frobenius mapping $\phi : GF(p^n) \to GF(p^n)$, given by $a \to a^p$, is a ring automorphism of order n (that is, ϕ^n is the identity mapping).

Proof. $\phi(ab) = (ab)^p \overset{\text{the multiplication in a field is commutative}}{\overset{\downarrow}{=}} a^p b^p = \phi(a)\phi(b)$.

Note that if p is a prime, then $p \mid \binom{p}{i}$ for $i = 1, 2, \ldots, p-1$.

$$\begin{aligned}
\phi(a+b) &= (a+b)^p \\
&\overset{\text{binomial theorem}}{\overset{\downarrow}{=}} \binom{p}{0}a^p b^0 + \cancel{\binom{p}{1}a^{p-1}}b^1 + \cancel{\binom{p}{2}a^{p-2}}b^2 + \cdots + \cancel{\binom{p}{p-1}a^1 b^{p-1}} + \binom{p}{p}a^0 b^p \\
&\overset{\text{char } GF(p^n)=p}{\overset{\downarrow}{=}} \binom{p}{0}a^p + \binom{p}{p}b^p \\
&= a^p + b^p \\
&= \phi(a) + \phi(b).
\end{aligned}$$

Therefore, ϕ is a homomorphism.

We know that $\ker\phi$ is an ideal of $GF(p^n)$, but an ideal of a field F must be $\{0\}$ or F itself. Since ϕ is not zero mapping, we have $\ker\phi \neq GF(p^n)$ and $\ker\phi = \{0\}$ and ϕ is one-to-one. On the other hand, since the number of the elements in the domain of ϕ is the same as the codomain of ϕ and ϕ is one-to-one, we get ϕ is onto. That is, ϕ is an isomorphism.

For any $a \in F$, if $a = 0$, then $\phi^n(a) = \phi^n(0) = 0 = a$. If $a \neq 0$, then $a \in GF(p^n)^*$. By Lagrange's Theorem, $|a|$ divides $|GF(p^n)^*| = p^n - 1$ and $a^{p^n-1} = 1$ and $a^{p^n} = a$. Then $\phi^n(a) = ((a\overbrace{^p)^p)^{\cdots})^p}^{n \text{ times}} = a^{p^n} = a$. That is, ϕ^n is the identity mapping. ■

22.12 Determine the possible finite fields whose largest proper subfield is $GF(2^5)$.

Proof. $GF(2^{10}), GF(2^{15}), GF(2^{25})$. ■

22.13 Prove that the degree of any irreducible factor of $x^8 - x$ over $\mathbb{Z}_2$ is 1 or 3.

Proof. We know that the splitting field of $x^8 - x = x^{2^3} - x$ is $GF(2^3)$. Let $f(x)$ be a irreducible factor of $x^8 - x$ over $\mathbb{Z}_2$. Then $f(x)$ splits in $GF(2^3)$ as well. Hence, we have $\mathbb{Z}_2[x]/\langle f(x)\rangle \cong F$ and a tower of fields

$$\overbrace{\mathbb{Z}_2 \leq F \leq GF(2^3)}^{3}.$$

Thus, $F \cong \mathbb{Z}_2$ or $F \cong GF(2^3)$ and $\deg f(x) \in \{1, 3\}$. ■

補充. 這題有另外的解法, 參考補充題。

22.14 Find the smallest field that has exactly 6 subfields.

Proof. $GF(2^{12})$. ■

22.15 Find the smallest field of characteristic 2 that contains an element whose multiplicative order is 5 and the smallest field of characteristic 3 that contains an element whose multiplicative order is 5.

Proof. $GF(2^4), GF(3^4)$.

For the first part of the question, it is sufficient to find the smallest n such that $5 \mid (2^n - 1)$. Then $GF(2^n)^* = \langle a\rangle$ and $|a^{\frac{2^n-1}{5}}| = 5$. The second part is similarly. ■

22.16 Verify that the factorization for $f(x) = x^3 + x^2 + 1$ over $\mathbb{Z}_2$ given in Example 2 is correct by expanding.

22.17 Show that x is a generator of the cyclic group $(\mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle)^*$.

Proof. Let $F = \mathbb{Z}_3[x]/\langle x^3+2x+1\rangle$. Since $|F^*| = 3^3 - 1 = 26$, by Lagrange's Theorem, $|x|$ divide 26 and $|x| \in \{1, 2, 13, 26\}$.

Note that $x^3 = -2x - 1 = x + 2$ and $x^4 = x \cdot x^3 = x(x+2) = x^2 + 2x$.

$$\begin{aligned} x^{12} &= (x^4)^3 \\ &= (x^2+2x)^3 \\ &= x^6 + 8x^3 \\ &= x^6 + 2x^3 \\ &= x^2 \cdot x^4 + 2(x+2) \\ &= x^2(x^2+2x) + 2x + 4 \\ &= x^4 + 2x^3 + 2x + 1 \\ &= (x^2+2x) + 2(x+2) + 2x + 1 \\ &= x^2 + 5 \\ &= x^2 + 2. \end{aligned}$$

$x^{13} = x \cdot x^{12} = x(x^2+2) = x^3 + 2x = (x+2) + 2x = 2 \neq 1$. That is, $|x| \neq 13$. Thus, $|x| = 26$ and x is a generator of F^*. ■

22.18 Suppose that $f(x)$ is a fifth-degree polynomial that is irreducible over $\mathbb{Z}_2$. Prove that x is a generator of the cyclic group $(\mathbb{Z}_2[x]/\langle f(x)\rangle)^*$.

Proof. Let $F = \mathbb{Z}_2[x]/\langle f(x)\rangle$. Then $|F^*| = 2^5 - 1 = 31$. By Lagrange's Theorem, $|x|$ divides $|F^*| = 31$. Therefore, $|x| = 31$ and x is a generator of F^*. ■

22.19 Show that x is not a generator of the cyclic group $(\mathbb{Z}_3[x]/\langle x^3+2x+2\rangle)^*$.

Proof. Let $F = \mathbb{Z}_3[x]/\langle x^3+2x+2\rangle$. Then $|F^*| = 3^3 - 1 = 26$. Note that $x^3 = -2x - 2 = x + 1$ and $x^9 = (x^3)^3 = (x+1)^3 = x^3 + 1 = (x+1) + 1 = x + 2$.

$$\begin{aligned} x^{12} &= x^9 \cdot x^3 \\ &= (x+2)(x+1) \\ &= x^2 + 2. \end{aligned}$$

$x^{13} = x \cdot x^{12} = x(x^2+2) = x^3 + 2x = (x+1) + 2x = 1$. That is, $|x| = 13$ and x is not a generator of F^* ■

22.20 If $f(x)$ is a cubic irreducible polynomial over $\mathbb{Z}_3$, prove that either x or $2x$ is a generator for the cyclic group $(\mathbb{Z}_3[x]/\langle f(x)\rangle)^*$.

Proof. If we want to prove that ($A \Rightarrow B$ or C), we can suppose that A and $\neg B$, then prove C.

Let $F = \mathbb{Z}_3[x]/\langle f(x)\rangle$. Then $|F^*| = 3^3 - 1 = 26$. By Lagrange's Theorem, $|x|$ divides $|F^*| = 26$ and $|x| \in \{1, 2, 13, 26\}$. Since $x \neq 1$ and $x^2 \neq 1$, if x is not a generator of F^*, then $|x| = 13$. It follows that $(2x)^2 = 4x^2 = x^2 \neq 1$ and $(2x)^{13} = 2x^{13} = 2 \neq 1$ because $2^{13} = (2^2)^6 \cdot 2 = 4^6 \cdot 2 \equiv 1^6 \cdot 2 = 2 \pmod 3$. Therefore, $|2x| = 26$. ■

22.21 Prove the uniqueness portion of Theorem 22.3 using a group theoretic argument.

Proof. ■

22.22 Suppose that α and β belong to $GF(81)^*$, with $|\alpha| = 5$ and $|\beta| = 16$. Show that $\alpha\beta$ is a generator of $GF(81)^*$.

Proof. We already know that $(\alpha\beta)^{80} = (\alpha^5)^{16}(\beta^{16})^5 = 1$. Hence, $|\alpha\beta| \leq 80$.

Consider the multiplicative groups $\langle\alpha\rangle$ and $\langle\beta\rangle$. By Lagrange's Theorem, if $c \in \langle\alpha\rangle \cap \langle\beta\rangle$, then $|c|$ divides $|\langle\alpha\rangle| = |\alpha| = 5$ and $|\langle\beta\rangle| = |\beta| = 16$. It follows that $|c| = 1$ and $c = 1$. That is, $\langle\alpha\rangle \cap \langle\beta\rangle = \{1\}$.

If $(\alpha\beta)^s = 1$, then $\alpha^s = \beta^{-s} \in \langle\alpha\rangle \cap \langle\beta\rangle$ and $\alpha^s = 1 = \beta^s$. It follows that $|\alpha| = 5$ divides s and $|\beta| = 16$ divides s. Since $\gcd(5, 16) = 1$, we have $5 \cdot 16 = 80$ divides s. When $s = |\alpha\beta|$, 80 divides $s = |\alpha\beta|$ and $80 \leq |\alpha\beta|$.

■

22.23 Construct a field of order 9 and carry out the analysis as in Example 1,

Proof. $\mathbb{Z}_3[x]/\langle x^2 + 2x + 1\rangle$. ■

22.24 Show that any finite subgroup of the multiplicative group of a field is cyclic.

Proof.

$$\begin{array}{cl}
 & G \leq F^*,\ |G| < \infty \\
\overset{\substack{F^* \text{ is abelian} \\ \downarrow}}{\Rightarrow} & G \text{ is a finite abelian group} \\
\overset{\substack{\text{Fundamental Theorem of} \\ \text{Finite Abelian Group} \\ \downarrow}}{\Rightarrow} & G \cong \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{r_s}},\ p_1, p_2, \ldots, p_s \text{ do not necessarily distinct} \\
\overset{\substack{\text{let } l = \text{lcm}(p_1^{r_1}, p_2^{r_2}, \ldots, p_s^{r_s}) \\ \downarrow}}{\Rightarrow} & \forall g \in G,\ g^l = 1 \text{ and } l \leq p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} \\
\Rightarrow & \text{every element in } G \text{ is a root of the polynomial } x^l - 1 \text{ over } \mathbb{Z}_p \\
\overset{\substack{x^l - 1 \text{ has at most } l \text{ roots} \\ \downarrow}}{\Rightarrow} & |G| \leq l \\
\Rightarrow & |G| = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} \leq l \\
\Rightarrow & p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} = l = \text{lcm}(p_1^{r_1}, p_2^{r_2}, \ldots, p_s^{r_s}) \\
\Rightarrow & \gcd(p_1^{r_1}, p_2^{r_2}, \ldots, p_s^{r_s}) = 1 \\
\Rightarrow & p_1, p_2, \ldots, p_s \text{ are distinct} \\
\Rightarrow & G \cong \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{r_s}} \cong \mathbb{Z}_{p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}} \text{ is cyclic}
\end{array}$$

■

22.25 Show that the set K in the proof of Theorem 22.3 is a subfield.

22.26 If $g(x)$ is irreducible over $GF(p)$ and $g(x)$ divides $x^{p^n} - x$, prove that $\deg g(x)$ divides n.

Proof. Let E be the splitting field of $g(x)$ over $\mathbb{Z}_p$. Then there exists $F \cong \mathbb{Z}_p[x]/\langle g(x)\rangle$ such that $F \le E$.

In addition, recall that the splitting field of $x^{p^n} - x$ is $GF(p^n)$. Since $g(x)$ divides $x^{p^n} - x$, all the roots of $g(x)$ is also a root of $x^{p^n} - x$. Thus, $E \le GF(p^n)$.

Therefore, we have a tower of fields

$$\overbrace{\mathbb{Z}_p \underbrace{\le}_{\deg g(x)} F \le E \le GF(p^n)}^{n}$$

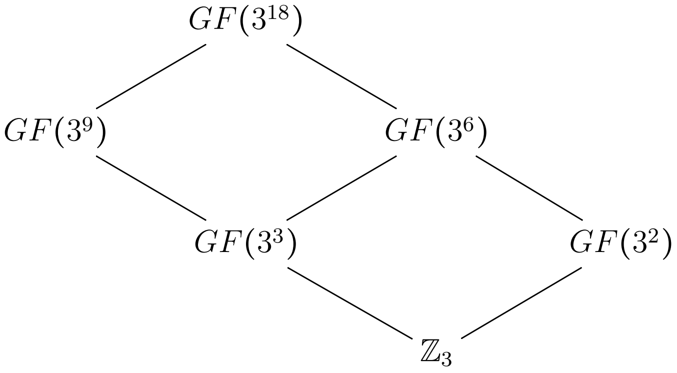
and $\deg g(x) \mid n$. ■

22.27 Use a purely group theoretic argument to show that if F is a field of order p^n, then every element of F^* is a zero of $x^{p^n} - x$.

Proof. By Lagrange's Theorem, for any $a \in F^*$, $|a|$ divides $|F^*| = p^n - 1$. That is, $a^{p^n-1} = 1$ and $a^{p^n} = a$. ■

22.28 Draw the subfield lattices of $GF(3^{18})$ and of $GF(2^{30})$.

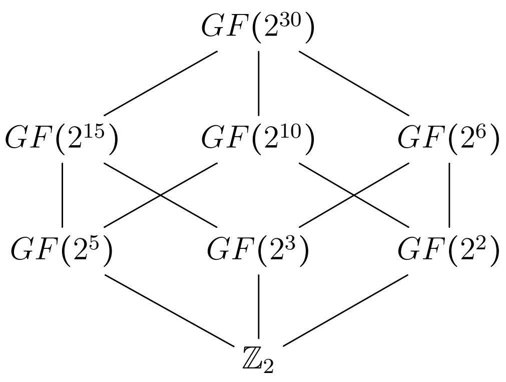
Proof.



■

22.29 How does the subfield lattice of $GF(2^{30})$ compare with the subfield lattice of $GF(3^{30})$?

Proof.



■

22.30* If $p(x)$ is a polynomial in $\mathbb{Z}_p[x]$ with no multiple zeros, show that $p(x)$ divides $x^{p^n} - x$ for some n.

Proof. Let E be the splitting field of $p(x)$ over $\mathbb{Z}_p$. Suppose that $p(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_{\deg p(x)}) \in E[x]$. By Exercise 21.20, Suppose that $[E : \mathbb{Z}_p] = n$. Then $E = GF(p^n)$. Since the elements in $E = GF(p^n)$ are roots of $x^{p^n} - x$, we get $\alpha_1, \alpha_2, \ldots, \alpha_{\deg p(x)}$ also are roots of $x^{p^n} - x$. That is, $p(x) \mid (x^{p^n} - x)$. ∎

22.31 Suppose that p is a prime and $p \neq 2$. Let a be a nonsquare in $GF(p)$—that is, a does not have the form b^2 for any b in $GF(p)$. Show that a is a nonsquare in $GF(p^n)$ if n is odd and that a is a square in $GF(p^n)$ if n is even.

Proof. Since a is a nonsquare in $\mathbb{Z}_p$, $x^2 - a$ has no root in $\mathbb{Z}_p$. Then $x^2 - a$ is irreducible over $\mathbb{Z}_p$ because $\deg(x^2 - a) = 2$. We have a field $F \cong \mathbb{Z}_p[x]/\langle x^2 - a\rangle$ such that $[F : \mathbb{Z}_p] = 2$. ∎

22.32 Let $f(x)$ be a cubic irreducible over $\mathbb{Z}_p$, where p is a prime. Prove that the splitting field of $f(x)$ over $\mathbb{Z}_p$ has order p^3 or p^6.

Proof. Let a be a root of $f(x)$ in the extension fields of $\mathbb{Z}_p(a) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$ of $\mathbb{Z}_p$. Suppose that $f(x) = (x - a)g(x)$.

If $g(x)$ has a root in $\mathbb{Z}_p(a)$, then $g(x)$ splits in $\mathbb{Z}_p(a)$ because $\deg g(x) = 2$. Thus, $\mathbb{Z}_p(a)$ is the splitting field for $f(x)$ and $[\mathbb{Z}_p(a) : \mathbb{Z}_p] = \deg f(x) = 3$ and $|\mathbb{Z}_p(a)| = p^3$.

If $g(x)$ has no root in $\mathbb{Z}_p(a)$, then $g(x)$ is irreducible over $\mathbb{Z}_p(a)$ because $\deg g(x) = 2$. Let b be a root of $g(x)$ in the extension field $\mathbb{Z}_p(a)(b) \cong \mathbb{Z}_p(a)[x]/\langle g(x)\rangle$ of $\mathbb{Z}_p(a)$. Then we have a tower of fields

$$\mathbb{Z}_p \underbrace{\leq}_{\deg f(x)=3} \mathbb{Z}_p(a) \underbrace{\leq}_{\deg g(x)=2} \mathbb{Z}_p(a)(b).$$

Therefore, $\mathbb{Z}_p(a)(b)$ is the splitting field for $f(x)$ over $\mathbb{Z}_p$ and $[\mathbb{Z}_p(a)(b) : \mathbb{Z}_p] = 6$ and $|\mathbb{Z}_p(a)(b)| = p^6$. ∎

補充. 參考補充題。

22.33 Show that every element of $GF(p^n)$ can be written in the form a^p for some unique a in $GF(p^n)$.

Proof. See Exercise 22.11. ϕ is onto. ∎

22.34 Suppose that F is a field of order 1024 and $F^* = \langle \alpha \rangle$. List the elements of each subfield of F.

Proof. The subfield lattice diagram is

$$\begin{tikzcd}
 & GF(2^{10}) \arrow[dl, dash] \arrow[dr, dash] & \\
GF(2^5) \arrow[dr, dash] & & GF(2^2) \arrow[dl, dash] \\
 & \mathbb{Z}_2 &
\end{tikzcd}$$

Since $F^* = \langle\alpha\rangle$, $|\alpha| = 1023 = 3\cdot 11\cdot 31$, we have $|\alpha^{33}| = 31$ and $|\alpha^{341}| = 3$. Thus, $GF(2^5) = \{0\}\cup\langle\alpha^{33}\rangle$ and $GF(2^2) = \{0\}\cup\langle\alpha^{341}\rangle$. ■

22.35 Suppose that F is a field of order 125 and $F^* = \langle\alpha\rangle$. Show that $\alpha^{62} = -1$.

Proof. Note that $|\alpha| = |F^*| = 125 - 1 = 124$. Recall that $|\alpha^s| = \frac{|\alpha|}{\gcd(|\alpha|,s)}$. Note that $|-1| = 2$. If $|\alpha^s| = \frac{|\alpha|}{\gcd(|\alpha|,s)} = \frac{124}{\gcd(124,s)} = 2$, then $\gcd(124,s) = 62$ and $s \mid 62$ and $s \equiv 62 \pmod{124}$. ■

22.36 Show that no finite field is algebraically closed.

22.37 Let E be the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Show that the set of zeros of $f(x)$ in E is closed under addition, subtraction, multiplication, and division (by nonzero elements).

Proof. Verify directly. ■

補充. This field is the finite field $GF(p^n)$.

22.38 Suppose that L and K are subfields of $GF(p^n)$. If L has p^s elements and K has p^t elements, how many elements does $L\cap K$ have?

Proof. $p^{\gcd(s,t)}$. ■

22.39 Give an example to show that the mapping $a\to a^p$ need not be an automorphism for arbitrary fields of prime characteristic p.

Proof. Consider the field $\mathbb{Z}_p(x)$. Then the mapping $a\to a^p$ is not onto. For if there exists $\frac{f(x)}{g(x)}\in\mathbb{Z}_p(x)$ such that $\left(\frac{f(x)}{g(x)}\right) = x$. Then $[f(x)]^p = x\cdot[g(x)]^p$ and

$$p\cdot\deg f(x) = \deg[f(x)]^p = \deg(x\cdot[g(x)]^p) = 1 + p\cdot\deg g(x).$$

Which is impossible. ■

22.40* In the field $GF(p^n)$, show that for every positive divisor d of n, $x^{p^n} - x$ has an irreducible factor over $GF(p)$ of degree d.

Proof. 參考補充 22.B 及補充 22.D ■

22.41 Let a be a primitive element for the field $GF(p^n)$, where p is an odd prime and n is a positive integer. Find the smallest positive integer k such that $a^k = p-1$.

Proof.

$$\begin{aligned} & a^k = p-1 = -1 \\ \Leftrightarrow\ & a^{2k} = 1 \\ \Leftrightarrow\ & 2k = p^n - 1 \\ \Leftrightarrow\ & k = \frac{p^n-1}{2} \end{aligned}$$

■

22.42* Let a be a primitive element for the field $GF(5^n)$, where n is a positive integer. Find the smallest positive integer k such that $a^k = 2$.

Proof.

$$\begin{aligned} & a^k = 2 \\ \Leftrightarrow\ & a^{2k} = 4 = -1 \\ \Leftrightarrow\ & a^{4k} = 1 \\ \Leftrightarrow\ & 4k = |GF(5^n)^*| = 5^n - 1 \\ \Leftrightarrow\ & k = \frac{5^n - 1}{4} \end{aligned}$$

■

22.43* Let p be a prime such that $p \pmod 4 = 1$. How many elements of order 4 are in $GF(p^n)^*$?

Proof. Observe the easy cases like $p = 5$, $n = 3$.

Suppose that $GF(p^n) = \langle a \rangle$. We want to find s such that $|a^s| = 4$. Since $|a^s| = \frac{p^n-1}{\gcd(s,p^n-1)} = 4 \Leftrightarrow \gcd(s, p^n - 1) = \frac{p^n-1}{4}$, we have $s = \frac{p^n-1}{4}k \le p^n - 1$ and $1 \le k \le 4$. Then

$$\gcd(s, p^n - 1) = \gcd(\frac{p^n - 1}{4}k, p^n - 1) = \gcd(\frac{p^n - 1}{4}k, \frac{p^n - 1}{4} \cdot 4).$$

$$\gcd(\frac{p^n - 1}{4}k, \frac{p^n - 1}{4} \cdot 4) = \frac{p^n - 1}{4} \Leftrightarrow k \in \{1, 3\}.$$

■

22.44* Let p be a prime such that $p \pmod 4 = 3$. How many elements of order 4 are in $GF(p^n)^*$?

補充 22.A Let a, b be elements of $GF(2^n)$, n odd. Show that $a^2 + ab + b^2 = 0$ implies $a = b = 0$.

Proof. If $b = 0$, then $a^2 = a^2 + ab + b^2 = 0$ and $a = 0$. If $b \neq 0$, then $a^2 + ab + b^2 = 0$ implies that $\left(\frac{a}{b}\right)^2 + \left(\frac{a}{b}\right) + 1 = 0$. That is, $\frac{a}{b}$ is a root of the irreducible polynomial $x^2 + x + 1$ over $\mathbb{Z}_2$ and $x^2 + x + 1$ is the minimal polynomial of $\frac{a}{b}$ over $\mathbb{Z}_2$. Therefore, we have a tower of fields

$$\overbrace{\mathbb{Z}_2 \underbrace{\le}_{2} \mathbb{Z}_2(\frac{a}{b}) \le GF(2^n)}^{n}.$$

Which is a contradiction because n is odd and $2 \nmid n$. ■

補充. 這題出現在 Lidl, p.79, exe.2.3.

補充 22.B Let $f(x)$ be an irreducible polynomial over $\mathbb{Z}_p$ of degree m. Then $f(x)$ divides $x^{p^n} - x$ if and only if m divides n.

Proof. (⇒) Let E be the splitting field of $f(x)$ over $\mathbb{Z}_p$. Then there exists $F \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$ such that $F \le E$.

In addition, recall that the splitting field of $x^{p^n} - x$ is $GF(p^n)$. Since $f(x)$ divides $x^{p^n} - x$, all the roots of $f(x)$ is also a root of $x^{p^n} - x$. Thus, $E \le GF(p^n)$.

Therefore, we have a tower of fields

$$\overbrace{\mathbb{Z}_p \underbrace{\le}_{m} F \le E \le GF(p^n)}^{n}$$

and $m \mid n$.

(⇐) Let a be a root of $f(x)$ in the extension field $\mathbb{Z}_p(a) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$ of $\mathbb{Z}_p$. Since $a \in \mathbb{Z}_p(a)^*$ and $|\mathbb{Z}_p(a)^*| = p^m - 1$, by Lagrange's Theorem, $a^{p^m - 1} = 1$ and $a^{p^m} = a$. Note that this identity also holds when $a = 0$. Assume that $n = ms$, then

$$a^{p^n} = a^{p^{ms}} = a^{\overbrace{p^m \cdot p^m \cdots p^m}^{s \text{ times}}} = \overbrace{((a^{p^m})^{p^m})^{\cdots})^{p^m}}^{s\text{ times}} = a.$$

That is, a is a root of $x^{p^n} - x$.

Since $f(x)$ is irreducible over $\mathbb{Z}_p$, either $f(x)$ divides $x^{p^n} - x$ or $\gcd(f(x), x^{p^n} - x) = 1$. If $\gcd(f(x), x^{p^n} - x) = 1$, then there exists $s(x)$ and $t(x)$ such that

$$f(x)s(x) + (x^{p^n} - x)t(x) = 1.$$

It follows that $0 = f(a)s(a) + (a^{p^n} - a)t(a) = 1$, a contradiction. Therefore, $f(x) \mid (x^{p^n} - x)$. ■

補充. 這個定理參考 Lidl, lem.2.13。

這個定理的 (⇐) 可以用來證明 Nicholson, p.304, 22.(a), 並更進一步證明 Fraleigh, p.305, 10。

這個定理的 (⇒) 可以用來證明 Gallian, p.396, 26及 Nicholson, p.304, 22.(b)。

這個定理的一個直接結果就是 Lidl, thm.3.20。

補充 22.C Factor $x^8 - x$ into irreducibles in $\mathbb{Z}_2[x]$.

補充. 這是 Nicholson, p304, 22.(c).

補充 22.D For any prime p and positive integer d, there exists an irreducible $f(x) \in \mathbb{Z}_p[x]$ with $\deg f(x) = d$.

Proof. Consider $F = GF(p^d)$. By Exercise 22.24, $(F - \{0\}, *) = \langle a\rangle$. Then $F = \mathbb{Z}_p(a)$. Let $m(x)$ be the minimal polynomial of a over $\mathbb{Z}_p$. Then $\deg m(x) = [\mathbb{Z}_p(a) : \mathbb{Z}_p] = [F : \mathbb{Z}_p] = [GF(p^d) : \mathbb{Z}_p] = d$. ■

補充 22.E For every finite field $\mathbb{Z}_p$ and every $n \in \mathbb{N}$, the product of all monic irreducible over $\mathbb{Z}_p$ whose degrees divide n is equal to $x^{p^n} - x$.

Proof. 參考補充 22.B。 ■

補充. 這個定理參考 Lidl, thm.3.20。

這個定理跟 Fraleigh, p.305, 13是一樣的。

23 Chapter 24

題組 orbit() divides $|G|$

24.63, 24.9

題組 Sylow 3rd Theorem

24.14, 24.17, 24.12, 24.22, 24.23, 24.24, 25.15, 24.27, 24.25

題組 Sylow 1st and 2nd Theorem

24.28, 24.46, 24.65, 24.55

題組 Internal Direct Product

24.26, 24.60, 24.33, 24.58, 24.20, 24.37, 24.19

題組 妙法蓮花 24.21, 24.18, 24.36, 24.64

題組 $n_p \in \{1, s\}, n_q \in \{1, t\}$

24.34

題組 $n_p = 1, n_q \in \{1, t\}$

24.39, 24.35

題組 Orbit-Stabilizer Theorem

24.44, 24.51, 24.71, 24.5, 24.3

題組 $H \triangleleft N(H)$

24.16

題組 $n_p = [G : N(H)]$

24.29

題組 Cauchy Theorem

24.54

題組 N/C Theorem (p.217)

24.69, 24.67, 24.68

題組 p-groups

24.41, 補充24.A, 補充24.B, 24.43, 24.50, 24.42

題組 Advanced Exercises

24.1, 24.62, 24.7, 24.40, 24.6, 24.8, 24.31, 24.11, 24.13, 24.30, 24.48, 24.49, 24.32, p.581, exe.3, 24.56, 24.47, 24.57, 24.52, 24.45, 24.66, 24.38, 24.59, 24.61

24.1 Show that conjugacy is an equivalence relation on a group.

Proof. We define a relation "∼" on a group G by

$$a \sim b \Leftrightarrow a \text{ is conjugate to } b \Leftrightarrow a = gbg^{-1} \text{ for some } g \in G.$$

Then

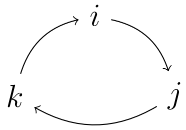
- $a = eae^{-1} \Rightarrow a \sim a.$
- $a \sim b \Rightarrow a = gbg^{-1} \Rightarrow b = (g^{-1})a(g^{-1})^{-1} \Rightarrow b \sim a.$
- $a \sim b, b \sim c \Rightarrow a = gbg^{-1}, b = hch^{-1} \Rightarrow a = (gh)c(h^{-1}g^{-1}) = (gh)c(gh)^{-1} \Rightarrow a \sim c.$

That is, "∼" is an equivalence relation on G. ■

補充. 由 Exercise 24.1及 Orbit-Stabilizer Theorem, 馬上就可以得到 Class Equation。

24.2 Calculate all conjugacy classes for the quaternions.

Proof. Quaternion Group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ 裡面的元素計算方法可以用下圖來記, 順時針的相鄰兩個元素相乘等於第三個元素, 逆時針的相鄰兩個元素相乘等於第三個元素的加法反元素。



$$\begin{aligned}
\text{orbit}(1) &= \{1\},\\
\text{orbit}(-1) &= \{-1\},\\
\text{orbit}(i) &= \{i, -i\},\\
\text{orbit}(j) &= \{j, -j\},\\
\text{orbit}(k) &= \{k, -k\}.
\end{aligned}$$

■

24.3 Show that the function T defined in the proof of Theorem 24.1 is well-defined, is one-to-one, and maps the set of left cosets onto the conjugacy class of a.

24.4 Show that $\text{orbit}(a) = \{a\}$ if and only if $a \in Z(G)$.

Proof. $\text{orbit}(a) = \{a\} \Leftrightarrow \forall g \in G, gag^{-1} = a \Leftrightarrow a \in Z(G).$ ■

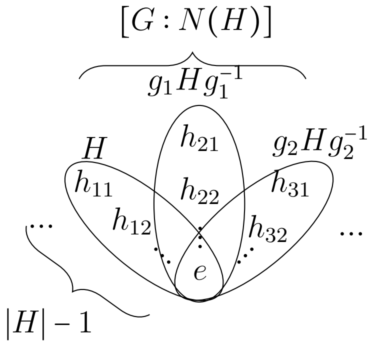
24.5 Let H be a subgroup of a group G. Prove that the number of conjugates of H in G is $|G : N(H)|$.

Proof. This is a special case of the Orbit-Stabilizer Theorem applies on the conjugation of G on the set of all subgroups of H. ■

補充. 由 Exercise 24.5及 Sylow 2nd Theorem, 馬上可以得到: If H is a Sylow p-subgroup of G, then $n_p = [G : N(H)]$.

24.6* Let H be a proper subgroup of a finite group G. Show that G is not the union of all conjugates of H.

Proof. Recall that the number of conjugate subgroup of H is $[G : N(H)]$. Note that $g_iHg_i^{-1} \cap g_jHg_j^{-1}$ not necessarily be $\{e\}$. But we want to consider the largest possible number of elements of $\bigcup_{g\in G} gHg^{-1}$, so we consider the following case.



That is, $g_iHg_i^{-1} \cap g_jHg_j^{-1} = \{e\}$. In this case,

$$\begin{aligned} |\bigcup_{g\in G} gHg^{-1}| &= 1 + [G : N(H)] \cdot (|H| - 1) \\ &\overset{\substack{H\le N(H)\le G \\ [G:H]\ge[G:N(H)] \\ \downarrow}}{\le} 1 + [G : H] \cdot (|H| - 1) \\ &= 1 + |G| - [G : H] \\ &\overset{\substack{H \text{ is proper} \\ [G:H]>1 \\ \downarrow}}{<} |G|. \end{aligned}$$

Even though the largest possible number of elements of $\bigcup_{g\in G} gHg^{-1}$, we still have $|\bigcup_{g\in G} gHg^{-1}| < |G|$. So $G \neq \bigcup_{g\in G} gHg^{-1}$. ■

補充. 記住兩件事, $H \cong gHg^{-1}$ and $|H| = |gHg^{-1}|$.

與 p.204, Exercise 9.64比較一下: Suppose that a group G has a subgroup of order n. Prove that the intersection of all subgroups of G of order n is a nornal subgroup of G.

Proof. If H is a subgroup of order n, we show that gHg^{-1} is also a subgroup of order n.

$e \in gHg^{-1}$ is clearly because $e = geg^{-1}$. If $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$, then

$$(gh_1g^{-1})(gh_2g^{-1}) = gh_1h_2g^{-1} \in gHg^{-1}$$

and

$$(gh_1g^{-1})^{-1} = gh_1^{-1}g \in gHg^{-1}.$$

Thus, gHg^{-1} is a subgroup of G. Define a mapping $f : H \to gHg^{-1}$ by $f(h) = ghg^{-1}$. Then f is onto and one-to-one. Therefore, H and gHg^{-1} have the same cardinality (the number of element).

Furthermore, if $gH_1g^{-1} = gH_2g^{-1}$, then $H_1 = g^{-1}gH_1g^{-1}g = g^{-1}gH_2g^{-1}g = H_2$. Thus, for any $g \in G$, if $\{H_i \mid i \in I\}$ is the set of all subgroup of G whose order is n, then $\{gH_ig^{-1} \mid i \in I\}$ is also the set of all subgroup of G whose order is n. It follows that

$$\bigcap_{|H|=n} H = \bigcap_{|H|=n} gHg^{-1}.$$

For any $x \in \bigcap_{|H|=n} H$ and $g \in G$,

$$gxg^{-1} \in \bigcap_{|H|=n} gHg^{-1} = \bigcap_{|H|=n} H.$$

That is, $\bigcap_{|H|=n} H \lhd G$. ■

24.7 If G is a group of odd order and $x \in G$, show that x^{-1} is not in orbit(x).

Proof. Suppose that $|G| = 2k+1$. Then by Lagrange's Theorem, for any $g \in G$, $|g|$ divides $|G|$ and $g^{2k+1} = g$.

$$\begin{array}{ll} \text{if} & x^{-1} \in \operatorname{orbit}(x) \\ \Rightarrow & x^{-1} = gxg^{-1} \text{ for some } g \in G \\ \Rightarrow & x = (x^{-1})^{-1} = (gxg^{-1})^{-1} = gx^{-1}g^{-1} = g^2xg^{-2} \\ \Rightarrow & x = g^2xg^{-2} = \cdots = g^{2k+2}xg^{-(2k+2)} = gxg^{-1} = x^{-1} \\ \Rightarrow & x^2 = 1 \\ \Rightarrow & |x| = 2 \text{ divides } |G|, \text{ a contradiction.} \end{array}$$

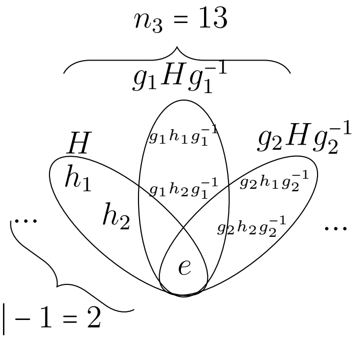
■

24.8* Determine the class equation for non-Abelian groups of orders 39 and 55.

Proof. Let G be a non-Abelian group of order 39. Note that $39 = 3 \cdot 13$. By Sylow 3rd Theorem and Exercise 24.14, $n_{13} \in \{1\}$ and $n_3 \in \{1, \cancel{4}, \cancel{7}, \cancel{10}, 13\}$. By Sylow 1st Theorem, a Sylow 13-subgroup in G is of order 13 and a Sylow 3-subgroup in G is of order 3.

If $n_3 = 1$, then let H be the only one Sylow 3-subgroup of G and K be the only one Sylow 13-subgroup of G. By Sylow 2nd Theorem, $H \lhd G$ and $K \lhd G$. Since $\gcd(|H|, |K|) = 1$, by Lagrange's Theroem, $H \cap K = \{e\}$. Since $|HK| = \frac{|H|\cdot|K|}{|H\cap K|} = \frac{13\cdot 3}{1} = 39 = |G|$, we have $HK = G$. Thus, G is the internal direct product of H and K. Then $G \cong H \oplus K \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{13} \cong \mathbb{Z}_{39}$, which is cyclic and abelian, contrary to the hypothesis. Therefore, $n_3 = 13$.

Let H be a Sylow 3-subgroup of G. By Sylow 2nd Theorem, all the Sylow 3-subgroup are conjugate each other. These 13 Sylow 3-subgroup are H, $g_1Hg_1^{-1}$, $g_2Hg_2^{-1}$, ..., $g_{12}Hg_{12}^{-1}$. Note that orbit$(h_1) \supseteq \{h_1, g_1h_1g_1^{-1}, g_2h_1g_1^{-1}, ..., g_{12}h_1g_{12}^{-1}\}$. Since orbit$(h_1)$ divides $|G|$ and $e \notin$ orbit(h_1), we have $|\text{orbit}(h_1)| = 11$ and orbit$(h_1) = \{h_1, g_1h_1g_1^{-1}, g_2h_1g_1^{-1}, ..., g_{12}h_1g_{12}^{-1}\}$. Similarly, orbit$(h_2) = \{h_2, g_1h_2g_1^{-1}, g_2h_2g_1^{-1}, ..., g_{12}h_2g_{12}^{-1}\}$. As the following figure indicates.



There are $39 - 2 \cdot 13 = 13$ elememts not in $H \cup g_1Hg_1^{-1} \cup g_2Hg_2^{-1} \cup \cdots \cup g_{12}Hg_{12}^{-1} - \{e\}$. These 13 elements form the only one Sylow 13-subgroup K of G. By Sylow 2nd Theorem, $K \triangleleft G$. Since $K \triangleleft G$, for any $k \in K$, $\text{orbit}(k) \subseteq K$. Select a fixed $k \neq e \in K$. Recall that $\text{orbit}(k)$ divides $|G|$. We claim that $\text{orbit}(k) = 3$.

If $|\text{orbit}(k)| = 39$, then $G = \text{orbit}(k) \subseteq K$, a contradiction.

If $|\text{orbit}(k)| = 13$, then $\text{orbit}(k) = K$ and $e \in K = \text{orbit}(k)$, which is impossible because $\text{orbit}(e) = \{e\} \cap \text{orbit}(k) = \varnothing$.

On the other hand, since G is not abelian, we have $G \neq Z(G)$ and $|Z(G)| \neq 39$. Since $Z(G)$ is a subgroup of G. By Lagrange's Theorm, $|Z(G)|$ divides $|G|$. If $|Z(G)| \in \{3, 13\}$, then $|G/Z(G)|$ is a prime and $G/Z(G)$ is a cyclic group and G is abelian and $G = Z(G)$, a contradiction. Thus, $|Z(G)| = 1$ and $Z(G) = \{e\}$. Therefore, $k \notin Z(G)$ and $|\text{orbit}(k)| \neq 1$.

Therefore, $|\text{orbit}(k)| = 3$. Suppose that $K - \{e\}$ is partition by the disjoint orbits $\text{orbit}(k_1)$, $\text{orbit}(k_2)$, $\text{orbit}(k_3)$ and $\text{orbit}(k_4)$. We have the class equation

$$\begin{aligned} |G| &= |Z(G)| + |\text{orbit}(h_1)| + |\text{orbit}(h_2)| + |\text{orbit}(k_1)| + |\text{orbit}(k_2)| + |\text{orbit}(k_3)| + |\text{orbit}(k_4)| \\ &= 1 + 13 + 13 + 3 + 3 + 3 + 3. \end{aligned}$$

■

24.9 Determine which of the equations below could be the class equation given in the proof of Theorem 24.2. For each part, provide your reasoning.

a. $9 = 3 + 3 + 3$
b. $21 = 1 + 1 + 3 + 3 + 3 + 3 + 7$
c. $10 = 1 + 2 + 2 + 5$
d. $18 = 1 + 3 + 6 + 8$

Proof. (a) Since $\{e\}$ is always a conjugacy class of G, 1 is always a term in the class equation.

(b) By Exercise 24.4, the number of 1 appear in the class equation is equal to $|Z(G)|$. In addition, since $Z(G)$ is a subgroup of G, by Lagrange's Theorem, $|Z(G)|$ divides $|G|$. But in the case (b), $\underbrace{1+1}_{2}$ does not divide 21.

(c) In D_5, the conjugacy classes are $\{1\}$, $\{a, a^4\}$, $\{a^2, a^3\}$, $\{b, ba, ba^2, ba^3, ba^4\}$.

(d) In this case, there is an element $x \in G$ such that $|\text{orbit}(x)| = 8$, which is a contradiction because $|\text{orbit}(x)| = 8$ does not divide $|G| = 18$. ■

24.10 Exhibit a Sylow 2-subgroup of S_4. Describe an isomorphism from this group to D_4.

Proof. Note that $|S_4| = 4! = 24 = 2^3 \cdot 3$. Let $a = (1234)$ and $b = (12)(34)$. Then $aba = b$ and $\langle a, b \rangle$ is a Sylow 2-subgroup of S_4 and $\langle a, b \rangle \cong D_4$. ■

24.11 Suppose that G is a group of order 48. Show that the intersection of any two distinct Sylow 2-subgorups of G has order 8.

Proof. Note that $48 = 2^4 \cdot 3$. Let H and K be two distinct Sylow 2-subgroup of G. Since $H \cap K \le H$, by Lagrange's Theorem, $|H \cap K|$ divides $|H| = 2^4 = 16$. Thus, $|H \cap K| \in \{1, 2, 4, 8, 16\}$. Since $H \ne K$, $|H \cap K| \ne 16$.

$$\text{If } \; |H \cap K| \le 4 \Rightarrow \frac{1}{|H \cap K|} \ge \frac{1}{4} \Rightarrow |HK| = \frac{|K| \cdot |K|}{|H \cap K|} \ge \frac{16 \cdot 16}{4} = 64 > |G|,$$

a contradiction. Therefore, $|H \cap K| = 8$. ■

補充. 類似的題目有 Fraleigh, p.331, exa.37.13, order 48; p.331, exa.37.14, order 36, 還要用到 $A \lhd B \le G \Rightarrow B \subseteq N(A)$.

1st, 24.12 Find all the Sylow 3-subgroups of S_4.

Proof. Note that $|S_4| = 4! = 24 = 2^3 \cdot 3$. By Sylow 3rd Theorem and Exercise 24.14, $n_3 \in \{1, 4, \cancel{7}\}$. By Sylow 1st Theorem, a Sylow 3-subgroup in S_4 is of order 3. All the Sylow 3-subgorups of S_4 are $\langle (123) \rangle$, $\langle (124) \rangle$, $\langle (134) \rangle$, and $\langle (234) \rangle$. ■

24.13 Let K be a Sylow p-subgroup of a finite group G. Prove that if $x \in N(K)$ and the order of x is a power of p, then $x \in K$.

Proof. Let $|G| = p^n m$, $p \nmid m$. Suppose that $|x| = p^s$. Recall that $K \lhd N(K) \le G$. Consider the factor group $N(K)/K$ and $xK \in N(K)/K$ and the tower of groups

$$\overbrace{K \lhd N(K) \underbrace{\le}_{n_p} G}^{m}.$$

Since $|xK|$ divides $|x| = p^s$ and $|xK|$ divides $|N(K)/K|$ and $|N(K)/K|$ divides m, we have $|xK| = 1$ and $xK = K$ and $x \in K$. ■

重要 24.14 Suppose that G is a group of order $p^n m$, where p is prime and p does not divide m. Show that the number of Sylow p-subgroups divides m.

Proof. By Sylow 3rd Theorem, $n_p \equiv 1 \pmod{p}$ and $n_p \mid |G| = p^n m$. Suppose that $n_p = ps + 1$ for some $s \in \mathbb{Z}$. Then $n_p = (ps + 1) \mid p^n m$ and $n_p \mid m$ because $\gcd(ps + 1, p) = 1$ and $\gcd(ps + 1, p^n) = 1$. ■

補充. 如果你熟悉 $H \le N(H)$ and $n_p = [G : N(H)]$, where H is a Sylow p-subgroup. 那麼這題可用如下解法更快速。Let H be a Sylow p-subgroup of G.

$$\overbrace{H \le N(H) \underbrace{\le}_{n_p} G}^{m}.$$

2nd, 24.15 Suppose that G is a group and $|G| = p^n m$, where p is prime and $p > m$. Prove that a Sylow p-subgroup of G must be normal in G.

Proof. By Sylow 3rd Theorem and Exercise 24.14, $n_p \in \{1\}$. By Sylow 2nd Theorem, the only one Sylow 7-subgroup is normal. ■

24.16 Let H be a Sylow p-subgroup of G. Prove that H is the only Sylow p-subgroup of G contained in $N(H)$.

Proof. If K is a Sylow p-subgroup of G and $K \leq N(H)$, then K is also a Sylow p-subgroup of $N(H)$.

Recall that $H \triangleleft N(H)$. By Sylow 2nd Theorem, H is the only one Sylow p-subgroup of $N(H)$.

Therefore, H is the only Sylow p-subgroup of G contained in $N(H)$. ■

24.17 Suppose that G is a group of order 168. If G has more than one Sylow 7-subgroup, exactly how many does it have?

Proof. Note that $168 = 2^3 \cdot 3 \cdot 7$. By Sylow 3rd Theorem and Exercise 24.14, $n_7 \in \{1, 8, \cancel{15}, \cancel{22}\}$. If $n_7 > 1$, then $n_7 = 8$. ■

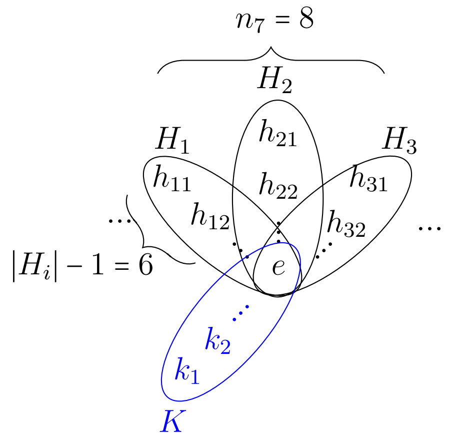
24.18 Show that every group of order 56 has a proper nontrivial normal subgroup.

Proof. Let G be a group of order 56. Note that $56 = 2^3 \cdot 7$. By Sylow 3rd Theorem and Exercise 24.14, $n_7 \in \{1, 8\}$. By Sylow 1st Theorem, a Sylow 7-subgroup in G is of order 7.

If $n_7 = 1$, then by Sylow 2nd Theorem, the only one Sylow 7-subgroup is normal and we are done.

If $n_7 = 8$, let $H_1, H_2, \ldots, H_8$ be all the Sylow 7-subgroups in G. By Lagrange's Theorem, $H_i \cap H_j = \{e\}$ for $i \neq j \in \{1, 2, \ldots, 8\}$ and for each $i \in \{1, 2, \ldots, 8\}$, if $h \neq e \in H_i$, then $|h| = 7$.

Thus, in each H_i, there are $|H_i| - 1 = 6$ elements of order 7. On the other hand, there are $n_7 = 8$ Sylow 7-subgroups. Thus, there are $6_{|H_i|-1} \cdot 8_{n_7} = 48$ elements of order 7. As the following figure indicates.



There are $56 - 48 = 8$ elements remaining (include identity e). These 8 elements form the only one Sylow 2-subgroup in G (by Sylow 1st Theorem). By Sylow 2nd Theorem, this only one Sylow 2-subgroup is normal. ■

補充. 這題也出現在 Nicholson, p.375, exa.7。order 992, 351, p^2q 也是同樣的方法。

24.19* What is the smallest composite (that is, nonprime and greater than 1) integer n such that there is a unique group of order n?

Proof. By Exercise 24.33, if $|G| = 15$, then $G \cong \mathbb{Z}_{15}$. The following table prove that 15 is the smallest composite integer n such that if $|G| = n$, then $G \cong \mathbb{Z}_{15}$.

$\lvert G\rvert$	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$G \cong$	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4$ $\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$\mathbb{Z}_5$	$\mathbb{Z}_6$ $S_3 \cong D_3$	$\mathbb{Z}_7$	$\mathbb{Z}_8$ $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ D_4 Q_8	$\mathbb{Z}_9$ $\mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_{10}$ D_5	$\mathbb{Z}_{11}$	$\mathbb{Z}_{12}$ $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ A_4 D_6 $\mathbb{Z}_3 \rtimes \mathbb{Z}_4 \cong Q_{12}$	$\mathbb{Z}_{13}$	$\mathbb{Z}_{14}$ D_7	$\mathbb{Z}_{15}$

■

24.20 Let G be a noncyclic group of order 21. How many Sylow 3-subgroups does G have?

Proof. $21 = 3 \cdot 7$. By Sylow 3rd Theorem and Exercise 24.14, $n_3 \in \{1, \cancel{4}, 7\}$ and $n_7 \in \{1\}$. By Sylow 2nd Theorem, there is only one Sylow 7-subgroup K of G and $K \lhd G$.

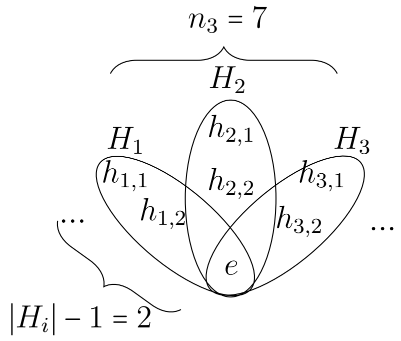
If $n_3 = 1$, then by Sylow 2nd Theorem, there is only one Sylow 3-subgroup H of G and $H \lhd G$. Since $\gcd(|H|, |K|) = 1$, by Lagrange's Theorem, we have $H \cap K = \{e\}$ and $|HK| = \frac{|H|\cdot|K|}{|H \cap K|} = \frac{3\cdot 7}{1} = 21 = |G|$. That is, $G = HK$. Therefore, G is the internal direct product of H and K and $G \cong H \oplus K \cong \mathbb{Z}_3 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{21}$. But G is not a cyclic group, which is a contradiction. Therefore, $n_3 = 7$. ■

24.21 Prove that a noncyclic group of order 21 must have 14 elements of order 3.

Proof. By Exercise 24.20, $n_3 = 7$. By Sylow 1st Theorem, a Sylow 3-subgroup in G is of order 3.

Let $H_1, H_2, \ldots, H_7$ be all the Sylow 3-subgroups in G. By Lagrange's Theorem, $H_i \cap H_j = \{e\}$ for $i \neq j \in \{1, 2, \ldots, 7\}$ and for each $i \in \{1, 2, \ldots, 7\}$, if $h \neq e \in H_i$, then $|h| = 3$.

Thus, in each H_i, there are $|H_i| - 1 = 2$ elements of order 3. On the other hand, there are $n_3 = 7$ Sylow 3-subgroups. Thus, there are $2_{|H_i|-1} \cdot 7_{n_3} = 14$ elements of order 3. As the following figure indicates.



■

1st, 24.22 How many Sylow 5-subgroups of S_5 are there? Exhibit two.

Proof. Note that $|S_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$. By Sylow 3rd Theorem and Exercise 24.14, $n_5 \in \{1, 6, \cancel{11}, \cancel{16}, \cancel{21}\}$. By Sylow 1st Theorem, a Sylow 5-subgroup in S_5 is of order 5. There are 6 Sylow 5-subgroups of S_5. $\langle(12345)\rangle$ and $\langle(12354)\rangle$ are two of them.

■

1st, 24.23 How many Sylow 3-subgroups of S_5 are there? Exhibit two.

Proof. Note that $|S_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$. By Sylow 3rd Theorem and Exercise 24.14, $n_3 \in \{1, 4, \cancel{7}, 10, \cancel{13}, \cancel{16}, \cancel{19}, \cancel{22}, \cancel{25}, \cancel{28}, \cancel{31}, \cancel{34}, \cancel{37}, 40\} = \{1, 4, 10, 40\}$. By Sylow 1st Theorem, a Sylow 3-subgroup in S_5 is of order 3. There are 10 Sylow 3-subgroups of S_5. $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(125)\rangle$, $\langle(134)\rangle$, $\langle(135)\rangle$, $\langle(145)\rangle$, $\langle(234)\rangle$, $\langle(235)\rangle$, $\langle(245)\rangle$, $\langle(345)\rangle$ are all of them.

■

1st, 24.24 What are the possibilities for the number of elements of order 5 in a group of order 100?

Proof. Let G be a group of order 100. Note that $100 = 2^2 \cdot 5^2$. By Sylow 3rd Theorem and Exercise 24.14, $n_5 \in \{1\}$. Let H be the only one Sylow 5-subgroup of G. By Sylow 1st Theorem, if $a \in G$ and $|a| = 5$, then $\langle a \rangle \leq H$.

By Sylow 1st Theorem, a Sylow 5-subgroup in G is of order $5^2 = 25$. By the corollary of Theorem 24.2, H is abelian. By the Fundamental Theorem of Finite Abelian Group, $H \cong \mathbb{Z}_{25}$ or $H \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5$. There are 4 elements of order 5 in $\mathbb{Z}_{25}$. There are 24 elements of order 5 in $\mathbb{Z}_5 \oplus \mathbb{Z}_5$. Therefore, the number of elements of order 5 in G might be 4 or 24. ■

補充. 從這題你應該注意到, Sylow p-subgroup 的 order 不一定是 p。一般來說, 如果 $|G| = p^n m$, $p \nmid m$, 則 Sylow p-subgroup in G 的 order 就是 p^n。

1st, 2nd, 24.25 What do the Sylow theorems tell you about any group of order 100?

Proof. Note that $100 = 2^2 \cdot 5^2$.
Sylow 1st Theorem: There is a subgroup of order 2 and a subgroup of order 5.
Sylow 3rd Theorem: $n_2 \in \{1, \cancel{3}, 5, \cancel{7}, \cancel{9}, \cancel{11}, \cancel{13}, \cancel{15}, \cancel{17}, \cancel{19}, \cancel{21}, \cancel{23}, 25\}$, $n_5 = 1$.
Sylow 2nd Theorem: The Sylow 5-subgroup is normal.

Note that a Sylow 2-subgroup in G is of order 4. The Sylow 5-subgroup in G is of order 25. ■

24.26 Prove that a group of order 175 is Abelian.

Proof. Note that $175 = 5^2 \cdot 7$. By Sylow 3rd Theorem and Exercise 24.14, $n_5 \in \{1, \cancel{6}\}$ and $n_7 \in \{1, \cancel{8}, \cancel{15}, \cancel{22}\}$. Let H be the only one Sylow 5-subgroup of G and K be the only one Sylow 7-subgroup of G. By Sylow 2nd Theorem, $H \lhd G$ and $K \lhd G$. Since $\gcd(|H|, |K|) = 1$, by Lagrange's Theroem, $H \cap K = \{e\}$. Since $|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{25 \cdot 7}{1} = 175 = |G|$, we have $HK = G$. Thus, G is the internal direct product of H and K. That is, $G \cong H \oplus K$.

Since $|H| = p^2$, by the Corollary of Theorem 24.2, H is abelian. Of course, $K \cong \mathbb{Z}_7$ is abelian. Therefore, $G \cong H \oplus K$ is abelian. ■

補充. 這題也出現在 Nicholson, p.374, exa.6。

重複 24.27 Let G be a group with $|G| = p^n m$, where p is a prime that does not divide m and $p \geq m$. Prove that the Sylow p-subgroup of G is normal.

Proof. See Exercise 24.15. ■

1st, 24.28 Determine the number of Sylow 2-subgroups of D_{2m}, where m is an odd integer at least 3.

Proof. By Sylow 1st Theorem, a Sylow 2-subgroup of D_{2m} is of order 2. There are m Sylow 2-subgroups of

$$D_{2m} = \{1, a, a^2, \ldots, a^{m-1}, b, ba, ba^2, \ldots, ba^{m-1} \mid |a| = m, |b| = 2, aba = b\}.$$

They are $\langle b \rangle$, $\langle ba \rangle$, $\langle ba^2 \rangle$, ...,$\langle ba^{m-1} \rangle$. ■

24.29 Let K be a Sylow 2-subgoup of D_{2m}, where m is an odd integer at least 3. Prove that $N(K) = K$.

Proof. By Exercise 24.28, $n_2 = m$. Consider the tower of groups

$$\overbrace{K \leq N(K) \underbrace{\leq}_{n_2 = m} D_{2m}}^{m}.$$

■

24.30* Generalize the argument given in Example 6 to obtain a theorem about groups of order $p^2 q$, where p and q are distinct primes.

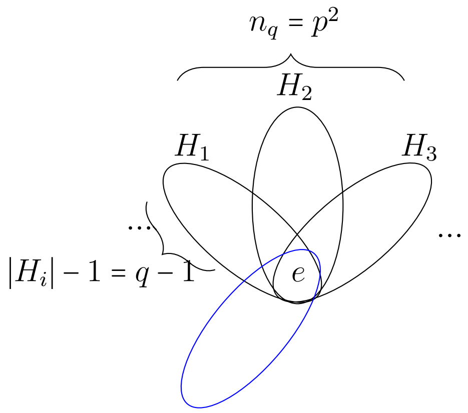
The theorem we generalize is as following: Let $|G| = p^2 q$, where p and q are distinct primes. Then G has either a normal Sylow p-subgroup or a normal Sylow q-subgroup. (C.f. Isaacs's *Finite Group Theory.*)

Proof. If $p > q$, then by Sylow 3rd Theorem, $n_p = 1$. By Sylow 2nd Theorem, the only one Sylow p-subgroup is normal in G.

If $p < q$, then by Exercise 24.14, $n_q \in \{1, p, p^2\}$. If $n_q = 1$, then we are done as the last case. If $n_q = p$, then by Sylow 3rd Theorem, $n_q = p \equiv 1 \pmod{q}$, which is impossible because $p < q$.

Suppose that $n_q = p^2$. Let $H_1, H_2, \ldots, H_{p^2}$ be all the Sylow q-subgroups in G. Note that the order of a Sylow q-subgroup is q (in this case). That is, $|H_i| = q$ for each $i = 1, 2, \ldots, p^2$. By Lagrange's Theorem, for any $h \neq e \in H_i$, we have $|h|$ divides $|H_i| = q$. Furthermore, $H_i \cap H_j = \{e\}$ for $i \neq j$. (If $e \neq h \in H_i \cap H_j$, then $|h| = q$ and $H_i = \langle h \rangle = H_j$, a contradiction.)

Now, in each H_i, there are $|H_i| - 1 = q - 1$ elements of order p^2. On the other hand, there are $n_q = p^2$ Sylow q-subgroups. Thus, there are $\underbrace{(q-1)}_{|H_i|-1} \cdot \underbrace{p^2}_{n_q} = p^2 q - p^2$ elements of order p^2. As the following figure indicates.



There are $p^2 q - (p^2 q - p^2) = p^2$ elements remaining (include identity e). These p^2 elements can't form the n_p Sylow p-subgroups. ■

24.31* What is the smallest possible odd integer that can be the order of a non-Abelian group?

Proof. 要用到 semidirect product。 ■

24.32 Prove that a group of order 375 has a subgroup of order 15.

Proof. Note that $375 = 3 \cdot 5^3$. By Sylow 3rd Theorem and Exercise 24.14, $n_3 \in \{1, \cancel{\cdots}, 25, \cancel{\cdots}\}$.

If $n_3 = 1$, then let H be the only one Sylow 3-subgroup of G. By Sylow 2nd Theorem, $H \lhd G$. Let K be a Sylow 5-subgroup of G. By Cauchy Theorem, there exists an element k in K such that $|k| = 5$. Let $L = \langle k \rangle$. Then HL is a subgroup of G (because $H \lhd G$) and

$$|HL| = \frac{|H| \cdot |L|}{|H \cap L|} = \frac{3 \cdot 5}{1} = 15.$$

If $n_3 = 25$, then let H be a Sylow 3-subgroup of G. Since $[G : N(H)] = n_3 = 25$, we have $|N(H)| = |G|/25 = 15$ and $N(H)$ is a subgroup of order 15. ■

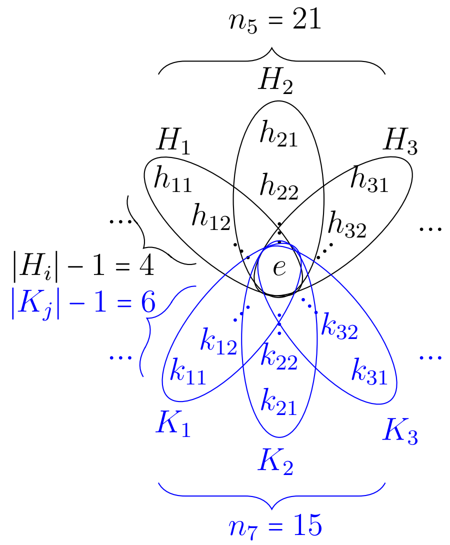
24.33 Without using Theorem 24.6, prove that a group of order 15 is cyclic.

Proof. See Exercise 24.26. ■

24.34 Prove that a group of order 105 contains a subgroup of order 35.

Proof. Note that $105 = 3 \cdot 5 \cdot 7$. By Sylow 3rd Theorem and Exercise 24.14, $n_5 \in \{1, \cancel{6}, \cancel{11}, \cancel{\cdots}, 21\}$ and $n_7 \in \{1, \cancel{8}, 15\}$.

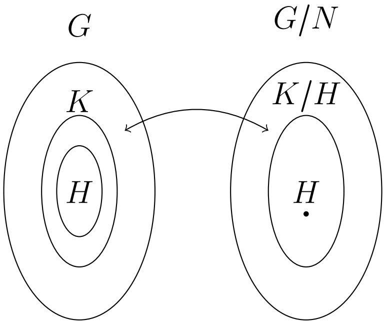
If $n_5 = 21$ and $n_7 = 15$, then there are $21 \cdot 4 = 84$ elements of order 5 and $15 \cdot 6 = 90$ elements of order 7, as the following figure indicates. The number of these elements exceed $|G|$, a contradiction. Therefore, either $n_5 = 1$ or $n_7 = 1$.



If $n_5 = 1$, then let H be the only one Sylow 5-subgroup of G. By Sylow 2nd Theorem, $H \lhd G$. By Cauchy Theorem or Sylow 1st Theorem, let K be a subgroup of order 7. Then HK is a subgroup of G and $|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = 35$. If $n_7 = 1$, then the argument is the same. ■

補充. 更多類似題目: Fraleigh, p.331, exa.37.12.

補充. 另解: If $n_5 = 1$, then by Sylow 2nd Theorem, the only one Sylow 5-subgroup H is normal. Consider the factor group G/H. Then $|G/H| = \frac{105}{5} = 3 \cdot 7$. In G/H, by Cauchy Theorem, there exists an element gH in G/H which is of order 7. Then $K/H = \langle gH \rangle$ is a subgroup of order 7 in G/H. By correspondence theorem, $K \leq G$ and $|K| = |K/H| \cdot |H| = 7 \cdot 5 = 35$.



If $n_7 = 1$, then we can use the same method to get a subgroup of order 35 in G.

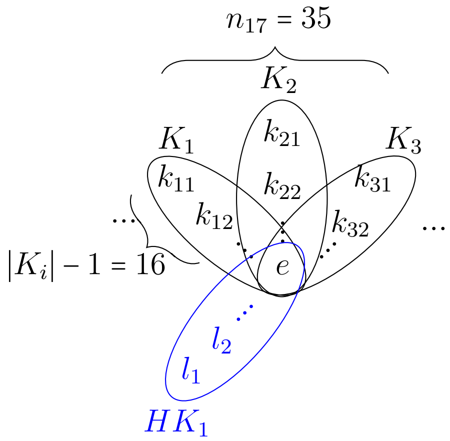
2nd, 24.35 Prove that a group of order 595 has a normal Sylow 17-subgroup.

Proof. Note that $595 = 5 \cdot 7 \cdot 17$. By Sylow 3rd Theorem and Exercise 24.14, we have $n_5 \in \{1, \cancel{6}, \cancel{11}, \cancel{16}, \cancel{\cdots}\}$ because $5 \nmid (17 \cdot 7 - 1)$. That is, $n_5 = 1$. Similarly, $n_{17} \in \{1, \cancel{18}, 35\}$. Let H be the only one Sylow 5-subgroup. By Sylow 2nd Theorem, $H \lhd G$.

If $n_{17} = 35$, let K_1, K_2, ..., K_{35} be these 35 Sylow 17-subgroups of G, then $K_1 \cup K_2 \cup \cdots \cup K_{35} - \{e\}$ contains $16 \cdot 35 = 560$ elements of order 17.

Since H is normal in G, HK_1 is also a subgroup of G and $|HK_1| = \frac{|H| \cdot |K_1|}{|H \cap K_1|} = 85$. By the method as in Exercise 24.33, HK_1 is a cyclic group.

Since $HK_1 \cong \mathbb{Z}_{85}$ has $\phi(85) = 64$ generators, we have 64 elements of order 85. Then there are $560 + 64 = 624$ elements in G, but $|G| = 595$, a contradiction. Therefore, $n_{17} = 1$ and by Sylow 2nd Theorem, the only one Sylow 17-subgroup is normal.



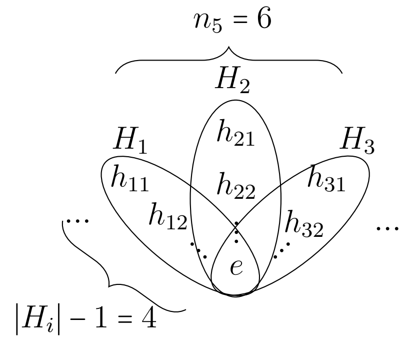
■

24.36 Let G be a group of order 60. Show that G has exactly four elements of order 5 or exactly 24 elements of order 5. Which of these cases holds for A_5?

Proof. Note that $60 = 2^2 \cdot 3 \cdot 5$. If $n_5 = 1$, let H be the only Sylow 5-subgroup of G, then there are 4 elements of order 5 in H. If there is another element a of order 5, by Sylow 1st Theorem, $|\langle a \rangle| = 5$ and $\langle a \rangle \subseteq H$. Thus, there are exactly 4 elements of order 5 in this case.

If $n_5 = 6$, let $H_1, H_2, ..., H_6$ be all the Sylow 5-subgroups in G. By Lagrange's Theorem, $H_i \cap H_j = \{e\}$ for $i \neq j \in \{1, 2, ..., 6\}$ and for each $i \in \{1, 2, ..., 6\}$, if $h \neq e \in H_i$, then $|h| = 5$.

Thus, in each H_i, there are $|H_i| - 1 = 4$ elements of order 5. On the other hand, there are $n_5 = 6$ Sylow 5-subgroups. Thus, there are $4_{|H_i|-1} \cdot 6_{n_5} = 24$ elements of order 5. As the following figure indicates.



By Sylow 3rd Theorem and Exercise 24.14, $n_5 \in \{1, 6, \cancel{11}\}$.

There are 24 elements of order 5 in A_5. They are (12345), (12354), (12435), (12453), (12534), ... ■

24.37* Show that the center of a group of order 60 cannot have order 4.

Proof. Let G be a group and $|G| = 60$ and $|Z(G)| = 4$. Since $Z(G) \lhd G$, consider the factor group $G/Z(G)$, $|G/Z(G)| = \frac{60}{4} = 15$. By Exercise 24.33, $G/Z(G)$ is cyclic, then by Theorem 9.3, G is abelian and $G = Z(G)$, a contradiction. ■

24.38 Suppose that G is a group of order 60 and G has a normal subgroup N of order 2. Show that

a. G has normal subgroups of order 6, 10, and 30.
b. G has subgroups of order 12 and 20.
c. G has a cyclic subgroup of order 30.

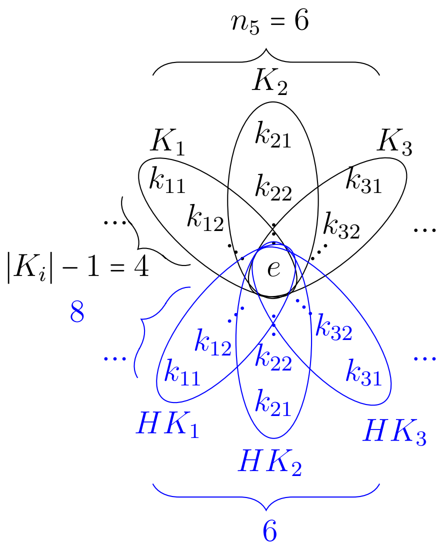
Proof. ■

24.39* Let G be a group of order 60. If the Sylow 3-subgroup is normal, show that the Sylow 5-subgroup is normal.

Proof. Note that $60 = 2^2 \cdot 3 \cdot 5$. By Sylow 3rd Theorem and Exercise 24.14, $n_5 \in \{1, 6, \cancel{11}\}$. Let H be the only one Sylow 3-subgroup. By Sylow 2nd Theorem, $H \lhd G$.

If $n_5 = 6$, let K_1, K_2, ..., K_6 be these six Sylow 5-subgroups of G, then $K_1 \cup K_2 \cup \cdots \cup K_6 - \{e\}$ contains $4 \cdot 6 = 24$ elements of order 5.

Since H is normal in G, for each $i = 1, 2, ..., 6$, HK_i is also a subgroup of G and $|HK_i| = \frac{|H| \cdot |K_i|}{|H \cap K_i|} = 15$. By Exercise 24.33, HK_i is a cyclic group. Note that $HK_i \cap HK_j$ does not necessarily be $\{e\}$. But we know that a generator of HK_i does not be in HK_j if $i \neq j$. Since $HK_i \cong \mathbb{Z}_{15}$ has $\phi(15) = 8$ generators, we have $8 \cdot 6 = 48$ elements of order 15. Then there are $24 + 48 = 72$ elements in G, but $|G| = 60$, a contradiction. Therefore, $n_5 = 1$ and by Sylow 2nd Theorem, the only one Sylow 5-subgroup is normal.

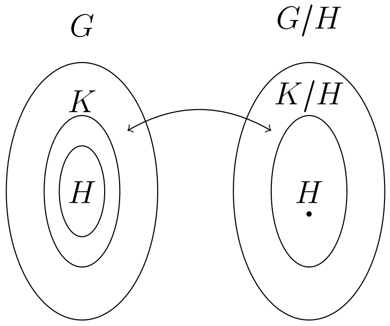


■

補充. 並不是每個元素都落在某個 Sylow p-subgroup 中。

correspondence theorem 24.40 Show that if G is a group of order 168 that has a normal subgroup of order 4, then G has a normal subgroup of order 28.

Proof. Note that $168 = 2^3 \cdot 3 \cdot 7$. Let H be a normal subgroup of order 4. Consider the factor group G/H. Then $|G/H| = \frac{168}{4} = 2 \cdot 3 \cdot 7$. In G/H, by Sylow 3rd Theorem and Exercise 24.14, $n_7 = 1$. Let K/H be the only one Sylow 7-subgroup in G/H. By Sylow 2nd Theorem, $K/H \lhd G/H$. Then by correspondence theorem, $K \lhd G$ and $|K| = |K/H| \cdot |H| = 7 \cdot 4 = 28$.



■

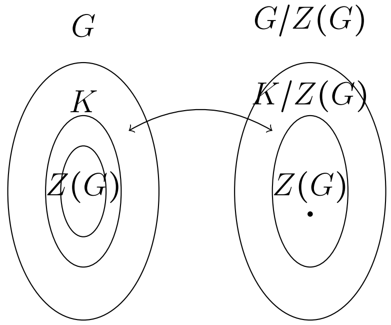
24.41 Suppose that p is prime and $|G| = p^n$. Show that G has normal subgroups of order p^k for all k between 1 and n (inclusive).

Proof. Use induction on n. When $n = 1$, the result holds obviously. Suppose the assertion holds when $n \geq 1$ and let G be a group with $|G| = p^{n+1}$.

If $|G| = |Z(G)|$, then G is abelian and every subgroup of G is normal. The result follows from Sylow 1st Theorem.

If $|G| \neq |Z(G)|$, suppose that $|Z(G)| = p^s$, where $s < n+1$. By induction hypothesis, $|Z(G)|$ has normal subgroups of order p^k for all $k = 1, 2, ..., s$. Recall that if $H \triangleleft Z(G) \leq G$, then $H \triangleleft G$. So those normal subgroup of $Z(G)$ are also normal subgroup of G.

On the other hand, since $Z(G) \triangleleft G$, consider the factor group $G/Z(G)$. By Theorem, 24.2, $|Z(G)| \neq 1$. That is, $s > 0$. Then $|G/Z(G)| = p^{(n+1)-s} < p^{n+1}$. By induction hypothesis, $G/Z(G)$ has normal subgroups of order p^k for all $k = 1, 2, ..., (n+1) - s$. By correspondence theorem, G has normal subgroup of order p^k for all $k = 1 + s, 2 + s, ..., ((n+1) - s) + s$.



Therefore, G has normal subgroups of order p^k for all $k = 1, 2, ..., n+1$. ■

24.42 Suppose that G is a group of order p^n, where p is prime, and G has exactly one subgroup for each divisor of p^n. Show that G is cyclic.

補充. compare with Exercise 11.22.

24.43 Suppose that p is prime and $|G| = p^n$. If H is a proper subgroup of G, prove that $N(H) > H$.

Proof. It follows immediately from the above supplementary exercise. ■

24.44 If H is a finite subgroup of a group G and $x \in G$, prove that $|N(H)| = |N(xHx^{-1})|$.

Proof. For any $x \in G$, consider the inner automorphism σ_x restrict to $N(H)$. That is, $\sigma_x|_{N(H)} : N(H) \to N(xHx^{-1})$. Since σ_x is an automorphism, $\sigma_x|_{N(H)}$ is well-define and one-to-one. We show that $\sigma_x|_{N(H)}$ is well-defined and onto.

Well-defined. If $g \in N(H)$, then $gHg^{-1} = H$ and

$$[\sigma_x|_{N(H)}(g)](xHx^{-1})[\sigma_x|_{N(H)}(g)]^{-1} = (xgx^{-1})(xHx^{-1})(xgx^{-1})^{-1} = xgHg^{-1}x^{-1} = xHx^{-1}.$$

Thus, $\sigma_x|_{N(H)}(g) \in N(xHx^{-1})$.

Onto. For any $g \in N(xHx^{-1})$, we have $g(xHx^{-1})g^{-1} = xHx^{-1}$ and $(x^{-1}gx)H(x^{-1}gx)^{-1} = H$. That is, $x^{-1}gx \in N(H)$. $x^{-1}gx$ belongs to the domain of $\sigma_x|_{N(H)}$. Then $\sigma_x|_{N(H)}(x^{-1}gx) = g \in N(xHx^{-1})$. ■

補充. If G is finite, then the result follows from $[G : N(H)] = |\text{orbit}(H)| = |\text{orbit}(xHx^{-1})| = [G : N(xHx^{-1})]$.

24.45 Let H be a Sylow 3-subgroup of a finite group G and let K be a Sylow 5-subgroup of G. If 3 divides $|N(K)|$, prove that 5 divides $|N(H)|$.

1st, 2nd, 24.46 If H is a normal subgroup of a finite group G and $|H| = p^k$ for some prime p, show that H is contained in every Sylow p-subgroup of G.

Proof. By Sylow 1st Theorem, $H \leq K$ for some Sylow p-subgroup K of G. By Sylow 2nd Theorem, every Sylow p-subgroup is conjugate to K. Thus, every Sylow p-subgroup is of the form gKg^{-1}. Therefore, $H = gHg^{-1} \leq gKg^{-1}$. ■

24.47* Suppose that G is a finite group and G has a unique Sylow p-subgroup for each prime p. Prove that G is the internal direct product of its nontrivial Sylow p-subgroups. If each Sylow p-subgroup is cyclic, is G cyclic? If each Sylow p-subgroup is Abelian, is G Abelian?

Proof. Suppose that $|G| = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$. For each prime divisor p_i of $|G|$, by Sylow 2nd Theorem, let H_i be the only one Sylow p-subgroup and $H_i \triangleleft G$. Note that $|H_i| = p_i^{r_i}$. It is sufficient to show that $G = H_1 H_2 \cdots H_s$ and $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_s = \{e\}$ for each $i = 1, 2, ..., s$. Then G is the internal direct product of $H_1, H_2, ..., H_s$. The desire follows from a lemma.

Lemma. Let $H_1, H_2, ..., H_n$ be finite subgroups of G, where $n \geq 2$ and $\gcd(|H_i|, |H_j|) = 1$ for any $i \neq j$. Then $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n = \{e\}$ for any $i = 1, 2, ..., n$ and $|H_1 H_2 \cdots H_n| = |H_1| \cdot |H_2| \cdots |H_n|$.

Proof of Lemma. We use induction on n. When $n = 2$, by Lagrange's Theorem and $\gcd(|H_1|, |H_2|) = 1$, we have $H_1 \cap H_2 = \{e\}$. The second part follows from the formula $|H_1 H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}$. Suppose the result holds when $n \geq 2$.

Let $H_1, H_2, ..., H_n, H_{n+1}$ be finite subgroups of G such that $\gcd(|H_i|, |H_j|) = 1$ for any $i \neq j$. For any $i = 1, 2, ..., n+1$, by induction hypothesis,

$$|H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_{n+1}| = |H_1| \cdot |H_2| \cdot \cdots \cdot |H_{i-1}| \cdot |H_{i+1}| \cdot \cdots \cdot |H_{n+1}|.$$

Thus,

$$\gcd(|H_i|, |H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_{n+1}|) = \gcd(|H_i|, |H_1| \cdot |H_2| \cdot \cdots \cdot |H_{i-1}| \cdot |H_{i+1}| \cdot \cdots \cdot |H_{n+1}|) = 1.$$

By Lagrange's Theorem, $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_{n+1} = \{e\}$.

Furthermore,

$$\begin{aligned} |H_1 H_2 \cdots H_{n+1}| &\overset{|HK| = \frac{|H| \cdot |K|}{|H \cap K|}}{\overset{\downarrow}{=}} \frac{|H_1 H_2 \cdots H_n| \cdot |H_{n+1}|}{|H_1 H_2 \cdots H_n \cap H_{n+1}|} \\ &\overset{\text{first part}}{\overset{\downarrow}{=}} |H_1 H_2 \cdots H_n| \cdot |H_{n+1}| \\ &\overset{\text{induction hypothesis}}{\overset{\downarrow}{=}} |H_1| \cdot |H_2| \cdot \cdots \cdot |H_n| \cdot |H_{n+1}| \end{aligned}$$

■

24.48 If G_p is a Sylow p-subgroup of a group G and H_p is a Sylow p-subgroup of a group H, prove that $G_p \oplus H_p$ is a Sylow p-subgroup of $G \oplus H$.

24.49 Let G be a finite group and let H be a normal Sylow p-subgroup of G. Show that $\alpha(H) = H$ for all automorphisms α of G.

Proof. If α is an automorphism on G, then $|\alpha(H)| = |H|$. By Sylow 1st Theorem, $\alpha(H)$ is also a Sylow p-subgroup of G. Since $H \lhd G$, by Sylow 2nd Theorem, H is the only one Sylow p-subgroup of G. Thus, $\alpha(H) = H$. ■

24.50* If H is a Sylow p-subgroup of a group, prove that $N(N(H)) = N(H)$.

Proof.

$$\begin{aligned}
x \in N(N(H)) \quad &\Rightarrow \quad xN(H)x^{-1} = N(H) \\
&\overset{\overset{H \le N(H)}{\downarrow}}{\Rightarrow} \quad xHx^{-1} \le N(H) \\
&\overset{\overset{\text{Exercise 24.16}}{\downarrow}}{\Rightarrow} \quad xHx^{-1} = H \\
&\Rightarrow \quad x \in N(H).
\end{aligned}$$

■

2nd, 24.51 Let p be a prime and H and K be Sylow p-subgroups of a group G. Prove that $|N(H)| = |N(K)|$.

Proof. By Sylow 2nd Theorem, any two Sylow p-subgroups are conjugate. Then by Exercise 24.44. ■

24.52 Let p be a group of order p^2q^2, where p and q are distinct primes, $q \nmid p^2 - 1$, and $p \nmid q^2 - 1$. Prove that G is Abelian. List three pairs of primes that satisfy these conditions.

24.53 Let H be a normal subgroup of a group G. Show that H is the union of the conjugacy classes in G of the elements of H. Is this true when H is not normal in G?

Proof. If $a \in H$, then $gag^{-1} \in gHg^{-1} = H$ for all $g \in G$ and $\text{orbit}(a) \subseteq H$.

Let $H = \langle (12) \rangle$. Which is not normal in S_3 and $\text{orbit}((12)) = \{(12), (13)\} \nsubseteq H$. ■

24.54 Let p be prime. If the order of every element of a finite group G is a power of p, prove that $|G|$ is a power of p.

Proof. For any prime divisor q of $|G|$, by Cauchy Theorem, there exists an element of order q. Thus, the prime divisor of $|G|$ is p. ■

2nd, 24.55 For each prime p, prove that all Sylow p-subgroups of a finite group are isomorphic.

Proof. By Sylow 2nd Theorem, any two Sylow p-subgroups H and K are conjugate. That is, $H = gKg^{-1}$ for some $g \in G$. Recall that the mapping $\sigma_g : K \to gKg^{-1} = H$ is an isomorphism, which is called an inner automorphism. ∎

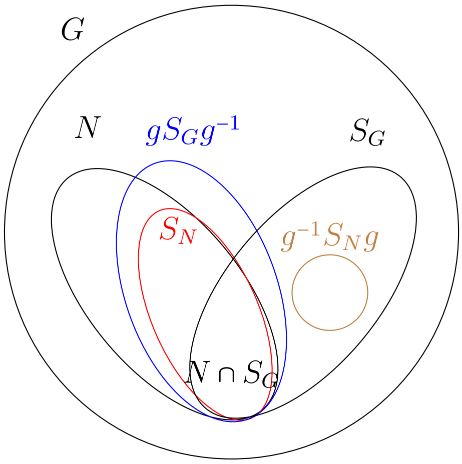
24.56* Suppose that N is a normal subgroup of a finite group G and S_G is a Sylow p-subgroup of G. Prove that $N \cap S_G$ is a Sylow p-subgroup of N.

Proof. [**方法一**] Suppose that $|G| = p^n m$ and $|N| = p^s t$, where $p \nmid m$ and $p \nmid t$.

$$\begin{aligned}
& H \lhd G \\
\Rightarrow\quad & HS_G \leq G \\
\Rightarrow\quad & \frac{p^s t \cdot \cancel{p^n}}{|N \cap S_G|} = \frac{|N| \cdot |S_G|}{|N \cap S_G|} = |NS_G| \text{ divides } |G| = \cancel{p^n} m \\
\Rightarrow\quad & \frac{p^s t}{|N \cap S_G|} \mid m \\
\overset{\gcd(p,m)=1}{\overset{\downarrow}{\Rightarrow}}\quad & |N \cap S_G| = p^s \\
\overset{N\cap S_G \leq N}{\overset{\downarrow}{\Rightarrow}}\quad & N \cap S_G \text{ is a Sylow } p\text{-subgroup in } N.
\end{aligned}$$

與 Exercise 9.66比較一下。

[**方法二**] Suppose that $|G| = p^n m$ and $p \nmid m$ and $|S_G| = p^n$.



Consider $N \cap S_G \leq S_G$. By Lagrange's Theorem, $|N \cap S_G| = p^t$.

Consider $N \cap S_G \leq N$. By Sylow 1st Theorem, there exists a Sylow p-subgroup S_N of N such that $N \cap S_G \leq S_N$.

We claim that $N \cap S_G = S_N$.

Since the order of S_N is a power of p, by Sylow 1st and 2nd Theorem, $S_N \leq gS_Gg^{-1}$ for some $g \in G$. Which implies that $g^{-1}S_Ng \leq S_G$.

On the other hand, since $S_N \leq N \lhd G$, we have $g^{-1}S_Ng \subseteq g^{-1}Ng \leq N$.

Therefore, $g^{-1}S_Ng \leq N \cap S_G$ and $|S_N| = |g^{-1}S_Ng| \leq |N \cap S_G|$. It follows that $N \cap S_G = S_N$ is a Sylow p-subgroup of N. ∎

24.57 Show that a group of order 12 cannot have nine elements of order 2.

Proof. ■

24.58 If $|G| = 36$ and G is non-Abelian, prove that G has more than one Sylow 2-subgroup or more than one Sylow 3-subgroup.

Proof. Note that $36 = 2^2 \cdot 3^2$. See Exercise 24.26. ■

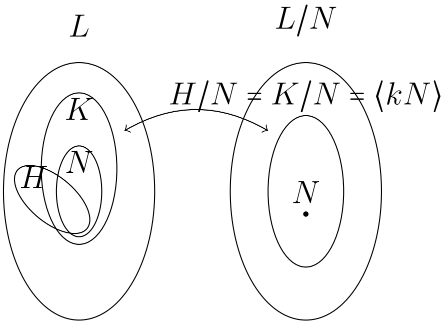
24.59* Suppose G is a finite group and p is a prime that divides $|G|$. Let n denote the number of elements of G that have order p. If the Sylow p-subgroup of G is normal, prove that p divides $n+1$.

Proof. [**方法一**] By Sylow 2nd Theorem, there exists only one Sylow p-subgroup L. For any element g of order p, $\langle g\rangle$ is a subgroup of order p. By Sylow 1st Theorem, $\langle g\rangle \leq L$. Then Thus, every element of order p is in L.

$$\begin{aligned}
\#\{g\in L : |g| = p\} &= |L| - \#\{g\in L : |g| = p^n\} - \#\{g\in L : |g| = p^{n-1}\}\\
&- \cdots - \#\{g\in L : |g| = p^2\} - \#\{g\in L : |g| = 1\}\\
&\overset{\text{cor. of thm.4.4}}{\overset{\downarrow}{=}} p^n - \phi(p^n)k_n - \phi(p^{n-1})k_{n-1} - \cdots - \phi(p^2)k_2 - 1\\
&= ps - 1.
\end{aligned}$$

[**方法二**] By Sylow 2nd Theorem, there exists only one Sylow p-subgroup L. For any element g of order p, $\langle g\rangle$ is a subgroup order p, by Sylow 1st Theorem, $\langle g\rangle \leq L$. Thus, all the elements of order p are in L.

By Exercise 24.41, there exists a subgroup N of order p, which is normal in G. as above, we can conclude that $N \lhd L$.



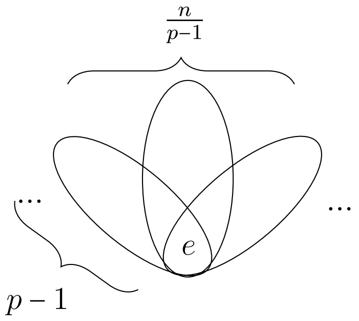
If $N \nsubseteq H \leq L$ and $|H| = p$, verify that $H/N = \{hN \mid h \in H\}$ is a subgroup of L/N. By Correspondence Theorem, there exists K such that $N \leq K$ and $K/N = H/N$. Note that $|K/N| = |H/N| = p$ and $|K| = p^2$. By the Corollary of Theorem 24.2, K is abelian. Write $K/N = \langle kN\rangle$, where $k \notin N$.

Since

$$\langle kn_i\rangle/N \ni (kn_i)^m N \overset{K\text{ is abelian}}{\overset{\downarrow}{=}} k^m n_i^m N = k^m N = (kN)^m \in \langle kN\rangle = K/N,$$

we have $\langle kn_i\rangle/N = K/N$ for each $n_i \in N = \{n_1, n_2, ..., n_p\}$. Note that $|\langle kn_i\rangle/N| = |K/N| = p$. So $\langle kn_i\rangle$ is a subgroup of order p. Hence, $\langle kn_1\rangle, \langle kn_2\rangle, ..., \langle kn_p\rangle$ are all distinct subgroups of L whose order is p such that $\langle kn_i\rangle/N = K/N$. The p subgroups $\langle kn_1\rangle, \langle kn_2\rangle, ..., \langle kn_p\rangle$ of L correspond to a same subgroup K.

Similarly, except N, every p subgroups of order p in L correspond to a same subgroup of order p^2. Let s be the number of subgroups of order p in L. Then $p \mid (s-1)$. Note that $s = \frac{n}{p-1}$, as the following figure indicates.



Therefore,

$$\begin{aligned} p \mid (s-1) = \left(\frac{n}{p-1} - 1\right) \quad &\Rightarrow \quad p(p-1) \mid n - (p-1) \\ &\Rightarrow \quad p \mid n - p + 1 \\ &\Rightarrow \quad p \mid n + 1 \end{aligned}$$

■

補充. 這題其實可以改成 G 是一個 p-group, 參考 Rotman's *An Introduction to the Theory of Groups*, p.75, lem.4.7 or Isaacs's *Finite Group Theory*, p.7, 1A.8.(b).

一次的成功是由九次的失敗所造就。助教在這裡分享我的解題思路, 我嘗試過哪些方法、在哪裡失敗過。

- 由 Sylow p-subgroup 是 normal 及 Sylow 2nd Theorem 知道, 這個 Sylow p-subgroup 是唯一的, 假設其爲 L。
- 由 Sylow 1st Theorem, 所有 order 爲 p 的 subgroup 都會落在 L 中, 所以我們只要考慮 $G = L$ 是 p-group 就好。
- 仿造 Sylow 3rd Theorem 的證明, 令 S 爲所有 order 爲 p 的 subgroup 構成的集合, 然後將 L 作用在其上。這個想法雖然行不通, 但其提供了我們一個很重要的線索, 就是我們要想辦法去研究 S。
- 你也可能會想要將某一個 order 爲 p 的 subgroup H 作用在 S 上, 這時候的 S_0 至少會有一個 H, 但這個方法一樣沒辦法有什麼突破。
- 在考慮 L 作用在 S 上時, 會考慮 $S_0 = \{s \in S \mid l \cdot s = s \text{ for all } l \in L\}$, 但這時候就沒有像 H 作用在 S 上那樣, 可以馬上知道 S_0 至少有一個元素 H 了。
- 不過我們發現 $N \in S_0 \Leftrightarrow N \triangleleft L$, 於是, 由 Exercise 24.41, 我們可以知道一定會有一個 $N \in S_0$。
- 考慮幾個簡單例子, 例如 D_4, 然後考慮這個例子之下的 S, 發現如果 $H \notin S_0$, 那麼 H 的 conjugate 也不屬於 S_0, 而且 H 的 conjugate 的個數似乎都會是 p。這仔細想想就不意外了, 如果

$$H \notin S_0 \Rightarrow H \ntriangleleft L \Rightarrow N(H) \neq L \Rightarrow [L : N(H)] > 1$$

而 H 的 conjugate 的個數等於 $[L : N(H)]$, 而因爲 L 是 p-group, 所以 $[L : N(H)]$ 總會是 p 的倍數。也就是說呢, order爲 p 的非 normal subgroup, 可以按照其之間是否 conjugate, 將其每 p 個分成一組。

- 不過麻煩的地方在於屬於 S_0 的 H, 因爲如果 $H \in S_0$, 則 $H \lhd L$, H 的 conjugate 都是其自己本身, 就沒辦法像上面不屬於 S_0 的 H 做一樣的討論, 當然也就不知道這些 H 是否也可以像不屬於 S_0 的 H 一樣, 每 p 個分成一組。
- 於是我們再觀察幾個簡單的例子, 例如 $D_4 \oplus \mathbb{Z}_2$ 或是 $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, 我們發現屬於 S_0 的 H, 也可以每 p 個分成一組, 雖然分法跟上面有一點不同, 所以需要做一些觀察與猜測。
- (這是另一條沒走過的方向) 既然有了 normal subgroup N, 記得 quotient group 的一個功能, 就是利用 correspondence theorem, 從 L/N 來獲取 L 的資訊。而 $|L/N| = |L|/p$, 我們或許可以用數學歸納法從 L/N 來得到 L 的資訊。

24.60 Determine the group of orer 45.

Proof. Note that $45 = 3^2 \cdot 5$. See Exercise 24.26. ■

24.61 Show that there are at most three nonisomorphic groups of order 21.

Proof. In fact, only two, see exe.31 ■

24.62 Prove that if H is a normal subgroup of index p^2 where p is prime, then $G' \subseteq H$. (G' is the commutator subgroup of G.)

Proof. By the Corollary of Theorem 24.2, a group of order p^2 is abelian. Therefore, $|G/H| = [G : H] = p^2$ and G/H is an abelian group. Which follows that $G' \subseteq H$. ■

24.63 Show that $\mathbb{Z}_2$ is the only group that has exactly two conjugacy classes.

Proof. Suppose that there are only two conjugacy classes of G. Since $\{e\}$ is a conjugacy class of G, where e is the identity of G. Let $e \neq x \in G$. Then $\text{orbit}(x) = G - \{x\}$ and $(|G| - 1) = |\text{orbit}(x)|$ divides $|G|$. It follows that $|G| = 2$. ■

24.64 What can you say about the number of elements of order 7 in a group of orer $168 = 8 \cdot 3 \cdot 7$?

Proof. Note that $168 = 2^3 \cdot 3 \cdot 7$. By Sylow 3rd Theorem and Exercise 24.14, $n_7 \in \{1, 8, \cancel{15}, \cancel{22}\}$.

By the method as in the Exercise 24.21, 24.18, 24.36, there are 6 or 48 elements of order 7. ■

1st, 2nd, 24.65 Explain why a group of order $4m$ where m is odd must have a subgroup isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ but cannot have both a subgroup isomorphic to $\mathbb{Z}_4$ and a subgroup isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Show that S_4 has a subgroup isomorphic to $\mathbb{Z}_4$ and a subgroup isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Proof. **Part I.** Let $|G| = 4m$, where $2 \nmid m$. By Sylow 1st Theorem, there exists a Sylow 2-subgroup H, which is of order 4. We already know that a group of order 4 must be isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Part II. By Sylow 1st Theorem again, a subgroup of order 4 in G is a Sylow 2-subgroup. If there are two Sylow 2-subgroups H and K such that $H \cong \mathbb{Z}_4$ and $K \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. By Sylow 2nd Theorem, any two Sylow 2-subgroups are conjugate each other, then $\mathbb{Z}_4 \cong H \cong K \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, a contradiction.

Part III. In S_4, $\langle(1234)\rangle \cong \mathbb{Z}_4$, $\langle(12),(34)\rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. ■

24.66 Let p be the smallest prime that divides the order of a finite group G. If H is a Sylow p-subgroup of G and is cyclic, prove that $N(H) = C(H)$.

3rd, 24.67 Let G be a group of order $715 = 5 \cdot 11 \cdot 13$. Let H be a Sylow 13-subgroup of G and K be a Sylow 11-subgroup of G. Prove that H is contained in $Z(G)$. Can the argument you used to prove that H is contained in $Z(G)$ also be used to show that K is contained in $Z(G)$?

Proof. Note that $715 = 5 \cdot 11 \cdot 13$. By Sylow 3rd Theorem and Exercise 24.14, $n_{13} \in \{1, \cancel{14}, \cancel{27}, \cancel{40}, \cancel{53}\}$.

$$\begin{aligned} n_{13} = 1 \quad &\Rightarrow \quad [G : N(H)] = n_{13} = 1 \\ &\Rightarrow \quad G = N(H) \\ &\Rightarrow \quad N(H)/C(H) = G/C(H) \leq \operatorname{Aut}(H) \cong \operatorname{Aut}(\mathbb{Z}_{13}) \overset{\overset{p.137, thm.6.5}{\downarrow}}{\cong} \mathbb{Z}_{12}. \end{aligned}$$

By Lagrange's Therem, the only possible of the order of the subgroup $G/C(H)$ of $\mathbb{Z}_{12}$ is 1. Thus, $G = C(H)$ and $H \leq Z(G)$.

Similarly, by Sylow 3rd Theorem and Exercise 24.14, $n_{11} \in \{1, \cancel{11}, \cancel{\cdots}\}$.

$$\begin{aligned} n_{13} = 1 \quad &\Rightarrow \quad [G : N(K)] = n_{11} = 1 \\ &\Rightarrow \quad G = N(K) \\ &\Rightarrow \quad N(K)/C(K) = G/C(K) \leq \operatorname{Aut}(K) \cong \operatorname{Aut}(\mathbb{Z}_{11}) \overset{\overset{\text{p.137, thm.6.5}}{\downarrow}}{\cong} \mathbb{Z}_{10}. \end{aligned}$$

We can't determine the order of the subgroup $G/C(K)$ of $\mathbb{Z}_{10}$, it might be 1 or 5, so we can't use this method to show that K is contained in $Z(G)$. ■

3rd, 24.68 Let G be a group of order $1925 = 5^2 \cdot 7 \cdot 11$ and H be a subgroup of order 7. Prove that $|C(H)|$ is divisible by 385. What can you say about $Z(G)$ if the Sylow 5-subgroup is not cyclic?

Proof. Note that $1925 = 5^2 \cdot 7 \cdot 11$. By Sylow 3rd Theorem and Exercise 24.14, $n_7 \in \{1, \cancel{8}, \cancel{15}, \cancel{22}, \cancel{28}, \cancel{\cdots}\}$.

$$\begin{aligned} n_7 = 1 \quad &\Rightarrow \quad [G : N(H)] = n_7 = 1 \\ &\Rightarrow \quad G = N(H) \\ &\Rightarrow \quad N(H)/C(H) = G/C(H) \leq \operatorname{Aut}(H) \cong \operatorname{Aut}(\mathbb{Z}_7) \overset{\overset{\text{p.137, thm.6.5}}{\downarrow}}{\cong} \mathbb{Z}_6. \end{aligned}$$

By Lagrange's Therem, the only possible of the order of the subgroup $G/C(H)$ of $\mathbb{Z}_6$ is 1. Thus, $G = C(H)$ and $385 = 5 \cdot 7 \cdot 11$ divides $|G| = |C(H)|$. ■

補充. 這題怪怪的, 得到的結果比所求更好, 也就是我們可以得到 $C(H) = G$, 後半段未解決。

2nd, 3rd, 24.69 Let G be a group with $|G| = 595 = 5\cdot 7\cdot 17$. Show that the Sylow 5-subgroup of G is normal in G and is contained in $Z(G)$.

Proof. Note that $595 = 5\cdot 7\cdot 17$. By Sylow 3rd Theorem and Exercise 24.14, $n_5 \in \{1, \cancel{6}, \cancel{11}, \cancel{16}, \cancel{\cdots}\}$. Let H be the only one Sylow 5-sbugroup. By Sylow 2nd Theorem, $H \lhd G$.

$$\begin{aligned} n_5 = 1 \quad &\Rightarrow \quad [G : N(H)] = n_5 = 1 \\ &\Rightarrow \quad G = N(H) \\ &\Rightarrow \quad N(H)/C(H) = G/C(H) \leq \operatorname{Aut}(H) \cong \operatorname{Aut}(\mathbb{Z}_5) \overset{\substack{\text{p.137, thm.6.5} \\ \downarrow}}{\cong} \mathbb{Z}_4. \end{aligned}$$

By Lagrange's Therem, the only possible of the order of the subgroup $G/C(H)$ of $\mathbb{Z}_4$ is 1. Thus, $G = C(H)$ and $H \leq Z(G)$. ∎

24.71 Prove that if x and y are in the same conjugacy class of a group, then $|C(x)| = |C(y)|$.

Proof. If x and y are in the same conjugacy class, then $\operatorname{orbit}(x) = \operatorname{orbit}(y)$ and $[G : C(x)] = |\operatorname{orbit}(x)| = |\operatorname{orbit}(y)| = [G : C(y)]$. ∎

補充 24.A If a group H of order p^n (p prime) acts on a finite set S and if $S_0 = \{x \in S \mid hx = x \text{ for all } h \in H\}$, then $|S| \equiv |S_0| \pmod p$.

Proof. Recall that $x \in S_0$ if and only if $\operatorname{orbit}(x) = \{x\}$ and $|\operatorname{orbit}(x)| = 1$. Let $\operatorname{orbit}(x_1), \operatorname{orbit}(x_2), \ldots, \operatorname{orbit}(x_m)$ be all distinct orbits whose cardinality greater than 1. That is, $|\operatorname{orbit}(x_i)| > 1$. By Class Equation and Orbit-Stabilizer Theorem,

$$|S| = |S_0| + \sum_{i=1}^{m} \operatorname{orbit}(x_i) = |S_0| + \sum_{i=1}^{m} [H : \operatorname{Stab}(x_i)].$$

Since $|H| = p^n$, we have $p \mid \sum_{i=1}^{m} [H : \operatorname{Stab}(x_i)] = |S| - |S_0|$ and $|S| \equiv |S_0| \pmod p$. ∎

補充 24.B If H is a p-subgroup of a finite group G, then $[N(H) : H] \equiv [G : H] \pmod p$. (a p-subgroup is a subgroup whose order is a power of prime.)

Proof. Let S be the set of all left cosets of H. Then $|S| = [G : H]$. Let H acts on S by translation. That is, $h \cdot sH = hsH$. Then $|S| \equiv |S_0| \pmod p$, where

$$\begin{aligned} sH \in S_0 \quad &\Leftrightarrow \quad h \cdot sH = hsH = sH, \forall h \in H \\ &\Leftrightarrow \quad s^{-1}hsH = H, \forall h \in H \\ &\Leftrightarrow \quad s^{-1}hs \in H, \forall h \in H \\ &\Leftrightarrow \quad shs^{-1} \in H, \forall h \in H \\ &\Leftrightarrow \quad sHs^{-1} \subseteq H, \forall h \in H \\ &\overset{\substack{\text{consider the inner automorphism} \\ \sigma_s : H \to sHs^{-1} \subseteq H \\ \downarrow}}{\Leftrightarrow} \quad sHs^{-1} = H, \forall h \in H \\ &\Leftrightarrow \quad s \in N(H) \end{aligned}$$

Since $H \lhd N(H)$, consider the factor group $N(H)/H$. Then $|S_0| = |N(H)/H|$ and

$$[G:H] = |S| \equiv |S_0| = [N(H):H] \pmod p.$$

■

p.581, exe.3 Show that a group of order $315 = 3^2 \cdot 5 \cdot 7$ has a subgroup of order 45.

Proof. Note that $315 = 3^2 \cdot 5 \cdot 7$. By Sylow 3rd Theorem and Exercise 24.14, $n_3 \in \{1, \cancel{4}, 7, \cancel{\cdots}\}$.

If $n_3 = 1$, then let H be the only one Sylow 3-subgroup of G. By Sylow 2nd Theorem, $H \lhd G$. Let K be a Sylow 5-subgroup of G. Then HK is a subgroup of G (because $H \lhd G$) and

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{9 \cdot 5}{1} = 45.$$

If $n_3 = 7$, then let H be a Sylow 3-subgroup of G. Since $[G : N(H)] = n_3 = 7$, we have $|N(H)| = |G|/7 = 45$ and $N(H)$ is a subgroup of order 45. ■

24 Chapter 25

Preliminaries

- □ Let $|G| = p^n m$ and $p \nmid m$. A subgroup of order p^n is called a Sylow p-subgroup of G.
- □ **Sylow 1st Theorem:** Let $|G| = p^n m$ and $p \nmid m$. For any $i = 1, 2, \ldots, n-1$, there exists a subgroup H of order p^i and a subgroup K of order p^{i+1} such that $H \lhd K$. In particular, a subgroup of prime power order is contained in a Sylow p-subgroup of G.
- □ **Sylow 2nd Theorem:** Any two Sylow p-subgroups are conjugate. In particular, H is the only one Sylow p-subgroup if and only if $H \lhd G$.
- □ **Sylow 3rd Theorem:** Let $|G| = p^n m$ and $p \nmid m$. Let n_p be the number of the Sylow p-subgroups. Then $n_p = ps + 1$ for some $s \in \mathbb{N} \cup \{0\}$ and $n_p \mid m$.

Preliminaries

- □ If $|G| = p^2$, then G is abelian.

  Proof. p.411, cor. ■

- □ If $|G| = pq$ and $p < q$ and $p \nmid q - 1$, then $|G|$ is cyclic.

  Proof. p.419, thm.24.6 ■

- □ If $A \lhd B \leq G$, then $B \leq N(A)$.

  Proof. It follows immediately from the definition of the normalizer $N(A) = \{g \in G \mid gAg^{-1} = A\}$. ■

- □ Suppose that $H \leq G$. $H \lhd G$ if and only if $N(H) = G$.

Proof. It follows immediately from the definition of the normalizer $N(H) = \{g \in G \mid gHg^{-1} = H\}$. ■

□ If H is a Sylow p-subgroup of G, then $[G : N(H)] = n_p$.

Proof. Recall that any two Sylow p-subgroups are conjugate. Let G acts on the set of all subgroup of G by conjugation. Then apply Orbit-Stabilizer Theorem on the stabilizer $N(H)$ and the orbit contains H. ■

Preliminaries

□ If G is abelian, then every subgroup is normal.

□ **Cauchy's Theorem:** If p is a prime and $p \mid |G|$, then there exists an element $a \in G$ such that $|a| = p$. In particular, $\langle a \rangle$ is a subgroup of order p.

□ Let H, K and L be three subgroups of G and $H \leq L$ and $K \leq L$. Then $HK \subseteq L$. Note that HK does not necessarily be a subgroup of G.

□ $|HK| = \frac{|H|\cdot|K|}{|H \cap |K|}$.

□ N/C **Theorem:** $N(H)/C(H)$ is isomorphic to a subgroup of $\operatorname{Aut}(H)$.

□ $\operatorname{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

□ If $xy = yx$ and $\langle x \rangle \cap \langle y \rangle = \{e\}$, then $|xy| = \text{l.c.m.}(|x|, |y|)$.

題組 Extended Cayley Theorem

25.3, 25.20

題組 Extended Cayley Theorem and $N(H)$

25.4, 課本範例 A

題組 Embedding Theorem

課本範例 B

題組 $A \triangleleft B \Rightarrow B \leq N(A)$

25.5

題組 N/C Theorem and Embedding Theorem

25.9, 25.7

題組 (Optional) $H_i \cap H_j \neq \{e\}$

課本範例C, 課本範例 D

題組 (Optional) Burnside's Normal Complement Theorem

25.6, 25.8

題組 Advanced Exercises

25.10~25.19, 25.22~25.31

題組 Group Action

補充 A, Foote, p.44, exa.6, Foote, p.126, 補充 B, prop.11, p.149, 補充 C, 補充 D, 補充 E

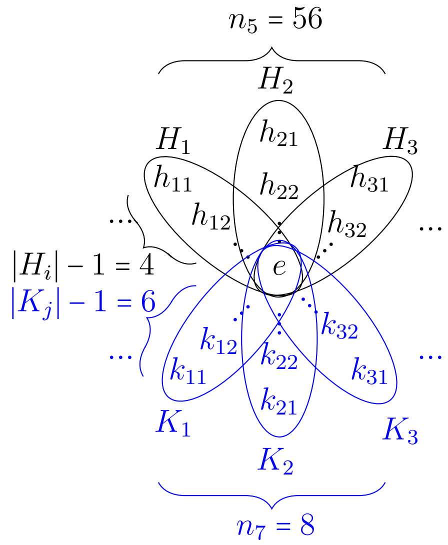
25.1 Prove thta there is no simple group of order $210 = 2 \cdot 3 \cdot 5 \cdot 7$.

Proof. By $2 \cdot$ Odd Test. ■

25.2 Prove thta there is no simple group of order $280 = 2^3 \cdot 5 \cdot 7$.

Proof. Note that $280 = 2^3 \cdot 5 \cdot 7$. By Sylow 3rd Theorem and Exercise 24.14, $n_5 \in \{1, \cancel{6}, \cancel{11}, \cancel{\cdots}, 56\}$ and $n_7 \in \{1, 8, \cancel{15}, \cancel{\cdots}\}$.

If $n_5 = 56$ and $n_7 = 8$, then there are $56 \cdot 4 = 224$ elements of order 5 and $8 \cdot 6 = 48$ elements of order 7, as the following figure indicates.



There are $280 - 224 - 48 = 8$ elements remaining (include identity e). These 8 elements form the only one Sylow 2-subgroup in G (by Sylow 1st Theorem). By Sylow 2nd Theorem, this only one Sylow 2-subgroup is normal. ■

25.3 Prove thta there is no simple group of order $216 = 2^3 \cdot 3^3$.

Proof. By Sylow 1st Theorem, there exists a Sylow 3-subgroup H. Then $[G : H] = 8$. By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_8$ with $\ker\theta \leq H \neq G$. We show that $\ker\theta \neq \{e\}$. Then $\ker\theta \triangleleft G$ and G is not simple.

If $\ker\theta = \{e\}$, then by First Isomorphism Theorem,

$$G \cong G/\{e\} = G/\ker\theta \cong \operatorname{Im}(\theta) \leq S_8.$$

It follows that

$$216 = 2^3 \cdot 3^3 = |G| \text{ divides } |S_8| = 8! = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1,$$

which is impossible. ■

補充. 類似的題目有 Nicholson, p.365, exa.1. order 36.

25.4 Prove thta there is no simple group of order $300 = 2^2 \cdot 3 \cdot 5^2$.

Proof. Let G be a group of order 300. By Sylow 3rd Theorem, $n_5 \in \{1, 6, \cancel{11}\}$.

If $n_5 = 1$, then let H be the only one Sylow 5-subgroup of G. By Sylow 2nd Theorem, $H \lhd G$ and we are done.

If $n_5 = 6$, then let H be a Sylow 5-subgroup of G. [key] Note that $[G : N(H)] = n_5 = 6$. By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_6$ with $\ker\theta \leq N(H) \overset{\overset{H \ntriangleleft G}{\downarrow}}{\neq} G$. We show that $\ker\theta \neq \{e\}$.

If $\ker\theta = \{e\}$, then by First Isomorphism Theorem,

$$G \cong G/\{e\} = G/\ker\theta \cong \mathrm{Im}(\theta) \leq S_6.$$

It follows that

$$300 = 2^2 \cdot 3 \cdot 5^2 = |G| \text{ divides } |S_6| = 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1,$$

which is impossible. ■

25.5 Prove thta there is no simple group of order $525 = 3 \cdot 5^2 \cdot 7$.

Proof. By Sylow 3rd Theorem, $n_7 \in \{1, 15\}$. If $n_7 = 1$, then let H be the only one Sylow 7-subgroup of G. By Sylow 2nd Theorem, $H \lhd G$ and we are done.

$$\begin{array}{cl}
\text{If} & n_7 = 15, \\
\text{let} & H \text{ be a Sylow 7-subgroup of } G. \\
\Rightarrow & [G : N(H)] = n_7 = 15 \\
\Rightarrow & |N(H)| = 35 \\
\Rightarrow & N(H) \text{ is cyclic and abelian} \\
\Rightarrow & \text{there exists } K \leq N(H) \text{ such that } |K| = 5 \\
\overset{\overset{N(H) \text{ is abelian}}{\downarrow}}{\Rightarrow} & K \lhd N(H) \\
\overset{\overset{A \lhd B \Rightarrow B \leq N(A)}{\downarrow}}{\Rightarrow} & N(H) \leq N(K) \\
\Rightarrow & 35 = |N(H)| \text{ divides } |N(K)|.
\end{array}$$

On the other hand, by Sylow 1st Theorem,

$$\begin{array}{cl}
 & K \leq L \text{ for some Sylow 5-subgroup } L \text{ of } G \\
\Rightarrow & |L| = 25 \\
\overset{\overset{|G| = p^2 \Rightarrow G \text{ abelian}}{\downarrow}}{\Rightarrow} & L \text{ abelian} \\
\Rightarrow & K \lhd L \\
\overset{\overset{A \lhd B \Rightarrow B \leq N(A)}{\downarrow}}{\Rightarrow} & L \leq N(K) \\
\Rightarrow & 25 = |L| \text{ divides } |N(K)| \\
\Rightarrow & \text{l.c.m.}(35, 25) = 175 \text{ divides } |N(K)| \\
\Rightarrow & |N(K)| \geq 175 \\
\Rightarrow & [G : N(K)] \leq \dfrac{3 \cdot 5^2 \cdot 7}{175} = 3, \\
 & \text{which is impossible by Extended Cayley Theorem.}
\end{array}$$

■

補充. 注意, 這題的解法包括了好幾個技巧, 要使用這些技巧需要一些條件, 而這些條件將會是你在判斷一個題目能不能用這個解法的依據。

- 例如 If $|N(H)| = pq$, $p > q$ and $q \nmid p-1$, then $N(H)$ is cyclic. Exercise 25.8乍看之下也可以用 Exercise 25.5一樣的方法來解, 但失敗在這一步。
- 當然, 有最主要的 $A \lhd B \le G \Rightarrow B \le N(A)$.
- 注意, 如果你選 $|K| = 7$ 的話, 就沒辦法得到 $K \le L$ 且 $|L| = 7^2$ 這件事, 因為 $7^2 \nmid |G|$。我們會選 $|K| = 5$ 是因為 $5^2 \mid |G|$.
- 你可以試試看如果用 n_5 討論的話會發生什麼事。

25.6 Prove thta there is no simple group of order $540 = 2^2 \cdot 3^3 \cdot 5$.

Proof. By Sylow 3rd Theorem, $n_5 \in \{1, 6, \cancel{11}, \cancel{16}, \cancel{\cdots}, 36, \cancel{\cdots}\}$.

If $n_5 = 1$, let H be the only one Sylow 5 subgroup of G, then by Sylow 2nd Theorem, $H \lhd G$.

If $n_5 = 6$, by Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_6$ and $\ker\theta$ is a proper nontrivial normal subgroup of G.

If $n_5 = 36$, let H be a Sylow 5-subgroup of G. Then $[G : N(H)] = n_5 = 36$ and $|N(H)| = \frac{2^2 \cdot 3^3 \cdot 5}{36} = 15$ and

$$|N(H)/C(H)| = 15/|C(H)| \text{ divides } |\mathrm{Aut}(H)| = |\mathrm{Aut}(\mathbb{Z}_5)| = 4.$$

It follows that $|C(H)| = 15$ and $C(H) = N(H)$. By Burnside's Normal Complement Theorem [5], there exists a normal subgroup of G such that $G = HK$ and $H \cap K = \{e\}$. ■

25.7 Prove thta there is no simple group of order $528 = 2^4 \cdot 3 \cdot 11$.

Proof. By Sylow 3rd Theorem, $n_{11} \in \{1, 12, \cancel{23}\}$.

If $n_{11} = 1$, let H be the only one Sylow 11-subgroup of G, then by Sylow 2nd Theorem, $H \lhd G$.

[5] https://ysharifi.wordpress.com/2011/01/20/burnsides-normal-complement-theorem-3/

If $n_{11} = 12$, let H be a Sylow 11-subgroup of G, then $[G : N(H)] = n_{11} = 12$.

$$\begin{tikzcd}
{[G : N(H)] = n_{11} = 12} \arrow[d, Rightarrow] \arrow[dr, Rightarrow, "\text{Embedding Theorem}"] & \\
{|N(H)| = \frac{2^4\cdot 3\cdot 11}{12} = 44} \arrow[d, Rightarrow, "N/C\text{ Theorem}"'] & {G \cong G_{\text{copy}} \le A_{12}} \arrow[dddddl, Rightarrow, "A_{12}\text{ has no element of order }22"] \\
{|N(H)/C(H)| = 44/|C(H)| \text{ divides } |\mathrm{Aut}(H)| = |\mathrm{Aut}(\mathbb{Z}_{11})| = 10} \arrow[d, Rightarrow] & \\
{|C(H)| \in \{22, 44\}} \arrow[d, Rightarrow, "\text{Cauchy's Theorem}"'] & \\
{\exists x \in C(H),\ |x| = 2} \arrow[d, Rightarrow, "{\exists y \in H,\ |y| = 11}"'] & \\
{xy = yx \text{ and } \langle x\rangle \cap \langle y\rangle = \{e\}} \arrow[d, Rightarrow] & \\
{|xy| = \text{l.c.m.}(2, 11) = 22} \arrow[d, Rightarrow] & \\
\text{a contradiction} &
\end{tikzcd}$$

■

25.8 Prove thta there is no simple group of order $315 = 3^2 \cdot 5 \cdot 7$.

25.9 Prove thta there is no simple group of order $396 = 2^2 \cdot 3^2 \cdot 11$.

Proof. By Sylow 3rd Theorem, $n_{11} \in \{1, 12, \cancel{23}, \cancel{34}\}$.

If $n_{11} = 1$, let H be the only one Sylow 11-subgroup of G, then by Sylow 2nd Theorem, $H \triangleleft G$.

If $n_{11} = 12$, let H be a Sylow 11-subgroup of G, then $[G : N(H)] = n_{11} = 12$.

$$\begin{tikzcd}
{[G : N(H)] = n_{11} = 12} \arrow[d, Rightarrow] \arrow[dr, Rightarrow, "\text{Embedding Theorem}"] & \\
{|N(H)| = \frac{2^2\cdot 3^2\cdot 11}{12} = 33} \arrow[d, Rightarrow] & {G \cong G_{\text{copy}} \le A_{12}} \arrow[dddl, Rightarrow, "A_{12}\text{ has no element of order }33"] \\
{N(H) \text{ is cyclic}} \arrow[d, Rightarrow] & \\
{\exists x \in C(H),\ |x| = 33} \arrow[d, Rightarrow] & \\
\text{a contradiction} &
\end{tikzcd}$$

■

25.10 Prove that there is no simple group of order n, where $201 \le n \le 235$ and n is not prime.

25.11 Without using the Generalized Cayley Theorem or its corollaries, prove that there is no simple group of order 112.

25.12 Without using the $2 \cdot$ Odd Test, prove that there is no simple group of order 210.

25.13 You may have noticed that all the "hard integers" are even. Choose three odd integers between 200 and 1000. Show that none of these is the order of a simple group unless it is prime.

25.14 Show that there is no simple group of order pqr, where p, q and r are primes (p, q, and r need not be distinct).

Proof. If $p > q > r$, then $n_p = 1$.

If $p = q \ne r$, then by Exercise 24.30.

If $p = q = r$, then by p.410, Theorem 24.2, $Z(G) \ne \{e\}$. If $Z(G) = G$, then G is abelian and every subgroup is normal. If $Z(G) \ne G$, then $Z(G)$ is a nontrivial proper normal subgroup. ■

25.15 Show that A_5 does not contain a subgroup of order 30, 20, or 15.

25.16 Show that S_5 does not contain a subgroup of order 40 or 30.

25.17 Prove that there is no simple group of order $120 = 2^3 \cdot 3 \cdot 5$.

25.18 Prove that if G is a finite group and H is a proper normal subgroup of large order, then G/H is simple.

25.19 Suppose that H is a subgroup of a fintie group G and that $|H|$ and $(|G:H|-1)!$ are relatively prime. Prove that H is normal in G. What does this tell you about a subgroup of index 2 in a finite group?

Proof. Let $[G:H] = m$. By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_m$ such that $\ker\theta \le H$. By First Isomorphism Theorem,

$$\begin{aligned}
& G/\ker\theta \cong \operatorname{Im}(\theta) \le S_m \\
\Rightarrow\quad & |G|/|\ker\theta| = |G/\ker\theta| = |\operatorname{Im}(\theta)| \text{ divides } |S_m| = m! \\
\overset{\substack{|G|=[G:H]\cdot|H|=m\cdot|H| \\ \downarrow}}{\Rightarrow}\quad & \frac{|G|}{|\ker\theta|} = \frac{m\cdot|H|}{|\ker\theta|} \mid m! \\
\Rightarrow\quad & \frac{|H|}{|\ker\theta|} \mid (m-1)! = ([G:H]-1)! \\
\overset{\substack{\frac{|H|}{|\ker\theta|} \text{ divides } |H|, \\ \gcd(|H|,([G:H]-1)!)=1 \\ \downarrow}}{\Rightarrow}\quad & \frac{|H|}{|\ker\theta|} = 1 \\
\Rightarrow\quad & |H| = |\ker\theta| \\
\overset{\substack{\ker\theta\le H \\ \downarrow}}{\Rightarrow}\quad & H = \ker\theta \lhd G.
\end{aligned}$$

■

重要 25.20 Suppose that $|G| = p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$, where p_i is prime and $p_1 < p_2 < \cdots < p_s$. If $H \le G$ and $[G : H] = p_1$, then $H \lhd G$. (Suppose that p is the smallest prime that divides $|G|$. Show that any subgroup of index p in G is normal in G.)

Proof. If $[G : H] = p_1$, then $|H| = p_1^{r_1-1}p_2^{r_2}\cdot p_s^{r_s}$. By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_{p_1}$ with $\ker\theta \le H$. We show that $\ker\theta = H$. Then $H = \ker\theta \lhd G$.

$$\begin{array}{cl}
\text{Suppose that} & \ker\theta = p_1^{r_1-1-t_1}p_2^{r_2-t_2}\cdots p_s^{r_s-t_s} \\
\overset{\substack{\text{First Isomorphism Theorem} \\ \downarrow}}{\Rightarrow} & |G/\ker\theta| = p_1^{t_1+1}p_2^{t_2}\cdots p_s^{t_s} = |\mathrm{Im}(\theta)| \text{ divides } |S_{p_1}| = p_1! \\
\Rightarrow & t_1 = t_2 = \cdots = t_s = 0 \text{ and } \ker\theta = H.
\end{array}$$

■

補充. 這個定理是 $[G : H] = 2 \Rightarrow H \lhd G$ 的推廣。

25.21 Prove that the only nontrivial proper normal subgroup of S_5 is A_5.

Proof. [**方法一**]

$$\begin{array}{cl}
\text{Suppose that} & \{e\} \subsetneqq H \subsetneqq S_5 \text{ and } A_5 \ne H \lhd S_5 \\
\overset{\substack{\text{normal } \cap \text{ normal } = \text{ normal} \\ \downarrow}}{\Rightarrow} & H \cap A_5 \lhd S_5 \\
\Rightarrow & H \cap A_5 \lhd A_5 \\
\overset{\substack{A_5 \text{ is simple} \\ \downarrow}}{\Rightarrow} & H \cap A_5 = A_5 \text{ or } \{e\} \\
 & \\
\text{If} & H \cap A_5 = A_5 \\
\Rightarrow & A_5 \le H \\
\overset{\substack{A_5 \ne H \ne S_5 \\ \downarrow}}{\Rightarrow} & |A_5| = 60 < |H| < 120 = |S_5|, \\
 & \text{a contradiction because } |H| \text{ divides } |S_5|. \\
\text{If} & H \cap A_5 = \{e\} \\
\overset{\substack{H \lhd G,\ HA_5 \le S_5 \\ \downarrow}}{\Rightarrow} & 120 = |S_5| \ge |HA_5| = \dfrac{|H| \cdot |A_5|}{|H \cap A_5|} = 60 \cdot |H| \\
\Rightarrow & |H| \le 2 \\
\overset{\substack{H \ne \{e\} \\ \downarrow}}{\Rightarrow} & |H| = 2 \text{ (Or use Exercise 5.23.)} \\
\Rightarrow & H = \langle h \rangle \text{ for some } h \in S_5 \text{ with } |h| = 2 \\
\overset{\substack{H \cap A_5 = \{e\},\ h \notin A_5 \\ \downarrow}}{\Rightarrow} & h = (ij) \text{ for some } i \ne j \in \{1, 2, 3, 4, 5\} \\
\overset{\substack{H \lhd S_5 \\ \downarrow}}{\Rightarrow} & \text{take } g = (ik) \in S_5,\ \text{where } k \notin \{i, j\},\ ghg^{-1} \in H, \\
 & \text{but } ghg^{-1} \ne h \text{ and } ghg^{-1} \ne e, \\
 & \text{a contradiction because } |H| = 2. \\
 & \text{(Or use Exercise 9.72 and Exercise 5.66)}
\end{array}$$

[**方法二**] Write down all the elements of S_5 and classify them by conjugacy classes. Count the number of elements in each conjugacy classes. Let H be a normal subgroup of S_5 and $H \neq \{e\}$ and $H \neq S_5$. H satisfy three conditions.

- A normal subgroup is an union of some conjugacy classes.
- By Exercise 5.23, all elements of H or half of them are even permutation.
- By Lagrange's Theorem, $|H|$ divides $|S_5| = 120$.

The only possible of $|H|$ is 60 and $H = A_5$.

1	20	15	24	10	20	30
e	(123)	(12)(34)	(12345)	(12)	(123)(45)	(1234)
	(132)	(12)(35)	(12354)	(13)	(132)(45)	(1243)
	(124)	(12)(45)	(12435)	(14)	(124)(35)	(1235)
	(142)	(13)(24)	(12453)	(15)	(142)(35)	(1253)
	(125)	(13)(25)	(12534)	(23)	(125)(34)	(1245)
	(152)	(13)(45)	(12543)	(24)	(152)(34)	(1254)
	(134)	(14)(23)	(13245)	(25)	(134)(25)	(1324)
	(143)	(14)(25)	(13254)	(34)	(143)(25)	(1342)
	(135)	(14)(35)	(13425)	(35)	(135)(24)	(1325)
	(153)	(15)(23)	(13452)	(45)	(153)(24)	(1352)
	(145)	(15)(24)	(13524)		(145)(23)	(1345)
	(154)	(15)(34)	(13542)		(154)(23)	(1354)
	(234)	(23)(45)	(14235)		(234)(15)	(1423)
	(243)	(24)(35)	(14253)		(243)(15)	(1432)
	(235)	(25)(34)	(14325)		(235)(14)	(1425)
	(253)		(14352)		(253)(14)	(1452)
	(245)		(14523)		(245)(13)	(1435)
	(254)		(14532)		(254)(13)	(1453)
	(345)		(15234)		(345)(12)	(1523)
	(354)		(15243)		(354)(12)	(1532)
			(15324)			(1524)
			(15342)			(1542)
			(15423)			(1534)
			(15432)			(1543)
						(2345)
						(2354)
						(2435)
						(2453)
						(2534)
						(2543)

■

25.22 Prove that a simple group of order 60 has a subgroup of order 6 and a subgroup of order 10.

Proof. ■

25.23 Show that $PSL(2,\mathbb{Z}_7) = SL(2,\mathbb{Z}_7)/Z(SL(2,\mathbb{Z}_7))$, which has order 168, is a simple group.

Proof. ■

25.24 Show that the permutations (12) and (12345) generate S_5.

Proof. 助教建議你, 先把下面的答案算出來, 再看看你能發現什麼事情。

$(12345) =$	$(12)(12345) =$	$(12345)(12) =$	$(12)(12345)(12) =$
$(12345)^2 =$	$(12)(12345)^2 =$	$(12345)^2(12) =$	$(12)(12345)^2(12) =$
$(12345)^3 =$	$(12)(12345)^3 =$	$(12345)^3(12) =$	$(12)(12345)^3(12) =$
$(12345)^4 =$	$(12)(12345)^4 =$	$(12345)^4(12) =$	$(12)(12345)^4(12) =$

Let $H = \langle (12), (12345) \rangle$. Then $(2345) = (12)(12345) \in H$, $(124) = (12)(12345)^3(12) \in H$ and $(12345) \in H$. By Lagrange's Theorem, $|(2345)| = 4$, $|(124)| = 3$ and $|(12345)| = 5$ all divide $|H|$. Hence, $4 \cdot 3 \cdot 5 = 60$ divides $|H|$ and $H = A_5$ or $H = S_5$. But (12) is an odd permutation in H, so $H = S_5$. ■

25.25 Suppose that a subgroup H of S_5 contains a 5-cycle and a 2-cycle. Show that $H = S_5$.

Proof. Let $\alpha = (c_1c_2c_3c_4c_5)$ and $\beta = (c_1c_i)$ be a 5-cycle and a 2-cycle in S_5, respectively, where $i \in \{2,3,4,5\}$. Note that

$$\begin{array}{rcl}
(c_1c_2c_3c_4c_5) & = & (c_1c_2c_3c_4c_5) \\
(c_1c_2c_3c_4c_5)^2 & = & (c_1c_3c_5c_2c_4) \\
(c_1c_2c_3c_4c_5)^3 & = & (c_1c_4c_2c_5c_3) \\
(c_1c_2c_3c_4c_5)^4 & = & (c_1c_5c_4c_3c_2)
\end{array}$$

Let $\gamma = (c_1c_2c_3c_4c_5)^{i-1} = (c_1c_ixyz)$. Then applies the same method in Exercise 25.24 on β and γ. ■

25.26* Suppose that G is a finite simple group and contains subgroups H and K such that $|G:H|$ and $|G:K|$ are prime. Show that $|H| = |K|$.

Proof. **Lemma 1.** If H and K are subgroups of a group G, then $[H : H \cap K] \leq [G : K]$. If $[G : K]$ is finite, then $[H : H \cap K] = [G : K]$ if and only if $G = KH$.

Lemma 2. Let H and K be subgroups of finite index of a group G. Then $[G : H \cap K]$ is finite and $[G : H \cap K] \leq [G : H][G : K]$. Furthermore, $[G : H \cap K] = [G : H][G : K]$ if and only if $G = HK$.

Proof of Exercise 25.26. If $[G : H] = [G : K]$, then the result follows from the formula $|H| \cdot [G : H] = |G| = |K| \cdot [G : K]$.

Suppose that $[G : H]$ and $[G : K]$ are two distinct primes. Then $\gcd([G : H], [G : K]) = 1$. Consider the two towers of groups

$$H \cap K \leq H \leq G$$

and

$$H \cap K \leq K \leq G.$$

Since $[G:H] \mid [G:H\cap K]$ and $[G:K] \mid [G:H\cap K]$ and $\gcd([G:H],[G:K]) = 1$, we have $[G:H]\cdot[G:K] \mid [G:H\cap K]$. By Lemma 2, we have $[G:H]\cdot[G:K] = [G:H\cap K]$ and $G = HK$.

Suppose that $|G| = p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$ and $[G:H] = p_i$ and $[G:K] = p_j$ for some $i \neq j \in \{1,2,\dots,s\}$. Then

$$\begin{aligned} p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s} &= |G| = |HK| = \frac{|H|\cdot|K|}{|H\cap K|} = |H|\cdot|K| \\ &= \underline{p_1^{r_1}p_2^{r_2}\cdots p_i^{r_i-1}\cdots p_s^{r_s}}\cdot\underline{p_1^{r_1}p_2^{r_2}\cdots p_j^{r_j-1}\cdots p_s^{r_s}} \\ &= p_1^{2r_1}p_2^{2r_2}\cdots p_i^{2r_i-1}\cdots p_j^{2r_j-1}\cdots p_s^{2r_s}. \end{aligned}$$

It follows that $r_k = 0$ for $k \neq i$ and $k \neq j$ and $r_i = r_j = 1$. That is, $|G| = p_ip_j$.

Suppose that $p_i < p_j$. Since the index $[G:H] = p_i$ is the smallest prime divisor of $|G|$, by Exercise 25.20, $H \lhd G$, contrary to the simplicity of G. ■

25.27 Show that (up to isomorphism) A_5 is the only simple group of order 60.

Proof. ■

25.28 Prove that a simple group cannot have a subgroup of index 4.

Proof. Let G be a group and H be a subgroup of G with $[G:H] = 4$. By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_4$ such that $\ker\theta \leq H$. Since G is normal and $\ker\theta \lhd G$, we have $\ker\theta = \{e\}$. By the First Isomorphism Theorem, $G \cong G/\{e\} = G/\ker\theta \cong \mathrm{Im}(\theta) \leq S_4$ and $|G|$ divides $|S_4| = 24$. That is, $|G| \in \{4,6,8,12,24\}$. An abelian group with these order is not simple. Furthermore, the smallest non-abelian simple group is of order 60 (A_5). Hence, a simple group which has a subgroup of index 4 cannot exist. ■

補充. 注意, 並沒有 $[G:H] = 4 \Rightarrow H \lhd G$ 這個定理, 例如 $H = \langle b\rangle$, $G = D_4$, $[G:H] = 4$, but $H \ntriangleleft G$.

這裡有一個想法, 不過做不出來, 或許你可以試試看。考慮

$$\underbrace{H \leq K \leq G}_{4}$$

如果 $[G:K] = 2$, 則 $K \lhd G$, 但因爲 G 是 simple, 所以 $K = G$ 或是 $K = H$。

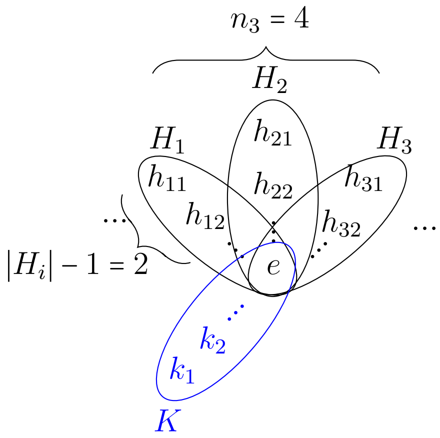
另外, 我也有想到用 classification of small groups 來做, 不過臨門差了一腳。

When $|G| = 4$, G is abelian and G is not simple.

When $|G| = 6$, $4 = [G:H]$ divides $|G| = 6$, a contradiction.

When $|G| = 8$, if G is abelian, then G is not simple. If G is non-abelian, then $G \cong D_4$ or $G \cong Q_8$. Both are not simple.

When $|G| = 12$, $|H| = 3$. Which means that H is a Sylow 3-subgroup of G. Since G is simple, we have $H \ntriangleleft G$ and $N(H) \neq G$. Consider the tower of groups $H \leq N(H) \leq G$. It follows that $N(H) = N$. Hence, $n_3 = [G:N(H)] = [G:H] = 4$. There are 4 Sylow 3-subgroups.



There are 8 elements of order 3. The remaining $12 - 8 = 4$ elements form the only one Sylow 2-subgroup K. By Sylow 2nd Theorem, K is normal in G. Contrary to the simplicity of G.

When $|G| = 24$, 到這裡我就卡住了。

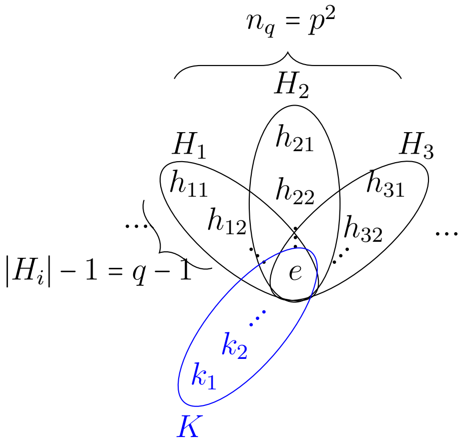
25.29 Prove that there is no simple group of order p^2q, where p and q are odd primes and $q > p$.

Proof. By Sylow 3rd Theorem and Exercise 24.14, $n_q \in \{1, p, p^2\}$.

If $n_q = 1$, then by Sylow 2nd Theorem, the only one Sylow q-subgroup is normal in G, contrary to the simplicity of G. Similarly, $n_p = 1$.

If $n_q = p^2$, let $H_1, H_2, ..., H_{p^2}$ be all the Sylow q-subgroups in G. By Lagrange's Theorem, $H_i \cap H_j = \{e\}$ for $i \neq j \in \{1, 2, ..., p^2\}$. For each $i \in \{1, 2, ..., p^2\}$, if $h \neq e \in H_i$, then $|h| = q$.

Thus, in each H_i, there are $|H_i| - 1 = q - 1$ elements of order q. On the other hand, there are $n_q = p^2$ Sylow q-subgroups. Thus, there are $(q-1)_{|H_i|-1} \cdot p^2_{n_q} = p^2q - p^2$ elements of order q. As the following figure indicates.



There are $p^2q - (p^2q - p^2) = p^2$ elements remaining (include identity e). These p^2 elements can only form a Sylow p-subgroup in G (by Sylow 1st Theorem), contrary to the fact $n_p = q$.

Therefore, $n_q = p$. Let K be a Sylow q-subgroup. Then $[G : N(K)] = n_q = p$ is the smallest prime divisor of $|G|$. By the Exercise 25.20, $N(K)$ is a normal subgroup of G and G is not simple. ■

類似 25.29 Prove that there is no simple group of order p^2q, where p and q are primes.

Proof. 我覺得應該屬於 ch.24的技巧。

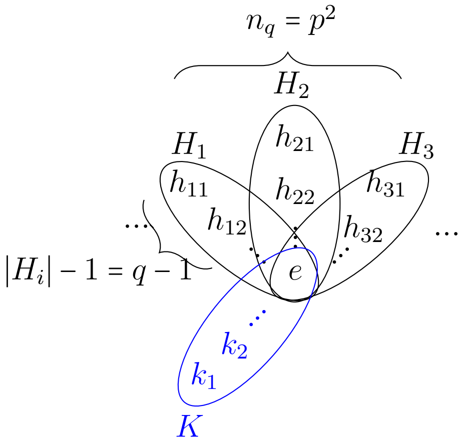
If $p = q$, since the center of a p-group is nontrivial and the center is normal, we are done. (Or by Sylow 1st Theorem, there exists $H \lhd G$ and $|H| = p^2$.)

If $p > q$, then by Sylow 3rd Theorem, $n_p = 1$. By Sylow 2nd Theorem, there exists only one normal Sylow p-subgroup of G.

If $p < q$, then by Sylow 3rd Theorem, $n_q \in \{1, p, p^2\}$. Since $n_q \equiv 1 \pmod{q}$ and $p < q$, we have $n_q \neq p$.

If $n_q = 1$, then by Sylow 2nd Theorem, the only one Sylow q-subgroup is normal.

If $n_q = p^2$, let $H_1, H_2, ..., H_{p^2}$ be all the Sylow q-subgroup of G. By Lagrange's Theorem, $H_i \cap H_j = \{e\}$ if $i \neq j$. Thus, there are $p^2 \cdot (q-1)$ elements of order q.



The remain $p^2q - p^2 \cdot (q-1) = p^2$ form the only one Sylow p-subgroup K of G. By Sylow 2nd Theorem, $K \lhd G$. ■

25.30 If a simple group G has a subgroup K that is a normal subgroup of two distinct maximal subgroups, prove that $K = \{e\}$.

25.31 Show that a finite group of even order that has a cyclic Sylow 2-subgroup is not simple.

Extended Cayley Theorem Let G be a group and $H \leq G$. If $[G : H] = m$, then there exists a homomorphism $\theta : G \to S_m$ with $\ker\theta \leq H$.

Proof. Let X be the set of all left cosets of H. Let G acts on X by left translation. That is, $g \cdot aH = gaH$. For any $g \in G$, define $\sigma_g : X \to X$, $\sigma_g(aH) = gaH$. Then σ_g is a bijection. That is, $\sigma_g \in S_X \cong S_m$. Define $\theta : G \to S_X$, $\theta(g) = \sigma_g$. Then θ is a homomorphism.

$$\begin{array}{ll}
\text{If} & k \in \ker\theta \\
\Rightarrow & \theta(k) = \mathrm{id}_{S_X},\ \text{ where } \mathrm{id}_{S_X} \text{ is the identity element in } S_X \\
 & \text{and the identity mapping on } X \\
\Rightarrow & \theta(k)(aH) = \mathrm{id}_{S_X}(aH) = aH \text{ for all } aH \in X \\
\overset{\overset{\text{take } a=e}{\downarrow}}{\Rightarrow} & \theta(k)(H) = kH = H \\
\Rightarrow & k \in H \\
\Rightarrow & \ker\theta \subseteq H
\end{array}$$

■

Embedding Theorem Let G be a group and $H \leq G$. If $[G:H] = m$, then $G \cong G' \leq A_m$. [6]

補充. 這個定理在 $2 \mid |G|$ 的時候才有用, 否則就跟 Extended Cayley Theorem 一樣。

可以把上面三個定理合併成一個定理: If $n_p \neq 1$ and G is simple, then $|G|$ divides $n_p!/2$. 雖然目前還沒有出現上面三個定理個別使用無法解決, 必須使用這個合併後的較強版本才能解決的題目, 但應該可以自己設計一個。

課本範例 A Prove thta there is no simple group of order $72 = 2^3 \cdot 3^2$.

Proof. 課本內文有證明。 ■

補充. 這題也出現在 Nicholson, p.375, exa.8.

課本範例 B Prove thta there is no simple group of order $112 = 2^4 \cdot 7$.

Proof. 課本內文有證明。 ■

課本範例 C Prove thta there is no simple group of order $144 = \cdot 2^4 \cdot 3^2$.

Proof. By Sylow 3rd Theorem, $n_3 \in \{1, 4, \cancel{7}, \cancel{10}, \cancel{13}, 16\}$.

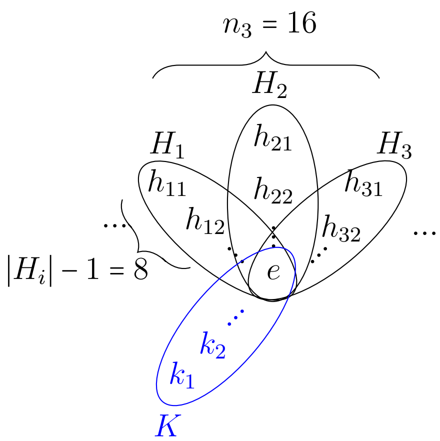
If $n_3 = 1$, let H be the only one Sylow 3-subgroup of G, then by Sylow 2nd Theorem, $H \lhd G$.

If $n_3 = 4$, let H be a Sylow 3-subgroup of G, then $[G : N(H)] = n_3 = 4$. By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_4$ and $\ker\theta$ is a proper nontrivial normal subgroup of G.

If $n_3 = 16$, let $H_1, H_2, ..., H_{16}$ be all the Sylow 3-subgroups of G. Note that $|H_i| = 9$ for $i = 1, 2, ..., 16$.

Case I: If $H_i \cap H_j = \{e\}$ for any $i \neq j$, then there are $(|H_i| - 1) \cdot n_3 = 8 \cdot 16 = 128$ elements in $\bigcup_{i=1}^{16} H_i - \{e\}$. There are $144 - 128 = 16$ elements in $(G - \bigcup_{i=1}^{16}) \bigcup \{e\}$. These elements form the only one Sylow 2-subgroup. By Sylow 2nd Thereom, this unique Sylow 2-subgroup is normal in G.

[6] http://goo.gl/sk3FJP



Case II: If $H_i \cap H_j \neq \{e\}$ for some $i \neq j$, then $\{e\} \neq H_i \cap H_j \leq H_i$ and $|H_i| = 3^2$. It follows that $|H_i \cap H_j| = 3$. On the other hand, $|H_i| = 3^2$ implies that H_i is abelian. Thus, $H_i \cap H_j \lhd H_i$ and $H_i \leq N(H_i \cap H_j)$. Similarly, $H_j \leq N(H_i \cap H_j)$.

$$\begin{tikzcd}
H_i, H_j \leq N(H_i \cap H_j) \arrow[d, Rightarrow] \arrow[dr, Rightarrow] & \\
H_iH_j \subseteq N(H_i \cap H_j) \arrow[d, Rightarrow] & 9 = |H_i| \text{ divides } |N(H_i \cap H_j)| \text{ divides } |G| = 2^4 \cdot 3^2 \arrow[d, Rightarrow] \\
|N(H_i \cap H_j)| \geq |H_iH_j| = \frac{|H_i|\cdot|H_j|}{H_i \cap H_j} = \frac{9\cdot 9}{3} = 27 \arrow[d, Rightarrow] & |N(H_i \cap H_j)| \in \{9, 18, 36, 72, 144\} \arrow[dl, Rightarrow] \\
|N(H_i \cap H_j)| \geq 36 \arrow[d, Rightarrow] & \\
[G : N(H_i \cap H_j)] \leq 4. &
\end{tikzcd}$$

By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_4$ and $\ker \theta$ is a proper nontrivial normal subgroup of G. ■

課本範例 D Prove thta there is no simple group of order $180 = 2^2 \cdot 3^2 \cdot 5$.

Proof. By Sylow 3rd Theorem, $n_3 \in \{1, 4, \cancel{7}, 10\}$, $n_5 \in \{1, 6, \cancel{11}, , \cancel{16}, , \cancel{21}, \cancel{26}, \cancel{31}, 36\}$

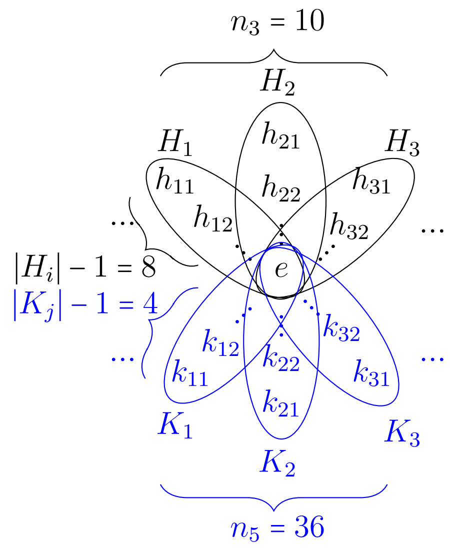
If $n_3 = 1$, let H be the only one Sylow 3-subgroup of G, then by Sylow 2nd Theorem, $H \lhd G$. $n_5 = 1$ is similar. So we assume that $n_5 > 1$.

If $n_3 = 4$, let H be a Sylow 3-subgroup of G, then $[G : N(H)] = n_3 = 4$. By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_4$ and $\ker \theta$ is a proper nontrivial normal subgroup of G.

If $n_3 = 10$ and $n_5 = 36$, let $H_1, H_2, \dots, H_{10}$ be all the Sylow 3-subgroups of G. Note that $|H_i| = 9$ for $i = 1, 2, \dots, 16$.

Case I: If $H_i \cap H_j = \{e\}$ for any $i \neq j$, then there are $(|H_i| - 1) \cdot n_3 = 8 \cdot 10 = 80$ elements in $\bigcup_{i=1}^{10} H_i - \{e\}$. On the other hand, let $K_1, K_2, \dots, K_{36}$ be all the Sylow

5-subgroups of G. Then there are $36\cdot 4 = 144$ elements of order 5. But $80+144 = 224$ exceed $|G| = 180$, this case is impossible.



Case II: If $H_i \cap H_j \neq \{e\}$ for some $i \neq j$, then $\{e\} \neq H_i \cap H_j \leq H_i$ and $|H_i| = 3^2$. It follows that $|H_i \cap H_j| = 3$. On the other hand, $|H_i| = 3^2$ implies that H_i is abelian. Thus, $H_i \cap H_j \lhd H_i$ and $H_i \leq N(H_i \cap H_j)$. Similarly, $H_j \leq N(H_i \cap H_j)$.

$$\begin{tikzcd}
H_i, H_j \leq N(H_i \cap H_j) \arrow[d, Rightarrow] \arrow[dr, Rightarrow] & \\
H_iH_j \subseteq N(H_i \cap H_j) \arrow[d, Rightarrow] & 9 = |H_i| \text{ divides } |N(H_i \cap H_j)| \text{ divides } |G| = 2^2 \cdot 3^2 \cdot 5 \arrow[d, Rightarrow] \\
|N(H_i \cap H_j)| \geq |H_iH_j| = \frac{|H_i|\cdot|H_j|}{H_i \cap H_j} = \frac{9\cdot 9}{3} = 27 \arrow[d, Rightarrow] & |N(H_i \cap H_j)| \in \{9, 18, 36, 45, 90, 180\} \arrow[dl, Rightarrow] \\
|N(H_i \cap H_j)| \geq 36 \arrow[d, Rightarrow] & \\
{[G : N(H_i \cap H_j)] \leq 5.} &
\end{tikzcd}$$

By Extended Cayley Theorem, there exists a homomorphism $\theta : G \to S_5$ and $\ker\theta$ is a proper nontrivial normal subgroup of G.

If $n_5 = 6$, let K be a Sylow 5-subgroup of G, then $[G : N(K)] = n_5 = 6$.

$$\begin{tikzcd}
{[G : N(K)] = n_5 = 6} \arrow[d, Rightarrow] \arrow[dr, Rightarrow, "\text{Embedding Theorem}"] & \\
N(K) = \frac{2^2 \cdot 3^2 \cdot 5}{6} = 30 \arrow[d, Rightarrow, "\text{p.418, exa.4}"'] & G \cong G_{\text{copy}} \leq A_6 \arrow[ddl, Rightarrow, "A_6 \text{ has no element of order } 15"] \\
\exists x \in N(K) \leq G,\ |x| = 15 \arrow[d, Rightarrow] & \\
\text{a contradiction} &
\end{tikzcd}$$

■

p.149, exa.5 Prove that A_4 does not contain a subgroup of order 6.

Proof. If A_4 has a subgroup of H order 6, then $[A_4 : H] = 12/6 = 2$ and $H \lhd G$. But all the normal subgroup of A_4 are $\{e\}$, A_4 and $\{e, (12)(34), (13)(24), (14)(23)\}$. ■

補充 25.A Let G be a group and let G act on itself defined by $a \cdot g = g^{-1}a$ for all $a, g \in G$. Prove that this is a group action.

Proof. $a \cdot e = e^{-1}a = ea = a$ and $a \cdot (g_1 g_2) = (g_1 g_2)^{-1} a = g_2^{-1} g_1^{-1} a = g_2^{-1}(a \cdot g_1) = (a \cdot g_1) \cdot g_2$. ■

補充. 注意, 如果定義成 $g \cdot a = g^{-1}a$, 就不會是一個 group action, 所以 left 跟 right 不能亂換。

補充 25.B Determine the conjugacy classes of S_4 and A_4.

Proof. In S_4,

$$\begin{aligned}
\text{orbit}(e) &= \{e\}, \\
\text{orbit}((12)) &= \{(12), (13), (14), (23), (24), (34)\}, \\
\text{orbit}((123)) &= \{(123), (132), (124), (142), (134), (143), (234), (243)\}, \\
\text{orbit}((1234)) &= \{(1234), (1243), (1324), (1342), (1423), (1432)\}, \\
\text{orbit}((12)(34)) &= \{(12)(34), (13)(24), (14)(23)\}.
\end{aligned}$$

In A_4,

$$\begin{aligned}
\text{orbit}(e) &= \{e\}, \\
\text{orbit}((123)) &= \{(123), (134), (142), (243)\}, \\
\text{orbit}((132)) &= \{(132), (124), (143), (234)\}, \\
\text{orbit}((12)(34)) &= \{(12)(34), (13)(24), (14)(23)\}.
\end{aligned}$$

■

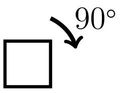
補充 25.C In S_4,

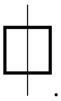
$$\begin{aligned}
\text{orbit}(e) &= \\
\text{orbit}((12)) &= \\
\text{orbit}((123)) &= \\
\text{orbit}((1234)) &= \\
\text{orbit}((12)(34)) &=
\end{aligned}$$

補充 25.D In $Q_8 = \{1, -1, i, -i, j, -j, k, -k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1, ij = k, kj = -i\}$,

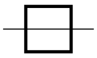
$$\begin{aligned}
1i1^{-1} &= \\
(-1)i(-1)^{-1} &= \\
iii^{-1} &= \\
(-i)i(-i)^{-1} &= \\
jij^{-1} &= \\
(-j)i(-j)^{-1} &= \\
kik^{-1} &= \\
(-k)i(-k)^{-1} &= \\
\text{orbit}(i) &=
\end{aligned}$$

補充 25.E In $D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3 \mid |a| = 4, |b| = 2, aba = b\}$, suppose that

$a =$ 

$, b =$  .

Then

$a^2 =$ $\quad$ $, a^3 =$ $\quad$ $, ba =$ $\quad$ $, ba^2 =$  , $\quad ba^3 =$ $\quad$.

$$\begin{aligned}
\text{orbit}(1) &= \\
\text{orbit}(a) &= \\
\text{orbit}(a^2) &= \\
\text{orbit}(b) &= \\
\text{orbit}(ba) &=
\end{aligned}$$

Foote, p.44, exe.6 Show that the action of G on itself by conjugation is faithful if and only if G has a trivail center.

Proof. Recall that a group action "·" is faithful if for all $x \in X$, $x \cdot g_1 = x \cdot g_2$ implies that $g_1 = g_2$.

($\Rightarrow$) If $g \in Z(G)$, then for all $a \in G$, $a \cdot g = gag^{-1} = agg^{-1} = a = a \cdot e$. Since the group action is faithful, we get $g = e$.

(⇐) Suppose that $Z(G) = \{e\}$.

$$\begin{aligned} &\text{If} && \text{for all } a \in G,\ a \cdot g_1 = a \cdot g_2 \\ &\Rightarrow && \text{for all } a \in G,\ g_1 a g_1^{-1} = g_2 a g_2^{-1} \\ &\Rightarrow && \text{for all } a \in G,\ g_1 a = g_2 a g_2^{-1} g_1 \\ &\Rightarrow && \text{for all } a \in G,\ g_2^{-1} g_1 a = a g_2^{-1} g_1 \\ &\Rightarrow && g_2^{-1} g_1 \in Z(G) = \{e\} \\ &\Rightarrow && g_2^{-1} g_1 = e \\ &\Rightarrow && g_1 = g_2 \end{aligned}$$

■

Foote, p.126, prop.11 Prove that two permutations are conjugate in S_n if and only if they have the same cycle structure.

Proof. (⇒) By cycle decomposition theorem, any permutation σ can be writed as a product of some disjoint cycles. That is, $\sigma = \gamma_1\gamma_2\cdots\gamma_m$ for some cycles γ_1, γ_2, ..., γ_m. Consider a conjugate $g\sigma g^{-1}$ of σ. Then

$$g\sigma g^{-1} = g\gamma_1\gamma_2\cdots\gamma_m g^{-1} = g\gamma_1 g^{-1} \cdot g\gamma_2 g^{-1} \cdots g\gamma_m g^{-1}.$$

W.L.O.G., suppose that $\gamma_1 = (ij\cdots)$. Then $g\gamma_1 g^{-1} = g(ij\cdots)g^{-1} = (g(i)\ g(j)\cdots)$. You can verify the last identity directly by compute $g(ij\cdots)g^{-1}(g(i))$.

(⇐) If two cycles $\gamma = (ij\cdots)$ and $\gamma' = (kl\cdots)$ have the same length, then let σ be the permutation such that $\sigma(i) = k$, $\sigma(j) = k$, ... Then $\sigma\gamma\sigma^{-1} = (\sigma(i)\ \sigma(j)\cdots) = (kl\cdots) = \gamma'$. That is, γ and γ' are conjugate. ■

Nicholson, p.375, exa.9 Show that no group of order p^2q^2 is simple when p and q are primes.

Proof. Extended Cayley Theorem. ■

Fraleigh, p.333, exe.38.6 Prove that no group of order 160 is simple.

Proof. Extended Cayley Theorem. ■

Fraleigh, p.332, exa.37.15 Every group of order $255 = 3 \cdot 5 \cdot 17$ is abelian.

Proof. commutator subgroup. ■

Fraleigh, p.333, exe.38.4 Prove that every group of order $5 \cdot 7 \cdot 47$ is abelian and cyclic.

Proof. commutator subgroup. ■

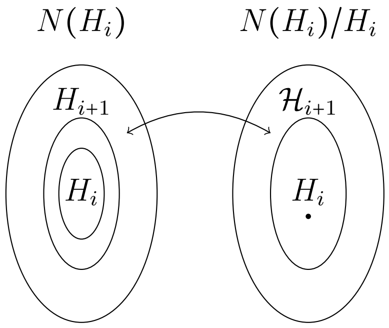
Grillet, p.76, 15. Show that $1 \trianglelefteq A_n \trianglelefteq S_n$ is the only composition series of S_n when $n \geq 5$.

Proof. Recall that A_n is simple for every $n \geq 5$. Then by the proof of Exercise 25.21. ■

Grillet, p.76, 16. Show that a group of order p^n, where p is prime, has a composition series of length n.

Proof. By Cauchy Theorem, there exists an element g of order p and a subgroup $H_1 = \langle g \rangle$ of order p.

For $1 \le i < n$, if H_i is a subgroup of order p^i. Recall that $H_i \lhd N(H_i)$. Consider the quotient group $N(H_i)/H_i$. By Exercise 24.43, $H_i \neq N(H_i)$, so $N(H_i)/H_i$ is nontrivial and p divides $|N(H_i)/H_i|$. By Cauchy Theorem again, there exists a subgroup $\mathcal{H}_{i+1}$ of $N(H_i)/H_i$, which is of order p. By Correspondence Theorem, there exists H_{i+1} which contains H_i and $|H_{i+1}/H_i| = |\mathcal{H}_+| = p$ and $|H_{i+1}| = p \cdot |H_i| = p^{i+1}$.



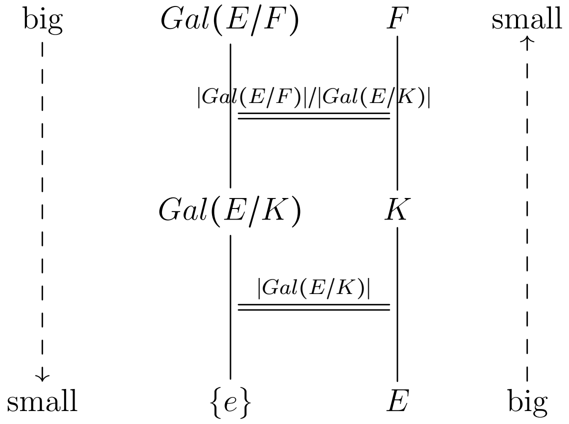
Since $|H_{i+1}| = p^{i+1}$ and $[H_{i+1} : H_i] = p$, by Exercise 25.20, $H_i \lhd H_{i+1}$. Therefore, we have a composition series $\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \cdots H_{n-1} \lhd H_n = G$ of length n. ■

補充. 許多書把這個當作 Sylow 1st Theorem 的一部分。

25 Chapter 32

題組 Galois Theory II

If char $F = 0$ or $|F| < \infty$, E is the splitting field for some polynomial in $F[x]$, then by the fundamental theorem of Galois theory, we have



32.4, 32.10, 32.12, 32.13

題組 Solvable

25.21, 32.27, 32.28, 32.29, 32.30

32.1 Let E be an extension field of $\mathbb{Q}$. Show that any automorphism of E acts as the identity on $\mathbb{Q}$.

32.2 Determine the group of field automorphisms of $GF(4)$.

32.3 Let E be an extension field of the field F. Show that the automorphism group of E fixing F is indeed a group.

32.4 Given that the automorphism gorup of $\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ is isomorphic to $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$, determine the number of subfields of $\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ that have degree 4 over $\mathbb{Q}$.

Proof. Let $E = \mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ and

$$a = \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{5} \to \sqrt{5} \\ \sqrt{7} \to \sqrt{7} \end{cases}, \quad b = \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{5} \to -\sqrt{5} \\ \sqrt{7} \to \sqrt{7} \end{cases}, \quad c = \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{5} \to \sqrt{5} \\ \sqrt{7} \to -\sqrt{7} \end{cases}$$

Then $Gal(E/\mathbb{Q}) = \langle a,b,c\rangle \cong \mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$.

By the fundamental theorem of Galois theory, we have

$$\begin{tikzcd}
\text{big} \arrow[dd, dashed] & Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2 \arrow[d, dash] \arrow[r, Rightarrow, "4"] & \mathbb{Q} \arrow[d, dash] & \text{small} \\
 & H =? \arrow[d, dash] & K \arrow[d, dash] & \\
\text{small} & \{e\} & E = \mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7}) & \text{big} \arrow[uu, dashed]
\end{tikzcd}$$

In $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$, a subgroup H has index 4 if and only if H is of order 2. Thus, $H = \langle h\rangle$ for some h of order 2. There are 7 elements in $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$ whose order are 2. Therefore, there are 7 subfields of $\mathbb{Q}(\sqrt{2},\sqrt{5},\sqrt{7})$ that have degree 4 over $\mathbb{Q}$. ∎

32.5 Let E be an extension field of a field F and let H be a subgroup of $Gal(E/F)$. Show that the fixed field of H is indeed a field.

32.6 Let E be the splitting field of x^4+1 over $\mathbb{Q}$. Find $Gal(E/\mathbb{Q})$. Find all subfields of E. Find the automorphisms of E that have fixed fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$, and $\mathbb{Q}(i)$. Is there an automorphism of E whose fixed field is $\mathbb{Q}$?

Proof.

- **Splitting Field:** Note that $x^8-1=(x^4-1)(x^4+1)$ and

$$\begin{aligned}
x^8-1 &= \underline{(x-1)}(x-\omega_8)\underline{(x-\omega_8^2)}(x-\omega_8^3)\underline{(x-\omega_8^4)}(x-\omega_8^5)\underline{(x-\omega_8^6)}(x-\omega_8^7) \\
&= \underline{(x-1)(x-\omega_4)(x-\omega_4^2)(x-\omega_4^3)}(x-\omega_8)(x-\omega_8^3)(x-\omega_8^5)(x-\omega_8^7) \\
&= \underline{(x^4-1)}(x-\omega_8)(x-\omega_8^3)(x-\omega_8^5)(x-\omega_8^7)
\end{aligned}$$

Thus, $x^4+1=(x-\omega_8)(x-\omega_8^3)(x-\omega_8^5)(x-\omega_8^7)$.

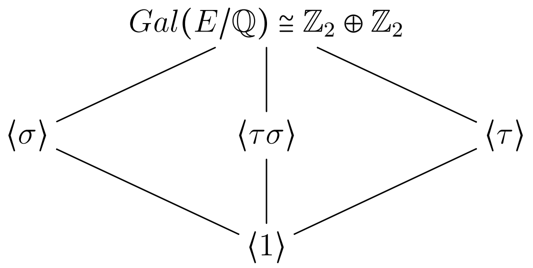
Since $\omega_8=\cos\frac{2\pi}{8}+i\sin\frac{2\pi}{8}=\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}$, the splitting field E of x^4+1 over $\mathbb{Q}$ is $\mathbb{Q}(\omega_8)=\mathbb{Q}(\sqrt{2},i)$. (Apply Eisenstein's Criterion with $p=2$ on $(x+1)^4+1$, one can show that x^4+1 is irreducible over $\mathbb{Q}$. It follows that x^4+1 is the minimal polynomial of ω_8 and $\overbrace{\underbrace{\mathbb{Q}\le}_{4}\mathbb{Q}(\omega_8)\le\mathbb{Q}(\sqrt{2},i)}^{4}$.

- **Galois Group:** The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is x^2-2. The minimal polynomial of i over $\mathbb{Q}$ is x^2+1. By theorem, if $f\in Gal(E/\mathbb{Q})$, then $f(\sqrt{2})\in\{\sqrt{2},-\sqrt{2}\}$ and $f(i)\in\{i,-i\}$. Let

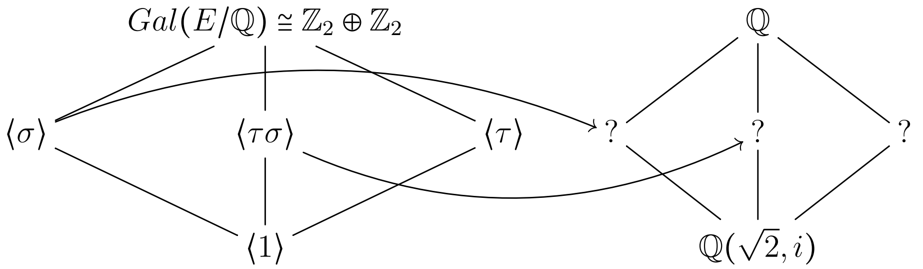
$$\sigma=\begin{cases}\sqrt{2}\to-\sqrt{2}\\ i\to i\end{cases},\quad \tau=\begin{cases}\sqrt{2}\to\sqrt{2}\\ i\to -i\end{cases}$$

Then $Gal(E/\mathbb{Q})=\langle\sigma,\tau\rangle\cong\mathbb{Z}_2\oplus\mathbb{Z}_2$.

- **Draw the Subgroup Lattice Diagram of the Galois Group:**


$Gal(E/\mathbb{Q})\cong\mathbb{Z}_2\oplus\mathbb{Z}_2$
$\langle\sigma\rangle$
$\langle\tau\sigma\rangle$
$\langle\tau\rangle$
$\langle 1\rangle$

- **Use the Galois Correspondence to Determine the Fixed Field of the Subgroups of the Galois Group:**

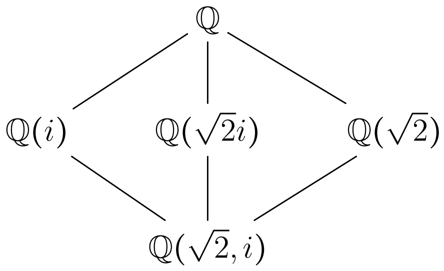


In this case, since $\sigma(i)=i$, the fixed field of $\langle\sigma\rangle$ is $\mathbb{Q}(i)$. Similarly, since

$$\tau\sigma(\sqrt{2}i)=\tau(\sigma(\sqrt{2})\sigma(i))=\tau((-\sqrt{2})\cdot i)=\tau(-\sqrt{2})\cdot\tau(i)=(-\sqrt{2})\cdot(-i)=\sqrt{2}i,$$

we get that the fixed field of $\langle\sigma\tau\rangle$ is $\mathbb{Q}(\sqrt{2}i)$. The fixed field of the automorphisms in $\langle\tau\rangle$ is $\mathbb{Q}(\sqrt{2})$. The fixed field of the identity mapping on E is $\mathbb{Q}$.

- **Draw the Subfield Lattice Diagram of the Splitting Field:**



■

32.10 Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. What is the order of the group $Gal(E/\mathbb{Q})$? What is the order of $Gal(\mathbb{Q}(\sqrt{10})/\mathbb{Q})$?

Proof. Let

$$\sigma = \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{5} \to \sqrt{5} \end{cases}, \quad \tau = \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{5} \to -\sqrt{5} \end{cases}$$

Then $Gal(E/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. By the fundamental theorem of Galois theory, we have

$$\begin{tikzcd}
\text{big} \arrow[ddd, dashed] & Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \arrow[dd, dash] & \mathbb{Q} \arrow[dd, dash] & \text{small} \\
 & \triangleleft & {} \arrow[l, Rightarrow, "2"'] & \\
 & Gal(E/\mathbb{Q}(\sqrt{10})) \arrow[d, dash] & \mathbb{Q}(\sqrt{10}) \arrow[d, dash] & \\
\text{small} & \{e\} & E = \mathbb{Q}(\sqrt{2}, \sqrt{5}) & \text{big} \arrow[uuu, dashed]
\end{tikzcd}$$

Therefore,

$$Gal(\mathbb{Q}(\sqrt{10}/\mathbb{Q}) \cong \frac{Gal(E/\mathbb{Q})}{Gal(E/\mathbb{Q}(\sqrt{10}))}$$

and

$$|Gal(\mathbb{Q}(\sqrt{10}/\mathbb{Q})| = \frac{|Gal(E/\mathbb{Q})|}{|Gal(E/\mathbb{Q}(\sqrt{10}))|} = 2.$$

■

32.12 Determine the Galois group of $x^{10} - 10x + 21$ over $\mathbb{Q}$.

Proof. $x^{10} - 10x + 21 = (x-3)(x-7)$. The splitting field of $x^{10} - 10x + 21$ over $\mathbb{Q}$ is $\mathbb{Q}$ and $Gal(\mathbb{Q}/\mathbb{Q}) = \{e\}$. ■

32.13 Determine the Galois group of $x^2 + 9$ over $\mathbb{R}$.

Proof. $x^2 + 9 = (x - 3i)(x + 3i)$. The splitting field of $x^2 + 9$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$. and $Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{e, \sigma\}$, where $\sigma(i) = -i$. ■

32.18 Determine the Galois group of $x^3 - 1$ over $\mathbb{Q}$ and $x^3 - 2$ over $\mathbb{Q}$.

Proof. For $x^3 - 1$.

- **Splitting Field:** Note that $x^3 - 1 = (x-1)(x^2+x+1) = (x-1)(x-\omega_3)(x-\omega_3^2)$. The splitting field E of $x^3 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega_3)$. Note that the splitting field is NOT $\mathbb{Q}(\sqrt{3}, i)$ even $\omega_3 = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$, because the minimal polynomial of ω_3 over $\mathbb{Q}$ is $x^2 + x + 1$ and $\overbrace{\mathbb{Q} \underbrace{\leq}_{2} \mathbb{Q}(\omega_3) \leq \mathbb{Q}(\sqrt{3}, i)}^{4}$.
- **Galois Group:** The minimal polynomial of ω_3 over $\mathbb{Q}$ is x^2+x+1. By theorem, if $f \in Gal(E/\mathbb{Q})$, then $f(\omega_3) \in \{\omega_3, \omega_3^2\}$. Let $\sigma \in Gal(E/\mathbb{Q})$ and $\sigma(\omega_3) = \omega_3^2$. Then $Gal(E/\mathbb{Q}) = \langle \sigma \rangle \cong \mathbb{Z}_2$.
- **Draw the Subgroup Lattice Diagram of the Galois Group:**

$$\begin{tikzcd}
Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2 \arrow[d, dash] \\
\langle 1 \rangle
\end{tikzcd}$$

- **Use the Galois Correspondence to Determine the Fixed Field of the Subgroups of the Galois Group:**

$$\begin{tikzcd}
Gal(E/\mathbb{Q}) \cong \mathbb{Z}_2 \arrow[d, dash] & \mathbb{Q} \arrow[d, dash] \\
\langle 1 \rangle & \mathbb{Q}(\omega_3)
\end{tikzcd}$$

- **Draw the Subfield Lattice Diagram of the Splitting Field:**

$$\begin{tikzcd}
\mathbb{Q} \arrow[d, dash] \\
\mathbb{Q}(\omega_3)
\end{tikzcd}$$

$\blacksquare$

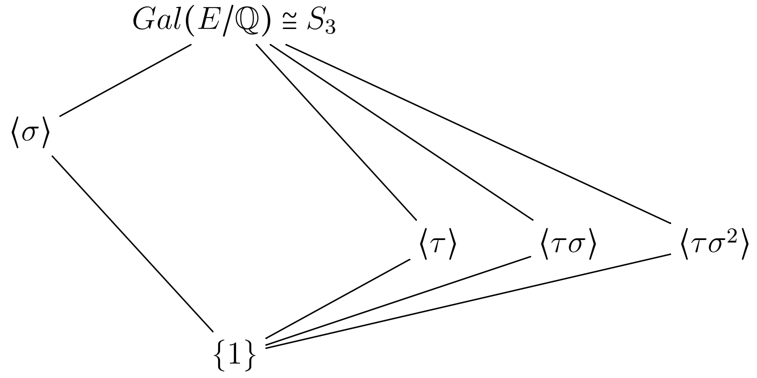
Proof. For $x^3 - 2$.

- **Splitting Field:** Note that $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega_3)(x - \sqrt[3]{2}\omega_3^2)$. The splitting field E of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega_3)$.
- **Galois Group:** The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$. The minimal polynomial of ω_3 over $\mathbb{Q}$ is $x^2 + x + 1$. By theorem, if $f \in Gal(E/\mathbb{Q})$, then $f(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \sqrt[3]{2}\omega_3, \sqrt[3]{2}\omega_3^2\}$ and $f(\omega_3) \in \{\omega_3, \omega_3^2\}$. Let

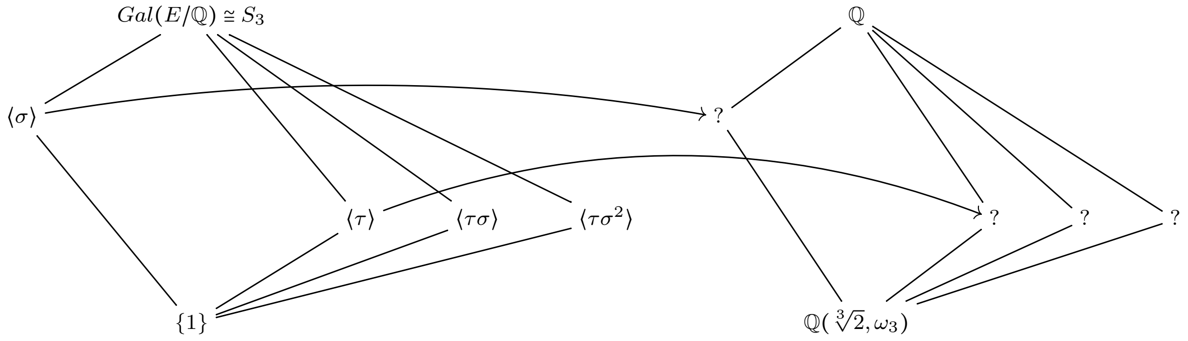
$$\sigma = \begin{cases} \sqrt[3]{2} \to \sqrt[3]{2}\omega_3 \\ \omega_3 \to \omega_3 \end{cases}, \quad \tau = \begin{cases} \sqrt[3]{2} \to \sqrt[3]{2} \\ \omega_3 \to \omega_3^2 \end{cases}$$

You can verify that $|\sigma| = 3$ and $|\tau| = 2$ and $\sigma\tau = \tau\sigma^2$. Then $Gal(E/\mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} \cong S_3 \cong D_3$.

- **Draw the Subgroup Lattice Diagram of the Galois Group:**


$Gal(E/\mathbb{Q}) \cong S_3$
$\langle\sigma\rangle$
$\langle\tau\rangle$
$\langle\tau\sigma\rangle$
$\langle\tau\sigma^2\rangle$
$\{1\}$

- **Use the Galois Correspondence to Determine the Fixed Field of the Subgroups of the Galois Group:**

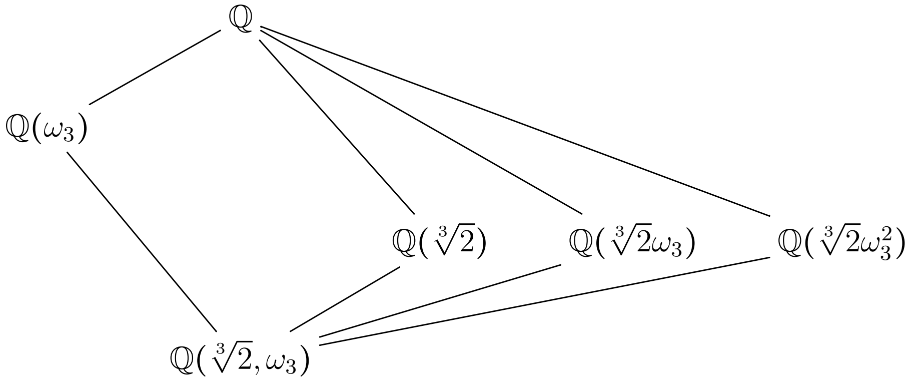

$Gal(E/\mathbb{Q}) \cong S_3$
$\langle\sigma\rangle$
$\langle\tau\rangle$
$\langle\tau\sigma\rangle$
$\langle\tau\sigma^2\rangle$
$\{1\}$
$\mathbb{Q}$
?
?
?
?
$\mathbb{Q}(\sqrt[3]{2}, \omega_3)$

In this case, since $\sigma(\omega_3) = \omega_3$, the fixed field of $\langle\sigma\rangle$ is $\mathbb{Q}(\omega_3)$. Since $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, the fixed field of $\langle\tau\rangle$ is $\mathbb{Q}(\sqrt[3]{2})$. Similarly, since

$$\tau\sigma(\sqrt[3]{2}\omega_3) = \tau(\sigma(\sqrt[3]{2})\sigma(\omega_3)) = \tau(\sqrt[3]{2}\omega_3 \cdot \omega_3) = \sqrt[3]{2}\omega_3^4 = \sqrt[3]{2}\omega_3,$$

we get that the fixed field of $\langle\tau\sigma\rangle$ is $\mathbb{Q}(\sqrt[3]{2}\omega_3)$.

- **Draw the Subfield Lattice Diagram of the Splitting Field:**


$\mathbb{Q}$
$\mathbb{Q}(\omega_3)$
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\sqrt[3]{2}\omega_3)$
$\mathbb{Q}(\sqrt[3]{2}\omega_3^2)$
$\mathbb{Q}(\sqrt[3]{2}, \omega_3)$

■

25.21 Prove that the only nontrivial proper normal subgroup of S_5 is A_5.

Proof.

$$
\begin{array}{cl}
\text{Suppose that} & \{e\} \lneqq H \lneqq S_5 \text{ and } A_5 \neq H \lhd S_5 \\
\overset{\substack{\text{normal } \cap \text{ normal } = \text{ normal} \\ \downarrow}}{\Rightarrow} & H \cap A_5 \lhd S_5 \\
\Rightarrow & H \cap A_5 \lhd A_5 \\
\overset{\substack{A_5 \text{ is simple} \\ \downarrow}}{\Rightarrow} & H \cap A_5 = A_5 \text{ or } \{e\} \\
 & \\
\text{If} & H \cap A_5 = A_5 \\
\Rightarrow & A_5 \leq H \\
\overset{\substack{A_5 \neq H \neq S_5 \\ \downarrow}}{\Rightarrow} & |A_5| = 60 < |H| < 120 = |S_5|, \\
 & \text{a contradiction because } |H| \text{ divides } |S_5|. \\
\text{If} & H \cap A_5 = \{e\} \\
\overset{\substack{H \lhd G,\ HA_5 \leq S_5 \\ \downarrow}}{\Rightarrow} & 120 = |S_5| \geq |HA_5| = \dfrac{|H| \cdot |A_5|}{|H \cap A_5|} = 60 \cdot |H| \\
\Rightarrow & |H| \leq 2 \\
\overset{\substack{H \neq \{e\} \\ \downarrow}}{\Rightarrow} & |H| = 2 \\
\Rightarrow & H = \langle h \rangle \text{ for some } h \in S_5 \text{ with } |h| = 2 \\
\overset{\substack{H \cap A_5 = \{e\},\ h \notin A_5 \\ \downarrow}}{\Rightarrow} & h = (ij) \text{ for some } i \neq j \in \{1, 2, 3, 4, 5\} \\
\overset{\substack{H \lhd S_5 \\ \downarrow}}{\Rightarrow} & ghg^{-1} \in H \text{ for any } g \in S_5, \\
 & \text{a contradiction because } |H| = 2.
\end{array}
$$

■

32.27 Show that S_5 is not solvable.

Proof. By Exercise 25.21, the only nontrivial proper normal subgroup of S_5 is A_5. In addition, A_5 is simple. Thus, there are only two group series of S_5. That is, $\{e\} \lhd S_5$ and $\{e\} \lhd A_5 \lhd S_5$. Both group series has a non-abelian factor. ■

32.28 Show that the dihedral groups are solvable.

Proof. $D_n = \langle\{a, b \mid |a| = n, |b| = 2, aba = b\}$ always has a group series $\{1\} \overbrace{\lhd}^{\cong \mathbb{Z}_n} \langle a \rangle \overbrace{\lhd}^{\cong \mathbb{Z}_2} D_n$, each factor is abelian. ■

32.29 Show that a group of order p^n, where p is prime, is solvable.

Proof. We use induction on n. When $p = 1$, $G \cong \mathbb{Z}_p$ is solvable. Suppose that a group of order p^n is solvable and $|G| = p^{n+1}$. By Sylow 1st Theorem, there exists a normal subgroup H of G which is of order p^n. By the induction hypothesis, H is solvable. Thus, we have H is solvable and $G/H \cong \mathbb{Z}_p$ is solvable, by Theorem 32.4 in p.563, G is also solvable. ■

32.30 Show that S_n is solvable when $n \leq 4$.

Proof. S_1 and S_2 are abelian.

$$\{e\} \overbrace{\lhd}^{\cong\mathbb{Z}_3} \langle(123)\rangle \overbrace{\lhd}^{\cong\mathbb{Z}_2} S_3.$$

$$\{e\} \overbrace{\lhd}^{\cong\mathbb{Z}_2\oplus\mathbb{Z}_2} \langle(12)(34),(13)(24)\rangle \overbrace{\lhd}^{\cong\mathbb{Z}_3} A_4 \overbrace{\lhd}^{\cong\mathbb{Z}_2} S_4.$$

■

26 Chapter 33

題組 Some Propertis of $\Phi_n(x)$

33.4, 33.5, 33.8, 33.10,

題組 以簡御繁

33.13, 33.14, 33.17

注意到這幾題的結果, 讓我們可以去計算 $\Phi_n(x)$, 即使 n 很大時

題組 Advanced Exercises

33.19, 33.20, 33.7, 33.9, 33.12, 33.11, 33.15

題組 Galois Theory

33.16, 33.18, 33.21

33.1 Determine the minimal polynomial for $\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)$ over $\mathbb{Q}$.

Proof. $\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right) = \cos\left(\frac{2\pi}{6}\right) + i\sin\left(\frac{2\pi}{6}\right) = \omega_6$, a primitive 6th root of unity. Its minimal polynomial is $\Phi_6(x)$. ■

33.2 Factor $x^{12} - 1$ as a product of irreducible polynomials over $\mathbb{Z}$.

Proof. By Theorem 33.3, $\Phi_n(x)$ is irreducible over $\mathbb{Z}$ for any n.

$$x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x).$$

■

33.3 Factor $x^8 - 1$ as a product of irreducible polynomials over $\mathbb{Z}_2, \mathbb{Z}_3$, and $\mathbb{Z}_5$.

Proof.

$$\begin{aligned} x^8 - 1 &= \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x) \in \mathbb{Z}[x] \\ &= (x-1)(x+1)(x^2+1)(x^4+1) \in \mathbb{Z}[x] \\ &= (x-1)(x-1)(x^2-1)(x^4-1) \in \mathbb{Z}_2[x] \\ &= (x-1)^8 \in \mathbb{Z}_2[x] \end{aligned}$$

Recall that

$$x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1) \in \mathbb{Z}[x].$$

We need to know the irreducibility of x^4+1 over $\mathbb{Z}_3$. Consider all the monic quadratic polynomial in $\mathbb{Z}_3[x]$ are

$$\begin{array}{rl}
\cancel{x^2} & \text{has root } 0 \\
x^2+1 & \leftarrow \\
\cancel{x^2+2} & \text{has root } 1 \\
\cancel{x^2+x} & \text{has root } 0 \\
\cancel{x^2+x+1} & \text{has root } 1 \\
x^2+x+2 & \leftarrow \\
\cancel{x^2+2x} & \text{has root } 0 \\
\cancel{x^2+2x+1} & \text{has root } 2 \\
x^2+2x+2 & \leftarrow
\end{array}$$

We cancel the polynomial which has a root in $\mathbb{Z}_3$. Then x^2+1, x^2+x+2 and x^2+2x+2 are all the monic irreducible quadratic polynomial over $\mathbb{Z}_3$.

Since x^4+1 has no root in $\mathbb{Z}_3$, if x^4+1 is reducible, then x^4+1 must be a product of two monic irreducible quadratic polynomials. By some computation.

$$\begin{array}{rcl}
(x^2+1)^2 & \neq & x^4+1 \\
(x^2+x+2)^2 & \neq & x^4+1 \\
(x^2+2x+2)^2 & \neq & x^4+1 \\
(x^2+1)(x^2+x+2) & \neq & x^4+1 \\
(x^2+x+2)(x^2+2x+2) & = & x^4+1 \\
(x^2+1)(x^2+2x+2) & \neq & x^4+1
\end{array}$$

Therefore,

$$x^8 - 1 = (x-1)(x+1)(x^2+1)\underline{(x^2+x+2)(x^2+2x+2)} \in \mathbb{Z}_3[x].$$

$$\begin{array}{rcl}
x^8 - 1 & = & (x-1)(x+1)(x^2+1)(x^4+1) \in \mathbb{Z}[x] \\
& = & (x-1)(x+1)(x^2-4)(x^4-4) \in \mathbb{Z}_5[x] \\
& = & (x-1)(x+1)(x+2)(x-2)(x^4-4) \in \mathbb{Z}_5[x] \\
& = & (x-1)(x+1)(x+2)(x-2)(x^2+2)(x^2-2) \in \mathbb{Z}_5[x]
\end{array}$$

(x^2+2) and (x^2-2) both have no root in $\mathbb{Z}_5$, they are irreducible over $\mathbb{Z}_5$.

■

33.4 For any $n > 1$, prove that the sum of all nth roots of unity is 0.

Proof. Let ω_n be a primitive nth root of unity.

$$x^n - 1 = (x-\omega_n)(x-\omega_n^2)(x-\omega_n^3)\cdots(x-\omega_n^n).$$

Compare the coefficients. ■

33.5 For any $n > 1$, prove that the product of the nth roots of unity is $(-1)^{n+1}$.

Proof. See Exercise 33.4. ■

33.6 Let ω be a primitive 12th root of unity over $\mathbb{Q}$. Find the minimal polynomial for ω^4 over $\mathbb{Q}$.

Proof. ω^4 is a primitive 3th root of unity over $\mathbb{Q}$. Its minimal polynomial is $\Phi_3(x)$. ■

33.7 Let F be a finite extension of $\mathbb{Q}$. Prove that there are only a finite number of roots of unity in F.

Proof. **Lemma.** $\lim_{n\to\infty} \phi(n) = \infty$, where $\phi(n) = \sharp\{d \in \mathbb{Z}^+ \mid \gcd(n,d) = 1\}$.

If $[F : \mathbb{Q}] = n$ and there are infinitely many number of roots of unity in F, then by Lemma, there exists $\omega_m \in F$ such that $\phi(m) > n$ and

$$\overbrace{\mathbb{Q} \underbrace{\le}_{\phi(m)} \mathbb{Q}(\omega_m) \le F}^{n},$$

a contradiction. ■

33.8 For any $n > 1$, prove that the irreducible factorization over $\mathbb{Z}$ of $x^{n-1} + x^{n-2} + \cdots + x + 1$ is $\prod \Phi_d(x)$, where the product runs over all positive divisors d of n greater than 1.

Proof.

$$\begin{aligned}
x^n - 1 &= \cancel{(x-1)}(x^{n-1} + x^{n-2} + \cdots + x + 1) \\
&= \prod_{d|n} \Phi_d(x) \\
&= \Phi_1(x) \prod_{1<d|n} \Phi_d(x) \\
&= \cancel{(x-1)} \prod_{1<d|n} \Phi_d(x)
\end{aligned}$$

■

33.9 If $2^n + 1$ is prime for some $n \ge 1$, prove that n is a power of 2. (Prime of the form $2^n + 1$ are called Fermat primes.)

補充. 這個定理很有名, Fermat當初發現這個定理的反向時, 他觀察到

$$\begin{aligned}
2^{2^1} + 1 &= 5 \\
2^{2^2} + 1 &= 17 \\
2^{2^3} + 1 &= 17 \\
2^{2^4} + 1 &= 257 \\
2^{2^5} + 1 &= 65537
\end{aligned}$$

全部都是質數, 所以 Fermat 宣稱只要是型如 $2^{2^n} + 1$ 的數字都是質數, 但後來數學家們發現他的這個猜測是錯的, 因爲 $2^{2^6} + 1$ 就不是質數。

33.10 Prove that $\Phi_n(0) = 1$ for all $n > 1$.

Proof. Use induction on n and

$$x^n - 1 = (x-1) \prod_{1<d|n} \Phi_d(x).$$

■

33.11 Prove that if a field contains the nth root of unity for n odd, then it also contains the $2n$th roots of unity.

Proof. It is immediately follows from Exercise 33.12.

Another method: When $n = 1$, the assertion holds obviously. If $\alpha \in F$ is a primitive nth root of unity, then $\Phi_n(\alpha) = 0$. Since $-\alpha \in F$ and $n > 1$ is odd, by Exercise 33.13, we have $\Phi_{2n}(-\alpha) = \Phi_n(\alpha) = 0$. That is, F contains a primitive $2n$th root of unity $-\alpha$. ■

33.12 Let m and n be relatively prime positive integers. Prove that the splitting field of $x^{mn} - 1$ over $\mathbb{Q}$ is the same as the splitting field of $(x^m - 1)(x^n - 1)$ over $\mathbb{Q}$.

Proof. **Lemma.** Suppose that $\gcd(m,n) = 1$. Let ω_m and ω_n be a primitive mth and nth root of unity, respectively. Then $\omega_m \cdot \omega_n = \omega_{mn}$ is a primitive mnth root of unity.

Proof of the Lemma. Since $\gcd(m,n) = 1$, $\langle\omega_m\rangle \cap \langle\omega_n\rangle = \{1\}$. If $(\omega_m\omega_n)^s = 1$, then $\omega_m^s = (\omega_n^s)^{-1} \in \langle\omega_m\rangle \cap \langle\omega_n\rangle = \{1\}$ and $\omega_m^s = 1 = \omega_n^s$. It follows that $m \mid s$ and $n \mid s$. Since $\gcd(m,n) = 1$, we have $mn \mid s$. Note that $(\omega_m\omega_n)^{mn} = (\omega_m)^{mn}(\omega_n)^{nm} = 1$. Therefore, mn is the multiplicative order of $\omega_m\omega_n$ and $\omega_m\omega_n = \omega_{mm}$.

The splitting field of $x^{mn}-1$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega_{mn})$. The splitting field of $(x^m-1)(x^n-1)$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega_m, \omega_n)$.

Since $\omega_{mn}^n = \omega_m$ and $\omega_{mn}^m = \omega_n$, we get $\mathbb{Q}(\omega_m, \omega_n) \subseteq \mathbb{Q}(\omega_{mn})$.

By Lemma, $\omega_{mn} \in \mathbb{Q}(\omega_m, \omega_n)$. Therefore, $\mathbb{Q}(\omega_{mn}) \subseteq \mathbb{Q}(\omega_m, \omega_n)$. ■

33.13 Prove that $\Phi_{2n}(x) = \Phi_n(-x)$ for all odd integers $n > 1$.

Proof. [**方法一**] First note that $\deg \Phi_{2n}(x) = \deg \Phi_n(-x)$. If $-\omega$ is a root of $\Phi_n(-x)$, then $|\omega| = n$ and $|-\omega| = \operatorname{lcm}(|-1|, |\omega|) = \operatorname{lcm}(2,n) \overset{\overset{n \text{ is odd}}{\downarrow}}{=} 2n$. That is, $-\omega$ is a root of $\Phi_{2n}(x)$. It follows that $\Phi_n(-x) \mid \Phi_{2n}(x)$. Hence $\Phi_n(-x) = \Phi_{2n}(x)$ because they have the same degree.

[**方法二**] Use induction on n. When $n = 3$,

$$\Phi_{2n}(x) = \Phi_6(x) = x^2 - x + 1 = (-x)^2 + (-x) + 1 = \Phi_3(-x).$$

Suppose that $\Phi_{2k}(x) = \Phi_k(-x)$ holds when $1 < k < n$ and k is odd. Then

$$\begin{aligned}
\Phi_{2n}(x) &= \frac{x^{2n}-1}{\prod\limits_{\substack{d|2n\\ d\neq 2n}} \Phi_d(x)} = \frac{(x^n-1)}{\prod\limits_{\substack{d|2n\\ d \text{ odd}}} \Phi_d(x)} \cdot \frac{(x^n+1)}{\prod\limits_{\substack{d|2n\\ d \text{ even}\\ d\neq 2n}} \Phi_d(x)} \\
&\overset{\substack{\gcd(d,2)=1\\ \downarrow}}{=} \frac{(x^n-1)}{\prod\limits_{\substack{d|n\\ d \text{ odd}}} \Phi_d(x)} \cdot \frac{(x^n+1)}{\prod\limits_{\substack{d|2n\\ d \text{ even}\\ d\neq 2n}} \Phi_d(x)} = \cancel{\frac{(x^n-1)}{\prod\limits_{\substack{d|n\\ d \text{ odd}}} \Phi_d(x)}} \cdot \frac{(x^n+1)}{\prod\limits_{\substack{2k|2n\\ k\neq n}} \Phi_{2k}(x)} \\
&\overset{\substack{n \text{ is odd}\\ \downarrow}}{=} \frac{(x^n+1)}{\prod\limits_{\substack{k|n\\ k \text{ odd}\\ k\neq n}} \Phi_{2k}(x)} = \frac{(x^n+1)}{\Phi_2(x)\cdot \prod\limits_{\substack{k|n\\ k \text{ odd}\\ 1<k<n}} \Phi_{2k}(x)} \\
&\overset{\substack{\text{induction hypothesis}\\ \downarrow}}{=} \frac{(x^n+1)}{\Phi_2(x)\cdot \prod\limits_{\substack{k|n\\ k \text{ odd}\\ 1<k<n}} \Phi_k(-x)} = \frac{\Phi_1(-x)}{\Phi_2(x)} \cdot \frac{(x^n+1)}{\Phi_1(-x)\cdot \prod\limits_{\substack{k|n\\ k \text{ odd}\\ 1<k<n}} \Phi_k(-x)} \\
&= \frac{-x-1}{x+1} \cdot \frac{(x^n+1)}{\prod\limits_{\substack{k|n\\ k \text{ odd}\\ 1\leq k<n}} \Phi_k(-x)} = (-1)\cdot \frac{-[(-x)^n-1]}{\prod\limits_{\substack{k|n\\ k \text{ odd}\\ 1\leq k<n}} \Phi_k(-x)} \\
&= \Phi_n(-x)
\end{aligned}$$

■

33.14 Prove that if p is a prime and k is a positive integer, then $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$. Use this to find $\Phi_8(x)$ and $\Phi_{27}(x)$.

Proof.

$$\begin{aligned}
\Phi_{p^k}(x) &= \frac{x^{p^k}-1}{\prod\limits_{\substack{d|p^k\\ d\neq p^k}} \Phi_d(x)} \\
&= \frac{(x^{p^{k-1}})^p-1}{\prod\limits_{d|p^{k-1}} \Phi_d(x)} \\
&= \frac{(x^{p^{k-1}})^p-1}{x^{p^{k-1}}-1} \\
&\overset{\substack{\Phi_p(x)=\frac{x^p-1}{\Phi_1(x)}=\frac{x^p-1}{x-1}\\ \downarrow}}{=} \Phi_p(x^{p^{k-1}})
\end{aligned}$$

$$\Phi_8(x) = \Phi_{2^3}(x) = \Phi_2(x^{2^{3-1}}) = \Phi_2(x^4) = x^4+1.$$

$$\Phi_{27}(x) = \Phi_{3^3}(x) = \Phi_3(x^{3^{3-1}}) = \Phi_3(x^9) = (x^9)^2+x^9+1.$$

■

33.15 Prove he assertion made in the proof of Theorem 33.5 that there exists a series of subgroups $H_0 \subset H_1 \subset \cdots \subset H_t$ with $|H_{i+1} : H_i| = 2$ for $i = 0, 1, 2, \ldots, t-1$.

33.16 Prove that $x^9 - 1$ and $x^7 - 1$ have isomorphic Galois groups over $\mathbb{Q}$.

33.17 Let p be a prime that does not divide n. Prove that $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.

Proof. Use induction on n. When $n = 1$,

$$\Phi_{pn}(x) = \Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = \Phi_1(x^p)/\Phi_1(x).$$

Suppose that $\Phi_{ps}(x) = \Phi_s(x^p)/\Phi_s(x)$ for any $s < n$. Then

$$\begin{aligned}
\Phi_{pn}(x) &= \frac{x^{pn} - 1}{\prod\limits_{\substack{d|pn\\ d\neq pn}} \Phi_d(x)} \\
&= \frac{(x^p)^n - 1}{\prod\limits_{\substack{p\nmid d\\ d|n}} \Phi_d(x) \prod\limits_{\substack{p|d\\ d=ps\\ s|n\\ s\neq n}} \Phi_{ps}(x)} \\
&= \frac{(x^p)^n - 1}{(x^n - 1)\cdot \prod\limits_{\substack{s|n\\ s\neq n}} \frac{\Phi_s(x^p)}{\Phi_s(x)}} \\
&= \frac{(x^p)^n - 1}{\frac{x^n - 1}{\prod\limits_{\substack{s|n\\ s\neq n}} \Phi_s(x)} \cdot \prod\limits_{\substack{s|n\\ s\neq n}} \Phi_s(x^p)} \\
&= \frac{\Phi_n(x^p)}{\Phi_n(x)}
\end{aligned}$$

■

33.18 Prove that the Galois groups of $x^{10} - 1$ and $x^8 - 1$ over $\mathbb{Q}$ are not isomorphic.

33.19 Let E be the splitting field of $x^5 - 1$ over $\mathbb{Q}$. Show that there is a unique field K with the property that $\mathbb{Q} \subset K \subset E$.

33.20 Let E be the splitting field of $x^6 - 1$ over $\mathbb{Q}$. Show that there is no field K with the property that $\mathbb{Q} \subset K \subset E$

Proof. Since $x^6 - 1 = \prod\limits_{i=1}^{6}(x - \omega_6^i)$, where ω_6 is a primitive 6th root of unity, the splitting field E for $x^6 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega_6)$. The minimal polynomial of ω_6 is $\Phi_6(x)$. Thus, $[E:\mathbb{Q}] = \deg \Phi_6(x) = 2$.

If K is a subfield of E and $\mathbb{Q} \leq K \leq E$, consider the tower of fields

$$\overbrace{\mathbb{Q} \leq K \leq E}^{2},$$

then $K = \mathbb{Q}$ or $K = E$. ■

33.21 Let $\omega = \cos(2\pi/15) - i\sin(2\pi/15)$. Find the three elements of $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ of order 2.

補充 33.A Use the identity

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

to determine the cyclotomic polynomials $\Phi_8(x)$ and $\Phi_{12}(x)$.

Proof.

$$\begin{aligned}
\Phi_8(x) &= \frac{x^8-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)} \\
&= \frac{\cancel{(x^4-1)}(x^4+1)}{\cancel{\Phi_1(x)\Phi_2(x)\Phi_4(x)}} \\
&= x^4+1.
\end{aligned}$$

$$\begin{aligned}
\Phi_4(x) &= \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} \\
&= \frac{\cancel{(x^2-1)}(x^2+1)}{\cancel{\Phi_1(x)\Phi_2(x)}} \\
&= x^2+1.
\end{aligned}$$

$$\begin{aligned}
\Phi_{12}(x) &= \frac{x^{12}-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)} \\
&= \frac{\cancel{(x^6-1)}(x^6+1)}{\cancel{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)}\Phi_4(x)} \\
&= \frac{(x^2)^3+1}{x^2+1} \\
&= \frac{\cancel{(x^2+1)}(x^4-x^2+1)}{\cancel{x^2+1}} \\
&= x^4-x^2+1.
\end{aligned}$$

■

補充 33.B

- □ $\Phi_1(x) =$
- □ $\Phi_2(x) =$
- □ $\Phi_3(x) =$
- □ $\Phi_4(x) =$
- □ $\Phi_5(x) =$
- □ $\Phi_6(x) =$
- □ $\Phi_7(x) =$
- □ $\Phi_8(x) =$
- □ $\Phi_9(x) =$
- □ $\Phi_{10}(x) =$
- □ $\Phi_{11}(x) =$
- □ $\Phi_{12}(x) =$