บทที่ 6
โฮโมมอร์ฟิซึมและไอโซมอร์ฟิซึม

จากทั้ง 5 บทที่ผ่านมาทำให้รู้จักกรุป และคุณสมบัติต่าง ๆ ของกรุป ในบทนี้จะกล่าวถึงความสัมพันธ์ระหว่างกรุปสองกรุปโดยอาศัยฟังก์ชันเป็นสื่อในการศึกษา เนื่องจากกรุปประกอบด้วย เซตและตัวดำเนินการ เราจึงสามารถแสดงความสัมพันธ์ระหว่างกรุปสองกรุปได้ ซึ่งมีลักษณะเช่นเดียวกันกับคณิตศาสตร์แขนงอื่น ๆ ที่ศึกษาความเหมือนของสองระบบที่เราสนใจ โดยอาศัยฟังก์ชันพิเศษเป็นสื่อกลาง ในบทนี้จะแบ่งเป็นสองส่วน คือ โฮโมมอร์ฟิซึม และไอโซมอร์ฟิซึม ดังนี้

โฮโมมอร์ฟิซึม

ปุณศยา พัฒนางกูร (2555: 146-148) ได้ให้นิยามและตัวอย่างของโฮโมมอร์ฟิซึม ดังนี้

บทนิยาม 6.1 กำหนดให้ $(G,\cdot)$ และ $(G',*)$ เป็นกรุปใด ๆ เรียกฟังก์ชัน $\theta : G \to G'$ ว่าโฮโมมอร์ฟิซึมหรือสาทิสสัณฐาน (homomorphism) ก็ต่อเมื่อ

$$\theta(a \cdot b) = \theta(a) * \theta(b) \text{ สำหรับทุก } a, b \in G$$

และเซตของโฮโมมอร์ฟิซึมทั้งหมดจาก G ไป G' เขียนแทนด้วยสัณลักษณ์ Hom(G,G')

นอกจากนี้ ยังมีฟังก์ชันชนิดต่าง ๆ ดังบทนิยามต่อไปนี้

บทนิยาม 6.2 กำหนดให้ G และ G' เป็นกรุปใด ๆ เรียกโฮโมมอร์ฟิซึมจาก G ไป G ว่าเอนโดมอร์ฟิซึมหรืออันตรสัณฐาน (endomorphism) ของ G และเซตของเอนโดมอร์ฟิซึมทั้งหมดของ G เขียนแทนด้วยสัญลัษณ์ End(G) เรียกโฮโมมอร์ฟิซึมชนิดหนึ่งต่อหนึ่งจาก G ไป G' ว่าโมโนมอร์ฟิซึม (monomorphism) จาก G ไป G' และเซตของโมโนมอร์ฟิซึมทั้งหมดจาก G ไป G' เขียนแทนด้วยสัญลักษณ์ Mon(G,G') และเรียกโฮโมมอร์ฟิซึมจาก G ไปทั่วถึง G' ว่าอิพิมอร์ฟิซึม (epimorphism) จาก G ไป G' และเซตของอิพิมอร์ฟิซึมทั้งหมดจาก G ไป G' เขียนแทนด้วยสัญลักษณ์ Epi(G,G')

ข้อสังเกต จากบทนิยาม 6.1 และ 6.2 จะพบว่า

1. End(G) $=$ Hom(G,G)
2. Mon(G,G') $= \{f \in$ Hom$(G,G') \mid f$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง$\}$
   Mon$(G,G') \subseteq$ Hom(G,G')
3. Epi(G,G') $= \{f \in$ Hom$(G,G') \mid f(G) = G'\}$
   นั่นคือ Epi$(G,G') \subseteq$ Hom(G,G')

ตัวอย่างที่ 6.1 กำหนดให้ G เป็นกรุปใด ๆ และ $i_G : G \to G$ เป็นฟังก์ชันเอกลักษณ์ จงพิจารณาว่าฟังก์ชัน i_G เป็นฟังก์ชันชนิดใด

วิธีทำ สมมติให้ $a, b \in G$
จาก $i_G(ab) = ab = i_G(a)i_G(b)$
ดังนั้น $i_G \in \text{End}(G)$
และเนื่องจาก i_G เป็นฟังก์ชันก์หนึ่งต่อหนึ่งและฟังก์ชันทั่วถึง
จะได้ว่า $i_G \in \text{Mon}(G, G)$ และ $i_G \in \text{Epi}(G, G)$

ตัวอย่างที่ 6.2 กำหนดให้ $(G, \cdot)$ และ $(G', *)$ เป็นกรุป และฟังก์ชัน $\theta : G \to G'$ กำหนดดังนี้ $\theta(a) = e'$ สำหรับทุก $a \in G$ เมื่อ e' เป็นสมาชิกเอกลักษณ์ของ G' จงพิจารณาว่าฟังก์ชัน θ เป็นฟังก์ชันชนิดใด

วิธีทำ สมมติให้ $a, b \in G$
จะได้ว่า $\theta(a \cdot b) = e' = e' * e' = \theta(a) * \theta(b)$
ดังนั้น $\theta \in \text{Hom}(G, G')$ และเรียก θ เช่นนี้ว่าฟังก์ชันศูนย์ (zero funtion)

ตัวอย่างที่ 6.3 กำหนดฟังก์ชัน $\theta : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ ดังนี้ $\theta(a) = 2^a$ สำหรับทุก $a \in G$ จงพิจารณาว่าฟังก์ชัน θ เป็นฟังก์ชันชนิดใด

วิธีทำ สมมติให้ $a, b \in \mathbb{R}$
จะได้ว่า $\theta(a + b) = 2^{a+b} = (2^a)(2^b) = \theta(a)\theta(b)$
จึงสรุปได้ว่า $\theta \in \text{Hom}(\mathbb{R}, \mathbb{R}^+)$
ถ้าสมมติให้ $y \in \mathbb{R}^+$
จะได้ว่ามี $x = \log_2 y \in \mathbb{R}$ ที่ทำให้ $\theta(x) = \theta(\log_2 y) = 2^{\log_2 y} = y$
ดังนั้น θ เป็นฟังก์ชันทั่วถึง
นั่นคือ $\theta \in \text{Epi}(\mathbb{R}, \mathbb{R}^+)$
ต่อไปสมมติให้ $\theta(a) = \theta(b)$
จะได้ว่า $2^a = 2^b$ ดังนั้น $a = b$
นั่นคือ θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น $\theta \in \text{Mon}(\mathbb{R}, \mathbb{R}^+)$

ตัวอย่างที่ 6.4 กำหนดฟังก์ชัน $\theta : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ ดังนี้ $\theta(a) = 3a$ สำหรับทุก $a \in G$ จงพิจารณาว่าฟังก์ชัน θ เป็นฟังก์ชันชนิดใด

วิธีทำ สมมติให้ $a, b \in \mathbb{Z}$
จะได้ว่า $\theta(a + b) = 3(a + b) = 3a + 3b = \theta(a) + \theta(b)$
นั่นคือ $\theta \in \text{End}(\mathbb{Z})$
ถ้าสมมติให้ $\theta(a) = \theta(b)$
จะได้ว่า $3a = 3b$ ดังนั้น $a = b$
นั่นคือ θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง
เพราะฉะนั้น $\theta \in \text{Mon}(\mathbb{Z}, \mathbb{Z})$

ถ้า θ เป็นโฮโมมอร์ฟิซึม แล้ว θ จะมีสมบัติดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 6.3 กำหนดให้ G และ G' เป็นกรุปที่มี e และ e' เป็นสมาชิกเอกลักษณ์ของ G และ G' ตามลำดับ ถ้า $\theta \in \text{Hom}(G, G')$ จะได้ว่า

1. $\theta(e) = e'$
2. $\theta(a^{-1}) = \theta(a)^{-1}$ สำหรับทุก $a \in G$
3. $\theta(a^k) = \theta(a)^k$ สำหรับทุก $a \in G$ และ $k \in \mathbb{Z}$
4. $\theta(G)$ เป็นกรุปย่อยของ G'

การพิสูจน์ กำหนดให้ $(G, \cdot)$ และ $(G', *)$ เป็นกรุปที่มี e และ e' เป็นสมาชิกเอกลักษณ์ของ G และ G' ตามลำดับ และ $\theta \in \text{Hom}(G, G')$

(1) สมมติให้ $a \in G$ พิจารณา
$\theta(a) * e' = \theta(a) = \theta(a \cdot e) = \theta(a) * \theta(e)$
เนื่องจาก G' มีสมบัติการตัดออก
ดังนั้น $e' = \theta(e)$

(2) สมมติให้ $a \in G$ เนื่องจาก

$$\theta(a^{-1}) * \theta(a) = \theta(a^{-1} \cdot a) = \theta(e) = e'$$

และ $$\theta(a) * \theta(a^{-1}) = \theta(a \cdot a^{-1}) = \theta(e) = e'$$

ดังนั้น $\theta(a^{-1})$ เป็นตัวผกผันของ $\theta(a)$
แต่ $\theta(a)^{-1}$ เป็นตัวผกผันของ $\theta(a)$ เช่นกัน
จึงสรุปได้ว่า $\theta(a^{-1}) = \theta(a)^{-1}$

(3) สมมติให้ $a \in G$ จะแบ่งการพิจารณาเป็น 3 กรณีดังนี้
กรณี $k \in \mathbb{N}$: กำหนดให้ $P(k)$ แทนข้อความ "$\theta(a^k) = \theta(a)^k$"
ถ้า $k = 1$ จะได้ $P(1)$ คือ ข้อความ $\theta(a^1) = \theta(a)^1$ ซึ่งเป็นจริง
ต่อไปให้ $P(m)$ เป็นจริง เมื่อ $m \in \mathbb{N}$
นั่นคือ $\theta(a^m) = \theta(a)^m$ ดังนั้น

$$\theta(a^{m+1}) = \theta(a^m \cdot a) = \theta(a^m) * \theta(a) = \theta(a)^m * \theta(a) = \theta(a)^{m+1}$$

เพราะฉะนั้น $P(m+1)$ เป็นจริง
โดยหลักการอุปนัยเชิงคณิตศาสตร์ ได้ว่า $\theta(a^k) = \theta(a)^k$ สำหรับทุก $k \in \mathbb{N}$

กรณี $k = 0$: $\theta(a^k) = \theta(a^0) = \theta(e) = e' = \theta(a)^0 = \theta(a)^k$

กรณี $k \in \mathbb{Z}^-$: จะได้ว่า $k = -m$ สำหรับบาง $m \in \mathbb{N}$ ทำให้ได้ว่า

$$\theta(a^k) = \theta(a^{-m}) = \theta((a^{-1})^m) = (\theta(a)^{-1})^m = \theta(a)^{-m} = \theta(a)^k$$

นั่นคือ $\theta(a^k) = \theta(a)^k$ สำหรับทุก $k \in \mathbb{Z}^-$
จากทั้ง 3 กรณี จึงสรุปได้ว่า $\theta(a^k) = \theta(a)^k$ สำหรับทุก $k \in \mathbb{Z}$

(4) เนื่องจาก $e' \in \theta(G)$
ดังนั้น $\theta(G) \neq \varnothing$
ต่อไปให้ $\theta(a), \theta(b) \in \theta(G)$
เพราะฉะนั้น $a, b \in G$
เนื่องจาก $a \cdot b \in G$ และ $\theta(a) * \theta(b) = \theta(a \cdot b)$
ดังนั้น $\theta(a) * \theta(b) \in \theta(G)$
สำหรับ $\theta(a) \in \theta(G)$ จะได้ว่า $\theta(a)^{-1}$ เป็นตัวผกผันของ $\theta(a)$
และจาก $a^{-1} \in G$ ดังนั้น $\theta(a)^{-1} = \theta(a^{-1}) \in \theta(G)$
สรุปได้ว่า $\theta(G) \leq G'$

วิธีหนึ่งที่ใช้ในการตรวจสอบความเป็นฟังก์ชันหนึ่งต่อหนึ่งของโฮโมมอร์ฟิซึม $\theta : G \to G'$ ทำได้ โดยพิจารณาเซตย่อยพิเศษของ G ที่เรียกว่าแก่นกลาง หรือเคอร์เนล (kernel) ของ θ ดังบทนิยามต่อไปนี้

บทนิยาม 6.4 กำหนดให้ G และ G' เป็นกรุปใด ๆ และ $\theta \in \text{Hom}(G, G')$ นิยาม

$$\ker(\theta) = \{g \in G \mid \theta(g) = e'\}$$

เมื่อ e' คือ สมาชิกเอกลักษณ์ของ G' จะเรียก $\ker(\theta)$ ว่าแก่นกลาง หรือเคอร์เนล (kernel) ของ θ

ข้อสังเกต เนื่องจาก $\theta(e) = e'$ เมื่อ e คือ สมาชิกเอกลักษณ์ของ G ดังนั้น $e \in \ker(\theta)$ นั่นคือ $\ker(\theta) \neq \varnothing$

ทฤษฎีบท 6.5 ถ้า G และ G' เป็นกรุปใด ๆ และ $\theta \in \text{Hom}(G, G')$ แล้ว

1. $\ker(\theta)$ เป็นกรุปย่อยปรกติของ G
2. θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อ $\ker(\theta) = \{e\}$

การพิสูจน์ กำหนดให้ G และ G' เป็นกรุปใด ๆ ที่มี e และ e' เป็นสมาชิกเอกลักษณ์ของ G และ G' ตามลำดับ และ $\theta \in$ Hom(G, G')

(1) สมมติให้ $K =$ ker(θ) จะแสดงว่า K เป็นกรุปย่อยปรกติของ G
ให้ $a, b \in K$ ดังนั้น $\theta(a) = e'$ และ $\theta(b) = e'$
พิจารณา $\theta(ab) = \theta(a)\theta(b) = e'e' = e'$
เพราะฉะนั้น $ab \in K$
นอกจากนี้ยังได้ว่า $\theta(a^{-1}) = \theta(a)^{-1} = (e')^{-1} = e'$
นั่นคือ $a^{-1} \in K$ จึงได้ว่า $K \leq G$
ต่อไปให้ $g \in G$ และ $gkg^{-1} \in gKg^{-1}$ เมื่อ $k \in K$ พิจารณา
$\theta(gkg^{-1}) = \theta(g)\theta(k)\theta(g^{-1}) = \theta(g)e'\theta(g^{-1}) = \theta(g)\theta(g^{-1}) = e'$
นั่นคือ $gkg^{-1} \in K$ จึงได้ว่า $gKg^{-1} \subseteq K$
เพราะฉะนั้น K เป็นกรุปย่อยปรกติของ G

(2) สมมติให้ θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง และ $a \in$ ker(θ)
ดังนั้น $\theta(a) = e'$ เนื่องจาก $\theta(e) = e'$ ดังนั้น $a = e$ นั่นคือ ker$(\theta) = \{e\}$
ในทางกลับกัน สมมติให้ ker$(\theta) = \{e\}$ และ $\theta(a) = \theta(b)$ เมื่อ $a, b \in G$
ดังนั้น $\theta(a)\theta(b)^{-1} = e'$
แต่เนื่องจาก $\theta(a)\theta(b)^{-1} = \theta(a)\theta(b^{-1}) = \theta(ab^{-1})$
เพราะฉะนั้น $\theta(ab^{-1}) = e'$ นั่นคือ $ab^{-1} \in$ ker$(\theta) = \{e\}$
ดังนั้น $ab^{-1} = e$ จึงได้ว่า $a = b$ นั่นคือ θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ไอโซโมมอร์ฟิซึม

บทนิยาม 6.6 กำหนดให้ G และ G' เป็นกรุปใด ๆ และ $\theta \in$ Hom(G, G') เรียก θ ว่าไอโซมอร์ฟิซึมหรือสมสัณฐาน (isomorphism) ก็ต่อเมื่อ θ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก G ทั่วถึง G' และเซตของไอโซมอร์ฟิซึมทั้งหมดจาก G ไป G' เขียนแทนด้วยสัญลักษณ์ Iso(G, G') และจะกล่าวว่า G ไอโซมอร์ฟิคกับ G' (G is isomorphic to G') ก็ต่อเมื่อ มีไอโซมอร์ฟิซึมจาก G ไป G' และใช้สัญลักษณ์ $G \cong G'$ แทนข้อความที่ว่า G ไอโซมอร์ฟิคกับ G' เรียกไอโซมอร์ฟิซึมจาก G ไป G ว่าออโตมอร์ฟิซึมหรืออัตสัณฐาน (automorphism) ของ G และเซตของออโตมอร์ฟิซึมทั้งหมดของ G เขียนแทนด้วยสัญลักษณ์ Aut(G)

ข้อสังเกต
1. Aut$(G) =$ Iso(G, G)
2. Aut$(G) \subseteq$ End(G)
3. Iso$(G, G') \subseteq$ Hom(G, G')
4. Iso$(G, G') =$ Mon$(G, G') \cap$ Epi(G, G')

หมายเหตุ กำหนดให้ G, G' และ G'' เป็นกรุปใด ๆ จะได้ว่า
1. เนื่องจากมีฟังก์ชันเอกลักษณ์ $i_G : G \xrightarrow[onto]{1-1} G$ โดยที่ $i_G \in$ End(G) ดังนั้น $G \cong G$
2. สมมติให้ $G \cong G'$ ดังนั้น จะมี $\theta \in$ Iso(G, G')

พิจารณาฟังก์ชัน $\theta^{-1} : G' \to G$
จะได้ว่า θ^{-1} เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก G' ทั่วถึง G
ถ้าสมมติให้ $b_1, b_2 \in G'$ เนื่องจาก θ เป็นฟังก์ชันทั่วถึง
จะได้ว่า $b_1 = \theta(a_1)$ และ $b_2 = \theta(a_2)$ สำหรับบาง $a_1, a_2 \in G$ ดังนั้น

$$\begin{aligned}
\theta^{-1}(b_1)\theta^{-1}(b_2) &= \theta^{-1}(\theta(a_1))\theta^{-1}(\theta(a_2)) \\
&= i_G(a_1)i_G(a_2) \ \text{(เนื่องจาก } \theta \text{ เป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง)} \\
&= a_1a_2 \\
&= i_G(a_1a_2) \\
&= \theta^{-1}(\theta(a_1a_2)) \\
&= \theta^{-1}(\theta(a_1)\theta(a_2)) \quad \text{(เนื่องจาก } \theta \in \mathsf{Hom}(G, G')) \\
&= \theta^{-1}(b_1b_2)
\end{aligned}$$

จึงได้ว่า $\theta^{-1} \in \mathsf{Hom}(G', G)$
ดังนั้น $\theta' \in \mathsf{Iso}(G', G)$ นั่นคือ $G' \cong G$

3. สมมติให้ $G \cong G'$ และ $G' \cong G''$
   จะได้ว่ามี $\theta \in \mathsf{Iso}(G, G')$ และ $\alpha \in \mathsf{Iso}(G', G'')$
   พิจารณาฟังก์ชัน $\alpha \circ \theta : G \longrightarrow G''$
   จะได้ว่า $\alpha \circ \theta$ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก G ทั่วถึง G''
   นอกจากนี้ยังได้ว่า สำหรับ $a_1, a_2 \in G$ จะได้ว่า

$$\begin{aligned}
(\alpha \circ \theta)(a_1)(\alpha \circ \theta)(a_2) &= (\alpha(\theta(a_1))(\alpha(\theta(a_2)) \\
&= (\alpha(\theta(a_1)(\theta(a_2)) \ \text{(เนื่องจาก } \alpha \in \mathsf{Hom}(G', G'')) \\
&= (\alpha(\theta(a_1a_2)) \ \text{(เนื่องจาก } \theta \in \mathsf{Hom}(G, G')) \\
&= (\alpha \circ \theta)(a_1a_2)
\end{aligned}$$

   จึงได้ว่า $\alpha \circ \theta \in \mathsf{Hom}(G, G'')$
   ดังนั้น $\alpha \circ \theta \in \mathsf{Iso}(G', G'')$ นั่นคือ $G \cong G''$
   จาก 1., 2. และ 3. สรุปได้ว่า $\cong$ เป็นความสัมพันธ์สมมูล

ในเรื่องไอโซมอร์ฟิคของกรุปนั้น มีตัวอย่างสำคัญที่ควรทราบดังทฤษฎีบทต่อไป

ทฤษฎีบท 6.7 ทุกกรุปวัฏจักรอนันต์จะไอโซมอร์ฟิคกับกรุป $(\mathbb{Z}, +)$ และทุกกรุปวัฏจักรจำกัดจะไอโซมอร์ฟิคกับกรุป $(\mathbb{Z}_n, +_n)$

การพิสูจน์ กำหนดให้ G เป็นกรุปวัฏจักรที่มี e เป็นสมาชิกเอกลักษณ์
ดังนั้น จะมี $g \in G$ ที่ทำให้ $G = \{g^n | n \in \mathbb{Z}\}$
จะแสดงว่า ทุกกรุปวัฏจักรที่เป็นกรุปอนันต์จะไอโซมอร์ฟิคกับกรุป $(\mathbb{Z}, +)$
โดยสมมติให้ G เป็นกรุปอนันต์ พิจารณาฟังก์ชัน $\theta : G \longrightarrow \mathbb{Z}$ ที่กำหนดโดย

$$\theta(g^k) = k \text{ สำหรับทุก } k \in \mathbb{Z}$$

กำหนดให้ $i, j \in \mathbb{Z}$ จะได้ว่า $g^i, g^j \in G$
เนื่องจาก G เป็นกรุปอนันต์ จึงได้ว่า $g^i = g^j$ ก็ต่อเมื่อ $i = j$
เพราะฉะนั้น θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง
สำหรับแต่ละ $j \in \mathbb{Z}$ จะมี $g^j \in G$ ที่ทำให้ $\theta(g^j) = j$
ดังนั้น θ เป็นฟังก์ชันทั่วถึง $\mathbb{Z}$
เนื่องจาก $\theta(g^i g^j) = \theta(g^{i+j}) = i + j = \theta(g^i) + \theta(g^j)$
ดังนั้น $\theta \in \mathsf{Hom}(G, \mathbb{Z})$
จึงสรุปได้ว่า $\theta \in \mathsf{Iso}(G, \mathbb{Z})$ นั่นคือ $G \cong \mathbb{Z}$
ต่อไปจะแสดงว่า ทุกกรุปวัฏจักรจำกัดไอโซมอร์ฟิคกับกรุป $(\mathbb{Z}_n, +_n)$
สมมติให้ G เป็นกรุปจำกัดที่มีอันดับ n
เนื่องจาก n เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้ $a^n = e$
จะได้ว่า $G = \{a^0, a, ..., a^{n-1}\}$
พิจารณาฟังก์ชัน $\theta : G \longrightarrow \mathbb{Z}_n$ ที่กำหนดโดย

$$\theta(a^k) = [k] \text{ สำหรับทุก } 0 \leq k \leq n-1$$

สมมติให้ $a^i, a^j \in G$ โดยที่ $\theta(a^i) = \theta(a^j)$
ดังนั้น $[i] = [j]$ ซึ่ง $0 \leq i \leq n-1$ และ $0 \leq j \leq n-1$
จะได้ว่า $i = j$ นั่นคือ $a^i = a^j$ จึงได้ว่า θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง
ถ้า $[k] \in \mathbb{Z}_n$ จะได้ว่า $0 \leq k \leq n-1$
เพราะฉะนั้น มี $a^k \in G$ ที่ทำให้ $\theta(a^k) = [k]$
นั่นคือ θ เป็นฟังก์ชันทั่วถึง
ต่อไปสมมติให้ $a^i, a^j \in G$
ถ้า $i + j < n$ แล้ว

$$\theta(a^i a^j) = \theta(a^{i+j}) = [i+j] = \theta(a^i) + \theta(a^j)$$

ถ้า $i + j \geq n$ จะได้ว่า

$$\begin{aligned}\theta(a^i a^j) = \theta(a^{i+j-n}) &= [i+j-n] \\ &= [i] + [j] + [-n] \\ &= [i] + [j] \\ &= \theta(a^i) + \theta(a^j)\end{aligned}$$

ดังนั้น $\theta \in \mathsf{Hom}(G, \mathbb{Z}_n)$ จึงสรุปได้ว่า $\theta \in \mathsf{Iso}(G, \mathbb{Z}_n)$ นั่นคือ $G \cong \mathbb{Z}_n$

ทฤษฎีบท 6.8 ทฤษฎีบทเคย์เลย์ (Cayley's Theorem)
กำหนดให้ G เป็นกรุปใด ๆ จะได้ว่า G ไอโซมอร์ฟิคกับบางกรุปย่อยของ

$$A(G) \text{ เมื่อ } A(G) = \{f \mid f : G \xrightarrow[onto]{1-1} G\}$$

การพิสูจน์ สำหรับแต่ละ $g \in G$ จะกำหนดฟังก์ชัน $f_g : G \longrightarrow G$ ดังนี้

$$f_g(x) = gx \text{ สำหรับทุก } x \in G$$

ต่อไปสมมติให้ $a \in G$
ถ้าให้ $b \in G$ แล้วจะมี $a^{-1}b \in G$ ที่ทำให้

$$f_a(a^{-1}b) = a(a^{-1}b) = (aa^{-1})b = eb = b$$

ดังนั้น f_a เป็นฟังก์ชันทั่วถึง G
สมมติให้ $f_a(x_1) = f_a(x_2)$ เมื่อ $x_1, x_2 \in G$
จะได้ว่า $ax_1 = ax_2$ นั่นคือ $x_1 = x_2$
จึงได้ว่า f_a เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น $f_a \in A(G)$
จึงสรุปได้ว่า $f_g \in A(G)$ สำหรับทุก $g \in G$
สมมติให้ $H = \{f_g \mid g \in G\}$ จะได้ว่า $H \subseteq A(G)$
พิจารณาฟังก์ชัน $\theta : G \longrightarrow A(G)$ ที่กำหนดโดย

$$\theta(g) = f_g \text{ สำหรับทุก } g \in G$$

เห็นได้ชัดว่า θ เป็นฟังก์ชันจาก G ทั่วถึง H นั่นคือ $\theta(G) = H$
ต่อไปสมมติให้ $e, g \in G$ จะได้ว่า สำหรับทุก $x \in G$

$$\begin{aligned} f_g(x) = f_{eg}(x) &= (eg)x = e(gx) \\ &= e(f_g(x)) = f_e(f_g(x)) = (f_e \circ f_g)(x) \end{aligned}$$

ในทำนองเดียวกัน จะได้ว่า $f_g(x) = (f_g \circ f_e)(x)$ สำหรับทุก $x \in G$
นั่นคือ $f_g = f_e \circ f_g = f_g \circ f_e$
เพราะฉะนั้น f_e เป็นสมาชิกเอกลักษณ์ของ $A(G)$
ต่อไปจะแสดงว่า θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง
ให้ $k \in \ker(\theta)$ จะได้ว่า $\theta(k) = f_e$
นั่นคือ $f_k = f_e$ ดังนั้น $f_e(e) = f_k(e)$
จึงได้ว่า $e = ee = ke = k$
นั่นคือ $\ker(\theta) = \{e\}$ ดังนั้น θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง
จึงสรุปได้ว่า $G \cong H$

หมายเหตุ เรียกกรุป H ในทฤษฎีบท 6.8 ว่าตัวแทนการเรียงสับเปลี่ยนของ G (the permutation representation of G)

ตัวอย่างที่ 6.5 กำหนดให้ $G = (\mathbb{Z}_3, +_3)$ จงหาตัวอย่างของตัวแทนการเรียงสับเปลี่ยนของกรุป G

วิธีทำ พิจารณา $A(G)$ คือกรุปการเรียงสับเปลี่ยนที่มีสมาชิก 6 ตัวดังนี้

$$\begin{array}{ccc} \begin{array}{r} [0] \longrightarrow [0] \\ e : [1] \longrightarrow [1] \\ [2] \longrightarrow [2] \end{array} & \begin{array}{r} [0] \longrightarrow [1] \\ \alpha : [1] \longrightarrow [0] \\ [2] \longrightarrow [2] \end{array} & \begin{array}{r} [0] \longrightarrow [1] \\ \beta : [1] \longrightarrow [2] \\ [2] \longrightarrow [0] \end{array} \\ \\ \begin{array}{r} [0] \longrightarrow [2] \\ \gamma : [1] \longrightarrow [1] \\ [2] \longrightarrow [0] \end{array} & \begin{array}{r} [0] \longrightarrow [0] \\ \delta : [1] \longrightarrow [2] \\ [2] \longrightarrow [1] \end{array} & \begin{array}{r} [0] \longrightarrow [2] \\ \theta : [1] \longrightarrow [0] \\ [2] \longrightarrow [1] \end{array} \end{array}$$

โดยทฤษฎีบทเคย์เลย์ จะได้ว่า $G \cong \{f_g \mid g \in G\}$
พิจารณาสมาชิกใน $\{f_g \mid g \in G\}$
จะได้ว่า $f_{[0]} = e, f_{[1]} = \beta$ และ $f_{[2]} = \theta$
นั่นคือ $G \cong \{e, \beta, \theta\}$
จึงได้ว่าตัวแทนการเรียงสับเปลี่ยนของ G คือ $\{e, \beta, \theta\}$

ทฤษฎีบทต่อไปนี้จะแสดงให้เห็นว่ามีโฮโมมอร์ฟิซึมจากกรุป G ทั่วถึงกรุปผลหารของ G เสมอ และเรียกโฮโมมอร์ฟิซึมดังกล่าวนี้ว่าโฮโมมอร์ฟิซึมธรรมชาติ (natural homomorphism)

ทฤษฎีบท 6.9 กำหนดให้ N เป็นกรุปย่อยปรกติของกรุป G และฟังก์ชัน $\theta : G \longrightarrow G/N$ กำหนดโดย

$$\theta(a) = Na \text{ สำหรับทุก } a \in G$$

จะได้ว่า $\theta \in \text{Epi}(G, G/N)$ โดยที่ $\ker(\theta) = N$

การพิสูจน์ กำหนดให้ N เป็นกรุปย่อยปรกติของกรุป G
ให้ฟังก์ชัน $\theta : G \longrightarrow G/N$ กำหนดโดย

$$\theta(a) = Na \text{ สำหรับทุก } a \in G$$

สมมติให้ $a, b \in G$ จะได้ว่า

$$\theta(ab) = N(ab) = (Na)(Nb) = \theta(a)\theta(b)$$

ดังนั้น $\theta \in \text{Hom}(G, G/N)$
สำหรับแต่ละ $Na \in G/N$ จะมี $a \in G$ ที่ทำให้ $\theta(a) = Na$
นั่นคือ θ เป็นฟังก์ชันทั่วถึง G/N
ดังนั้น $\theta \in \text{Epi}(G, G/N)$ นอกจากนี้ ยังได้อีกว่า

$$\begin{aligned} \ker(\theta) &= \{a \in G | \theta(a) = N\} \\ &= \{a \in G | Na = N\} \\ &= \{a \in G | a \in N\} \\ &= N \end{aligned}$$

กำหนดให้ G และ G' เป็นกรุปโดยแม้ว่ามี $\alpha \in \text{Epi}(G, G')$ จะได้ว่า ถ้า $\ker(\alpha) \neq \{e\}$

ก็ไม่อาจสรุปได้ว่า $G \cong G'$ อย่างไรก็ตามโดยอาศัยแนวคิดของทฤษฎีบท 6.9 จะพิสูจน์ได้ว่ากรุปผลหาร $G/\ \text{ker}(\alpha) \cong G'$ ซึ่งเป็นสมบัติสำคัญอันหนึ่งทางพีชคณิต ดังกล่าวในทฤษฎีบทต่อไปนี้

ทฤษฎีบท 6.10 ทฤษฎีบทหลักมูลโฮโมมอร์ฟิซึม (The funamental homomorphism theorem)
กำหนดให้ G และ G' เป็นกรุป โดยมี $\alpha \in \text{Epi}(G, G')$ และ $\text{ker}(\alpha) = K$ จะได้ว่า $G/K \cong G'$

การพิสูจน์ กำหนดให้ G และ G' เป็นกรุป e' เป็นสมาชิกเอกลักษณ์ของ G' และ
$\alpha \in \text{Epi}(G, G')$ สมมติให้ $K = \text{ker}(\alpha)$
โดยทฤษฎีบท 6.5 จะได้ว่า K เป็นกรุปย่อยปรกติของ G
โดยทฤษฎีบทเคย์เลย์ ทำให้ได้ว่าฟังก์ชัน $\theta : G \longrightarrow G/K$ ที่กำหนดโดย

$$\theta(a) = Ka \text{ สำหรับทุก } a \in G$$

เป็นโฮโมมอร์ฟิซึมจาก G ทั่วถึง G/N พิจารณาแผนภาพต่อไปนี้

กำหนดฟังก์ชัน $\beta : G/K \longrightarrow G'$ โดยที่

$$\beta(Ka) = \alpha(a) \text{ สำหรับทุก } Ka \in G/N$$

จะแสดงว่า β เป็นฟังก์ชัน
สมมติให้ $Ka, Kb \in G/N$ และ $Ka = Kb$
เนื่องจาก $a = ea \in Ka$ ดังนั้น $a \in Kb$
และจะมี $k \in K$ ที่ทำให้ $a = kb$ เพราะฉะนั้น

$$\beta(Ka) = \alpha(a) = \alpha(kb) = \alpha(k)\alpha(b) = e'\alpha(b) = \alpha(b) = \beta(Kb)$$

ดังนั้น β เป็นฟังก์ชัน และเนื่องจาก α เป็นฟังก์ชันทั่วถึง G'
ดังนั้น ถ้า $g' \in G'$ แล้วจะมี $g \in G$ ที่ทำให้ $\alpha(g) = g'$
ทำให้ได้ว่ามี $Kg \in G/K$ ที่ทำให้ $\beta(Kg) = \alpha(g) = g'$
จึงได้ว่า β เป็นฟังก์ชันทั่วถึง G'
ต่อไปจะแสดงว่า β เป็นโฮโมมอร์ฟิซึม สมมติให้ $Kx, Ky \in G/K$

เนื่องจาก $\beta((Kx)(Ky)) = \beta(K(xy)) = \alpha(xy)$
$= \alpha(x)\alpha(y) = \beta(Kx)\beta(Ky)$
ดังนั้น $\beta \in \mathrm{Hom}(G/N, G')$
ต่อไปจะแสดงว่า β เป็นฟังก์ชันหนึ่งต่อหนึ่ง
ให้ $Kz \in \ker(\beta)$ ดังนั้น $\beta(Kz) = e'$
นั่นคือ $\alpha(z) = e'$
จึงได้ว่า $z \in \ker(\alpha) = K$ เพราะฉะนั้น $Kz = K$
แต่ K เป็นสมาชิกเอกลักษณ์ของกรุป G/K ซึ่ง $K \in \ker(\beta)$
ดังนั้น $\ker(\beta) = \{K\}$ และจะได้ว่า β เป็นฟังก์ชันหนึ่งต่อหนึ่ง
จึงสรุปได้ว่า $\beta \in \mathrm{Iso}(G/K, G')$
นั่นคือ $G/K \cong G'$

สรุปท้ายบท

จากเนื้อหาที่กล่าวมาข้างต้นพบว่า การสร้างฟังก์ชันทั้งโฮโมมอร์ฟิซึมและไอโซมอร์ฟิซึม ทำให้เกิดทฤษฎีที่สำคัญ ทั้งทฤษฎีเคเลย์ ซึ่งสามารถบอกได้ว่า ไม่ว่าจะเลือกกรุปใดขึ้นมา กรุปนั้นจะต้องไอโซมอร์ฟิคกับบางกรุปย่อยของ $A(G)$ และทฤษฎีบทหลักมูลโฮโมมอร์ฟิซึม ซึ่งนับเป็นหนึ่งในทฤษฎีของพีชคณิตนามธรรมที่มีประโยชน์และถูกนำไปต่อยอดทางทฤษฎีอย่างกว้างขวาง รวมถึงเป็นแนวทาง และต้นแบบเมื่อมีการขยายแนวคิดเชิงทฤษฎี เพื่อทำให้เกิดประโยชน์ในวงกว้างต่อไป