因此 $\mathrm{Aut}(G)\simeq(\pm 1\}$。

例題: 請決定 $\boldsymbol{Z}_9$ 的自同構羣。

解: 設 f: $\boldsymbol{Z}_9\longrightarrow\boldsymbol{Z}_9$ 是自同構。若 $f(\overline{1})=\overline{i}$。因爲 f 是單射，因此 $\overline{i}\ \overline{x}=\overline{0}$ 的充要條件是 $\overline{x}=\overline{0}$。可見 i 必與 9 互質。答案: $\mathrm{Aut}(\boldsymbol{Z}_9)\cong\{\overline{1},\ \overline{2},\ \overline{4},\ \overline{5},\ \overline{7},\ \overline{8}\}=\boldsymbol{Z}_9^{\times}$。一般的情形，$\mathrm{Aut}\ (\boldsymbol{Z}_n)=\boldsymbol{Z}_n^{\times}$（請利用引理2.44.）。

例題: 請決定 S_3 的自同構羣。

解: 因爲 $Z(S_3)=\{\varepsilon\}$，S_3 的元素所決定的內自構都不一樣，所以 $\mathrm{Aut}\ (S_3)$ 至少有 6 個元素。

另一方面，S_3 所有秩爲 2 的元素是 $\{(1\ 2),\ (1\ 3),\ (2\ 3)\}$，而任何自同構一定把秩爲 2 的元素對應到秩爲 2 的元素。因此，任何自同構把 $\{(1\ 2),\ (1\ 3),\ (2\ 3)\}$ 對應到 $\{(1\ 2),\ (1\ 3),\ (2\ 3)\}$。而 S_3 至多只有 6 種可能把 $\{(1\ 2),\ (1\ 3),\ (2\ 3)\}$ 對應到其自身。如果 $(1\ 2),\ (1\ 3),\ (2\ 3)$ 的函數值一經確定，這個函數卽已確定，因爲任何置換都可表示成 $(1\ 2),\ (1\ 3),\ (2\ 3)$ 的乘積。

結論是，$\mathrm{Aut}\ (S_3)$ 恰有 6 個元素，每一個都是內自同構，並且 $\mathrm{Aut}(S_3)\simeq S_3$。

討論: 若 $n\neq 6$ 且 $n\geqslant 3$，則 $\mathrm{Aut}\ (S_n)\simeq S_n$。有興趣的讀者請看〔Suzuki, 1982, 第299～300頁〕。

習題

1. 令 x_1 與 x_2 是羣 G 的元素。試證，x_1 與 x_2 互爲共軛的充分必要條件是存在一個 G 的內自同構 φ_a，使得 $x_2=\varphi_a(x_1)$。
2. 設 G 是羣。若 $Z(G)=\{1\}$，則 $Z(\mathrm{Aut}(G))=\{id\}$。
3. 設 G 是秩爲 n 的羣。試證 $|\mathrm{Aut}(G)|<n^a$，其中 a 是某個實數並且 $a\leqslant\log_2 n$。（提示: 令 $\{x_1,\cdots,x_m\}$ 是 G 的最小生成集。則 $|\mathrm{Aut}\ G|<n^m$。令 H_i 是 $\{x_1,\cdots,x_i\}$ 生成的子羣，則 $H_i\supsetneq H_{i-1}$。根據定理2.31.，$n=|G|=\langle H_m: H_{m-1}\rangle\langle H_{m-1}: H_{m-2}\rangle\cdots\langle H_1:\{1\}\rangle\geqslant 2^m$。）
4. 若 φ: $\boldsymbol{Q}\longrightarrow\boldsymbol{Z}_n$ 是羣的同態，則 $\varphi(a)=0\ \forall a\in\boldsymbol{Q}$。
5. 設 $\boldsymbol{Q}^+=\{r\in\boldsymbol{Q}: r>0\}$，$(\boldsymbol{Q};+)$ 與 $(\boldsymbol{Q}^+;\times)$ 會不會同構？$(\boldsymbol{Z}[x];+)$ 與 $(\boldsymbol{Q}^+;\times)$ 會不會同構？（提示: 如果 $\frac{12}{25}=2^2\cdot 3\cdot 5^{-2}\in\boldsymbol{Q}^+$，我們把它對應到 $2+x-2x^2$。你能否由此想到 $\boldsymbol{Q}^+$ 到 $\boldsymbol{Z}[x]$ 的某一個同構？）
6. 在第 2.26 小節的第二個例題，如果把 $3\nmid|G|$ 的條件去掉，結果會變得怎樣呢？例如，你能不能找個秩爲27的羣 G，使得 $\forall x, y\in G$, $(xy)^3=x^3y^3$，但是 G 不是交換羣？

第四節 子羣與正則子羣

2.30.

回憶一下子羣的定義（定義 2.17.）。設 $(G;\circ)$ 是羣，H 是 G 的子集合，並且 $H\neq\phi$，如果 H 在「$\circ$」的運算下形成羣，則 H 叫做 G 的子羣。

如果 H 是 G 的子羣，那麼 H 與 G 有同樣的單位元，因爲，令 1_H 是 H 的單位元，則 $1_H\cdot 1_H=1_H$。但是 H 的運算和 G 的運算一樣，因此 $1_H\cdot 1_H=1_H$ 在 G 之內也成立。可見 1_H 是 G 的單位元。

引理: 設 $(G;\circ)$ 是羣，H 是 G 的子集合，且 $H\neq\phi$。則 H 是 G 的子羣 $\Longleftrightarrow\forall x, y\in H$, xy, $x^{-1}\in H$。

證明: "⇒" 因爲 $(H;\circ)$ 是羣，如果 $x, y\in H$，顯然 $xy\in H$，並且存在一個元素 $z\in H$ 使得 $x\circ z=z\circ x=1$，由逆元的唯一性（引理2.3.(2)）可知 $x^{-1}=z\in H$。

"⇐" 只需證明 $1\in H$。因爲 $H\neq\phi$，令 $x\in H$。因此 $x^{-1}\in H$。現在 $x, x^{-1}\in H$，因此可得 $1=x\cdot x^{-1}\in H$。

例如，$(\boldsymbol{Z};+;0)$ 是 $(\boldsymbol{Q};+;0)$ 的子羣，$(\boldsymbol{Q};+;0)$ 是 $(\boldsymbol{R};+;0)$ 的子羣；$\{z\in\boldsymbol{C}:|z|=1\}$ 是 $(\boldsymbol{C}\setminus\{0\};\times;1)$ 的子羣。$\{\overline{0},\overline{2}\}$ 是 $\boldsymbol{Z}_4$ 的子羣。A_n 是 S_n 的子羣。

$G=\{\pm1\}$ 在通常的乘法之下形成羣。G是 $(\boldsymbol{Z};+;0)$ 的子集合，但是它不是 $(\boldsymbol{Z};+;0)$ 的子羣，因爲二者的運算並不同，其單位元也不同。

2.31.

定理：(Lagrange 定理) 若G是有限羣，H是其子羣，則 $|H|\,\big|\,|G|$。

證明：若 $x\in G$，定義 $xH=\{xh\in G: h\in H\}$。

步驟1：$G=\bigcup_{x\in G}xH$

因爲 $xH\subset G$，顯然 $G\supset\bigcup_{x\in G}xH$。另一方面，$\forall x\in G$，$x=x\cdot1\in xH$。所以 $G\subset\bigcup_{x\in G}xH$.

步驟2：若 $x, y\in G$，則 $xH=yH$ 或 $xH\cap yH=\phi$。

如果 $z\in xH\cap yH$，則 $x^{-1}z, y^{-1}z\in H$。故 $y^{-1}x=(y^{-1}z)\cdot(x^{-1}z)^{-1}\in H$（注意 $(x^{-1}z)^{-1}\in H$，因爲H是子羣）。當然 $x^{-1}y\in H$ 也成立。現在 $xH=(y\cdot y^{-1}x)H=y\cdot\{(y^{-1}x)H\}\subset y\cdot H$，因爲 $y^{-1}x\in H$ 且H是子羣。同理 $yH\subset xH$。

步驟3：由步驟2，我們可以把 $G=\bigcup_{x\in G}xH$ 中重覆 xH 的丟掉，得 $G=\bigcup_{i=1}^{n}x_iH$，其中當 $i\neq j$ 時 $x_iH\cap x_jH=\phi$。令 $|xH|$ 代表集合 xH 元素的個數。但是 $|xH|=|H|$（何故？），得 $|G|=n\cdot|H|$。

定義：當羣H是有限羣G的子羣，定義 $[G: H]=\dfrac{|G|}{|H|}$。$[G: H]$ 叫做H在G中的指標（index）。根據以上 Lagrange 定理，$[G: H]$ 是個正整數，顯然，$|G|=|H|\cdot[G: H]$。

2.32.

定義：設H是羣G的子羣。定義 $xH=\{xh\in G: h\in H\}$，xH 叫做H的一個左陪集（left coset）。同樣的，定義右陪集（right coset）$Hx=\{hx\in G: h\in H\}$。

若 A, B只是羣G的子集，我們可以仿照陪集的寫法，定義 $A\cdot B=\{ab\in G: a\in A, b\in B\}$。如果 $A=\{a\}$ 只有一個元素，我們常把 $\{a\}B$ 寫成 aB；同樣的，$A\{b\}$ 就是 Ab。如果A是G的子集，定義 $A^{-1}=\{a^{-1}: a\in A\}$。和通常的習慣一樣，$|A|$ 表示A的元素個數。

根據定理2.31.的證明，我們得到以下引理。

引理：設H是羣G的子羣，則 $xH=yH\Longleftrightarrow x^{-1}y\in H$, $Hx=Hy\Longleftrightarrow xy^{-1}\in H$。

定理：設H是羣G的子羣，則G有一個左陪集表示法（left coset decomposition），即存在元素 $x_i\in G$, $i\in I$, I是某個指標集（index set），使得 $G=\bigcup_{i\in I}x_iH$，其中當 $i\neq j$ 時 $x_iH\neq x_jH$。同樣的，G 有一個右陪集表示法，$G=\bigcup_{i\in I}Hy_i$，其中當 $i\neq j$ 時 $Hy_i\neq Hy_j$。注意，在左陪集表示法與右陪集表示法中，我們可以使用同一個指標集 I。

證明：只需證明左、右陪集表示法中可以採用同樣的指標集。在 $G=\bigcup_{i\in I}x_iH$，兩邊同取逆元，得 $G=G^{-1}=\bigcup_{i\in I}H^{-1}x_i^{-1}=\bigcup_{i\in I}Hx_i^{-1}$。如果$Hx_i^{-1}\cap Hx_j^{-1}\neq\phi$，則同取逆元之後有 $x_iH\cap x_jH\neq\phi$，故 $i=j$。因此 $G=\bigcup_{i\in I}Hy_i$, $y_i=x_i^{-1}$。

2.33.

現在我們要把羣的生成集（定義2.14.）的概念加以推廣。

如果 $(G;\circ;1)$ 是一個羣，$x\in G$，H是包含x的子羣。很顯然，當 $n=0,\pm1,\pm2,\cdots$時，$x^n\in H$。另一方面，$K=\{x^n: n=0,\pm1,\pm2,\cdots\}$ 是G的子羣。所以K是包含x的最小子羣。我們就說，K是$\{x\}$生成的羣（subgroup generated by $\{x\}$），$\{x\}$ 是K的生成集（generating set），記爲 $K=\langle x\rangle$。

一般的，如果S是G的任意子集，包含S的最小子羣K叫做由S生成的子羣（subgroup generated by S），而S叫做K的生成集（generating set），記爲 $K=\langle S\rangle$。問題：K的元素是那些呢？

顯然，如果從S取出任意n個個元素 $x_1, x_2,\cdots, x_n$ ($x_1,\cdots, x_n$ 容許重複，n是任意整數，$n\geqslant 0$)，$x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n}$ 必然落在K之內，其中 $\varepsilon_i=\pm1$。可是這些元素 $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n}$ 所形成的集合是G的子羣。因此，我們得到以下引理，

引理：設S是羣G的子集合。則 $\langle S\rangle=\{x_1^{\varepsilon_1}\cdots x_n^{\varepsilon_n}\in G: n=0, 1, 2,\cdots, \varepsilon_i=\pm1, x_i\in S, x_1,\cdots, x_n$ 容許重複$\}$。

例如，$\boldsymbol{Z}_9=\langle\overline{1}\rangle=\langle\overline{2}\rangle$，但是 $\boldsymbol{Z}_9\neq\langle\overline{3}\rangle$，因爲 $\langle\overline{3}\rangle=\{\overline{0}, \overline{3}, \overline{6}\}\neq\boldsymbol{Z}_9$。如果 $x, y\in G$，則 $\langle x\rangle=\{x^n: n=0, \pm1, \pm2,\cdots\}$，$\langle x, y\rangle=\{x^n: n\in\boldsymbol{Z}\}\cup\{y^n: n\in\boldsymbol{Z}\}\cup\{x^ny^m: n, m\in\boldsymbol{Z}\}\cup\{y^nx^m: n, m\in\boldsymbol{Z}\}\cup\{x^{n_1}y^{m_1}x^{n_2}: n_1, m_1, n_2\in\boldsymbol{Z}\}\cup\cdots$。

例題：若H是G的子羣且 $H\neq G$，請證明 $G=\langle G\setminus H\rangle$。

證明：由左陪集表示式（定理2.32.），$G=\bigcup\limits_{x_i\in I}x_iH$。可以令 $x_{i_0}=1$，故 $G\setminus H=\bigcup\limits_{i\neq i_0}x_iH$。因此只需證明 $H\subset\langle G\setminus H\rangle$。任取$h\in H$。令 $x_i\notin H$。則 $x_i^{-1}, x_ih\notin H$。所以 $h=x_i^{-1}(x_ih)\in\langle G\setminus H\rangle$。

2.34.

在定義 2.18.，我們定義羣的秩與元素的秩。現在我們要討論它們的關係。

設G是羣，$x\in G$。考慮 $\langle x\rangle=\{x^n\in G: n\in\boldsymbol{Z}\}$。

第一種可能：不可能找到正整數m使得 $x^m=1$。在這種情形下，$x^n(n=0, \pm1, \pm2,\cdots)$ 都是相異的元素（何故？）。定義 $f: \boldsymbol{Z}\longrightarrow\langle x\rangle$, $f(n)=x^n$，則f是羣的同構。因爲 $\langle x\rangle$ 是無限羣，我們不妨規定 ord $(x)=\infty$。

第二種可能：存在正整數m使得 $x^m=1$。令k是滿足 $x^k=1$ 的最小正整數，則 $\langle x\rangle=\{x^n\in G: n\in\boldsymbol{Z}\}=\{x^i: 0\leq i\leq k-1\}$，並且 x^i $(0\leq i\leq k-1)$ 都是相異的元素（何故？）。定義 $f: \boldsymbol{Z}_k\longrightarrow\langle x\rangle$, $f(\overline{i})=x^i$，則f是羣的同構。注意，我們定義 ord $(x)=k$，但是 $k=|\langle x\rangle|$。所以 ord $(x)=|\langle x\rangle|$。

引理：設G是羣，$x\in G$。

(1)ord(x) 正好是子羣 $\langle x\rangle$ 的秩。

(2)如果 ord$(x)=k$，則$\langle x\rangle\simeq\boldsymbol{Z}_k$。如果ord$(x)=\infty$，則 $\langle x\rangle\simeq\boldsymbol{Z}$。

(3)如果G是有限羣，則 ord $(x)\,\big|\,|G|$。

證明：(3)根據 Lagrange 定理（定理2.31.）。

例題：請列出 S_3 中各元素的秩。

解：$|S_3|=3!=6$。6的因子有 1, 2, 3, 6。

秩	元　　素
1	ε
2	(1 2), (1 3), (2 3)
3	(1 2 3), (1 3 2)

S_3 沒有秩爲 6 的元素。

例題：請列出 $\boldsymbol{Z}_{12}$ 中各元素的秩。

解:

秩	元　　素
1	$\overline{0}$
2	$\overline{6}$
3	$\overline{4}$, $\overline{8}$
4	$\overline{3}$, $\overline{9}$
6	$\overline{2}$, $\overline{10}$
12	$\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$

2.35.

例題: 請列出 S_4 的所有子羣。

解: $|S_4|=4!=24$, 24 的各種因子有 1, 2, 3, 4, 6, 8, 12, 24。但是 S_4 沒有秩爲 6, 8, 12的元素（請參考第2.19.小節）。

秩爲 24: S_4

秩爲 12: A_4（爲什麼 A_4 是秩爲12的唯一子羣？）

秩爲 8: $P_1=\langle(1\ 2\ 3\ 4),\ (1\ 3)\rangle$, $P_2=\langle(1\ 2\ 4\ 3),\ (1\ 4)\rangle$, $P_3=\langle(1\ 3\ 2\ 4),\ (1\ 2)\rangle$。

秩爲 6: $H_1=\langle(1\ 2),\ (1\ 2\ 3)\rangle$, $H_2=\langle(1\ 2),\ (1\ 2\ 4)\rangle$, $H_3=\langle(1\ 3),\ (1\ 3\ 4)\rangle$, $H_4=\langle(2\ 3),\ (2\ 3\ 4)\rangle$。

秩爲 4: $K_1=\langle(1\ 2\ 3\ 4)\rangle$, $K_2=\langle(1\ 2\ 4\ 3)\rangle$, $K_3=\langle(1\ 3\ 2\ 4)\rangle$, $V=\{\varepsilon,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3\}$, $N_1=\langle(1\ 2),\ (3\ 4)\rangle$, $N_2=\langle(1\ 3),\ (2\ 4)\rangle$, $N_3=\langle(1\ 4),\ (2\ 3)\rangle$。

秩爲 3: $\langle(1\ 2\ 3)\rangle$, $\langle(1\ 2\ 4)\rangle$, $\langle(1\ 3\ 4)\rangle$, $\langle(2\ 3\ 4)\rangle$。

秩爲 2: $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(1\ 4)\rangle$, $\langle(2\ 3)\rangle$, $\langle(2\ 4)\rangle$, $\langle(3\ 4)\rangle$。

秩爲 1: $\{\varepsilon\}$。

其中 P_1 P_2, P_3 其實與秩爲 8 的二面體羣是同構的（見第2.21.與2.47.小節）。

2.36.

如果H是G的子羣，我們可以考慮H的左陪集和右陪集。讀者可能希望 $xH=Hx$。但是，在一般情形，這是不可能的。

例如，在 S_4，令 $H=\{\varepsilon,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$，則 $(1\ 4)\cdot H=\{(1\ 4),\ (1\ 2\ 3\ 4),\ (1\ 3\ 2\ 4)\}$，$H\cdot(1\ 4)=\{(1\ 4),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)\}$，顯然 $(1\ 4)\cdot H\neq H\cdot(1\ 4)$。

定義: 設H是羣G的子羣。如果 $\forall x\in G,\ xH=Hx$，H叫做G的正則子羣（或稱正規子羣，normal subgroup）記爲$H\lhd G$。

在以上的定義，我們可以把「$\forall x\in G,\ xH=Hx$」的條件寫成「$\forall x\in G,\ xHx^{-1}=H$」。

如果H是G的有限子羣，「$xH=Hx$」和「$xH\subset Hx$」是等價的，因爲，當 $xH\subset Hx$ 時，$xHx^{-1}\subset H$，而 $|xHx^{-1}|=|H|<\infty$，故 $xHx^{-1}=H$。但是，當 $|H|=\infty$ 時，「$xH=Hx$」與「$xH\subset Hx$」並不是等價。例如，令

$$G=\left\{\begin{pmatrix} r & s\\ 0 & 1\end{pmatrix}:\ r,\ s\in\boldsymbol{R},\ r\neq 0\right\},\quad H=\left\{\begin{pmatrix} 1 & n\\ 0 & 1\end{pmatrix}:\ n\in\boldsymbol{Z}\right\},$$

在矩陣乘法之下，G形成羣，H是G的子羣。考慮

$$x=\begin{pmatrix} n & 0\\ 0 & 1\end{pmatrix},\ n=2,3,4,\cdots\cdots。$$

很容易可以檢驗出來，$xHx^{-1}\subset H$, $x^{-1}Hx\neq H$。

正則子羣的概念是 E. Galois 最先提出的。有了這個概念，我們才能有效的研究羣的更深入的性質。

如果G是交換羣，G的任意子羣都是正則子羣，因爲 $xHx^{-1}=\{xhx^{-1}\in G:\ h\in H\}=\{hxx^{-1}\in G:\ h\in H\}=\{h\in G:\ h\in H\}=H$。但是我們可以找到羣$G$，使得$G$不是交換羣，但是$G$的任意子羣都是正則子羣（本章第九節習題 9）。

讀者不難檢查出來，S_4 的所有子羣中（第2.35.小節），只有 S_4, A_4, V, $\{\varepsilon\}$ 是正則子羣。

引理：若H是羣G的子羣，以下三個敍述是等價的，

(1)H是G的正則子羣，

(2)$\forall x\in G,\ \forall h\in H,\ xhx^{-1}$ 必定落在H之內，

(3)$\forall x\in G,\ \forall s\in S,\ xsx^{-1}$ 必定落在H之內，其中S是H的某個生成集。

證明：「(1)⇒(2)」與「(2)⇒(3)」由讀者自己證明。

「(3)⇒(1)」：若 $h\in H$，則 h 可寫成 $s_1^{\pm1}s_2^{\pm1}\cdots s_n^{\pm1}$，其中 $s_i\in S$。$xhx^{-1}=x(s_1^{\pm1}\cdots s_n^{\pm1})x^{-1}=(xs_1^{\pm1}x^{-1})\cdot(xs_2^{\pm1}x^{-1})\cdots(xs_n^{\pm1}x^{-1})=(xs_1x^{-1})^{\pm1}\cdot(xs_2x^{-1})^{\pm1}\cdots(xs_nx^{-1})^{\pm1}$；但 $xs_ix^{-1}\in H$ 且H是子羣，故 $xhx^{-1}\in H$。因此我們已證明 $\forall x\in G,\ xHx^{-1}\subset H$。因此 $x^{-1}\cdot H\cdot x=x^{-1}H(x^{-1})^{-1}\subset H$，兩邊同時左乘$x$、右乘 x^{-1}，得 $H\subset xHx^{-1}$。因此 $\forall x\in G,\ xHx^{-1}=H$。

討論：我們已經定義了共軛元的概念（定義2.19.）。以上引理的第二個條件說，子羣H是正則子羣的充分必要條件是，如果 $x\in H$，則x所有共軛元也都在H之內。仿照共軛元的定義，我們也可以定義共軛子羣的概念。設H是羣G的子羣，$x\in G$，則我們稱H與 xHx^{-1} 互爲共軛子羣（conjugate subgroups）。$H\lhd G$ 的充分必要條件是H只有一個共軛子羣，即H本身。

2.37.

引理：設G是羣。

(1)$Z(G)=\{a\in G:\ \forall x\in G,\ ax=xa\}$ 是 G 的正則子羣。

(2)$[G,\ G]$ 也是G的正則子羣，其中 $[G,\ G]$ 是由 $\{xy\ x^{-1}y^{-1}\in G:\ x,\ y\in G\}$ 生成的子羣。

證明：(3)根據引理 2.36.，只需證明 $z(xyx^{-1}y^{-1})z^{-1}\in[G,\ G]$，$\forall x,\ y,\ z\in G$。令 $u=xy\ x^{-1}\ y^{-1}$，則 $z(xy\ x^{-1}\ y^{-1})z^{-1}=zuz^{-1}=(zu\ z^{-1}\ u^{-1})\cdot u$，而$zu\ z^{-1}\ u^{-1},\ u=xy\ x^{-1}\ y^{-1}\in[G,\ G]$!

定義：令 $[G,\ G]$ 是 $\{xyx^{-1}y^{-1}\in G:\ x,\ y\in G\}$ 生成的子羣，$[G,\ G]$ 叫做G的換位子羣（commutator subgroup）。形如 $xyx^{-1}y^{-1}$ 的元素叫做換位子（commutator）。

在 S_n 中，換位子一定是偶置換（何故？）。請猜猜看，偶置換是不是一定是換位子？

習題

1. 設G是羣，H是G的子集合，$H\neq\phi$。H是G的子羣的充分必要條件是，$\forall x,\ y\in H,\ xy^{-1}\in H$。
2. 秩爲p的羣（p是質數）必與 $\boldsymbol{Z}_p$ 同構。
3. 設 $H\subset K\subset G$，並且 H 與 K 都是有限羣G的子羣。試證 $[G:\ H]=[G:\ K][K:\ H]$。
4. (1)設 G 有兩種右陪集表示法，$G=\bigcup\limits_{i\in I}Hx_i=\bigcup\limits_{j\in J}Hy_j$，其中 I 與 J 是指標集（定理2.32.）。則$|I|=|J|$。(2)因此，甚至當 $|G|=\infty$ 時，我們也可以定義 $[G:\ H]$，因爲只要定義 $[G:\ H]=|I|$，其中 $G=\bigcup\limits_{i\in I}Hx_i$ 是一種 右陪集表示法。(3)試證 $[G:\ H]=[G:\ K][K:\ H]$，其中H與K是羣G的子羣，$H\subset K\subset G$。請注意，我們不假設G是有限羣。
5. 設H與K是羣G的子羣。(1)請舉例說明 HK 不一定是G的子羣。(2)若H與K都是有限羣，則 $|HK|=\dfrac{|H||K|}{|H\cap K|}$。(3) HK 是G的子羣的充分必要條件是$HK=KH$。(4)若$H\lhd G$，則 $HK=KH$。
6. 設H是羣G的子集合，$H\neq\phi$。H是G的子羣的充分必要條件是 $H^{-1}\subset H$ 與 $H\cdot H\subset H$。

7.設H, K是有限羣G的子羣。試證(1)$〔G: H\cap K〕\leqslant〔G: H〕\cdot〔G: K〕$，(2)若$〔G: H〕$與$〔G: K〕$互質，則$G=HK$。

8.若H是羣G的子羣，且$〔G: H〕=2$，則$H\lhd G$。

9.若$H\lhd K, K\lhd G$，試舉例說明$H\lhd G$不一定成立。

10.設H與K是羣G的子羣。如果$〔G: H〕<\infty, 〔G: K〕<\infty$，則$〔G: H\cap K〕<\infty$。請注意，我們不假設$G$是有限羣。

11.設H與K是有限羣G的子羣，則$|HxK|=|H|\cdot〔K: x^{-1}Hx\cap K〕$。

第五節　商羣與同構定理

2.38.

請讀者回憶一下，在第1.5.小節，我們怎樣定義$\boldsymbol{Z}_n$。事實上我們那時候取$G=\boldsymbol{Z}, H=n\boldsymbol{Z}=\{0,\pm n,\pm 2n,\cdots\}$，考慮左陪集$H, 1+H=\{1, 1\pm n, 1\pm 2n, 1\pm 3n,\cdots\}, 2+H, 3+H,\cdots,(n-1)+H$；那時候，我們把$H$記爲$\overline{0}$，$1+H$記爲$\overline{1},\cdots,(n-1)+H$記爲$\overline{n-1}$。然後我們再定義陪集的加法與乘法。

在一般情形，當G是任意的羣，H是其子羣，我們也想用類似的手法造出G對於H的商羣。我們把G對於H的商羣記爲G/H。

所謂商羣G/H，其元素是H的左陪集$xH, \forall x\in G, xH$有時也記爲$\overline{x}$。如果$x, y\in G$，那麼，$xH=yH\Longleftrightarrow\overline{x}=\overline{y}\Longleftrightarrow y^{-1}x\in H$。其次是定義兩個左陪集如何相乘，我們定義$\forall x, y\in G, xH\cdot yH=xyH$。

以上的乘法其實並不是定義得合理。例如，$H\cdot xH=xH$（依以上乘法的定義）；任取$h\in H$，則$H=hH$，故$H\cdot xH=hH\cdot xH=hx\cdot H$（仍然是依以上乘法的定義）。因此，如果以上的乘法定義得合理的話，則$xH=hxH\ \forall x\in G$。也就是說，$x^{-1}hx\in H\ \forall x\in G, \forall h\in H$，即$xHx^{-1}\subset H\ \forall x\in G$。所以要定義商羣$G/H$的先決條件必須是$H\lhd G$!

定義：令$H\lhd G$，我們定義商羣（quotient group或factor group）如下，記爲G/H，

G/H的元素，$xH=\overline{x}, \forall x\in G$。

G/H的運算，$xH\cdot yH=xyH$或$\overline{x}\cdot\overline{y}=\overline{xy}$。

在這定義之下，G/H形成羣，其單位元是$H=\overline{1}$，$xH=\overline{x}$的逆元是$x^{-1}H=\overline{x^{-1}}$。$xH$與$yH$代表商羣的同一個元素的充分必要條件是$y^{-1}x\in H$。

因爲$H\lhd G$，所以$xH=Hx$。因此商羣G/H的元素既可以看成是左陪集，也可以看成是右陪集。

當$G=\boldsymbol{Z}, H=n\boldsymbol{Z}=\{0, \pm n, \pm 2n,\cdots\}$，則$G/H\simeq\boldsymbol{Z}_n$。當$G=\boldsymbol{Z}_9, H=\{\overline{0},\overline{3},\overline{6}\}$，則$G/H\simeq\boldsymbol{Z}_3$。在一般的情形，當$G=\boldsymbol{Z}_{nm}, H=\{\overline{0}, \overline{m}, \overline{2m},\cdots,\overline{(n-1)m}\}$，則$G/H\simeq\boldsymbol{Z}_m$。

例題：若$〔G; G〕$是G的換位子羣（定義2.37.），請證明：(1)$G/〔G, G〕$是交換羣(2)若$H\lhd G$，且G/H是交換羣，則$H\supset〔G, G〕$。

證明：令$N=〔G, G〕$。

(1)$\forall x, y\in H$，我們想檢查$xN\cdot yN=yN\cdot xN$。但是$xN\cdot yN=xyN=(yx)\cdot(x^{-1}y^{-1}xy)N=yxN=yN\cdot xN$。

(2)若G/H是交換羣，則$\forall x, y\in G, xH\cdot yH=yH\cdot xH$。但是$xH\cdot yH=xyH, yH\cdot xH=yxH$。故$xyH=yxH$。得$\forall x, y\in G; x^{-1}y^{-1}xy\in H$。但是$N=〔G, G〕=\langle x^{-1}y^{-1}xy: x, y\in G\rangle$。得證$N\subset H$。

討論：我們知道：G是交換羣$\Longleftrightarrow〔G, G〕=\{1\}$（何故？）。以上例題說，$〔G, G〕$是測量羣$G$可不可交換的一種指標。我們可以利用它來求$S_n$的換位子羣。例如，考慮$S_4$的換位子羣。

因爲 $〔S_4, S_4〕 \lhd S_4$，並且 S_4 的正則子羣只有 $\{\varepsilon\}$, V, A_4, S_4，但是 $S_4/\{\varepsilon\}$ 與 S_4/V 都是不可交換羣（何故？），而 $S_4/A_4 \simeq \{\pm 1\}$。故知 $〔S_4, S_4〕 = A_4$。

2.39.

定義：設 $H \lhd G$。定義函數 p: $G \longrightarrow G/H$，其中 $p(x) = xH$, $\forall x \in G$。p 是羣的蓋同態，我們說，p 是羣 G 到其商羣 G/H 的自然同態（natural homomorphism）。

2.40.

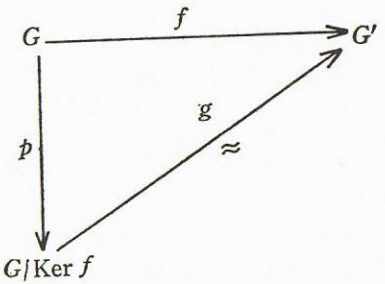
在以下三個小節（第2.41., 2.42., 2.43.小節）我們要討論三個同構定理。這三個同構定理是研究羣的結構的基本工具，它們是 E. Noether 發現的。B. L. van der Waerden 在 Noether 的誄辭說：「直和（direct sum），相交型分解式（intersection decomposition），商模與同構定理，像一組紅線貫穿她的後期的研究工作。」

2.41.

定理(第一同構定理)：

(1)若 $H \lhd G$，則 p: $G \longrightarrow G/H$ 是蓋同態，其中 p 是自然同態。從另一方面而言，如果 f: $G \longrightarrow G'$ 是羣的蓋同態，則必存在唯一的函數 g: $G/\mathrm{Ker}\ f \longrightarrow G'$，使得 $f = g \circ p$ 並且 g 是羣的同構。

(2)更一般的，如果 f: $G \longrightarrow G'$ 是羣的同態，則必存在唯一的函數 g: $G/\mathrm{Ker}\ f \longrightarrow G'$，使得 $f = g \circ p$ 並且 g 是羣的單同態（請參考下圖）。



討論：(1)這個定理的第(1)部分表示，羣G的蓋同態其實與G的商羣是一樣的，因爲 G' 與 $G/\mathrm{Ker}f$ 是同構的。從另一個角度來說，如果 $H \lhd G$，我們想決定羣 G/H 的結構。我們只需找一個蓋同態 f: $G \longrightarrow G'$ 使得 $H = \mathrm{Ker}f$，則 G/H 與 G' 是同構的。

(2)這個定理的第(2)部分表示，任意同態 f 必可寫成兩個同態的合成函數，第一個同態是蓋射（p只與 $\mathrm{Ker}f$ 有關），第二個同態是單射。

證明：(1)令 f: $G \longrightarrow G'$ 是羣的蓋同態，$K = \mathrm{Ker}f$。

g 的唯一性：如果 $f = g \circ p$，則 $\forall x \in G$, $g(x \cdot K) = g(p(x)) = g \circ p(x) = f(x)$。因此只要 g 存在，$g(xK)$ 就不得不定義爲 $f(x)$。

g 的存在性：定義 $g(xK) = f(x)$, $\forall x \in G$。這個定義是適當的（well-defined）：如果 $xK = yK$，則 $y^{-1}x \in K$。故 $g(xK) = f(x) = f(y \cdot y^{-1}x) = f(y) \cdot f(y^{-1}x) = f(y) = g(yK)$。

g 顯然是蓋同態。

g 是單射：如果 $1 = g(xK) = f(x)$，則 $x \in K$。故 $xK = K$。

第(2)部分的證明與第(1)部分類似。請讀者自己補充。

例如，考慮 f: $S_n \longrightarrow \{\pm 1\}$，$f$（偶置換）$=1$，$f$（奇置換）$=-1$。因爲$f$是蓋同態，且Ker$f=A_n$，故$S_n/A_n \simeq \{\pm 1\}$。

同樣的，考慮 f: $GL_3(\boldsymbol{R}) \longrightarrow \boldsymbol{R}^\times$, $f(A)=\det(A)$。因爲，Ker $f=SL_3(\boldsymbol{R})$，故 $GL_3(\boldsymbol{R})/SL_3(\boldsymbol{R}) \simeq \boldsymbol{R}^\times$。

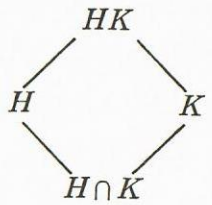
考慮 f: $\boldsymbol{Z}_{nm} \longrightarrow \boldsymbol{Z}_m$, $f(\overline{i})=\overline{i}$（變數的$\overline{i}$是模 nm 的，函數值的$\overline{i}$是模m的）。Ker $f=\{\overline{0}, \overline{m}, \overline{2m}, \cdots, \overline{(n-1)m}\}$。故 $\boldsymbol{Z}_{nm}/\{\overline{0}, \overline{m}, \overline{2m}, \cdots, \overline{(n-1)m}\} \simeq \boldsymbol{Z}_m$。

2.42.

定理(第二同構定理)：設H與K是羣G的子羣，且 $K \lhd G$，則 $(H \cap K) \lhd H$, HK 是G的子羣，且 $HK/K \simeq H/H \cap K$。

討論：(1)若H與K只是子羣，HK不一定是子羣。如 $G=S_3$, $H=\langle(12)\rangle$, $K=\langle(13)\rangle$，則$HK=\{\varepsilon, (1\ 2), (1\ 3), (1\ 3\ 2)\}$。$4=|HK| \nmid |G|=6$，故$HK$不是子羣。若$K \lhd G$，則有$HK=KH$（請參考以下的證明）。

(2)這個定理的主要部分是 $HK/K \simeq H/H \cap K$，可以看做左式 HK/K 如果「分子」、「分母」同時消去K的部分（約分！）就得到右式 $H/H \cap K$。下圖是這些子羣的相對關係圖：



證明：令 $N=H \cap K$, $x \in H$。$xNx^{-1} \subset xHx^{-1}=H$（因爲 $x \in H$），$xNx^{-1} \subset xKx^{-1} \subset K$（因爲$K \lhd G$）。故$xNx^{-1} \subset H \cap K = N$。

HK是子羣：(1)如果 $h_1, h_2 \in H, k_1, k_2 \in K$，則 $(h_1k_1)\cdot(h_2k_2) = h_1h_2(h_2^{-1}k_1h_2)\cdot k_2 = (h_1h_2)\cdot\{(h_2^{-1}k_1h_2)\cdot k_2\} \in HK$。

(2)如果 $h \in H$, $k \in K$，則 $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}\cdot(hk^{-1}h^{-1}) \in HK$。

定義函數f如下，

f: $H \longrightarrow HK/K$

$h \longrightarrow hK$

f顯然是蓋同態（何以是同態？）。請讀者自己檢驗 Kerf$=H \cap K$。由第一同構定理（定理2.41.），得 $H/H \cap K \simeq HK/K$。

在$\boldsymbol{Z}$之中，令 $n\boldsymbol{Z}=\{0, \pm n, \pm 2n, \cdots\}$。注意，$n\boldsymbol{Z}+m\boldsymbol{Z}=(n, m)\boldsymbol{Z}$, $n\boldsymbol{Z} \cap m\boldsymbol{Z}=[n, m]\boldsymbol{Z}$，其中 (n, m) 與 $[n, m]$ 分別是n與m的最大公因數與最小公倍數。由第二同構定理，$(n, m)\boldsymbol{Z}/n\boldsymbol{Z}=n\boldsymbol{Z}+m\boldsymbol{Z}/n\boldsymbol{Z} \simeq m\boldsymbol{Z}/n\boldsymbol{Z} \cap m\boldsymbol{Z}=m\boldsymbol{Z}/[n, m]\boldsymbol{Z}$。

例題：請注意 $A_n(n \geqslant 5)$是單羣（定義2.50.與定理2.55.）。試證，(1)S_n 的換位子羣是 $A_n(n \geqslant 2)$，(2)A_3 的換位子羣是$\{\varepsilon\}$，A_4 的換位子羣是 $V=\{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$，$A_n$ 的換位子羣是 $A_n(n \geqslant 5)$。

證明：根據例題2.38.的討論，不妨只考慮 $S_n(n \geqslant 5)$。令 $H=[S_n, S_n]$。因爲換位子都是偶置換，故$H \subset A_n$。但是$H \lhd S_n$，故有 $H \lhd A_n$。而 A_n 是單羣，可知 $H=A_n$ 或 $\{\varepsilon\}$。若 $H=\{\varepsilon\}$，根據例題2.38.，$S_n \simeq S_n/\{\varepsilon\}=S_n/H$ 是交換羣，矛盾。

(2)令N是 A_n 的換位子羣（$n \geqslant 5$）。

因爲 A_n 是單羣，且 $N \lhd A_n$。故 $N=\{\varepsilon\}$ 或 A_n。若 $N=\{\varepsilon\}$，則 $A/N \simeq A_n/\{\varepsilon\} \simeq A_n$ 是交換羣，矛盾。

因爲 A_3 是交換羣，其換位子都是 ε。

至於 A_4，它不是交換羣，所以換位子羣不是 $\{\varepsilon\}$。但是 A_4 的正則子羣只有 $\{\varepsilon\}$, V, A_4，且 A_4/V 是交換羣（何故？）。故 A_4 的換位子羣是V。

2.43.

定理(第三同構定理):

(1)若 $N\lhd G$，則G中包含N的子羣與 G/N 的子羣成一對一對應，其對應如下:

$$\{H: H\supset N, H\text{是子羣}\}\longleftrightarrow\{G/N \text{ 的子羣}\},$$

$$H\rightsquigarrow H/N$$

$$p^{-1}(H')\leftsquigarrow H'$$

其中 $p: G\longrightarrow G/N$ 是自然同態。在這對應，如果 $H\lhd G$，則 $H/N\lhd G/N$; 如果 $H'\lhd G'$，則 $p^{-1}(H')\lhd G$。

(2)若 $N\subset K\subset G$、且 $N\lhd G$, $K\lhd G$。則 $G/N/K/N\simeq G/K$。

證明: (1)關於子羣的一對一對應只需證明：若 $H\supset N$，則 $p^{-1}(H/N)=H$ 與 $p^{-1}(H')/N\simeq H'$ (何故？) 這些請讀者自己檢查。設 $H\supset N$ 且 $H\lhd G$; $\forall x\in G$，則 $(xN)\cdot H/N\cdot(xN)^{-1}=p(x)\cdot p(H)\cdot p(x^{-1})=p(xHx^{-1})=p(H)=H/N$，故 $H/N\lhd G/N$。

(2)定義函數 f 如下，

$$f: G/N\longrightarrow G/K$$

$$xN\longmapsto xK$$

f 顯然是羣的蓋同態，並且 Ker $f=\{xN: x\in K\}$。由第一同構定理（定理2.41.）可得 $G/N/K/N\simeq G/K$。

2.44.

本小節與下一小節將應用同構定理來討論循環羣與有限生成交換羣的結構。

定義: 羣G如果可以由一個元素 x 生成，則G叫做循環羣 (cyclic group)。

根據引理2.34.，當 $\mathrm{ord}(x)=\infty$ 時，$G=\langle x\rangle\simeq\boldsymbol{Z}$，這時候$G$叫做無限循環羣；當 $\mathrm{ord}(x)=n<\infty$ 時，$G=\langle x\rangle\simeq\boldsymbol{Z}_n$，這時候$G$叫做秩爲$n$的有限循環羣。

定理: (1)$\boldsymbol{Z}$的所有子羣是 $n\boldsymbol{Z}$，其中 $n=0, 1, 2,\cdots$。$\boldsymbol{Z}$ 的所有子羣都是循環羣。

(2)若 $k|n$，則 $\boldsymbol{Z}_n$ 恰有一個秩爲k的子羣，這些子羣是 $\boldsymbol{Z}_n$ 的所有子羣。$\boldsymbol{Z}_n$ 的所有子羣都是循環羣。

證明: (1)令H是$\boldsymbol{Z}$的子羣，且 $H\neq\{0\}$。令$n=\min\{r\in H: r$是正整數$\}$。顯然 $n\boldsymbol{Z}\subset H$。若 $r\in H$，令 $r=nq+s$，其中 $0\leq s<n$。則 $s=r-nq\in H$。故 $s=0$。

(2)因 $\boldsymbol{Z}\longrightarrow\boldsymbol{Z}_n$ 是蓋同態，由第二同構定理（定理2.42.）可知，$\boldsymbol{Z}_n$ 的所有子羣對應到$\boldsymbol{Z}$中包含 $n\boldsymbol{Z}$ 的子羣。利用(1)的結果，$\boldsymbol{Z}$ 的子羣是 $\{0\}$ 與 $k\boldsymbol{Z}$。但是 $k\boldsymbol{Z}\supset n\boldsymbol{Z}\Longleftrightarrow k|n$（何故？)由第三同構定理（定理2.43.），$\boldsymbol{Z}/n\boldsymbol{Z}/k\boldsymbol{Z}/n\boldsymbol{Z}\simeq\boldsymbol{Z}/k\boldsymbol{Z}$; 故$\frac{n}{k}\boldsymbol{Z}/n\boldsymbol{Z}$ 在 $\boldsymbol{Z}/n\boldsymbol{Z}$ 的指標是$\frac{n}{k}$，也就是，它的秩是k。

引理: $\boldsymbol{Z}$的生成元只有 1 與 -1。$\boldsymbol{Z}_n$ 的生成元是$\bar{i}$，其中 $1\leq i<n$ 且i與n互質。

證明: 若 $|r|\geqslant 2$，則 $[\boldsymbol{Z}: r\boldsymbol{Z}]=|r|\neq 1$，因此 $\boldsymbol{Z}\neq\langle r\rangle$。若$1\leq i<n$, 且$i$與$n$的最大公因數是$d$, 則 $\langle\bar{i}\rangle=i\boldsymbol{Z}+n\boldsymbol{Z}/n\boldsymbol{Z}\simeq i\boldsymbol{Z}/i\boldsymbol{Z}\cap n\boldsymbol{Z}\simeq i\boldsymbol{Z}/[i,n]\boldsymbol{Z}\simeq\boldsymbol{Z}/\frac{[i,n]}{i}\boldsymbol{Z}=\boldsymbol{Z}/\frac{n}{d}\boldsymbol{Z}$，恰有$\frac{n}{d}$個元素。所以 $\langle\bar{i}\rangle=\boldsymbol{Z}_n\Longleftrightarrow d=1$。

討論: 定義函數 φ, $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(n)$ 是從1到n的正整數內，與n互質的整數個數。因此 $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(p)=p-1$, 如果p是質數。φ叫做 Euler 函數。

由以上引理知，$\boldsymbol{Z}_n$ 恰有 $\varphi(n)$ 個生成元。事實上 $\boldsymbol{Z}_n^{\times}$ 的元素就是 $\boldsymbol{Z}_n$ 所有的生成元。

2.45.

定義: 若 G_1 與 G_2 是羣，我們定義其直積 (direct product)，記爲 $G_1\times G_2$。$G_1\times G_2$ 的元素是 (x_1, x_2), $\forall x_1\in G_1$ $\forall x_2\in G_2$, 其中 (x_1, x_2) 表示有序數偶 (也就是說, $(x_1, x_2)=(y_1, y_2)$ 的充要條件是 $x_1=y_1$ 與 $x_2=y_2$)。$G_1\times G_2$ 的運算是 $(x_1, x_2)\cdot(y_1, y_2)=(x_1y_1, x_2y_2)$。直積的定義可以推廣到任意 n 個羣 G_1, $G_2,\cdots, G_n$。如果每個 G_i 都是交換羣，我們就把直積叫做直和 (direct sum)，記爲 $G_1\oplus G_2\oplus\cdots\oplus G_n$。$G^n$ 表示用 n 個 G 做直積或直和所得到的羣。

引理: (1)若 n 與 m 互質，則 $\boldsymbol{Z}_{nm}\simeq\boldsymbol{Z}_n\oplus\boldsymbol{Z}_m$。

(2)$\boldsymbol{Z}_{p^{n+m}}$ 與 $\boldsymbol{Z}_{p^n}\oplus\boldsymbol{Z}_{p^m}$ 不會同構 (其中 $n, m\geqslant 1$)。

證明: (1)定義函數 f

$$f: \boldsymbol{Z}\longrightarrow\boldsymbol{Z}_n\oplus\boldsymbol{Z}_m$$
$$i\longmapsto(\overline{i}, \overline{i})$$

其中 $(\overline{i}, \overline{i})$ 的第一個 $\overline{i}$ 是模 n 的，第二個 $\overline{i}$ 是模 m 的。

f 是羣的同態。由中國餘數定理 (第1.10.小節)，可知 f 是蓋射。$\mathrm{Ker}f=[n, m]$ $\boldsymbol{Z}=nm\boldsymbol{Z}$。得 $\boldsymbol{Z}_{nm}\simeq\boldsymbol{Z}_n\oplus\boldsymbol{Z}_m$。

(2)設 $n\geqslant m$。$\boldsymbol{Z}_{p^n}\oplus\boldsymbol{Z}_{p^m}$ 至少有兩個秩爲 p^m 的循環子羣，即 $\langle(\overline{p^{n-m}}, \overline{0})\rangle$ 與 $\langle(\overline{0}, \overline{1})\rangle$。但是 $\boldsymbol{Z}_{p^{n+m}}$ 是循環羣，由定理 2.44.(2), $\boldsymbol{Z}_{p^{m+n}}$ 只有一個秩爲 p^m 的子羣。因此這兩個羣不可能同構。

例題: (1)若 n 與 m 互質，證明 $\varphi(nm)=\varphi(n)\cdot\varphi(m)$。

(2)若 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，其中 $p_1, p_2,\cdots, p_k$ 是相異質數，$\alpha_1,\cdots, \alpha_k$ 是正整數，則 $\varphi(n)=n\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$。

證明: (1)$\boldsymbol{Z}_n\oplus\boldsymbol{Z}_m$ 的生成元是 $(\overline{i}, \overline{j})$ 其中 i 與 n 互質且 j 與 m 互質，理由: 因爲 im 與 n 互質，取整數 r 使得 $imr\equiv 1 \pmod n$，則 $mr(\overline{i}, \overline{j})=(\overline{1}, \overline{0})$，同理 $(\overline{0}, \overline{1})\in\langle(\overline{i}, \overline{j})\rangle$。從另一方面來看 $\boldsymbol{Z}_{nm}\simeq\boldsymbol{Z}_n\oplus\boldsymbol{Z}_m$ (引理 2.45.)，計算兩邊生成元的個數，得 $\varphi(nm)=\varphi(n)\cdot\varphi(m)$。

(2)因爲 $\varphi(p^m)=p^m-p^{m-1}$ (與 p^m 不互質的是 $p, 2p, 3p,\cdots, p^{m-1}\cdot p$)，利用(1)的結果，可得(2)。

例題: 證明 $n=\sum_{d\mid n}\varphi(d)$

證明: $\forall\overline{i}\in\boldsymbol{Z}_n$，$\overline{i}$ 是 $\boldsymbol{Z}_n$ 某個秩爲 $\mathrm{ord}(\overline{i})$ 的子羣 (即 $\langle\overline{i}\rangle$) 的生成元。但是對於任意正整數 d 使得 $d\mid n$，$\boldsymbol{Z}_n$ 恰有一個秩爲 d 的子羣，這個子羣有 $\varphi(d)$ 個生成元。故得證。

例題: 請決定羣 $G=\boldsymbol{Z}_{175}\oplus\boldsymbol{Z}_{40}\oplus\boldsymbol{Z}_5$ 中秩爲 5^n 的元素的個數，$n=0, 1, 2, 3,\cdots$。

解: $G=\boldsymbol{Z}_{175}\oplus\boldsymbol{Z}_{40}\oplus\boldsymbol{Z}_5\simeq\boldsymbol{Z}_7\oplus\boldsymbol{Z}_{25}\oplus\boldsymbol{Z}_8\oplus\boldsymbol{Z}_5\oplus\boldsymbol{Z}_5\simeq\boldsymbol{Z}_8\oplus\boldsymbol{Z}_7\oplus\boldsymbol{Z}_{25}\oplus\boldsymbol{Z}_5\oplus\boldsymbol{Z}_5$，所求的元素數目爲 $25\cdot 5\cdot 5=625$。

交換羣 $G=\boldsymbol{Z}\oplus\boldsymbol{Z}_9\oplus\boldsymbol{Z}_8\oplus\boldsymbol{Z}_{25}$ 是有限生成的，也就是說，如果令 $S=\{(1,\overline{0}, \overline{0}, \overline{0}), (0, \overline{1}, \overline{0}, \overline{0}), (0, \overline{0}, \overline{1}, \overline{0}), (0, \overline{0}, \overline{0}, \overline{1})\}$，則 $G=\langle S\rangle$。一般的，如果交換羣 G 是有限生成 (例如，G 是有限羣)，則 G 必同構於類似 $\boldsymbol{Z}^2\oplus\boldsymbol{Z}_9\oplus\boldsymbol{Z}_3\oplus\boldsymbol{Z}_{343}\oplus\boldsymbol{Z}_5$ 這種羣。這就是所謂的交換羣基本定理，我們暫時不證明這個定理，只將其結果敍述如下:

交換羣基本定理 (定理6.12.): 若 G 是有限生成交換羣，則 $G\simeq\boldsymbol{Z}_{p_1^{\alpha_1}}\oplus\boldsymbol{Z}_{p_2^{\alpha_2}}\oplus\cdots\oplus\boldsymbol{Z}_{p_k^{\alpha_k}}\oplus\boldsymbol{Z}^m$，其中 k 與 m 是正整數或零，$p_1\ p_2,\cdots, p_k$ 是容許重複的質數，$\alpha_1,\cdots, \alpha_k$ 是正整數 (如果 $k>0$ 時)。

例題: 令 $V\{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}\subset S_4$。請證明 V 與 $\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2$ 同構。

證明: V 是有限交換羣，且 $|V|=4$。由交換羣基本定理，可知 $V\simeq\boldsymbol{Z}_4$ 或 $\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2$。但是 V 沒有秩爲 4 的元素。故 V 與

$Z_2 \oplus Z_2$ 同構。我們鼓勵讀者直接找一個V到 $Z_2 \oplus Z_2$ 的同構。

例題: 若p是質數，$G=(Z_p)^n$ 叫做基本交換羣 (elementary abelian group)。G的每個元素的秩，除了單位元之外，都是p。事實上G可以看做係數在 Z_p 的n維向量空間。

例題: 設n是任意正整數，$(Z_n)^\times$ 是循環羣的充分必要條件是 $n=2, 4, p^r, 2p^r$，其中 p 是奇質數，r是任意正整數（定理7.9.）。讀者願意自己證明 $(Z_{2^r})^\times \simeq Z_2 \times Z_{2^{r-2}} (r \geqslant 3)$ 嗎?

例題: 請問有幾種（不同構的）秩爲625的交換羣?

解: $625=5^4=5^3\cdot 5=5^2\cdot 5^2=5^2\cdot 5\cdot 5=5\cdot 5\cdot 5\cdot 5$，故有 5 種秩爲625的交換羣，即 Z_{625}, $Z_{125}\oplus Z_5$, $Z_{25}\oplus Z_{25}$, $Z_{25}\oplus Z_5\oplus Z_5$, $Z_5\oplus Z_5\oplus Z_5\oplus Z_5$。這5種交換羣都不同構（只要檢驗秩爲 625, 125, 25,…的元素的個數）。

例題: 請問有幾種（不同構的）秩爲225的交換羣?

解: $225=9\cdot 25=3^2\cdot 5^2$; 故有 4 種，即 Z_{225}, $Z_9\oplus Z_5\oplus Z_5$, $Z_3\oplus Z_3\oplus Z_{25}$, $Z_3\oplus Z_3\oplus Z_5\oplus Z_5$。

習題

1. 設 $V=\{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}\subset S_4$。請證明 $S_4/V\simeq S_3$。
2. 設 $H\lhd G$。如果H與 G/H 都是交換羣，G是否必是交換羣?
3. 設 $f: G\longrightarrow G'$ 是羣G到羣 G' 的同態，H是G的子羣。如果 G' 是交換羣，並且 $H\supset \mathrm{Ker} f$，則 $H\lhd G$。
4. 設G是有限羣，H與K是G的子羣，並且 $K\lhd G$。(1)若 $[G: K]$ 與 $|H|$ 互質，則 $H\subset K$; (2)若$|K|$ 與 $[G: H]$ 互質，則 $K\subset H$。
5. 設H是循環羣G的子羣，且$[G: H]=n$。試驗$G/H\simeq Z_m$。
6. 試證 Q/Z 的有限生成子羣都是有限循環羣。Q/Z 的任意子羣是不是都是循環羣?
7. 設G是羣。如果不爲G的任意子羣都是循環羣，G是不是循環羣?（提示: 設 p 是任意質數，$G=\{z\in C: z^{p^n}=1, n\in N\}$，則 $(G; \times; 1)$ 是羣。）
8. 設H是 $(Q; +; 0)$ 的子羣，且 $H=\langle \frac{192}{1617}, \frac{7659}{1232}, \frac{115}{308}\rangle$。請找個有理數 r 使得 $H=\langle r\rangle$。
9. 設 n 是正整數，G是 Z^n 的子羣，且$G\neq\{0\}$。則$G\simeq Z^k$，其中 k 是某個正整數，$k\leq n$。（提示: 令 $m=\min\{|r|: \text{存在 } r_1,\cdots,r_{n-1} \text{ 使得} (r_1,\cdots, r_{n-1}, r)\in G\}$。設$a=(m_1,\cdots, m_{n-1}, m)\in G$, $H=\{(r_1,\cdots,r_n)\in G: r_n=0\}$，則 $G\simeq H\oplus\langle a\rangle$。）
10. $(C\setminus\{0\}; \times; 1)$是不是有限生成羣? 試證$\left\{1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{n}, \cdots\right\}$ 在 $(Q; +; 0)$ 之內生成的子羣不是有限生成羣。

第六節 生成集與關係

2.46.

例題: 設 $G=\langle x, y\rangle$，且 $x^3=y^2=1$, $yxy^{-1}=x^{-1}$。則 $G=\{1, x, x^2, y, xy, x^2y\}$，因爲 $yx^i=yx^iy^{-1}\cdot y=(yxy^{-1})^iy=(x^{-1})^iy=x^{-i}y$。但是$G$是否眞的有 6 個元素嗎? 這就要看 x 與 y 是否還有其他關係。顯然 $(xy)^2=1$，因爲 $(xy)^2=xy\cdot xy=x\cdot yxy^{-1}=x\cdot x^{-1}=1$; 所以 $(xy)^2=1$ 這個關係可以由 $x^3=y^2=yxy^{-1}x=1$ 導出來。如果 x, y 的任何關係式都可以由 $x^3=y^2=yxy^{-1}x=1$ 導出，我們就說G是由 x, y 生成，而其關係爲 $x^3=y^2=yxy^{-1}x=1$，記爲 $G=\langle x, y: x^3=y^2=yxy^{-1}x=1\rangle$。

第九節 Sylow 定理

2.71.

任給有限羣G，G有什麼樣的子羣呢？

Lagrange 定理（定理2.31.）說，如果H是G的子羣，則$|H|\big||G|$。反之，若正整數m整除$|G|$，是不是可找到子羣H使得$|H|=m$？

考慮$G=A_5$。A_5是不是有一個秩爲30的子羣H呢？如果這種子羣H的確存在，則$H\lhd G$（定理2.66.或本章第五節習題8）。但是A_5是單羣。矛盾。可見A_5不可能有秩爲30的子羣。

Sylow 定理保證在某些情況子羣的存在性。它還告訴我們這些子羣的數目。以下是這個定理的敍述。

定理（Sylow 定理）：設有限羣G的秩是n，p是質數，且$p^r||n$（也就是，$p^r|n$, $p^{r+1}\nmid n$）。

(1)必存在一個秩爲p^r的子羣。這種子羣叫做p-Sylow子羣。

(2)p-Sylow子羣的個數是$\equiv 1(\mathrm{mod}\ p)$，並且可以整除$|G|=n$。同時所有的$p$-Sylow子羣都互爲共軛。

(3)$\forall 1\leq i\leq r$，必可找到一個秩爲p^i的子羣。任意的秩爲p^i的子羣必包含在某一個p-Sylow子羣。

Sylow 定理是十九世紀數學家（如, O. Hölder, F.N. Cole）研究可解羣與單羣的主要工具。當然，以今日的眼光來看，Sylow 定理不過是近世代數一個基本定理，只憑 Sylow 定理很難再得到特別好的結果，有限羣論的研究已經大量的運用羣表現理論的結果。

事實上 E. Galois 早已預見 Sylow 定理的存在，他說，

如果質數 p 可以整除置換羣 G 的秩，則G必有秩爲 p 的子羣。Galois 沒有把這個定理的證明寫出來，1844年 Cauchy 把它的證明發表，他甚至證明了 Sylow 定理第(1)部分的兩個特殊情形：(i) 若 $p\mid|G|$，則G有一個秩爲 p 的子羣，(ii)若 $p'\|n!$，則 S_n 有一個秩爲 p' 的子羣。完整的 Sylow 定理是挪威數學家 L. Sylow (1832～1918) 在1872年證明的。

和 Sylow 定理類似的是以下的定理。

定理 (P. Hall)： 有限羣G是可解羣的充分必要條件是，對於 $|G|$ 的任意因數分解，$|G|=mn$ (m與n互質)，恒可找到秩爲m的子羣。

我們不準備證明 P. Hall 的定理，Sylow 定理的證明則延到第2.82.小節。我們想先討論 Sylow 定理的應用（第2.73～2.81.小節）。

2.72.

若H是G的子羣，$x\in G$，那麼 xHx^{-1} 叫做H的共軛子羣（引理2.36.的討論）。H 有多少共軛子羣呢？和計算共軛元的數目一樣（第2.53.小節），我們先定義正則化子。

定義：設H是羣G的子羣，定義 $N_G(H)=\{x\in G: xHx^{-1}=H\}$。$N_G(H)$ 是G的子羣，它叫做H在G之內的正則化子（normalizer of H in G）。

引理：設H是羣G的子羣。

(1)$H\lhd N_G(H)$

(2)如果 K 是 G 的子羣，$H\subset K\subset G$，且 $H\lhd K$，則 $K\subset N_G(H)$。因此，$H\lhd G$ 的充分必要條件是 $N_G(H)=G$。

(3)H恰有 $〔G: N_G(H)〕$ 個共軛子羣。

證明：(1) 與 (2) 完全根據正則化子的定義，(3)的證明與引理2.53.非常相似，因此留給讀者自己處理。

2.73.

這一小節的目的是證明秩爲45的羣是交換羣。

(1)3-Sylow 子羣與 5-Sylow 子羣是正則子羣，令其分別是H與K。

3-Sylow 子羣的數目是 $1+3m$，且 $1+3m\mid 5$。故 $1+3m=1$。因爲它只有一個共軛子羣，所以一定是正則子羣。

(2)$H\cap K=\{1\}$

因爲 $|H\cap K|$ 可以整除 $|H|$，也可以整除 $|K|$，但是$|H|$與 $|K|$ 互質。

(3)$\forall x\in H,\ \forall y\in K,\ xy=yx$。

考慮 $xyx^{-1}y^{-1}$。注意 $(xyx^{-1})\cdot y^{-1}\in K$ 並且 $x(yx^{-1}y^{-1})\in H$。故 $xyx^{-1}\ y^{-1}\in H\cap K=\{1\}$。

(4)$G=HK$

$H/H\cap K=HK/K$，故 $〔HK: K〕=〔H: H\cap K〕=9$。得證 $|HK|=45=|G|$。（讀者也可利用本章第四節習題5(2)）。

(5)G的元素可寫成 xy 與 $x'y'$，$x,\ x'\in H,\ y,\ y'\in K$。因爲$H$與$K$都是可換羣（定理2.69.），故 $(xy)(x'y')=x(yx')y'=x(x'y)y'=(xx')(yy')=\cdots=(x'y')(xy)$。

2.74.

現在我們要證明秩爲 6 的羣必與 $\boldsymbol{Z}_6$ 或 S_3 同構。

由 Sylow 定理，存在一個秩爲 3 的子羣，因其指標爲 2，故爲正則子羣，顯然這是一個循環羣，令此子羣爲 $\langle x\rangle$。$\mathrm{ord}(x)=3$。

同理可找到 y，使得 $\mathrm{ord}(y)=2$。

因爲 $y\langle x\rangle y^{-1}=\langle x\rangle$。故 $yxy^{-1}=x$ 或 x^{-1}。

注意，$\langle x\rangle\cap\langle y\rangle=\{1\}$。故 $G=\langle x\rangle\cdot\langle y\rangle=\{1,\ x,\ x^2,\ y,\ xy,$

$x^2y\}$。

若 $yxy^{-1}=x$，則G同構於可換羣 Z_6。

若 $yxy^{-1}=x^{-1}$，則G同構於二面體羣$D_3\simeq S_3$(例題2.46.)。

2.75.

我們要對秩爲 8 的羣加以分類。

設G是秩爲 8 的羣。

若G是交換羣，則G同構於 Z_8, $Z_4\oplus Z_2$ 或 $Z_2\oplus Z_2\oplus Z_2$。

現在考慮G是不可交換羣的情形。G沒有秩爲 8 的元素，否則它就變成循環羣。G必有秩爲 4 的元素，否則G是交換羣（本章第一節習題 5 ）。令 $x\in G$, $\mathrm{ord}(x)=4$。取 $y\in G\setminus\langle x\rangle$。$G=\langle x\rangle\cup y\langle x\rangle$。因爲 $G/\langle x\rangle$ 的秩爲 2，故 $y^2\in\langle x\rangle$。

如果 $y^2=x$ 或 x^{-1}，則因 $\mathrm{ord}(x)=4$，故 $\mathrm{ord}(y)=8$，矛盾。因此 $y^2=1$ 或 x^2。

因 $[G:\langle x\rangle]=2$，故 $yxy^{-1}=x$ 或 x^{-1}。如果 $yxy^{-1}=x$，則G是交換羣。故只有 $yxy^{-1}=x^{-1}$。

結論是G只有兩種可能，

(1)$G=\langle x, y\rangle$, $\mathrm{ord}(x)=4$, $\mathrm{ord}(y)=2$, $yxy^{-1}=x^{-1}$。

(2)$G=\langle x, y\rangle$, $\mathrm{ord}(x)=4$, $y^2=x^2$, $yxy^{-1}=x^{-1}$。

第 (1) 種情形，$G\simeq D_4$。第二種情形的 G 叫做四元數羣（quaternion group），並且這兩個羣不會同構，因爲前者只有兩個秩爲 4 的元素，後者卻有六個秩爲 4 的元素。有關四元數請參考4.32.小節。

討論：請證明四元數羣和以下的羣同構，

$$G=\{\pm 1, \pm i, \pm j, \pm k\},\ i^2=j^2=k^2=-1,\ ij=-ji=k,\ jk=-kj=i,\ ki=-ik=j。$$

2.76.

以下是秩小於16的羣的分類。請讀者自己檢驗你能不能證明每個情形，

秩	羣
1	$\{1\}$
2	Z_2
3	Z_3
4	Z_4, $Z_2\oplus Z_2$
5	Z_5
6	Z_6, S_3
7	Z_7
8	Z_8, $Z_4\oplus Z_2$, $Z_2\oplus Z_2\oplus Z_2$, D_4, 四元數羣。
9	Z_9, $Z_3\oplus Z_3$
10	Z_{10}, D_5
11	Z_{11}
12	Z_{12}, $Z_2\oplus Z_2\oplus Z_3$, D_6, $\langle x, y, z: x^3=y^2=z^2=1, yz=zy, xyx^{-1}=z, xzx^{-1}=yz\rangle$, $\langle x, y: x^3=y^4=1, yxy^{-1}=x^{-1}\rangle$
13	Z_{13}
14	Z_{14}, D_7
15	Z_{15}

說明：(1)$|G|=10$的情形。與第2.73.小節的討論類似，$G=\{1, x,\cdots, x^5, y, xy,\cdots, x^5y\}$。$yxy^{-1}=x$, x^{-1}, x^2 或 x^3。但是 $yxy^{-1}=x^2$ 或 x^3 不可能，因爲，若 $yxy^{-1}=x^2$，則 $x=y^2xy^{-2}=yx^2y^{-1}=(x^2)^2=x^4$。

(2)$|G|=12$ 的情形要用到以下第2.77.小節的結果。再分別就 2-Sylow 子羣同構於 Z_4 或 $Z_2\oplus Z_2$ 加以討論。

2.77.

設G是有限羣，p, q 是相異質數。這一小節的目的是證明

以下性質，

(1)若 $|G|=pq$，則G的某一 Sylow 子羣是正則子羣。

(2)若 $|G|=p^2q$，則G的某一 Sylow 子羣是正則子羣。

現在證明如下:

(1)令 $p<q$。考慮 q-Sylow 子羣。其數目是 $1+qm$，且 $1+qm$ 可以整除 pq。故 $1+qm|p$。但是 $q>p$。故 $1+qm=1$。但是 q-Sylow 子羣的共軛子羣也是 q-Sylow 子羣，現在只有1個 q-Sylow 子羣。所以 q-Sylow 子羣是正則子羣。

(2)如果只有一個 p-Sylow 子羣或只有一個 q-Sylow 子羣，本命題得證。因此，不妨假設 $p<q$（何故？），並且 q-Sylow 子羣的數目 $1+qm$。因 $1+qm|p^2$，得 $p^2=1+qm$。$q|(p-1)(p+1)$，故 $q=p+1$。但 p, q 是質數且 $q=p+1$，故 $p=2, q=3, |G|=12$。現在 3-Sylow 子羣有4個，每個 3-Sylow 子羣是秩爲3的循環羣，因此總共有 $1+4\cdot2=9$ 個元素。至少還有一個秩爲4的 2-Sylow 子羣，剩下的 $12-9$ 個元素全在這個 2-Sylow 子羣。因此再沒有其他的 2-Sylow 子羣。

2.78.

設G是秩爲 p^3q 的羣，其中 p, q 是相異質數。我們想要證明，如果G的 Sylow 子羣都不是正則子羣，則 $G\simeq S_4$。注意 $|S_4|=2^3\cdot3$。

(1)若 $p>q$，則 p-Sylow 子羣是正則子羣。因此，$p<q$。

(2)若 q-Sylow 子羣有 p^3 個，則 p-Sylow 子羣只有一個。因爲q-Sylow子羣是秩爲q的循環羣，所以 p^3 個q-Sylow 子羣共有 $1+p^3(q-1)=1+p^3q-p^3$ 個元素。$|G|=p^3q$。因此只剩下 p^3-1 個元素。可見只有一個 p-Sylow 子羣。此與已知假設矛盾。

(3)$p=2$，且 $q=3$。

因爲 q-Sylow 子羣有 $1+qm$ 個，故 $1+qm=p^2$。得 $q=p+1$。故 $p=2, q=3$，並且恰有4個 3-Sylow 子羣。

(4)令H是某個 3-Sylow 子羣的正規化子，由 Sylow 定理與引理 2.72.(3)，可知 $[G: H]=4$。利用H作置換表現，由定理2.65.，令K是此置換表現的核，則K是正則子羣，$K\subset H$，$[G: K]|4!$。因爲 $|H|=6$，故 $|K|=1, 2, 3,$ 或 6。如果$|K|=1$，則 $G\simeq S_4$。我們要把其他情形除掉。

(5)如果 $K\lhd G$，$|K|=3$。則K是正則的 3-Sylow 子羣，矛盾。

(6)如果 $K\lhd G$，$|K|=2$。則 $|G/K|=12$。因此 G/K 的某一 Sylow 子羣是正則的(第2.77.小節)。若 $P\supset K$，$P/K\lhd G/K$ 且 $|P/K|=4$，則 $|P|=8$，且 $P\lhd G$，故P是正則的 2-Sylow 子羣。若 $Q\supset K$，$Q/K\lhd G/K$ 且 $|Q/K|=3$，則 $Q\lhd G$ 且 $|Q|=6$。但是秩爲6的羣必與 $\boldsymbol{Z}_6$ 或 S_3 同構（第2.74.小節）。現在Q的 2-Sylow 子羣K是正則的，故 $Q\simeq\boldsymbol{Z}_6$ 是循環羣。令N是Q的 3-Sylow 子羣，我們要證明 $N\lhd G$，故G的 3-Sylow 子羣是正則的，又一個矛盾。$\forall x\in G$, $xNx^{-1}\subset xQx^{-1}=Q$。但是 xNx^{-1} 與N是循環羣Q之內秩爲3的子羣，故 $xNx^{-1}=N$。

(7)若 $|K|=6$，則$K=H$。故$H\lhd G$。已知H是某一 3-Sylow 子羣P的正則化子，故 $P\lhd H$。$\forall x\in G$, $xPx^{-1}\subset xHx^{-1}=H$，故 xPx^{-1} 也是H的 3-Sylow 子羣。但是 $P\lhd H$，故 $xPx^{-1}=P$。得證 $P\lhd G$，又一矛盾。

2.79.

設G是秩爲 p^2q^2 的羣，其中 p, q 是相異質數。現在我們要證明G的某一個 Sylow 子羣必是正則子羣。

令 $p<q$。假設G的所有 Sylow 子羣都不是正則子羣。與

第 2.78. 小節之(3)一樣，$p=2$, $q=3$ 且 3-Sylow 子羣共有 4 個。我們將證明 2-Sylow 子羣共有 3 個。

假設 2-Sylow 子羣共有 3 個，與第2.78.小節之(4)一樣，找出 $K\lhd G, |K|=6$, $K\subset H$，其中H是某個 2-Sylow 子羣的正則化子（因此，與第 2.78. 小節之(7)一樣，H 不是 G 的正則子羣）。$|G/K|=6$，且 $|H/K|=2$, H/K 不是 G/K 的正則子羣（因爲H不是G的正則子羣），由第 2.74. 小節，$G/K\simeq S_3$。令 $N\supset K$, $|N/K|=3$，則 $N/K\lhd G/K$。故 $N\lhd G$。令P是N的 3-Sylow 子羣，則 $P\lhd N$ 因爲 $[N: P]=2$。P是G的3-Sylow 子羣。$\forall x\in G$, $xPx^{-1}\subset xNx^{-1}=N$，而$P$是$N$的唯一 3-Sylow 子羣，故 $xPx^{-1}=P$。得證 $P\lhd G$，矛盾。

現在目標是證明G共有 3 個 2-Sylow 子羣。

第一步驟：令Q是 3-Sylow 子羣。因爲 $[G: Q]=4$ 且 $|Q|=9$，故存在 K, $K\subset Q$, $K\lhd G$, $|K|=3$（何故？）

第二步驟：存在 N, $N\lhd G$, $N\supset K$, $[G: N]=3$。

因爲 $|G/K|=12$。由第2.77.小節，G/K 的 2-Sylow 子羣或 3-Sylow 子羣必定是正則的。若其 3-Sylow 子羣是正則的，則存在子羣 H, $H\supset K$, $|H/K|=3$，且 $H/K\lhd G/K$。故 $H\lhd G$並且H是G的 3-Sylow 子羣，矛盾。

第三步驟：G的 2-Sylow 子羣必包含於N。

令R是N的 2-Sylow 子羣，則 $|R|=4$。若 R' 是G的任意 2-Sylow 子羣，由 Sylow 定理，必有 $x\in G$ 使得 $R'=xRx^{-1}$。故 $R'=x\ Rx^{-1}\subset xNx^{-1}=N$。

第四步驟：N頂多有 3 個 2-Sylow 子羣，因爲 $|N|=12$。因此G只有 3 個 2-Sylow 子羣。

2.80.

在這一小節我們要證明，若G是秩爲60的單羣，則$G\simeq A_5$。

注意 $|G|=60=2^2\cdot 3\cdot 5$。因爲G是單羣，故 Sylow 子羣都不是正規子羣。2-Sylow 子羣的個數是 3, 5, 或 15, 3-Sylow 子羣的個數是 4 或10。5-Sylow 子羣的個數是 6 。我們要找到一個子羣H，使得 $[G: H]=5$。假設H已經找到，利用置換表現，$\Phi: G\longrightarrow S_5$ 是單同態（因爲G是單羣），因此$[S_5: Im(\Phi)]=2$。所以$Im(\Phi)=A_5$，否則 $(Im(\Phi)\cap A_5)\lhd A_5$，矛盾（或直接引用例題2.66.）。所以，$\Phi: G\longrightarrow A_5$ 是同構。

現在的目的是證明 2-Sylow 子羣共有 5 個。我們要把其他情形一一除掉。

(1)如果 2-Sylow 子羣有 3 個，利用置換表現，$G\longrightarrow S_3$ 是單同態，所以 $60=|G|\leq|S_3|=6$，矛盾。

(2)如果 3-Sylow 子羣有 4 個，也是不可能的。

(3)如果 2-Sylow 子羣有15個，並且這些子羣與 $\boldsymbol{Z}_4$ 同構。

計算各 Sylow 子羣元素數目（2-Sylow 子羣只計算生成元的數目），得 $1+15\cdot 2+10\cdot 2+6\cdot 4=75$，也是矛盾。

(4)最後一個情形，2-Sylow 子羣有15個，3-Sylow 子羣有10個，5-Sylow 子羣有 6 個，並且 2-Sylow 子羣與 $\boldsymbol{Z}_2\oplus\boldsymbol{Z}_2$ 同構。

令P是任意的 2-Sylow 子羣，$x\in P$, $x\neq 1$。考慮 $C_G(x)$。因爲P是交換羣，故 $P\subset C_G(x)$。我們要證明 $P\neq C_G(x)$。否則，P將是包含 x 的唯一 2-Sylow 子羣（若Q是 2-Sylow 子羣，$x\in Q\Rightarrow Q\subset C_G(x)=P$，故 $Q=P$）；因此，任何兩個相異的 2-Sylow 子羣的交集只有一個元素。利用這個結果，計算 Sylow 子羣的元素數目，又得一矛盾。

所以 $P\subsetneq C_G(x)\subsetneq G$（因爲 $Z(G)=\{1\}$），可知 $|C_G(x)|=12$或20。若 $[G: C_G(x)]=3$，則 $G\longrightarrow S_3$ 是單同態，矛盾。若 $[G: C_G(x)]=5$，則 $G\simeq A_5$，但是 A_5 只有 5 個 2-Sylow 子羣，即 $\langle(1\ 2)(3\ 4),\ (1\ 3)(2\ 4)\rangle$, $\langle(1\ 2)(3\ 5),\ (1\ 3)(2$

5)⟩,…，但是我們假設G有15個 2-Sylow 子羣，矛盾。

2.81.

例題：秩爲100以內的單羣，除了 $\boldsymbol{Z}_p$（p是質數）之外，只有 A_5。

證明：令G是單羣，$|G|\leqslant 100$。

根據第 2.77.～2.80. 小節與定理2.68.，我們只需考慮 $|G|=pqr$（p, q, r 是相異質數）或 $|G|=48$, 72, 80, 84, 90, 96 的情形。

(1)$|G|=pqr$, $p<q<r$。

則 r-Sylow 子羣是正則子羣。

(2)$|G|=90$

若 5-Sylow 子羣有 6 個，3-Sylow 子羣有10個。和第 2.80. 小節之(4)一樣，任取 3-Sylow 子羣P的元素x，$x\neq 1$，則 $P\subsetneq C_G(x)$。則$|C_G(x)|=18$, 45或90。若$〔G: C_G(x)〕=5$ 且G是單羣，則 $G\longrightarrow S_5$ 是單同態，矛盾。在 $〔G: C_G(x)〕=2$ 或 1 時，G顯然有正則子羣H，$H\neq\{1\}$。

2.82.

現在回到 Sylow 定理（定理2.71.）的證明。

引理 1：設 P 是羣 G 的子羣，$|G|=p^r\cdot m$（p 是質數，$p\nmid m$），$|P|=p^r$, $N_G(P)$ 是P的正則化子。如果H是 $N_G(P)$ 的子羣並且 $|H|=p^s$，則 $H\subset P$。

證明：在 $N_G(P)$ 之內考慮，$P\lhd N_G(P)$。故 $HP/P\simeq H/H\cap P$。可知 $|H/H\cap P|=p^h$。故 $|HP|=p^{r+h}$。因 HP 是 $N_G(P)$ 的子羣，HP 也是G的子羣。所以 $p^{r+h}\mid|G|=p^rm$。故 $h=0$，也就是 $H\cap P=H$。

引理 2：設G是有限交換羣，p是質數。如果 $p\mid|G|$，則 G必有秩爲 p 的元素。

證明：這個引理是交換羣基本定理（第2.45.小節或定理6.12.）的簡單推論。不過我們將給出一個直接的證明。

根據 $|G|$ 作歸納法，任取 $x\in G$, $x\neq 1$。在循環羣 $\langle x\rangle$ 取一個元素 y 使得 $\mathrm{ord}(y)$ 是質數。若 $\mathrm{ord}(y)=p$，y 就是所求元素。否則考慮 $G/\langle y\rangle$。由歸納法假設，必有 $z\in G$，z 在 $G/\langle y\rangle$ 的秩是 p。因此 $z^p\in\langle y\rangle$。若 $z^p=1$，則 z 是所求的元素；若 $z^p=y^i$，其中 $1\leqslant i\leqslant q-1$, $q=\mathrm{ord}(y)$，則 $\mathrm{ord}(z)=pq$，在循環羣 $\langle z\rangle\simeq\boldsymbol{Z}_{pq}$ 必可找到秩爲 p 的元素。

Sylow 定理（定理2.71.）的證明：

(1)根據 $|G|$ 作數學歸納法。

考慮共軛類恒等式（定理2.67.），

$$|G|=|Z(G)|+\sum_{i=1}^{r}〔G: C_G(\tau_i)〕,\ \text{其中}〔G: C_G(\tau_i)〕\neq 1。$$

若 $p\nmid Z(G)$，則必有某個 i 使得 $p\nmid〔G: C_G(\tau_i)〕$。因此 $p^r\mid C_G(\tau_i)$。但是$|C_G(\tau_i)|<|G|$。由歸納法假設，$C_G(\tau_i)$ 必有秩爲 p^r 的子羣。

若 $p\mid Z(G)$，由本小節引理 2，令 $x\in Z(G)$, $\mathrm{ord}(x)=p$。因爲 $x\in Z(G)$, $\langle x\rangle\lhd G$。考慮 $G/\langle x\rangle$。由歸納法假設，$G/\langle x\rangle$ 必有秩爲 p^{r-1} 的子羣；令H是G的子羣，$H\supset\langle x\rangle$ 且 $|H/\langle x\rangle|=p^{r-1}$。則 $|H|=p^r$。

(2)令P是 p-Sylow 子羣，X是所有的 p-Sylow 子羣的集合，Y是與P共軛的子羣所形成的集合。我們將證明 $|Y|\equiv 1\pmod p$，且 $Y=X$。

令 Φ_1: $P\times Y\longrightarrow Y$ 是P在Y上的作用，其中 $\Phi_1(x, Q)=xQx^{-1}$ $\forall x\in P$。顯然，$\{P\}$ 形成一個軌道。如果O是一個不含P的軌道，則 $|O|\neq 1$：因爲，取 $P_1\in O$，如果 $\forall x\in P$, $xP_1x^{-1}=P_1$，則 $P\subset N_G(P_1)$，利用本小節引理 1，得 $P\subset P_1$，矛盾。因爲 $|O|\neq 1$ 且 $|O|\mid|P|$，故 $|O|\equiv 0\pmod p$。可知

$|Y|\equiv 1 \pmod{p}$。

如果 P_2 是 p-Sylow 子羣且 P_2 和 P 不共軛，我們將導出一個矛盾現象。令 Φ_2: $P_2\times Y\longrightarrow Y$ 是 P_2 在 Y 的作用，其中 $\forall x\in P_2$, $\forall Q\in X$, $\Phi_2(x, Q)=xQx^{-1}$。$P_2\notin Y$，因此 P_2 不在這個羣作用的任何軌道。和上一段的討論方法一樣，若 O 是任意軌道，則 $|O|\equiv 0 \pmod{p}$。因此 $|Y|\equiv 0 \pmod{p}$。這和我們已證出的 $|Y|\equiv 1 \pmod{p}$ 違反。

因爲所有的 p-Sylow 子羣都互爲共軛，因此 p-Sylow 子羣的個數是 $[G: N_G(P)]$（引理2.72.(3)）。

⑶我們先證明秩爲 p^i 的子羣 H 必包含在某一 p-Sylow 子羣。令 Φ_3: $H\times X\longrightarrow X$ 是 H 在 X 上的作用，X 是所有 p-Sylow 子羣的集合，$\forall x\in H$, $\forall Q\in X$, $\Phi_3(x, Q)=xQx^{-1}$。如果 O 是這種羣作用的軌道並且 $|O|\neq 1$，則 $|O|\equiv 0 \pmod{p}$（因爲 $|O|\,\big|\,|H|$）。但是 $|X|\equiv 1 \pmod{p}$，所以必有一個只有一個元素 P 的軌道。因此 $xPx^{-1}=P$ $\forall x\in H$。可得 $H\subset N_G(P)$。利用本小節引理 1，$H\subset P$。

令 P 是 p-Sylow 子羣。因 $Z(P)\neq\{1\}$，利用引理 3，取出 $x\in Z(P)$ 使得 $\mathrm{ord}(x)=p$。顯然 $\langle x\rangle\lhd P$。考慮 $P/\langle x\rangle$。由歸納法假設，$P/\langle x\rangle$ 必有秩爲 p^{i-1} 的子羣。因此 P 必有秩爲 p^i 的子羣。

2.83.

例題: 試討論 S_4 的 Sylow 子羣。

解: $|S_4|=24=3\cdot 2^3$。

3-Sylow 子羣是由秩爲 3 的元素生成。仿照本章第2.5節例題21的方法，S_4 有 $\binom{4}{3}\cdot 2=8$ 個秩爲 3 的元素。但是一個秩爲 3 的羣恰有 2 個生成元。總共有 4 個 3-Sylow 子羣，即 $\langle(1\ 2\ 3)\rangle$, $\langle(1\ 2\ 4)\rangle$, $\langle(1\ 3\ 4)\rangle$, $\langle(2\ 3\ 4)\rangle$。

2-Sylow 子羣的尋找可先由四元羣着手。$V=\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$。$(1\ 2)(3\ 4)$ 的中核化子包含 V 並且是 8 個元素的子羣，即 $\langle(1\ 4\ 2\ 3), (1\ 3)(2\ 4)\rangle$（見定理 2.54. 的證明），這就是一個 2-Sylow 子羣。

討論: 以上解法並不好，它藉助我們過去的經驗，並且似乎不能推廣到其他情形。其實只要把答案改寫一下，變成: $\langle(1\ 2), (3\ 4), (1\ 3\ 2\ 4)\rangle$ 就不難看出一般情形。注意 $(1\ 3\ 2\ 4)$ 是在子羣 $\langle(1\ 2)\rangle\times\langle(3\ 4)\rangle$ 的正則化子之內。

例題: 請找一個 S_9 的 3-Sylow 子羣。

解: $|S_9|=3^4\cdot m$, $3\nmid m$。

考慮 $H=\langle(1\ 2\ 3)\rangle\times\langle(4\ 5\ 6)\rangle\times\langle(7\ 8\ 9)\rangle$。$|H|=3^3$。但是 H 一定包含在某一個 3-Sylow 子羣 P 之內。$[P: H]=3$。故只要找 $\sigma\in N_{S_9}(H)$, $\sigma\notin H$, $\mathrm{ord}(\sigma)=3^4$ 即可得到 $P=\langle H, \sigma\rangle$。令 $\sigma=(1\ 4\ 7\ 2\ 5\ 8\ 3\ 6\ 9)$。因爲 H 的元素的秩頂多是 3，而 $\mathrm{ord}(\sigma)=9$，故 $\sigma\notin H$。

討論: 你現在知道如何找 S_{p^k} 的 p-Sylow 子羣嗎？只要把 $\{1, 2, 3, \cdots, p^k\}$ 分成 p 類：$\{1, 2, \cdots, p^{k-1}\}$, $\{p^{k-1}+1, \cdots, 2p^{k-1}\}$, $\cdots$, $\{(p-1)p^{k-1}+1, (p-1)p^{k-1}+2, \cdots, p^k\}$。各造其 p-Sylow 子羣，得 $P_1, P_2, \cdots, P_p$。$|P_i|=p^{1+p+\cdots+p^{k-2}}$，故 $|P_1\times P_2\times\cdots\times P_p|=p^{p+p^2+\cdots+p^{k-1}}$。若 P 是包含 $P_1\times P_2\times\cdots\times P_p$ 的 p-Sylow 子羣，則 $[P: P_1\times P_2\times\cdots\times P_p]=p$。故只要找到 $\sigma\in N_{S_{p^k}}(P_1\times\cdots\times P_p)$, $\sigma\notin P_1\times\cdots\times P_p$, $\mathrm{ord}(\sigma)=p^k$。令 σ 是把 $P_1, P_2, \cdots, P_p$ 的對應文字作輪換的置換即可。

例題: 敍述求 S_n 的 p-Sylow 子羣的方法。

解: 考慮 n 的 p 進位表示法：$n=\alpha_0+\alpha_1 p+\cdots+\alpha_k p^k$, $0\leqslant\alpha_i\leqslant p-1$。把 $\{1, 2, \cdots, n\}$ 分成 $1+\alpha_1+\alpha_2+\cdots+\alpha_k$ 類，即：前 α_0 個文字一類，再來是 p 個文字一類，一共做 α_1 次，再來是 p^2 個文字一類，一共做 α_2 次，以次類推。然後個別做

p-Sylow 子羣，再取直積，即得 S_n 的 p-Sylow 子羣。請讀者算一算這些子羣的秩。

習題

1. 設H是有限羣G的子羣，且$H\subsetneq G$。試證 $G\neq \bigcup_{x\in G} xHx^{-1}$。
2. 請決定秩爲168的單羣含有幾個秩爲 7 的元素。
3. 設G是秩爲231的羣，H 是其 11-Sylow 子羣。則 $H\subset Z(G)$。
4. 設G是秩爲30的羣。試證G含有一個秩爲15的元素 x，並且$\langle x\rangle\lhd G$。
5. 請把秩爲30的羣加以分類。
6. 設 p 是質數，請把秩爲 p^3 的羣加以分類。（提示：請參考本章第八節習題 4。）
7. 設H是有限羣G的子羣，$|H|=p^s$，其中p是質數，s是正整數。(1)$p\nmid[N_G(H):H]$ 的充分必要條件是 $p\nmid[G:H]$，(2)若H是p-Sylow子羣，則$N_G(N_G(H))=N_G(H)$，(3)若K是 p-Sylow 子羣，且 $H\trianglelefteq K$，則 HK 不是G的子羣。
8. 試求 S_3, S_4, S_5 的 2-Sylow 子羣與 3-Sylow 子羣。
9. 試證四元數羣（第2.75.小節）的每個子羣都是正則子羣。

第十節　討論

2.84.

羣論是目前數學研究非常活躍的一個分支。主要的研究範圍有，有限羣論 (finite group theory)，組合羣論 (combinatorial group theory)，羣表現理論 (group representation theory)，同調羣論 (homological group theory)。此外還有交換羣與有序羣 (ordered group) 的研究。

即使以有限羣論而言，我們可以討論一般羣的結構問題（如，p 羣，可解羣，羣擴張），置換羣的各種性質，有限單羣的分類、表現理論及其應用。

如果不限制在純粹的羣論，我們還可以看到羣的廣泛的應用，例如，李羣 (Lie groups)，代數羣 (algebraic groups)，不變量理論 (invariant theory)。

具有本章的基礎，讀者如果想做更進一步的研習，不妨參考以下書籍:

〔1〕 B. Huppert and N. Blackburn, *Finite groups*, 3 vols, Springer Grundlehren math. Wiss. vol. 134, 242, 243, Springer-Verlag, 1967, 1982, Berlin.

〔2〕 M. I. Kargapolov and Ju. I. Merzljakov, *Fundamentals of the theory of groups*, GTM vol. 62, Springer-Verlag, 1979, Berlin.

〔3〕 J. Rotman, *The theory of groups*, Allyn and Bacon, 1973, Boston.

〔4〕 M. Suzuki, *Group theory*, Springer Grundlehren math. Wiss. vol. 247, Springer-Verlag, 1982, Berlin.

其中〔3〕最適合初學者。〔1〕是近乎百科全書型的書。〔2〕與〔4〕討論的題材比〔3〕深入很多。

事實上，學那麼多的羣論並不見得是完全必要的。讀者可以直接進入和羣論有關的其他領域。例如，以下著作是極佳的表現理論的入門書籍，

〔5〕 J. P. Serre, *Linear representation of finite groups*, GTM vol. 42, Springer-Verlag, 1977, New York.

有關組合羣論與拓樸學的關係，不妨參考以下書籍

〔6〕 J. Stillwell, *Classical topology and combinatorial group theory*, GTM vol. 72, 1980, Springer-Verlag, New York.

不變量理論的入門書籍是,

〔7〕 L. C. Grove and C. T. Benson, *Finite reflection groups*, GTM vol. 99, Springer-Verlag, 1985, New York.

〔8〕 T. A. Springer, *Invariant theory*, Springer LNM no. 585, Springer-Verlag, 1977, Berlin.

〔9〕 R. P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. 1 (1979) 475～511.

〔7〕介紹有限羣的不變量，非常淺顯易懂。〔9〕討論不變量與組合數學的聯繫。〔8〕是介紹古典不變量的入門書籍。

想學習李羣的讀者不妨從以下書籍入手,

〔10〕 J. F. Adams, *Lectures on Lie groups*, Benjamin Inc., 1969, New York.

〔11〕 C. Chevalley, *Theory of Lie groups* vol. 1, Princeton Univ. Press, 1946 Princeton.