บทที่ 5
กรุปย่อยปกติและกรุปผลหาร

กรุปย่อยเป็นคำเฉพาะที่สามารถให้คำจำกัดความในทางคณิตศาสตร์ได้เช่นเดียวกับคำอื่น ๆ อีกหลายคำ เช่น ความสัมพันธ์ ฟังก์ชัน เป็นต้น จะสังเกตเห็นว่าบางกรุปมีสับเซตที่มีคุณสมบัติเป็นกรุปภายใต้ตัวดำเนินการเดียวกัน เช่น กรุปของจำนวนจริงภายใต้การบวกมีเซตของจำนวนเต็มภายใต้การบวกมีคุณสมบัติเป็นกรุปเช่นเดียวกันซึ่งจะถูกเรียกว่ากรุปย่อย สำหรับบทนี้จะแบ่งเนื้อหาออกเป็น 2 ส่วน ส่วนแรกจะแนะนำให้รู้จักกรุปย่อย และสมบัติเบื้องต้น รวมถึงทฤษฎีที่ตรวจสอบการเป็นกรุปย่อย และส่วนสุดท้ายจะแนะนำให้รู้จักกรุปย่อยปกติ ซึ่งนำไปสู่ทฤษฎีที่สำคัญ คือ ทฤษฎีบทของลากรานจ์ ยิ่งไปกว่านั้นจะแนะนำการสร้างกรุปชนิดหนึ่งจากกรุปย่อย ซึ่งเรียกว่ากรุปผลหาร ดังนี้

นิยามและสมบัติเบื้องต้นของกรุปย่อย

บทนิยาม 5.1 กำหนดให้ G และ $\emptyset \neq H \subseteq G$ เป็นกรุป จะเรียก H ว่าเป็นกรุปย่อย (subgroups) ของ G ถ้า H เป็นกรุปภายใต้การดำเนินการเดียวกันกับของ G เราจะใช้สัญลักษณ์ $H \leq G$ แทน H เป็นกรุปย่อยของ G

ข้อสังเกต จะเห็นว่า G และ $\{e\}$ เป็นกรุปย่อยของ G เราเรียกกรุปย่อยทั้งสองว่ากรุปย่อยชัด (trivial subgroups)

ตัวอย่างที่ 5.1 กำหนดให้ $G = \{1, -1, i, -i\}$ เป็นเซตย่อยของเซตของจำนวนเชิงซ้อน และ $\times$ เป็นการคูณปกติของจำนวนเชิงซ้อน ถ้า $D = \{1, -1\}$ จงแสดงว่า D เป็นกรุปย่อยของ G ภายใต้การดำเนินการ $\times$

วิธีทำ พิจารณาตารางการดำเนินการได้ดังนี้

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

จากตัวอย่างที่ 3.6 ได้ว่า $(G, \times)$ เป็นกรุป
จาก $D \subseteq G$ จะแสดงว่า $(D, \times)$ เป็นกรุป

(1) พิจารณาตารางการดำเนินการได้ดังนี้

$\times$	1	-1
1	1	-1
-1	-1	1

จากตารางการดำเนินการจะได้ว่า $(D, \times)$ มีสมบัติปิด

(2) จากจำนวนเชิงซ้อนมีสมบัติการเปลี่ยนหมู่ภายใต้การคูณ
ดังนั้น $(D, \times)$ มีสมบัติการเปลี่ยนหมู่

(3) มี 1 เป็นสมาชิกเอกลักษณ์ของ D ดังนั้น $(D, \times)$ มีสมบัติการมีเอกลักษณ์

(4) จาก $1 \times 1 = 1$ และ $(-1) \times (-1) = 1$
ดังนั้น $(D, \times)$ มีสมบัติการมีตัวผกผัน
จาก (1), (2), (3) และ (4) สรุปได้ว่า $(D, \times)$ เป็นกรุป
นั่นคือ D เป็นกรุปย่อยของ G ภายใต้การดำเนินการ $\times$

ตัวอย่างที่ 5.2 ให้ $G = \{0, 1, 2, 3\}$ ให้ $*$ เป็นการดำเนินการบน G กำหนดดังนี้

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

จะได้ว่า $(G, *)$ เป็นกรุป ถ้าให้ $H = \{0, 2\}$ จงแสดงว่า H เป็นกรุปย่อยของ G ภายใต้การดำเนินการ $*$

วิธีทำ (1) พิจารณาตารางการดำเนินการได้ดังนี้

$*$	0	2
0	0	2
2	2	0

จากตารางการดำเนินการจะได้ว่า $(H, *)$ มีสมบัติปิด

(2) จาก $(G, *)$ มีสมบัติการเปลี่ยนหมู่ ดังนั้น $(H, *)$ มีสมบัติการเปลี่ยนหมู่

(3) มี 0 เป็นสมาชิกเอกลักษณ์ของ H ดังนั้น $(H, *)$ มีสมบัติการมีเอกลักษณ์

(4) จาก $0 * 0 = 0$ และ $2 * 2 = 0$
ดังนั้น $(H, *)$ มีสมบัติการมีตัวผกผัน
จาก (1), (2), (3) และ (4) สรุปได้ว่า $(H, *)$ เป็นกรุป
นั่นคือ H เป็นกรุปย่อยของ G ภายใต้การดำเนินการ $*$

ทฤษฎีบท 5.2 กำหนดให้ G เป็นกรุป และ $\varnothing \neq H \subseteq G$ จะได้ว่า H เป็นกรุปย่อยของ G ก็ต่อเมื่อ

1. ถ้า $a, b \in H$ แล้ว $ab \in H$
2. ถ้า $a \in H$ แล้ว $a^{-1} \in H$

การพิสูจน์ ($\Rightarrow$) ถ้า H เป็นกรุปย่อยของ G จะเห็นได้ชัดว่า 1. และ 2. จริง

($\Leftarrow$) สมมติให้ 1. และ 2. จริง จะแสดงว่า H เป็นกรุป
นั่นคือ ต้องแสดงว่า H มีสมบัติการเปลี่ยนหมู่ และมีเอกลักษณ์ $e \in H$
เนื่องจาก H เป็นเซตย่อยของ G และ G มีสมบัติการเปลี่ยนหมู่
ดังนั้น H มีสมบัติการเปลี่ยนหมู่
ถ้า $a \in H$ โดย 2. $a^{-1} \in H$ และโดย 1. $e = aa^{-1} \in H$
นั่นคือ มีเอกลักษณ์ $e \in H$

ทฤษฎีบท 5.3 กำหนดให้ G และ $\emptyset \neq H \subseteq G$ จะกล่าวว่า H เป็นกรุปย่อยของ G ก็ต่อเมื่อ ถ้า $a, b \in H$ แล้ว $ab^{-1} \in H$

การพิสูจน์ กำหนดให้ H เป็นกรุปย่อยของ G

($\Rightarrow$) สมมติ $a, b \in H$
จากสมบัติการมีอินเวอร์สของกรุป จะได้ว่า $a, b^{-1} \in H$
จากกรุปมีสมบัติปิด ดังนั้น $ab^{-1} \in H$

($\Leftarrow$) สมมติ $a \in H$
พิจารณา $e = aa^{-1} \in H$
เนื่องจาก $e \in H$ และ $a \in H$ ดังนั้น $ea^{-1} \in H$
นั่นคือ $a^{-1} \in H$
ต่อไปนี้จะแสดงว่า H มีสมบัติปิด
สมมติ $a, b \in H$ ดังนั้น $a, b^{-1} \in H$
จะได้ว่า $a(b^{-1})^{-1} \in H$
นั่นคือ $ab \in H$
โดยทฤษฎีบท 5.2 จะได้ว่า H เป็นกรุปย่อยของ G

ตัวอย่างที่ 5.3 ให้ $n \in \mathbb{N}$ และ $n\mathbb{Z} = \{x \in \mathbb{Z} | x = nk, \exists k \in \mathbb{Z}\}$ จงแสดงว่า $(n\mathbb{Z}, +)$ เป็นกรุปย่อยของ $(\mathbb{Z}, +)$

วิธีทำ กำหนดให้ $x, y \in n\mathbb{Z}$
จะมี $h, k \in \mathbb{Z}$ ซึ่งทำให้ $x = nh$ และ $y = nk$
ดังนั้น $x + y = nh + nk = n(h + k) \in n\mathbb{Z}$
จะมี $h, k \in \mathbb{Z}$ ซึ่งทำให้ $x = nh$ และ $y = nk$
เนื่องจาก $x + 0 = x$ ดังนั้น 0 เป็นตัวเอกลักษณ์
เนื่องจาก $x + (-x) = 0$ ดังนั้น $-x$ เป็นตัวผกผันของ x
เพราะฉะนั้น $-x = -nh = n(-h) \in n\mathbb{Z}$
โดยทฤษฎีบท 5.2 จะได้ $n\mathbb{Z}$ เป็นกรุปย่อยของ $(\mathbb{Z}, +)$

ทฤษฎีบท 5.4 กำหนดให้ G เป็นกรุป และ H เป็นเซตย่อยจำกัดที่ไม่ว่างของกรุป G ถ้า $ab \in H$ สำหรับทุก $a, b \in H$ แล้ว H เป็นกรุปย่อยของ G

การพิสูจน์ โดยทฤษฎีบท 5.2 ถ้าเราพิสูจน์ได้ว่า สำหรับทุก ๆ $a \in H, a^{-1} \in H$
จะสรุปได้ว่า H เป็นกรุปย่อยของ G
ให้ $a \in H$
เนื่องจาก H มีสมบัติปิด
จะได้ว่า $a^2 = aa \in H, a^3 = a^2a \in H, ..., a^m \in H, ...$
ดังนั้น สำหรับทุก $m \in \mathbb{Z}$ จะได้ว่า $a, a^2, a^3, ..., a^m, ... \in H$
เนื่องจาก H เป็นเซตจำกัด
ดังนั้น มีจำนวนเต็ม r, s ซึ่ง $r > s > 0$ ที่ทำให้ $a^r = a^s$
จะได้ $e = a^{r-s} \in H$
เนื่องจาก $r - s - 1 \geq 0$ ดังนั้น $a^{r-s-1} \in H$
เนื่องจาก $aa^{r-s-1} = a^{r-s} = e$ จะได้ว่า $a^{-1} = a^{r-s-1}$
ดังนั้น $a^{-1} \in H$
นั่นคือ H เป็นกรุปย่อยของ G

บทนิยาม 5.5 กำหนดให้ G เป็นกรุป และ H เป็นกรุปย่อยของ G สำหรับ $a, b \in G$ จะกล่าวว่า a คอนกรูเอนซ์กับ b มอดุโล H (a is congruent to b modulo H) ก็ต่อเมื่อ $ab^{-1} \in H$ และเขียนแทน " a คอนกรูเอนซ์กับ b มอดุโล H " ด้วยสัญลักษณ์ $a \equiv b \mod H$

ตัวอย่างที่ 5.4 จงพิสูจน์ว่า ความสัมพันธ์ $a \equiv b \mod H$ เป็นความสัมพันธ์สมมูลบนกรุป G

วิธีทำ กำหนดให้ G เป็นกรุปที่มี e เป็นสมาชิกเอกลักษณ์ของ G และ $H \leq G$
สมมติให้ $a, b, c \in G$

(1) เนื่องจาก $aa^{-1} = e \in H$
ดังนั้น $a \equiv a \mod H$

(2) สมมติให้ $a \equiv b \mod H$
ดังนั้น $ab^{-1} \in H$
เนื่องจาก $H \leq G$ จะได้ว่า $ba^{-1} = (b^{-1})^{-1}a^{-1} = (ab^{-1})^{-1} \in H$
นั่นคือ $b \equiv a \mod H$

(3) สมมติให้ $a \equiv b \mod H$ และ $b \equiv c \mod H$
เพราะฉะนั้น $ab^{-1}, bc^{-1} \in H$
จาก $H \leq G$ จะได้ว่า $ac^{-1} = a(e)c^{-1} = a(b^{-1}b)c^{-1} = (ab)^{-1}(bc)^{-1} \in H$
นั่นคือ $a \equiv c \mod H$

จาก $(1), (2)$ และ (3) สรุปได้ว่า $a \equiv b \mod H$ เป็นความสัมพันธ์สมมูล

บทนิยาม 5.6 กำหนดให้ H เป็นกรุปย่อยของกรุป G และ $a \in G$ จะเรียกเซต $Ha = \{ha \mid h \in H\}$ ว่าโคเซตทางขวา (right coset) ของ H ใน G และเรียกเซต $aH = \{ah \mid h \in H\}$ ว่าโคเซตทางซ้าย (left coset) ของ H ใน G

ตัวอย่างที่ 5.5 ถ้าให้ $H = \{[0], [2], [4]\} \subset \mathbb{Z}_6$ จงแสดงว่า H เป็นกรุปย่อยของ $(\mathbb{Z}_6, +_6)$ และหาโคเซตทางขวาของ H ทั้งหมดใน G

วิธีทำ พิจารณาตารางการดำเนินการของ H ภายใต้การดำเนินการ $+_6$

$+_6$	$[0]$	$[2]$	$[4]$
$[0]$	$[0]$	$[2]$	$[4]$
$[2]$	$[2]$	$[4]$	$[0]$
$[4]$	$[4]$	$[0]$	$[2]$

เห็นได้ชัดว่า $(H, +_6)$ มีสมบัติปิด
โดยทฤษฎีบท 5.4 จะได้ว่า H เป็นกรุปย่อยของ G

พิจารณา $H +_6 [0] = \{h +_6 [0] \mid h \in H\}$

$$= \{[0] +_6 [0], [2] +_6 [0], [4] +_6 [0]\}$$

$$= \{[0], [2], [4]\}$$

พิจารณา $H +_6 [1] = \{h +_6 [1] \mid h \in H\}$

$$= \{[1] +_6 [0], [2] +_6 [1], [4] +_6 [1]\}$$

$$= \{[1], [3], [5]\}$$

ในทำนองเดียวกัน จะได้ว่า

$$H +_6 [2] = \{[0], [2], [4]\} = H +_6 [4]$$

$$H +_6 [3] = \{[1], [3], [5]\} = H +_6 [5]$$

ดังนั้น $\{[0], [2], [4]\}$ และ $\{[1], [3], [5]\}$ เป็นโคเซตทางขวาของ H ทั้งหมดใน G

ทฤษฎีบท 5.7 กำหนดให้ H เป็นกรุปย่อยของกรุป G และ $a \in G$ จะได้ว่า

$$Ha = \{x \in G \mid a \equiv x \mod H\} = [a]$$

การพิสูจน์ เนื่องจากความสัมพันธ์ดังกล่าวเป็นความสัมพันธ์สมมูล ดังนั้น ชั้นสมมูล

$$[a] = \{x \in G \mid a \equiv x \mod H\}$$

เราจะแสดงว่า $Ha = \{x \in G | a \equiv x (modH)\}$
สมมติให้ $ha \in Ha$ ดังนั้น $h \in H$
ถ้าให้ e เป็นสมาชิกเอกลักษณ์ของ G จะได้ว่า

$$a(ha)^{-1} = a(a^{-1}h^{-1}) = (aa)^{-1}h^{-1} = eh^{-1} = h^{-1} \in H$$

ดังนั้น $a \equiv ha \mod H$
นั่นคือ $ha \in \{x \in G | a \equiv x \mod H\}$
จึงได้ว่า $Ha \subseteq \{x \in G | a \equiv x \mod H\}$
ต่อไปสมมติให้ $b \in \{x \in G \mid a \equiv x \mod H\}$
จะได้ว่า $a \equiv b \mod H$
ดังนั้น $ab^{-1} \in H$
นั่นคือ มี $h \in H$ ที่ทำให้ $ab^{-1} = h$
เพราะฉะนั้น $h^{-1}a = b$
จึงได้ว่า $b \in Ha$
ดังนั้น $\{x \in G \mid a \equiv x \mod H\} \subseteq Ha$
จึงสรุปได้ว่า $Ha = \{x \in G | a \equiv x \mod H\} = [a]$

หมายเหตุ เนื่องจาก $[a] = Ha$ จะได้ว่า $G = \bigcup_{a \in G} [a] = \bigcup_{a \in G} (Ha)$ ในตัวอย่างที่ 5.5 พิจารณากรุป $(\mathbb{Z}_6, +_6)$ เมื่อ $H = \{[0], [2], [4]\}$ จะได้ว่า

$$\mathbb{Z}_6 = \bigcup_{a \in \mathbb{Z}_6} (Ha) = (H +_6 [0] \cup (H +_6 [1])$$

ทฤษฎีบท 5.8 กำหนดให้ H เป็นกรุปย่อยของกรุป G และ $a, b \in G$ ถ้า Ha และ Hb เป็นโคเซตทางขวาของ H ใน G แล้วจะมีการสมนัยหนึ่งต่อหนึ่งระหว่าง Ha และ Hb

การพิสูจน์ กำหนดให้ Ha และ Hb เป็นโคเซตทางขวาของ H ใน G
และกำหนด $f : Ha \to Hb$ ดังนี้

$$f(ha) = hb \text{ สำหรับทุก } h \in H$$

เห็นได้ชัดว่า f เป็นฟังก์ชันทั่วถึง
ต่อไปจะแสดงว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง
สมมติให้ $ha, h'a \in H$ และ $f(ha) = f(h'a)$
ดังนั้น $hb = h'b$
อาศัยสมบัติการตัดออก จะได้ว่า $h = h'$
นั่นคือ $ha = h'a$

ทฤษฎีบท 5.9 ทฤษฎีบทลากรานจ์ (Lagrange's Theorem)
ถ้า G เป็นกรุปจำกัด และ H เป็นกรุปย่อยของ G แล้ว $|H| \mid |G|$

การพิสูจน์ กำหนดให้ G เป็นกรุปจำกัดที่มี e เป็นสมาชิกเอกลักษณ์ และ $H \leq G$
จาก $H = He$ ดังนั้นจำนวนสมาชิกของ H จะเท่ากับจำนวนสมาชิกของ He
โดยทฤษฎีบท 5.8 สำหรับทุก $a \in G$
จะได้ว่า จำนวนสมาชิกของ He เท่ากับจำนวนสมาชิกของ Ha
ดังนั้น จำนวนสมาชิกของโคเซตทางขวาของ H เท่ากับจำนวนสมาชิกของ H
ให้ k คือจำนวนโคเซตทางขวาของ H ใน G ที่แตกต่างกันทั้งหมด
เนื่องจาก $G = \bigcup_{a \in \mathbb{G}} (Ha)$ ทำให้ได้ว่า $|G| = k \times |H|$
นั่นคือ $|H| \mid |G|$

บทแทรก 5.10 ถ้า G เป็นกรุปจำกัดที่มี e เป็นสมาชิกเอกลักษณ์ และ G มีอันดับเป็นจำนวนเฉพาะ แล้ว

1. กรุปย่อยของ G คือ $\{e\}$ และ G เท่านั้น
2. G เป็นกรุปวัฏจักร

การพิสูจน์ กำหนดให้ G เป็นกรุปจำกัดที่มี e เป็นสมาชิกเอกลักษณ์ และ
G มีอันดับเป็น p เมื่อ p เป็นจำนวนเฉพาะ

(1) โดยทฤษฎีบทลากรานจ์ จะได้ว่า กรุปย่อยของ G มีเพียง $\{e\}$ และ G เท่านั้น

(2) เนื่องจาก $|G| > 1$
สมมติให้ $a \in G$ โดยที่ $a \neq e$
พิจารณา $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$
สมมติให้ $a^r, a^s \in \langle a \rangle$
จะได้ว่า $a^r a^s = a^{r+s} \in \langle a \rangle$
สำหรับแต่ละ $a^t \in < a >$ จะมี $a^{-t} \in \langle a \rangle$ ที่ทำให้ $a^t a^{-t} = a^0 = e$
โดยทฤษฎีบท 5.2 จะได้ว่า $\langle a \rangle \leq G$ และ $|\langle a \rangle| = m \geq 2$
โดยทฤษฎีบทลากรานจ์ จะได้ว่า $m|p$ ดังนั้น $m = p$
นั่นคือ $\langle a \rangle = G$ จึงได้ว่า G เป็นกรุปวัฏจักร

บทนิยาม 5.11 กำหนดให้ H เป็นกรุปย่อยของกรุป G ดรรชนี (index) ของ H ใน G หมายถึง จำนวนของโคเซตทางขวา (หรือโคเซตทางซ้าย) ของ H ใน G ที่แตกต่างกันทั้งหมด และเขียนแทนดรรชนีของ H ใน G ด้วยสัญลักษณ์ $(G : H)$

จากตัวอย่างที่ 5.5 จะได้ว่า $(\mathbb{Z}_6 : H) = 2$ ผลพลอยได้จากทฤษฎีบทลากรานจ์ที่เกี่ยวข้องกับอันดับของสมาชิกในกรุปจำกัดที่มีอยู่หลายลักษณะโดยก่อนอื่นจะให้นิยามของอันดับของสมาชิกดังนี้

บทแทรก 5.12 ถ้า G เป็นกรุปจำกัด และ $a \in G$ แล้ว $|a| \Big| |G|$

การพิสูจน์ กำหนดให้ G เป็นกรุปจำกัดที่มี e เป็นสมาชิกเอกลักษณ์ของ G และ $a \in G$ โดยทฤษฎีบท 4.3 จะได้ว่า

$$\langle a \rangle = \{\ a^n \mid n \in \mathbb{Z}\ \} = \{\ e, a, ..., a^{m-1}\ \}$$

เมื่อ m เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ $a^m = e$
และ $\langle a \rangle$ เป็นกรุปย่อยของ G ที่ซึ่ง $|\langle a \rangle| = m$
โดยทฤษฎีบทลากรานจ์ จะได้ว่า $|\langle a \rangle| \Big| |G|$ แต่ $|\langle a \rangle| = |a|$
เพราะฉะนั้น $|a| \Big| |G|$

บทแทรก 5.13 ถ้า G เป็นกรุปจำกัดที่มี e เป็นสมาชิกเอกลักษณ์ของ G และ $a \in G$ แล้ว $a^{|G|} = e$

การพิสูจน์ กำหนดให้ G เป็นกรุปจำกัดที่มี e เป็นสมาชิกเอกลักษณ์ของ G
และ $a \in G$ จาก $|a| \Big| |G|$
จะได้ว่ามี $k \in \mathbb{N}$ ที่ทำให้ $|G| = k|a|$
เพราะฉะนั้น $a^{|G|} = a^{k|a|} = (a^{|a|})^k = (e)^k = e$

กรุปย่อยปกติและกรุปผลหาร

การสร้างกรุปใหม่จากกรุปที่กำหนดให้ทำได้หลายวิธี วิธีหนึ่งที่สำคัญในทางคณิตศาสตร์ คือ การสร้างโดยอาศัยความสัมพันธ์สมมูลที่กำหนดบนกรุปนั้นเอง และเรียกกรุปที่สร้างโดยวิธีนี้ว่ากรุปผลหาร ปุณศยา พัฒนางกูร (2555: 139-144) ได้ให้นิยาม ตัวอย่าง และทฤษฎีที่เกี่ยวข้อง ดังนี้

บทนิยาม 5.14 กำหนดให้ N เป็นกรุปย่อยของกรุป G เรียก N ว่ากรุปย่อยปรกติ (nolmal subgroup or invariant subgroup) ของ G ก็ต่อเมื่อ $gng^{-1} \in N$ สำหรับทุก $g \in G$ และ $n \in N$ ดังนั้น $gNg^{-1} = \{gng^{-1} | n \in N\}$ จะได้ว่า N เป็นกรุปย่อยปรกติของ G ก็ต่อเมื่อ $gNg^{-1} \subseteq N$ สำหรับทุก $g \in G$

หมายเหตุ ในกรณีที่ N เป็นกรุปย่อยของอาบีเลียนกรุป G จะได้ว่า N เป็นกรุปย่อยปรกติของ G เสมอ ทั้งนี้เพราะว่า

$$\begin{aligned} gNg^{-1} &= \{gng^{-1} \mid n \in N\} \\ &= \{ngg^{-1} \mid n \in N\} \\ &= \{ne \mid n \in N\} \text{ เมื่อ } e \text{ เป็นสมาชิกเอกลักษณ์ของ } G \\ &= \{n \mid n \in N\} \\ &= N \end{aligned}$$

ตัวอย่างที่ 5.6 กำหนดให้ $S = \{1, 2, 3\}$ และ $A(S) = \{f \mid f : S \xrightarrow[onto]{1-1} S\} = \{e, \alpha, \beta, \gamma, \delta, \theta\}$ โดยที่

$$e : \begin{array}{r} 1 \longrightarrow 1 \\ 2 \longrightarrow 2 \\ 3 \longrightarrow 3 \end{array} \qquad \alpha : \begin{array}{r} 1 \longrightarrow 2 \\ 2 \longrightarrow 1 \\ 3 \longrightarrow 3 \end{array} \qquad \beta : \begin{array}{r} 1 \longrightarrow 2 \\ 2 \longrightarrow 3 \\ 3 \longrightarrow 1 \end{array}$$

$$\gamma : \begin{array}{r} 1 \longrightarrow 3 \\ 2 \longrightarrow 2 \\ 3 \longrightarrow 1 \end{array} \qquad \delta : \begin{array}{r} 1 \longrightarrow 1 \\ 2 \longrightarrow 3 \\ 3 \longrightarrow 2 \end{array} \qquad \theta : \begin{array}{r} 1 \longrightarrow 3 \\ 2 \longrightarrow 1 \\ 3 \longrightarrow 2 \end{array}$$

จงแสดงว่า $(A(S), \circ)$ เป็นกรุป ยิ่งไปกว่านั้น ถ้า $H = \{e, \alpha\}$ และ $K = \{e, \beta, \theta\}$ จงพิจารณาว่า H และ K เป็นกรุปย่อยปกติหรือไม่ อย่างไร

วิธีทำ พิจารณาตารางการดำเนินการของ $A(S)$ ภายใต้การดำเนินการ $\circ$

$\circ$	e	α	β	γ	δ	θ
e	e	α	β	γ	δ	θ
α	α	e	γ	β	θ	δ
β	β	δ	θ	α	γ	e
γ	γ	θ	δ	e	β	α
δ	δ	β	α	θ	e	θ
θ	θ	γ	e	δ	α	β

จะได้ว่า $(A(S), \circ)$ เป็นกรุป
นอกจากนี้ จะได้ว่า $H \leq A(S)$ และ $K \leq A(S)$
เนื่องจาก $\beta H \beta^{-1} = \beta H \theta = \{\beta \circ e \circ \theta, \beta \circ \alpha \circ \theta\} = \{e, \delta\} \nsubseteq H$
ดังนั้น H ไม่เป็นกรุปย่อยปรกติของ $A(S)$

เพราะว่า
$$\begin{aligned} eKe^{-1} &= eKe &&= \{\, e, \beta, \theta \,\} \subseteq K \\ \alpha K \alpha^{-1} &= \alpha K \alpha &&= \{\, e, \theta, \beta \,\} \subseteq K \\ \beta K \beta^{-1} &= \beta K \theta &&= \{\, e, \beta, \theta \,\} \subseteq K \\ \gamma K \gamma^{-1} &= \gamma K \gamma &&= \{\, e, \theta, \beta \,\} \subseteq K \\ \delta K \delta^{-1} &= \delta K \delta &&= \{\, e, \theta, \beta \,\} \subseteq K \end{aligned}$$
และ
$$\theta K \theta^{-1} = \theta K \beta = \{\, e, \beta, \theta \,\} \subseteq K$$

ดังนั้น K เป็นกรุปย่อยปรกติของ $A(S)$

เงื่อนไขอื่น ๆ ที่สามารถใช้ตรวจสอบความเป็นกรุปย่อยปรกติมีดังนี้

ทฤษฎีบท 5.15 กำหนดให้ N เป็นกรุปย่อยของกรุป G จะได้ว่าข้อความต่อไปนี้สมมูลกัน

1. N เป็นกรุปย่อยปรกติของ G
2. $gNg^{-1} = N$ สำหรับทุก $g \in G$
3. $gN = Ng$ สำหรับทุก $g \in G$
4. $(Ng_1)(Ng_2) = N(g_1g_2)$ สำหรับทุก $g_1, g_2 \in G$

การพิสูจน์ กำหนดให้ N เป็นกรุปย่อยของกรุป G และ e เป็นสมาชิกเอกลักษณ์ของ G

(1.) $\Longrightarrow$ (2.) กำหนดให้ N เป็นกรุปย่อยปรกติของกรุป G
จะได้ว่า $gNg^{-1} \subseteq N$ สำหรับทุก ๆ $g \in G$
ถ้าให้ $g \in G$ แล้ว $g^{-1} \in G$
ดังนั้น $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subseteq N$
ต่อไปสมมติให้ $n \in N$ จะได้ว่า $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$
นั่นคือ $N \subseteq gNg^{-1}$
จึงสรุปได้ว่า gNg^{-1} = N สำหรับทุก $g \in G$

(2.) $\Longrightarrow$ (3.) กำหนดให้ $gNg^{-1} = N$ สำหรับทุก $g \in G$
สมมติให้ $g \in G$ จะได้ว่า $(gNg^{-1})g = Ng$
แต่ $(gNg^{-1})g = gN(g^{-1}g) = gN(e) = gN$
เพราะฉะนั้น $gN = Ng$ สำหรับทุก $g \in G$

(3.) $\Longrightarrow$ (4.) กำหนดให้ $gN = Ng$ สำหรับทุก $g \in G$
และสมมติให้ $g_1, g_2 \in G$ จะได้ว่า $(g_1N)g_2 = (Ng_1)g_2$
เนื่องจาก $NN = N$ เมื่อ $NN = \{n_1n_2 \mid n_1n_2 \in N\}$
ดังนั้น $(g_1NN)g_2 = (Ng_1)g_2$
แต่ $(Ng_1)g_2 = N(g_1g_2)$
และ $(g_1NN)g_2 = (g_1N)(Ng_2) = (Ng_1)(Ng_2)$
จึงสรุปได้ว่า $(Ng_1)(Ng_2) = N(g_1g_2)$ สำหรับทุก $g_1, g_2 \in G$

(4.) $\Longrightarrow$ (1.) กำหนดให้ $(Ng_1)(Ng_2) = N(g_1g_2)$ สำหรับทุก $g_1, g_2 \in G$
และสมมติให้ $g \in G$
เนื่องจาก $g^{-1} \in G$ ดังนั้น $(Ng)(Ng^{-1}) = N(gg^{-1}) = N(e) = N$
นั่นคือ $N(gNg^{-1}) = N$
ถ้า $gng^{-1} \in gNg^{-1}$ จะได้ว่า $gng^{-1} = e(gng^{-1}) \in N(gNg^{-1})$
นั่นคือ $gng^{-1} \in N$
จึงสรุปได้ว่า $gNg^{-1} \subseteq N$ สำหรับทุก $g \in G$
นั่นคือ N เป็นกรุปย่อยปรกติของ G

หมายเหตุ จากบทนิยาม 5.6 และทฤษฎีบท 5.7 จะได้ว่า Na คือ ชั้นสมมูลของ a ใน G ที่เกิดจากความสัมพันธ์สมมูล $a \equiv b \mod N$ ดังนั้น ถ้าให้ G/N คือ เซตที่ประกอบไปด้วยชั้นสมมูลที่เกิดจากความสัมพันธ์ดังกล่าว และกำหนดความสัมพันธ์บน G/N แล้วจะได้ว่าความสัมพันธ์ที่ว่านั้นเป็นการดำเนินการทวิภาคบน G/N

บทนิยาม 5.16 กำหนดให้ N เป็นกรุปย่อยปรกติของกรุป G และ $G/N = \{Ng \mid g \in G\}$ กำหนดความสัมพันธ์บน G/N ดังนี้

$$(Ng_1)(Ng_2) = N(g_1g_2) \text{ สำหรับทุก } Ng_1, Ng_2 \in G/N$$

ทฤษฎีบท 5.17 กำหนดให้ N เป็นกรุปย่อยปรกติของกรุป G จะได้ว่าเซต G/N กับการดำเนินการทวิภาคในบทนิยาม 5.16 เป็นกรุป และเรียก G/N ว่ากรุปการหาร (factor group or quotient group) ของ G โดย N

การพิสูจน์ สมมติให้ $Ng_1, Ng_2, Ng_3 \in G/N$

(1) จากนิยาม 5.16 $(Ng_1)(Ng_2) = N(g_1g_2) \in G/N$
นั่นคือ G/N มีสมบัติการปิด

(2) พิจารณา
$$\begin{aligned}((Ng_1)(Ng_2))(Ng_3) &= (N(g_1g_2))(Ng_3)\\ &= (N(g_1g_2))(Ng_3)\\ &= N(g_1(g_2g_3))\\ &= (Ng_1)(N(g_2g_3))\\ &= (Ng_1)((Ng_2)(Ng_3))\end{aligned}$$
นั่นคือ G/N มีสมบัติการเปลี่ยนหมู่

(3) พิจารณา $Ne = N$ เมื่อ e เป็นสมาชิกเอกลักษณ์ของ G
สำหรับทุก $g \in G$ จะได้ว่า $(Ne)(Ng) = N(eg) = Ng$
และ $(Ng)(Ne) = N(ge) = Ng$
นั่นคือ Ne เป็นสมาชิกเอกลักษณ์ของ G/N

(4) สำหรับแต่ละ $Ng \in G/N$ จะมี $Ng^{-1} \in G/N$ ที่ทำให้
$$(Ng)(Ng^{-1} = N(gg^{-1}) = Ne = N$$
$$(Ng^{-1})(Ng) = N(g^{-1}g) = Ne = N$$
ดังนั้น Ng^{-1} เป็นตัวผกผันของ Ng จึงได้ว่า G/N เป็นกรุป

ทฤษฎีบท 5.18 กรุปผลหาร $\mathbb{Z}/n\mathbb{Z}$ คือกรุป $(\mathbb{Z}_n, +_n)$ เมื่อ $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$

การพิสูจน์ เนื่องจาก $(\mathbb{Z}, +)$ เป็นอาบีเลียนกรุป
ดังนั้น $n\mathbb{Z}$ เป็นกรุปย่อยปรกติของ $\mathbb{Z}$ และ $\mathbb{Z}/n\mathbb{Z}$ ประกอบด้วยสมาชิกต่อไปนี้

$$n\mathbb{Z} + 0 = \{nz + 0 \mid z \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x \equiv 0 \mod n\} = [0]$$
$$n\mathbb{Z} + 1 = \{nz + 1 \mid z \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x \equiv 1 \mod n\} = [1]$$
$$n\mathbb{Z} + 2 = \{nz + 2 \mid z \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x \equiv 2 \mod n\} = [2]$$
$$\vdots$$
$$\begin{aligned} n\mathbb{Z} + (n-1) &= \{nz + (n-1) \mid z \in \mathbb{Z}\} \\ &= \{x \in \mathbb{Z} \mid x \equiv n-1 \mod n\} = [n-1] \end{aligned}$$

สำหรับ $n\mathbb{Z} + a, n\mathbb{Z} + b \in \mathbb{Z}/n\mathbb{Z}$
จะได้ว่า $(n\mathbb{Z} + a) + (n\mathbb{Z} + b) = n\mathbb{Z} + (a + b)$
นั่นคือ $[a] + [b] = [a + b]$ ดังนั้น $\mathbb{Z}/n\mathbb{Z}$ คือ กรุป $(\mathbb{Z}_n, +_n)$

ในกรณีที่ G เป็นกรุปจำกัด จะได้ว่า ความสัมพันธ์ระหว่างอันดับของ G/N กับอันดับของ G และอันดับของ N มีดังนี้

ทฤษฎีบท 5.19 ถ้า N เป็นกรุปย่อยปรกติของ G แล้ว $|G/N| = \dfrac{|G|}{|N|}$

การพิสูจน์ ให้ G เป็นกรุปจำกัด และ N เป็นกรุปย่อยปรกติของกรุปของ G
เนื่องจาก $G/N = \{Na \mid a \in G\}$
คือ เซตของโคเซตทางขวาของ N ใน G ทั้งหมด
จากการพิสูจน์ทฤษฎีบทลากรานจ์ จะได้ว่า $\dfrac{|G|}{|N|}$
คือ จำนวนโคเซตทางขวาของ N ใน G ที่แตกต่างกันทั้งหมด เพราะฉะนั้น

$$|G/N| = \frac{|G|}{|N|}$$

สรุปท้ายบท

จากเนื้อหาทั้งหมดที่กล่าวมาในบทนี้จะเห็นว่า เราศึกษากรุปย่อย และสมบัติเบื้องต้น โดยส่วนมากจะเป็นทฤษฎีที่ตรวจสอบการเป็นกรุปย่อย โดยพื้นฐานแล้วจะพบว่า การที่เราจะกล่าวว่า กรุป ๆ หนึ่งเป็นกรุปย่อยของอีกกรุปหนึ่งนั้นไม่เพียงเป็นเซตย่อยของกรุปหลังเท่านั้น แต่ผลของการดำเนินการของสมาชิกสองตัวใด ๆ ในกรุปแรกจะต้องให้ผลลัพธ์เช่นเดียวกันกับการดำเนินการของสมาชิกสองตัวนั้นในกรุปหลัง นอกจากนี้ทฤษฎีของกรุปย่อยปกติ ทฤษฎีบทลากรานจ์ กรุปผลหาร ยังทำให้ทราบว่า กรุปใด ๆ ที่เราสนใจ มีกรุปย่อยหรือไม่ และมีจำนวนเท่าไร