# ทฤษฎีกรุปเบื้องต้น

# INTRODUCTION TO GROUP THEORY

โดย ศาสตราจารย์ ดร. ฉวีวรรณ รัตนประเสริฐ
ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

สำหรับวรกฤตน์ เพื่อความก้าวหน้าค่ะ
ฉวีวรรณ รัตนประเสริฐ
20 ตุลาคม 2558



พิมพ์ครั้งที่ 1 : 2553 จำนวน 206 หน้า
พิมพ์ที่ โรงพิมพ์มหาวิทยาลัยศิลปากร

โครงการตำรา คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร

# คำนำ

## INTRODUCTION

การศึกษาวิชาพีชคณิตนามธรรมของนักศึกษาวิชาเอกคณิตศาสตร์ในระดับบัณฑิตศึกษา นักศึกษาจะพบกับการศึกษาเชิงนามธรรมล้วนๆ เป็นครั้งแรก แม้ว่าจะศึกษากับโครงสร้างที่เรียบง่ายที่สุดอย่าง "กรุป (group)" ก็ตาม นักศึกษาส่วนใหญ่มักจะไม่คุ้นเคยและไม่เข้าใจเจตคติของวิชา ทำให้เกิดปัญหาในระหว่างเรียนอยู่เสมอๆ ผู้เขียนได้เคยสอนรายวิชานี้มาหลายปี จึงค่อนข้างเข้าใจปัญหาของนักศึกษา ทำให้เกิดแรงบันดาลใจที่จะเขียนหนังสือเรื่อง "ทฤษฎีกรุปเบื้องต้น" เล่มนี้ขึ้น โดยมุ่งเน้นเฉพาะเรื่อง "กรุป" เพียงเรื่องเดียว และเขียนแบบให้รายละเอียดของความเป็นมา ทำให้นักศึกษาเข้าใจกระบวนวิธีคิดในวิชาคณิตศาสตร์แขนง "พีชคณิต" เพื่อให้การ ศึกษาเชิงนามธรรมกับโครงสร้างอื่นๆ เข้าใจได้ง่ายขึ้น

อนึ่ง ในการศึกษาวิชาคณิตศาสตร์ในแขนงใดก็ตาม นักศึกษาต้องมีความรู้มูลฐานที่จำเป็นต่อการศึกษาวิชาคณิตศาสตร์โดยทั่วไป ได้แก่ เซต ผลแบ่งกั้นและความสัมพันธ์สมมูล ฟังก์ชันและการเรียงสับเปลี่ยน โดยเฉพาะเรื่องการดำเนินการและสมบัติของการดำเนินการ ผู้เขียนจึงสรุปเรื่องราวเหล่านี้ไว้เป็นบทที่ 1

มโนมติของวิชาพีชคณิตนามธรรมเป็นการขยายแนวความคิดจากสมบัติของระบบจำนวน โดยเฉพาะระบบจำนวนเต็ม ตัวอย่างที่สำคัญที่มักยกประกอบการศึกษาจึงเป็นตัวอย่างที่เกี่ยวกับระบบจำนวน ในบทที่ 2 ผู้เขียนจึงรวบรวมความรู้มูลฐานและทฤษฎีบทสำคัญๆ ในทฤษฎีจำนวน

ในบทที่ 3 ได้กล่าวถึงที่มาและความสำคัญที่จะต้องศึกษาทฤษฎีกรุป ให้นิยามกรุปเชิงนามธรรมและกรุปย่อย พร้อมตัวอย่างกรุปและกรุปย่อย และศึกษาสมบัติมูลฐานของกรุป

ในบทที่ 4 เราศึกษากรุปบนเซตของการเรียงสับเปลี่ยนบนเซตจำกัดและเซตอนันต์ซึ่งเป็นต้นกำเนิดของกรุป และเรารู้จักกันแพร่หลายในชื่อ กรุปสมมาตร กรุปการสมมาตร และกรุปไดฮิดรัล นอกจากนี้กรุปต่างๆ เหล่านี้ยังจะมีบทบาทสำคัญในบทต่อๆ ไปด้วย

ในบทที่ 5 เราจะย้อนรอยแนวคิดของของท่าน โชแซฟ ลุยส์ ลากรองจ์ (Joseph Louis Lagrange) นักคณิตศาสตร์ชาวฝรั่งเศส และพิสูจน์ทฤษฎีบทของลากรองจ์ซึ่งแสดงความสัมพันธ์ของอันดับของกรุปจำกัด อันดับของกรุปย่อยและอันดับของสมาชิกในกรุป แสดงผลพลอยได้ที่เป็นต้นกำเนิดของวิชาเกี่ยวกับการนับ การสร้างกรุปผลหาร ตัวอย่างและการประยุกต์

ในบทที่ 6 เราศึกษามโนมติของการสมสัณฐานจากความเข้าใจได้ของมนุษย์ไปสู่ความหมายของสมสัณฐานในคณิตศาสตร์ กล่าวถึงการสมสัณฐานกันและไม่สมสัณฐานกันของกรุป

โดยยกตัวอย่างที่สำคัญและรู้จักกันแพร่หลาย พิสูจน์ทฤษฎีบทของเคย์เลย์ซึ่งเป็นทฤษฎีบทการแทนกรุปด้วยกรุปการสมมาตร ทำให้เห็นว่า แม้ว่าเราจะนิยามกรุปในเชิงนามธรรมสักเพียงใด กรุปเหล่านั้นก็คือกรุปของวิธีเรียงสับเปลี่ยนที่เราคุ้นเคยกันเป็นอย่างดีแล้วนั่นเอง และยังทำให้เราสามารถจำแนก (ภายใต้การเป็นสมสัณฐาน) กรุปวัฏจักรและกรุปย่อยวัฏจักร ตลอดจนเห็นความสัมพันธ์ของกรุปย่อยวัฏจักรและอันดับของสมาชิกของกรุป

ในบทที่ 7 เราศึกษาการส่งระหว่างกรุปซึ่งยืนยงโครงสร้าง แต่ไม่จำเป็นต้องเป็นสมสัณฐานซึ่งเราจะเรียกการส่งในลักษณะเช่นนี้ว่า "สาทิสสัณฐาน" ศึกษาสมบัติมูลฐานของสาทิสสัณฐาน สมบัติซึ่งยืนยงภายใต้สาทิสสัณฐาน กรุปย่อยปรกติ ส่วนกลาง และพิสูจน์ทฤษฎีบทมูลฐานของสาทิสสัณฐานซึ่งอาจถือได้ว่าเป็นหัวใจของการศึกษาพีชคณิตนามธรรม

ในบทที่ 8 ซึ่งเป็นบทสุดท้าย เราศึกษาโครงสร้างของกรุปโดยผ่านทางกรุปผลคูณตรงซึ่งเป็นวิธีการศึกษาโครงสร้างเชิงพีชคณิตอีกวิธีหนึ่งซึ่งแตกต่างจากที่ศึกษามาในบทก่อนๆ กรุปผลคูณตรงที่เราจะศึกษาเป็นกรุปที่สร้างขึ้นในสองลักษณะ อย่างหนึ่งเป็นการสร้างจากกรุปย่อยของกรุปในลักษณะแบบเดียวกันกับการกระจายจำนวนเต็มออกในรูปผลคูณของตัวประกอบหรือตัวหารของจำนวนนั้น ทำให้เราเห็นโครงสร้างของกรุปได้ง่ายขึ้น อย่างที่สองเป็นการสร้างจากผลคูณคาร์ทีเซียนของกรุป อย่างไรก็ตามเราจะแสดงการพิสูจน์ว่ากรุปที่ได้จากการสร้างทั้งสองแบบนั้นสมสัณฐานกัน

สำหรับคำศัพท์เทคนิค ผู้เขียนได้แปลเป็นภาษาไทยทั้งหมดโดยยึดพจนานุกรมศัพท์คณิตศาสตร์ ฉบับราชบัณฑิตยสถานเป็นหลัก โดยวงเล็บศัพท์ภาษาอังกฤษดั้งเดิมไว้ด้วย นอกจากนี้ยังรวบรวมศัพท์เทคนิคทั้งหมดไว้ในบัญชีศัพท์ท้ายเล่ม

ผู้เขียนหวังเป็นอย่างยิ่งว่า หนังสือกึ่งตำราเล่มนี้ จะมีประโยชน์สำหรับผู้เริ่มต้นศึกษาวิชาพีชคณิตนามธรรม ประโยชน์ใดๆ ที่เกิดขึ้นจากความรู้ของหนังสือเล่มนี้ผู้เขียนขอน้อมรำลึกในพระคุณของอาจารย์ที่ได้ประสิทธิ์ประสาทความรู้ให้เสมอมา ส่วนข้อบกพร่องที่ท่านพบ ผู้เขียนขอน้อมรับในความผิดพลาดนั้นไว้

ผู้เขียนขอขอบคุณ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร ที่ให้ทุนสนับสนุนการเขียนตำราจากกองทุนส่งเสริมและพัฒนาคณะวิทยาศาสตร์ เพื่อส่งเสริมให้คณาจารย์เขียนตำราที่มีคุณภาพ ขอขอบคุณ คุณฐกร ธรรมประทีป ที่ได้ช่วยวาดรูปสวยๆ ในหนังสือเล่มนี้

ศาสตราจารย์ ดร. ฉวีวรรณ รัตนประเสริฐ

มิถุนายน 2553

# สารบัญ

# บทที่ 1
# ความรู้พื้นฐาน
# BASIC CONCEPTS

ในบทนี้ จะทบทวนความรู้มูลฐานที่จำเป็นต่อการศึกษาวิชาคณิตศาสตร์ทั่วไป โดยเฉพาะวิชาพีชคณิตนามธรรมซึ่งได้แก่ เซต ผลแบ่งกั้น ความสัมพันธ์สมมูล ฟังก์ชัน วิธีเรียงสับเปลี่ยนและการดำเนินการ โดยขอกล่าวสรุปแต่ละเรื่องพอเป็นสังเขป

## 1.1 เซต

ในชีวิตประจำวันเราเรียกการรวมกันอยู่ของสิ่งต่างๆ ว่า กอง หมู่ ฝูง กลุ่ม ตัวอย่างเช่นกองหนังสือ ฝูงนก ฯลฯ ในทางคณิตศาสตร์ใช้คำว่า "*เซต (set)*" แทนการรวมกันอยู่ของสิ่งต่างๆ ดังกล่าว เช่นเซตของจำนวนเต็มบวก เซตของวันในหนึ่งสัปดาห์ เป็นต้น และเรียกสิ่งที่อยู่ภายในเซตว่า "*สมาชิกของเซต (an element of a set)*" ตัวอย่างเช่นสมาชิกของเซตของจำนวนเต็มซึ่งมีเป็นจำนวนอนันต์ได้แก่ . . ,-3, -2, -1, 0, 1, 2, 3, . . . เป็นต้น โดยถือว่า "เซต" และ "สมาชิกของเซต" เป็นคำอนิยาม นั่นคือคำที่ไม่ให้คำจำกัดความแต่เข้าใจได้ตรงกัน โดยทั่วไปนิยมใช้อักษรภาษาอังกฤษตัวพิมพ์ใหญ่ A, B, C, . . . แทนเซตและแทนสมาชิกของเซตด้วยอักษรภาษาอังกฤษตัวพิมพ์เล็ก a, b, c, . . . เป็นต้น

ถ้า x เป็นสมาชิกของเซต A จะเขียนแทนความหมายนี้ด้วยสัญลักษณ์ "$x \in A$" และในทำนองกลับกันถ้า x ไม่เป็นสมาชิกของ A หรือไม่อยู่ใน A จะเขียนแทนด้วยสัญลักษณ์ "$x \notin A$"

เซตๆ หนึ่งจะประกอบด้วยสมาชิกใดก็ได้ แต่ถ้ากล่าวถึงเซตหนึ่งเช่น เซต A และสิ่งหนึ่งที่เรียกว่า a แล้วข้อความ "$a \in A$" และ "$a \notin A$" เป็นจริงเพียงข้อความเดียวเท่านั้น เราเรียกเซต A เช่นนี้ว่า *เซตกำหนดแจ่มชัด (well defined set)* ตัวอย่างเช่นถ้า A เป็นเซตของจำนวนเต็มคู่ แล้วจะทราบว่า $0 \in A$, $6 \in A$, $1 \notin A$ และ $7 \notin A$ เป็นต้น ดังนั้น A เป็นเซตที่กำหนดแจ่มชัด แต่ถ้าให้ B เป็นเซตของนักวิทยาศาสตร์ยอดเยี่ยมที่สุดของโลก 10 ท่านแล้ว B ไม่เป็นเซตกำหนดแจ่มชัดเพราะไม่มีกฎเกณฑ์กำหนดความเป็นนักวิทยาศาสตร์ยอดเยี่ยม จึงไม่สามารถบอกได้ว่านักวิทยาศาสตร์ท่านใดบ้างอยู่ในเซต B

มีวิธีการเขียนหรือกำหนดเซตอย่างง่ายๆ 3 วิธีได้แก่

1. บรรยายลักษณะของสมาชิกในเซต เช่นเซตของจำนวนเต็มบวก เป็นต้น

2. เขียนเซตแบบแจกแจงสมาชิกทุกตัวในเซต วิธีนี้จะเขียนสมาชิกของเซตทุกตัวลงในวงเล็บปีกกาและใช้เครื่องหมายจุลภาค " , " คั่นระหว่างสมาชิกแต่ละตัว เช่น

   {a, b, c}

   {อาทิตย์, จันทร์, อังคาร, พุธ, พฤหัสบดี, ศุกร์, เสาร์}

   {2, 4, 6, 8, 10}

   เป็นต้น

3. เขียนเซตแบบกำหนดเงื่อนไขหรือสมบัติของสมาชิกในเซต ดังนี้

   { x | x มีสมบัติ P }

   ตัวอย่างเช่น { x | x เป็นจำนวนเต็มคู่} ซึ่งจะหมายถึงเซต { . . . , -4, -2, 0, 2, 4, 6, 8, . . .}

   หรือ {2, 4, 6, 8, . . . ,100} = { x | x เป็นจำนวนเต็มคู่และ $2 \leq x \leq 100$} เป็นต้น

พิจารณาเซตแต่ละเซต อาจพบว่าสมาชิกทุกตัวของเซตหนึ่งอาจเป็นสมาชิกของเซตอื่นอีกเซตหนึ่งได้เช่นสมาชิกทุกตัวของเซตของจำนวนเต็มบวกเป็นสมาชิกของเซตของจำนวนเต็ม ดังนั้นถ้า A และ B เป็นเซตและแต่ละสมาชิกของ A เป็นสมาชิกของ B จะกล่าวว่า A เป็น *เซตย่อย (subset)* ของ B และเขียนแทนด้วยสัญลักษณ์

$$A \subseteq B \text{ หรือ } B \supseteq A$$

สังเกตว่า $A \subseteq B$ ได้รวมกรณีที่ A = B ไว้ด้วยนั่นคือ A และ B เป็นเซตที่มีสมาชิกชุดเดียวกัน และโดยความเป็นจริงแล้ว

$$A = B \text{ ก็ต่อเมื่อ } A \subseteq B \text{ และ } B \subseteq A$$

แต่ถ้า $A \subseteq B$ และ $A \neq B$ จะกล่าวว่า A เป็น *เซตย่อยแท้ (proper subset)* ของ B ซึ่งเขียนแทนด้วยสัญลักษณ์

$$A \subset B \text{ หรือ } B \supset A$$

จากความหมายของ "A เป็นเซตย่อยของ B" จะได้ข้อความสมมูลกัน 3 ข้อความต่อไปนี้คือ

1. $A \subseteq B$
2. ถ้า $x \in A$ แล้ว $x \in B$
3. ถ้า $x \notin B$ แล้ว $x \notin A$

ขอให้สังเกตว่าข้อความ 3 เป็นข้อความแย้งสลับที่ของข้อความ 2 ซึ่งในบางครั้งการพิสูจน์ $A \subseteq B$ โดยการพิสูจน์ข้อความ 3 จะง่ายกว่าการพิสูจน์ข้อความ 2

สำหรับกรณีเซต A ไม่เป็นเซตย่อยของเซต B จะเขียนแทนด้วยสัญลักษณ์

$A \not\subset B$

ซึ่งเป็นจริง ก็ต่อเมื่อ มีสมาชิกอย่างน้อยหนึ่งตัวใน A ที่ไม่เป็นสมาชิกของ B และการกล่าวว่ามีสมาชิกในเซตหนึ่งที่ไม่เป็นสมาชิกของอีกเซตหนึ่งก็คือการกล่าวว่าเซตทั้งสองไม่เป็นเซตเดียวกัน ดังนั้นถ้า A เป็นเซตย่อยแท้ของ B จึงหมายความว่า

(ก) ถ้า $x \in A$ แล้ว $x \in B$ และ (ข) มี $u \in B$ ซึ่ง $u \notin A$

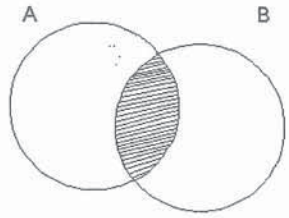
สำหรับเซตที่ไม่มีสมาชิกจะเรียกว่า *เซตว่าง (empty set)* และเขียนแทนด้วยสัญลักษณ์ $\phi$ หรือ { } ดังนั้นข้อความ "$x \in \phi$" จึงเป็นเท็จเสมอซึ่งทำให้ข้อความ "$x \in \phi$ และ $x \notin A$" เป็นเท็จด้วยซึ่งข้อความ "$x \in \phi$ และ $x \notin A$" เป็นนิเสธของข้อความ 3 ข้างต้น เพราะฉะนั้นข้อความ "$\phi \subseteq A$ สำหรับทุกๆ เซต A" เป็นจริง

เซตของเซตย่อยทั้งหมดของเซต A เรียกว่า *เซตกำลัง (power set)* ของ A ซึ่งเขียนแทนด้วยสัญลักษณ์ P(A) หรือ $2^A$ นั่นคือ

$$2^A = P(A) = \{x \mid x \subseteq A\}$$

ตัวอย่างเช่นถ้า A = {a, b} แล้ว P(A) = {$\phi$, {a}, {b}, {a, b} } เป็นต้น

เราใช้สัญลักษณ์ |A| แทนขนาด (cardinality) ของเซต A และถ้า A เป็น *เซตจำกัด (finite set)* นั่นคือเป็นเซตที่มีจำนวนสมาชิกเท่ากับศูนย์หรือจำนวนเต็มบวกตัวหนึ่งแล้ว |A| ก็คือจำนวนสมาชิกของ A และในกรณีเช่นนี้ $|P(A)| = 2^{|A|}$ ส่วนเซตที่ไม่เป็นเซตจำกัดจะเรียกว่า *เซตอนันต์ (infinite set)*




รูป 1.1.1

ถ้า A และ B เป็นเซตแล้ว *ส่วนร่วม (intersection)* ของ A กับ B คือเซตที่มีสมาชิกเป็นสมาชิกส่วนร่วมของ A และของ B จะใช้สัญลักษณ์แทนส่วนร่วมของ A กับ B ด้วย $A \cap B$ นั่นคือ

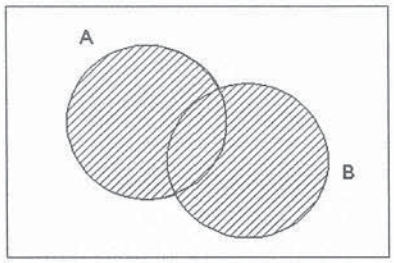
$$A \cap B = \{x \mid x \in A \text{ และ } x \in B\}$$

โดยมีแผนภาพแทนเซตนี้ดังส่วนที่แรเงาในรูป 1.1.1

*ส่วนรวม (union)* ของเซต A และเซต B คือเซตที่เป็นการรวมกันอยู่ของสมาชิกของ A กับของ B ซึ่งเขียนแทนด้วยสัญลักษณ์ $A \cup B$ นั่นคือ

$$A \cup B = \{x \mid x \in A \text{ หรือ } x \in B\}$$

โดยมีแผนภาพแทนเซตนี้ดังส่วนที่แรเงาในรูป 1.1.2




**รูป** 1.1.2

เราเรียกแผนภาพดังเช่นรูป 1.1.1 และรูป 1.1.2 ว่า *แผนภาพของเวนน์ (Venn diagram)*

1.1.1 **ตัวอย่าง** ให้ $S = \{a, b, c\}$, $T = \{c, d, e\}$ และ $U = \{d, e\}$ แล้ว $a \in S$, $a \notin T$, $S \not\subseteq T$, $U \subseteq T$, $S \cap T = T \cap S = \{c\}$ และ $S \cup T = T \cup S = \{a, b, c, d, e\}$ ❍

สำหรับสมบัติที่สำคัญของส่วนร่วมและส่วนรวม จะกล่าวสรุปใน 2 ทฤษฎีบทต่อไปนี้โดยไม่พิสูจน์และผู้อ่านอาจพิสูจน์ได้เองอย่างง่ายๆ โดยใช้แผนภาพของเวนน์ จึงขอละไว้เป็นแบบฝึกหัด

1.1.2 **ทฤษฎีบท** ให้ A, Bและ C เป็นเซต แล้ว

1. $A \cap A = A = A \cup A$ และ $(A \cup B) \cap A = A = (A \cap B) \cup A$
2. $A \cap B = B \cap A$ และ $A \cup B = B \cup A$
3. $A \cap B \subseteq A$, $B \subseteq A \cup B$
4. ถ้า $A \subseteq B$ แล้ว $A \cap B = A$ และ $A \cup B = B$
5. $A \cap (B \cap C) = (A \cap B) \cap C$
6. $A \cup (B \cup C) = (A \cup B) \cup C$
7. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
8. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ❐

1.1.3 **ทฤษฎีบท** ถ้า A และ B เป็นเซตจำกัด แล้ว $|A \cup B| = |A| + |B| - |A \cap B|$ ❐

เราอาจพบว่าส่วนร่วมของเซตสองเซตอาจเป็นเซตว่างได้ ดังเช่นในตัวอย่าง 1.1.1 จะเห็นว่า $S \cap U = \phi$ และสำหรับเซตสองเซตใดที่มีส่วนร่วมเป็นเซตว่าง จะเรียกเซตทั้งสองนั้นว่า *เซตต่างสมาชิก (disjoint sets)* และถ้า A และ B เป็นเซตจำกัดและเป็นเซตต่างสมาชิกกัน แล้วเห็นได้ชัดว่า $|A \cup B| = |A| + |B|$

ในการประยุกต์ทฤษฎีของเซต จะเห็นว่าเซตทั้งหลายที่กำลังพิจารณากันอยู่นั้นเป็นเซตย่อยของเซตๆ หนึ่งเสมอซึ่งเราเรียกเซตดังกล่าวนั้นว่า *เอกภพ (universe)* หรือ *เอกภพสัมพัทธ์ (relative universe)* ตัวอย่างเช่นสำหรับจำนวนเต็ม $n \geq 2$ นิยามให้ $P_n = \{x^n \mid x$ เป็นจำนวนเต็ม $\}$ แล้ว $P_n$ เป็นเซตของจำนวนเต็ม สำหรับแต่ละ $n \geq 2$ ดังนั้นในกรณีนี้เซตของจำนวนเต็มทั้งหมดซึ่งนิยมเขียนแทนด้วยสัญลักษณ์ Z เป็นเอกภพสัมพัทธ์ นอกจากนี้จะเห็นว่าส่วนร่วมและส่วนรวมของเซตทั้งหลายที่เป็นเซตย่อยของเอกภพสัมพัทธ์จะเป็นเซตย่อยของเอกภพสัมพัทธ์ด้วย

เพื่อความสะดวกในการกล่าวถึงต่อไป จะใช้สัญลักษณ์ต่อไปนี้แทนเซตของจำนวนต่างๆ

| | | |
|---|---|---|
| N | แทน | เซตของจำนวนธรรมชาติหรือก็คือจำนวนนับทั้งหมด |
| Z | แทน | เซตของจำนวนเต็มทั้งหมด |
| Q | แทน | เซตของจำนวนตรรกยะทั้งหมด |
| R | แทน | เซตของจำนวนจริงทั้งหมด |
| C | แทน | เซตของจำนวนเชิงซ้อนทั้งหมด |

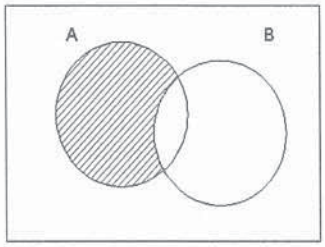
สมมติว่า U เป็นเอกภพสัมพัทธ์และ $A \subseteq U$ ในบางครั้งเราอาจสนใจสมาชิกที่ไม่อยู่ใน A เช่น ถ้า U = R และ A = Q แล้วเซตของสมาชิกที่ไม่อยู่ใน A ก็คือเซตของจำนวนอตรรกยะ เราเรียกเซตของสมาชิกที่อยู่ใน U แต่ไม่อยู่ใน A ว่า *เซตเติมเต็ม (complement)* ของ A และเขียนแทนด้วยสัญลักษณ์ $A^c$ หรือ $U - A$ หรือ $A'$ นั่นคือ

$$U - A = \{x \mid x \in U \text{ และ } x \notin A\}$$

โดยการนิยามในลักษณะเดียวกับ $U - A$ ถ้า A และ B เป็นเซตย่อยของ U จะนิยามเซต

$$A - B = \{x \mid x \in A \text{ และ } x \notin B\}$$

และเรียกว่า *เซตผลต่าง (difference set)* ของ A และ B โดยมีแผนภาพแทนเซตนี้ ดังส่วนที่แรเงาในรูป 1.1.3 และขอให้สังเกตจากนิยามของเซต $A \cap B$ และ $A - B$ ว่า $A - B = A \cap B'$




รูป 1.1.3

1.1.4 **ทฤษฎีบท** ให้ U แทนเอกภพสัมพัทธ์ A และ B เป็นเซตย่อยของ U แล้ว

1. $A \cup U = U$ และ $A \cap U = A$
2. $A \cup \phi = A$ และ $A \cap \phi = \phi$
3. $A \cup A' = U$ และ $A \cap A' = \phi$
4. $U' = \phi$ และ $\phi' = U$
5. $(A')' = A$
6. กฎเดอมอร์แกน(de Morgan's Law) :

   $(A \cup B)' = A' \cap B'$ และ $(A \cup B)' = A' \cup B'$ ❐

ส่วนร่วมและส่วนรวมที่กล่าวมาข้างต้น เป็นการนิยามส่วนร่วมและส่วนรวมของเซตสองเซต และหากเรามีเซตมากกว่าสองเซตเช่น A, B และ C และต้องการหาส่วนรวมของเซตทั้งสาม เราจะต้องเริ่มต้นด้วยการหาส่วนรวม $A \cup B$ หรือ $B \cup C$ หรือ $A \cup C$ ก่อนแล้วจึงนำเซตผลลัพธ์ไปหาส่วนรวมกับเซตที่เหลือ ผลลัพธ์จึงอาจเป็น $(A \cup B) \cup C$ หรือ $A \cup (B \cup C)$ หรือ $B \cup (A \cup C)$ อย่างไรก็ตามผลของทฤษฎีบท 1.1.2 ข้อ 6 ทำให้ทราบว่าเซตผลลัพธ์เหล่านี้เป็นเซตเดียวกัน นอกจากนี้หากเรามีหมู่ของเซต เราก็อาจขยายผลของทฤษฎีบท 1.1.2 ข้อ 6 กล่าวถึงส่วนร่วมและส่วนรวมของเซตในหมู่ของเซตนั้นโดยไม่ต้องคำนึงว่าจะต้องหาส่วนร่วมหรือส่วนรวมของเซตคู่ใดก่อน ในตอนท้ายของหัวข้อนี้ จึงจะขอให้นิยามส่วนร่วมและส่วนรวมของหมู่ของเซต

ให้ $I$ และ $\mathcal{A}$ เป็นเซต ถ้า $I$ ไม่ใช่เซตว่างและแต่ละ $A \in \mathcal{A}$ กำหนดให้มี $i \in I$ ซึ่ง $A = A_i$ นั่นคือ กำหนดให้แต่ละ $i \in I$ เป็นชื่อของสมาชิกจาก $\mathcal{A}$ แล้วเราอาจเขียน $\mathcal{A}$ แบบบอกเงื่อนไขได้เป็น

$$\mathcal{A} = \{A_i \mid i \in I\}$$

เราเรียก I ว่า *เซตดรรชนี (index set)* และเรียกสมาชิกของเซตดรรชนีว่า *ดรรชนี (index)* ถ้าเซตดรรชนี I เป็นเซตจำกัด เช่น I = {1, 2, . . . , n } เมื่อ n เป็นจำนวนเต็มบวกหรือ I = **N** แล้วเราอาจแจกแจง $\{A_i | i \in I\}$ ได้ตามลำดับดังนี้

$$\{A_i | i \in I\} = \{A_1, A_2, \ldots, A_n\} \quad \text{หรือ} \quad \{A_i | i \in I\} = \{A_1, A_2, \ldots, A_n, \ldots\}$$

1.1.5 **บทนิยาม** ให้ I เป็นเซตดรรชนีและ X เป็นหมู่ของเซตซึ่งดรรชนีโดย I นั่นคือ $X = \{A_i | i \in I\}$ เราเรียกเซตซึ่งประกอบด้วยสมาชิกที่เป็นสมาชิกของเซตจาก X อย่างน้อยหนึ่งตัวว่า *ส่วนรวมของ X (union of X)* และเขียนแทนด้วยสัญลักษณ์ $\cup\{A_i | i \in I\}$ หรือ $\bigcup_{i \in I} A_i$ นั่นคือ

$$\cup\{A_i | i \in I\} = \bigcup_{i \in I} A_i = \{x \mid (\exists i \in I)(x \in A_i)\}$$

เรียกเซตซึ่งประกอบด้วยสมาชิกที่เป็นสมาชิกของทุกๆ เซตจาก X ว่า *ส่วนร่วมของ X (intersection of X)* และเขียนแทนด้วยสัญลักษณ์ $\cap\{A_i | i \in I\}$ หรือ $\bigcap_{i \in I} A_i$ นั่นคือ

$$\cap\{A_i | i \in I\} = \bigcap_{i \in I} A_i = \{x \mid (\forall i \in I)(x \in A_i)\}$$

เนื่องจากเซตทุกๆ เซตอาจถูกพิจารณาเป็นเซตดรรชนี ดังนั้นถ้า X เป็นหมู่ของเซตซึ่งดรรชนีสมาชิกของ X ด้วย X แล้วส่วนรวมและส่วนร่วมของ X จะเขียนแทนด้วยสัญลักษณ์ตามลำดับ ดังนี้

$$\cup X = \cup\{T | T \in x\} = \{x \mid (\exists T \in X)(x \in T)\}$$

และ $$\cap X = \cap\{T | T \in x\} = \{x \mid (\forall T \in X)(x \in T)\}$$

ขอให้สังเกตว่าถ้า X = {T} หรือ X = {A, B} แล้ว $\cup X = \cup\{T\} = T$, $\cap X = \cap\{T\} = T$, $\cup X = \cup\{A, B\} = A \cup B$ และ $\cap X = \cap\{A, B\} = A \cap B$ เป็นกรณีที่ศึกษาผ่านมา

ถ้า I = {1, 2, ... , n } แล้วอาจเขียน $\cup\{A_i | i \in I\}$ หรือ $\cap\{A_i | i \in I\}$ เป็น $\bigcup_{i=1}^{n} A_i$ หรือ $\bigcap_{i=1}^{n} A_i$ ตามลำดับ และ

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \ldots \cup A_n \quad \text{และ} \quad \bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$

1.1.6 **ตัวอย่าง**

1. $\bigcup\{\{3,4,5\},\{5,6\},\phi\} = \{3,4,5\}\cup\{5,6\}\cup\phi = \{3,4,5,6\}$ และ

   $\bigcap\{\{3,4,5\},\{5,6\},\phi\} = \{3,4,5\}\cap\{5,6\}\cap\phi = \phi$

2. $\bigcup_{n=1}^{\infty}[n,n+1] = [1,2]\cup[2,3]\cup\ldots\cup[n,n+1]\cup\ldots = [1,\infty)$

และ $\bigcup_{n=1}^{4}[n,n+1] = [1,5]$

แต่ $\bigcap_{n=1}^{\infty}[n,n+1] = \phi = \bigcap_{n=1}^{4}[n,n+1]$

และ $\bigcap_{n=3}^{4}[n,n+1] = [3,4]\cap[4,5] = \{4\}$ ○

ทฤษฎีบทสามทฤษฎีบทต่อไปนี้ เป็นการวางนัยทั่วไปของสมบัติของส่วนร่วมและส่วนรวมซึ่งสามารถพิสูจน์ได้ดยตรงจากนิยาม จึงขอละการพิสูจน์ไว้เป็นแบบฝึกหัดสำหรับผู้อ่าน

1.1.7 **ทฤษฎีบท** ให้ I เป็นเซตที่ไม่ใช่เซตว่างและ B เป็นเซต แล้ว

$$\left(\bigcup_{i\in I}A_i\right)\cup B = \bigcup_{i\in I}(A_i\cup B), \qquad \left(\bigcap_{i\in I}A_i\right)\cap B = \bigcap_{i\in I}(A_i\cap B)$$

$$\left(\bigcup_{i\in I}A_i\right)\cap B = \bigcup_{i\in I}(A_i\cap B) \text{ และ } \left(\bigcap_{i\in I}A_i\right)\cup B = \bigcap_{i\in I}(A_i\cup B)$$ □

1.1.8 **ทฤษฎีบท** ให้ A เป็นเซต แล้ว

1. ถ้า $C\in A$ แล้ว $C\subseteq\bigcup A$
2. ถ้า $C\in A$ แล้ว $\bigcap A\subseteq C$
3. $\bigcap A\subseteq\bigcup A$
4. ถ้า D เป็นเซตซึ่ง $C\subseteq D$ สำหรับทุก $C\in A$ แล้ว $\bigcup A\subseteq D$
5. ถ้า D เป็นเซตซึ่ง $D\subseteq C$ สำหรับทุก $C\in A$ แล้ว $D\subseteq\bigcap A$ □

### 1.1.9 การวางนัยทั่วไปของกฎเดอมอร์แกน (Generalized de Morgan's Laws)

ถ้า I เป็นเซตที่ไม่ใช่เซตว่าง แล้ว $\left(\bigcup_{i\in I} A_i\right)' = \bigcap_{i\in I} A_i'$ และ $\left(\bigcap_{i\in I} A_i\right)' = \bigcup_{i\in I} A_i'$ ❐

**แบบฝึกหัด 1.1**

1. กำหนดให้ A, B และ C เป็นเซต จงพิสูจน์ว่า
   1.1 ถ้า $A \subseteq B$ และ $B \subseteq C$ แล้ว $A \subseteq C$
   1.2 ถ้า $B \subseteq A$ และ $C \subseteq A$ แล้ว $B \cup C \subseteq A$
   1.3 $A \cap B = A$ ก็ต่อเมื่อ $A \subseteq B$
   1.4 $(A \cap B)\, A = A = (A \cup B) \cap A$
   1.5 $A \cap B = (A \cup B) - ((A - B) \cup (B - A)) = A - (A - B) = B - (B - A)$
   1.6 $A \cap (B' \cap C)' \subseteq B \cup (A \cap C')$
2. จงพิสูจน์ทฤษฎีบท 1.1.2, 1.1.3, 1.1.4, 1.1.7, 1.1.8 และ 1.1.9
3. สำหรับแต่ละ $n \in \mathbf{N}$ กำหนดให้ $B_n = \mathbf{N} - \{1, 2, \ldots, n\}$ และ $X = \{B_n \mid n \in \mathbf{N}\}$ จงหาส่วนร่วมและส่วนรวมของ X
4. จงพิสูจน์ว่า $\bigcup_{a\in R} (-a, a) = \mathbf{R}$ และ $\bigcap_{a\in R} (-a, a) = \{0\}$
5. จงพิสูจน์ว่า $\bigcup \phi = \phi$ และ $\bigcap \phi = U$
6. ถ้า $A \subseteq B$ แล้ว $\bigcup A \subseteq \bigcup B$ และ $\bigcap B \subseteq \bigcap A$
7. ให้ I เป็นเซตดรรชนีและ $\{A_i \mid i \in I\}$ และ $\{B_i \mid i \in I\}$ เป็นหมู่ของเซตซึ่ง $A_i \subseteq B_i$ สำหรับแต่ละ $i \in I$ จงพิสูจน์ว่า $\bigcup_{i\in I} A_i \subseteq \bigcup_{i\in I} B_i$ และ $\bigcap_{i\in I} A_i \subseteq \bigcap_{i\in I} B_i$
8. ให้ I และ J เป็นเซตดรรชนีและ $\{A_i \mid i \in I\}$ และ $\{B_j \mid j \in J\}$ เป็นหมู่ของเซตซึ่งสำหรับแต่ละ $i \in I$ มี $j \in J$ ที่ทำให้ $B_j \subseteq A_i$ จงพิสูจน์ว่า $\bigcap_{j\in J} B_j \subseteq \bigcap_{i\in I} A_i$

## 1.2 ความสัมพันธ์

ในทางคณิตศาสตร์ การกล่าวถึงสมาชิกสองตัวจากเซตสองเซต อันดับของการกล่าวถึงสมาชิกทั้งสองตัวนี้อาจมีผลทำให้ความหมายเปลี่ยนแปลงได้เช่น $2 < 3$ มีความหมายในทางคณิตศาสตร์ แต่ $3 < 2$ ไม่เกิดขึ้นในทางคณิตศาสตร์ เป็นต้น ในหัวข้อนี้ จะขอแสดงวิธีการทางคณิตศาสตร์ที่จะกล่าวถึงสมาชิกทั้งสองตัวภายใต้เงื่อนไขเกี่ยวกับอันดับของกล่าวถึงสมาชิกทั้งสอง

ถ้า x และ y เป็นสมาชิกจากเซต A และ B ตามลำดับ จะเรียกเซต $\{\{x\}, \{x, y\}\}$ ที่กำหนดโดย x และ y ว่า *คู่อันดับ (ordered pair)* ของ x และ y และเขียนแทนด้วยสัญลักษณ์ (x , y) นั่นคือ

$$(x, y) = \{\{x\}, \{x, y\}\}$$

สังเกตจากนิยามคู่อันดับ จะเห็นว่า (x, y) และ (y, x) ไม่เป็นคู่อันดับเดียวกันถ้า $x \neq y$ ดังจะแสดงการพิสูจน์ให้เห็นจริงในทฤษฎีบทต่อไปนี้

1.2.1 **ทฤษฎีบท** ให้ A และ B เป็นเซต $x, u \in A$ และ $y, v \in B$ แล้ว (x, y) และ (u, v) เป็นคู่อันดับเดียวกัน ก็ต่อเมื่อ $x = u$ และ $y = v$

**บทพิสูจน์** เห็นได้ชัดว่าถ้า $x = u$ และ $y = v$ แล้ว $\{x\} = \{u\}$ และ $\{x, y\} = \{u, v\}$ ทำให้ได้ $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$ ซึ่งแสดงว่า $(x, y) = (u, v)$ เราจึงจะพิสูจน์บทกลับโดยสมมติให้ $(x, y) = (u, v)$ แล้วจะแยกการพิจารณาเป็น 2 กรณี ดังนี้

(ก) ถ้า $x = y$ ในกรณีนี้จะได้ว่า $(x, y) = (x, x) = \{\{x\}, \{x, x\}\} = \{\{x\}\}$ ดังนั้น $\{\{u\}, \{u, v\} = \{\{x\}\}$ ซึ่งแสดงว่า $\{u\} = \{u, v\} = \{x\}$ ทำให้สรุปได้ว่า $x = u = y = v$

(ข) ถ้า $x \neq y$ ในกรณีนี้ $\{x\} \neq \{x, y\}$ ดังนั้น $\{x\} \neq \{u, v\}$ เพราะมิฉะนั้น $x = u = y$ ซึ่งจะเกิดเป็นข้อขัดแย้งกันเอง

เนื่องจาก $\{x\} \in \{\{u\}, \{u, v\}\}$ และ $\{x\} \neq \{u, v\}$ ทำให้ได้ $\{u\} = \{x\}$ นั่นคือ $x = u$ และเช่นเดียวกันเพราะ $\{x, y\} \in \{\{u\}, \{u, v\}\}$ และ $\{u, v\} \neq \{x\}$ ดังนั้น $\{u, v\} = \{x, y\}$ ทำให้ได้ว่า $y \in \{u, v\}$ แต่ $y \neq u$ เพราะมิฉะนั้นแล้ว $x = u = y$ ซึ่งทำให้เกิดข้อขัดแย้ง จึงสรุปว่า $y = v$

ดังนั้นไม่ว่ากรณีใดถ้า $(x, y) = (u, v)$ แล้ว $x = u$ และ $y = v$ ❐

จากการสังเกต เราพบว่า x และ y ต่างไม่เป็นสมาชิกของคู่อันดับ (x, y) อย่างไรก็ตามเราเรียก x และ y ว่า *องค์ประกอบ (component)* ของคู่อันดับ (x, y) โดยเรียก x ว่า *คู่อันดับหน้า (first*

*component)* และเรียก y ว่า *คู่อันดับหลัง (second component)* เราใช้สัญลักษณ์ $A \times B$ แทนเซตของคู่อันดับทั้งหมดที่มีคู่อันดับหน้าเป็นสมาชิกของ A และคู่อันดับหลังเป็นสมาชิกของ B และเรียก $A \times B$ ว่า *ผลคูณคาร์ทีเซียน (cartesian product)* ของ A และ B นั่นคือ

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

ตัวอย่างเช่น ถ้า $A = \{1, 2, 3\}$ และ $B = \{a, b\}$ แล้ว

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

และ $$B \times A = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

และตัวอย่างนี้ยังแสดงให้เห็นว่า โดยทั่วไปแล้ว $A \times B \neq B \times A$ และโดยทฤษฎีบท 1.2.1 จะได้ว่า $A \times B$ และ $B \times A$ เป็นเซตเดียวกัน ก็ต่อเมื่อ A และ B เป็นเซตเดียวกัน นั่นคือ

$$A \times B = B \times A \iff A = B$$

นอกจากนี้ $$A \times \phi = \phi \times A = \phi$$

ประโยชน์สำคัญประการหนึ่งของผลคูณคาร์ทีเซียนคือการให้นิยาม "ความสัมพันธ์" เพราะความสัมพันธ์เป็นคำแสดงการเกี่ยวข้องกันระหว่างสมาชิกจากเซตสองเซตเช่น a เป็นบิดาของ b ซึ่งในกรณีนี้ b จะไม่เป็นบิดาของ A นั่นคืออันดับการกล่าวถึงสมาชิกสองตัวที่สัมพันธ์กันนั้นมีผลทำให้ความหมายเปลี่ยนแปลงได้

1.2.2 **บทนิยาม** ให้ A และ B เป็นเซต *ความสัมพันธ์ (relation)* r จาก A ไปยัง B คือเซตย่อยของ $A \times B$ และถ้า r เป็นความสัมพันธ์จาก A ไปยัง A จะเรียก r ว่าความสัมพันธ์ใน A

*โดเมน (domain)* ของความสัมพันธ์ r จาก A ไปยัง B คือเซตของคู่อันดับหน้าของคู่อันดับซึ่งอยู่ใน r และ*พิสัย (range)*ของ r คือเซตของคู่อันดับหลังของคู่อันดับซึ่งอยู่ใน r โดยใช้สัญลักษณ์ D(r) และ R(r) แทนโดเมนและพิสัยของ r ตามลำดับ นั่นคือ

$$D(r) = \{ a \in A \mid (a, b) \in r \} \quad \text{และ} \quad R(r) = \{ b \in B \mid (a, b) \in r \}$$

ถ้า $(a, b) \in r$ จะกล่าวว่า a มีความสัมพันธ์ r กับ b และอาจเขียนแทนด้วยสัญลักษณ์ "a r b" ตัวอย่างเช่น < เป็นความสัมพันธ์ใน Z เมื่อเขียน $3 < 4$ จะหมายความว่า $(3, 4) \in <$ และโดยกลับกันเป็นต้น

เราอาจสังเกตว่าถ้า A และ B เป็นเซตและ r เป็นความสัมพันธ์จาก A ไปยัง B แล้วสำหรับแต่ละคู่อันดับ $(a, b) \in r$ หรือ $a\ r\ b$ เราจะได้ว่า (b, a) จะเป็นสมาชิกของ $B \times A$ ทำให้ได้ว่าเซต

$$\{ (b, a) \in B \times A \mid (a, b) \in r \}$$

เป็นความสัมพันธ์จาก B ไปยัง A ซึ่งกำหนดโดย r เราจึงเรียกเซต $\{(b, a) \in B \times A \mid (a, b) \in r\}$ ว่า *ความสัมพันธ์ผกผัน (inverse relation)* ของ r และเขียนแทนด้วยสัญลักษณ์ $r^{-1}$ ดังนั้น

$$r^{-1} = \{ (b, a) \in B \times A \mid (a, b) \in r \}$$

และโดยการพิสูจน์อย่างง่ายๆ จะได้ว่า

1. $(r^{-1})^{-1} = r$
2. $D(r) = R(r^{-1})$ และ $R(r) = D(r^{-1})$

ความสัมพันธ์ในเซต A ที่มีสมบัติแบ่งกั้น A ออกเป็นเซตย่อยของ A หลาย ๆ เซตโดยที่เซตย่อยทั้งหลายเหล่านั้นไม่มีสมาชิกร่วมกันเลย ตัวอย่างเช่น "เท่ากับ =" เป็นความสัมพันธ์ในเซต Z ที่ทำให้เกิดเซตของเซตย่อยของ Z ซึ่งแต่ละเซตย่อยมีสมาชิกเพียงตัวเดียว หรือ "การเท่ากันทุกประการของสามเหลี่ยมบนระนาบ" ก็เป็นความสัมพันธ์ในเซตของสามเหลี่ยมที่มีสมบัติดังกล่าวเป็นต้น และจะสังเกตเห็นว่าความสัมพันธ์ชนิดนี้พบได้บ่อยในทุกๆ สาขาวิชาคณิตศาสตร์ เราเรียกความสัมพันธ์ที่มีสมบัติดังกล่าวว่าความสัมพันธ์สมมูลและนิยมเขียนแทนความสัมพันธ์สมมูลด้วยสัญลักษณ์ $\sim$

1.2.3 **บทนิยาม** ความสัมพันธ์ $\sim$ ในเซต A เป็น *ความสัมพันธ์สมมูล (equivalence relation)* ถ้า $\sim$ สอดคล้องสมบัติ 3 ประการต่อไปนี้

1. สมบัติสะท้อน (reflexive) นั่นคือ $a \sim a$ สำหรับทุก ๆ $a \in A$
2. สมบัติสมมาตร (symmetric) นั่นคือ สำหรับทุกๆ $a, b \in A$ ถ้า $a \sim b$ แล้ว $b \sim a$
3. สมบัติถ่ายทอด (transitive) นั่นคือ สำหรับทุกๆ $a, b, c \in A$ ถ้า $a \sim b$ และ $b \sim c$ แล้ว $a \sim c$

**หมายเหตุ** ถ้า $\sim$ เป็นความสัมพันธ์สมมูลและ $a \sim b$ จะอ่านว่า a เทียบเท่า(equivalent to) b และใช้คำอื่นในกรณีเฉพาะเช่น "เท่ากัน" ใน Z หรือ "เท่ากันทุกประการ" ในเซตของสามเหลี่ยม เป็นต้น

1.2.4 **ตัวอย่าง** ให้ L แทนเซตของเส้นตรงทั้งหมดบนระนาบในระบบพิกัดฉาก และนิยามความสัมพันธ์ $\sim$ ใน L โดย $L_1 \sim L_2$ ก็ต่อเมื่อ $L_1$ ขนานกับ $L_2$ (ใช้สัญลักษณ์แทนด้วย $L_1 // L_2$) สำหรับทุกๆ $L_1, L_2 \in L$ แล้ว $\sim$ เป็นความสัมพันธ์สมมูลบน L ❍

1.2.5 **ตัวอย่าง** ให้ p แทนจุดคงตัวจุดหนึ่งบนระนาบ P และสำหรับ x, y ใน P นิยาม $x \sim y$ ก็ต่อเมื่อ $|x-p| = |y-p|$ เมื่อ $|x-p|$ และ $|y-p|$ แทนระยะทางจากจุด x และ y มายังจุด p ตามลำดับแล้วเห็นได้ชัดว่า $\sim$ เป็นความสัมพันธ์สมมูลใน P ❍

จากตัวอย่าง 1.2.5 ได้ว่า $\sim$ แบ่งกั้น P ออกเป็นเซตย่อยๆ ซึ่งแต่ละเซตย่อยคือเซตของจุดบนเส้นรอบวงของวงกลมที่มีจุดศูนย์กลางที่ p และรัศมีเป็นค่าคงตัวค่าหนึ่งซึ่งเป็นระยะห่างจากจุดบนวงกลมนั้นๆ ถึงจุด p เราจะให้ชื่อเรียกเซตย่อยๆ เหล่านี้ซึ่งขึ้นกับแต่ละความสัมพันธ์สมมูลดังบทนิยามต่อไปนี้

1.2.6 **บทนิยาม** ให้ $\sim$ เป็นความสัมพันธ์สมมูลในเซต A และสำหรับแต่ละ $a \in A$ นิยามเซต $\bar{a} = \{ x \in A \mid x \sim a \}$ และเรียกว่า *ชั้นสมมูล (equivalent class)* กำหนดโดย a สัมพัทธ์กับ $\sim$

จากสมบัติของความสัมพันธ์สมมูล ทำให้สังเกตเห็นว่า $a \in \bar{a}$ และถ้า $b \in \bar{a}$ แล้ว $a \in \bar{b}$ ด้วย ทฤษฎีบท 1.2.7 ต่อไปนี้ กล่าวถึงสมบัติเบื้องต้นของชั้นสมมูลเหล่านี้

1.2.7 **ทฤษฎีบท** ให้ $\sim$ เป็นความสัมพันธ์สมมูลในเซต A แล้ว

1. $\bar{a} \neq \phi$ สำหรับแต่ละ $a \in A$
2. สำหรับทุก ๆ $a, b \in A$ ถ้า $b \in \bar{a}$ แล้ว $\bar{a} = \bar{b}$
3. $\bar{a} = \bar{b}$ หรือ $\bar{a} \cap \bar{b} = \phi$ สำหรับทุกๆ $a, b \in A$
4. ถ้า $\wp$ เป็นเซตของชั้นสมมูลสัมพัทธ์กับ $\sim$ ทั้งหมดแล้ว $\bigcup \wp = A$

**บทพิสูจน์** 1. จากบทนิยามของชั้นสมมูลและสมบัติความสัมพันธ์สมมูล จะได้ $a \in \bar{a}$ ดังนั้น $\bar{a} \neq \phi$ สำหรับแต่ละ $a \in A$

2. ให้ $a, b \in A$ โดยที่ $b \in \bar{a}$ แล้ว $a \sim b$ และจะแสดงว่า $\bar{a} = \bar{b}$ จึงให้ $x \in \bar{a}$ แล้ว $x \sim a$ และจาก $a \sim b$ ด้วย ดังนั้นโดยสมบัติถ่ายทอดของ $\sim$ จะได้ $x \sim b$ ซึ่งแสดงว่า $x \in \bar{b}$ เพราะฉะนั้น $\bar{a} \subseteq \bar{b}$ และโดยการพิสูจน์ทำนองเดียวกัน จะได้ว่า $\bar{b} \subseteq \bar{a}$ ซึ่งทำให้สรุปได้ว่า $\bar{a} = \bar{b}$

3. ให้ $a, b \in A$ และสมมติในทางตรงข้ามว่า $\bar{a} \neq \bar{b}$ และ $\bar{a} \cap \bar{b} \neq \phi$ แล้วจะมี $c \in A$ ซึ่ง $c \in \bar{a} \cap \bar{b}$ นั่นคือ $c \in \bar{a}$ และ $c \in \bar{b}$ ทำให้ได้โดยข้อ (2) ว่า $\bar{a} = \bar{c} = \bar{b}$ ซึ่งขัดแย้งกับ $\bar{a} \neq \bar{b}$ เพราะฉะนั้นข้อ 3 เป็นจริง

4. เพราะว่า $\bar{a} \subseteq A$ สำหรับทุกๆ $a \in A$ จึงได้ว่า $\cup \wp \subseteq A$ ในทางกลับกันถ้าให้ $x \in A$ แล้ว $x \in \bar{x}$ ซึ่งแสดงว่ามี $\bar{x} \in \wp$ ที่ทำให้ $x \in \bar{x}$ นั่นคือ $x \in \cup \wp$ ทำให้ได้ $A \subseteq \cup \wp$ ดังนั้น $A = \cup \wp$ ❐

**1.2.8 บทนิยาม** ให้ A เป็นเซต เรียกเซต $\wp$ ของเซตย่อยของ A ว่า *ผลแบ่งกั้น (partition)* A ถ้า

1. $\wp \neq \phi$ และ $B \neq \phi$ สำหรับแต่ละ $B \in \wp$
2. $A = \cup \wp$
3. $B \cap C = \phi$ หรือ $B = C$ สำหรับทุกๆ $B, C \in \wp$

ตัวอย่างเช่นเซต { {1}, {2, 5}, {3}, {4} }, { {1, 3, 4}, {2, 5} }, { {1}, {2}, {3}, {4}, {5} } ต่างเป็นผลแบ่งกั้นเซต {1, 2, 3, 4, 5 }

ขอให้สังเกตว่าถ้า $\wp$ เป็นผลแบ่งกั้น A แล้วแต่ละสมาชิกของ A จะอยู่ในเซตที่เป็นสมาชิกของ $\wp$ เซตใดเซตหนึ่งและเพียงเซตเดียวเท่านั้น

โดยผลของทฤษฎีบท 1.2.7 ถ้า $\sim$ เป็นความสัมพันธ์สมมูลในเซต A แล้วเซตของชั้นสมมูลทั้งหมดจะเป็นผลแบ่งกั้นหนึ่งของ A เราเรียกเซตของชั้นสมมูลว่า *"ผลแบ่งกั้น A ซึ่งกำหนดโดย $\sim$"* และทฤษฎีบทต่อไปนี้ก็จะแสดงให้เห็นว่าบทกลับก็เป็นจริงด้วย นั่นคือแต่ละผลแบ่งกั้นเซต A จะกำหนดความสัมพันธ์สมมูลใน A เช่นกัน

**1.2.9 ทฤษฎีบท** ให้ $\wp$ เป็นผลแบ่งกั้นเซต A และนิยามความสัมพันธ์ $\sim$ ใน A ดังนี้

$$a \sim b \iff \text{มี } C \in \wp \text{ ซึ่ง } a, b \in C$$

สำหรับทุกๆ $a, b \in A$ แล้ว $\sim$ เป็นความสัมพันธ์สมมูลใน A ซึ่งจะเรียก $\sim$ ว่า *ความสัมพันธ์สมมูลกำหนดโดย* $\wp$

**บทพิสูจน์** ให้ $\sim$ เป็นความสัมพันธ์ใน A ซึ่งนิยามโดย $a \sim b$ ก็ต่อเมื่อ มี $C \in \wp$ ซึ่ง $a, b \in C$ สำหรับทุกๆ $a, b \in A$ และให้ $a \in A$ แล้วโดยสมบัติข้อ 2 ของผลแบ่งกั้น $\wp$ ของ A จะมี $C \in \wp$ ซึ่ง $a \in C$ นั่นคือมี $C \in \wp$ ซึ่ง $a, a \in C$ ดังนั้น $a \sim a$

สมบัติสมมาตรเห็นได้ชัด เนื่องจากสำหรับทุกๆ $a, b \in A$ ถ้ามีเซต $B \in \wp$ ซึ่ง $a, b \in B$ แล้ว $b, a \in B$ จึงจะพิสูจน์สมบัติถ่ายทอดโดยให้ $a, b, c \in A$ ซึ่ง $a \sim b$ และ $b \sim c$ แล้วจะมีเซต $C, D \in \wp$ ซึ่ง $a, b \in C$ และ $b, c \in D$ ดังนั้น $b \in C \cap D$ ทำให้ได้โดยสมบัติข้อ 3 ของ $\wp$ ว่า $C = D$ ซึ่งแสดงว่ามี $C \in \wp$ ซึ่ง $a, b, c \in C$ เพราะฉะนั้น $a \sim c$ ❐

ตัวอย่างเช่น เซตของจำนวนเต็มคู่และเซตของจำนวนเต็มคี่เป็นสมาชิกของผลแบ่งกั้น Z และความสัมพันธ์สมมูล $\sim$ ใน Z กำหนดโดยผลแบ่งกั้นนี้ตามทฤษฎีบท 1.2.9 นิยามโดย

$a \sim b \quad \Leftrightarrow \quad$ a และ b ทั้งคู่เป็นจำนวนคู่หรือทั้งคู่เป็นจำนวนคี่

สำหรับทุกๆ $a, b \in Z$ เป็นต้น

ท้ายสุดของหัวข้อนี้ จะขอกล่าวถึงความสัมพันธ์ในเซต A ที่มีประโยชน์มาก โดยเฉพาะการพิสูจน์สมบัติสำคัญๆ ของจำนวนจริง ได้จากการทราบสมบัติของจำนวนจริงภายใต้ความสัมพันธ์นี้

โดยทั่วไป การกล่าวถึงสมบัติของความสัมพันธ์ในเซต A เรานิยมพิจารณาสมบัติ 4 ข้อได้แก่ "สมบัติสะท้อน" "สมบัติสมมาตร" "สมบัติถ่ายทอด" ซึ่งความสัมพันธ์ในเซต A ใดสอดคล้องสมบัติทั้งสามข้อนี้ เราเรียกว่า "ความสัมพันธ์สมมูล" ซึ่งเราได้ศึกษาไปข้างต้นแล้วว่าความสัมพันธ์สมมูล ทำให้เราสามารถแบ่งกั้นเซตได้ แต่ความสัมพันธ์ใดที่สอดคล้อง"สมบัติสะท้อน" "สมบัติปฏิสมมาตร" "สมบัติถ่ายทอด" เราจะเรียกว่า "อันดับ" และอันดับ ทำให้เราสามารถจัดวางเรียงสมาชิกในเซตได้อย่างเป็นระบบ

1.2.10 **บทนิยาม** ให้ A เป็นเซตและ $R \subseteq A \times A$ เราเรียก R ว่า *อันดับ (order)* บน A ถ้า R สอดคล้องสมบัติต่อไปนี้

1. สมบัติสะท้อน (reflexivity) นั่นคือ $(a, a) \in R$ สำหรับทุกๆ $a \in A$

2. สมบัติปฏิสมมาตร (anti–symmetric) นั่นคือ สำหรับทุกๆ $a, b \in A$ ถ้า $(a, b) \in R$ และ $(b, a) \in R$ แล้ว $a = b$
3. สมบัติถ่ายทอด (transitivity) นั่นคือ สำหรับทุกๆ $a, b, c \in A$ ถ้า $(a, b) \in R$ และ $(b, c) \in R$ แล้ว $(a, c) \in R$

และเรียก $r \subseteq A \times A$ ว่า r *อันดับโดยแท้ (strictly order)* บน A ถ้า r สอดคล้องสมบัติต่อไปนี้

1. สมบัติไม่สะท้อน (irreflexivity) นั่นคือ $(a, a) \notin r$ สำหรับทุกๆ $a \in A$
   [ขอให้สังเกตว่าสมบัตินี้ไม่ใช่นิเสธของสมบัติสะท้อน]
2. สมบัติถ่ายทอด(transitivity) นั่นคือ ถ้า $(a, b) \in r$ และ $(b, c) \in r$ แล้ว $(a, c) \in r$ สำหรับทุกๆ $a, b, c \in A$

เราจะได้ความสมนัยกันของอันดับและอันดับโดยแท้บนเซต A ดังจะกล่าวในทฤษฎีบทต่อไปนี้ โดยขอละการพิสูจน์ไว้เป็นแบบฝึกหัดสำหรับผู้อ่าน

### 1.2.11 ทฤษฎีบท

1. ถ้า $R \subseteq A \times A$ เป็นอันดับบนเซต A แล้วความสัมพันธ์ $r \subseteq A \times A$ ซึ่งนิยามสำหรับทุก ๆ $a, b \in A$ ดังต่อไปนี้ เป็นอันดับโดยแท้บน A

$$(a, b) \in r \iff (a, b) \in R \text{ และ } a \neq b$$

2. ในทำนองคู่กันถ้า $r \subseteq A \times A$ เป็นอันดับโดยแท้บน A แล้วความสัมพันธ์ $R \subseteq A \times A$ ซึ่งนิยามสำหรับทุก ๆ $a, b \in A$ ดังต่อไปนี้ เป็นอันดับบน A

$$(a, b) \in R \iff a = b \text{ หรือ } (a, b) \in r$$

❐

ตัวอย่างเช่น "น้อยกว่าหรือเท่ากับ $\leq$" บนเซตของจำนวนเป็นอันดับบนเซตของจำนวน โดยมี "น้อยกว่าโดยแท้ $<$" เป็นอันดับโดยแท้ที่สมนัยกันตามทฤษฎีบท 1.2.11 หรือ "เซตย่อย $\subseteq$" เป็นอันดับบนเซตของเซต โดยมี "เซตย่อยแท้ $\subset$" เป็นอันดับโดยแท้ที่สมนัยกันตามทฤษฎีบท 1.2.11 เป็นต้น

โดยทั่วไปที่ไม่มีการกล่าวเป็นอย่างอื่น เรานิยมใช้สัญลักษณ์ $\leq$ และ $<$ แทนอันดับและอันดับโดยแท้ ตามลำดับและอ่านว่า "น้อยกว่าหรือเท่ากับ" และ "น้อยกว่าโดยแท้" ตามที่เราคุ้นเคยกับการใช้ในระบบจำนวน

## แบบฝึกหัด 1.2

1. จงแสดงว่า $A\times(B\times C) = (A\times B)\times C$ สำหรับทุกๆ เซต A, B และ C
2. จงให้บทนิยามของ $A_1 \times A_2 \times \ldots \times A_n$ สำหรับทุกๆ จำนวนเต็มบวก n และทุกๆ เซต $A_1, A_2, \ldots, A_n$
3. ให้ A, B และ C เป็นเซต จงพิสูจน์ว่าข้อความ "ถ้า $A \neq \phi$ และ $A\times B = A\times C$ แล้ว $B = C$" เป็นจริงหรือไม่ และถ้าไม่มีเงื่อนไข "$A \neq \phi$" แล้วข้อความยังคงเป็นจริงหรือไม่
4. ให้ r และ s เป็นความสัมพันธ์จากเซต A ไปยังเซต B จงพิสูจน์ว่าข้อความต่อไปนี้เป็นจริงหรือเท็จ

   4.1 $D_{r\cap s} \subseteq D_r \cap D_s$ 4.2 $D_r \cap D_s \subseteq D_{r\cap s}$
5. จงแสดงว่า ถ้า $\sim$ เป็นความสัมพันธ์สมมูลในเซต S แล้วจะมีเซต U และฟังก์ชัน $\alpha : S \rightarrow U$ ซึ่ง $a \sim b \Leftrightarrow \alpha(a) = \alpha(b)$ สำหรับทุกๆ $a, b \in S$
6. จงแสดงว่า ถ้า S และ U เป็นเซตและ $\alpha : S \rightarrow U$ เป็นฟังก์ชัน แล้วความสัมพันธ์ $\sim$ ใน S ซึ่งนิยามโดย $a \sim b \Leftrightarrow \alpha(a) = \alpha(b)$ สำหรับทุกๆ $a, b \in S$ เป็นความสัมพันธ์สมมูลใน S
7. ให้ S เป็นเซตและ U เป็นเซตย่อยของ S และนิยามความสัมพันธ์ $\sim$ ในเซตกำลัง P(U) โดย $A \sim B \Leftrightarrow A \cap U = B \cap U$ สำหรับทุก ๆ เซตย่อย A และ B ของ U จงแสดงว่า $\sim$ เป็นความสัมพันธ์สมมูลใน P(U)
8. ให้ m เป็นจำนวนเต็มที่มากกว่า 1 และนิยามความสัมพันธ์ $\sim$ ในเซต Z ของจำนวนเต็มทั้งหมดโดย

   $a \sim b \Leftrightarrow$ m เป็นตัวหาร(หรือตัวประกอบ) $a - b$ สำหรับทุกๆ $a, b \in Z$

   จงแสดงว่า $\sim$ ความสัมพันธ์สมมูลใน Z
9. ให้ $\sim$ เป็นความสัมพันธ์สมมูลในเซต A ที่ไม่ใช่เซตว่างและ $\wp$ เป็นผลแบ่งกั้น A กำหนดโดย $\sim$ จงแสดงว่าถ้า R เป็นความสัมพันธ์สมมูลใน A กำหนดโดย $\wp$ (ดังนิยามในทฤษฎีบท 1.2.9) แล้ว $R = \sim$ (นั่นคือ $a \sim b$ ก็ต่อเมื่อ $a R b$ สำหรับทุกๆ $a, b \in A$)

10. ให้ $\wp$ เป็นผลแบ่งกั้นเซต A ที่ไม่ใช่เซตว่างและ $\sim$ เป็นความสัมพันธ์สมมูลใน A กำหนดโดย $\wp$ (ดังนิยามในทฤษฎีบท 1.2.9) จงแสดงว่าถ้า $\wp'$ เป็นเซตของชั้นสมมูลซึ่งเป็นผลแบ่งกั้น A กำหนดโดย $\sim$ แล้ว $\wp = \wp'$

11. ให้ $Z^+$ แทนเซตของจำนวนเต็มบวกทั้งหมดและนิยาม $\sim \subseteq Z^+ \times Z^+$ โดย

$$m \sim n \Leftrightarrow (\exists t \in Z^+)(mn = t^2)$$

แล้ว $\sim$ เป็นความสัมพันธ์สมมูลใน **N** หรือไม่ ถ้าเป็นจงเขียนชั้นสมมูลที่มี 2 เป็นสมาชิก

## 1.3 ฟังก์ชัน

ในการศึกษาโครงสร้างพีชคณิตในวิชาพีชคณิตนามธรรม สิ่งแรกที่เกี่ยวข้องและมีความสำคัญยิ่งคือการดำเนินการ เพราะโครงสร้างพีชคณิตประกอบด้วยเซตที่ไม่เป็นเซตว่างเซตหนึ่งกับการดำเนินการบนเซตนั้น แต่เพราะการดำเนินการคือฟังก์ชันและฟังก์ชันก็เป็นพื้นฐานสำคัญมากเรื่องหนึ่งของการศึกษาคณิตศาสตร์และโครงสร้างพีชคณิต ในหัวข้อนี้เราจึงจะทบทวนเรื่องเกี่ยวกับฟังก์ชันพอเป็นสังเขป

ฟังก์ชันเป็นตัวดำเนินการที่สำคัญในทุกๆ แขนงของวิชาคณิตศาสตร์ ในวิชาแคลคูลัสของฟังก์ชันตัวแปรเดียว เราศึกษาฟังก์ชันที่ส่งจากเซตของจำนวนจริงไปยังเซตของจำนวนจริง ตัวอย่างง่ายๆ ได้แก่ฟังก์ชันซึ่งกำหนดโดย $f(x) = x^2$ เป็นฟังก์ชันที่ส่งแต่ละจำนวนจริง x ไปยังจำนวนจริงบวก $x^2$ หรือฟังก์ชันซึ่งนิยามโดย $f(x) = \sin x$ เป็นฟังก์ชันที่ส่งแต่ละจำนวนจริง x ไปยังจำนวนจริง $\sin x$ ซึ่งมีค่าในช่วงปิด [0, 1] เราสังเกตว่าเซตของจำนวนจริง **R** ในตัวอย่างที่กล่าวถึงได้ทำหน้าที่ถึงสองครั้ง คือครั้งแรก $x \in \mathbf{R}$ ที่จะถูกส่งไปและครั้งที่สอง $f(x) \in \mathbf{R}$ เป็นตัวที่ถูกกำหนดโดย x แต่โดยทั่วไปฟังก์ชันไม่จำเป็นต้องถูกกำหนดบนเซตของจำนวนจริงเท่านั้น ดังนั้นในบทนิยามข้างล่างนี้และที่จะกล่าวถึงต่อๆ ไป จะใช้สัญลักษณ์ S และ T (อาจใช้สัญลักษณ์เป็นอย่างอื่นๆ ก็ได้) แทนเซตที่ฟังก์ชันถูกกำหนดและถูกส่งไปตามลำดับ

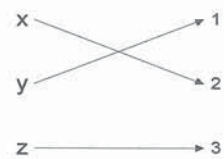
1.3.1 **บทนิยาม** *ฟังก์ชัน (function)* หรือ *การส่ง (mapping)* จากเซต S ไปยังเซต T คือความสัมพันธ์ของ S และ T โดยที่แต่ละสมาชิกของ S มีความสัมพันธ์กับสมาชิกของ T ได้เพียงตัวเดียวเท่านั้น

เราเรียก S ว่า *โดเมน (domain)* ของฟังก์ชันและเรียก T ว่า *โคโดเมน (codomain)* หรือ *พิสัย*

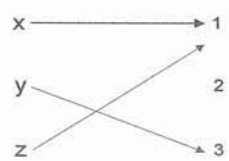
*(range)* ของฟังก์ชัน โดยนิยมใช้อักษรกรีกแทนฟังก์ชันเช่น $\alpha, \beta, \gamma$ , . . . เป็นต้น และถ้า $\alpha$ เป็นฟังก์ชันจาก S ไปยัง T จะเขียนแทนด้วยสัญลักษณ์ $\alpha : S \longrightarrow T$ หรือ $S \xrightarrow{\alpha} T$

ถ้า $\alpha$ เป็นฟังก์ชันจาก S ไปยัง T และ x เป็นสมาชิกใน S แล้วจะมีสมาชิกเพียงตัวเดียวเท่านั้นใน T ซึ่งจะสัมพันธ์กับ x จึงกำหนดสัญลักษณ์ $\alpha(x)$ แทนสมาชิกดังกล่าวและเรียกว่า *ภาพ (image)* ของ x ภายใต้ $\alpha$ โดยอาจเขียน $x \xrightarrow{\alpha} y$ เพื่อชี้ว่า y เป็นภาพของ x ภายใต้ $\alpha$ และถ้า $y = \alpha(x)$ ซึ่งเป็นสมาชิกใน T จะเรียก x ว่า *ภาพผกผัน (inverse image)* ของ y (ซึ่งอาจมีได้มากกว่า 1 ตัว) ภายใต้ $\alpha$

1.3.2 **ตัวอย่าง** ให้ $S = \{x, y, z\}$ และ $T = \{1, 2, 3\}$ แล้ว $\alpha$ ซึ่งกำหนดโดย $\alpha(x) = 2, \alpha(y) = 1$ และ $\alpha(z) = 3$ เป็นตัวอย่างของฟังก์ชันจาก S ไปยัง T และเราอาจแสดงการส่งของฟังก์ชันนี้ได้ด้วยแผนภาพข้างล่างนี้




หรืออีกฟังก์ชันหนึ่งจาก S ไปยัง T คือ $\beta : S \longrightarrow T$ ซึ่งกำหนดโดย $\beta(x) = 1, \beta(y) = 3$ และ $\beta(z) = 1$ โดยมีแผนภาพการส่งแสดงดังรูปข้างล่างนี้




○

ต่อไปเป็นตัวอย่างแสดงฟังก์ชันซึ่งรู้จักกันโดยทั่วไปและมีการกล่าวถึงอยู่เสมอ

1.3.3 **ตัวอย่าง**

1. สำหรับเซต S ใดๆ เรานิยมใช้สัญลักษณ์ $\iota_s$ แทนฟังก์ชันจาก S ไปยัง S ซึ่งกำหนดโดย $\iota_s(x) = x$ สำหรับทุกๆ $x \in s$ และเรียกว่า *ฟังก์ชันเอกลักษณ์ (identity function)* บน S
2. สำหรับแต่ละคู่อันดับ (s, t) ของจำนวนจริง s และ t กฎ (rule) ที่กำหนดโดย $(s, t) \longrightarrow s + t$ เป็นฟังก์ชันจากผลคูณคาร์ทีเซียน $R \times R$ (ซึ่งคือเซตของคู่อันดับของจำนวนจริง) ไปยังเซตของจำนวนจริง ○

ถ้า $\alpha : S \longrightarrow T$ และ A เป็นเซตย่อยของ S แล้ว $\alpha(A)$ เป็นสัญลักษณ์แทนเซตของสมาชิกใน T ซึ่งเป็นภาพของสมาชิกใน A ภายใต้ $\alpha$ นั่นคือ

$$\alpha(A) = \{ y \in T \mid \text{มี } x \in A \text{ ซึ่ง } y = \alpha(x) \}$$

และเรียกเซตนี้ว่า *ภาพ (image) ของ A ภายใต้* $\alpha$

ในทางกลับกันถ้า $\alpha : S \longrightarrow T$ และ B เป็นเซตย่อยของ T แล้ว $\alpha^{-1}(B)$ เป็นสัญลักษณ์แทนเซตของสมาชิกใน S ซึ่งเป็นภาพผกผันของสมาชิกใน B นั่นคือ

$$\alpha^{-1}(B) = \{ x \in S \mid \alpha(x) \in B \}$$

และเรียกเซตนี้ว่า *ภาพผกผัน (inverse image) ของ B ภายใต้* $\alpha$

ตัวอย่างเช่น สำหรับฟังก์ชัน $\alpha$ และ $\beta$ ของตัวอย่าง 1.3.1 จะได้ว่า $\alpha(\{x,z\}) = \{2, 3\}$, $\beta(\{x,z\}) = \{1\}$, $\alpha^{-1}(\{2,3\}) = \{x, z\}$ และ $\beta^{-1}(\{1\}) = \{x, z\}$ เป็นต้น

1.3.3 **บทนิยาม** ให้ S และ T เป็นเซตและ $\alpha : S \longrightarrow T$ และ $\beta : S \longrightarrow T$ จะกล่าวว่า $\alpha$ และ $\beta$ เป็นฟังก์ชันเดียวกัน นั่นคือ $\alpha = \beta$ ถ้า $\alpha(x) = \beta(x)$ สำหรับทุกๆ $x \in S$

1.3.4 **บทนิยาม** ให้ S และ T เป็นเซตและ $\alpha : S \longrightarrow T$ ถ้า $\alpha(S) = T$ (นั่นคือสำหรับแต่ละ $y \in T$ จะมี $x \in S$ อย่างน้อยหนึ่งตัวซึ่ง $\alpha(x) = y$) จะเรียก $\alpha$ ว่า *ฟังก์ชันทั่วถึง* (*surjective function* หรือ *surjection* หรือ *onto function*)

ตัวอย่างเช่นในตัวอย่าง 1.3.2 ฟังก์ชัน $\alpha$ เป็นฟังชันทั่งถึง แต่ฟังก์ชัน $\beta$ ไม่เป็นฟังก์ชันทั่วถึง เพราะว่าภาพของ S ภายใต้ $\beta$ คือ {1, 3} ซึ่งเป็นเซตย่อยแท้ของโคโดเมน T หรือฟังก์ชันที่กำหนดบนเซตของจำนวนจริงโดย $f(x) = x^2$ และ $f(x) = \sin x$ ต่างไม่เป็นฟังก์ชันทั่วถึง ทั้งนี้เพราะภาพของ R ภายใต้ฟังก์ชันที่กำหนดโดย $f(x) = x^2$ เป็นเซตของจำนวนจริงบวกและศูนย์ ส่วนภาพของ R ภายใต้ฟังก์ชันที่กำหนดโดย $f(x) = \sin x$ เป็นเซตของจำนวนจริงระหว่าง 1 และ -1 แต่ฟังก์ชันที่กำหนดบนเซตของจำนวนจริงโดย $f(x) = e^x$ เป็นฟังก์ชันทั่วถึง เป็นต้น

1.3.5 **บทนิยาม** ให้ S และ T เป็นเซตและ $\alpha : S \longrightarrow T$ จะเรียก $\alpha$ ว่า *ฟังก์ชันหนึ่งต่อหนึ่ง*

(*injective function* หรือ *injection* หรือ *one-to-one function*) ถ้าสมาชิกที่ต่างกันใน S มีภาพภายใต้ $\alpha$ ที่ต่างกันใน T นั่นคือเมื่อข้อความในรูปสัญลักษณ์ต่อไปนี้เป็นจริง

$$(\forall x_1, x_2 \in S)\,[x_1 \neq x_2 \rightarrow \alpha(x_1) \neq \alpha(x_2)]$$

ซึ่งสมมูลกับ $(\forall x_1, x_2 \in S)\,[\alpha(x_1) = \alpha(x_2) \rightarrow x_1 = x_2]$

ตัวอย่างเช่น ฟังก์ชันเอกลักษณ์บนแต่ละเซตและฟังก์ชัน $\alpha$ ในตัวอย่าง 1.3.2 ต่างเป็นฟังก์ชันหนึ่งต่อหนึ่ง แต่ฟังก์ชัน $\beta$ ในตัวอย่าง 1.3.2 ไม่เป็นฟังก์ชันหนึ่งต่อหนึ่งเพราะว่า $x \neq z$ แต่ $\beta(x) = 1 = \beta(z)$ หรือฟังก์ชันที่กำหนดบนเซตของจำนวนจริงโดย $f(x) = x^2$ และ $f(x) = \sin x$ ต่างไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะว่า $f(x) = x^2 = f(-x)$ แม้ว่า $x \neq -x$ สำหรับทุกๆ จำนวนจริง $x \neq 0$ และ $f(x) = \sin x = \sin(x + 2n\pi)$ สำหรับทุกๆ จำนวนจริง x และสำหรับทุก ๆ จำนวนเต็ม n

หรือฟังก์ชัน $\alpha$ ซึ่งกำหนดบนเซตของจำนวนจริงโดย $\alpha(x) = x - 1$ เป็นฟังชันหนึ่งต่อหนึ่งเพราะว่าถ้า $x_1, x_2 \in R$ และ $\alpha(x_1) = \alpha(x_2)$ แล้ว $x_1 - 1 = x_2 - 1$ ซึ่งทำให้ได้ $x_1 = x_2$ และขอให้สังเกตว่าฟังก์ชัน $\alpha$ นี้ก็เป็นฟังก์ชันทั่วถึงด้วย

1.3.6 **บทนิยาม** ให้ S และ T เป็นเซตและ $\alpha : S \rightarrow T$ จะเรียก $\alpha$ ว่า *ฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง* (*bijective function* หรือ *bijection*) หรืออาจเรียกว่า *ฟังก์ชันสมนัยหนึ่งต่อหนึ่ง* (*one-to-one correspondence*) ถ้า $\alpha$ เป็นทั้งฟังก์ชันหนึ่งต่อหนึ่งและฟังก์ชันทั่วถึง

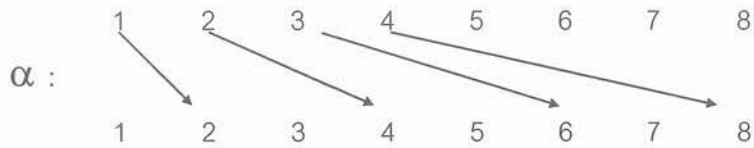
และถ้ามีฟังก์ชันสมนัยหนึ่งต่อหนึ่งจาก S ไปทั่วถึง T จะกล่าวว่า S และ T มีความสมนัยหนึ่งต่อหนึ่งหรือกล่าวว่า S และ T เป็นเซตที่มี *ขนาด (cardinality)* เดียวกันและเขียนแทนความหมายนี้ด้วยสัญลักษณ์ $|S| = |T|$

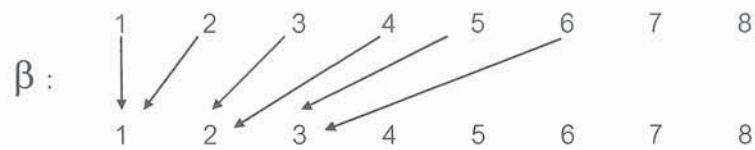
ตัวอย่างเช่นเซตของจำนวนเต็มทั้งหมดกับเซตของจำนวนคู่ทั้งหมดเป็นเซตที่มีขนาดเท่ากัน เพราะมีฟังก์ชันซึ่งส่งแต่ละจำนวนเต็ม n ไปยังจำนวนคู่ 2n เป็นฟังก์ชันสมนัยหนึ่งต่อหนึ่งและในทำนองเดียวกันฟังก์ชันซึ่งส่งแต่ละจำนวนเต็ม n ไปยังจำนวนคี่ 2n + 1 ก็เป็นฟังก์ชันสมนัยหนึ่งต่อหนึ่ง เซตของจำนวนเต็มทั้งหมดกับเซตของจำนวนคู่ทั้งหมด ทำให้ได้ว่าเซตทั้งสามมีขนาดเดียวกัน เป็นต้น

1.3.7 **ตัวอย่าง** ให้ $\alpha$ และ $\beta$ เป็นฟังก์ชันจากเซตของจำนวนนับ $Z^+ = \{1, 2, 3, \ldots\}$ ไปยัง $Z^+$ นิยามตามลำดับดังต่อไปนี้

$\alpha(n) = 2n$ สำหรับทุกๆ จำนวนนับ n และ $\beta(n) = \begin{cases} \frac{n+1}{2} & \text{ถ้า } n \text{ เป็นจำนวนคี่} \\ \frac{n}{2} & \text{ถ้า } n \text{ เป็นจำนวนคู่} \end{cases}$

โดยมีแผนภาพการส่งของฟังก์ชันทั้งสองแสดงตามลำดับ ดังรูปข้างล่างนี้




แล้วเห็นได้ชัดว่า $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง แต่ไม่เป็นฟังก์ชันทั่วถึง ในขณะที่ $\beta$ เป็นฟังก์ชันทั่วถึง แต่ไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง ❍

ขอให้สังเกตว่าตัวอย่าง 1.3.7 ยังแสดงให้เห็นว่าสำหรับเซตอนันต์ S อาจมีฟังก์ชันหนึ่งต่อหนึ่งจาก S ไปยัง S ที่ไม่เป็นฟังก์ชันทั่วถึง หรือมีฟังก์ชันทั่วถึงจาก S ไปยัง S ที่ไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง ในขณะที่ถ้า S เป็นเซตจำกัดและ $\alpha$ เป็นฟังก์ชันจาก S ไปยัง S แล้ว $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อ $\alpha$ เป็นฟังก์ชันทั่วถึง

1.3.8 **ตัวอย่าง** ให้ S และ T เป็นเซตและนิยามฟังก์ชัน $\alpha : S\times T \rightarrow S$ โดย $\alpha(a,b) = a$ สำหรับทุกๆ $a \in S$ และ $b \in T$ แล้วเห็นได้ชัดว่า $\alpha$ เป็นฟังก์ชันทั่วถึง แต่ไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง

เราเรียกฟังก์ชัน $\alpha$ ซึ่งนิยามเช่นนี้ว่า *ภาพฉาย (projection)* ของ $S\times T$ ลงบน S และในทำนองเดียวกันฟังก์ชัน $\beta : S\times T \rightarrow T$ ซึ่งนิยามโดย $\beta(a,b) = b$ สำหรับทุกๆ $a \in S$ และ $b \in T$ จะเป็น *ภาพฉาย* ของ $S\times T$ ลงบน T ❍

1.3.9 **ทฤษฎีบท** ให้ S และ T เป็นเซตและ $\alpha : S \rightarrow T$

1. $\alpha(A \cup B) = \alpha(A) \cup \alpha(B)$ สำหรับทุกๆ เซตย่อย A และ B ของ S

2. $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อ $\alpha(A\cap B) = \alpha(A)\cap\alpha(B)$ สำหรับทุกๆ เซตย่อย A และ B ของ S

**บทพิสูจน์** 1. ให้ Aและ B เป็นเซตย่อยของ S และให้ $y\in \alpha(A\cup B)$ แล้วจะมี $x\in A\cup B$ ซึ่ง $y=\alpha(x)$ ถ้า $x\in A$ จะได้ว่ามี $x\in A$ ซึ่ง $y=\alpha(x)$ ซึ่งทำให้ได้ $y\in \alpha(A)$ หรือถ้า $x\in B$ จะได้ว่ามี $x\in B$ ซึ่ง $y=\alpha(x)$ ซึ่งทำให้ได้ $y\in \alpha(B)$ ดังนั้นไม่ว่ากรณีใด $y\in \alpha(A)\cup\alpha(B)$ เพราะฉะนั้น $\alpha(A\cup B)\subseteq \alpha(A)\cup\alpha(B)$

ในทางกลับกันให้ $y\in \alpha(A)\cup\alpha(B)$ แล้ว $y\in \alpha(A)$ หรือ $y\in \alpha(B)$ ถ้า $y\in \alpha(A)$ จะมี $x\in A$ ซึ่ง $y=\alpha(x)$ และถ้า $y\in \alpha(B)$ ก็จะมี $t\in B$ ซึ่ง $y=\alpha(t)$ แต่ $A\subseteq A\cup B$ และ $B\subseteq A\cup B$ ดังนั้น $x, t \in A\cup B$ ซึ่งแสดงว่า ไม่ว่ากรณีใดจะมี $x\in A\cup B$ ซึ่ง $y=\alpha(x)$ จึงได้ว่า $y\in \alpha(A\cup B)$ ทำให้ได้ $\alpha(A)\cup\alpha(B)\subseteq \alpha(A\cup B)$

2. ให้ $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง แล้วเพราะ $A\cap B\subseteq A$ และ $A\cap B\subseteq B$ ดังนั้น $\alpha(A\cap B) \subseteq \alpha(A)$ และ $\alpha(A\cap B)\subseteq \alpha(B)$ ทำให้ได้ $\alpha(A\cap B)\subseteq \alpha(A)\cap\alpha(B)$ จึงเหลือเพียงแสดงว่า $\alpha(A)\cap\alpha(B)\subseteq \alpha(A\cap B)$ จึงให้ $y\in \alpha(A)\cap\alpha(B)$ แล้ว $y\in \alpha(A)$ และ $y\in \alpha(B)$ ดังนั้นจะมี $x_1\in A$ และมี $x_2\in B$ ซึ่ง $y=\alpha(x_1)$ และ $y=\alpha(x_2)$ ทำให้ได้ $\alpha(x_1)=\alpha(x_2)$ และเพราะ $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ดังนั้น $x_1 = x_2$ ซึ่งแสดงว่า $x_1,x_2\in A\cap B$ เพราะฉะนั้นมี $x_1\in A\cap B$ ซึ่ง $y=\alpha(x_1)$ ทำให้ได้ว่า $y\in \alpha(A\cap B)$

ในการพิสูจน์บทกลับ ให้ข้อความ " $\alpha(A\cap B)=\alpha(A)\cap\alpha(B)$ สำหรับทุกๆ เซตย่อย A และ B ของ S" เป็นจริงและจะพิสูจน์ว่า $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง จึงให้ $x_1,x_2\in S$ โดยที่ $x_1\neq x_2$ และนิยามเซต $A = \{x_1\}$ และ $B = \{x_2\}$ แล้ว A และ B เป็นเซตย่อยของ S โดยที่ $\alpha(x_1)\in \alpha(A)$ และ $\alpha(x_2)\in \alpha(B)$ และจะได้โดยข้อความของสมมติฐานว่า $\alpha(A\cap B) = \alpha(A)\cap\alpha(B)$ แต่ $A\cap B$ เป็นเซตว่าง ดังนั้น $\alpha(A)\cap\alpha(B)$ เป็นเซตว่างด้วย จึงทำให้ $\alpha(x_1)\notin \alpha(B)$ ซึ่งแสดงว่า $\alpha(x_1)\neq \alpha(x_2)$ เพราะฉะนั้น $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ❐

สมมติว่า S, T และ U เป็นเซตและ $\alpha : S\rightarrow T$ และ $\beta : T\rightarrow U$ แล้วสำหรับแต่ละ $x\in S$ จะได้ว่า $\alpha(x)\in T$ ซึ่งทำให้การเขียนสัญลักษณ์ $\beta(\alpha(x))$ มีความหมายและหมายถึงสมาชิกใน U ดังนั้นแผนภาพการส่ง

$$x \xrightarrow{\alpha} \alpha(x) \xrightarrow{\beta} \beta(\alpha(x))$$

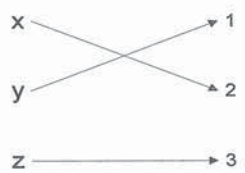
แสดงการส่งสมาชิก $x \in S$ ด้วย $\alpha$ ได้ $\alpha(x)$ และตามด้วยการส่ง $\alpha(x) \in T$ โดย $\beta$ ได้ $\beta(\alpha(x))$ ใน U ทำให้เกิดฟังก์ชันใหม่ $\gamma: S \rightarrow U$ จาก S ไปยัง U กำหนดโดย $\gamma(x) = \beta(\alpha(x))$ สำหรับแต่ละ $x \in S$ เราจึงเรียกฟังก์ชัน $\gamma$ นี้ว่า *ฟังก์ชันประกอบ (composite function)* ของ $\alpha$ และ $\beta$ โดยจะเขียนแทนด้วยสัญลักษณ์ $\beta \circ \alpha$ ดังนั้น

$$(\beta \circ \alpha)(x) = \beta(\alpha(x))$$

สำหรับทุกๆ $x \in S$

ขอให้สังเกตว่าถ้า $\alpha: S \rightarrow T$ แล้ว $\iota_s \circ \alpha = \alpha$ และ $\iota_s \circ \alpha = \alpha$

1.3.10 **ตัวอย่าง** ให้ $S = \{x, y, z\}$ และ $T = \{1, 2, 3\}$ และ $U = \{a, b, c\}$ และนิยาม $\alpha: S \rightarrow T$ และ $\beta: T \rightarrow U$ โดย $\alpha(x) = 2, \alpha(y) = 1, \alpha(z) = 3$, $\beta(1) = b$, $\beta(2) = c$ และ $\beta(3) = a$ แล้ว $\beta \circ \alpha$ เป็นฟังก์ชันจาก S ไปยัง U ที่มีกฎการส่งกำหนดดังนี้ $\beta \circ \alpha(x) = c$, $\beta \circ \alpha(y) = b$




❍

1.3.11 **ตัวอย่าง** ให้ $\alpha: R \rightarrow R$ และ $\beta: R \rightarrow R$ นิยามตามลำดับสำหรับแต่ละ $x \in R$ ดังนี้

$$\alpha(x) = x^2 + 2 \quad \text{และ} \quad \beta(x) = x - 1$$

แล้วสำหรับแต่ละ $x \in R$ จะได้ $\beta \circ \alpha(x) = \beta(\alpha(x)) = \beta(x^2 + 2) = x^2 + 2 - 1 = x^2 + 1$

และ $\alpha \circ \beta(x) = \alpha(\beta(x)) = \alpha(x - 1)) = (x - 1)^2 + 2 = x^2 - 2x + 3$ ❍

ขอให้สังเกตจากตัวอย่าง 1.3.11 ว่า ถ้าเราแทน $x = 0$ จะได้ $(\beta \circ \alpha)(0) = 1$ แต่ $(\alpha \circ \beta)(0) = 3$ ซึ่งแสดงว่าโดยทั่วไป $\alpha \circ \beta$ และ $\beta \circ \alpha$ ไม่เป็นฟังก์ชันเดียวกัน

1.3.12 **ทฤษฎีบท** ให้ S, T, U และ V เป็นเซต $\alpha: S \rightarrow T$, $\beta: T \rightarrow U$ และ $\gamma: U \rightarrow V$ แล้ว $\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha$

**บทพิสูจน์** เพราะว่า $\beta \circ \alpha : S \rightarrow U$ และ $\gamma \circ \beta: T \rightarrow V$ ดังนั้น $\gamma \circ (\beta \circ \alpha) : S \rightarrow V$ และ $(\gamma \circ \beta) \circ \alpha: S \rightarrow V$ และเพื่อแสดงว่า $\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha$ เราจึงให้ $x \in S$ แล้วโดยนิยาม

ของฟังก์ชันประกอบ จะได้ $((\gamma \circ \beta) \circ \alpha)(x) = (\gamma \circ \beta)(\alpha(x)) = \gamma(\beta(\alpha(x)) = \gamma((\beta \circ \alpha)(x)) = (\gamma \circ (\beta \circ \alpha))(x)$ ซึ่งเป็นอันจบการพิสูจน์ ❐

ทฤษฎีบทต่อไป พิสูจน์ได้โดยตรงจากบทนิยาม จึงขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

1.3.13 **ทฤษฎีบท** ให้ S, T และ U เป็นเซต $\alpha : S \rightarrow T$ และ $\beta : T \rightarrow U$

1. ถ้า $\alpha$ และ $\beta$ ต่างเป็นฟังก์ชันหนึ่งต่อหนึ่งแล้ว $\beta \circ \alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง
2. ถ้า $\alpha$ และ $\beta$ ต่างเป็นฟังก์ชันทั่วถึงแล้ว $\beta \circ \alpha$ เป็นฟังก์ชันทั่วถึง
3. ถ้า $\alpha$ และ $\beta$ ต่างเป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึงแล้ว $\beta \circ \alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง ❐

1.3.14 **ทฤษฎีบท** ให้ S, T และ U เป็นเซต $\alpha : S \rightarrow T$ และ $\beta : T \rightarrow U$

1. ถ้า $\beta \circ \alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง แล้ว $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง
2. ถ้า $\beta \circ \alpha$ เป็นฟังก์ชันทั่วถึงแล้ว $\beta$ เป็นฟังก์ชันทั่วถึง
3. ถ้า $\beta \circ \alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง แล้ว $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและ $\beta$ เป็นฟังก์ชันทั่วถึง

**บทพิสูจน์** 1. ให้ $\beta \circ \alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและให้ $x_1, x_2 \in S$ โดยที่ $\alpha(x_1) = \alpha(x_2)$ แล้วเพราะ $\alpha(x_1)$ และ $\alpha(x_2)$ เป็นสมาชิกตัวเดียวกันใน T ดังนั้น $\beta(\alpha(x_1)) = \beta(\alpha(x_2))$ นั่นคือ $(\beta \circ \alpha)(x_1) = (\beta \circ \alpha)(x_2)$ ทำให้ได้โดยความเป็นฟังก์ชันหนึ่งต่อหนึ่งของ $\beta \circ \alpha$ ว่า $x_1 = x_2$ เพราะฉะนั้น $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

2. ให้ $\beta \circ \alpha$ เป็นฟังก์ชันทั่วถึงและให้ $y \in U$ แล้วเพราะว่า $\beta \circ \alpha : S \rightarrow U$ เป็นฟังก์ชันทั่วถึง ดังนั้นจะมี $x \in S$ ซึ่ง $y = (\beta \circ \alpha)(x)$ แต่ $(\beta \circ \alpha)(x) = \beta(\alpha(x))$ และ $\alpha(x)$ เป็นสมาชิกของ T จึงได้ว่ามี $t = \alpha(x) \in T$ ซึ่ง $y = \beta(t)$ เพราะฉะนั้น $\beta$ เป็นฟังก์ชันทั่วถึง

3. เป็นผลจากข้อ 1 และข้อ 2 ❐

เราสังเกตว่าถ้า A และ B เป็นเซตและ $f : A \rightarrow B$ แล้วความสัมพันธ์ผกผัน $f^{-1} \subseteq B \times A$ ของ f ซึ่งกำหนดโดย

$$(x, y) \in f \Leftrightarrow (y, x) \in g \quad [\text{ซึ่งสมมูลกับ} \quad y = f(x) \Leftrightarrow x = f^{-1}(y)]$$

อาจไม่เป็นฟังก์ชัน เพราะแต่ละสมาชิกใน B อาจมีการจับคู่กับสมาชิกใน A มากกว่า 1 ตัว แต่ถ้าแต่ละสมาชิกใน B จับคู่กับสมาชิกใน A ได้อย่างมากเพียงหนึ่งเดียวแล้ว $f^{-1}$ จะเป็นฟังก์ชันจาก B ไปยัง A เราจึงได้ทฤษฎีบทต่อไปนี้ซึ่งจะขอละการพิสูจน์ไว้เป็นแบบฝึกหัดสำหรับผู้อ่าน

**1.3.15 ทฤษฎีบท** ให้ A และ B เป็นเซตและ $f : A \rightarrow B$ แล้ว

1. $f^{-1} : B \rightarrow A$ ก็ต่อเมื่อ f เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง
2. ถ้า $f^{-1} : B \rightarrow A$ แล้ว $f^{-1}$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง
3. ถ้า $f^{-1} : B \rightarrow A$ แล้ว $f^{-1} \circ f = \iota_A$ และ $f \circ f^{-1} = \iota_B$ ❐

**หมายเหตุ** ถ้าความสัมพันธ์ผกผัน $f^{-1}$ ของ f เป็นฟังก์ชัน เราจะเรียก $f^{-1}$ ว่า*ฟังก์ชันผกผัน (inverse function)* ของ f

## แบบฝึกหัด 1.3

1. ให้ $S = \{1, 2, 3, 4\}$ จงหาจำนวนฟังก์ชันทั้งหมดจาก S ไปยังเซตในข้อต่อไปนี้ พร้อมอธิบายเหตุผลประกอบ

   1.1 $\{x\}$ 1.2 $\{x, y\}$ 1.3 $\{x, y, z\}$

2. ให้ $f : A \rightarrow B$ และ $g : C \rightarrow D$ และนิยาม $h(x) = \begin{cases} f(x) & \text{ถ้า } x \in A \\ g(x) & \text{ถ้า } x \in C \end{cases}$ จงพิสูจน์ว่าเงื่อนไขที่ทำให้ $h : A \cup C \rightarrow B \cup D$ คือ $A \cap C = \phi$
3. ให้ A, B และ C เป็นเซต $\alpha, \beta : A \rightarrow B$ และ $\gamma : B \rightarrow C$ จงพิสูจน์ว่าถ้า $\gamma \circ \alpha = \gamma \circ \beta$ และ $\gamma$ เป็นฟังก์ชันหนึ่งต่อหนึ่งแล้ว $\alpha = \beta$
4. ให้ Z แทนเซตของจำนวนเต็มทั้งหมด $f : Z \rightarrow Z \times Z$ และ $g : Z \times Z \rightarrow Z$ กำหนดตามลำดับโดย $f(a) = (a+3, 1)$ และ $g(a, b) = a + b$ สำหรับแต่ละ $a, b \in Z$ จงแสดงว่า

   4.1 f เป็นฟังก์ชันหนึ่งต่อหนึ่ง แต่ไม่เป็นฟังก์ชันทั่วถึง

   4.2 g เป็นฟังก์ชันทั่วถึง แต่ไม่เป็นฟังก์ชันหนึ่งต่อหนึ่ง

   4.3 $g \circ f$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง

5. ให้ A, B และ C เป็นเซต $\alpha : A \rightarrow B$ และ $\beta : B \rightarrow C$ จงพิสูจน์ว่าถ้า $\beta \circ \alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงแล้ว $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและ $\beta$ เป็นฟังก์ชันทั่วถึง
6. จงพิสูจน์ทฤษฎีบท 1.3.13 และ 1.3.15
7. ให้ $f : X \rightarrow Y$, $A \subseteq X$ และ $C \subseteq Y$ จงแสดงว่า "f เป็นฟังก์ชันหนึ่งต่อหนึ่ง" เป็นเงื่อนไขเพียงพอและเงื่อนไขจำเป็นสำหรับข้อความ "$A = f^{-1}(f(A))$ สำหรับทุก ๆ $A \subseteq X$"
8. จงพิสูจน์ว่า ข้อความในข้อต่อไปนี้เป็นจริงหรือไม่

   8.1 ถ้า $f : X \rightarrow Y$ เป็น surjective แล้ว $Y - f(A) \subseteq f(X - A)$ สำหรับทุกๆ $A \subseteq X$

   8.2 ถ้า $f : X \rightarrow Y$ เป็น surjective แล้ว $f(X - A) \subseteq Y - f(A)$ สำหรับทุกๆ $A \subseteq X$

   8.3 ให้ $f : X \rightarrow Y$ และ $g : X \rightarrow Y$ ถ้า $f \subseteq g$ แล้ว $f = g$

## 1.3 การดำเนินการ

ดังกล่าวแล้วว่า ในการศึกษาโครงสร้างพีชคณิตในวิชาพีชคณิตนามธรรม สิ่งแรกที่เกี่ยวข้องและมีความสำคัญยิ่งคือการดำเนินการ เพราะโครงสร้างพีชคณิตประกอบด้วยเซตที่ไม่เป็นเซตว่างเซตหนึ่งกับการดำเนินการบนเซตนั้น ในหัวข้อนี้จึงจะศึกษาความหมายและสมบัติทั่วไปของการดำเนินการ เพื่อเป็นพื้นฐานสำหรับการศึกษาโครงสร้างพีชคณิตที่จะกล่าวถึงในบทต่อๆ ไป

ให้ A เป็นเซต ในหัวข้อความสัมพันธ์ ได้แนะนำเซตผลคูณคาร์ทีเซียน $A \times A$ และถ้าพิจารณา A และ $A \times A$ เป็นเซต เราก็สามารถหาผลคูณคาร์ทีเซียน $A \times (A \times A)$ และเมื่อดำเนินการเช่นเดียวกันนี้ต่อไปเรื่อยๆ เราก็จะได้ผลคูณคาร์ทีเซียน $A \times A$, $A \times (A \times A)$, $A \times (A \times (A \times A))$, . . . ถ้าใช้สัญลักษณ์ $A^1$ แทน A, $A^2$ แทน $A \times A$, $A^3$ แทน $A \times (A \times A)$ . . . เราก็จะมีสัญลักษณ์ $A^n$ แทนผลคูณคาร์ทีเซียน $A \times \ldots \times A$ ทั้งหมด n ครั้ง สำหรับแต่ละจำนวนเต็มบวก n

สังเกตว่าเมื่อนำจำนวนเต็ม 2 จำนวนมาบวกกันจะได้จำนวนเต็มตัวที่สาม และแต่ละคู่ของจำนวนเต็มก็จะให้ผลบวกเป็นจำนวนเต็มตัวที่สามเพียงหนึ่งเดียวเท่านั้น และนั่นแสดงว่า "การบวก" ของจำนวนเต็มเป็นฟังก์ชันจาก $Z^2$ ไปยัง Z เราเรียกฟังก์ชันในลักษณะเช่นนี้ว่า "การดำเนินการ"

ให้ A เป็นเซตและ n เป็นจำนวนเต็มบวก *การดำเนินการลำดับชั้นที่ n (n-ary operation)* บน A คือฟังก์ชัน $f : A^n \rightarrow A$ และเรียก n ว่า *ค่าลำดับชั้น (arity)* ของการดำเนินการ

ถ้า n = 1, 2, 3 เรามีชื่อเรียก f เฉพาะว่า *การดำเนินการเอกภาค (unary-operation)* *การดำเนินการทวิภาค (binary operation)* และ *การดำเนินการไตรภาค (ternary operation)* ตามลำดับ

ตัวอย่างการดำเนินการที่เราคุ้นเคยกันเป็นอย่างดีได้แก่ การบวก + การลบ – การคูณ × และการหาร ÷ บนเซตของจำนวน(จริง) ซึ่งต่างเป็นการดำเนินการทวิภาค เพราะแต่ละคู่ของจำนวนจริง จะกำหนดจำนวนจริงตัวหนึ่งและเพียงตัวเดียวเท่านั้นที่จะเป็น "ผลบวก" "ผลต่าง" "ผลคูณ" หรือ "ผลหาร" สำหรับแต่ละกรณี

โดยมากเราคุ้นเคยกับการดำเนินการทวิภาค ซึ่งอาจใช้สัญลักษณ์ที่ต่างจาก การบวก + การลบ – การคูณ × และการหาร ÷ บนเซตของจำนวน เช่นอาจแทนการดำเนินการทวิภาคด้วย * หรือ ∘ (สำหรับฟังก์ชันประกอบ) หรือ $\cup$ หรือ $\cap$ (ในเรื่องเซต) เป็นต้น

ให้ A เป็นเซตและ * เป็นการดำเนินการทวิภาคบน A นั่นคือ * ส่งแต่ละ คู่ (m, n) ใน $A^2$ ไปยัง *(m, n) ใน A ซึ่งเรานิยมแทนภาพ *(m, n) ด้วย m*n

ตัวอย่างเช่น * : $N^2 \rightarrow N$ นิยามโดย (m, n) $\rightarrow m^n$ สำหรับแต่ละคู่ (m, n) ของจำนวนธรรมชาติใน $N^2$ เรานิยมเขียนแทน $m*n = m^n$ เป็นต้น

ขอให้สังเกตจากนิยามของการดำเนินการว่า แม้ "การคูณ" จะเป็นการดำเนินการบน Z แต่ "การหาร" ไม่เป็นการดำเนินการบน Z เพราะว่า ÷(1, 2) = 1÷2 ไม่เป็นสมาชิกของ Z นอกจากนี้ถ้า $S \neq \phi$ และให้ M(S) แทนเซตของฟังก์ชันทั้งหมดจาก S ไปยัง S แล้ว $\beta \circ \alpha$ เป็นสมาชิกเพียงหนึ่งเดียวสำหรับแต่ละคู่ $\alpha$ และ $\beta$ ใน M(S) ซึ่งแสดงว่าฟังก์ชันประกอบเป็นการดำเนินการบน M(S)

ถ้า $S \neq \phi$ เป็นเซตจำกัดและ * เป็นการดำเนินการทวิภาคบน S เราอาจแสดงภาพของ * ทั้งหมดโดยตาราง เราสร้างตารางดังกล่าวโดยเริ่มด้วยการสร้างสี่เหลี่ยมจัตุรัสแทนตาราง แล้วเขียน * ลงบนมุมซ้าย สมาชิกทั้งหมดของ S เรียงลำดับให้เป็นแถวอยู่บนสุดและเป็นหลักอยู่ทางซ้ายสุดของตาราง สำหรับแต่ละ a, b $\in$ S เราเขียนภาพ a*b ณ ตำแหน่งที่ตัดกันของแถวที่มี a อยู่ทางซ้ายสุดกับหลักที่มี b อยู่บนสุด ดังตัวอย่างตารางข้างล่างนี้เป็นการนิยามการดำเนินการทวิภาค * บน S = {u, v, w} และจากตารางเราได้ว่า u*v = w, v*u = v เป็นต้น

| * | u | v | w |
|---|---|---|---|
| u | u | w | w |
| v | v | w | v |
| w | w | u | v |

**ตาราง 1.4.1**

**หมายเหตุ** ตารางแสดงการนิยามการดำเนินการทวิภาคบนเซตจำกัด S ขนาด n จะประกอบด้วย $n^2$ ตำแหน่ง และหากเราสร้างตารางสี่เหลี่ยมจัตุรัสที่ประกอบด้วย $n^2$ ตำแหน่งซึ่งมีตำแหน่งหนึ่งตำแหน่งใดที่เขียนสมาชิกของ S ต่างไปจากตารางเดิม ตารางใหม่ที่สร้างขึ้นจะเป็นการนิยามการดำเนินการทวิภาคบน S ที่ต่างจากการดำเนินการเดิม

ในการศึกษาการดำเนินการทวิภาค เราสนใจการดำเนินการที่สอดคล้องสมบัติดังจะกล่าวในบทนิยามต่อไปนี้

1.4.1 **บทนิยาม** ให้ $* : S^2 \rightarrow S$ เป็นการดำเนินการทวิภาคบนเซต S

1. เรากล่าวว่า * สอดคล้อง *กฎการเปลี่ยนหมู่ (associative law)* บน S ถ้า $a*(b*c) = a*(b*c)$ สำหรับทุกๆ $a, b, c \in S$
2. เรากล่าวว่า * สอดคล้อง *กฎการสลับที่ (commutative law)* ถ้า $a*b = b*a$ สำหรับทุกๆ $a, b \in S$
3. เรากล่าวว่า $e \in S$ เป็น *เอกลักษณ์* (identity) ของ S ภายใต้ * ถ้า $a*e = a = e*a$ สำหรับทุกๆ $a \in S$
4. ถ้ามี $e \in S$ เป็นเอกลักษณ์ของ S ภายใต้ * และ $a, b \in S$ เรากล่าวว่า b เป็น *ตัวผกผัน (inverse)* ของ a ใน S ภายใต้ * ถ้า $a*b = e = b*a$

ตัวอย่างเช่น การบวกและการคูณบนเซตของจำนวนจริงสอดคล้องกฎการเปลี่ยนหมู่และกฎการสลับที่ และมี 0 และ 1 เป็นเอกลักษณ์ภายใต้การบวกและการคูณตามลำดับ แต่ "การลบ" บนเซตของจำนวนจริงไม่สอดคล้องกฎการเปลี่ยนหมู่และกฎการสลับที่ เพราะว่า $2 - (3 - 4) = 2 - (-1) = 3$ ในขณะที่ $(2 - 3) - 4 = (-1) - 4 = -4$ หรือ $2 - 3 = -1$ แต่ $3 - 2 = 1$ ตามลำดับ

การดำเนินการ $* : N^2 \rightarrow N$ บนเซตของจำนวนธรรมชาติซึ่งนิยามโดย $(m, n) \rightarrow m^n$ สำหรับแต่ละคู่ (m, n) ของจำนวนธรรมชาติไม่สอดคล้องกฎการเปลี่ยนหมู่ เพราะว่า $2*(3*2) = 2*(3^2) = 2*9 = 2^9 = 512$ แต่ $(2*3)*2 = (2^3)*2 = 8*2 = 8^2 = 64$

การดำเนินการที่นิยามดังตาราง 1.4.1 ไม่สอดคล้องกฎการสลับที่ เพราะว่า $u*v = w$ แต่ $v*u = v$

1.4.2 **ตัวอย่าง** ให้ S, T, U และ V เป็นเซต $\alpha : S \rightarrow T$, $\beta : T \rightarrow U$ และ $\gamma : U \rightarrow V$ แล้วสำหรับแต่ละ $x \in S$ จะได้ว่า

$$(\gamma \circ (\beta \circ \alpha))(x) = \gamma((\beta \circ \alpha)(x)) = \gamma(\beta(\alpha(x)) = (\gamma \circ \beta)(\alpha(x))$$
$$= ((\gamma \circ \beta) \circ \alpha)(x)$$

ซึ่งแสดงว่า $\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha$ นั่นคือฟังก์ชันประกอบ $\circ$ เป็นการดำเนินการที่สอดคล้องกฎการเปลี่ยนหมู่ นอกจากนี้ฟังก์ชันเอกลักษณ์ยังเป็นเอกลักษณ์บนเซตของฟังก์ชันภายใต้การดำเนินการฟังก์ชันประกอบ ❍

ถ้า a เป็นจำนวนเต็ม เราทราบว่า $a + (-a) = 0 = -a + a$ และเพราะว่าตัวผกผันต้องเป็นสมาชิกของเซตนั้นด้วย จึงได้ว่าแต่ละจำนวนเต็มมีตัวผกผันภายใต้การบวก แต่มีจำนวนเต็มบวกมากมายไม่มีตัวผกผันภายใต้การบวกบนเซตของจำนวนเต็มบวกทั้งหมด

นอกจากนี้ 1 และ –1 เท่านั้นที่มีตัวผกผันภายใต้การคูณบนเซต Z ของจำนวนเต็มทั้งหมด ในขณะที่ทุกๆ จำนวนจริงที่ไม่ใช่ศูนย์ จะมีตัวผกผันภายใต้การคูณบนเซต R ของจำนวนจริงทั้งหมด เป็นต้น

ในการกล่าวถึงเซตๆ หนึ่งที่มีการนิยามการดำเนินการทวิภาคบนเซตนั้น ถ้าการนิยามกล่าวในเชิงนามธรรม หรือไม่มีการกล่าวถึงการดำเนินการทวิภาคสองตัวที่ต่างกัน เรานิยมละสัญลักษณ์ของการดำเนินการ กล่าวคือจะเขียน ab แทนภาพของการดำเนินการและอ่านว่า "ผลคูณของ a และ b" สำหรับแต่ละคู่สมาชิก a และ b ในเซตนั้น

1.4.3 **บทนิยาม** ให้ S เป็นเซตซึ่ง $S \neq \phi$ และมีการดำเนินการทวิภาคนิยามบน S สำหรับแต่ละจำนวนเต็มบวก n เราจะใช้สัญลักษณ์ $\prod_{i=1}^{n} a_i$ แทนผลคูณในอันดับ $a_1, a_2, \ldots, a_n$ ของสมาชิก $a_1, a_2, \ldots, a_n$ ใน S และกำหนดผลคูณในรูปอุปนัยดังนี้

$$\prod_{i=1}^{n} a_i = (\prod_{i=1}^{n-1} a_i)a_n$$

จากบทนิยาม 1.4.2 จะได้ว่า $\prod_{i=1}^{1} a_i = a_1$, $\prod_{i=1}^{2} a_i = a_1a_2$, $\prod_{i=1}^{3} a_i = (a_1a_2)a_3$, $\prod_{i=1}^{4} a_i = ((a_1a_2)a_3)a_4, \ldots$ เป็นต้น

นอกจากนี้เราอาจสังเกตว่า ถ้าการดำเนินการสอดคล้องกฎการเปลี่ยนหมู่ ซึ่งแสดงว่าสัญลักษณ์ $(a_1a_2)a_3$ และ $a_1(a_2a_3)$ แทนสมาชิกตัวเดียวกันในเซตนั้น ทำให้เราอาจละวงเล็บในการ

เขียนผลคูณของ 3 สมาชิก แล้วการเขียนผลคูณ $\prod_{i=1}^{n} a_i$ เมื่อ $n \geq 3$ อาจจะละวงเล็บได้เช่นเดียวกับกรณี n = 3 หรือไม่ เราจะแสดงความจริงนี้ในชื่อว่า "การวางนัยทั่วไปของกฎการเปลี่ยนหมู่"

### 1.4.4 ทฤษฎีบทการวางนัยทั่วไปของกฎการเปลี่ยนหมู่

ให้ S เป็นเซตซึ่ง $S \neq \phi$ และมีการดำเนินการทวิภาคนิยามบน S ซึ่งสอดคล้องกฎการเปลี่ยนหมู่ ถ้า $a_1, a_2, \ldots, a_n$ เป็นสมาชิก n ตัวใน S สำหรับจำนวนเต็มบวก n แล้วการเปลี่ยนหมู่ในอันดับ $a_1, a_2, \ldots, a_n$ จะเป็นเช่นใดก็ตาม ผลคูณของสมาชิก n ตัวนี้ในอันดับ $a_1, a_2, \ldots, a_n$ จะเท่ากันและเท่ากับ $\prod_{i=1}^{n} a_i$

**บทพิสูจน์** เราจะแสดงว่าโดยอุปนัยเชิงคณิตศาสตร์แบบเข้ม (ดูหัวข้อ 2.3) บนจำนวนเต็มบวก $n \geq 3$ ว่าแต่ละแบบของการเปลี่ยนหมู่ในผลคูณของสมาชิก n ตัวนี้ในอันดับ $a_1, a_2, \ldots, a_n$ เท่ากับ $\prod_{i=1}^{n} a_i$ ซึ่งจะทำให้ได้ว่าผลคูณของทุกแบบของการเปลี่ยนหมู่เท่ากัน

โดยกฎการเปลี่ยนหมู่ของการดำเนินการบน S ทำให้ได้ว่าทฤษฎีบทเป็นจริงสำหรับ n = 3 จึงสมมติว่าทฤษฎีบทเป็นจริงสำหรับผลคูณของสมาชิก m ตัวสำหรับ $1 \leq m < n$ และให้ $a_1, a_2, \ldots, a_n$ เป็นสมาชิก n ตัวใน S และให้ x แทนผลคูณของสมาชิก n ตัวในอันดับ $a_1, a_2, \ldots, a_n$ ในแบบใดแบบหนึ่งที่กำลังพิจารณา ดังนั้น x จึงเป็นภาพของการดำเนินการทวิภาคนี้ ทำให้ได้ว่ามี c และ d ใน S ซึ่ง x = cd และจากข้อสมมติจะได้ว่ามี k ซึ่ง $1 \leq k < n$ และ c เป็นผลคูณของสมาชิก k ตัวในอันดับ $a_1, a_2, \ldots, a_k$ และ d เป็นผลคูณของสมาชิก $n - k$ ตัวในอันดับ $a_{k+1}, a_{k+2}, \ldots, a_n$ และเพราะว่า $1 \leq k < n$ และ $1 \leq n-k < n$ ดังนั้นโดยสมมติฐานของอุปนัยเชิงคณิตศาสตร์อย่างเข้ม จะได้ว่า $c = \prod_{i=1}^{k} a_i$ และ $d = \prod_{i=k+1}^{n} a_i$ ซึ่งทำให้ได้

$$x = cd = (\prod_{i=1}^{k} a_i)(\prod_{i=k+1}^{n} a_i) = (\prod_{i=1}^{k} a_i)[(\prod_{i=k+1}^{n-1} a_i)\, a_n] = [(\prod_{i=1}^{k} a_i)(\prod_{i=k+1}^{n-1} a_i)]\, a_n =$$

และเพราะ $1 \leq n-1 < n$ เราจะได้โดยสมมติฐานของอุปนัยเชิงคณิตศาสตร์ อีกครั้งว่า

$$(\prod_{i=1}^{k} a_i)(\prod_{i=k+1}^{n-1} a_i) = \prod_{i=1}^{n-1} a_i$$

ดังนั้น $x = (\prod_{i=1}^{n-1} a_i)\, a_n = \prod_{i=1}^{n} a_i$ ซึ่งเป็นอันจบการพิสูจน์ ❐

โดยทฤษฎีบท 1.4.4 การคูณสมาชิก n ตัวใดๆ เมื่อ n เป็นจำนวนเต็มบวก เราอาจละวงเล็บโดยเขียนผลคูณ $\prod_{i=1}^{n} a_i$ ได้เป็น $a_1a_2 \ldots a_n$

ในทำนองเดียวกันกับทฤษฎีบทการวางนัยทั่วไปของกฎการเปลี่ยนหมู่ เราก็สามารถกล่าวถึงการวางนัยทั่วไปของกฎการสลับที่ ดังจะแสดงในทฤษฎีบทต่อไป

1.4.5 **ทฤษฎีบท** ให้ S เป็นเซตซึ่ง $S \neq \phi$ และมีการดำเนินการทวิภาคนิยามบน S ซึ่งสอดคล้องกฎการเปลี่ยนหมู่และการสลับที่ ถ้า $a_1, a_2, \ldots, a_n$ เป็นสมาชิก n ตัวใน S สำหรับจำนวนเต็มบวก n แล้ว ผลคูณของ $a_1, a_2, \ldots, a_n$ ในอันดับใดๆ ก็ตามจะเท่ากัน

**บทพิสูจน์** โดยทฤษฎีบทการวางนัยทั่วไปของกฎการเปลี่ยนหมู่ ทำให้เขียนผลคูณของ $a_1, a_2, \ldots, a_n$ ได้เป็น $a_1a_2 \ldots a_n$ และโดยกฎการสลับที่ จะได้

$$a_1a_2 \ldots a_n = a_1a_2 \ldots a_{k-1}(a_ka_{k+1})\, a_{k+2} \ldots a_n = a_1a_2 \ldots a_{k-1}(a_{k+1}a_k)\, a_{k+2} \ldots a_n$$

ซึ่งแสดงว่า ไม่ว่าจะนำ $a_1, a_2, \ldots, a_n$ มาคูณกันในอันดับใดๆ ก็ตาม ก็สามารถประยุกต์กฎการเปลี่ยนหมู่ทำให้ได้ผลคูณอยู่ในรูปผลคูณในอันดับ $a_1, a_2, \ldots, a_n$ ได้เสมอ ซึ่งทำให้ผลคูณในอันดับต่างๆ นั้นเท่ากันและเท่ากับ $a_1a_2 \ldots a_n$ ❐

ในทฤษฎีบท 1.4.5 ถ้า $a_1 = a_2 = \ldots = a_n = a$ แล้ว $\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a = aa \ldots a$ (n ครั้ง) ในกรณีเช่นนี้ เราจะใช้สัญลักษณ์ $a^n$ แทน $\prod_{i=1}^{n} a = aa \ldots a$ โดยกำหนดค่า $a^n$ ในรูปอุปนัยโดย

$$a^n = \prod_{i=1}^{n} a = (\prod_{i=1}^{n-1} a)\, a = a^{n-1}a$$

ทำให้ได้ $a^1 = a$, $a^2 = aa$, $a^3 = aaa$, $a^4 = aaaa, \ldots$ เป็นต้น

## แบบฝึกหัด 1.4

1. ถ้ากำหนด * บน Z โดย $a*b = \frac{a+b}{ab}$ สำหรับแต่ละ $a, b \in Z$ แล้ว * ไม่เป็นการดำเนินการบน Z เพราะมีจำนวนเต็ม a และ b ซึ่ง $\frac{a+b}{ab}$ ไม่เป็นจำนวนเต็ม ตัวอย่างเช่น $\frac{2+3}{(2)(3)} = \frac{5}{6}$ ไม่เป็นจำนวนเต็ม

จงพิจารณาว่าการนิยาม * บน Z ที่กำหนดในแต่ละข้อต่อไปนี้เป็นการดำเนินการบน Z หรือไม่ เพราะเหตุใด

1.1 $a*b = ab + 1$ 1.2 $a*b = \frac{a+b}{2}$ 1.3 $a*b = 2^{ab}$

1.4 $a*b = \sqrt{ab}$ 1.5 $a*b = 3$ 1.6 $a*b = a$

2. จงพิจารณาว่าการนิยาม * บนเซตที่กำหนดในแต่ละข้อต่อไปนี้ เป็นการดำเนินการบนเซตนั้น หรือไม่ เพราะเหตุใด

2.1 $a*b = \sqrt{|ab|}$ บน Q 2.2 $a*b = a \ln b$ บนเซตของจำนวนจริงบวก

2.3 $a*b$ เป็นรากของสมการ $x^2 - a^2b^2 = 0$ บนเซตของจำนวนจริงทั้งหมด

2.4 $a*b = |a-b|$ บนเซตของจำนวนเต็มที่ไม่ใช่จำนวนลบ

3. จงแสดงการตรวจสอบว่า * ในข้อ 1 และข้อ 2 เฉพาะที่เป็นการดำเนินการ สอดคล้องสมบัติใดบ้างของสมบัติที่นิยามไว้ในบทนิยาม 1.4.1

4. จงเติมตารางต่อไปนี้ให้สมบูรณ์ ตามเงื่อนไขที่กำหนดให้ในแต่ละข้อ

| * | u | v |
|---|---|---|
| u | | |
| v | | |

4.1 เพื่อให้ u เป็นเอกลักษณ์ และทำได้ทั้งหมดกี่วิธี

4.2 เพื่อให้ u และ v เป็นเอกลักษณ์ และพิจารณาว่าจะทำได้หรือไม่

5. จงเติมตารางข้างลางนี้ให้สมบูรณ์ เพื่อให้ * สอดคล้องกฎการสลับที่ มีเอกลักษณ์ และแต่ละสมาชิกมีตัวผกผัน

| * | w | x | y | z |
|---|---|---|---|---|
| w | y | | | x |
| x | z | w | | |
| y | | | | |
| z | | | | w |

6. จงแสดงการตรวจสอบว่าการดำเนินการ * บน R ที่กำหนดในแต่ละข้อต่อไปนี้สอดคล้องสมบัติใดบ้างของสมบัติที่นิยามไว้ในบทนิยาม 1. 4.1

   6.1 $a*b = a + b + 1$ 6.2 $a*b = a + 2b + 4$

   6.3 $a*b = a + 2b - ab$ 6.4 $a*b = |a+b|$

7. จงแสดงว่า จะมีเอกลักษณ์ได้เพียงตัวเดียวเท่านั้นบนแต่ละเซต ภายใต้แต่ละการดำเนินการที่กำหนดบนเซตนั้นๆ

8. ให้ * เป็นการดำเนินการบนเซต S และ T เป็นเซตย่อยของ S ซึ่งมีสมบัติปิดภายใต้ * (นั่นคือ $a*b \in T$ สำหรับทุกๆ a, b $\in T$ จงแสดงว่าถ้า * สอดคล้องกฎการเปลี่ยนหมู่ (กฎการสลับที่) บน S แล้ว * สอดคล้องกฎการเปลี่ยนหมู่ (กฎการสลับที่) บน T

9. ให้ * เป็นการดำเนินการซึ่งสอดคล้องกฎการเปลี่ยนหมู่บนเซต S จงแสดงว่า

$$a_1*(a_2*(a_3*a_4)) = a_1*((a_2*a_3)*a_4) = (a_1*(a_2*a_3))*a_4$$
$$= (a_1*a_2)*(a_3*a_4) = ((a_1*a_2)*a_3)*a_4$$

   สำหรับทุกๆ $a_1, a_2, a_3, a_4 \in S$

10. ให้ * เป็นการดำเนินการบนเซต S และมี $e \in S$ เป็นเอกลักษณ์ภายใต้ * จงแสดงว่าถ้าสมการ $(a*b)*(c*d) = (a*c)*(b*d)$ เป็นจริง สำหรับทุกๆ a, b, c, d $\in S$ แล้ว * สอดคล้องกฎการเปลี่ยนหมู่และกฎการสลับที่บน S

11. ให้ S เป็นเซตที่มีสมาชิกมากกว่า 1 ตัวและนิยามการดำเนินการ *บน S โดย $a*b = b$ สำหรับทุกๆ a, b $\in S$ จงแสดงว่า * ไม่สอดคล้องกฎการสลับที่และไม่มีสมาชิกตัวใน S เป็นเอกลักษณ์ภายใต้ *

12. ให้ S เป็นเซตที่ไม่ใช่เซตว่างและ * เป็นการดำเนินการบน S ซึ่งสอดคล้องกฎการสลับที่ จงแสดงว่า $(ab)^n = a^n b^n$ สำหรับทุกๆ a, b $\in S$ และทุกๆ จำนวนเต็มบวก n

# บทที่ 2
# ทฤษฎีจำนวนเบื้องต้น
# INTRODUCTION TO NUMBER THEORY

ในการศึกษาวิชาพีชคณิตนามธรรม ตัวอย่างสำคัญและตัวอย่างที่ยกให้เห็นได้อย่างชัดเจนส่วนใหญ่เป็นตัวอย่างเกี่ยวกับจำนวน โดยเฉพาะอย่างยิ่งระบบจำนวนเต็ม ในบทนี้จึงขอทบทวนทฤษฎีบทที่เป็นมูลฐานสำคัญในระบบจำนวนเต็ม

## 2.1 จำนวนธรรมชาติกับหลักอุปนัยเชิงคณิตศาสตร์

มนุษย์เราประดิษฐ์จำนวนขึ้นมาก็เพื่อใช้บอกขนาดของความมาก-น้อยของสิ่งต่างๆ เช่นใช้บอกว่ามีสัตว์เลี้ยงอยู่เท่าใด มีเนื้อที่เพาะปลูกอยู่กี่ไร่ จะเห็นว่าสิ่งของที่เราบอกความมาก-น้อยมักเป็นสิ่งของเต็มหน่วยเช่น มีวัว 4 ตัว มีช้าง 3 เชือก ส้ม 1 กิโลกรัมมี 10 ลูก เป็นต้น และเพราะจำนวนเป็นสิ่งประดิษฐ์ จึงเป็นสิ่งนามธรรมหรือสัญลักษณ์ที่ไม่มีจริงในโลก แต่มนุษย์มักไม่รู้สึกว่าจำนวนเต็มหน่วยเหล่านี้เป็นสิ่งนามธรรม การใช้นามธรรมดังกล่าวนี้จึงถือเป็นความสำเร็จอันยิ่งใหญ่ของมวลมนุษยชาติที่สามารถดึงกระบวนการนามธรรมออกมาใช้เสมือนเป็นรูปธรรมที่มีอยู่ในโลกจริงๆ และอาจสัมผัสได้ เราจึงเรียกจำนวนที่ประดิษฐ์ขึ้นเพื่อใช้บอกขนาดนี้ว่าจำนวนธรรมชาติหรือจำนวนนับและเขียนแทนเซตของจำนวนธรรมชาติทั้งหมดด้วยสัญลักษณ์ N นั่นคือ

$$N = \{1, 2, 3, \ldots\}$$

อย่างไรก็ตามเพราะว่ามนุษย์เป็นสัตว์สังคม การอยู่ร่วมกันจึงอาจมีการแลกเปลี่ยนสิ่งของ เครื่องใช้ สัตว์เลี้ยง หรือแม้แต่อาหาร ซึ่งในยุคปัจจุบันเราเรียกว่า "การค้าขาย" และในการค้าขายจะมีการไว้วางใจให้สินเชื่อหรือของแลกเปลี่ยนล่วงหน้า เมื่อประมาณ 1000 ปีก่อนหน้านี้มนุษย์ใช้สัญลักษณ์ "จำนวนลบ" ในลักษณะเป็นตัวช่วยคำนวณเกี่ยวกับการให้สินเชื่อ เช่นนาย ก. มีสินเชื่อกับนาย ข. $-a$ หน่วย หมายความว่าถ้านาย ข. นำจำนวนสินค้าจำนวน $a$ หน่วยมาคืนให้ ก็จะลบล้างสินเชื่อหมดไป คนธรรมดาทั่วไปในสมัยนั้นที่ไม่อยู่ในวงการค้าจะรู้สึกว่าสัญลักษณ์ -1, -2, . . . เหล่านี้เป็นนามธรรมมากๆ แต่ในปัจจุบันนี้ เราเรียกจำนวนเหล่านี้ว่า "จำนวนเต็มลบ" และไม่รู้สึกว่าจำนวนเหล่านี้เป็นนามธรรมอีกต่อไป ดังนั้นความเป็นนามธรรมในวันนี้อาจไม่รู้สึกว่าเป็นนามธรรมอีกในวันข้างหน้า นอกจากนี้วงการค้ายังทำให้เกิดสัญลักษณ์ "0" ที่ใช้แทนการสมดุลหรือการลบล้างกันพอดีและเรียก

กันว่า "ศูนย์" ต่อมาในบางกลุ่มคนก็ใช้ "0" ในความหมายของการไม่มีอะไรหรือนับแล้วไม่ได้อะไร "0" จึงอาจถูกรวมเป็น "จำนวนนับ" ด้วยและขอให้สังเกตว่าถ้าเราใช้สัญลักษณ์ a แทนจำนวนลบแล้ว –a จะแทนจำนวนธรรมชาติ

ในหัวข้อนี้ เราจะศึกษาสมบัติสำคัญของจำนวนธรรมชาติที่จะเป็นประโยชน์ต่อการศึกษาพีชคณิตต่อไปและดังได้กล่าวแล้วว่า เราเรียกจำนวนที่ประดิษฐ์ขึ้นเพื่อใช้บอกขนาดว่า "จำนวนธรรมชาติ (natural number)" หรือ "จำนวนนับ" และเขียนแทนเซตของจำนวนธรรมชาติทั้งหมดด้วยสัญลักษณ์ N นั่นคือ

$N = \{1, 2, 3, \ldots\}$

และกำหนดให้ N เป็นเซตเล็กสุดซึ่งสอดคล้องสมบัติ 5 ข้อต่อไปนี้

P1. มีจำนวนธรรมชาติซึ่งเป็นสมาชิกตั้งต้นของ N เขียนแทนด้วยสัญลักษณ์ 1

P2. จำนวนธรรมชาติ n แต่ละจำนวนมี n+1 เป็นพจน์ตามหลังน้อยสุด

P3. พจน์ตามหลังของแต่ละจำนวนธรรมชาติต้องไม่เป็นสมาชิกตั้งต้น 1 ของ N

P4. ถ้าพจน์ตามหลังตัวน้อยสุดของจำนวนธรรมชาติ n และ m เป็นจำนวนเดียวกันแล้ว n และ m เป็นจำนวนธรรมชาติจำนวนเดียวกันและโดยกลับกัน

P5. ถ้า T เป็นเซตย่อยของ N ซึ่งสอดคล้องเงื่อนไข 2 ข้อต่อไปนี้คือ

(ก) $1 \in T$ และ

(ข) พจน์ตามหลังน้อยสุดของ n เป็นสมาชิกของ T สำหรับทุกๆ $n \in T$

แล้ว T = N

นั่นคือ N เท่านั้นที่เป็นเซตย่อยของ N ซึ่งสอดคล้อง (ก) และ (ข)

สังเกตว่าสมบัติ P5. ทำให้เราสามารถพิสูจน์ข้อความเป็นจริง สำหรับทุกๆ จำนวนธรรมชาติ โดยกำหนดเซตย่อยของ N ให้เป็นเซตของ $n \in N$ ซึ่งข้อความที่ต้องการพิสูจน์เป็นจริงที่ n แล้วแสดงให้เห็นว่าเซตย่อยดังกล่าวสอดคล้อง (ก) และ (ข) ของ P5 ก็จะทำให้เราสรุปได้ว่าเซตย่อยนั้นคือ N ซึ่งแสดงว่าข้อความนั้นๆ เป็นจริงสำหรับทุกๆ $n \in N$ เรารู้จักวิธีการพิสูจน์นี้กันเป็นอย่างดีในชื่อว่า "หลักอุปนัยเชิงคณิตศาสตร์"

### 2.1.1 **หลักอุปนัยเชิงคณิตศาสตร์** (Principle of Mathematical Induction)

สำหรับแต่ละจำนวนธรรมชาติ n ให้ P(n) แทนข้อความเปิดที่มี n เป็นตัวแปร ถ้า P(n) สอดคล้องกับเงื่อนไข 2 ข้อต่อไปนี้คือ

1. P(1) เป็นจริง และ
2. สำหรับแต่ละจำนวนธรรมชาติ k ถ้า P(k) เป็นจริง แล้ว P(k+1) เป็นจริง

แล้ว P(n) เป็นจริงสำหรับทุกๆ จำนวนธรรมชาติ n

**บทพิสูจน์** กำหนดให้ $T = \{ n \in \mathbf{N} \mid P(n)$ เป็นจริง $\}$ แล้วโดยเงื่อนไขข้อ 1 ว่า P(1) เป็นจริง ดังนั้น $1 \in T$ และเพื่อพิสูจน์ว่า T สอดคล้องข้อ 2 ของ P5. เราให้ $n \in T$ แล้ว n เป็นจำนวนธรรมชาติซึ่ง P(n) เป็นจริง แต่โดยเงื่อนไขข้อ 2 ของหลักอุปนัยซึ่งเป็นสมมติฐานของการพิสูจน์ ทำให้ได้ P(n+1) เป็นจริง ดังนั้น $n+1 \in T$ เพราะฉะนั้นโดย P5. จะได้ $T = \mathbf{N}$ ซึ่งแสดงว่า P(n) เป็นจริงสำหรับทุกๆ จำนวนธรรมชาติ n ❐

**แบบฝึกหัด 2.1**

1. จงพิสูจน์ว่า เอกลักษณ์หรืออสมการ ในข้อต่อไปนี้เป็นจริง สำหรับทุกๆ จำนวนเต็มบวก n
   1.1 $n < 2^n$
   1.2 $1 + 3 + 5 + \ldots + (2n+1) = (n+1)^2$
   1.3 $1 + 3 + 9 + \ldots + 3^n = \dfrac{3^{n+1} - 1}{2}$
2. จงพิสูจน์ว่า $n^2 + n$ เป็นจำนวนเต็มคู่ สำหรับทุกๆ จำนวนเต็มบวก n
3. จงพิสูจน์ว่า 6 เป็นตัวประกอบของ $n^3 - n$ สำหรับทุกๆ จำนวนเต็มบวก n
4. จงพิสูจน์ว่า 8 เป็นตัวหารของ $5^{2n} - 1$ สำหรับทุกๆ จำนวนเต็มบวก n
5. จงพิสูจน์ว่าสำหรับทุกๆ จำนวนเต็มบวก n ผลบวกของจำนวนเต็มคี่บวก 2n+1 จำนวนแรกเป็นจำนวนคี่

## 2.2 สมบัติเบื้องต้นของจำนวนเต็ม

นักคณิตศาสตร์ได้นำ "จำนวนธรรมชาติ" "0" และ "จำนวนเต็มลบ" มารวมกันและเรียกว่าเซตของจำนวนเต็มทั้งหมด (the set of all integers) และเขียนแทนเซตนี้ด้วยสัญลักษณ์ Z และสมมติว่าทุกคนรู้จักจำนวนเต็มและทราบว่าระบบจำนวนเต็มสอดคล้องตามสมบัติทางพีชคณิตและการเป็นอันดับ ต่อไปนี้

$A_0$ : มีการดำเนินการ $+ : Z \times Z \rightarrow Z$ ซึ่งเรียกว่า "การบวก" และสำหรับแต่ละ $a, b \in Z$ เรียกภาพ $+(a, b)$ ของ $(a, b)$ ว่า *ผลบวก (sum)* ของ a และ b และแทนด้วย a+b

$M_0$ : มีการดำเนินการจาก $Z \times Z$ ไปยัง Z ซึ่งเรียกว่า "การคูณ" และสำหรับแต่ละ $a, b \in Z$ เรียกภาพของ (a, b) ภายใต้การดำเนินการนี้ว่า *ผลคูณ (product)* ของ a และ b และเขียนแทนด้วย ab

$A_1M_1$ : $(a + b) + c = a + (b + c)$ และ $(ab)c = a(bc)$ สำหรับทุกๆ $a, b, c \in Z$ นั่นคือการบวกและการคูณสอดคล้องสมบัติการเปลี่ยนหมู่ (associative)

$A_2M_2$ : $a + b = b + a$ และ $ab = ba$ สำหรับทุกๆ $a, b, c \in Z$ นั่นคือการบวกและการคูณสอดคล้องกับสมบัติการสลับที่ (commutative)

$A_3M_3$ : มีจำนวนเต็มซึ่งเขียนแทนด้วย 0 และ 1 ที่ทำให้ $a + 0 = a$ และ $a1 = a$ สำหรับทุกๆ จำนวนเต็ม a เรียก 0 ว่าเอกลักษณ์การบวก(additive identity) และเรียก 1 ว่าเอกลักษณ์การคูณ (multiplicative identity)

$A_4$ : สำหรับแต่ละจำนวนเต็ม a จะมีจำนวนเต็มเพียงหนึ่งเดียวซึ่งเขียนแทนด้วย -a ที่ทำให้ $a + (-a) = 0$ และเรียก -a ว่า จำนวนลบ (negative) ของ a

C : สำหรับจำนวนเต็ม a, b และ c ถ้า $ab = ac$ และ $a \neq 0$ แล้ว $b = c$ และเรียกสมบัตินี้ว่า "กฎการตัดออกภายใต้การคูณ (cancellation law for multiplication)"

D : $a(b + c) = ab + ac$ สำหรับทุกๆ $a, b, c \in Z$ นั่นคือการบวกมีสมบัติการกระจาย (distributive) เหนือการคูณ

เราสามารถพิสูจน์ทฤษฎีบทต่อไปนี้ได้โดยตรงจากสมบัติดังกล่าวข้างต้น จึงขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

2.2.1 **ทฤษฎีบท** ให้ a b และ c เป็นจำนวนเต็ม แล้ว

1. กฎการตัดออกภายใต้การบวก (cancellation law for addition)
   ถ้า $a + c = b + c$ แล้ว $a = c$
2. $a0 = 0 = 0a$
3. $-(a + b) = (-a) + (-b)$
4. $-(-a) = a$ และ $(-a)(-b) = ab$
5. $(-a)b = -(ab) = a(-b)$ ❐

โดยสมบัติ $A_4$ เราสามารถนิยามการดำเนินการ "การลบ – " บน Z โดยกำหนดให้

$$a - b = a + (-b)$$

สำหรับทุกๆ a, b $\in Z$ ซึ่งทำให้เราสามารถนิยามอันดับบน Z ที่จะแทนด้วยสัญลักษณ์ $\leq$ ดังจะกล่าวในทฤษฎีบทต่อไป

2.2.2 **อันดับบน** Z (Order on Z) ความสัมพันธ์ใน Z ซึ่งกำหนดโดย

$$\leq \; = \{ (a, b) \in Z \times Z \mid a = b \text{ หรือ } b - a \in N \}$$

สอดคล้องสมบัติ 3 ประการต่อไปนี้

1. สมบัติสะท้อน (reflexive) นั่นคือ $a \leq a$ สำหรับทุกๆ $a \in Z$
2. สมบัติปฏิสมมาตร (anti-symmetric) นั่นคือ สำหรับทุกๆ a, $b \in Z$ ถ้า $a \leq b$ และ $b \leq a$ แล้ว $a = b$
3. สมบัติถ่ายทอด (transitive) นั่นคือ สำหรับทุกๆ a, b, c $\in Z$ ถ้า $a \leq b$ และ $b \leq c$ แล้ว $a \leq c$

นั่นคือ $\leq$ เป็นอันดับบน Z ❐

จะขอละการพิสูจน์ว่าความสัมพันธ์ $\leq$ ซึ่งนิยามใน 2.2.2 เป็นอันดับบน Z ไว้เป็นแบบฝึกหัด และถ้า (a, b) $\in \leq$ จะเขียนแทนด้วย $a \leq b$ หรือเขียนแทนด้วย $b \geq a$ และอ่านว่า "a น้อยกว่าหรือเท่ากับ b" หรือ "b มากกว่าหรือเท่ากับ a" ตามลำดับ นอกจากนี้อันดับโดยแท้ซึ่งสมนัยกับ $\leq$ นิยามโดย

$$< \; = \{ (a, b) \in Z \times Z \mid a \leq b \text{ และ } a \neq b \}$$

และถ้า (a, b) $\in <$ เราจะเขียนแทนด้วย $a < b$ หรือเขียนแทนด้วย $b > a$ และอ่านว่า "a น้อยกว่า b" หรือ "b มากกว่า a" ตามลำดับ

2.2.3 **สมบัติของอันดับบน** Z

1. *กฎไตรวิภาค (Trichotomy Law)* สำหรับแต่ละคู่ a, $b \in Z$ ข้อความใดข้อความหนึ่งใน 3 ข้อความต่อไปนี้เป็นจริงและเป็นจริงเพียงหนึ่งเดียวคือ $a < b$ หรือ $a = b$ หรือ $b < a$
2. $0 < a$ สำหรับทุกๆ จำนวนเต็มบวก a
3. สำหรับทุกๆ จำนวนเต็ม a และ b ถ้า $0 < a$ และ $0 < b$ แล้ว $0 < a + b$ ❐

2.2.4 **ทฤษฎีบท** ให้ a b และ c เป็นจำนวนเต็ม

1. ถ้า $a < b$ และ $b < c$ แล้ว $a < c$
2. ถ้า $a < b$ แล้ว $a + c < b + c$

3. ถ้า $a < b$ และ $c > 0$ แล้ว $ac < bc$
4. ถ้า $a < b$ และ $c < 0$ แล้ว $ac > bc$ ❐

**แบบฝึกหัด 2.2**

1. จงพิสูจน์ทฤษฎีบท 2.2.1 ถึง ทฤษฎีบท 2.2.4 พร้อมแสดงว่า ทฤษฎีบท 2.2.4 เป็นจริงสำหรับ $\leq$ ด้วย
2. จงแสดงว่าอันดับ $\leq$ บน Z ไม่เป็นความสัมพันธ์สมมูล
3. จงแสดงว่าถ้า a เป็นจำนวนเต็มซึ่ง $a \neq 0$ แล้ว $aa = a^2 > 0$
4. จงแสดงว่า a และ b เป็นจำนวนเต็มซึ่ง $a \neq 0$ และ $b \neq 0$ แล้ว $ab \neq 0$
5. จงแสดงว่าเซต N ของจำนวนเต็มบวกสอดคล้องสมบัติพีชคณิตและการเป็นอันดับของ Z ยกเว้นสมบัติ $A_3$ และ $A_4$

## 2.3 หลักการเป็นอันดับอย่างดี

ในหัวข้อ 2.2 เราได้แสดงการนิยาม "อันดับ" บนเซต Z ของจำนวนเต็มทั้งหมดซึ่งทำให้ Z เป็นเซตอันดับและสมบัติสำคัญที่เกิดขึ้นเกี่ยวกับเซตอันดับ Z คือสมบัติของอันดับของ Z ที่กำกัดลงบนเซต N ของจำนวนเต็มบวก นั่นคือหลักการเป็นอันดับอย่างดีและสมบัตินี้ทำให้สามารถพิสูจน์ "หลักอุปนัยเชิงคณิตศาสตร์อย่างเข้ม" บน N ซึ่งเป็นข้อความสมมูลกับ "หลักอุปนัยเชิงคณิตศาสตร์" ที่กล่าวมาแล้วในหัวข้อ 2.1 แต่การพิสูจน์ข้อความสำคัญและมีประโยชน์ในทางคณิตศาสตร์ บางข้อความก็ไม่อาจทำได้ด้วย "หลักอุปนัยเชิงคณิตศาสตร์" แต่กลับพิสูจน์ได้โดย "หลักอุปนัยเชิงคณิตศาสตร์อย่างเข้ม"

ในหัวข้อนี้ เราจึงจะศึกษาหลักการที่สำคัญทั้งสองหลักการดังกล่าวพอเป็นสังเขป

2.3.1 **บทนิยาม** ให้ T เป็นเซตย่อยของ N ซึ่งไม่ใช่เซตว่างและ $m \in T$ จะกล่าวว่า m เป็น *สมาชิกน้อยสุด (least element)* ของ T ถ้า $m \leq n$ สำหรับทุกๆ $n \in T$

2.3.2 **ทฤษฎีบท** 1 เป็นสมาชิกน้อยสุดของ N

**บทพิสูจน์** ให้ $T = \{ n \in N \mid 1 \leq n \}$ แล้วโดยสมบัติสะท้อนของ $\leq$ บน N จะได้ $1 \leq 1$ ดังนั้น $1 \in T$ ต่อไปให้ $n \in T$ แล้ว $1 \leq n$ และโดยนิยามของ $\leq$ จะได้ว่า $n \leq n + 1$ และโดยสมบัติถ่ายทอดของ $\leq$

บน N จะได้ $1 \leq n+1$ ซึ่งแสดงว่า $n+1 \in T$ เพราะฉะนั้น T สอดคล้อง P5. ทำให้ได้ $T = N$ ❐

2.3.3 **บทแทรก** สำหรับแต่ละ $n \in N$ จะไม่มี $k \in N$ ซึ่ง $n < k < n+1$

**บทพิสูจน์** ให้ $n \in N$ และสมมติในทางตรงกันข้ามว่ามี $k \in N$ ซึ่ง $n < k < n+1$ แล้วจะมี $p, q \in N$ ซึ่ง $k = n+p$ และ $n+1 = k+q$ ทำให้ได้ $n + 1 = n + (p + q)$ และโดยกฎการตัดออกสำหรับการบวกจะได้ $1 = p+q$ และโดยนิยามของ $\leq$ จะได้ว่า $p < 1$ ซึ่งจะขัดแย้งกับการเป็นสมาชิกน้อยสุดของ 1 ใน N เพราะฉะนั้นบทแทรกเป็นจริง ❐

สำหรับทฤษฎีบทต่อไปจะขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

2.3.4 **ทฤษฎีบท** 1. สำหรับแต่ละ $m, n \in N$ ถ้า $m < n$ แล้ว $m+1 \leq n$

และ 2. $m < n$ ก็ต่อเมื่อ $m+1 < n+1$ สำหรับทุกๆ $m, n \in N$ ❐

2.3.5 **หลักการเป็นอันดับอย่างดี** (Well–Ordering Principle) แต่ละเซตย่อยของ N ที่ไม่ใช่เซตว่างมีสมาชิกน้อยสุด

**บทพิสูจน์** สำหรับแต่ละ $n \in N$ ให้ $P(n)$ แทนข้อความ "ถ้า $B \subseteq N$ และมี $x \in B$ ซึ่ง $x \leq n$ แล้ว B มีสมาชิกน้อยสุด" และให้ $T = \{ n \in N \mid P(n) \text{ เป็นจริง} \}$

เนื่องจาก 1 เป็นสมาชิกน้อยสุดของ N ดังนั้นถ้า $B \subseteq N$ และมี $x \in B$ ซึ่ง $x \leq 1$ แล้ว $x = 1$ และ 1 เป็นสมาชิกน้อยสุดของ B ทำให้ได้ว่า $1 \in T$ ต่อไปให้ $n \in T$ ซึ่งแสดงว่าถ้า $B \subseteq N$ และมี $x \in B$ ซึ่ง $x \leq n$ แล้ว B มีสมาชิกน้อยสุด และให้ $B \subseteq N$ ซึ่งมี $x \in B$ โดยที่ $x \leq n+1$ แล้วถ้า B ไม่มีสมาชิกซึ่งน้อยกว่า $n+1$ แล้ว $n+1$ เป็นสมาชิกน้อยสุดของ B แต่ถ้ามี $x \in B$ ซึ่ง $x < n+1$ แล้วเพราะไม่มี $k \in N$ ซึ่ง $n < k < n+1$ จะได้ว่า $x \leq n$ ดังนั้นมี $x \in B$ ซึ่ง $x \leq n$ และเพราะ $n \in T$ ดังนั้น B มีสมาชิกน้อยสุด ซึ่งแสดงว่า $P(n+1)$ เป็นจริง เพราะฉะนั้นไม่ว่ากรณีใด $n+1 \in T$ เพราะฉะนั้นโดยหลักอุปนัยเชิงคณิตศาสตร์ จะได้ว่า $P(n)$ เป็นจริง สำหรับทุกๆ $n \in N$

ต่อไปให้ $S \subseteq N$ ซึ่ง S ไม่ใช่เซตว่างและให้ $m \in S$ แล้ว $m \in N$ ดังนั้นโดยผลของย่อหน้าก่อนจะได้ว่า $P(m)$ เป็นจริง และเพราะ $S \subseteq N$ ซึ่งมี $m \leq m$ จึงสรุปได้ว่า S มีสมาชิกน้อยสุด ❐

2.3.6 **ตัวอย่าง** จงประยุกต์หลักการเป็นอันดับอย่างดีพิสูจน์ว่า $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ สำหรับทุกๆ $n \in N$

**วิธีทำ** ให้ $E = \{ n \in N \mid 1 + 2 + \ldots + n = \frac{n(n+1)}{2} \}$ แล้ว $E \subseteq N$ และเพราะว่า $\frac{1(1+1)}{2} = 1$ ดังนั้น $1 \in E$ สมมติว่า $S = N - E$ ไม่เป็นเซตว่าง แล้วโดยหลักการเป็นอันดับอย่างดี จะมี $m \in S$ เป็นสมาชิกน้อยสุด ทำให้ได้ $m \neq 1$ เพราะ $1 \in E$ ดังนั้น $m > 1$ ทำให้ได้โดยนิยามของ $<$ ว่าจะมี $p \in N$ ซึ่ง $m = p+1$ เพราะฉะนั้น $p < m$ และโดยการเลือก m จะได้ว่า $p \notin S$ ดังนั้น $p \in E$ ทำให้ได้ $1 + 2 + \ldots + p = \frac{p(p+1)}{2}$ และได้

$$1 + 2 + \ldots + m = 1 + 2 + \ldots + p + (p+1) = \frac{p(p+1)}{2} + (p+1)$$
$$= \frac{(p+1)(p+1+1)}{2} = \frac{m(m+1)}{2}$$

ทำให้ได้ $m \notin E$ และ $m \in E$ เกิดเป็นข้อขัดแย้งกันเอง เพราะฉะนั้น N–E เป็นเซตว่างซึ่งทำให้ได้ $E = N$

❍

เราจะปิดท้ายหัวข้อนี้ด้วยการพิสูจน์ข้อความที่สมมูลกับหลักอุปนัยเชิงคณิตศาสตร์ซึ่งรู้จักกันในชื่อว่า "หลักอุปนัยเชิงคณิตศาสตร์อย่างเข้ม"

2.3.7 **หลักอุปนัยเชิงคณิตศาสตร์อย่างเข้ม** (Strong Principle of Mathematical Induction)

สำหรับแต่ละจำนวนธรรมชาติ n ให้ P(n) แทนข้อความเปิดที่มี n เป็นตัวแปร ถ้า P(n) สอดคล้องกับเงื่อนไขต่อไปนี้

1. P(1) เป็นจริง และ
2. สำหรับแต่ละจำนวนธรรมชาติ k ถ้า P(i) เป็นจริงสำหรับทุก ๆ จำนวนธรรมชาติ i ซึ่ง $1 \leq i \leq k$ แล้ว P(k+1) เป็นจริง

แล้ว P(n) เป็นจริงสำหรับทุก ๆ จำนวนธรรมชาติ n

**บทพิสูจน์** สังเกตว่าหลักทั้งสองของอุปนัยเชิงคณิตศาสตร์ ต่างกันเฉพาะเงื่อนไขที่ 2 ของทั้งสองหลักการ โดยที่เงื่อนไขที่ 2 ของหลักที่ 2 เป็นเงื่อนไขที่แข็งกว่าของหลักที่ 1 อย่างไรก็ตามเราจะพิสูจน์หลักที่ 2 นี้ด้วยการแสดงว่าเงื่อนไขที่ 2 ของทั้งสองหลักสมมูลกัน

สมมติให้เงื่อนไขที่ 2 ของหลักที่ 1 เป็นจริง แต่เงื่อนไขที่ 2 ของหลักที่ 2 เป็นเท็จ แล้วจะมี $k \in N$ ที่ทำให้ P(i) เป็นจริงทุกๆ $i \in N$ ซึ่ง $1 \leq i \leq k$ แต่ P(k+1) เป็นเท็จ และกำหนดเซต

$S = \{ n \in \mathbf{N} \mid P(n)$ เป็นเท็จ $\}$

แล้ว S เป็นเซตย่อยของ **N** ที่ไม่ใช่เซตว่าง (เพราะว่า $k+1 \in S$) ดังนั้นโดยหลักการเป็นอันดับอย่างดี จะมี $m \in \mathbf{N}$ ซึ่ง m เป็นสมาชิกน้อยสุดของ S เพราะฉะนั้น P(m) เป็นเท็จ และเนื่องจาก P(1) เป็นจริง ดังนั้น $m \neq 1$ ซึ่งทำให้ได้ $m > 1$ แล้วโดยนิยามของ < จะมี $t \in \mathbf{N}$ ซึ่ง $m = t + 1$ เพราะฉะนั้น $t < m$ และโดยการเลือก m จะได้ว่า $t \notin S$ นั่นคือ P(t) เป็นจริง แต่โดยเงื่อนไขที่ 2 ของหลักที่ 1 ทำให้ได้ P(m) ซึ่งคือ P(t +1) เป็นจริง จึงเกิดเป็นข้อขัดแย้งกันเอง ดังนั้นเงื่อนไขที่ 2 ของหลักที่ 2 ต้องเป็นจริงด้วย

สำหรับการพิสูจน์ว่าเงื่อนไขที่ 2 ของหลักที่ 1 เป็นจริง ถ้าเงื่อนไขที่ 2 ของหลักที่ 2 เป็นจริงทำได้ในทำนองเดียวกัน จึงขอละไว้เป็นแบบฝึกหัด ❐

**แบบฝึกหัด 2.3**

1. ให้ $u_1, u_2, \ldots$ เป็นลำดับซึ่งกำหนดโดย $u_1 = 6, u_2 = 9$ และสำหรับ $n \geq 3$ นิยาม $u_n = 3u_{n-1} + 18u_{n-2}$ จงพิสูจน์ว่า $u_n$ เป็นพหุคูณของ $3^n$ สำหรับทุกๆ จำนวนเต็มบวก n
2. สำหรับแต่ละจำนวนนับ n นิยาม $b_{n+3} = b_{n+2} + b_{n+1} + b_n$ โดยกำหนด $b_t = t$ สำหรับ $t = 1, 2, 3$ จงพิสูจน์ว่า $b_n < 2^n$ สำหรับทุกๆ จำนวนนับ n
3. จงพิสูจน์ว่า $\left(\frac{3+\sqrt{17}}{2}\right)^n + \left(\frac{3-\sqrt{17}}{2}\right)^n$ เป็นจำนวนคี่ สำหรับทุกๆ จำนวนเต็มบวก n
4. จงแสดงว่าถ้า a และ b เป็นจำนวนเต็มซึ่ง $a < b$ แล้ว $a + 1 \leq b$
5. ให้ $\phi \neq A \subseteq Z$ จะกล่าวว่า A เป็นอันดับอย่างดี ถ้า B มีสมาชิกน้อยสุด สำหรับทุกๆ $B \subseteq A$ ซึ่ง $B \neq \phi$ จงพิสูจน์ว่า
   5.1 Z ไม่เป็นเซตอันดับอย่างดี
   5.2 ถ้า $A \subseteq Z$ เป็นเซตอันดับอย่างดีและ $\phi \neq B \subseteq A$ แล้ว B เป็นเซตอันดับอย่างดี
6. ให้ $\phi \neq A \subseteq Z$ และ $c \in Z$ ซึ่ง $c \leq m$ สำหรับทุกจำนวนเต็ม m จงแสดงว่า A เป็นเซตอันดับอย่างดี [ข้อแนะนำ : ถ้า $c < 0$ พิจารณาเซต $A' = \{m - c + 1 \mid m \in A\}$]

## 2.4 การหารและขั้นตอนการหาร

แม้ว่าเราจะไม่สามารถนิยามการหารให้เป็นการดำเนินการบนเซต Z ได้ เพราะมีบางคู่ของจำนวนเต็มเมื่อหารกันแล้วได้ผลหารที่ไม่เป็นจำนวนเต็ม ตัวอย่างเช่น 3 กับ 4 หรือ 5 กับ 6 เป็นต้น แต่บางคู่ของจำนวนเต็มก็อาจหารกันแล้วได้ผลหารที่เป็นจำนวนเต็ม ตัวอย่างเช่น 18 เมื่อหารด้วย 6 จะ

ได้ผลหารเป็นจำนวนเต็ม 3 เป็นต้น อย่างไรก็ตามเราอาจกล่าวถึงสมบัติการหารใน Z ด้วยขั้นตอนการหารซึ่งจะนำเราไปสู่การนิยาม "ตัวหาร" "ตัวหารร่วม" และ "ตัวหารร่วมมาก" ในที่สุด

2.4.1 **ทฤษฎีบท** ให้ a และ b เป็นจำนวนเต็มโดยที่ $b > 0$ แล้วจะมีจำนวนเต็ม q และ r คู่หนึ่งและเพียงคู่เดียวเท่านั้นซึ่งทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$

**บทพิสูจน์** ให้ a และ b เป็นจำนวนเต็มโดยที่ $b > 0$ เราจะแสดงก่อนว่า จะมีจำนวนเต็ม q และ r คู่หนึ่งซึ่งทำให้ $a = bq + r$ โดยที่ $0 \leq r < b$ โดยเริ่มต้นด้วยกำหนดเซต S ดังนี้

ให้ $S = \{ a - bt \mid t \in Z \}$ แล้ว S ไม่เป็นเซตว่างเพราะว่า $a \in S$ ต่อไปให้ $S'$ เป็นเซตย่อยของ S ซึ่งประกอบด้วยสมาชิกที่ไม่ใช่จำนวนเต็มลบ แล้ว $S'$ ไม่เป็นเซตว่างเพราะว่าถ้า $a \geq 0$ แล้ว $a \in S'$ แต่ถ้า $a < 0$ แล้ว $a - ba \in S$ และเพราะ $1 - b \leq 0$ ดังนั้น $a(1 - b) \geq 0$ ทำให้ได้ $a - ba = a(1 - b) \in S'$

ถ้า $0 \in S'$ แล้ว 0 เป็นสมาชิกน้อยสุดของ $S'$ และถ้า $0 \notin S'$ แล้ว $S'$ เป็นเซตย่อยของเซตของจำนวนเต็มบวกซึ่งไม่ใช่เซตว่าง ทำให้ได้โดยหลักการเป็นอันดับอย่างดีว่า $S'$ มีสมาชิกน้อยสุด ดังนั้นไม่ว่ากรณีใดจะมี $r \in S'$ ซึ่งเป็นสมาชิกน้อยสุด ทำให้ได้ $r \geq 0$ และเพราะ $r \in S$ จึงมีจำนวนเต็ม q ซึ่ง $r = a - bq$ หรือก็คือ $a = bq + r$ เราจึงเหลือที่จะต้องพิสูจน์ว่า $r < b$ โดยสมมติในทางตรงข้ามว่า $r \geq b$ แล้ว $a - b(q+1) = a - bq - b = r - b \geq 0$ ซึ่งทำให้ $a - b(q+1) \in S'$ โดยที่ $a - b(q+1) = a - bq - b < a - bq = r$ จึงเกิดข้อขัดแย้งกับการเลือกให้ r เป็นสมาชิกน้อยสุดใน $S'$ ดังนั้น $r < b$

สุดท้ายเราจะแสดงว่าคู่ของจำนวนเต็ม q และ r ที่เกิดขึ้นในย่อหน้าก่อนมีเพียงคู่เดียว โดยสมมติว่า $q_1$ และ $r_1$ เป็นจำนวนเต็มอีกคู่หนึ่งซึ่ง $a = bq_1 + r_1$ โดยที่ $0 \leq r_1 < b$ ทำให้ได้ $r - r_1 = a - bq - a + bq_1 = b(q_1 - q)$ ดังนั้น b เป็นตัวหารของ $r - r_1$ ถ้า $r \neq r_1$ เราอาจสมมติว่า $r > r_1$ [ ถ้า $r < r_1$ เราจะพิจารณาสมการ $r_1 - r = b(q - q_1)$ แทน] จะได้ $r - r_1 > 0$ และ $b > 0$ ทำให้ได้ $q_1 - q \geq 1$ ดังนั้น $r - r_1 = b(q - q_1) \geq b$ แต่ $r - r_1 < b - r_1 < b$ จึงเกิดเป็นข้อขัดแย้งกันเอง เพราะฉะนั้น $r = r_1$ ซึ่งทำให้ $b(q - q_1) = 0$ โดยที่ $b > 0$ ดังนั้น $q_1 - q = 0$ ซึ่งก็คือ $q_1 = q$ ❐

2.4.2 **ขั้นตอนการหารสำหรับจำนวนเต็ม** (Division Algorithm for Integers)

ถ้า a และ b เป็นจำนวนเต็มโดยที่ $b \neq 0$ แล้วจะมีจำนวนเต็ม q และ r คู่หนึ่งและเพียงคู่เดียวเท่านั้นซึ่งทำให้ $a = bq + r$ โดยที่ $0 \leq r < |b|$

**บทพิสูจน์** เราเหลือเพียงการพิสูจน์กรณี $b < 0$ ซึ่งจะได้ว่า $-b > 0$ แล้วโดยขั้นตอนการหาร จะมีจำนวนเต็ม $q_1$ และ $r$ ซึ่ง $a = (-b)q_1 + r$ โดยที่ $0 \leq r_1 < -b = |b|$ และโดยการเลือก $q = -q_1$ จะได้ $a = bq + r$ โดยที่ $0 \leq r < |b|$ ซึ่งเป็นอันจบการพิสูจน์ ❐

**หมายเหตุ** ในขั้นตอนการหาร เราเรียก a ว่า *ตัวตั้งหาร(dividend)* เรียก b ว่า*ตัวหาร (divisor)* เรียก q ว่า *ผลหาร (quotient)* และเรียก r ว่า *เศษเหลือ (remainder)*

ถ้า $r = 0$ แล้ว $a = bq$ จะกล่าวว่า *b หาร a ลงตัว (b divides a)* และเรียก b ว่า*ตัวประกอบ (factor)* หรือ *ตัวหาร (divisor)* ของ a และเรียก a ว่า *ตัวคูณ (multiple)* ของ b และจะเขียนแทนความหมายนี้ด้วยสัญลักษณ์ $b \mid a$ ดังนั้น

$b \mid a \iff b \neq 0$ และมีจำนวนเต็ม q ซึ่ง $a = bq$

2.4.3 **สมบัติเกี่ยวกับการหาร** ให้ a, b, c และ d เป็นจำนวนเต็ม แล้ว

1. $a \mid 0$, $1 \mid a$ และ $a \mid a$
2. $a \mid b$ และ $b \mid a$ ก็ต่อเมื่อ $a = \pm b$
3. ถ้า $a \mid b$ แล้ว $a^n \mid b^n$ สำหรับทุกๆ จำนวนเต็มบวก n
4. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$
5. ถ้า $a \mid b$ และ $c \mid d$ แล้ว $ac \mid bd$
6. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bx+cy)$ สำหรับทุกๆ จำนวนเต็ม x และ y

**บทพิสูจน์** ให้ a, b, c และ d เป็นจำนวนเต็ม

1. เพราะว่า $0 = 0a$ และ $a = 1a$

2. ให้ $a|b$ และ $b|a$ แล้วโดยความหมายของการหาร จะได้ว่า $a \neq 0$ และ $b \neq 0$ ถ้า a และ b ต่างเป็นจำนวนเต็มบวกทั้งคู่หรือเป็นจำนวนเต็มลบทั้งคู่ แล้วจะมีจำนวนเต็มบวก s และ t ซึ่ง $a = bs$ และ $b = at$ เพราะว่า $s \geq 1$ และ $t \geq 1$ ดังนั้น $a = bs \geq b1 = b$ และ $b = at \geq a1 = a$ และเพราะ $\geq$ เป็นอันดับ เราจึงได้ $a = b$ แต่ถ้า a หรือ b จำนวนใดจำนวนหนึ่งเป็นจำนวนเต็มบวก และอีกจำนวนหนึ่งเป็นจำนวนเต็มลบ ซึ่งโดยไม่เสียนัยทั่วไปขอสมมติให้ a เป็นจำนวนเต็มบวกและ b เป็นจำนวนลบ แล้ว $-b$ เป็นจำนวนเต็มบวกโดยที่ $a \mid -b$ และ $-b \mid a$ ทำให้ได้โดยกรณีจำนวนเต็มบวกทั้งคู่ว่า $a = -b$ เพราะฉะนั้นไม่ว่ากรณีใด $a = b$ หรือ $a = -b$

สำหรับบทกลับเห็นได้ชัด จึงขอละไว้เป็นแบบฝึกหัด

3. พิสูจน์โดยอุปนัยเชิงคณิตศาสตร์ ส่วนข้อ 4 และข้อ 5 พิสูจน์โดยตรงจากบทนิยามของการหารจึงขอละไว้เป็นแบบฝึกหัด

6. ให้ $a \mid b$ และ $a \mid c$ และให้ x และ y เป็นจำนวนเต็ม แล้วจะมีจำนวนเต็ม s และ t ซึ่ง $b = as$ และ $c = at$ ดังนั้น $bx + cy = asx + aty = a(sx + ty)$ โดยที่ $sx + ty$ เป็นจำนวนเต็ม ซึ่งแสดงว่า $a \mid (bx + cy)$ ❐

การประยุกต์ขั้นพื้นฐานของการหารคือการหาตัวประกอบหรือตัวหารทั้งหมดของแต่ละจำนวนเต็มที่ไม่ใช่ 1 และเมื่อกำหนดจำนวนเต็มให้คู่หนึ่ง อาจพบว่าจำนวนเต็มทั้งสองมีตัวประกอบที่เหมือนกันได้และมีได้มากกว่าหนึ่งตัว ซึ่งเราเรียกตัวประกอบที่เหมือนกันว่าตัวหารร่วม และตัวหารร่วมที่สำคัญและมีบทบาทมากที่สุดได้แก่ตัวหารร่วมที่มีตัวหารร่วมตัวอื่นๆ ทุกตัวเป็นตัวประกอบซึ่งแน่นอนว่าต้องมีขนาดมากกว่าตัวหารร่วมตัวอื่นๆ เราจึงเรียกตัวหารร่วมดังกล่าวนี้ว่าตัวหารร่วมมาก

2.4.4 **บทนิยาม** ให้ a, b และ c เป็นจำนวนเต็มโดยที่ $c \neq 0$ จะเรียก c ว่า *ตัวหารร่วม (common divisor)* ของ a และ b ถ้า $c \mid a$ และ $c \mid b$

และจะเรียกจำนวนเต็ม d ว่า *ตัวหารร่วมมาก (greatest common divisor)* ของ a และ b ถ้า $d > 0$ และสอดคล้องสมบัติต่อไปนี้

(ก) d เป็นตัวหารร่วมของ a และ b นั่นคือ $d \mid a$ และ $d \mid b$

(ข) d มากกว่าตัวหารร่วมทุกๆ ตัวของ a และ b นั่นคือถ้า c เป็นจำนวนเต็มซึ่ง $c|a$ และ $c|b$ แล้ว $d \geq c$

ตัวอย่างเช่น ตัวหารร่วมของ 12 และ 42 คือ $\pm 1$, $\pm 2$, $\pm 3$ และ $\pm 6$ และ 6 เป็นตัวหารร่วมมากของ 12 และ 42 เป็นต้น

ทฤษฎีบทต่อไป จะแสดงว่าสำหรับแต่ละคู่ของจำนวนเต็มซึ่งไม่เป็นศูนย์พร้อมกัน จะมีตัวหารร่วมมากของจำนวนเต็มทั้งสองได้เสมอและมีได้เพียงจำนวนเดียวเท่านั้น

2.4.5 **ทฤษฎีบท** ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ หรือ $b \neq 0$ แล้วจะมีจำนวนเต็มบวก d เพียงจำนวนเดียวเท่านั้นซึ่งเป็นตัวหารร่วมมากของ a และ b และยิ่งไปกว่านั้นจะมีจำนวนเต็ม s และ t ซึ่ง $d = as + bt$

**บทพิสูจน์** เราสังเกตว่าตัวหารร่วมมากของ a กับ 0 คือ a ถ้า $a > 0$ และคือ $-a$ ถ้า $a < 0$ และในทำนองเดียวกัน ตัวหารร่วมมากของ 0 กับ b คือ b หรือ $-b$ แล้วแต่กรณี จึงเหลือการพิสูจน์เฉพาะกรณี $a \neq 0$ และ $b \neq 0$ และในกรณีดังกล่าว ขอให้นิยามเซต S ดังนี้

$$S = \{ ax + by \mid x \text{ และ } y \text{ เป็นจำนวนเต็ม} \}$$

แล้ว $a, b \in S$ เพราะว่า $a = a1 + b0$ และ $b = a0 + b1$ ดังนั้น S ไม่เป็นเซตว่าง และเพราะว่า $a^2 = aa + b0 \in S$ ดังนั้นเซตย่อย $S'$ ของ S ซึ่งประกอบด้วยจำนวนเต็มบวกจะไม่เป็นเซตว่างเช่นกัน ทำให้ได้โดยหลักการเป็นอันดับอย่างดีว่า จะมีจำนวนเต็มบวก d ซึ่งเป็นสมาชิกน้อยสุดของ $S'$ และโดยสมบัติการเป็นสมาชิกของ S จะมีจำนวนเต็ม s และ t ซึ่ง $d = as + bt$

ต่อไปจะแสดงว่า d เป็นตัวหารร่วมของ a และ b ด้วยการแสดงว่า d เป็นตัวหารของทุกๆ สมาชิกของ S โดยให้ $u \in S$ แล้วจะมีจำนวนเต็ม x และ y ซึ่ง $u = ax + by$ และโดยขั้นตอนการหารจะมีจำนวนเต็ม q และ r ซึ่ง $u = dq + r$ โดยที่ $0 \leq r < d$ ดังนั้น $r = u - dq = ax + by - (as + bt)q = a(x - sq) + b(y - tq) \in S$ ถ้า $r > 0$ แล้ว $r \in S'$ และ $r < d$ ซึ่งจะขัดแย้งกับการเป็นสมาชิกน้อยสุดของ d ใน $S'$ เพราะฉะนั้น $r = 0$ ซึ่งทำให้ $u = dq$ แสดงว่า d เป็นตัวหารของ u และเพราะ $a, b \in S$ ดังนั้น d เป็นตัวหารร่วมของ a และ b ยิ่งไปกว่านั้นเพราะว่า $d = as + bt$ ดังนั้นถ้า c เป็นจำนวนเต็มบวกซึ่งเป็นตัวหารร่วมของ a และ b แล้ว $c \mid d$ ทำให้มีจำนวนเต็มบวก k (นั่นคือ $k \geq 1$) ซึ่ง $d = ck$ จึงได้ว่า $d \geq c$ เพราะฉะนั้น d เป็นตัวหารร่วมมากของ a และ b

สุดท้ายเราจะพิสูจน์ว่าตัวหารร่วมมากของ a และ b มีเพียงหนึ่งเดียว โดยสมมติว่า $d'$ เป็นตัวหารร่วมมากของ a และ b แล้วโดยสมบัติการเป็นตัวหารร่วมมากของทั้งคู่ จะได้ว่า $d \geq d'$ และ $d' \geq d$ ทำให้ได้โดยสมบัติปฏิสมมาตรของ $\geq$ ว่า $d = d'$ ซึ่งเป็นอันจบการพิสูจน์ ❐

**2.4.6 บทแทรก** ถ้า d เป็นตัวหารร่วมมากของจำนวนเต็ม a และ b และ c เป็นจำนวนเต็มซึ่งเป็นตัวหารร่วมของ a และ b แล้ว $c \mid d$ ❐

2.4.7 **ข้อตกลง**

1. เนื่องจากตัวหารร่วมมากของแต่ละคู่ของจำนวนเต็ม a และ b มีเพียงหนึ่งเดียว เราจึงใช้สัญลักษณ์แทนตัวหารร่วมมากของ a และ b ได้ และสัญลักษณ์ที่รู้จักกันอย่างแพร่หลาย คือ (a, b) ตัวอย่างเช่น (12, 42) = 6 และ (25, 33) = 1 เป็นต้น

2. ถ้า (a, b) = 1 จะกล่าวว่า a และ b เป็น *จำนวนเฉพาะสัมพัทธ์ (relatively prime)* ของกันและกัน
3. แม้ว่าตัวหารร่วมมากของจำนวนเต็มจะเป็นจำนวนเต็มบวก แต่เราก็นิยามให้ (0, 0) = 0

ในกรณีที่ a และ b เป็นจำนวนเต็มที่มีขนาดใหญ่ เช่น a = 1750 และ b = 20572 หรือ a = -5789 และ b = -49563 เป็นต้น การหาตัวหารร่วมมากของ a และ b โดยตรงจากบทนิยามอาจจะเสียเวลามากและไม่สะดวก จึงมีผู้คิดหาวิธีการหาตัวหารร่วมมากโดยวิธีอื่น และวิธีการของท่านยุคลิด (Euclid) ก็เป็นที่นิยมกันมาจนถึงปัจจุบัน โดยรู้จักกันในชื่อ "ขั้นตอนยุคลิด"

### 2.4.8 ขั้นตอนยุคลิด (Euclidean Algorithm)

ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ หรือ $b \neq 0$ และเพื่อความสะดวกจะขอพิจารณาเฉพาะกรณี b > 0 (ถ้า b < 0 จะใช้ –b แทน b) แล้วโดยขั้นตอนการหาร จะมีจำนวนเต็ม $q_1$ และ $r_1$ ซึ่ง

$a = bq_1 + r_1$ โดยที่ $0 \leq r_1 < b$ ..... (1)

ถ้า $r_1 = 0$ แล้ว $b \mid a$ และ b เป็นตัวหารร่วมมากของ a และ b แต่ถ้า $r_1 > 0$ แล้วโดยขั้นตอนการหาร จะมีจำนวนเต็ม $q_2$ และ $r_2$ ซึ่ง

$b = r_1q_2 + r_2$ โดยที่ $0 \leq r_2 < r_1 < b$ ..... (2)

สมมติให้ $k \geq 2$ เป็นจำนวนเต็มซึ่งขั้นตอนดังกล่าวข้างต้น ดำเนินมาถึงขั้นที่ k นั่นคือมีจำนวนเต็ม $q_k$ และ $r_k$ ซึ่ง

$r_{k-2} = r_{k-1}q_k + r_k$ โดยที่ $0 \leq r_k < r_{k-1} < \ldots < r_1 < b$ ..... (k)

ถ้า $r_k = 0$ แล้วขั้นตอนวิธีจะสิ้นสุด แต่ถ้า $r_k \neq 0$ แล้วโดยขั้นตอนการหาร จะมีจำนวนเต็ม $q_{k+1}$ และ $r_{k+1}$ ซึ่ง

$r_{k-1} = r_kq_{k+1} + r_{k+1}$ โดยที่ $0 \leq r_{k+1} < r_k < \ldots < r_1 < |b|$ ..... (k+1)

โดยหลักอุปนัยเชิงคณิตศาสตร์ ขั้นตอนวิธีการดังกล่าวจะดำเนินไปเรื่อยๆ แต่เพราะว่า $r_1 > r_2 > r_3 > \ldots > r_{k-1} > r_k > r_{k+1} > \ldots > 0$ ซึ่งจะเห็นว่าแต่ละ $r_i$ เป็นจำนวนเต็มบวกที่มีค่าน้อยลง (ครั้งละอย่างน้อย 1) เรื่อยๆ เมื่อ i เพิ่มขึ้น ดังนั้นขั้นตอนวิธีการจะต้องสิ้นสุด นั่นคือมีจำนวนเต็มบวก n ซึ่ง $r_{n+1} = 0$ เพราะฉะนั้น $r_{n-1} = r_nq_{n+1}$ และเราจะพิสูจน์ว่า $r_n = (a, b)$

อย่างแรกจะพิสูจน์ว่า $r_n \mid a$ และ $r_n \mid b$ จาก $r_{n-1} = r_nq_{n+1}$ ทำให้ได้ $r_n \mid r_{n-1}$ ดังนั้นจะมีจำนวนเต็ม m ซึ่ง $r_{n-1} = r_nm$ ทำให้ได้ $r_{n-2} = r_{n-1}q_n + r_n = r_nmq_n + r_n = r_n(mq_n+1)$ ดังนั้น $r_n \mid r_{n-2}$ จึงสมมติว่า k เป็น

จำนวนเต็มซึ่ง $1 \leq k \leq n-1$ และ $r_n | r_t$ สำหรับทุกๆ $k \leq t \leq n-1$ แล้วจะมีจำนวนเต็ม x และ y ซึ่ง $r_k = r_n x$ และ $r_{k+1} = r_n y$ แล้วโดยการพิจารณาย้อนกลับของขั้นตอนการหารจะได้ $r_{k-1} = r_k q_{k-1} + r_{k+1} = r_n x q_{k-1} + r_n y = r_n(xq_{k-1} + y)$ ทำให้ได้ว่า $r_n | r_{k-1}$ ดังนั้นโดยวิธีอุปนัยจะได้ว่า $r_n | r_k$ สำหรับทุกๆ $1 \leq k \leq n-1$ เมื่อกำหนดให้ $r_0 = b$ เพราะฉะนั้น $r_n | b$ และ $r_n | r_1$ ซึ่งทำให้มีจำนวนเต็ม s และ t ซึ่ง $b = r_n s$ และ $r_1 = r_n t$ และจาก $a = bq_1 + r_1 = r_n s q_1 + r_n t = r_n(sq_1 + t)$ ทำให้ได้ว่า $r_n | a$

อย่างที่สองให้ c เป็นจำนวนเต็มซึ่ง $c | a$ และ $c | b$ แล้วจะมีจำนวนเต็ม u และ v ซึ่ง $a = cu$ และ $b = cv$ และเพราะว่า $r_1 = a - bq_1 = cu - cvq_1 = c(u - vq_1)$ ดังนั้น $c | r_1$ จึงสมมติว่า $c | r_t$ สำหรับทุกๆ $1 \leq t < k$ แล้วจะมีจำนวนเต็ม s และ t ซึ่ง $r_{k-1} = ct$ และ $r_{k-2} = cs$ แล้ว $r_k = r_{k-2} - r_{k-1}q_{k-2} = cs - ctq_{k-2} = c(s - tq_{k-2})$ ซึ่งแสดงว่า $c | r_k$ ดังนั้นโดยหลักอุปนัยเชิงคณิตศาสตร์ จะได้ว่า $c | r_k$ สำหรับทุกๆ $1 \leq k \leq n$ เพราะฉะนั้น $c | r_n$ ดังนั้น $r_n$ เป็นตัวหารร่วมมากของ a และ b ❐

2.4.9 **ตัวอย่าง** จงหาตัวหารร่วมมากของ 1001 และ 357 และเขียนตัวหารร่วมมากในรูปผลบวกเชิงเส้นของ 1001 และ 357

**วิธีทำ** เราประยุกต์ขั้นตอนยุคลิด ดังนี้

$$1001 = 357(2) + 287$$
$$357 = 287(1) + 70$$
$$287 = 70(4) + 7$$
$$70 = 7(10)$$

ดังนั้น (1001, 357) = 7 และโดยขั้นตอนย้อนกลับ จะได้ 7 เขียนในรูปผลบวกเชิงเส้นของ 1001 และ 357 ดังนี้

$$7 = 287 - 70(4) = 287 - [357 - 287(1)](4) = 287(5) - 357(4)$$
$$= [1001 - 357(2)](5) - 357(4) = 1001(5) + 357(-14)$$ ○

ในทำนองคู่กัน เมื่อกล่าวถึงตัวหารและตัวหารร่วมมากของจำนวนเต็ม จะต้องกล่าวถึงตัวคูณและตัวคูณร่วมน้อยของจำนวนเต็มด้วย

2.4.10 **บทนิยาม** ให้ a, b และ c เป็นจำนวนเต็มโดยที่ $a \neq 0$ และ $b \neq 0$ จะเรียก c ว่า *ตัวคูณร่วม (common multiple)* ของ a และ b ถ้า $a | c$ และ $b | c$

และเรียกจำนวนเต็ม m ว่า *ตัวคูณร่วมน้อย (least common multiple)* ของ a และ b ถ้า $m > 0$ และสอดคล้องสมบัติต่อไปนี้

(ก) m เป็นตัวคูณร่วมของ a และ b นั่นคือ $a \mid m$ และ $b \mid m$

(ข) m น้อยกว่าตัวคูณร่วมทุกๆ ตัวของ a และ b นั่นคือถ้า c เป็นจำนวนเต็มซึ่ง $a \mid m$ และ $b \mid m$ แล้ว $c \geq m$

ขอละการพิสูจน์ว่า สำหรับแต่ละคู่ของจำนวนเต็ม a และ b โดยที่ $a \neq 0$ หรือ $b \neq 0$ จะมีจำนวนเต็มบวก m เพียงจำนวนเดียวเท่านั้นซึ่งเป็นตัวคูณร่วมน้อยของ a และ b ไว้เป็นแบบฝึกหัด และเรานิยมใช้สัญลักษณ์ [a, b] แทนตัวคูณร่วมน้อยของ a และ b สำหรับทฤษฎีบทต่อไป จะกล่าวถึงความสัมพันธ์ของ a และ b กับตัวหารร่วมมากและตัวคูณร่วมน้อยของ a และ b

**2.4.11 ทฤษฎีบท** ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ หรือ $b \neq 0$ แล้ว $ab = (a, b)[a, b]$

**บทพิสูจน์** ให้ a และ b เป็นจำนวนเต็มโดยที่ $a \neq 0$ หรือ $b \neq 0$ แล้วโดยทฤษฎีบท 2.4.5 จะมีจำนวนเต็มบวก d ซึ่งเป็นตัวหารร่วมมากของ a และ b และจะมีจำนวนเต็ม s, t, x และ y ซึ่ง $a = ds$, $b = dt$ และ $d = ax + by$ ทำให้ได้ $d = dsx + dty = d(sx + ty)$ และโดยสมบัติ C ในหัวข้อ 2.2 สำหรับ $d \neq 0$ จะได้ $1 = sx + ty$

เราสังเกตว่า $ab = (ds)(dt) = d(dst)$ และเห็นได้ชัดว่า a และ b ต่างเป็นตัวหารของ dst เราจึงเหลือเพียงแสดงว่า dst เป็นตัวคูณร่วมน้อยของ a และ b โดยให้ c เป็นจำนวนเต็มบวกซึ่งเป็นตัวคูณร่วมของ a และ b แล้วจะมีจำนวนเต็ม p และ q ซึ่ง $c = ap = bq$ และจาก $1 = sx + ty$ เราจะได้ $c = csx + cty = bqsx + apty = dtqsx + dspty = dst(qx + py)$ ซึ่งแสดงว่า dst เป็นตัวหารของ c และเพราะว่าทั้ง c และ dst ต่างเป็นจำนวนเต็มบวก ดังนั้น $c \geq dst$ เพราะฉะนั้น dst เป็นตัวคูณร่วมน้อยของ a และ b ❐

## แบบฝึกหัด 2.4

1. จงพิสูจน์ทฤษฎีบท 2.4.3 ข้อ 3 ข้อ 4 และ ข้อ 5
2. จงหาตัวหารร่วมมากของ a และ b ต่อไปนี้ พร้อมทั้งเขียนให้อยู่ในรูปผลบวกเชิงเส้น $as + bt$

   2.1 $a = 6432$ และ $b = -132$ 2.2 $a = -3456$ และ $b = -7234$

3. ให้ a, b และ m เป็นจำนวนเต็มซึ่ง $(a, m) = (b, m) = 1$ จงแสดงว่า $(ab, m) = 1$
4. ให้ a, b และ c เป็นจำนวนเต็มซึ่ง $a \neq 0$ และ $c \neq 0$ จงแสดงว่าถ้า $(a, c) = d$, $a \mid b$ และ $c \mid b$ แล้ว $ac \mid bd$
5. ให้ a, b, $a_1$ และ $b_1$ เป็นจำนวนเต็ม จงแสดงว่าถ้า $d = (a, b)$ โดยที่ $a = a_1d$ และ $b = b_1d$ แล้ว $(a_1, b_1) = 1$
6. ให้ a และ b เป็นจำนวนเต็ม จงแสดงว่าถ้า $(a, b) = 1$ แล้ว $(a + b, a - b) = 1$ หรือ $(a + b, a - b) = 2$
7. ให้ a และ b เป็นจำนวนเต็ม จงพิสูจน์ว่า

   7.1 $(a,b) = [a,b]$ ก็ต่อเมื่อ $a = \pm b$

   7.2 $[a, b] = [a, -b] = [-a, b] = [-a, -b]$

   **หมายเหตุ** ผลของ 7.2 ทำให้กล่าวได้ว่าในการหาตัวคูณร่วมน้อยของ a และ b เป็นการเพียงพอที่จะหาเฉพาะกรณีที่ a และ b เป็นจำนวนเต็มบวก
9. จงพิสูจน์ว่า $6 \mid a(a+1)(2a+1)$ สำหรับทุกๆ จำนวนเต็ม a
10. จงพิสูจน์ว่า $(a^n, b^n) = (a, b)^n$ สำหรับทุกๆ จำนวนเต็มบวก n

## 2.5 จำนวนเฉพาะ

ถ้าพิจารณาตัวหารทั้งหมดของแต่ละจำนวนเต็ม จะพบว่าบางจำนวนอาจมีตัวหารเพียงแค่ $\pm 1$ กับ จำนวนนั้นและลบของจำนวนนั้น เช่น 3, 7 หรือ 11 เป็นต้น แต่บางจำนวนเต็มอาจมีจำนวนตัวหารมากกว่า 4 ตัวนี้ ตัวอย่างเช่น ตัวหารทั้งหมดของ 8 ได้แก่ $\pm 1$, $\pm 2$, $\pm 4$, $\pm 8$ เป็นต้น ในหัวข้อนี้เราจึงจะศึกษาสมบัติของจำนวนเต็มซึ่งจำแนกตามจำนวนของตัวหาร

2.5.1 **บทนิยาม** เราเรียกจำนวนเต็มบวก p ว่า *จำนวนเฉพาะ (prime number)* ถ้า $p > 1$ และ $c = \pm 1$ หรือ $c = \pm p$ เมื่อใดก็ตามที่ c เป็นจำนวนเต็มซึ่งเป็นตัวหารของ p

ถ้า n เป็นจำนวนเต็มที่ไม่ใช่ 0 ไม่ใช่ $\pm 1$ และไม่ใช่จำนวนเฉพาะ เราจะเรียก n ว่า *จำนวนประกอบ(composite number)* นั่นคือ

n เป็นจำนวนประกอบ ก็ต่อเมื่อ $n \notin \{0, \pm 1\}$ และมีจำนวนเต็ม c และ d ซึ่ง $n = cd$ (ทำให้ c และ d ไม่ใช่ $\pm 1$ ทั้งคู่)

นอกเหนือจากการตรวจสอบโดยบทนิยามว่า จำนวนเต็มตัวใดเป็นจำนวนเฉพาะหรือจำนวนประกอบ เรายังมีเกณฑ์ตรวจสอบอีกแบบหนึ่ง ดังจะแสดงในทฤษฎีบทต่อไปนี้

2.5.2 **ทฤษฎีบท** ให้ $p > 1$ เป็นจำนวนเต็มแล้ว p เป็นจำนวนเฉพาะ ก็ต่อเมื่อ $(p, n) = 1$ หรือ $p \mid n$ สำหรับทุกๆ จำนวนเต็ม n

**บทพิสูจน์** ให้ p เป็นจำนวนเฉพาะและ n เป็นจำนวนเต็มซึ่ง $(p, n) \neq 1$ ให้ d เป็นจำนวนเต็มบวกซึ่ง $d = (p, n)$ แล้ว $d > 1$ และ $d \mid p$ แต่ p เป็นจำนวนเฉพาะ จึงได้ว่า $d = p$ ซึ่งแสดงว่า $p = (p, n)$ ดังนั้น $p \mid n$

ในการพิสูจน์บทกลับให้ $p > 1$ เป็นจำนวนเต็มซึ่ง $(p, n) = 1$ หรือ $p \mid n$ สำหรับทุกๆ จำนวนเต็ม n และเพื่อพิสูจน์ว่า p เป็นจำนวนเฉพาะ เราให้ c เป็นจำนวนเต็มซึ่ง $c \neq \pm 1$ และ $c \mid p$ แล้วโดยสมมติฐานจะได้ $(p, c) = 1$ หรือ $p \mid c$ แต่ถ้า $c \mid p$ แล้วเพราะ $c \neq \pm 1$ ดังนั้น $(p, c) \neq 1$ จึงได้ว่า $p \mid c$ และจาก $c \mid p$ และ $p \mid c$ จะได้ $c = \pm p$ ทำให้ได้ว่า p เป็นจำนวนเฉพาะ ❐

ความสำคัญอย่างหนึ่งของจำนวนเฉพาะซึ่งรู้จักกันเป็นอย่างดีในชื่อของทฤษฎีบทหลักมูลของเลขคณิตซึ่งกล่าวว่าทุกๆ จำนวนเต็มซึ่งมากกว่า 1 เขียนได้ในรูปผลคูณของจำนวนเฉพาะ ตัวอย่างเช่น $15 = (3)(5)$, $6 = (2)(3)$, $16 = 2^4$ หรือ $17 = (17)(1)$ เป็นต้น แต่ก่อนอื่นจะขอพิสูจน์ทฤษฎีบทสองทฤษฎีบทต่อไปนี้ เพื่อนำไปประยุกต์พิสูจน์ทฤษฎีบทหลักมูลของเลขคณิตดังกล่าว

2.5.3 **ทฤษฎีบท** ให้ a, b และ c เป็นจำนวนเต็ม ถ้า $a \mid bc$ และ $(a, b) = 1$ แล้ว $a \mid c$

**บทพิสูจน์** ให้ a, b และ c เป็นจำนวนเต็มซึ่ง $a \mid bc$ และ $(a, b) = 1$ แล้ว $a \neq 0$ และ $b \neq 0$ เพราะว่า $(a, b) = 1$ แล้วโดยทฤษฎีบท 2.4.5 จะมีจำนวนเต็ม r, s และ t ซึ่ง $1 = ar + bs$ และ $bc = at$ ทำให้ได้ $c = car + cbs = car + ats = a(cr + ts)$ ซึ่งแสดงว่า $a \mid c$ ❐

2.5.4 **ทฤษฎีบท** ให้ p เป็นจำนวนเฉพาะ n เป็นจำนวนเต็มบวกและ $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มซึ่ง $p \mid a_1a_2 \ldots a_n$ แล้วจะมี $i = 1, 2, \ldots, n$ ซึ่ง $p \mid a_i$

**บทพิสูจน์** ให้ p เป็นจำนวนเฉพาะ แล้วจะพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์บน n ดังนี้

สำหรับแต่ละจำนวนเต็มบวก n ให้ P(n) แทนข้อความ "ถ้า $a_1, a_2, \ldots, a_n$ เป็นจำนวนเต็มซึ่ง $p \mid a_1a_2 \ldots a_n$ แล้วจะมี $i = 1, 2, \ldots, n$ ซึ่ง $p \mid a_i$" แล้วเห็นได้ชัดว่า P(1) เป็นจริง

ให้ k เป็นจำนวนเต็มบวกซึ่ง P(k) เป็นจริง นั่นคือถ้า $a_1, \ldots, a_k$ เป็นจำนวนเต็มซึ่ง $p|a_1a_2\ldots a_k$ แล้วจะมี $i = 1,\ldots, k$ ซึ่ง $p|a_i$ ให้ $a_1, \ldots, a_{k+1}$ เป็นจำนวนเต็มซึ่ง $p \mid a_1a_2\ldots a_ka_{k+1}$ ถ้า $p \mid a_{k+1}$ แล้วจะมี $i = k$ ซึ่ง $p \mid a_i$ ดังนั้น P(k+1) เป็นจริง แต่ถ้า p ไม่เป็นตัวหารของ $a_{k+1}$ แล้วเพราะ $p \mid ra_k$ โดยที่ $r = a_1a_2\ldots a_k$ ดังนั้นโดยทฤษฎีบท 2.5.3 จะได้ว่า $p \mid a_1a_2\ldots a_k$ ทำให้ได้โดยสมมติฐานของหลักอุปนัยเชิงคณิตศาสตร์ว่า จะมี $i = 1,\ldots, k$ ซึ่ง $p \mid a_i$ ดังนั้นจะมี $1 \leq i \leq k+1$ ซึ่ง $p \mid a_i$ แสดงว่า P(k+1) เป็นจริง เพราะฉะนั้นไม่ว่ากรณีใด จะได้ P(k+1) เป็นจริง

เพราะฉะนั้นโดยหลักอุปนัยเชิงคณิตศาสตร์ จะได้ว่าทฤษฎีบทเป็นจริง ❐

2.5.5 **บทนิยาม** ให้ n เป็นจำนวนเต็มบวก จะกล่าวว่า *n เขียนได้ในรูปผลคูณของจำนวนเฉพาะ (n is a product of primes)* ถ้ามีจำนวนเต็มบวก r และจำนวนเฉพาะ $p_1, p_2, \ldots, p_r$ ซึ่ง $n = p_1p_2\ldots p_r$ และเรียกเซต $\{p_1, p_2, \ldots, p_r\}$ ว่าชุดของจำนวนเฉพาะซึ่งมีผลคูณเป็น n

2.5.6 **ทฤษฎีบทหลักมูลของเลขคณิต** (Fundamental Theorem of Arithmetic)

แต่ละจำนวนเต็ม $n > 1$ เขียนได้ในรูปผลคูณของจำนวนเฉพาะ และชุดของจำนวนเฉพาะซึ่งมีผลคูณเป็น n มีเพียงชุดเดียว

**บทพิสูจน์** ก่อนอื่นเราจะพิสูจน์ว่า สำหรับแต่ละจำนวนเต็ม $n > 1$ เขียนได้ในรูปผลคูณของจำนวนเฉพาะ โดยกำหนดให้ S แทนเซตของจำนวนเต็ม $m > 1$ ซึ่งไม่สามารถเขียนได้ในรูปผลคูณของจำนวนเฉพาะ แล้วจะแสดงว่า S เป็นเซตว่าง โดยสมมติในทางตรงข้ามว่า S ไม่เป็นเซตว่าง แล้ว S เป็นเซตย่อยของเซตของจำนวนเต็มบวกที่ไม่ใช่เซตว่าง ดังนั้นโดยหลักการเป็นอันดับอย่างดี ทำให้ได้ว่า S มีสมาชิกน้อยสุด ให้ n เป็นสมาชิกน้อยสุดของ S แล้วขอให้สังเกตว่าทุกๆ จำนวนเฉพาะเขียนได้ในรูปผลคูณของจำนวนเฉพาะ (นั่นคือจำนวนเฉพาะนั้นเอง) ดังนั้นทุกๆ จำนวนเฉพาะไม่เป็นสมาชิกของ S ทำให้ได้ว่า n เป็นจำนวนประกอบ นั่นคือมีจำนวนเต็มบวก r และ s ซึ่ง $n = rs$ โดยที่ $1 < r < n$ และ $1 < s < n$ แล้วโดยสมบัติการเป็นสมาชิกน้อยสุดของ n ใน S จะได้ว่า r และ s ไม่เป็นสมาชิกของ S ซึ่งแสดงว่า r และ s แต่ละตัวเขียนได้ในรูปผลคูณของจำนวนเฉพาะ จึงทำให้ n เขียนได้ในรูปผลคูณของจำนวนเฉพาะด้วย ทำให้เกิดเป็นข้อขัดแย้งกันเอง เพราะฉะนั้น S เป็นเซตว่าง

ต่อไปสมมติว่า n เป็นจำนวนเต็มซึ่ง $n > 1$ และมี $\{p_1, p_2, \ldots, p_r\}$ และ $\{q_1, q_2, \ldots, q_s\}$ ต่างเป็นชุดของจำนวนเฉพาะซึ่งมีผลคูณเป็น n แล้ว $p_1p_2\ldots p_r = n = q_1q_2\ldots q_s$ เพราะว่า $p_1$ เป็นตัวหาร

ของ $p_1p_2 \ldots p_r$ ดังนั้นจึงเป็นตัวหารของ $q_1q_2 \ldots q_s$ และโดยทฤษฎีบท 2.5.4 จะมี $1 \leq j \leq s$ ซึ่ง $p_1 | q_j$ ทำให้ได้ว่า $p_1 = q_j$ และโดยกฎการตัดออกภายใต้การคูณของจำนวนเต็ม จะได้

$$p_2 \ldots p_r = q_1q_2 \ldots q_{j-1}q_{j+1} \ldots q_s \qquad \ldots\ldots\ldots (1)$$

และด้วยวิธีการเดียวกัน จะมี $k \in \{1, \ldots, j-1, j+1, \ldots, s\}$ ซึ่ง $p_2 = q_k$ และเมื่อดำเนินวิธีการนี้ซ้ำไปเรื่อยๆ r ครั้ง จะได้ว่า ทางซ้ายมือของสมการ (1) เป็น 1 และทางขวามือของสมการ (1) เป็นผลคูณของจำนวนเฉพาะ ซึ่งจะเป็นไปได้ ก็ต่อเมื่อ $r = s$ และจะทำให้ได้ $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_r\}$ จึงเป็นอันจบการพิสูจน์ ❐

ขอให้สังเกตว่า การเขียนจำนวนเต็ม $n > 1$ ในรูปผลคูณของจำนวนเฉพาะนั้น ชุดของจำนวนเฉพาะที่มีผลคูณเป็น n ซึ่งมีเพียงชุดเดียว อาจมีจำนวนเฉพาะที่ซ้ำกันได้ และในกรณีเช่นนี้ อาจเขียน n ในรูปผลคูณของจำนวนเฉพาะกำลังต่างๆ ดังนี้

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

เมื่อ $p_1, \ldots, p_k$ เป็นจำนวนเฉพาะและ $e_1, \ldots, e_k$ เป็นจำนวนเต็มบวก ตัวอย่างเช่น

$$2420 = (2)(11)(5)(11)(2) = 2^2 \cdot 5 \cdot 11^2$$

หรือ $$2552 = (2)(2)(2)(11)(29) = 2^3 \cdot 11 \cdot 29$$ เป็นต้น

ผลของทฤษฎีบทพื้นฐานของเลขคณิต ทำให้กล่าวได้ว่า จำนวนเฉพาะมีได้มากมายนับไม่ถ้วน ดังจะแสดงการพิสูจน์ในทฤษฎีบทต่อไป

2.5.7 **ทฤษฎีบท** มีจำนวนเฉพาะเป็นจำนวนอนันต์

**บทพิสูจน์** สมมติว่าทฤษฎีบทไม่เป็นจริง นั่นคือมีจำนวนเฉพาะเพียงจำนวนจำกัดเท่านั้น ให้ n เป็นจำนวนเต็มบวกและ $p_1, \ldots, p_n$ เป็นจำนวนเฉพาะทั้งหมดที่มีอยู่ และกำหนดให้ $a = p_1 \ldots p_n + 1$ แล้วโดยทฤษฎีบทหลักมูลของเลขคณิต a เขียนได้ในรูปผลคูณของจำนวนเฉพาะ ทำให้ได้ว่ามี $1 \leq j \leq n$ ซึ่ง $p_j | a$ ดังนั้นมีจำนวนเต็ม q ซึ่ง $a = p_jq$ ทำให้ได้

$$1 = a - p_1 \ldots p_n = p_jq - p_1 \ldots p_n = p_j(q - p_1 \ldots p_{j-1}p_{j+1} \ldots p_n)$$

แสดงว่า $p_i | 1$ ซึ่งเป็นไปไม่ได้ ดังนั้น $p_1, \ldots, p_n$ ทุกตัวไม่เป็นตัวหารของ a จึงเกิดเป็นข้อความขัดแย้งกันเอง เพราะฉะนั้นทฤษฎีบทเป็นจริง ❐

แม้ว่าจำนวนเฉพาะจะมีมากมายนับไม่ถ้วน แต่ก็ยังไม่มีสูตรสำหรับการหาจำนวนเฉพาะตัวถัดไปจากจำนวนเฉพาะที่เรารู้จักมาก่อน ทั้งนี้เพราะจำนวนเฉพาะกระจายกันอยู่อย่างไม่มีรูปแบบที่แน่นอน บางตัวอาจอยู่ติดกันเช่น 2 และ 3 บางตัวอาจเป็นจำนวนเฉพาะที่อยู่ถัดจากจำนวนเฉพาะตัวก่อนหน้าเพียงแค่ 2 จำนวนเช่น 3, 5 และ 7 หรือ 17 กับ 19 แต่บางตัวอาจอยู่ห่างจากจำนวนเฉพาะตัวก่อนหน้ามากกว่า 2 จำนวนเช่น 7 กับ 11 เป็นต้น อย่างไรก็ตามสำหรับจำนวนประกอบ เราจะได้ความจริงในทางตรงข้าม กล่าวคือสำหรับแต่ละจำนวนเต็มบวก n ใดๆ เราจะมีจำนวนประกอบ n จำนวนที่เรียงติดกันเสมอ ได้แก่

$(n+1)! + 2,\ (n+1)! + 3, (n+1)! + 4, \ldots, (n+1)! + (n+1)$

เมื่อ $(n+1)! = (n+1)\cdot n\cdots 3\cdot 2\cdot 1$ เพราะว่าจำนวน $(n+1)! + j$ จะมี j เป็นตัวหาร สำหรับแต่ละ j ซึ่ง $2 \leq j \leq n+1$

2.5.8 **บทนิยาม** ให้ n เป็นจำนวนเต็ม จะกล่าวว่า n เป็น *จำนวนคู่ (even number)* ถ้ามีจำนวนเต็ม m ที่ทำให้ $n = 2m$ และจะเรียกจำนวนที่ไม่ใช่จำนวนคู่ว่า *จำนวนคี่ (odd number)*

สังเกตจากขั้นตอนการหาร ถ้า n เป็นจำนวนเต็มซึ่งเป็นจำนวนคี่ แล้วจะมีจำนวนเต็ม m และ r ซึ่ง $n = 2m + r$ โดยที่ $r = 0$ หรือ $r = 1$ แต่ถ้า $r = 0$ แล้ว $n = 2m$ ทำให้ n เป็นจำนวนคู่ซึ่งขัดแย้งกับสมมติฐาน ดังนั้น $n = 2m +1$ และในทำนองกลับกันถ้า n เป็นจำนวนเต็มซึ่งมีจำนวนเต็ม m ที่ทำให้ $n = 2m+1$ แล้ว n ไม่เป็นจำนวนคู่ ดังนั้น n เป็นจำนวนคี่ จึงสรุปได้ว่า

"จำนวนเต็ม n เป็นจำนวนคี่ ก็ต่อเมื่อมี จำนวนเต็ม m ที่ทำให้ $n = 2m + 1$"

โดยบทนิยามของจำนวนคู่ จะเห็นว่าจำนวนคู่ทุกๆ จำนวนเป็นตัวคูณของ 2 ดังนั้นจำนวนคู่ที่ไม่ใช่ 2 จะไม่เป็นจำนวนเฉพาะ เราจึงกล่าวได้ว่าจำนวนเฉพาะทุกจำนวนที่ไม่ใช่ 2 เป็นจำนวนคี่ ยิ่งไปกว่านั้นเมื่อหารจำนวนเฉพาะที่เป็นจำนวนคี่ด้วย 4 จะได้เศษเป็น 1 หรือ 3 ทำให้สรุปได้ว่าถ้า p เป็นจำนวนเฉพาะที่เป็นจำนวนคี่ แล้วจะมีจำนวนเต็ม m ที่ทำให้ $p = 4m +1$ หรือ $p = 4m +3$

## แบบฝึกหัด 2.5

1. จงหาจำนวนเฉพาะทั้งหมดที่น้อยกว่าหรือเท่ากับ 100
2. จงเขียนจำนวนเต็มต่อไปนี้ ในรูปผลคูณของจำนวนเฉพาะ

   2.1 7234 2.2 6432 2.3 –34568

3. จงแสดงว่า $\sqrt{p}$ เป็นจำนวนอตรรกยะ สำหรับทุก ๆ จำนวนเฉพาะ p
4. ให้ $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ และ $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$ โดยที่ $p_1, p_2, \ldots, p_n$ เป็นจำนวนเฉพาะที่แตกต่างกันและ $\alpha_i$ และ $\beta_i$ เป็นจำนวนเต็มบวกหรือศูนย์สำหรับทุกๆ $i = 1, 2, \ldots, n$ จงพิสูจน์ว่า

   4.1 $(a, b) = p_1^{\delta_1} p_2^{\delta_2} \ldots p_n^{\delta_n}$ เมื่อ $\delta_i = \min\{\alpha_i, \beta_i\} = \begin{cases} \alpha_i & \text{ถ้า } \alpha_i \le \beta_i \\ \beta_i & \text{ถ้า } \alpha_i \ge \beta_i \end{cases}$

   สำหรับทุกๆ $i = 1, 2, \ldots, n$

   4.2 $[a, b] = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n}$ เมื่อ $\gamma_i = \max\{\alpha_i, \beta_i\} = \begin{cases} \beta_i & \text{ถ้า } \alpha_i \le \beta_i \\ \alpha_i & \text{ถ้า } \alpha_i \ge \beta_i \end{cases}$

   สำหรับทุกๆ $i = 1, 2, \ldots, n$
5. จงพิสูจน์ว่าผลคูณของจำนวนเต็มที่เขียนได้ในรูปแบบ 4k+1 ตั้งแต่ 2 จำนวนขึ้นไปเป็นจำนวนเต็มที่เขียนได้ในรูปแบบ 4k+1
6. จงพิสูจน์ว่ามีจำนวนเฉพาะที่เขียนได้ในรูปแบบ 4k+3 เป็นจำนวนนับไม่ถ้วน
7. จงพิสูจน์ว่าถ้า p เป็นจำนวนเฉพาะซึ่ง p+2 และ p+4 ต่างก็เป็นจำนวนเฉพาะแล้ว p = 2
8. จงพิสูจน์ว่ามีจำนวนเฉพาะที่เขียนได้ในรูปแบบ 6k+5 เป็นจำนวนนับไม่ถ้วน
9. จงพิสูจน์ว่าในลำดับเลขคณิต a, a + d, a + 2d, a +3d, . . . ซึ่ง (a, d) = 1 จะมีพจน์เรียงกันอย่างน้อย n พจน์ที่ทุกๆ พจน์เป็นจำนวนประกอบไม่ว่า n จะเป็นจำนวนเต็มบวกใดๆ
10. ให้ a และ b เป็นจำนวนเต็ม จงพิสูจน์ว่าถ้า a และ b มี *ภาวะ (parity)* เดียวกัน [นั่นคือ a และ b เป็นจำนวนคู่ทั้งคู่ หรือ a และ b เป็นจำนวนคี่ทั้งคู่] แล้ว a + b เป็นจำนวนคู่ แต่ถ้า a และ b มีภาวะต่างกันแล้ว a + b เป็นจำนวนคี่

## 2.6 คอนกรูเอนซ์

ในการกล่าวถึงจำนวนเต็มสองจำนวน โดยประยุกต์ขั้นตอนการหารจะทำให้สามารถกล่าวถึงผลหารและเศษเหลือของการหารจำนวนหนึ่งด้วยอีกจำนวนหนึ่งได้ และถ้ากำหนดตัวหารให้เป็นจำนวนเต็มบวกคงตัว แล้วเห็นได้ชัดว่าเศษเหลือจากการหารจำนวนเต็มต่างๆ ด้วยตัวหารที่เป็นจำนวนเต็มคงตัวนั้นเป็นจำนวนเต็มที่เรียงลำดับกันเป็นคาบ ตัวอย่างเช่นกำหนดให้ 3 เป็นตัวหารคงตัวแล้วเศษเหลือจากการหารจำนวนเต็ม 0, 1, 2, 3, 4, 5, 6, 7, ... จะคือ 0, 1, 2, 0, 1, 2, 0, 1, 2, ... ตามลำดับ ดังนั้นเราอาจจำแนกจำนวนเต็มออกเป็นหมู่ โดยให้แต่ละหมู่ของจำนวนเต็มมีค่าของเศษ

เหลือจากการหารด้วยจำนวนเต็มบวกคงตัวเท่าๆ กัน และจะกล่าวว่าจำนวนเต็มสองจำนวนใดๆ สัมพันธ์กัน ถ้าจำนวนทั้งสองหารด้วยจำนวนเต็มบวกที่คงตัวแล้วเหลือเศษเท่ากัน

ในหัวข้อนี้ จะกล่าวถึงสมบัติที่สำคัญของความสัมพันธ์ในเซตของจำนวนเต็มซึ่งกำหนดในรูปของเศษเหลือดังกล่าว

2.6.1 **บทนิยาม** ให้ a และ b เป็นจำนวนเต็มและ m เป็นจำนวนเต็มบวก จะกล่าวว่า a *คอนกรูเอนซ์ (congruence)* กับ b *มอดูโล (modulo)* m ถ้า $m \mid (a - b)$ และจะเขียนแทนความหมายนี้ด้วยสัญลักษณ์ $a \equiv b \pmod{m}$

แต่ถ้า m ไม่เป็นตัวหารของ $a - b$ จะกล่าวว่า b ไม่คอนกรูเอนซ์กับ a มอดูโล m

ตัวอย่างเช่นจำนวนเต็มสองจำนวนมีความสัมพันธ์คอนกรูเอนซ์มอดูโล 2 ก็ต่อเมื่อจำนวนเต็มทั้งสองเป็นจำนวนคู่ทั้งคู่หรือจำนวนคี่ทั้งคู่ นั่นคือจำนวนทั้งสองมีภาวะเดียวกัน (ดูความหมายในแบบฝึกหัด 2.5 ข้อ 10) ตัวอย่างอื่นๆ ได้แก่

$17 \equiv 3 \pmod{7}$ เพราะว่า 7 เป็นตัวหารของ $17 - 3 = 14$

$4 \equiv 22 \pmod{9}$ เพราะว่า 9 เป็นตัวหารของ $4 - 22 = -18$

$19 \equiv 19 \pmod{11}$ เพราะว่า 11 เป็นตัวหารของ $0 = 19 - 19$

แต่ 17 ไม่คอนกรูเอนซ์กับ 3 มอดูโล 8 ก็เพราะว่า 8 ไม่เป็นตัวหารของ $14 = 17 - 3$ เป็นต้น

ขอให้สังเกตว่าถ้า $m = 0$ และ $a \equiv b \pmod{m}$ แล้ว 0 จะเป็นตัวหารของ $a - b$ แต่ 0 เป็นตัวหารของจำนวนเต็ม x ใดๆ ก็ต่อเมื่อ $x = 0$ ดังนั้นการกล่าวว่า $a \equiv b \pmod{0}$ จึงสมมูลกับการกล่าวว่า $a - b = 0$ ซึ่งก็คือ $a = b$ นั่นเอง นอกจากนี้สำหรับ $m = 1$ จะได้ว่า $a \equiv b \pmod{1}$ ก็ต่อเมื่อ 1 เป็นตัวหารของ $a - b$ แต่ 1 เป็นตัวหารของจำนวนเต็ม x ใดๆ ดังนั้นทุกๆ คู่ของจำนวนเต็มจะสัมพันธ์คอนกรูเอนซ์กันมอดูโล 1 เพราะฉะนั้นการกล่าวถึงคอนกรูเอนซ์มอดูโล m จึงจะกล่าวเฉพาะกรณี $m > 1$ เท่านั้น

2.6.2 ทฤษฎีบท คอนกรูเอนซ์มอดูโล m เป็นความสัมพันธ์สมมูลใน Z สำหรับทุกๆ จำนวนเต็มบวก m

**บทพิสูจน์** ให้ m เป็นจำนวนเต็มบวกและให้ a, b และ c เป็นจำนวนเต็ม

1. เนื่องจาก $a - a = 0$ และ $m \mid 0$ ดังนั้น $a \equiv a \pmod{m}$

2. ให้ $a \equiv b(\text{mod } m)$ แล้ว $m \mid (a - b)$ ทำให้มีจำนวนเต็ม k ซึ่ง $a - b = km$ ดังนั้น $b - a = (-k)m$ ซึ่งแสดงว่า $m \mid (b - a)$ เพราะว่า $-k$ ก็เป็นจำนวนเต็ม จึงได้ว่า $b \equiv a \pmod m$

3. ให้ $a \equiv b \pmod m$ และ $b \equiv c \pmod m$ แล้ว $m \mid (a - b)$ และ $m \mid (b - c)$ และจากทฤษฎีบท 2.4.3 ข้อ 6 จะได้ $m \mid [(a - b) + (b - c)]$ ซึ่งสมมูลกับ $m \mid (a - c)$ ดังนั้น $a \equiv c \pmod m$

จาก (1), (2) และ (3) สรุปได้ว่า คอนกรูเอนซ์มอดูโล m เป็นความสัมพันธ์สมมูลใน Z ❐

2.6.3 **ทฤษฎีบท** ให้ m เป็นจำนวนเต็มบวกและ a, b และ c เป็นจำนวนเต็มซึ่ง $a \equiv b \pmod m$ และ $c \equiv d \pmod m$ แล้ว

1. $a + c \equiv b + d \pmod m$
2. $ac \equiv bd \pmod m$
3. $a^n \equiv b^n \pmod m$ สำหรับทุกๆ จำนวนเต็มบวก n

**บทพิสูจน์** ให้ $a \equiv b \pmod m$ และ $c \equiv d \pmod m$ แล้ว $m \mid (a - b)$ และ $m \mid (c - d)$ ดังนั้น

$$m \mid [(a - b) + (c - d)] \quad \text{ซึ่งสมมูลกับ} \quad m \mid [(a + c) - (b + d)]$$

เพราะฉะนั้น $a + c \equiv b + c \pmod m$ นอกจากนี้

$$m \mid [c(a - b) + b(c - d] \quad \text{ซึ่งสมมูลกับ} \quad m \mid (ac - bd)$$

เพราะฉะนั้น $ac \equiv bd \pmod m$

ดังนั้นข้อ 1 และข้อ 2 ของทฤษฎีบทเป็นจริง สำหรับการพิสูจน์ข้อ 3 ใช้การอ้างอิงทฤษฎีบท 2.6.3 ข้อ 2 และหลักอุปนัยเชิงคณิตศาสตร์ ❐

สังเกตจากผลของทฤษฎีบท 2.6.3 ได้ว่าความสัมพันธ์คอนกรูเอนซ์มอดูโล m มีสมบัติทางพีชคณิตคล้ายกับความสัมพันธ์ "เท่ากับ" ในเซตของจำนวนเต็มยกเว้นกฎการตัดออกสำหรับการคูณ ตัวอย่างเช่นถ้า $a = 2$, $b = 6$ และ $c = 3$ แล้ว $ac \equiv bd \pmod 6$ แต่ a ไม่คอนกรูเอนซ์กับ b มอดูโล 6 เป็นต้น อย่างไรก็ตามทฤษฎีบท 2.6.4 และบทแทรกจะแสดงสมบัติสำคัญที่ทำให้กฎการตัดออกเป็นจริงสำหรับความสัมพันธ์คอนกรูเอนซ์มอดูโล m ด้วย

2.6.4 **ทฤษฎีบท** ให้ m, $m_1$ และ d เป็นจำนวนเต็มบวก ถ้า a และ b เป็นจำนวนเต็มซึ่ง $ac \equiv bc \pmod m$ และ $d = (c, m)$ โดยที่ $m_1 d = m$ แต่ m ไม่เป็นตัวหารของ c แล้ว $a \equiv b \pmod{m_1}$

**บทพิสูจน์** ให้ $ac \equiv bc \pmod{m}$ แล้ว $m \mid (ac - bc)$ ทำให้มีจำนวนเต็ม k ซึ่ง $ac - bc = km$ และเพราะ $d = (c, m)$ ดังนั้น $d \mid c$ และ $d \mid m$ นั่นคือมีจำนวนเต็ม $c_1$ และ $m_1$ ซึ่ง $c = c_1d$ และ $m = m_1d$ ตามลำดับและโดยการแทนค่าใน $ac - bc = km$ จะได้ $a(c_1d) - b(c_1d) = k(m_1d)$ ทำให้ได้ $c_1(a - b) = km_1$ แต่ m ไม่เป็นตัวหารของ c จึงทำให้ $c \neq 0$ และดังนั้น $d \neq 0$ ด้วย

จาก $c_1(a - b) = km_1$ จะได้ $m_1 \mid c_1(a - b)$ แต่โดยแบบฝึกหัด 4 ข้อ 5 แสดงว่า $(m_1, c_1) = 1$ ซึ่งโดยทฤษฎีบท 2.5.4 ทำให้สรุปได้ว่า $m_1 \mid (a - b)$ ซึ่งทำให้ได้ $a \equiv b \pmod{m_1}$ ❐

ถ้าแทน $d = 1$ ในทฤษฎีบท 2.6.4 เราจะได้บทแทรกต่อไปนี้

2.6.5 **บทแทรก** ให้ m เป็นจำนวนเต็มบวก ถ้า a, b และ c เป็นจำนวนเต็มซึ่ง $ac \equiv bc \pmod{m}$ และ $(c, m) = 1$ แล้ว $a \equiv b \pmod{m}$ ❐

เพราะว่าคอนกรูเอนซ์มอดูโล m เป็นความสัมพันธ์สมมูลสำหรับทุกๆ จำนวนเต็มบวก m ดังนั้นจะมีผลแบ่งกั้น Z ซึ่งกำหนดโดยคอนกรูเอนซ์มอดูโล m สำหรับแต่ละจำนวนเต็มบวก m ตัวอย่างเช่น เซตของจำนวนเต็มคู่และเซตของจำนวนเต็มคี่เป็นสมาชิกทั้งหมดของผลแบ่งกั้น Z ที่กำหนดโดยคอนกรูเอนซ์มอดูโล 2 เป็นต้น

พิจารณาแต่ละจำนวนเต็มบวก m จะเห็นว่าการหารจำนวนเต็มต่างๆ ด้วย m จะมีเศษเหลือเป็นจำนวนเต็มบวกที่แตกต่างกันทั้งหมด m ตัวได้แก่ 0, 1, 2, ... , m–1 และเราจะพิสูจน์ทฤษฎีบท 2.6.6 ต่อไปนี้ว่าจำนวนเต็มใดๆ ซึ่งเมื่อหารด้วย m แล้วเหลือเศษ r $(0 \leq r < m)$ จะมีความสัมพันธ์คอนกรูเอนซ์มอดูโล m กับ r หรือกล่าวได้ว่า จำนวนเต็มนั้นๆ จะอยู่ในเซตสมมูลเดียวกันกับ r และถ้าเราใช้สัญลักษณ์ $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(m-1)}$ แทนเซตสมมูลที่มี 0, 1, 2, ..., m–1 เป็นสมาชิกอยู่ตามลำดับแล้ว ทฤษฎีบท 2.6.8 และทฤษฎีบท 2.6.9 จะแสดงความจริงว่า $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(m-1)}\}$ เป็นผลแบ่งกั้น Z

2.6.6 **ทฤษฎีบท** ให้ m เป็นจำนวนเต็มบวกและ a เป็นจำนวนเต็ม แล้วจะมีจำนวนเต็มบวก r ที่น้อยสุดซึ่ง $r \in \{0, 1, \ldots, m-1\}$ และ $a \equiv r \pmod{m}$

**บทพิสูจน์** ให้ m เป็นจำนวนเต็มบวกและ a เป็นจำนวนเต็ม แล้วโดยขั้นตอนการหารจะมีจำนวนเต็ม q และ r เพียงคู่เดียวซึ่ง $a = qm + r$ โดยที่ $0 \leq r < m$ ดังนั้น $r \in \{0, 1, \ldots, m-1\}$ และ r เป็นจำนวน

เต็มไม่เป็นลบที่น้อยสุดซึ่งสอดคล้องขั้นตอนการหาร นอกจากนี้ $a = mq + r$ ซึ่งสมมูลกับ $a - r = mq$ จะทำให้ได้ $m \mid (a - r)$ ซึ่งแสดงว่า $a \equiv r \pmod{m}$ ❐

ขอให้สังเกตว่า เราอาจกล่าวทฤษฎีบท 2.6.6 ได้อีกอย่างหนึ่งว่า "จำนวนเต็ม a คอนกรูเอนซ์มอดูโล m กับเศษเหลือจากการหาร a ด้วย m" ซึ่งเราสามารถนำหลักนี้ไปใช้ในการหาเศษที่เกิดจากการหารด้วยจำนวนเต็มบวก ดังจะแสดงให้เห็นในตัวอย่างต่อไปนี้

2.6.7 **ตัวอย่าง** จงหาเศษที่ได้จากการหาร $(19)^3(288)^2$ ด้วย 5

**วิธีทำ** เนื่องจาก $19 \equiv 4 \pmod{5}$ ดังนั้นโดยจากทฤษฎีบท 2.6.3 ข้อ 3 จะได้ $(19)^3 \equiv 4^3 \pmod{5}$

แต่ $4^3 - 4 = 4(4^2 - 1) = (4)(15)$ ทำให้ได้ $4^3 \equiv 4 \pmod{5}$ และโดยสมบัติการถ่ายทอดของคอนกรูเอนซ์ จะได้ $(19)^3 \equiv 4 \pmod{5}$ และเช่นเดียวกันจาก $288 \equiv 3 \pmod{5}$ จะได้โดยทฤษฎีบท 2.6.3 ข้อ 3 ว่า $(288)^2 \equiv 3^2 \pmod{5}$ แต่ $3^2 - 4 = 5$ จึงได้ $3^2 \equiv 4 \pmod{5}$ แล้วโดยสมบัติการถ่ายทอดของคอนกรูเอนซ์ ทำให้ได้ $(288)^2 \equiv 4 \pmod{5}$ ดังนั้นโดยทฤษฎีบท 2.6.3 ข้อ 2 จะได้ว่า $(19)^3(288)^2 \equiv (4)(4) \pmod{5}$ แต่ $16 \equiv 1 \pmod{5}$ ดังนั้นโดยสมบัติการถ่ายทอดอีกครั้งหนึ่ง จะได้ว่า $(19)^3(288)^2 \equiv 1 \pmod{5}$ ซึ่งแสดงว่าการหาร $(19)^3(288)^2$ ด้วย 5 จะเหลือเศษ 1 ❍

2.6.8 **ทฤษฎีบท** ให้ m เป็นจำนวนเต็มบวก แล้ว a จะไม่คอนกรูเอนซ์กับ b มอดูโล m สำหรับทุกๆ จำนวนเต็ม $0 \leq a \neq b \leq m-1$

**บทพิสูจน์** ให้ a และ b เป็นจำนวนเต็มซึ่ง $0 \leq a < b \leq m-1$ แล้ว $0 < b - a \leq m - a - 1 < m-1$ ดังนั้น $b - a$ ไม่เป็นพหุคูณของ m ซึ่งแสดงว่า a จะไม่คอนกรูเอนซ์กับ b มอดูโล m ❐

2.6.9 **ทฤษฎีบท** ให้ m เป็นจำนวนเต็มบวก แล้วผลแบ่งกั้นซึ่งกำหนดโดยคอนกรูเอนซ์มอดูโล m ประกอบด้วยสมาชิกเพียง m ตัวเท่านั้น

**บทพิสูจน์** ให้ m เป็นจำนวนเต็มบวกและ a เป็นจำนวนเต็ม แล้วโดยทฤษฎีบท 2.6.6 จะมี r เพียงจำนวนเดียวซึ่ง $r \in \{0, 1, \ldots, m-1\}$ และ $a \equiv r \pmod{m}$ และโดยทฤษฎีบท 2.6.7 และการใช้สัญลักษณ์ $\bar{r}$ ที่กำหนดดังข้างต้น จะได้ว่า $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{(m-1)}\}$ เป็นผลแบ่งกั้น Z ซึ่งประกอบด้วยสมาชิกเพียง m ตัวเท่านั้น ❐

2.6.10 **บทนิยาม** เราเรียกเซตสมมูลที่กำหนดโดยคอนกรูเอนซ์มอดูโล m ว่า *เรซิดิวคลาสมอดูโล m (residue class modulo m)*

ถ้า m เป็นจำนวนเต็มบวกและ a และ x เป็นจำนวนเต็ม แล้ว $a \equiv x \pmod{m}$ ซึ่งสมมูลกับ $a \in \bar{x}$ ก็ต่อเมื่อ $\bar{a} = \bar{x}$ และถ้า $x_0 \in \bar{0}$ $x_1 \in \bar{1}$, . . ., $x_{m-1} \in \overline{(m-1)}$ แล้ว $\{\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{m-1}\}$ ก็จะเป็นผลแบ่งกั้น Z เช่นเดียวกัน ดังนั้นผลแบ่งกั้น Z เหล่านี้ก็คือเซตของเรซิดิวคลาสมอดูโล m เช่นกัน

2.6.11 **บทนิยาม** ให้ m เป็นจำนวนเต็มบวก เราเรียกผลแบ่งกั้น $\{\bar{0}, \bar{1}, \ldots, \overline{(m-1)}\}$ ของ Z ว่า *เซตสมบูรณ์ของเรซิดิวคลาสมอดูโล m (complete residue class modulo m)* และเขียนแทนเซตนี้ด้วย $Z_m$

2.6.12 **ตัวอย่าง** สำหรับ m = 6 จะได้ $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ โดยที่

$$\bar{0} = \{\ldots, 12, 6, 0, 6, 12, \ldots\}$$

$$\bar{1} = \{\ldots, 11, 5, 1, 7, 13, \ldots\}$$

$$\bar{2} = \{\ldots, 10, 4, 2, 8, 14, \ldots\}$$

$$\bar{3} = \{\ldots, 9, 3, 3, 9, 15, \ldots\}$$

$$\bar{4} = \{\ldots, 8, 2, 4, 10, 16, \ldots\}$$

$$\bar{5} = \{\ldots, 7, 1, 5, 11, 17, \ldots\}$$

จากทฤษฎีบท 2.6.3 ข้อ 1 และข้อ 2 ถ้า m เป็นจำนวนเต็มบวกและ a และ b เป็นจำนวนเต็มซึ่ง $a \equiv b \pmod{m}$ แล้ว $\bar{a} = \bar{b}$ นอกจากนี้ถ้า m เป็นจำนวนเต็มบวกและ a, b, c และ d เป็นจำนวนเต็ม เราจะสามารถพิสูจน์ได้ว่า ถ้า $\bar{a} = \bar{b}$ และ $\bar{c} = \bar{d}$ แล้ว $\overline{a+c} = \overline{b+d}$ และ $\overline{ac} = \overline{bd}$ ซึ่งแสดงว่าเราสามารถนิยามการดำเนินการ $\oplus$ และ $\otimes$ บน $Z_m$ โดย

$$\bar{a} \oplus \bar{b} = \overline{a+b} \qquad \text{และ} \qquad \bar{a} \otimes \bar{b} = \overline{ab}$$

เราเรียก $\bar{a} \oplus \bar{b}$ ว่าผลบวกของเรซิดิวคลาส $\bar{a}$ และ $\bar{b}$ ซึ่งคือเรซิดิวคลาสที่มีจำนวนเต็ม a+b เป็นสมาชิกอยู่และในทำนองเดียวกันเราเรียก $\bar{a} \otimes \bar{b}$ ว่าผลคูณของเรซิดิวคลาส $\bar{a}$ และ $\bar{b}$ ซึ่งคือเรซิดิวคลาสที่มีจำนวนเต็ม ab เป็นสมาชิก

เราสามารถพิสูจน์ได้ว่า $\oplus$ และ $\otimes$ สอดคล้องสมบัติการสลับที่และการเปลี่ยนหมู่ ด้วยสมบัติการสลับที่และการเปลี่ยนหมู่ของ "การบวก" และ "การคูณ" บน Z ตามลำดับ นอกจากนี้ยังมี $\overline{0}$ และ $\overline{1}$ เป็นเอกลักษณ์การบวก $\oplus$ และเอกลักษณ์การคูณ $\otimes$ ตามลำดับ และสุดท้ายแต่ละจำนวนเต็ม a จะมีจำนวนเต็ม -a ที่ทำให้ $\bar{a}\oplus\overline{(-a)}=\overline{0}$ หรือกล่าวได้ว่าแต่ละสมาชิกของ $Z_m$ มีตัวผกผันภายใต้ $\oplus$

แต่มีเพียงบางตัวใน $Z_m$ เท่านั้นที่มีตัวผกผันภายใต้ $\otimes$ ตัวอย่างเช่น สำหรับ m = 6 จะเห็นว่า $\bar{2}$ และ $\bar{3}$ ใน $Z_6$ ไม่มีตัวผกผันภายใต้ $\otimes$ แต่ $\bar{5}\in Z_6$ มี $\bar{5}$ ซึ่ง $\bar{5}\otimes\bar{5}=\overline{25}=\bar{1}$ เป็นต้น

สุดท้ายถ้า m เป็นจำนวนเต็มบวกและ $\bar{a}, \bar{b}, \bar{c} \in Z_m$ เราสามารถพิสูจน์ได้ว่า

$$\bar{a}\otimes(\bar{b}\oplus\bar{c}) = \bar{a}\otimes(\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab}\oplus\overline{ac} = (\bar{a}\otimes\bar{b})\oplus(\bar{a}\otimes\bar{c})$$

นั่นคือ $Z_m$ สอดคล้องกฎการกระจายของ $\otimes$ เหนือ $\oplus$

## แบบฝึกหัด 2.6

1. ให้ m เป็นจำนวนเต็มบวกและ a, b, c และ d เป็นจำนวนเต็ม จงแสดงว่าถ้า $a + b \equiv c \pmod{m}$ และ $b \equiv d \pmod{m}$ แล้ว $a + d \equiv c \pmod{m}$
2. ให้ m และ n เป็นจำนวนเต็มบวกและ a และ b เป็นจำนวนเต็ม จงแสดงว่า
   2.1 ถ้า $a \equiv b \pmod{n}$ และ $m|n$ แล้ว $a \equiv b \pmod{m}$
   2.2 มีจำนวนเต็ม x ซึ่ง $a + x \equiv b \pmod{n}$
3. ให้ m เป็นจำนวนเต็มบวกและ a และ b เป็นจำนวนเต็ม จงแสดงว่า ถ้า $a \equiv b \pmod{m}$ และ $(a, m) = 1$ แล้ว $(b, m) = 1$
4. จงหาจำนวนเต็มบวก a ซึ่งน้อยสุดที่ทำให้
   4.1 $a \equiv (22)(312) \pmod{7}$ 4.2 $a \equiv (3)(7)(13)(515)(23) \pmod{11}$
5. จงแสดงว่า $a^2 \equiv 0 \pmod{4}$ หรือ $a^2 \equiv 1 \pmod{4}$ สำหรับทุกๆ จำนวนเต็ม a
6. จงหาผลบวกและผลคูณ ในข้อต่อไป
   6.1 $\bar{3}\otimes(\bar{2}\oplus\bar{4})$ 6.2 $\bar{3}\oplus(\bar{2}\otimes\bar{4})$
7. ให้ n เป็นจำนวนเต็มบวก จงแสดงว่าสำหรับแต่ละจำนวนเต็ม a ซึ่ง (a, n) = 1 จะมีจำนวนเต็ม b ซึ่ง $\bar{a}\otimes\bar{b}=\bar{1}$
8. จงแสดงว่าจำนวนเต็มบวก n เป็นจำนวนเฉพาะ ก็ต่อเมื่อ สำหรับทุกๆ $\bar{a},\bar{b}\in Z_n$ ถ้า $\bar{a}\otimes\bar{b}=\bar{0}$ แล้ว $\bar{a}=\bar{0}$ หรือ $\bar{b}=\bar{0}$

# บทที่ 3

# กรุปและสมบัติมูลฐาน

# GROUPS AND THEIR ELEMENTARY PROPERTIES

พีชคณิตคือระบบหรือโครงสร้างทางคณิตศาสตร์ที่ประกอบด้วยเซตที่ไม่เป็นเซตว่างเซตหนึ่งกับการดำเนินการบนเซตนั้นตั้งแต่ 1 การดำเนินการขึ้นไป สอดคล้องกับกลุ่มของสัจพจน์กลุ่มหนึ่ง แล้วจากสัจพจน์เหล่านี้ ทำให้สรุปในเชิงตรรกศาสตร์เป็นทฤษฎีบทต่างๆ ที่จะอธิบายโครงสร้างเชิงพีชคณิตของระบบคณิตศาสตร์นั้นๆ ต่อไป ลักษณะการเข้าสู่ระบบคณิตศาสตร์ระบบหนึ่งๆ ด้วยการเริ่มจากสัจพจน์ นอกจากจะง่ายต่อการเข้าใจถึงแก่นแท้และสาระสำคัญของระบบคณิตศาสตร์ที่กำลังพิจารณาอยู่แล้ว ยังบอกได้ถึงความแตกต่าง ความคล้ายคลึงและความสัมพันธ์ของตัวอย่างต่างๆ ที่ยกขึ้นมาประกอบระบบคณิตศาสตร์นั้นๆ ได้อีกด้วย

ในบทนี้ เราจะเริ่มด้วยการศึกษาระบบคณิตศาสตร์ที่ประกอบด้วยการดำเนินการทวิภาคหนึ่งตัวบนเซตที่ไม่ใช่เซตว่างเซตหนึ่งซึ่งสอดคล้องกับสัจพจน์ 4 ข้อ ดังจะนิยามให้เห็นต่อไป และจะเรียกระบบคณิตศาสตร์เหล่านี้ว่ากรุป ซึ่งเป็นระบบคณิตศาสตร์ที่มีประโยชน์และมีรูปแบบง่ายต่อการอธิบายโครงสร้างพีชคณิตของระบบคณิตศาสตร์ที่สุด และจากสัจพจน์ของกรุป เราจะได้ทฤษฎีบทซึ่งเป็นพื้นฐานร่วมของโครงสร้างเชิงพีชคณิตของระบบคณิตศาสตร์เกือบทุกระบบอีกด้วย

## 3.1 บทนิยามและตัวอย่างของกรุป

ในหัวข้อนี้ เราจะให้บทนิยามของกรุปและยกตัวอย่างกรุปที่คุ้นเคยและกรุปที่จะเป็นประโยชน์ต่อการศึกษาเรื่องกรุปต่อไป

3.1.1 **บทนิยาม** เราเรียกโครงสร้างคณิตศาสตร์ที่ประกอบด้วยเซต G ซึ่งไม่ใช่เซตว่างกับการดำเนินการทวิภาคกำหนดบน G ว่า *กรุป (group)* ถ้าการดำเนินการนี้สอดคล้องสมบัติข้อ 1, 3 และ 4 ของบทนิยาม 1.4.1 บนเซต G นั่นคือ

1. $a(bc) = (ab)c$ สำหรับทุกๆ $a, b, c \in G$
2. มี $e \in G$ เป็นเอกลักษณ์ นั่นคือ $ae = a = ea$ สำหรับทุกๆ $a \in G$

3. แต่ละสมาชิกของ G มีตัวผกผันใน G นั่นคือสำหรับแต่ละ $a \in G$ มีสมาชิก $b \in G$ ซึ่ง $ab = e = ba$

ขอให้สังเกตจากบทนิยามของกรุปข้อ 2 ว่า เราไม่สามารถนิยามกรุปบนเซตว่างได้ เพราะกรุปต้องมีสมาชิกอย่างน้อยหนึ่งตัวที่เป็นเอกลักษณ์ของกรุป

3.1.2 **ตัวอย่าง** ให้ $Z^e$ เป็นสัญลักษณ์แทนเซตของจำนวนเต็มคู่ทั้งหมดแล้ว $Z^e$ เป็นกรุปภายใต้การบวกในความหมายปกติ เพราะมี 0 เป็นเอกลักษณ์ของ $Z^e$ สำหรับแต่ละ $x \in Z^e$ จะมี $-x \in Z^e$ ซึ่ง $x + (-x) = 0 = (-x) + x$ และเป็นที่ทราบกันดีว่าการบวกสอดคล้องกับกฎการเปลี่ยนหมู่บนเซตของจำนวน ดังนั้นการบวกสอดคล้องกับกฎการเปลี่ยนหมู่บน $Z^e$ ด้วย

แต่ถ้าให้ $Z^+$ เป็นสัญลักษณ์แทนเซตของจำนวนเต็มบวกทั้งหมดแล้ว $Z^+$ กับการบวกในความหมายปกติไม่เป็นกรุป เพราะ $Z^+$ ไม่มีเอกลักษณ์และแม้ว่าจะรวม 0 เป็นสมาชิกของเซตนี้แล้วก็ยังได้ว่า $Z^+ \cup \{0\}$ ไม่เป็นกรุป เพราะสมาชิกของเซตแต่ละตัวไม่มีตัวผกผัน ❍

**หมายเหตุ** ถ้ากล่าวถึงเซตที่เป็นเซตย่อยของเซตของจำนวนจริง จะใช้ "การบวก +" หรือ และ "การคูณ ·" ในความหมายปกติ ถ้าไม่มีการนิยามเป็นอย่างอื่น

3.1.3 **ตัวอย่าง** ให้ A เป็นเซตและนิยามการดำเนิน "*ผลต่างสมมาตร (symmetric difference)* $\Delta$" บนเซตกำลัง P(A) ดังนี้

$$X \Delta Y = (X - Y) \cup (Y - X)$$

สำหรับทุกๆ $X \subseteq A$ และ $Y \subseteq A$ แล้วเห็นได้ชัดโดยทฤษฎีของเซตว่า $\Delta$ สอดคล้องกับกฎการเปลี่ยนหมู่บน P(A) มี $\phi$ เป็นเอกลักษณ์ของ P(A) และแต่ละ $X \subseteq A$ จะได้ว่า X เป็นตัวผกผันของตัวเองดังนั้น $(P(A), \Delta)$ เป็นกรุป ❍

3.1.4 **ตัวอย่าง** สำหรับแต่ละคู่ของจำนวนจริง a และ b ซึ่ง $a \neq 0$ จะนิยามฟังก์ชัน $\alpha_{a,b}: R \rightarrow R$ โดย

$$\alpha_{a,b}(x) = ax + b \qquad \text{..... (3.1.1)}$$

สำหรับแต่ละจำนวนจริง x แล้ว

1. สำหรับแต่ละจำนวนจริง x จะเห็นว่า $\alpha_{1,0}(x) = x$ ซึ่งแสดงว่า $\alpha_{1,0}$ เป็นฟังก์ชันเอกลักษณ์
2. ถ้า $A = \{\alpha_{a,b}: R \rightarrow R \mid a, b \in R, a \neq 0$ และ $\alpha_{a,b}$ มีนิยามดัง (3.1.1)$\}$ แล้วฟังก์ชันประกอบเป็นการดำเนินการบน A เพราะสำหรับ a, b, c, d $\in R$ ซึ่ง $a \neq 0$ และ $c \neq 0$ จะได้ว่า $ac \neq 0$ และ

$$(\alpha_{a,b} \circ \alpha_{c,d})(x) = \alpha_{a,b}(\alpha_{c,d}(x)) = \alpha_{a,b}(cx + d) = a(cx + d) + b$$
$$= acx + ad + b = \alpha_{ac,ad+b}(x)$$

สำหรับทุกๆ $x \in R$

3. เนื่องจากแต่ละ $\alpha_{a,b}$ ที่มีนิยามดัง (3.1.1) เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก R ไปบน R และจากข้อ 2 จะได้ $ac = 1$ และ $ad + b = 0$ ก็ต่อเมื่อ $c = a^{-1}$ และ $d = -a^{-1}b$ ดังนั้นสำหรับแต่ละจำนวนจริง a และ b ซึ่ง $a \neq 0$ จะมี $\alpha_{a^{-1},a^{-1}b}$ เป็นฟังก์ชันผกผันของ $\alpha_{a,b}$
4. เนื่องจาก A เป็นเซตย่อยของหมู่ของฟังก์ชันทั้งหมดจาก R ไปยัง R ดังนั้นฟังก์ชันประกอบสอดคล้องกับกฎการเปลี่ยนหมู่บน A

จาก 1 – 4 ทำให้สรุปได้ว่า (A, ∘) เป็นกรุป ❍

3.1.5 **ตัวอย่าง** ให้ $A = \{a, b, c\}$ และนิยามการดำเนินการ * และ · ดังตารางข้างล่างนี้

| * | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | b | c | a |
| c | c | a | b |

| · | a | b | c |
|---|---|---|---|
| a | c | a | b |
| b | a | b | c |
| c | b | c | a |

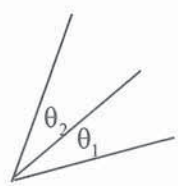
แล้วเห็นได้ชัดว่า * และ · ต่างสอดคล้องกฎการเปลี่ยนหมู่

จากตารางของ * พบว่า a เป็นเอกลักษณ์ของ $\{a, b, c\}$ และตัวผกผันของ a, b, c ภายใต้ * คือ a, b, c ตามลำดับ ส่วนตารางของ · แสดงว่า b เป็นเอกลักษณ์ของ $\{a, b, c\}$ และตัวผกผันของ a, b, c ภายใต้ · คือ c, b, a ตามลำดับ ทำให้สรุปได้ว่า (A,*) และ (A, ·) ต่างก็เป็นกรุป แต่ไม่ใช่กรุปเดียวกัน เพราะว่า $b*b = c$ ใน ขณะที่ $b \cdot b = b$ ซึ่งแสดงว่า * และ · ไม่เป็นฟังก์ชันเดียวกัน ❍

3.1.6 **บทนิยาม** ให้ G เป็นกรุป เราจะกล่าวว่า G เป็น *กรุปอาบีเลียน (abelian group)* หรือ *กรุปสลับที่ (commutative group)* ถ้า ab = ba สำหรับทุกๆ คู่สมาชิก a, b ใน G และจะเรียก G ว่า *กรุปนอนอาบีเลียน (non-abelian group)* ถ้า G ไม่เป็นกรุปอาบีเลียน

กรุปในตัวอย่าง 3.1.2, 3.1.3 และ 3.1.5 เป็นตัวอย่างของกรุปอาบีเลียน ในขณะที่กรุปในตัวอย่าง 3.1.4 เป็นตัวอย่างของนอนกรุปอาบีเลียน เพราะ $\alpha_{1,2} \circ \alpha_{2,3} = \alpha_{2,5}$ แต่ $\alpha_{2,3} \circ \alpha_{1,2} = \alpha_{2,7}$

3.1.7 **ตัวอย่าง** ให้ p เป็นจุดคงตัวจุดหนึ่งในระนาบและ G เป็นเซตของการหมุนระนาบรอบจุด p ถ้าเราพิจารณาว่าการหมุนระนาบรอบจุด p เป็นฟังก์ชันจากเซตของจุดในระนาบไปยังเซตเดิม แล้วสำหรับแต่ละคู่ $\alpha_1$ และ $\alpha_2$ ใน G ซึ่งคือการหมุนระนาบรอบจุด p แบบทวนเข็มนาฬิกาไป $\theta_1$ และ $\theta_2$ เรเดียน ตามลำดับ จะทำให้สามารถนิยาม $\alpha_1\alpha_2$ เป็นการหมุนระนาบรอบจุด p แบบทวนเข็มนาฬิกาไป $\theta_1 + \theta_2$ เรเดียน ดังแสดงในรูป 3.1.1 ทำให้ได้ว่าฟังก์ชันประกอบเป็นการดำเนินการบน G และโดยตัวอย่าง 1.4.2 ฟังก์ชันประกอบสอดคล้องกับกฎการเปลี่ยนหมู่ ฟังก์ชันเอกลักษณ์ใน G คือการหมุนระนาบรอบจุด p เท่ากับ 0 เรเดียนและสำหรับแต่ละการหมุนระนาบรอบจุด p ในทิศทางตรงกันข้ามกับ $\theta$ เรเดียนจะเป็นฟังก์ชันผกผัน




**รูป** 3.1.1

เพราะฉะนั้น G กับฟังก์ชันประกอบเป็นกรุป และเนื่องจากการบวกกันของเรเดียนซึ่งเป็นจำนวนจริง สอดคล้องกฎการสลับที่ ทำให้ได้ว่าฟังก์ชันประกอบบน G สอดคล้องกฎการสลับที่ด้วยซึ่งทำให้ G เป็นกรุปอาบีเลียน ○

3.1.8 **บทนิยาม** ให้ G เป็นกรุป เราเรียกขนาด (cardinality) ของเซต G ว่า *อันดับ (order)* ของ G และเขียนแทนด้วยสัญลักษณ์ $|G|$

ถ้า G เป็นเซตจำกัดแล้วขนาดของ G คือจำนวนสมาชิกของเซต G ดังนั้นอันดับของ G เป็นจำนวนจำกัดและในกรณีเช่นนี้ เราเรียก G ว่า *กรุปจำกัด (finite group)* และถ้า G ไม่เป็นกรุปจำกัดจะเรียก G ว่า *กรุปอนันต์ (infinite group)*

ตัวอย่างเช่น กรุปในตัวอย่าง 3.1.5 เป็นกรุปจำกัดที่มีอันดับ 3 ในขณะที่กรุปของจำนวนเต็มและกรุปในตัวอย่าง 3.1.7 เป็นตัวอย่างของกรุปอนันต์ เป็นต้น

3.1.9 **ตัวอย่าง** ให้ $G = \{1,-1, i ,-i\}$ เป็นเซตย่อยของจำนวนเชิงซ้อนโดยที่ $i^2 = -1$ และพิจารณาการคูณตามความหมายปกติ ดังแสดงในตารางข้างล่างนี้

| $\cdot$ | 1 | –1 | i | –i |
|---|---|---|---|---|
| 1 | 1 | –1 | i | –i |
| –1 | –1 | 1 | –i | i |
| i | i | –i | –1 | 1 |
| –i | –i | i | 1 | –1 |

เห็นได้ชัดว่า G กับการคูณเป็นกรุปอาบีเลียนอันดับจำกัดเท่ากับ 4 โดยมี 1 เป็นเอกลักษณ์และตัวผกผันของ 1,-1, i, -i คือ 1,-1, -i, i ตามลำดับ ❍

3.1.10 **ตัวอย่าง** ให้ n เป็นจำนวนเต็มบวก ในหัวข้อ 2.6 ได้แสดงให้เห็นแล้วว่าเซตสมบูรณ์ $Z_n = \{\bar{0}, \bar{1}, \ldots, \overline{(n-1)}\}$ ของเรซิดิวคลาสมอดูโล m กับการดำเนินการ $\oplus$ เป็นกรุปอาบีเลียนที่มีอันดับ n

หมู่ของกรุป $(Z_n,\oplus)$ ทำให้เห็นตัวอย่างของกรุปจำกัดทุกๆ อันดับ และในการกล่าวถึงการแยกชนิดของกรุปอันดับจำกัด ตัวอย่างของกลุ่มอาบีเลียนที่ยกให้เห็นเสมอจะอยู่ในรูปของกรุป $(Z_n,\oplus)$ ❍

3.1.11 ตัวอย่าง ให้ $S \neq \phi$ เป็นเซตและพิจารณาเซต L(S) ของฟังก์ชันหนึ่งต่อหนึ่งและไปบนทั้งหมดจาก S ไปยัง S แล้วในหัวข้อ 1.3 ได้แสดงให้เห็นแล้วว่าฟังก์ชันประกอบ $\circ$ เป็นการดำเนินการบน L(S) สอดคล้องกับกฎการเปลี่ยนหมู่ แต่ไม่สอดคล้องกับกฎการสลับที่ มีฟังก์ชันเอกลักษณ์เป็นสมาชิกเอกลักษณ์ และแต่ละสมาชิกใน L(S มีตัวผกผัน ดังนั้น $(L(S), \circ)$ เป็นกรุปนอนอาบีเลียน

ถ้า S มีขนาดจำกัดเท่ากับจำนวนเต็มบวก n แล้ว $(L(S), \circ)$ เป็นกรุปจำกัดที่มีอันดับ n! ❍

**3.1.12 ตัวอย่าง** ให้ (G, $*$) และ (H, $\cdot$) เป็นกรุป และนิยามการดำเนินการ $\Diamond : (G\times H)^2 \rightarrow G\times H$ โดย $(a, b)\Diamond(c, d) = (a*c, b\cdot d)$ ซึ่งเราเรียกการดำเนินการที่นิยามในลักษณะเช่นนี้ว่า *การดำเนินการตามองค์ประกอบ(componentwise operation)* แล้วขอละการพิสูจน์ว่า $(G\times H, \Diamond)$ เป็นกรุปซึ่งเรียกว่า *ผลคูณตรง(direct product)* ของกรุป G และ H

นอกจากนี้เห็นได้ชัดว่า ถ้า G และ H ต่างเป็นกรุปจำกัดที่มีอันดับ m และ n ตามลำดับ แล้ว $G\times H$ เป็นกรุปจำกัดด้วยและมีอันดับ mn ❍

## แบบฝึกหัด 3.1

1. จงแสดงว่าเซตของจำนวนกับการบวกและการคูณของจำนวนในความหมายปกติ ที่กำหนดในแต่ละข้อต่อไปนี้เป็นกรุปหรือไม่

   1.1 R, + 1.2 R, $\cdot$ 1.3 {0}, $\cdot$ 1.4 {1 }, $\cdot$

   1.5 {-1, 1}, $\cdot$ 1.6 {-1, 0, 1}, + 1.7 $\{2^m \mid m\in Z\}$

   1.8 $\{10k \mid k\in Z\}$

2. จงแสดงว่าเซต G กับการดำเนินการซึ่งนิยาม $a*b$ ให้สำหรับแต่ละ $a, b\in G$ ในแต่ละข้อต่อไปนี้เป็นกรุปอาบีเลียนหรือไม่ และสำหรับข้อที่ไม่เป็นกรุปอาบีเลียน จงยกคู่ของสมาชิกในกรุปซึ่งไม่สอดคล้องสมบัติสลับที่

   2.1 $G = Z,\ a*b = 0$ 2.2 $G = Q - \{1\},\ a*b = a + b - ab$

   2.3 $G = Z,\ a*b = \min\{a, b\} = \begin{cases} a & \text{ถ้า } a\leq b \\ b & \text{ถ้า } a>b \end{cases}$

   2.4 $G = R^+\times R^+,\ (a,b)*(c,d) = (ac - bd, ad + bc)$

3. ให้ M(2, Z) เป็นเซตของเมตริกซ์ขนาด 2x2 ซึ่งมีสมาชิกเป็นจำนวนเต็มทั้งหมด จงแสดงว่า M(2, Z) กับการบวกของเมตริกซ์เป็นกรุป [นั่นคือสำหรับ a, b, c, d, w, x, y, z จำนวนเต็ม เรานิยาม $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} a+w & b+x \\ c+y & d+z \end{pmatrix}$]

4. จงแสดงว่า $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a \in R - \{0\} \right\}$ เป็นกรุปภายใต้การคูณของเมทริกซ์

5. ให้ S เป็นเซตซึ่ง $S \neq \phi$ และ M(S) แทนเซตของฟังก์ชันทั้งหมดจาก S ไปยัง S จงแสดงว่า M(S) กับการประกอบกันของฟังก์ชันไม่เป็นกรุป

6. ให้ M(R) แทนเซตของฟังก์ชันทั้งหมดจาก R ไปยัง R จงแสดงว่า

   6.1 M(R) กับการบวกระหว่างฟังก์ชัน [นั่นคือสำหรับแต่ละ $f, g \in M(R)$ กำหนดให้ $(f + g)(x) = f(x) + g(x)$ สำหรับทุกๆ $x \in R$] เป็นกรุป

   6.2 $\{f \in M(R) \mid f(x) \neq 0$ สำหรับทุกๆ $x \in R\}$ กับการคูณระหว่างฟังก์ชัน [นั่นคือสำหรับแต่ละ $f, g \in M(R)$ กำหนด $(fg)(x) = f(x)g(x)$ สำหรับทุกๆ $x \in R$] เป็นกรุป

7 จงพิสูจน์ว่าถ้า G และ H เป็นกรุปอาบีเลียน แล้ว $G \times H$ เป็นกรุปอาบีเลียน

8 จงพิสูจน์ว่าถ้า G และ H เป็นกรุปซึ่งสอดคล้องสมบัติที่กล่าวว่า "ทุกๆ สมาชิกเป็นตัวผกผันของตัวเอง" แล้ว $G \times H$ เป็นกรุปซึ่งสอดคล้องสมบัติดังกล่าวด้วย

## 3.2 สมบัติของสมาชิกในกรุปและกฎการยกกำลัง

พิจารณากรุปต่างๆ จะเห็นว่าแต่ละกรุปมีเอกลักษณ์เพียงตัวเดียว และแต่ละสมาชิกของกรุปก็มีตัวผกผันเพียงตัวเดียวในกรุปนั้นๆ ในหัวข้อนี้เราจะศึกษาความจริงเหล่านี้ พร้อมทั้งศึกษากฎการคูณในกรุปทุกๆ กรุป ตลอดจนสมบัติที่เกี่ยวกับสมาชิกในกรุป

3.2.1 **ทฤษฎีบท** ให้ G เป็นกรุป แล้ว

1. เอกลักษณ์ของ G จะมีเพียงหนึ่งเดียว
2. แต่ละสมาชิกของ G จะมีตัวผกผันเพียงหนึ่งเดียว

**บทพิสูจน์** ให้ G เป็นกรุป

1. ให้ e และ f ต่างเป็นเอกลักษณ์ของ G แล้ว $ex = x = xe$ สำหรับทุกๆ $x \in G$ ....(ก) และ $fy = y = yf$ สำหรับทุกๆ $y \in G$ ....(ข) ดังนั้นถ้าแทน x ด้วย f ในข้อความ (ก) จะได้ $ef = f$ และในทำนองเดียวกันถ้าแทน y ด้วย e ในข้อความ (ข) จะได้ $ef = f$ ทำให้ได้ $e = ef = f$

2. ให้ e แทนเอกลักษณ์ของ G ให้ $a \in G$ และให้ b และ c ต่างเป็นตัวผกผันของ a แล้ว $ab = e = ba$ และ $ca = e = ac$ ทำให้ได้ $b = be = b(ac) = (ba)c = ec = c$ ❐

**ข้อตกลง** ขอทบทวนว่า สำหรับเซตๆ หนึ่งที่มีการกำหนดการดำเนินการที่แตกต่างกันสองการดำเนินการบนเซตนั้น ถ้าเซตเดียวกันนั้นกับแต่ละการดำเนินการเป็นกรุป แล้วกรุปทั้งสองที่เกิดขึ้นไม่เป็นกรุปเดียวกัน ดังนั้นการกล่าวถึงกรุปทั้งสองจะกล่าวเฉพาะเซตของกรุปอย่างเดียวไม่ได้ อย่างไรก็ตามในการกล่าวถึงกรุปนามธรรมทั่วๆ ไป ที่ไม่มีการกำหนดการดำเนินการอย่างชัดแจ้ง หรือไม่มีการนิยามการดำเนินการที่ต่างกันบนเซตนั้นมากกว่าหนึ่งการดำเนินการ เรานิยมเขียนเฉพาะเซตแทนกรุป เช่นกล่าวว่า "กรุป G" เป็นต้น โดยเรียกภาพของแต่ละคู่ a, b ในเซตว่า "ผลคูณของ a และ b" และเขียนแทนด้วยสัญลักษณ์ ab

เนื่องจากเอกลักษณ์ของกรุปมีเพียงหนึ่งเดียวและตัวผกผันของแต่ละสมาชิกในกรุปก็มีเพียงหนึ่งเดียว เราจึงอาจใช้สัญลักษณ์แทนสิ่งที่มีเพียงหนึ่งเดียวได้ เพราะจะไม่ทำให้เกิดการสับสน และเรานิยมใช้ e และ $a^{-1}$ แทนเอกลักษณ์ของกรุปและตัวผกผันของสมาชิก a ในกรุปตามลำดับ สำหรับกรุปที่ใช้สัญลักษณ์แทนการดำเนินการเป็น "การบวก +" เราจะใช้สัญลักษณ์ a + b, 0 และ -a แทน ab, e และ $a^{-1}$ ตามลำดับ

ในกรณีที่มีการกล่าวถึงกรุปหลายๆ กรุปพร้อมๆ กัน จะใช้สัญลักษณ์ $e_G$ แทนเอกลักษณ์ของกรุป G

3.2.2 **ทฤษฎีบท** ให้ G เป็นกรุป แล้ว

1. $(a^{-1})^{-1} = a$ สำหรับทุกๆ $a \in G$
2. $(ab)^{-1} = b^{-1}a^{-1}$ สำหรับทุกๆ $a, b \in G$

**บทพิสูจน์** 1. ให้ $a \in G$ แล้วเพราะว่า $(a^{-1})^{-1}$ และ $a^{-1}$ เป็นตัวผกผันของ $a^{-1}$ และของ a ตามลำดับ ทำให้ได้ $a^{-1}a = e = aa^{-1}$ ซึ่งแสดงว่า a เป็นตัวผกผันของ $a^{-1}$ เช่นกัน แต่ทฤษฎีบท 3.2.1 กล่าวว่าตัวผกผันของ $a^{-1}$ มีเพียงหนึ่งเดียว ดังนั้น $(a^{-1})^{-1}$ และ a จึงต้องเป็นสมาชิกตัวเดียวกันใน G เพราะฉะนั้น $(a^{-1})^{-1} = a$

2. ให้ $a, b \in G$ เพราะว่า $(ab)^{-1}$ เป็นตัวผกผันของ ab ดังนั้นการแสดงว่า $(ab)^{-1} = b^{-1}a^{-1}$ จึงเพียงพอที่จะพิสูจน์ว่า $b^{-1}a^{-1}$ เป็นตัวผกผันของ ab เช่นกัน เพราะว่า

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$$

และ $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$

ดังนั้น $b^{-1}a^{-1}$ เป็นตัวผกผันของ ab ตามต้องการ ❐

3.2.3 **กฎการตัดออก (Cancellation Law)** ให้ G เป็นกรุป ถ้า $a,b,c \in G$ และ $ab = ac$ แล้ว $b = c$

**บทพิสูจน์** ให้ $a, b, c \in G$ โดยที่ $ab = ac$ แล้ว $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c$ ❐

3.2.4 **ทฤษฎีบท** ให้ G เป็นกรุปและ $a, b \in G$ แล้วสมการ $ax = b$ และ $xa = b$ แต่ละสมการมีคำตอบใน G เพียงคำตอบเดียวคือ $x = a^{-1}b$ และ $x = ba^{-1}$ ตามลำดับ

**บทพิสูจน์** ให้ $a, b \in G$ แล้วเพราะว่า $a(a^{-1}b) = (aa^{-1})b = eb = b$ และ $(ba^{-1})a = b(a^{-1}a) = be = b$ ดังนั้น $a^{-1}b$ และ $ba^{-1}$ เป็นคำตอบของสมการ $ax = b$ และ $xa = b$ ตามลำดับ

ต่อไปให้ c และ d เป็นคำตอบของสมการ $ax = b$ และ $xa = b$ ตามลำดับ แล้ว $ac = b$ และ $da = b$ ตามลำดับ ทำให้ได้ $c = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b$ และ $d = d(aa^{-1}) = (da)a^{-1} = ba^{-1}$ ซึ่งแสดงว่าสมการ $ax = b$ และ $xa = b$ แต่ละสมการมีคำตอบใน G เพียงคำตอบเดียว คือ $x = a^{-1}b$ และ $x = ba^{-1}$ ตามลำดับ ❐

เนื่องจากการดำเนินการของกรุปสอดคล้องกับกฎการเปลี่ยนหมู่ ทฤษฎีบทการวางนัยทั่วไปของกฎการเปลี่ยนหมู่ จึงเป็นจริงสำหรับการดำเนินการของกรุปด้วย ทำให้ได้ว่าสำหรับแต่ละจำนวนเต็มบวก n ผลคูณของสมาชิก n ตัว $a_1, a_2, \ldots, a_n$ ในกรุปในอันดับ $a_1, a_2, \ldots, a_n$ จะเท่ากันเสมอและเท่ากับ $\prod_{i=1}^{n} a_i$ ไม่ว่าการเปลี่ยนหมู่ในอันดับ $a_1, a_2, \ldots, a_n$ จะเป็นเช่นใดก็ตาม ดังนั้นการคูณสมาชิก n ตัวใดๆ เราอาจละวงเล็บโดยเขียนผลคูณ $\prod_{i=1}^{n} a_i$ ได้เป็น $a_1a_2 \ldots a_n$ และถ้า $a_1 = a_2 = \ldots = a_n = a$ แล้ว $a^n = a^{n-1}a$

เมื่อประยุกต์ทฤษฎีบทการวางนัยทั่วไปของกฎการเปลี่ยนหมู่ ทฤษฎีบท 3.2.2 และอุปนัยเชิงคณิตศาสตร์ เราจะได้บทแทรกต่อไปนี้

3.2.5 **บทแทรก** ถ้า G เป็นกรุป แล้ว $(a_1a_2\ldots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\ldots a_2^{-1}a_1^{-1}$ สำหรับทุกๆ $a_1, a_2, \ldots, a_n \in G$ และทุกๆ จำนวนเต็มบวก n ❐

3.2.6 **บทนิยาม** ให้ G เป็นกรุปที่มี e เป็นเอกลักษณ์และ $a \in G$ จะใช้สัญลักษณ์ $a^0$ แทน e และสำหรับแต่ละจำนวนเต็มบวก n จะเรียก $a^n = a^{n-1}a$ ว่า *กำลัง n ($n^{th}$ power)* ของ a หรือ *a ยกกำลัง n (a power n)* และใช้สัญลักษณ์ $a^{-n}$ แทนตัวผกผันของ $a^n$

ดังนั้นถ้า n เป็นจำนวนเต็มลบแล้ว $a^n$ คือตัวผกผันของ $a^{-n}$ ทำให้กล่าวถึงทฤษฎีบทเกี่ยวกับการคูณและตัวผกผันของสมาชิกในรูปยกกำลังได้ดังนี้

3.2.7 **ทฤษฎีบท** ให้ G เป็นกรุป $a \in G$ และ m และ n เป็นจำนวนเต็ม แล้ว

1. $a^{-n} = (a^n)^{-1} = (a^{-1})^n$
2. $a^n a^m = a^{n+m}$
3. $(a^n)^m = a^{nm}$

**บทพิสูจน์** ให้ G เป็นกรุป $a \in G$ และ m และ n เป็นจำนวนเต็ม

1. เนื่องจาก $a^0 = a^{-0} = e$ ดังนั้นข้อ 1 เป็นจริงเมื่อ $n = 0$ และสำหรับ $n > 0$ เราได้ว่า $e = e^n = (aa^{-1})^n = (aa^{-1})(aa^{-1}) \ldots (aa^{-1})$ (n ครั้ง) และ $e = e^n = (a^{-1}a)^n = (a^{-1}a)(a^{-1}a) \ldots (aa^{-1})$ (n ครั้ง) และ $aa^{-1} = a^{-1}a$ ดังนั้น $e = e^n = a^n(a^{-1})^n$ และ $e = e^n = (a^{-1})^n a^n$ ซึ่งแสดงว่า $(a^{-1})^n$ เป็นตัวผกผันของ $a^n$ ทำให้ได้ $(a^n)^{-1} = (a^{-1})^n$ แต่โดยนิยามทำให้ได้ว่า $a^{-n} = (a^n)^{-1}$

ถ้า $n < 0$ แล้ว $-n > 0$ ให้ $m = -n$ แล้วโดยกรณี $n > 0$ จะได้ $a^{-n} = ((a^{-n})^{-1})^{-1} = (a^{-1})^m)^{-1} = (a^{-m})^{-1} = (a^n)^{-1}$ และ $a^{-n} = [(a^{-1})^{-1}]^{-n} = [(a^{-1})^{-1}]^m = ((a^{-1})^m)^{-1} = (a^{-1})^{-m} = (a^{-1})^n$ ซึ่งแสดงว่า $(a^n)^{-1} = a^{-n} = (a^{-1})^n$

2. ถ้า $n = 0$ หรือ $m = 0$ หรือ $m + n = 0$ (นั่นคือ m และ n ต่างภาวะกัน) แล้วเห็นได้ชัดว่าข้อ 2 เป็นจริง จึงเหลือที่จะต้องแสดงกรณีที่ m และ n มีภาวะเดียวกัน

ถ้า m และ n เป็นจำนวนเต็มบวกทั้งคู่ สำหรับแต่ละ m จะแสดงว่าข้อ 2 เป็นจริงโดยอุปนัยเชิงคณิตศาสตร์บน n ถ้า $n = 1$ เห็นได้ชัดโดยบทนิยามในรูปอุปนัยของ $a^m$ ว่า $a^m a^1 = a^m a = a^{m+1}$ จึงสมมติให้ $a^m a^k = a^{m+k}$ สำหรับแต่ละจำนวนเต็มบวก k ทำให้ได้ว่า $a^m a^{k+1} = a^m(a^k a) = (a^m a^k)a = a^{m+k}a = a^{(m+k)+1} = a^{m+(k+1}$

ถ้า m และ n เป็นจำนวนเต็มลบทั้งคู่ แล้ว -m และ -n เป็นจำนวนเต็มบวกทั้งคู่ แล้วโดยผลของกรณีเป็นจำนวนเต็มบวกทั้งคู่และทฤษฎีบท 3.2.3 ข้อ 2 จะได้

$$a^m a^n = a^{-(-m)}a^{-(-n)} = (a^{-m}a^{-n})^{-1} = (a^{-m-n})^{-1} = (a^{-(m+n)})^{-1} = a^{m+n}$$

3. ถ้า $m = 0$ หรือ $n = 0$ แล้วเห็นได้ชัดว่าข้อ 3 เป็นจริง จึงสมมติให้ $m \neq 0$ และ $n \neq 0$

ให้ m เป็นจำนวนเต็มที่ไม่เป็นศูนย์ ถ้า $n > 0$ เราสามารถพิสูจน์ด้วยอุปนัยเชิงคณิตศาสตร์ในทำนองเดียวกับการพิสูจน์ข้อ 2 และถ้า $n < 0$ แล้ว $-n > 0$ ทำให้พิสูจน์ได้โดยใช้ผลของกรณี $n > 0$ ❐

สำหรับกรุปที่มีการดำเนินการคือการบวกซึ่งกล่าวแล้วว่าเราจะใช้สัญลักษณ์ 0, -a และ a+b แทนเอกลักษณ์ ตัวผกผันของ a และผลบวกของ a และ b ตามลำดับ ดังนั้น $a^n$ จึงกลายเป็น na ซึ่งหมายถึงผลบวก n ครั้ง (a + a +…+ a) ของ a และทฤษฎีบท 3.2.5 ของกรณีนี้จึงเขียนได้เป็นดังนี้

1. $n(-a) = -(na) = (-n)a$
2. $na + m = (n + m)a$
3. $n(ma) = (nm)a$

## แบบฝึกหัด 3.2

1. ให้ G เป็นกรุปซึ่งมี e เป็นเอกลักษณ์และ $a, b, c \in G$ จงพิสูจน์ข้อความในข้อต่อไปนี้
   1.1 ถ้ามี $a \in G$ ซึ่ง $ab = b$ แล้ว $a = e$
   1.2 ถ้า $ab = e$ แล้ว $ba = e$
   1.3 ถ้า $abc = e$ แล้ว $cab = e = bca$
   1.4 ถ้าตัวผกผันของ a, b, c คือตัวมันเอง และ $ab = c$ แล้ว $bc = a$ และ $ca = b$
2. ให้ G เป็นเซตจำกัด จงแสดงว่าถ้ามีการดำเนินการบน G ซึ่งสอดคล้องสมบัติการเปลี่ยนหมู่และกฎการตัดออกใน G แล้ว G กับการดำเนินการดังกล่าวเป็นกรุป
3. ให้ G เป็นกรุปและ $a, b, c \in G$ จงหา $x \in G$ ทั้งหมดซึ่งสอดคล้องกับทุกๆ สมการที่กำหนดในแต่ละข้อต่อไปนี้
   3.1 $x^2b = xa^{-1}c$ 3.2 $x^2a = bxc^{-1}$ และ $acx = xac$
   3.3 $x^2 = a^2$ และ $x^5 = e$ 3.4 $(xax)^3 = bx$ และ $x^2a = (xa)^{-1}$
4. ให้ n เป็นจำนวนเต็มบวกและ $Z_n = \{\bar{0}, \bar{1}, \ldots, \overline{(n-1)}\}$ เป็นเซตของเรซิดิวคลาสมอดูโล n แล้ว $Z_n$ กับ $\otimes$ เป็นกรุป ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

5. ให้ G เป็นเซตซึ่ง $G \neq \phi$ แลมีการดำเนินการที่นิยามบน G สอดคล้องสมบัติการเปลี่ยนหมู่และสมบัติว่าถ้า $a, b \in G$ แล้วจะมี $c, d \in G$ ซึ่ง $ca = b$ และ $ad = b$ จงแสดงว่า G กับการดำเนินการนี้เป็นกรุป
6. ให้ G เป็นเซตซึ่ง $G \neq \phi$ และมีการดำเนินการที่นิยามบน G สอดคล้องสมบัติการเปลี่ยนหมู่และสมบัติต่อไปนี้

   (ก) มี $e \in G$ ซึ่ง $ea = a$ สำหรับทุกๆ $a \in G$

   (ข) ถ้า $a \in G$ แล้วจะมี $b \in G$ ซึ่ง $ba = e$

   จงแสดงว่า G กับการดำเนินการนี้เป็นกรุป
7. จงพิสูจน์ว่า G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ $(ab)^n = a^n b^n$ สำหรับทุกๆ จำนวนเต็ม n และทุกๆ $a, b \in G$
8. จงพิสูจน์ว่าถ้า G เป็นกรุปซึ่ง $a^2 = e$ สำหรับทุกๆ $a \in G$ แล้ว G เป็นกรุปอาบีเลียน
9. จงสร้างกรุปนอนอาบีเลียนขนาด 2n สำหรับแต่ละจำนวนเต็มบวก n
10. ให้ G เป็นกรุป จงพิสูจน์ว่า

    10.1 ถ้า $a, b \in G$ ซึ่ง $ab = ba$ แล้ว $a^{-1}b^{-1} = b^{-1}a^{-1}$, $ab^{-1} = b^{-1}a$, $a^2b = aba$, $a^2b^2 = b^2a^2$

    10.2 $ab = ba$ ก็ต่อเมื่อ $aba^{-1} = b$ สำหรับทุกๆ $a, b \in G$

    10.3 $ab = ba$ ก็ต่อเมื่อ $aba^{-1}b^{-1} = e$ สำหรับทุกๆ $a, b \in G$

## 3.3 กรุปย่อย

การศึกษาโครงสร้างของกรุป เรามีวิธีหลักอยู่ 2 วิธี วิธีหนึ่งคือการหากรุปย่อยทั้งหมดของกรุปนั้นๆ เพื่อแยกพิจารณาโครงสร้างของแต่ละกรุปย่อยซึ่งมีขนาดเล็กกว่า แต่ยังคงมีโครงสร้างของกรุปใหญ่นั้นอยู่ อีกวิธีหนึ่งคือการหาฟังก์ชันสาทิสสัณฐานจากกรุปที่พิจารณาอยู่ไปยังกรุปที่คุ้นเคย ทำให้เราเห็นโครงสร้างบางส่วนของกรุปนั้นๆ จากภาพของฟังก์ชันสาทิสสัณฐาน จะเห็นว่าวิธีทั้งสองดังกล่าวมีจุดมุ่งหมายเดียวกัน แต่เป็นวิธีการที่ต่างกัน ในหัวข้อนี้เราจะศึกษาวิธีแรกก่อน โดยเริ่มศึกษาวิธีการเกี่ยวกับกรุปย่อยและในบทต่อๆ ไป จึงจะกล่าวถึงฟังก์ชันสาทิสสัณฐาน

จากตัวอย่างในหัวข้อ 3.1 จะเห็นว่ามีบางเซตย่อยของกรุปเท่านั้นที่สอดคล้องกับบทนิยามของกรุปภายใต้การดำเนินการเดียวกัน ตัวอย่างเช่น $Z^e$ เป็นเซตย่อยของเซต Z และต่างก็เป็นกรุปภายใต้การบวกเช่นเดียวกัน เป็นต้น เซตย่อยของกรุปที่มีสมบัติเป็นกรุปดังกล่าว เราเรียกว่ากรุปย่อย

3.3.1 **บทนิยาม** ให้ G เป็นกรุปและ H เป็นเซตย่อยของ G จะเรียก H ว่า *กรุปย่อย (subgroup)* ของ G ถ้า H เป็นกรุปภายใต้การดำเนินการของ G ซึ่งกำกัดลงบน H

3.3.2 **ตัวอย่าง** ในตัวอย่างนี้แสดงกรุปย่อยของกรุป

1. ภายใต้การบวกในความหมายปกติบนเซตของจำนวน จะได้ว่า Z เป็นกรุปย่อยของ Q และ Q เป็นกรุปย่อยของ R และ R เป็นกรุปย่อยของ C
2. {–1, 1} เป็นกรุปย่อยของกรุปของจำนวนจริง R ภายใต้การคูณในความหมายปกติ
3. สำหรับแต่ละจำนวนเต็มคงตัว k จะได้ $\{mk \mid m \in Z\}$ เป็นกรุปย่อยของ Z
4. ทุกๆ กรุปเป็นกรุปย่อยของตัวเอง
5. ถ้า e เป็นเอกลักษณ์ของกรุป G แล้ว {e} เป็นกรุปย่อยของ G
6. ถ้า G เป็นกรุปและ $a \in G$ แล้ว $\{a^n \mid n \in Z\}$ เป็นกรุปย่อยของ G
7. ถ้า G และ H เป็นกรุป แล้ว $\{e_G\} \times H$ และ $G \times \{e_H\}$ เป็นกรุปย่อยของกรุปผลคูณตรง $G \times H$

❍

เราสังเกตว่าถ้า H เป็นกรุปย่อยของ G แล้วเอกลักษณ์ของ H ต้องสอดคล้องกับสมการ $e_H x = e_H$ ใน H ซึ่งสมการดังกล่าวมี $e_H$ เป็นเพียงคำตอบเดียว นั่นคือ $e_H e_H = e_H$ และเอกลักษณ์นี้ต้องเป็นจริงใน G จึงทำให้ได้ $e_H = e_H^{-1} e_H = e_G$ จึงได้ว่าเอกลักษณ์ของ H และของ G เป็นตัวเดียวกัน หรือกล่าวอีกนัยหนึ่งได้ว่า เอกลักษณ์ของ G เป็นเอกลักษณ์ของทุกๆ กรุปย่อยของ G ยิ่งไปกว่านั้นเราทราบแล้วว่าตัวผกผันของแต่ละสมาชิกในกรุปมีเพียงตัวเดียว ดังนั้นตัวผกผันของแต่ละ h ในกรุปย่อยต้องคือตัวผกผันของ h ใน G

สำหรับการพิจารณาว่าเซตย่อย H ของ G เป็นกรุปย่อยของ G หรือไม่ เราต้องแสดงว่า H กับการคูณใน G ซึ่งกำกัดลงบน H สอดคล้องกับบทนิยาม 3.1.1 อย่างแรกก็คือแสดงว่าการคูณใน G ซึ่งกำกัดลงบน H เป็นการดำเนินการบน H และเพราะว่าการคูณเป็นฟังก์ชัน เราจึงเหลือเพียงแสดงว่าการคูณเป็นฟังก์ชันจาก $H \times H$ ไปยัง H นั่นคือแสดงว่า $ab \in H$ สำหรับทุกๆ $a, b \in H$ ซึ่งเราเรียกสมบัติของ H เช่นนี้ว่า "สมบัติปิด (closure law) " อย่างที่สองต้องแสดงว่าการคูณสอดคล้องกฎการเปลี่ยนหมู่ใน H ด้วย ซึ่งโดยแบบฝึกหัดท้ายหัวข้อ 1.4 ได้แสดงให้เห็นแล้วถ้าการคูณสอดคล้องกฎการเปลี่ยนหมู่ในเซตใหญ่ การคูณก็จะสอดคล้องกฎการเปลี่ยนหมู่ในเซตย่อย และสุดท้ายในย่อหน้าก่อน

เราได้แสดงแล้วว่าเอกลักษณ์ของ G เป็นเอกลักษณ์ของ H และตัวผกผันของแต่ละ h ใน H คือตัวผกผันของ h ใน G

เราจึงได้เกณฑ์การตรวจสอบว่าเซตย่อย H ของกรุป G เป็นกรุปย่อยของ G หรือไม่ จะต้องแสดงดังต่อไปนี้

1. H มีสมบัติปิดภายใต้การคูณของ G (H is closed under operation of G) นั่นคือแสดงว่า $ab \in H$ สำหรับทุกๆ $a, b \in H$

2. $e \in H$ เมื่อ e เป็นเอกลักษณ์ของ G

3. ถ้า $a \in H$ แล้ว $a^{-1} \in H$ เมื่อ $a^{-1}$ เป็นตัวผกผันของ a ใน G

3.3.3 **เกณฑ์การตรวจสอบกรุปย่อย** (Subgroup Criterion) ให้ G เป็นกรุปและ $\phi \neq H \subseteq G$ ข้อความต่อไปนี้สมมูลกัน

1. H เป็นกรุปย่อยของ G

2. ข้อความ (ก) และ (ข) ต่อนี้เป็นจริง

   (ก) $ab \in H$ สำหรับทุกๆ $a, b \in H$ และ (ข) $a^{-1} \in H$ สำหรับทุกๆ $a \in H$

3. $ab^{-1} \in H$ สำหรับทุกๆ $a, b \in H$

**บทพิสูจน์** (1) $\Rightarrow$ (2) เห็นได้ชัดโดยนิยามของกรุปย่อย ในการพิสูจน์ (2) $\Rightarrow$ (3) ให้ $a, b \in H$ แล้วโดย (ข) จะได้ $b^{-1} \in H$ ซึ่งทำให้ได้โดย (ก) ว่า $ab^{-1} \in H$

ในการพิสูจน์ (3) $\Rightarrow$ (1) ให้ $\phi \neq H \subseteq G$ และสอดคล้องข้อความ "$ab^{-1} \in H$ สำหรับทุกๆ $a, b \in H$" และจะแสดงว่า H สอดคล้องกับบทนิยาม 3.1.1 ดังนี้

1. การคูณสอดคล้องกฎการเปลี่ยนหมู่ โดยการวิเคราะห์ข้างต้น

2. จาก $H \neq \phi$ ดังนั้นจะมี $a \in H$ แล้วโดยสมมติฐานจะได้ $aa^{-1} \in H$ แต่ $aa^{-1} = e$ เป็นเอกลักษณ์ใน G เพราะฉะนั้นเอกลักษณ์ e ของ G เป็นสมาชิกของ H และดังนั้นเป็นเอกลักษณ์ของ H ด้วย

3. ให้ $a \in H$ แล้วโดยสมมติฐานจะได้ว่า $e = aa^{-1} \in H$ แต่โดยสมบัติของ $a^{-1}$ ซึ่งเป็นตัวผกผันของ a ใน G จะได้ว่า $aa^{-1} = a^{-1}a$ เพราะฉะนั้น $a^{-1}a \in H$ ซึ่งโดยสมมติฐานอีกครั้ง จะได้ว่า $(a^{-1}a)a^{-1} \in H$ แต่ $(a^{-1}a)a^{-1} = a^{-1}(aa^{-1}) = a^{-1}e = a^{-1}$ ดังนั้น $a^{-1} \in H$

จาก (1), (2) และ (3) ทำให้ได้ว่า H เป็นกรุปภายใต้การดำเนินการของ G เพราะฉะนั้น H เป็นกรุปย่อยของ G ❐

3.3.4 **บทแทรก** ให้ G เป็นกรุปและ $\phi \neq H \subseteq G$ ถ้า H เป็นเซตจำกัดและมีสมบัติปิดภายใต้การดำเนินการของ G แล้ว H เป็นกรุปย่อยของ G

**บทพิสูจน์** ให้ $a \in H$ แล้วเนื่องจาก H มีสมบัติปิด จะได้ว่าสมาชิก $a, a^2, a^3, \ldots, a^k, \ldots$ ต่างเป็นสมาชิกของ H แต่เพราะ H เป็นเซตจำกัด ดังนั้นสมาชิกดังกล่าวจะไม่แตกต่างกันทั้งหมด ทำให้ได้ว่ามีจำนวนเต็ม $m > n > 0$ ซึ่ง $a^m = a^n$ และโดยทฤษฎีบท 3.2.5 จะได้ว่า $a^{m-n} = e$ ซึ่งสมมูลกับ $e = a^{m-n} = (a^{m-n-1})a = a(a^{m-n-1})$ ทำให้ได้ว่า $a^{-1} = a^{m-n-1} \in H$ ซึ่งแสดงว่าถ้า $a \in H$ แล้ว $a^{-1} \in H$

ให้ $a, b \in H$ แล้วโดยย่อหน้าก่อนจะได้ $b^{-1} \in H$ ทำให้ได้ว่า $ab^{-1} \in H$ เพราะ H มีสมบัติปิด ดังนั้นโดยเกณฑ์การตรวจสอบกรุปย่อยจะได้ว่า H เป็นกรุปย่อยของ G ❐

จากตัวอย่าง 3.1.2 ซึ่งแสดงว่า $Z^+$ ไม่เป็นกรุปภายใต้การบวกในความหมายปกติบนเซตของจำนวน ดังนั้น $Z^+$ ไม่เป็นกรุปย่อยของ R แม้ว่า $Z^+$จะมีสมบัติปิดภายใต้การบวกก็ตาม ทำให้เราเห็นตัวอย่างที่แสดงว่า บทแทรก 3.3.4 ไม่เป็นจริงสำหรับเซตย่อยของกรุปอนันต์

3.3.5 **บทแทรก** ให้ G เป็นกรุปจำกัดและ $\phi \neq H \subseteq G$ ถ้า H มีสมบัติปิดภายใต้การดำเนินการของ G แล้ว H เป็นกรุปย่อยของ G

**บทพิสูจน์** เนื่องจาก G เป็นเซตจำกัด ดังนั้น H จะเป็นเซตจำกัดและจะได้โดยตรงจากบทแทรก 3.3.4 ว่า H เป็นกรุปย่อยของ G ❐

3.3.6 **ตัวอย่าง** พิจารณากรุป $G = \{1,-1, i ,-i\}$ ในตัวอย่าง 3.1.9 เราพบว่า $\{1,-1\}$ มีสมบัติปิดภายใต้การคูณของ G และ G เป็นกรุปจำกัด ดังนั้นโดยบทแทรก 3.3.5 จะได้ว่า $\{1,-1\}$ เป็นกรุปย่อยของ G ❍

เนื่องจากกรุปย่อยของกรุปเป็นเซตย่อยของกรุป เราจึงควรศึกษาพฤติกรรมของกรุปย่อยทั้งหลายภายใต้การดำเนินการของเซต ได้แก่ "ส่วนร่วม (intersection)" และ "ส่วนรวม (union)"

เราสังเกตว่าถ้า $K = \{3m \mid m \in Z\}$ และ $H = \{4m \mid m \in Z\}$ แล้วโดยตัวอย่าง 3.3.2 ข้อ 3 จะได้ว่า K และ H ต่างเป็นกรุปย่อยของ Z ภายใต้การบวกและเราเห็นได้ชัดว่า

$$K \cap H = \{12m \mid m \in Z\}$$

เป็นเซตในรูปแบบเดียวกันกับ K และ H ดังนั้นโดยตัวอย่าง 3.3.2 ข้อ 3 จะได้ว่า $K \cap H$ เป็นกรุปย่อยของ Z เราจะแสดงว่าความจริงเช่นนี้เกิดขึ้นในกรณีทั่วไปด้วย

3.3.7 **ทฤษฎีบท** ให้ C แทนหมู่ของกรุปย่อยของกรุป G แล้วส่วนร่วม $\cap C$ ของสมาชิกใน C เป็นกรุปย่อยของ G

**บทพิสูจน์** ให้ $H = \cap C$ แล้วเพราะเอกลักษณ์ e ของ G เป็นเอกลักษณ์ของทุกๆ กรุปย่อยของ G ดังนั้น $e \in H$ ทำให้ได้ว่า H ไม่เป็นเซตว่าง ต่อไปให้ $a, b \in H$ แล้ว a และ b เป็นสมาชิกของทุกๆ กรุปย่อยใน C ทำให้ได้โดยเกณฑ์การตรวจสอบกรุปย่อยว่า $ab^{-1}$ เป็นสมาชิกของทุกๆ กรุปย่อยเหล่านั้น ดังนั้น $ab^{-1} \in H$ ซึ่งโดยเกณฑ์การตรวจสอบกรุปย่อยอีกครั้งหนึ่ง จะได้ว่า H เป็นกลุ่มย่อยของ G ❐

พิจารณา $K = \{\bar{0}, \bar{6}\}$ และ $H = \{\bar{0}, \bar{4}, \bar{8}\}$ ซึ่งต่างก็เป็นกรุปย่อยของ $Z_{12}$ แต่ $K \cup H = \{\bar{0}, \bar{4}, \bar{6}, \bar{8}\}$ ไม่เป็นกรุปย่อยของ $Z_{12}$ เพราะ $\{\bar{0}, \bar{4}, \bar{6}, \bar{8}\}$ ไม่มีสมบัติปิดภายใต้การบวกของ $Z_{12}$ แสดงว่าโดยทั่วไปแล้วส่วนรวมของกรุปย่อยของ G อาจไม่เป็นกรุปย่อยของ G

เราจึงศึกษาหาเงื่อนไขที่จะทำให้ส่วนรวมของกรุปย่อยของกรุป G เป็นกรุปย่อยของ G

3.3.8 **ทฤษฎีบท** ให้ K และ H เป็นกรุปย่อยของกรุป G แล้ว $K \cup H$ เป็นกรุปย่อยของ G ก็ต่อเมื่อ $K \subseteq H$ หรือ $H \subseteq K$

**บทพิสูจน์** ให้ K และ H เป็นกรุปย่อยของกรุป G ซึ่ง K ไม่เป็นเซตย่อยของ H และ H ไม่เป็นเซตย่อยของ K แล้วจะมี $a, b \in G$ ซึ่ง $a \in K - H$ และ $b \in H - K$ แล้วพิจารณาผลคูณ ab ดังนี้

ถ้า $ab \in K$ แล้วเพราะ $a^{-1} \in K$ ดังนั้น $b = (a^{-1}a)b = a^{-1}(ab) \in K$ แต่ $b \in H - K$ ทำให้เกิดเป็นข้อขัดแย้งกันเอง และถ้า $ab \in H$ ก็จะเกิดข้อขัดแย้งกันเองในทำนองเดียวกัน เพราะฉะนั้น ab ไม่เป็นสมาชิกของ $K \cup H$ ทั้งๆ ที่ $a, b \in K \cup H$ ทำให้ได้ว่า $K \cup H$ ไม่เป็นกรุปย่อยของ G เพราะ $K \cup H$ ไม่มีสมบัติปิด

ต่อไปให้ K และ H เป็นกรุปย่อยของกรุป G ซึ่ง $K \subseteq H$ หรือ $H \subseteq K$ แล้ว $K \cup H = H$ หรือ $K \cup H = K$ ซึ่งไม่ว่ากรณีใด $K \cup H$ เป็นกรุปย่อยของ G ❐

โดยทฤษฎีบท 3.3.8 จะได้ว่าทุกๆ กรุปจะไม่เป็นส่วนรวมของกรุปย่อยซึ่งเป็นเซตย่อยแท้ของกรุปนั้น ทั้งนี้เพราะถ้า K และ H เป็นกรุปย่อยของกรุป G ซึ่งต่างเป็นเซตย่อยแท้ของ G และ $G = K \cup H$ แล้วทฤษฎีบท 3.3.8 จะทำให้ได้ $G = K \cup H = K$ หรือ $G = K \cup H = H$ ซึ่งไม่ว่ากรณีใดจะทำให้ G เป็นเซตย่อยแท้ของ G เองซึ่งเป็นไปไม่ได้

## แบบฝึกหัด 3.3

1. จงแสดงว่าเซตที่กำหนดในข้อต่อไปนี้เป็นกรุปย่อยของกรุปในตัวอย่าง 3.1.4

   1.1 $\{\alpha_{a,0} \mid a \in R$ และ $a \neq 0\}$ 1.2 $\{\alpha_{1,b} \mid b \in R\}$

2. จงพิสูจน์ว่ากรุปย่อยของกรุปย่อยจะเป็นกรุปย่อย นั่นคือถ้า A เป็นกรุปย่อยของกรุป G และ B เป็นกรุปย่อยของ A แล้ว B เป็นกรุปย่อยของ G
3. จงแสดงว่า $\{\overline{0}, \overline{4}, \overline{8}, \overline{12}\}$ เป็นกรุปย่อยของ $Z_{16}$
4. จงพิสูจน์ว่า A เป็นกรุปย่อยของ (Z; +) ก็ต่อเมื่อ มีจำนวนเต็มบวก m ซึ่ง $A = \{km \mid k \in Z\}$
5. ให้ G เป็นกรุปและ $\phi \neq H \subseteq G$ จงแสดงว่าข้อความต่อไปนี้สมมูลกัน

   (ก) H เป็นกรุปย่อยของ G

   (ข) $H^2 \subseteq H$ และ $H^{-1} \subseteq H$ เมื่อ $H^2 = HH$ และ $H^{-1} = \{a^{-1} \mid a \in H\}$

   (ค) $HH^{-1} \subseteq H$

   (ง) ถ้า $h \in H$ แล้ว $hH = H$
6. ให้ G เป็นกรุป จงแสดงว่า $H = \{ a \in G \mid (ax)^2 = (xa)^2$ สำหรับทุกๆ $x \in G \}$ เป็นกรุปย่อยของ G
7. ให้ G เป็นกรุปและ $f : G \rightarrow G$ เป็นฟังก์ชัน เราเรียก $a \in G$ ว่า *คาบ(period)* ของ f ถ้า $f(x) = f(ax)$ สำหรับทุกๆ $x \in G$

   จงพิสูจน์ว่าถ้า $H_f$ เป็นเซตของคาบของ f ทั้งหมด แล้ว $H_f$ เป็นกรุปย่อยของ G

8. ให้ H เป็นกรุปย่อยของกรุป G และให้ $K = \{x \in G \mid xax^{-1} \in H$ ก็ต่อเมื่อ $a \in H\}$ จงพิสูจน์ว่า K เป็นกรุปย่อยของ G และ H เป็นกรุปย่อยของ K
9. ให้ G และ H เป็นกรุป จงพิสูจน์ว่า
   9.1 $\{(a, e) \mid a \in G\}$ เป็นกรุปย่อยของ $G \times H$
   9.2 $\{(a, a) \mid a \in G\}$ เป็นกรุปย่อยของ $G \times G$
10. ให้ G เป็นกรุปอาบีเลียน
   10.1 จงพิสูจน์ว่า $H^{(n)} = \{a^n \mid a \in G\}$ เป็นกรุปย่อยของ G สำหรับทุกจำนวนเต็มบวก n
   10.2 จงแสดงว่า $\bigcup_{n \geq 1} H^{(n)}$ ยังคงเป็นกรุปย่อยของ G หรือไม่

## 3.4 ตัวก่อกำเนิดและกรุปวัฏจักร

ให้ G เป็นกรุปและ $\phi \neq S \subseteq G$ เราอาจพิจารณาหมู่ C ของกรุปย่อยของ G ทั้งหลายที่มี S เป็นเซตย่อยของกรุปย่อยเหล่านั้น นั่นคือ

$$C = \{H \mid H \text{ เป็นกรุปย่อยของ } G \text{ และ } S \subseteq H\}$$

แล้ว C เป็นหมู่ของกรุปย่อยของกรุป G ดังนั้นโดยทฤษฎีบท 3.3.7 ส่วนร่วม $\cap C$ ของสมาชิกใน C เป็นกรุปย่อยของ G นอกจากนี้ $\cap C$ เป็นกรุปย่อยเล็กสุดของ G ที่มี S เป็นเซตย่อย เพราะว่าถ้า H เป็นกรุปย่อยของ G ซึ่ง $S \subseteq H$ แล้ว $H \in C$ ทำให้ได้ $\cap C \subseteq H$

3.4.1 **บทนิยาม** ให้ G เป็นกรุปและ $\phi \neq S \subseteq G$ เราใช้สัญลักษณ์ $\langle S \rangle$ แทนกรุปย่อยเล็กสุดของ G ที่มี S เป็นเซตย่อย นั่นคือ

$$\langle S \rangle = \cap\{H \mid H \text{ เป็นกรุปย่อยของ } G \text{ และ } S \subseteq H\}$$

และเรียกว่า *กรุปย่อยที่ก่อกำเนิดโดย S (subgroup generated by S)* โดยเรียก S ว่า *ตัวก่อกำเนิด (generator)* ของกรุปย่อย $\langle S \rangle$

ถ้า S เป็นเซตจำกัดนั่นคือ $S = \{a_1, a_2, \ldots, a_n\}$ สำหรับบางจำนวนเต็ม n เรานิยมใช้สัญลักษณ์ $\langle a_1, a_2, \ldots, a_n \rangle$ แทน $\langle \{a_1, a_2, \ldots, a_n\} \rangle$

ขอให้สังเกตว่า $\langle S \rangle$ เป็นกรุปย่อยของ G ซึ่งสอดคล้องสมบัติ 3 ประการต่อไปนี้

1. $S \subseteq <S>$
2. $<S>$ เป็นกรุปย่อยของ G
3. ถ้า H เป็นกรุปย่อยของ G และ $S \subseteq H$ แล้ว $<S> \subseteq H$

ตัวอย่างเช่น กรุปของจำนวนเต็มทั้งหมดเป็นกรุปย่อยของจำนวนจริงที่เล็กสุดซึ่งมีเซตของจำนวนเต็มคี่ทั้งหมดเป็นเซตย่อย ดังนั้นกรุปของจำนวนเต็มทั้งหมดก่อกำเนิดโดยเซตของจำนวนเต็มคี่ทั้งหมด เป็นต้น

แม้ว่าเราจะทราบว่า $<S>$ เป็นกรุปย่อยของ G ที่เล็กสุดซึ่งมี S เป็นเซตย่อยก็ตาม เราก็ยังต้องการทราบว่าอะไรบ้างที่เป็นสมาชิกของ $<S>$ และจะสัมพันธ์กับสมาชิกของ S อย่างไร เราจะแสดงในทฤษฎีบทต่อไปว่าสมาชิกของ $<S>$ เขียนได้ในรูปผลคูณจำกัดของสมาชิกใน S

3.4.2 **ทฤษฎีบท** ให้ G เป็นกรุปและ $\phi \neq S \subseteq G$ แล้วทุกๆ สมาชิกของ $<S>$ เขียนได้ในรูปผลคูณ $a_1a_2 \ldots a_n$ ของสมาชิก $a_i \in S$ หรือ $a_i^{-1} \in S$ สำหรับ $i = 1, 2, \ldots, n$ หรือกล่าวได้ว่า

$$<S> = \{a_1a_2 \ldots a_n \mid a_i \in S \text{ หรือ } a_i^{-1} \in S\}$$

**บทพิสูจน์** ให้ $H = \{a_1a_2 \ldots a_n \mid a_i \in S \text{ หรือ } a_i^{-1} \in S\}$ และให้ $x, y \in H$ แล้วจะมี $a_1, \ldots, a_n, b_1, b_2, \ldots, b_m \in S$ หรือ $a_1^{-1}a_2^{-1}, \ldots, a_n^{-1}, b_1^{-1}, \ldots, b_m^{-1} \in S$ ซึ่ง $x = a_1a_2 \ldots a_n$ และ $y = b_1b_2 \ldots b_m$ ทำให้ได้ $xy^{-1} = a_1a_2 \ldots a_nb_m^{-1} \ldots b_1^{-1} \in H$ ดังนั้น H เป็นกรุปย่อยของ G ยิ่งไปกว่านั้น $S \subseteq H$ และเพราะว่า $<S>$ เป็นกรุปย่อยของ G ที่เล็กสุดซึ่งมี S เป็นเซตย่อย เราจะได้ $<S> \subseteq H$

แต่ $<S>$ เป็นกรุปย่อยของ G ซึ่งมี S เป็นเซตย่อย ทำให้ได้ว่าทุกๆ สมาชิกของ S เป็นสมาชิกของ $<S>$ และเพราะ $<S>$ มีสมบัติปิด ดังนั้นสมาชิกในรูปผลคูณ $a_1a_2 \ldots a_n$ เมื่อ $a_i \in S$ หรือ $a_i^{-1} \in S$ จะเป็นสมาชิกของ $<S>$ ซึ่งแสดงว่า $H \subseteq <S>$

จาก $<S> \subseteq H$ และ $H \subseteq <S>$ เราจะได้ $H = <S>$ ตามต้องการ ❐

กรณีเฉพาะที่สำคัญของกรุปย่อยที่มี S เป็นเซตย่อย เกิดขึ้นเมื่อ S เป็นเซตโทน นั่นคือเซตที่ประกอบด้วยสมาชิก a ของ G เพียงตัวเดียว และโดยทฤษฎีบท 3.4.2 ทำให้ได้บทแทรกต่อไปนี้

3.4.3 **บทแทรก** ให้ G เป็นกรุปและ $a \in G$ แล้ว $<a> = \{a^n \mid n \in Z\}$
[สำหรับกรุปที่มีการดำเนินการคือการบวก เราจะได้ $<a> = \{na \mid n \in Z\}$] ❐

3.4.4 **บทนิยาม** ให้ G เป็นกรุปและ $a \in G$ เราเรียก <a> ว่า *กรุปย่อยวัฏจักร (cyclic subgroup)* ของ G ที่มี a เป็นตัวก่อกำเนิด และถ้ามี $a \in G$ ซึ่ง G = <a> จะเรียก G ว่า *กรุปวัฏจักร (cyclic group)* ที่มี a เป็นตัวก่อกำเนิด

ถ้า G เป็นกรุปวัฏจักร แล้วบทแทรก 3.4.3 ทำให้ทราบว่าสมาชิกของ G เขียนได้ในรูปกำลังต่างๆ ของ a ซึ่งเป็นตัวก่อกำเนิดของ G และเนื่องจาก $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$ สำหรับทุกๆ จำนวนเต็ม m และ n ดังนั้นทุกๆ กรุปวัฏจักรเป็นกรุปอาบีเลียน ยิ่งไปกว่านั้น $\langle a \rangle = \langle a^{-1} \rangle$ สำหรับทุกๆ $a \in G$ นั่นคือถ้า a เป็นตัวก่อกำเนิดกรุป G แล้วตัวผกผัน $a^{-1}$ ของ a เป็นตัวก่อกำเนิดกรุป G ด้วย

พิจารณากรุปของจำนวนเต็ม Z จะได้ว่า <0> = { 0 }, $Z^e$ = <2> = <-2> และ Z = <1> = <-1> นั่นคือ Z และ $Z^e$ เป็นตัวอย่างของกรุปวัฏจักรที่มี 1 และ 2 เป็นตัวก่อกำเนิดตามลำดับ

3.4.5 **ตัวอย่าง** พิจารณากรุปย่อย <9, 12 > ของกรุปของจำนวนเต็ม Z จะเห็นว่า $3 = 12 + (-9) \in$ <9, 12 > ทำให้ได้ว่าพหุคูณของ 3 ทุกตัวเป็นสมาชิกของ <9,12> จึงได้ $\langle 3 \rangle \subseteq \langle 9, 12 \rangle$ แต่ $\{9, 12\} \subseteq \langle 3 \rangle$ และ <9, 12> เป็นกรุปย่อยเล็กสุดของ Z ที่มี 9 และ 12 เป็นสมาชิก ดังนั้น $\langle 9, 12 \rangle \subseteq \langle 3 \rangle$ เพราะฉะนั้น <9, 12> = <3>

เราสังเกตว่า 3 เป็นตัวหารร่วมมากของ 9 และ 12 ดังนั้นเราอาจดำเนินวิธีการข้างต้นเพื่อพิสูจน์ในกรณีทั่วไปว่า ถ้า m และ n เป็นจำนวนเต็มและ d = (m, n) แล้ว <m, n > = <d> ❍

3.4.6 **ตัวอย่าง** พิจารณากรุป $\{1,-1, i ,-i\}$ ในตัวอย่าง 3.1.9 จะเห็นว่า $i^0 = 1$, $i^1 = 1$, $i^2 = -1$ และ $i^3 = -i$ ดังนั้น $\{1,-1, i ,-i\} = \langle i \rangle$ เป็นกรุปย่อยวัฏจักรของจำนวนเชิงซ้อน C ❍

พิจารณากรุปของจำนวนเต็มภายใต้การบวกซึ่งได้แสดงไว้ข้างต้นแล้วว่าเป็นกรุปวัฏจักร และขอให้สังเกตว่าทุกๆ กรุปย่อยของกรุปของจำนวนเต็มภายใต้การบวก สามารถเขียนได้ในรูป <n> เมื่อ n เป็นจำนวนเต็ม ทฤษฎีบทต่อไปจะแสดงความจริงเช่นนี้ในกรณีทั่วไปว่า ทุกๆ กรุปย่อยของกรุปวัฏจักรเป็นกรุปวัฏจักร

3.4.7 **ทฤษฎีบท** ทุกๆ กรุปย่อยของกรุปวัฏจักรเป็นกรุปวัฏจักร

**บทพิสูจน์** ให้ $G = \langle a \rangle$ เป็นกรุปวัฏจักรและ H เป็นกรุปย่อยของ G แล้วทุกสมาชิกของ G และของ H เขียนได้ในรูป $a^k$ เมื่อ k เป็นจำนวนเต็มและถ้า e เป็นเอกลักษณ์ของ G แล้ว $\{e\} = \langle e \rangle$ เป็นกรุปย่อยวัฏจักร จึงจะพิจารณากรณีที่ $H \neq \{e\}$ ดังนั้นจะมีจำนวนเต็ม m ที่ไม่ใช่ 0 ซึ่ง $a^m \in H$ และเพราะ H เป็นกรุปย่อยของ G จึงได้ว่า $a^m$ และ $a^{-m}$ ต่างเป็นสมาชิกของ H ซึ่งแสดงว่า H มีสมาชิกในรูปกำลังที่เป็นบวกของ a ทำให้ได้โดยหลักการเป็นอันดับอย่างดีว่าจะมีจำนวนเต็มบวก n ตัวน้อยสุดซึ่ง $a^n \in H$

ต่อไปจะแสดงว่า $H = \langle a^n \rangle$ เนื่องจาก $a^n \in H$ ดังนั้น $\langle a^n \rangle \subseteq H$ จึงให้ $a^k$ เป็นสมาชิกของ H เมื่อ k เป็นจำนวนเต็ม แล้วโดยขั้นตอนการหาร จะมีจำนวนเต็ม q และ r ซึ่ง $k = nq + r$ โดยที่ $0 \leq r < n$ ทำให้ได้ว่า $a^r = a^{k-nq} = a^k(a^n)^{-q}$ และเพราะ $a^k$ และ $a^n$ ต่างเป็นสมาชิกของกรุปย่อย H ดังนั้น $a^r \in H$ แล้วโดยการเลือก n เป็นจำนวนเต็มบวกตัวน้อยสุดของและ $r \geq 0$ ทำให้ได้ $r = 0$ และได้ $a^k = a^{nq} = (a^n)^q \in \langle a^n \rangle$ ซึ่งเป็นอันจบการพิสูจน์ ❐

จากบทพิสูจน์ของทฤษฎีบท 3.4.7 ทำให้ได้ว่าถ้า a เป็นตัวก่อกำเนิดของกรุปวัฏจักร G แล้ว การหาตัวก่อกำเนิดของกรุปย่อย H ของ G ก็คือการหาจำนวนเต็มบวก n ตัวน้อยสุดที่ทำให้ $a^n \in H$

3.4.8 **บทแทรก** ถ้า $\{e\} \neq H$ เป็นกรุปย่อยของกรุป $\langle a \rangle$ แล้ว $H = \langle a^n \rangle$ เมื่อ n เป็นจำนวนเต็มบวกน้อยสุดซึ่ง $a^n \in H$ ❐

ต่อไปเราจะศึกษาสมบัติและโครงสร้างที่สำคัญของกรุปย่อยวัฏจักร

3.4.9 **ทฤษฎีบท** ให้ G เป็นกรุปที่มี e เป็นเอกลักษณ์ $a \in G$ และมีจำนวนเต็ม r และ s ซึ่ง $r \neq s$ ที่ทำให้ $a^r = a^s$ แล้ว

1. มีจำนวนเต็มบวก n ตัวน้อยสุดซึ่ง $a^n = e$
2. ถ้า t เป็นจำนวนเต็มแล้ว $a^t = e$ ก็ต่อเมื่อ n เป็นตัวหารของ t
3. $e = a^0, a, a^2, \ldots, a^{n-1}$ เป็นสมาชิกที่ต่างกันทั้งหมดใน G และ $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$

**บทพิสูจน์** ให้ G เป็นกรุปที่มี e เป็นเอกลักษณ์ $a \in G$ และมีจำนวนเต็ม r และ s ซึ่ง $r \neq s$ ที่ทำให้ $a^r = a^s$

1. เราอาจสมมติให้ $r < s$ แล้ว $s - r > 0$ เนื่องจาก $a^r = a^s$ ดังนั้น $a^{s-r} = e$ เราจึงกำหนดให้ $T = \{m \in Z^+ \mid a^m = e\}$ แล้ว $s - r$ เป็นสมาชิกของ T ดังนั้น T เป็นเซตย่อยที่ไม่ใช่เซตว่างของ $Z^+$ เรา

จะได้โดยหลักการเป็นอันดับอย่างดีว่า T มีสมาชิกตัวน้อยสุด ให้ n เป็นสมาชิกตัวน้อยสุดของ T แล้ว $a^n = e$

2. ให้ t เป็นจำนวนเต็ม แล้วโดยขั้นตอนการหารจะมีจำนวนเต็ม q และ r ซึ่ง $t = nq + r$ โดยที่ $0 \leq r < n$ ถ้า $a^t = e$ แล้ว $e = a^t = a^{nq+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$ แต่เพราะ $r < n$ จึงได้ว่า r ไม่เป็นสมาชิกของ S ถ้า $r > 0$ ดังนั้น $a^r = e$ ก็ต่อเมื่อ $r = 0$ ทำให้ได้ $t = nq$ ซึ่งแสดงว่า n เป็นตัวหารของ t

สำหรับบทกลับถ้า n เป็นตัวหารของ t แล้วจะมีจำนวนเต็ม q ซึ่ง $t = nq$ เพราะฉะนั้น $a^t = a^{nq} = (a^n)^q = e^q = e$

3. เพื่อจะแสดงว่า $a^0, a, a^2, \ldots, a^{n-1}$ เป็นสมาชิกที่ต่างกันทั้งหมดใน G เราจะสมมติในทางตรงกันข้ามว่ามี $0 \leq r < s < n$ ที่ทำให้ $a^r = a^s$ ดังนั้น $a^{s-r} = e$ และ $s - r > 0$ แต่โดยข้อ 2 จะได้ว่า n เป็นตัวหารของ $s - r$ โดยที่ $s - r < n$ ซึ่งจะเกิดขึ้นพร้อมๆ กันได้ ก็ต่อเมื่อ $s - r = 0$ นั่นคือก็ต่อเมื่อ $s = r$ ซึ่งทำให้เกิดเป็นข้อขัดแย้งกันเอง ดังนั้น $a^0, a, a^2, \ldots, a^{n-1}$ เป็นสมาชิกที่ต่างกันทั้งหมดใน G

สำหรับแต่ละจำนวนเต็ม m จะได้ $a^m \in \langle a \rangle$ ดังนั้น $\{e, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$ ต่อไปให้ x เป็นสมาชิกใดๆ ใน $\langle a \rangle$ แล้วจะมีจำนวนเต็ม t ซึ่ง $x = a^t$ และโดยขั้นตอนการหาร จะมีจำนวนเต็ม q และ r ซึ่ง $t = nq + r$ โดยที่ $0 \leq r < n$ ทำให้ได้ $a^t = a^{nq+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$ แต่เพราะ $0 \leq r < n$ ดังนั้น $a^t = a^r \in \{e, a, \ldots, a^{n-1}\}$ เพราะฉะนั้น $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$ ❐

**3.4.10 บทแทรก** ให้ G เป็นกรุปวัฏจักรที่มีอันดับจำกัดเท่ากับ n ถ้า a เป็นตัวก่อกำเนิดของ G แล้ว

1. $a^0, a, a^2, \ldots, a^{n-1}$ เป็นสมาชิกที่ต่างกันทั้งหมดใน G
2. $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$
3. n เป็นจำนวนเต็มบวกตัวน้อยสุดซึ่ง $a^n = e$
4. $a^k = a^j$ ก็ต่อเมื่อ $k \equiv j \pmod{n}$ สำหรับทุกๆ จำนวนเต็ม k และ j ❐

**3.4.11 บทนิยาม** ให้ G เป็นกรุปและ $a \in G$ เราเรียกจำนวนเต็มบวก n ตัวน้อยสุดซึ่ง $a^n = e$ ว่า *อันดับ (order)* ของ a และเขียนแทนด้วยสัญลักษณ์ $|a|$ และกล่าวว่า a มี *อันดับจำกัด (finite order)* [สำหรับกรุปที่มีการดำเนินการคือการบวก จะได้ว่า a มีอันดับ n ก็ต่อเมื่อ $na = 0$ ]

แต่ถ้าไม่มีจำนวนเต็มดังกล่าวสำหรับ a จะกล่าวว่า a มี *อันดับอนันต์ (infinite order)*

ขอให้สังเกตว่าคำว่า 'อันดับ' ถูกกำหนดใช้ใน 2 ความหมายคืออันดับของกรุปซึ่งคือขนาดของกรุปและอันดับของสมาชิก a ในกรุปซึ่งคือจำนวนเต็มบวก n ตัวน้อยสุดที่ทำให้ $a^n = e$ หรือ $na = 0$ และแม้ว่าความหมายทั้งสองของ 'อันดับ' จะต่างกัน ทฤษฎีบท 3.4.12 ต่อไปนี้จะกล่าวถึงความสัมพันธ์ของความหมายทั้งสอง

3.4.12 **ทฤษฎีบท** ให้ G เป็นกรุปและ $a \in G$ แล้ว

1. $|a| = |\langle a \rangle|$
2. ถ้า n และ m เป็นจำนวนเต็มบวกซึ่ง $|a| = n$ และ $a^m = e$ แล้ว n เป็นตัวหารของ m

**บทพิสูจน์** ให้ G เป็นกรุปและ $a \in G$

1. ถ้า $|a|$ เป็นจำนวนจำกัดเท่ากับจำนวนเต็มบวก n แล้วโดยบทแทรก 3.4.9 จะได้ว่า $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ ทำให้ได้ $|\langle a \rangle| = n = |a|$ แต่ถ้า a มีอันดับอนันต์แล้วจะไม่มีจำนวนเต็มบวก m ใดๆ ซึ่ง $a^m = e$ นั่นคือถ้า r และ s เป็นจำนวนเต็มที่ต่างกัน แล้ว $a^r \neq a^s$ ดังนั้นเซต $\{e, a, a^2, \ldots, a^{n-1}, \ldots\}$ เป็นเซตย่อยของ $\langle a \rangle$ ดังนั้น $|\langle a \rangle|$ เป็นจำนวนอนันต์

2. ให้ n และ m เป็นจำนวนเต็มบวกซึ่ง $|a| = n$ และ $a^m = e$ แล้วโดยความหมายของ $|a| = n$ จะได้ว่า $m \geq n$ ดังนั้นโดยขั้นตอนการหาร จะมีจำนวนเต็ม q และ r ซึ่ง $m = nq + r$ โดยที่ $0 \leq r < n$ ทำให้ได้ว่า $e = a^m = a^{nq+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$ แต่ n เป็นจำนวนเต็มบวกน้อยสุดซึ่ง $a^n = e$ ทำให้ได้ $r = 0$ เพราะฉะนั้น n เป็นตัวหารของ m ❐

3.4.13 **บทแทรก** ถ้า G เป็นกรุปวัฏจักรอันดับจำกัด n แล้วจะมี $a \in G$ ซึ่ง $a^n = e$ ❐

3.4.14 **บทแทรก** มีกรุปวัฏจักรอันดับ n สำหรับแต่ละจำนวนเต็มบวก n

**บทพิสูจน์** ให้ n เป็นจำนวนเต็มบวกแล้ว $Z_n = \langle \bar{1} \rangle = \{m\bar{1} \mid m \in Z\}$ เป็นกรุปวัฏจักรและ $Z_n$ มีสมาชิก n ตัว ❐

3.4.15 **ตัวอย่าง** เนื่องจาก $Z_2$ เป็นกรุปวัฏจักรอันดับ 2 ดังนั้น $Z_2 \times Z_2$ เป็นกรุปที่มีอันดับ 4 ให้ $a \in Z_2$ แล้ว $a^2 = 0$ ทั้งนี้เพราะ $Z_2 = \{\bar{0}, \bar{1}\}$ โดยที่ $\bar{0} \oplus \bar{0} = \bar{0}$ และ $\bar{1} \oplus \bar{1} = \bar{0}$ ดังนั้นถ้า $(a, b) \in Z_2 \times Z_2$

แล้ว $(a, b)^2 = (a^2, b^2) = (\bar{0},\bar{0})$ ซึ่งแสดงว่าไม่มีสมาชิกตัวใดของ $Z_2 \times Z_2$ ที่มีอันดับ 4 ทำให้สรุปโดยบทแทรก 3.4.12 ได้ว่า $Z_2 \times Z_2$ ไม่เป็นกรุปวัฏจักร ❍

ในการศึกษาที่ผ่านมา ยังไม่มีการกล่าวถึงวิธีการหาตัวก่อกำเนิดของกรุปวัฏจักรและจากตัวอย่างของกรุปวัฏจักร จะเห็นว่ามีสมาชิกของกรุปวัฏจักรที่ไม่เป็นตัวก่อกำเนิด เช่น 1 และ -1 จะไม่เป็นตัวก่อกำเนิดของกรุปวัฏจักร $\{1,-1, i ,-i\}$ และเช่นเดียวกันจำนวนเต็มตัวอื่นๆ ที่ไม่ใช่ 1 และ -1 จะไม่เป็นตัวก่อกำเนิดกรุป Z เป็นต้น ดังนั้นต่อไปนี้เราจึงควรกล่าวถึงเกณฑ์การพิจารณาว่าสมาชิกตัวใดของกรุปวัฏจักรเป็นตัวก่อกำเนิดของกรุปวัฏจักรนั้น

3.4.16 **ทฤษฎีบท** ให้ G เป็นกรุปวัฏจักรอันดับจำกัด n ถ้า m และ d เป็นจำนวนเต็มบวกซึ่ง $d = (n, m)$ แล้ว $|a^m| = r$ เมื่อ $n = rd$

**บทพิสูจน์** ให้ $d = (n, m)$ แล้วจะมีจำนวนเต็มบวก r และ s ซึ่ง $n = rd$ และ $m = sd$ โดยที่ $(r, s) = 1$ ดังนั้น $(a^m)^r = (a^{sd})^r = (a^s)^{dr} = (a^s)^n = (a^n)^s = e^s = e$ ซึ่งแสดงว่ามีจำนวนเต็มบวก r ซึ่ง $(a^m)^r = e$ ทำให้ได้โดยหลักการเป็นอันดับอย่างดีว่าจะมีจำนวนเต็มบวก q ตัวน้อยสุดซึ่ง $a^{mq} = e$ นั่นคือ $|a^m| = q$ และโดยทฤษฎีบท 3.4.11 จะได้ r เป็นตัวหารของ q

แต่ n เป็นตัวหารของ mq นั่นคือ rd เป็นตัวหารของ sdq ซึ่งสมมูลกับ r เป็นตัวหารของ sq โดยที่ $(r, s) = 1$ จึงได้ว่า r เป็นตัวหารของ q เพราะฉะนั้นจาก r เป็นตัวหารของ q และ q เป็นตัวหารของ r จะได้ $r = q = |a^m|$ ❐

ขอให้สังเกตว่าถ้า $d = 1$ ในทฤษฎีบท 3.4.16 เราจะได้บทแทรกต่อไปนี้

3.4.17 **บทแทรก** ให้ m และ n เป็นจำนวนเต็มบวก แล้ว $|a^m| = n$ ก็ต่อเมื่อ $(n, m) = 1$ ❐

3.4.18 **ทฤษฎีบท** ให้ G เป็นกรุปวัฏจักรที่ก่อกำเนิดโดย $a \in G$

1. ถ้า G เป็นกรุปจำกัดอันดับ n แล้ว $a^m$ เป็นตัวก่อกำเนิดของ G ก็ต่อเมื่อ $(n, m) = 1$ สำหรับทุกๆ จำนวนเต็มบวก m

2. ถ้า G เป็นกรุปอนันต์ แล้ว a และ $a^{-1}$ เท่านั้นที่เป็นตัวก่อกำเนิดของ G

**บทพิสูจน์** ข้อ 1 เป็นผลโดยตรงของบทแทรก 3.4.16 ในการพิสูจน์ข้อ 2 เรากำหนดให้ G เป็นกรุปอนันต์และสมมติว่ามีจำนวนเต็ม m ที่ไม่ใช่ 1 และ -1 ซึ่ง $a^m$ เป็นตัวก่อกำเนิดของ G แล้วเพราะ $a \in G$ ดังนั้นจะมีจำนวนเต็ม k ซึ่ง $a = a^{mk}$ ทำให้ได้ว่า $a^{mk-1} = e$ นั่นคือมีจำนวนเต็ม mk–1 ที่ไม่ใช่ 0 ที่ทำให้ $a^{mk-1} = e$ ซึ่งจะทำให้ได้ G เป็นกรุปจำกัด เกิดข้อขัดแย้งกับสมมติฐาน ทำให้สรุปว่า m คือ 1 หรือ -1

❐

ถ้ามีคำถามว่า จะมีสมาชิกที่ต่างกันทั้งหมดในกรุป G เป็นจำนวนเท่าใดที่เป็นตัวก่อกำเนิดของ G จะเห็นว่าทฤษฎีบท 3.4.18 ได้ให้คำตอบแล้วว่า จะมีเท่ากับจำนวนเต็มซึ่งเป็นจำนวนเฉพาะสัมพัทธ์กับอันดับของ G และโดยทฤษฎีบทของออยเลอร์ในทฤษฎีจำนวน ก็จะทำให้ได้ว่ามีตัวก่อกำเนิดของกรุป G ที่ต่างกันทั้งหมด $\varphi(n)$ ตัว เมื่อ n เป็นอันดับของ G

ก่อนจบหัวข้อนี้ จะแสดงวิธีการสร้างกรุปย่อยขึ้นใหม่จากกรุปย่อยเดิมหรือจากกรุปที่กำหนด ซึ่งจะเป็นประโยชน์สำหรับการศึกษาเรื่องกรุปต่อไป

3.4.19 **บทนิยาม** ให้ G เป็นกรุปและ H และ K เป็นเซตย่อยของ G ซึ่งต่างไม่เป็นเซตว่าง เราเรียกเซตที่นิยามดังนี้

$$HK = \{hk \mid h \in H \text{ และ } k \in K\}$$

ว่า *ผลคูณ (product)* ของ H และ K

ถ้า H = K จะใช้สัญลักษณ์ $H^2$ แทน HH ในทำนองเดียวกันถ้า H หรือ K เป็นเซตที่ประกอบสมาชิกเพียงตัวเดียว {a} จะใช้สัญลักษณ์ Ha หรือ aK แทน H{a} หรือ {a}K ตามลำดับ

| . | e | a | $a^2$ | b | c | d |
|---|---|---|---|---|---|---|
| e | e | a | $a^2$ | b | c | d |
| a | a | $a^2$ | e | c | d | b |
| $a^2$ | $a^2$ | e | a | d | b | c |
| b | b | d | c | e | $a^2$ | a |
| c | c | b | d | a | e | $a^2$ |
| d | d | c | b | $a^2$ | a | e |

ปัญหาแรกที่เราควรจะพิจารณาก็คือถ้า H และ K ต่างเป็นกรุปย่อยของกรุป G แล้ว HK ยังคงเป็นกรุปย่อยของ G หรือไม่ เราจะตอบคำถามนี้ด้วยการพิจารณากรุป $G = \{e, a, a^2, b, c, d\}$ ซึ่งมีตารางการคูณแสดงดังตารางข้างบน แล้วจะเห็นว่า $H = \{e, b\}$ และ $K = \{e, c\}$ ซึ่งต่างเป็นกรุปย่อยของ G แต่เซต $HK = \{e, b, c, a^2\}$ และ $KH = \{e, b, c, a\}$ ต่างก็ไม่เป็นกรุปย่อยของ G และยิ่งไปกว่านั้นเราสังเกตว่า $HK \neq KH$

ทฤษฎีบทต่อไป จะแสดงให้เห็นว่า HK = KH เป็นเงื่อนไขจำเป็นและเพียงพอที่จะทำให้ HK เป็นกรุปย่อยของ G

3.4.20 **ทฤษฎีบท** ให้ H และ K เป็นกรุปย่อยของกรุป G แล้ว HK เป็นกรุปย่อยของ G ก็ต่อเมื่อ HK = KH

**บทพิสูจน์** ให้ HK เป็นกรุปย่อยของ G และให้ $h \in H$ และ $k \in K$ แล้วผลคูณ $kh = (h^{-1}k^{-1})^{-1}$ เป็นตัวผกผันของ $h^{-1}k^{-1} \in HK$ ดังนั้น $kh \in HK$ ซึ่งแสดงว่า $KH \subseteq HK$ ในทางกลับกันให้ $a \in HK$ แล้ว $a^{-1} \in HK$ ดังนั้นจะมี $h_1 \in H$ และ $k_1 \in K$ ซึ่ง $a^{-1} = h_1k_1$ ทำให้ได้ $a = (a^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1}$ และเพราะว่า $k_1^{-1} \in K$ และ $h_1^{-1} \in H$ ดังนั้น $a \in KH$

ในการพิสูจน์บทกลับ กำหนดให้ HK = KH แล้วเพราะ $e \in H$ และ $e \in K$ ดังนั้น $e = ee \in HK$ ซึ่งแสดงว่า HK ไม่เป็นเซตว่าง ต่อไปให้ $a, b \in HK$ แล้วจะมี $h, h_1 \in H$ และ $k, k_1 \in K$ ซึ่ง $a = hk$ และ $b = h_1k_1$ ซึ่งทำให้ได้

$$ab^{-1} = (hk)(h_1k_1)^{-1} = (hk)(k_1^{-1}h_1^{-1}) = h((kk_1^{-1})h_1^{-1})$$

แต่เพราะว่า $kk_1^{-1} \in K$ ดังนั้น $(kk_1^{-1})h_1^{-1} \in KH$ โดยที่ KH = HK ทำให้ได้ $(kk_1^{-1})h_1^{-1} \in HK$ จึงมี $h_2 \in H$ และ $k_2 \in K$ ซึ่ง $(kk_1^{-1})h_1^{-1} = h_2k_2$ เพราะฉะนั้น

$$ab^{-1} = h((kk_1^{-1})h_1^{-1}) = h(h_2k_2) = (hh_2)k_2 \in HK$$

โดยเกณฑ์การตรวจสอบกรุปย่อย เราจะได้ว่า HK เป็นกรุปย่อยของ G ❐

3.4.21 **บทแทรก** ถ้า H และ K เป็นกรุปย่อยของกรุปอาบีเลียน G แล้ว HK เป็นกรุปย่อยของ G ❐

เราสังเกตต่อไปว่า ถ้า H และ K เป็นกรุปย่อยของกรุป G แล้ว $H = He \subseteq HK$ และ $K = eK \subseteq HK$ ทำให้ได้ว่า $H \cup K \subseteq HK$ ดังนั้นถ้า HK เป็นกรุปย่อยของ G แล้ว HK เป็นกรุปย่อยที่มี $H \cup K$

เป็นเซตย่อย ทฤษฎีบทสุดท้ายเราจะแสดงว่าถ้า HK เป็นกรุปย่อยของ G แล้ว HK เป็นกรุปย่อยเล็กสุดที่มี $H \cup K$ เป็นเซตย่อย นั่นคือ $HK = \langle H \cup K \rangle$

3.4.22 **ทฤษฎีบท** ให้ H, K และ HK เป็นกรุปย่อยของกรุป G แล้ว $HK = \langle H \cup K \rangle$

**บทพิสูจน์** ด้วยการวิเคราะห์ในย่อหน้าก่อน เราจะได้ว่า HK เป็นกรุปย่อยที่มี $H \cup K$ เป็นเซตย่อย แต่ $\langle H \cup K \rangle$ เป็นกรุปย่อยเล็กสุดที่มี $H \cup K$ เป็นเซตย่อย ดังนั้น $\langle H \cup K \rangle \subseteq HK$

ในทางกลับกัน เพราะว่า $H \subseteq H \cup K$ และ $K \subseteq H \cup K$ และ $\langle H \cup K \rangle$ มีสมบัติปิดภายใต้การดำเนินการของ G ดังนั้น $hk \in \langle H \cup K \rangle$ สำหรับทุกๆ $h \in H$ และ $k \in K$ ซึ่งแสดงว่า $HK \subseteq \langle H \cup K \rangle$ จึงเป็นอันจบการพิสูจน์ ❐

3.4.23 **ตัวอย่าง** พิจารณากรุปย่อย $\{\bar{0}, \bar{6}\}$ และ $\{\bar{0}, \bar{4}, \bar{8}\}$ ของกรุป $Z_{12}$ เนื่องจาก $Z_{12}$ เป็นกรุปอาบีเลียนดังนั้น $\{\bar{0}, \bar{6}\} \oplus \{\bar{0}, \bar{4}, \bar{8}\} = \langle \{\bar{0}, \bar{4}, \bar{6}, \bar{8}\} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$ เป็นกรุปย่อยของ $Z_{12}$ ❍

**แบบฝึกหัด 3.4**

1. ให้ m และ n เป็นจำนวนเต็ม จงแสดงว่า $\langle m \rangle$ เป็นกรุปย่อยของ $\langle n \rangle$ ก็ต่อเมื่อ n เป็นตัวประกอบของ m
2. จงหากรุปย่อยของ Z ซึ่งก่อกำเนิดโดย 10 และ 15
3. จงแสดงว่ากรุป Z ก่อกำเนิดโดย 5 และ 7
4. จงแสดงว่ากรุป $Z_{10}$ ก่อกำเนิดโดย $\bar{2}$ และ $\bar{5}$
5. จงแสดงว่ากรุป $Z_{12}$ ก่อกำเนิดโดย $\bar{6}$ และ $\bar{9}$
6. ให้ G เป็นกรุปและสำหรับแต่ละจำนวนเต็มบวก n ให้ $H_n$ แทนเซตของสมาชิกใน G ซึ่งมีอันดับเป็นตัวหารของ n นั่นคือ $H_n = \{a \in G \mid |a| \text{ เป็นตัวหารของ } n\}$ จงแสดงว่า $H_n$ เป็นกรุปย่อยของ G สำหรับแต่ละจำนวนเต็มบวก n
7. จงแสดงว่าถ้า a และ b เป็นสมาชิกของกรุป G ซึ่ง $(|a|, |b|) = 1$ และ $ab = ba$ แล้ว $|ab| = |a||b|$

8. ให้ m และ n เป็นจำนวนเต็ม จงแสดงว่า <m, n> เป็นกรุปย่อยของ Z โดยเฉพาะอย่างยิ่ง <m, n> = <d> ก็ต่อเมื่อ d = (m, n)
9. จงแสดงว่าถ้า G เป็นกรุปจำกัด แล้วจะมีจำนวนเต็มบวก n และ $a_1, a_2, \ldots, a_n$ เป็นสมาชิกใน G ซึ่ง $G = \langle a_1, a_2, \ldots, a_n \rangle$
10. จงแสดงว่า <(1 2), (1 3), (1 4) > = $S_4$ = <(1 2), (1 2 3 4)>
11. จงเขียนตารางการคูณของกรุป G ในแต่ละข้อต่อไปนี้
    11.1 $G = \{e, a, b, b^2, ab, ab^2\}$ โดยที่ตัวก่อกำเนิด a และ b สอดคล้อง $a^2 = e = b^3$ และ $ba = ab^2$
    11.2 $G = \{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ โดยที่ตัวก่อกำเนิด a และ b สอดคล้อง $a^2 = e = b^4$ และ $ba = ab^3$
    11.3 $G = \{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ โดยที่ตัวก่อกำเนิด a และ b สอดคล้อง $a^4 = e, a^2 = b^2$ และ $ba = ab^3$
    11.4 $G = \{e, a, b, c, ab, bc, ac, abc\}$ โดยที่ตัวก่อกำเนิด a, b และ c สอดคล้อง $a^2 = b^2 = c^2 = e$
12. จงแสดงว่ากรุป $Z_{10}$ ก่อกำเนิดโดย $\bar{2}$ และ $\bar{5}$
13. จงแสดงว่า $Z_2 \times Z_3$ และ $Z_3 \times Z_4$ ต่างเป็นกรุปวัฏจักร แต่กรุป $Z_2 \times Z_4$ ไม่เป็นกรุปวัฏจักร
14. ให้ G เป็นกรุปซึ่งมีตัวก่อกำเนิด 2 ตัวคือ a และ b จงแสดงว่าถ้า ab = ba แล้ว G เป็นกรุปอาบีเลียน
15. ให้ G เป็นกรุปและ $a, b \in G$ จงแสดงว่าถ้า $|a| = |b| = |ab| = 2$ แล้ว ab = ba และ {e, a, b, ab} เป็นกรุปย่อยของ G

# บทที่ 4
# กรุปสมมาตรและกรุปการสมมาตร
# SYMMETRIC GROUP AND GROUP OF SYMMETRY

ในการศึกษาเรื่องกรุปซึ่งเป็นระบบคณิตศาสตร์ที่ได้แนะนำเบื้องต้นไปแล้วในบทที่ 3 ถ้าการดำเนินการของกรุปสอดคล้องสมบัติการสลับที่ เราเรียกกรุปนั้นว่ากรุปอาบีเลียนและเราได้เห็นตัวอย่างกรุปเหล่านี้แล้วมากมายในบทที่ 3 โดยเฉพาะอย่างยิ่งกรุปของจำนวนเต็มมอดูโล m เมื่อ m เป็นจำนวนเต็มบวกเป็นตัวอย่างของหมู่กรุปอาบีเลียนที่สำคัญ แต่ถ้าการดำเนินการของกรุปไม่สอดคล้องสมบัติการสลับที่ เราจะเรียกกรุปนั้นว่ากรุปนอนอาบีเลียนและเราก็ได้เห็นตัวอย่างของกรุปเหล่านี้มาบ้างแล้วในบทที่ 3 หมู่ของกรุปนอนอาบีเลียนที่สำคัญได้แก่กรุปของฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงบนเซตๆ หนึ่งที่เราจะเรียกว่ากรุปของวิธีเรียงสับเปลี่ยนซึ่งเราจะศึกษารายละเอียดและแสดงชนิดของกรุปเหล่านี้กันในบทนี้

## 4.1 กรุปสมมาตร

เราเรียกฟังก์ชันชนิดหนึ่งต่อหนึ่งและไปบนจากเซต S ซึ่งไม่ใช่เซตว่างไปยัง S ว่า *วิธีเรียงสับเปลี่ยน (permutation)* บน S โดยใช้สัญลักษณ์ L(S) แทนหมู่หรือเซตของวิธีเรียงสับเปลี่ยนทั้งหมดบน S ในบทที่ 1 และตัวอย่าง 3.1.11 ในบทที่ 3 ได้แสดงให้เห็นว่า "ฟังก์ชันประกอบ" เป็นการดำเนินการบนเซตของฟังก์ชันและ L(S) กับฟังก์ชันประกอบเป็นกรุปซึ่งเราเรียกกรุป $(L(S);\circ)$ ว่า *กรุปสมมาตร (symmetric group)* บน S

ให้ $S = \{1, 2\}$ แล้วจะมีฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึงจากเซต S ไปยัง S ทั้งหมดเพียง 2 ฟังก์ชันคือฟังก์ชันเอกลักษณ์ $\iota_S$ และ $\pi : S \longrightarrow S$ นิยามโดย $\pi(1) = 2$ และ $\pi(2) = 1$ และเราสังเกตว่า $\iota_S \circ \pi = \pi = \pi \circ \iota_S$ ดังนั้น $(\{\iota_S, \pi\};\circ)$ เป็นกรุปสมมาตรบนเซตจำกัดซึ่งเป็นกรุปอาบีเลียน

4.1.1 **ตัวอย่าง** ให้ L เป็นเซตของการแปลงเชิงเส้นเอกฐานทั้งหมดบนระนาบ $R\times R = R^2$ นั่นคือ $f \in L$ ก็ต่อเมื่อ $f : R^2 \longrightarrow R^2$ นิยามโดย

$$f(x, y) = (a_{11}x + a_{12}y, a_{21}x + a_{22}y)$$

เมื่อ $x, y, a_{11}, a_{12}, a_{21}, a_{22} \in R$ และ $a_{11}a_{22} - a_{12}a_{21} \neq 0$

เพราะว่าการแปลงเชิงเส้นเอกฐานบนระนาบเป็นฟังก์ชันหนึ่งต่อหนึ่งและเป็นฟังก์ชันทั่วถึง ฟังก์ชันประกอบของการแปลงเชิงเส้นเอกฐานยังคงเป็นการแปลงเชิงเส้นเอกฐาน ดังนั้น L เป็นกรุปสมมาตรบนเซตอนันต์ $R^2$ ซึ่งเป็นกรุปนอนอาบีเลียน ❍

ถ้า S เป็นเซตซึ่งไม่ใช่เซตว่างและ $\alpha \in L(S)$ เราอาจเขียนแทน $\alpha$ ในรูปแบบดังนี้

$$\alpha = \begin{pmatrix} \cdots & x & \cdots \\ \cdots & \alpha(x) & \cdots \end{pmatrix}$$

โดยที่แถวบนเป็นสมาชิกจากโดเมน S ทั้งหมดและแถวล่างเป็นสมาชิกทั้งหมดของ S ซึ่งเป็นภาพภายใต้ $\alpha$ ของสมาชิกที่ตรงกันกับแถวบน

ถ้า S เป็นเซตจำกัดที่มีสมาชิก n ตัวคือ $x_1, x_2, \ldots, x_n$ จะใช้สัญลักษณ์ $S_n$ แทน L(S) และเรียก $S_n$ ว่า *กรุปสมมาตรบน n สมาชิก (symmetric group on n elements)* และเราเขียนแทน $\alpha \in S_n$ ได้ดังนี้

$$\alpha = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_{i1} & x_{i2} & \cdots & x_{in} \end{pmatrix} \qquad \ldots\ldots\ldots(4.1.1)$$

โดยที่ $x_{ik}$ เป็นภาพของ $x_i$ ภายใต้ $\alpha$ สำหรับทุกๆ $1 \leq i \leq n$

ตัวอย่างเช่นถ้า $S = \{x_1, x_2, x_3, x_4\}$ และ $\alpha \in S_4$ กำหนดโดย $\alpha : x_1 \rightarrow x_2,\ x_2 \rightarrow x_4,\ x_4 \rightarrow x_3$ และ $x_3 \rightarrow x_1$ เราสามารถเขียน $\alpha$ ในรูปแบบ (4.1.1) ได้ดังนี้

$$\alpha = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_4 & x_1 & x_3 \end{pmatrix}$$

แม้ว่าการเขียน $\alpha$ ในรูปแบบ (4.1.1) จะเป็นวิธีที่สั้นและง่ายในการแสดงการส่งสมาชิกของ $\alpha$ ก็ตาม แต่การเขียน $S = \{x_1, x_2, \ldots, x_n\}$ ก็สมมูลกับการแสดงว่า $x_i$ เป็นสมาชิกตัวที่ i ของ S ดังนั้นถ้า S เป็นเซตจำกัดที่มีสมาชิก n ตัว เราจึงนิยมให้ $S = \{1,2,\ldots,n\}$ และเขียน (4.1.1) ในรูปแบบดังนี้

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \qquad \ldots\ldots\ldots(4.1.2)$$

และสำหรับ $\alpha \in S_4$ ของตัวอย่างข้างต้นก็จะเขียนได้เป็น $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ เป็นต้น

ถ้า $\alpha$ เป็นฟังก์ชันเอกลักษณ์บนเซต $S = \{1,2,\ldots,n\}$ นั่นคือ $\alpha(x) = x$ สำหรับทุกๆ $x \in S$ แล้ว จะแทน $\alpha$ ด้วย $\iota_S$ หรือ $\varepsilon$ ซึ่งเขียนในรูปแบบของ (4.1.2) ได้ดังนี้

$$\alpha = \iota_s = \varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

ซึ่งต่อไปเราจะเรียกวิธีเรียงสับเปลี่ยนนี้ว่า *วิธีเรียงสับเปลี่ยนเอกลักษณ์ (identity permutation)*

เพื่อให้สอดคล้องกับสัญลักษณ์ที่ใช้แทนวิธีเรียงสับเปลี่ยน $\alpha \in L(S)$ เมื่อ $S \neq \phi$ ในรูปแบบ (4.1.1) จะเขียน $\alpha(x)$ แทนภาพของ $x \in S$ ภายใต้ $\alpha$ และจะเขียนแทนฟังก์ชันประกอบของ $\alpha, \beta \in L(S)$ ด้วย $\alpha\beta$ ซึ่งต่อไปจะเรียกว่า *ผลคูณ (product)* ของ $\alpha$และ $\beta$ โดยกำหนดให้ $\beta$ เป็นฟังก์ชันที่ส่งสมาชิกก่อนแล้วตามด้วยฟังก์ชัน $\alpha$ ดังนี้

$$(\alpha\beta)(x) = \alpha(\beta(x))$$

เมื่อ x เป็นสมาชิกใดๆ ใน S ซึ่งโดยทฤษฎีบท 1.3.13 จะได้ว่า $\alpha\beta \in L(S)$

ถ้า $S = \{1, 2, \dots, n\}$ และ $\alpha, \beta \in L(S)$ กำหนดโดย

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix} \quad \text{และ} \quad \beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \beta(1) & \beta(2) & \dots & \beta(n) \end{pmatrix}$$

ตามลำดับ แล้วเพราะ $\{1, 2, \dots, n\} = \{\alpha(1), \alpha?(2), \dots, \alpha(n)\} = \{\beta(1), \beta(2), \dots, \beta(n)\}$ ดังนั้น

$$\alpha\beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n \\ \beta(1) & \beta(2) & \dots & \beta(n) \end{pmatrix}$$

$$= \begin{pmatrix} \beta(1) & \beta(2) & \dots & \beta(n) \\ \alpha\beta(1) & \alpha\beta(2) & \dots & \alpha\beta(n) \end{pmatrix}\begin{pmatrix} 1 & 2 & \dots & n \\ \beta(1) & \beta(2) & \dots & \beta(n) \end{pmatrix}$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha\beta(1) & \alpha\beta(2) & \dots & \alpha\beta(n) \end{pmatrix} \qquad \dots\dots\dots(4.1.3)$$

ตัวอย่างเช่น ถ้า $S = \{1, 2, 3\}$ และ $\alpha, \beta \in S_3$ กำหนดโดย $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ และ $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ แล้วโดยรายละเอียดของ (4.1.3) ที่กล่าวไว้ข้างต้น เราสามารถหาผลคูณของ $\alpha$ และ $\beta$ ในรูปแบบของ (4.1.3) ได้ดังแผนภาพข้างล่างนี้

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}$$

โดยเริ่มจากการหาภาพของ 1 ภายใต้ $\alpha\beta$ ให้เริ่มต้นหาภาพของ 1 ภายใต้ $\beta$ ซึ่งเท่ากับ 3 แล้วต่อจากนั้นหาภาพของ 3 ภายใต้ $\alpha$ ซึ่งเท่ากับ 2 จึงได้ว่าภาพของ 1 ภายใต้ $\alpha\beta$ เท่ากับ 2 เป็นต้น ทำให้ได้

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

ถ้า $S = \{1, 2, 3, 4, 5\}$ และ $\alpha, \beta \in S_5$ นิยามโดย $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$ และ

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

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

และ $$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

ถ้า $n \geq 3$ และ $\alpha, \beta \in S_n$ กำหนดโดย

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ 1 & 3 & 2 & 4 & 5 & \cdots \end{pmatrix} \text{ และ } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ 3 & 2 & 1 & 4 & 5 & \cdots \end{pmatrix}$$

แล้ว $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ 2 & 3 & 1 & 4 & 5 & \cdots \end{pmatrix}$ และ $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ 3 & 1 & 2 & 4 & 5 & \cdots \end{pmatrix}$ ดังนั้น

$\alpha\beta \neq \beta\alpha$ จึงกล่าวได้ว่า $S_n$ เป็นกรุปนอนอาบีเลียน สำหรับทุกๆ $n \geq 3$

**หมายเหตุ** สำหรับเซต $S \neq \phi$ เราจะสรุปสมบัติของการคูณบน L(S) ได้ดังต่อไปนี้

1. การคูณเป็นการดำเนินการบน L(S) ซึ่งสอดคล้องสมบัติการเปลี่ยนหมู่
2. การคูณบน L(S) ไม่สอดคล้องสมบัติการสลับที่
3. เนื่องจาก $\iota_s$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ดังนั้น $\iota_s \in L(S)$ และเป็นเอกลักษณ์ของ L(S) ภายใต้การคูณ และถ้า $S = \{1, 2, \ldots, n\}$ แล้ว $\iota_s = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$
4. เนื่องจากสมาชิกของ L(S) เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก S ไปบน S ดังนั้นแต่ละสมาชิกของ L(S) มีตัวผกผัน และถ้า $S = \{1, 2, \ldots, n\}$ และ $\alpha \in S_n$ แล้ว $\alpha^{-1} \in S_n$ โดยที่

$$\alpha^{-1}\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

ทำให้ได้ $$\alpha^{-1} = \begin{pmatrix} \alpha(1) & \alpha(2) & \ldots & \alpha(n) \\ 1 & 2 & \ldots & n \end{pmatrix}$$

ถ้า S = {1} จะมีวิธีเรียงสับเปลี่ยนบน S เพียงตัวเดียวเท่านั้นคือ $\iota_s = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ และถ้า S = {1,2} จะมีวิธีเรียงสับเปลี่ยนบน S ทั้งหมด 2 ตัวคือ $\iota_s = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ และ $\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ และถ้า S = {1, 2, 3} จะมีวิธีเรียงสับเปลี่ยนบน S ทั้งหมด 6 ตัวดังต่อไปนี้

$$\iota_s = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \psi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \phi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\psi^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \psi\phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \phi\psi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

นั่นคือ $|S_1| = 1$, $|S_2| = 2 = 1.2$ และ $|S_3| = 6 = 1.2.3$ ในทฤษฎีบทต่อไป เราจะพิสูจน์ในกรณีทั่วไปว่า $|S_n| = 1.2.3\ldots n$ สำหรับทุกๆ จำนวนเต็มบวก n

**หมายเหตุ** สำหรับแต่ละจำนวนเต็มบวก n เราเรียกจำนวนที่เป็นผลคูณ 1.2.3…n ว่า *แฟกตอเรียล (factorial)* n และเขียนแทนด้วย n! นั่นคือ n! = 1.2.3…n

4.1.2 **ทฤษฎีบท** ถ้า n เป็นจำนวนเต็มบวกและ $S = \{1, 2, \ldots, n\}$ แล้วจะมีวิธีเรียงสับเปลี่ยนบน S ทั้งหมด n! ตัว นั่นคือ $|S_n| = n!$

**บทพิสูจน์** เนื่องจากจำนวนสมาชิกของ $S_n$ เท่ากับจำนวนวิธีทั้งหมดของการนำจำนวนเต็มบวก n ตัว 1, 2, 3,…,n วางลงในที่ว่างต่างๆ กัน n แห่งโดยที่แต่ละจำนวนจะต้องถูกวางลงและสามารถถูกวางลงในที่ว่างเพียงแห่งเดียว เราจึงจะคำนวณหาวิธีทั้งหมดของการวางจำนวนเหล่านี้แทนการหาจำนวนสมาชิกของ $S_n$ โดยตรง

ถ้าเราเริ่มต้นด้วยการวางจำนวนเต็มลงในที่ว่างเรียงกัน n แห่งโดยเริ่มจากทางซ้ายสุดจะเห็นว่ามี n วิธีของการวางจำนวนเต็มเหล่านี้ในที่ว่างแห่งแรกและเมื่อวางจำนวนเต็มตัวใดลงไปแล้วจำนวนนั้นจะไม่ถูกนำไปวางในที่ว่างแห่งอื่นๆ อีกจึงทำให้มีอยู่ n –1 วิธีที่จะวางจำนวนเต็มที่เหลือในที่ว่างแห่งที่สองและด้วยเหตุผลเดียวกัน จะมีอยู่ n–2, n–3 ,…, 2 และ 1 วิธีที่จะวางจำนวนเต็มที่เหลือลงในที่ว่างแห่งที่ สาม สี่ ห้า … n ตามลำดับ

โดยการประยุกต์หลักการนับขั้นพื้นฐานซึ่งกล่าวว่าว่า "*ถ้ามี s วิธีของการกระทำสิ่งหนึ่ง และ r วิธีของการกระทำอีกสิ่งหนึ่ง แล้วจำนวนวิธีของการกระทำสองสิ่งนั้นพร้อมๆ กัน มีอยู่ rs วิธี*" เราจึงประยุกต์อุปนัยเชิงคณิตศาสตร์สรุปได้ว่า จำนวนวิธีทั้งหมดที่จะวางจำนวนเต็มลงในที่ว่างเรียงกัน n แห่งดังกล่าวข้างต้นเท่ากับ n(n-1)…2.1 = n! วิธี ❐

## แบบฝึกหัด 4.1

1. ให้ $S = \{1, 2, 3, 4\}$ และ $\alpha, \beta, \gamma \in S_4$ กำหนดโดย $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ และ $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ จงหาผลคูณ $\alpha\beta, \alpha\gamma, \gamma\beta, \beta\gamma, (\alpha\beta)\gamma, \alpha(\beta\gamma), \alpha^2\gamma^6, \alpha^{-1}, \beta^{-1}, (\alpha\beta)^{-1}, \alpha^{-1}\beta^{-1}$ และ $\beta^{-1}\alpha^{-1}$

2. ให้ $S = \{1, 2, 3, 4, 5\}$ และ $f, g \in S_5$ กำหนดโดย $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ และ $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$ จงหากรุปย่อยของ $S_5$ ซึ่งก่อกำเนิดโดย f และ g

3. ให้ $\alpha$ เป็นวิธีเรียงสับเปลี่ยนบนเซต $S \neq \phi$ จงแสดงว่ามีฟังก์ผกผัน $\alpha^{-1}$ เป็นวิธีเรียงสับเปลี่ยนบน S

4. ให้ $\alpha, \beta$ และ $\gamma$ เป็นวิธีเรียงสับเปลี่ยนบนเซต $S \neq \phi$ จงแสดงว่า

   4.1 $\alpha\beta$ เป็นวิธีเรียงสับเปลี่ยนบน S

   4.2 $(\alpha\beta)\gamma = \alpha(\beta\gamma)$

   4.3 $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$

5. ให้ m และ n เป็นจำนวนเต็มซึ่ง $m \geq 0$ และ $n > 0$ จงแสดงว่าถ้า $\alpha$ เป็นวิธีเรียงสับเปลี่ยนใน $S_n$ แล้ว $\underbrace{\alpha.\alpha...\alpha}_{\text{m ครั้ง}} \in S_n$ และ $(\alpha^m)^{-1} = (\alpha^{-1})^m \in S_n$ เมื่อ $\alpha^0 = \iota_s$

6. จงแสดงว่าถ้า $\alpha \in S_n$ และ $i \in \{1, 2, \ldots, n\}$ ซึ่ง $\alpha(i) = i$ แล้ว $\alpha^m(i) = i$ สำหรับทุกๆ จำนวนเต็ม m

7. ให้ k และ m เป็นจำนวนเต็มและ n เป็นจำนวนเต็มบวกซึ่ง $\alpha \in S_n$ จงแสดงว่า $\alpha^k\alpha^m = \alpha^{k+m}$ และ $(\alpha^k)^m = \alpha^{km}$

8. ให้ S เป็นเซตที่ไม่ใช่เซตว่างและ $\alpha$ เป็นวิธีเรียงสับเปลี่ยนบน S และ $a \in S$ เรากล่าวว่า $\alpha$ *ตรึง (fixed)* a ถ้า $\alpha(a) = a$ และกล่าวว่า $\alpha$ *เคลื่อนย้าย (move)* a ถ้า $\alpha(a) \neq a$ จงพิสูจน์ว่า

   8.1 ถ้า G เป็นเซตของวิธีเรียงสับเปลี่ยนทั้งหมดบนเซต S ที่ไม่ใช่เซตว่างซึ่งตรึงสมาชิกคงตัว $a \in S$ แล้ว G เป็นกรุปย่อยของ L(S)

   8.2 ถ้า S เป็นเซตอนันต์และ G เป็นเซตของวิธีเรียงสับเปลี่ยนทั้งหมดบน S ซึ่งเคลื่อนย้ายสมาชิกของ S เพียงจำนวนจำกัดตัว แล้ว G เป็นกรุปย่อยของ L(S)

   8.3 ถ้า S เป็นเซตจำกัด T เป็นเซตย่อยของ S และ G เป็นเซตของวิธีเรียงสับเปลี่ยน $\alpha$ ทั้งหมดบน S ซึ่ง $\alpha(a) \in T$ แล้ว G เป็นกรุปย่อยของ L(S)

   8.4 จงยกตัวอย่างแสดงว่าข้อ 8.3 ไม่เป็นจริง ถ้า S เป็นเซตอนันต์

## 4.2 การแทนวิธีเรียงสับเปลี่ยนด้วยวัฏจักร

ในหลายๆ สาขาวิชาทางคณิตศาสตร์จำเป็นต้องประยุกต์วิธีเรียงสับเปลี่ยนบนเซตจำกัด เช่น ในทางเรขาคณิต ทางสถิติ หรือทางพีชคณิตมูลฐาน นอกจากนี้วิธีเรียงสับเปลี่ยนบนเซตจำกัด ยังจำเป็นในทางวิทยาศาสตร์และเทคโนโลยี และเราทราบมาจากบทที่แล้วว่าเซตของวิธีเรียงสับเปลี่ยนทั้งหมดบนเซตจำกัดเป็นกรุปภายใต้การดำเนินการ "การคูณ" จึงเกิดการศึกษาสมบัติทางพีชคณิตของกรุปเหล่านี้มาอย่างต่อเนื่อง อย่างไรก็ตามการเขียนวิธีเรียงสับเปลี่ยนให้อยู่ในรูปที่ยิ่งง่ายก็ยิ่งจะเป็นผลดีต่อการศึกษาวิธีเรียงสับเปลี่ยน ในหัวข้อนี้เราจึงจะศึกษาหาวิธีการเขียนวิธีเรียงสับเปลี่ยนในรูปแบบที่ง่ายขึ้นกว่าเดิม

4.2.1 **บทนิยาม** ให้ n เป็นจำนวนเต็มบวก $\alpha \in S_n$ และ $x, y \in S$ เรากล่าวว่า x เป็น $\alpha$ - *สมมูล* *($\alpha$ - equivalent)* กับ y ถ้ามีจำนวนเต็ม k ซึ่ง $\alpha^k(x) = y$ และเขียนแทนความหมายนี้ด้วยสัญลักษณ์

$$x \overset{\alpha}{\sim} y$$

ตัวอย่างเช่นถ้า $S = \{1, 2, 3, 4, 5\}$ และ $\alpha \in S_5$ นิยามโดย $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$

แล้ว $1 \overset{\alpha}{\sim} 3$ เพราะ $\alpha(1) = 3$ และ $1 \overset{\alpha}{\sim} 2$ เพราะ $\alpha^{-1}(1) = 2$ หรือ $\alpha^2(1) = 2$ เป็นต้น

4.2.2 **ทฤษฎีบท** ให้ $S = \{1, 2, \ldots, n\}$ และ $\alpha \in S_n$ แล้ว $\alpha$ - สมมูลเป็นความสัมพันธ์สมมูลบน S

**บทพิสูจน์** 1. ให้ $x \in S$ เนื่องจาก $\alpha^0 = \iota_S \in S_n$ และ $\iota_S(x) = x$ เพราะฉะนั้น $x \overset{\alpha}{\sim} x$

2. ให้ $x, y \in S$ โดยที่ $x \overset{\alpha}{\sim} y$ แล้วจะมีจำนวนเต็ม k ซึ่ง $\alpha^k(x) = y$ และเพราะ $\alpha \in S_n$ โดยที่ $S_n$ เป็นกรุป ทำให้ได้ว่า $\alpha^{-k} \in S_n$ ดังนั้น -k เป็นจำนวนเต็มซึ่ง $\alpha^{-k}(y) = \alpha^{-k}(\alpha^k(x)) = \alpha^0(x) = x$ เพราะฉะนั้น $y \overset{\alpha}{\sim} x$

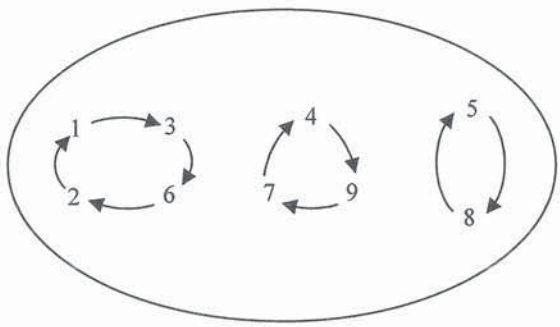
3. ให้ $x, y, z \in S$ ซึ่ง $x \overset{\alpha}{\sim} y$ และ $y \overset{\alpha}{\sim} z$ แล้วจะมีจำนวนเต็ม k และ m ซึ่ง $\alpha^k(x) = y$ และ $\alpha^m(y) = z$ ทำให้ได้ว่า k + m เป็นจำนวนเต็มซึ่ง $\alpha^{m+k}(x) = \alpha^m(\alpha^k(x)) = \alpha^m(y) = z$ เพราะฉะนั้น $x \overset{\alpha}{\sim} z$

จาก (1) , (2) และ (3) สรุปได้ว่า $\alpha$ - สมมูลเป็นความสัมพันธ์สมมูลบน S ❐

โดยสมบัติของความสัมพันธ์สมมูล จะได้ว่ามีผลแบ่งกั้น S ซึ่งกำหนดโดยความสัมพันธ์ $\alpha$ - สมมูลและเราจะเรียกแต่ละเซตสมมูลที่เป็นสมาชิกของผลแบ่งกั้น S ซึ่งกำหนดโดย $\alpha$ - สมมูลนี้ว่า *วงโคจร(orbit)* ของ $\alpha$ และโดยเสมบัติของผลแบ่งกั้น ถ้า A และ B เป็นวงโคจรของ $\alpha$ แล้ว $A \cap B = \phi$ หรือ A = B อย่างใดอย่างหนึ่ง และถ้า $s \in S$ จะมีวงโคจร $A \subseteq S$ ของ $\alpha$ เพียงเซตเดียวซึ่ง $s \in A$ และโดยนิยามของ $\alpha$ - สมมูล สามารถเขียน A ได้ดังนี้

$$A = \{\alpha^k(s) \mid k \in Z\}$$

4.2.3 **ตัวอย่าง** ให้ $\alpha \in S_9$ นิยามโดย $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 6 & 9 & 8 & 2 & 4 & 5 & 7 \end{pmatrix}$ แล้ว $\alpha$ แบ่งกั้น S ออกเป็น 3 วงโคจร ได้แก่ $\{1, 2, 3, 6\}$, $\{4, 7, 9\}$ และ $\{5, 8\}$ ดังแผนภาพ




❍

ถ้า S เป็นเซตจำกัดและ $s \in S$ แล้วโดยหลักการเป็นอันดับอย่างดี จะมีจำนวนเต็มบวก k ตัวน้อยสุดซึ่งขึ้นกับ s และทำให้ $\alpha^k(s) = s$ จึงได้ว่าวงโคจรของ $\alpha$ ที่มี s เป็นสมาชิกจะประกอบด้วย s, $\alpha(s), \alpha^2(s), \ldots, \alpha^{k-1}(s)$ เราจะเรียกวงโคจรของ $\alpha$ ที่เขียนในอันดับ $(s, \alpha(s), \alpha^2(s), \ldots, \alpha^{k-1}(s))$ ว่า *วัฏจักร (cycle)* ของ $\alpha$ และเรียก k ว่า *ความยาว (length)* ของวัฏจักร $(s, \alpha(s), \alpha^2(s), \ldots, \alpha^{k-1}(s))$

4.2.4 **ทฤษฎีบท** ให้ n เป็นจำนวนเต็มบวกและ $\alpha \in S_n$ ถ้า A เป็นวงโคจรของ $\alpha$ ที่ประกอบด้วยสมาชิก r ตัวแล้ว $A = \{x, \alpha(x), \ldots, \alpha^{r-1}(x)\}$ สำหรับทุกๆ $x \in A$

**บทพิสูจน์** ให้ $x \in A$ แล้วโดยบทนิยามของวงโคจรของ $\alpha$ จะได้ว่า

$$\{x, \alpha(x), \ldots, \alpha^{r-1}(x)\} \subseteq A = \{\alpha^k(s) \mid k \in Z\}$$

แต่ A ประกอบด้วยสมาชิกเพียง r ตัว ดังนั้นถ้า $\{x, \alpha(x), \ldots, \alpha^{r-1}(x)\}$ เป็นเซตที่มีสมาชิกต่างกันทั้งหมด แล้ว $A = \{x, \alpha(x), \ldots, \alpha^{r-1}(x)\}$

เราจึงจะแสดงว่าเซต $\{x, \alpha(x), \ldots, \alpha^{r-1}(x)\}$ ประกอบด้วยสมาชิกที่ต่างกันทั้งหมด โดยสมมติว่า $\{x, \alpha(x), \ldots, \alpha^{r-1}(x)\}$ มีจำนวนสมาชิกน้อยกว่า r ตัว นั่นคือมีจำนวนเต็ม i และ j ซึ่ง $0 \leq i < j \leq r-1$ และ $\alpha^i(x) = \alpha^j(x)$ แล้ว $x = \alpha^0(x) = \alpha^{-i}(\alpha^i(x)) = \alpha^{-i}(\alpha^j(x)) = \alpha^{j-i}(x)$ โดยที่ $0 < j - i \leq r-1$ แต่เนื่องจาก A ประกอบด้วยสมาชิก r ตัว ดังนั้นจะมีจำนวนเต็ม k ซึ่ง $\alpha^k(x) \in A$ แต่ $\alpha^k(x) \notin \{x, \alpha(x), \ldots, \alpha^{r-1}(x)\}$

พิจารณาจำนวนเต็ม k และ $j - i > 0$ โดยขั้นตอนการหาร จะมีจำนวนเต็ม q และ s ซึ่ง $k = (j - i)q + s$ โดยที่ $0 \leq s < j - i$ ทำให้ได้ $\alpha^k(x) = \alpha^{(j-i)q+s}(x) = \alpha^s(\alpha^{(j-i)q}(x)) = \alpha^s(x)$ แต่ $0 \leq s < j-i < r-1$ จึงทำให้ $\alpha^k(x) = \alpha^s(x) \in \{x, \alpha(x), \ldots, \alpha^{r-1}(x)\}$ จึงเกิดข้อขัดแย้งกันเอง ดังนั้น $\alpha^i(x) \neq \alpha^j(x)$ สำหรับทุก $0 \leq i \neq j \leq r-1$ จึงเป็นอันจบการพิสูจน์ ❐

4.2.5 **บทแทรก** ให้ $\alpha \in S_n$ ถ้า A เป็นวงโคจรของ $\alpha$ ที่ประกอบด้วยสมาชิก r ตัวและ $x \in A$ แล้ว $A = \{x, \alpha(x), \ldots, \alpha^{r-1}(x)\} = \{\alpha^i(x), \alpha^{i+1}(x), \ldots, \alpha^{i+r-1}(x)\}$ สำหรับทุกๆ จำนวนเต็ม i และยิ่งไปกว่านั้น $\alpha^r(x) = x$

**บทพิสูจน์** เพราะว่า $\alpha^i(x) \in A$ สำหรับทุกๆ จำนวนเต็ม i และโดยทฤษฎีบท 4.2.4 ซึ่งกล่าวว่า x เป็นสมาชิกตัวใดก็ได้ใน A จึงจะแทนที่ x ด้วย $\alpha^i(x)$ ในทฤษฎีบท 4.2.4 ทำให้ได้ว่า

$$A = \{\alpha^i(x), \alpha^{i+1}(x), \ldots, \alpha^{i+r-1}(x)\}$$

ในทำนองเดียวกันสำหรับ $\alpha(x) \in A$ ก็จะได้ $\{\alpha(x), \alpha^2(x), \ldots, \alpha^r(x)\} = A = \{x, \alpha(x), \ldots, \alpha^{r-1}(x)\}$ ทำให้ได้ $\{\alpha(x), \ldots, \alpha^{r-1}(x)\} \cup \{\alpha^r(x)\} = \{x\} \cup \{\alpha(x), \ldots, \alpha^{r-1}(x)\}$ ดังนั้น $\alpha^r(x) = x$ ❐

4.2.6 **ตัวอย่าง** ให้ $S = \{1, 2, 3, 4, 5, 6\}$ และ $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 7 \end{pmatrix}$ ในการหาวงโคจรทั้งหมดของ $\theta$ เราจะประยุกต์ทฤษฎีบท 4.2.4 โดยเริ่มจากวงโคจรของ $\theta$ ที่มี 1 เป็นสมาชิกซึ่งประกอบด้วย $1 = \theta^0(1), \theta^1(1) = 2, \theta^2(1) = \theta(2) = 1$ ซึ่งแสดงว่าวงโคจรของ $\theta$ ที่มี 1 เป็นสมาชิกจะมี 2 เป็นสมาชิกด้วย

ต่อไปพิจารณาวงโคจรของ $\alpha$ ที่มี 3 เป็นสมาชิกซึ่งประกอบ $3 = \theta^0(3)$ เพียงตัวเดียวและวงโคจรของ $\theta$ ที่มี 4 เป็นสมาชิกจะประกอบด้วย $4 = \theta^0(4), \theta^1(4) = 5, \theta^2(4) = \theta(5) = 6$ และ $\theta^3(4) =$

$\theta(6) = 4$ ดังนั้นวงโคจรทั้งหมดของ $\alpha$ ได้แก่ {1, 2}, {3} และ {4, 5, 6} ❍

4.2.7 **บทนิยาม** ให้ $S = \{1, 2, \ldots, n\}$ และ $\alpha \in S_n$ จะกล่าวว่า $\alpha$ เป็น *วัฏจักรที่มีความยาว k (cycle of length k)* หรือ $\alpha$ เป็น *k – วัฏจักร (k-cycle)* ถ้า

1. มีวงโคจร A ของ $\alpha$ ที่ประกอบด้วยสมาชิก k ตัว

และ 2. วงโคจรอื่นๆ ของ $\alpha$ ที่ต่างจาก A มีสมาชิกเพียงตัวเดียว

ตัวอย่างเช่น $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 6 & 2 \end{pmatrix}$ ใน $S_6$ เป็นวัฏจักรที่มีความยาว 3 เพราะว่าวงโคจรทั้งหมดของ $\alpha$ คือ {1}, {2, 5, 6}, {3}, {4} และ $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 2 & 5 \end{pmatrix}$ ใน $S_6$ ก็เป็นวัฏจักรที่มีความยาว 3 เช่นกัน และมีวงโคจรเป็นเซตชุดเดียวกับของ $\alpha$ แม้ว่า $\alpha$ และ $\beta$ จะเป็นวิธีเรียงสับเปลี่ยนที่ต่างกัน และจากตัวอย่างนี้ทำให้สังเกตได้ว่าวงโคจรของวิธีเรียงสับเปลี่ยนจะไม่ใช่ตัวกำหนดของวิธีเรียงสับเปลี่ยนนั้นๆ เราจึงจะศึกษาหาตัวกำหนดที่แน่นอนของวิธีเรียงสับเปลี่ยน

ให้ n เป็นจำนวนเต็มบวกและ $\alpha \in S_n$ ซึ่งเป็น k -วัฏจักร ถ้า k = 1 แล้วทุกวงโคจรของ $\alpha$ มีสมาชิกเพียงตัวเดียว นั่นคือ $\alpha$ เป็นวิธีเรียงสับเปลี่ยนเอกลักษณ์ ในกรณีเช่นนี้ จะเขียนแทน $\alpha$ ด้วยสัญลักษณ์ (1) หรือ (i) เมื่อ $i \in \{1,2,\ldots,n\}$

ถ้า $k \geq 2$ และ A เป็นวงโคจรของ $\alpha$ ซึ่งมีสมาชิก k ตัว แล้วโดยทฤษฎีบท 4.2.4 จะได้ว่า $A = \{x, \alpha(x), \ldots, \alpha^{k-1}(x)\}$ สำหรับทุกๆ $x \in A$ ทำให้ได้ว่า $\alpha: x \rightarrow \alpha(x)$, $\alpha : \alpha(x) \rightarrow \alpha^2(x)$, ... , $\alpha : \alpha^{k-1}(x) \rightarrow \alpha^k(x) = x$ และ $\alpha : y \rightarrow y$ ถ้า $y \notin A$ ดังนั้นวัฏจักร $(x, x\alpha, \ldots, x\alpha^{r-1})$ ของ $\alpha$ จึงเป็นเสมือนตัวแทนของ $\alpha$ จึงนิยมเขียนแทน $\alpha$ ในกรณีนี้ด้วยสัญลักษณ์

$$\alpha = (x \;\; \alpha(x) \ldots \alpha^{k-1}(x))\,(y_1)\,(y_2) \ldots (y_k)$$

โดยที่ $y_i \notin A$ สำหรับ $i = 1, 2, \ldots, k$ หรืออย่างสั้นๆ ดังนี้

$$\alpha = (x \;\; \alpha(x) \;\; \ldots \;\; \alpha^{k-1}(x))$$

ตัวอย่างเช่น $\alpha = (1\,3\,4\,2\,6)$ หมายถึง $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 2 & 5 & 1 & 6 & 7 \end{pmatrix}$ ใน $S_7$

หรือ $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 2 & 5 & 1 & 7 & 8 & 9 \end{pmatrix}$ ใน $S_9$ เป็นวัฏจักรที่มีความยาว 5 ซึ่งอาจเขียนแทน $\alpha$ ด้วยสัญลักษณ์อันใดอันหนึ่งต่อไปนี้

(1 3 2 4 5), (2 4 5 1 3), (5 1 3 2 4), (1 3 2 4 5)(7), (6)(1 3 2 4 5) หรือ (6) (7) (3 2 4 5 1) เป็นต้น

**หมายเหตุ** โดยทฤษฎีบท 4.2.4 ทำให้การเขียนสัญลักษณ์แทนวัฏจักร อาจเริ่มต้นด้วยสมาชิกในวงโคจรตัวใดก็ได้และอาจเขียนหรือละทิ้งวัฏจักรที่มีความยาว 1 ได้

ถ้า $\alpha$ และ $\beta$ เป็น k-วัฏจักรและ r–วัฏจักรใน $S_n$ ตามลำดับแล้วเราสามารถหาผลคูณของ $\alpha$ และ $\beta$ ได้ดังเช่นการหาผลคูณของวิธีเรียงสับเปลี่ยนทั่วไป ตัวอย่างเช่น ถ้า (1 3 2 4) และ (6 5 3) เป็น 4 – วัฏจักร และ 3 – วัฏจักรใน $S_6$ แล้ว

$$(1\ 3\ 2\ 4)(6\ 5\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 1 & 5 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 6 & 4 & 3 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 1 & 2 & 5 \end{pmatrix} \qquad = (1\ 3\ 6\ 5\ 2\ 4)$$

โดยความเป็นจริง เราอาจหาผลคูณของวัฏจักร ได้อย่างง่ายๆ โดยตรง โดยไม่ต้องแทนวัฏจักรในรูปแบบเต็มของวิธีเรียงสับเปลี่ยนดังจะแสดงให้เห็นในตัวอย่างต่อไปนี้

ให้ $\alpha$ = (5 1 3) และ $\beta$ = (6 5 4 1) เป็น 3–วัฏจักรและ 4–วัฏจักรใน $S_6$ เราจะหาผลคูณ $\alpha\beta$ = (5 1 3)(6 5 4 1) โดยตรง เราต้องเริ่มต้นที่ $\beta$ ซึ่งจะพิจารณาให้ $\beta$ ส่งสมาชิกตัวใดใน {1, 2, 3, 4, 5, 6} ก็ได้ แต่ในที่นี้จะขอเริ่มต้นด้วย $\beta$ ส่ง 1

$\beta$ ส่ง 1 ไป 6 และ $\alpha$ ส่ง 6 ไป 6 ดังนั้นผลคูณ $\alpha\beta$ ส่ง 1 ไป 6

$\beta$ ส่ง 2 ไป 2 คงที่และ $\alpha$ ส่ง 2 ไป 2 คงที่เช่นกัน ดังนั้นผลคูณ $\alpha\beta$ ส่ง 2 ไป 2

$\beta$ ส่ง 3 ไป 3 คงที่และ $\alpha$ ส่ง 3 ไป 5 ดังนั้นผลคูณ $\alpha\beta$ ส่ง 3 ไป 5

$\beta$ ส่ง 4 ไป 1 และ $\alpha$ ส่ง 1 ไป 3 ดังนั้นผลคูณ $\alpha\beta$ ส่ง 4 ไป 3

$\beta$ ส่ง 5 ไป 4 และ $\alpha$ ส่ง 4 ไป 4 คงที่ ดังนั้นผลคูณ $\alpha\beta$ ส่ง 5 ไป 4

$\beta$ ส่ง 6 ไป 5 และ $\alpha$ ส่ง 5 ไป 1 ดังนั้นผลคูณ $\alpha\beta$ ส่ง 6 ไป 1

เพราะฉะนั้น $\alpha\beta = (5\ 1\ 3)(6\ 5\ 4\ 1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 5 & 3 & 4 & 1 \end{pmatrix}$

ถ้าเราเรียก k–วัฏจักรใน $S_n$ อย่างสั้นๆ ว่าวัฏจักรใน $S_n$ แล้วตัวอย่างทั้งสองข้างต้นแสดงให้เห็นว่าผลคูณของวัฏจักรไม่จำเป็นต้องเป็นวัฏจักร

4.2.8 **บทนิยาม** ให้ $\alpha,\beta \in S_n$ เป็นวัฏจักรที่มีความยาว $r > 1$ และ $s > 1$ ตามลำดับ จะกล่าวว่า $\alpha$ และ $\beta$ เป็น *วัฏจักรต่างสมาชิก (disjoint cycles)* ถ้า $A \cap B = \phi$ เมื่อ A และ B เป็นวงโคจรที่มีความยาว r ของ $\alpha$ และ B เป็นวงโคจรที่มีความยาว s ของ $\beta$

นั่นคือถ้า $a_1,a_2,\ldots,a_r$, $b_1b_2,\ldots,b_s$ เป็นสมาชิกของ $\{1,2,\ldots,n\}$ ซึ่ง $\alpha = (a_1,a_2,\ldots,a_r)$ และ $\beta = (b_1b_2,\ldots,b_s)$ แล้ว $a_i \neq b_j$ สำหรับทุกๆ $i = 1,2,\ldots,r$ และ $j = 1,2,\ldots,s$

ตัวอย่างเช่น (1 4 5) และ (2 3) เป็นวัฏจักรต่างสมาชิกใน $S_5$ แต่ (1 4 5) และ (2 3 5) ไม่เป็นวัฏจักรต่างสมาชิกใน $S_5$ เพราะมี 5 เป็นสมาชิกร่วมกัน เป็นต้น

4.2.9 **ทฤษฎีบท** ถ้า $\alpha$ และ $\beta$ เป็นวัฏจักรต่างสมาชิกใน $S_n$ แล้ว $\alpha\beta = \beta\alpha$

**บทพิสูจน์** ให้ $\alpha = (a_1\ a_2\ \ldots\ a_r)$ และ $\beta = (b_1\ b_2\ \ldots\ b_s)$ เป็นวัฏจักรต่างสมาชิกใน $S_n$ แล้ว $\{a_1, a_2,\ldots, a_r\} \cap \{b_1, b_2, \ldots, b_s\} = \phi$ และเพื่อจะแสดงว่า $\alpha\beta = \beta\alpha$ เราให้ $x \in S$ แล้ว $x \in \{a_1, a_2,\ldots, a_r\}$ หรือ $x \in \{b_1, b_2, \ldots, b_s\}$ หรือ $x \in S - \{a_1, a_2, \ldots, a_r, b_1, b_2,\ldots,b_s\}$

$x \in \{a_1, a_2,\ldots, a_r\}$ หรือ $x \in \{b_1, b_2, \ldots, b_s\}$ เราสามารถพิสูจน์ได้ในทำนองเดียวกัน จึงจะพิสูจน์เฉพาะกรณี $x \in \{a_1, a_2,\ldots, a_r\}$ ซึ่งจะได้ว่า $x \notin \{b_1, b_2, \ldots, b_s\}$ และ $\alpha(x) \in \{a_1, a_2,\ldots, a_r\}$ ดังนั้น $\beta(x) = x$ และ $\beta(\alpha(x)) = \alpha(x)$ ทำให้ได้ $(\alpha\beta)(x) = \alpha(x) = (\beta\alpha)(x)$

ต่อไปพิจารณากรณี $x \in S - \{a_1, a_2, \ldots, a_r, b_1, b_2,\ldots,b_s\}$ แล้ว $x \notin \{a_1, a_2,\ldots, a_r\}$ และ $x \notin \{b_1, b_2, \ldots, b_s\}$ ดังนั้น $\alpha(x) = x = \beta(x)$ ทำให้ได้ $\alpha\beta(x) = \alpha(x) = x = \beta(x) = \beta\alpha(x)$

ไม่ว่ากรณีใด จะได้ $\alpha\beta(x) = \beta\alpha(x)$ ซึ่งแสดงว่า $\alpha\beta = \beta\alpha$ ❐

พิจารณา $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 6 \end{pmatrix}$ ใน $S_8$ เนื่องจาก $\alpha(1) = 2$, $\alpha(2) = 4$, $\alpha(4) = 1$, $\alpha(3) = 5$, $\alpha(5) = 3$ และ $\alpha(6) = 7$, $\alpha(7) = 8$, $\alpha(8) = 6$ ดังนั้นวงโคจรทั้งหมดของ $\alpha$ ประกอบด้วย {1,2,4}, {3,5} และ {6,7,8} นอกจากนี้เรายังสามารถแยกพิจารณาว่าแต่ละวงโคจรเป็นวงโคจรของวัฏจักรต่างสมาชิก 3 วัฏจักรคือ (1 2 4), (3 5) และ (6 7 8) โดยที่

$$\alpha = (1\ 2\ 4)(3\ 5)(6\ 7\ 8)$$

ซึ่งทำให้สรุปในกรณีนี้ว่า วิธีเรียงสับเปลี่ยน $\alpha$ เป็นผลคูณของวัฏจักรต่างสมาชิก ทฤษฎีบทต่อไปจะแสดงว่าความจริงเช่นนี้ก็จะเกิดขึ้นในกรณีทั่วไปด้วย

4.2.10 **บทนิยาม** ให้ n และ k เป็นจำนวนเต็มบวกและ $\alpha_1, \alpha_2, \ldots, \alpha_k$ ต่างเป็นวัฏจักรที่มีความยาวอย่างน้อย 2 ใน $S_n$ จะเรียก $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ ว่า *ชุดของวัฏจักรต่างสมาชิก (set of disjoint cycles)* ถ้า $\alpha_i$ และ $\alpha_j$ เป็นวัฏจักรต่างสมาชิกสำหรับแต่ละ $1 \leq i \neq j \leq k$

4.2.11 **ทฤษฎีบท** ให้ n เป็นจำนวนเต็มบวกและ $\alpha \in S_n$ แล้วจะมีชุดของวัฏจักรต่างสมาชิกที่มีผลคูณเป็น $\alpha$ และมีเพียงชุดเดียว

**บทพิสูจน์** เห็นได้ชัดว่าทฤษฎีบทเป็นจริงสำหรับ $\alpha$ ที่เป็นวิธีเรียงสับเปลี่ยนเอกลักษณ์หรือเป็นวัฏจักร จึงจะพิจารณากรณีที่ $\alpha$ เป็นวิธีเรียงสับเปลี่ยนซึ่งไม่เป็นวัฏจักรและจะแบ่งการพิสูจน์ออกเป็น 2 ตอน คือ

1. แสดงว่ามี $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ เป็นชุดของวัฏจักรต่างสมาชิกที่มีผลคูณเป็น $\alpha$

และ 2. ถ้ามี $\{\beta_1, \beta_2, \ldots, \beta_m\}$ เป็นอีกชุดหนึ่งของวัฏจักรต่างสมาชิกที่มีผลคูณเป็น $\alpha$ แล้ว

$$\{\beta_1, \beta_2, \ldots, \beta_m\} = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$$

1. เนื่องจาก $\alpha$ ไม่เป็นวัฏจักร ดังนั้น $\alpha \neq (1)$ จึงสมมติให้ $A_1, A_2, \ldots, A_k$ เป็นวงโคจรของ $\alpha$ ที่ต่างมีสมาชิกมากกว่าหนึ่งตัว และสำหรับแต่ละ $i = 1, 2, \ldots, k$ กำหนดให้ $|A_i| = n_i$ แล้วโดยทฤษฎีบท 4.2.3 ถ้า $x_i \in A_i$ แล้ว $x_i, \alpha(x_i), \alpha^2(x_i), \ldots, \alpha^{n_i - 1}(x_i)$ เป็นสมาชิกที่ต่างกันทั้งหมดของ $A_i$ และเพราะ $A_i \cap A_j = \phi$ ถ้า $i \neq j$ เราจะได้

$$\{(x_1\ \alpha(x_1) \ldots \alpha^{n_1 - 1}(x_1)),\ (x_2\ \alpha(x_2) \ldots \alpha^{n_2 - 1}(x_2)), \ldots,\ (x_k\ \alpha(x_k) \ldots \alpha^{n_k - 1}(x_k))\}$$

เป็นชุดของวัฏจักรต่างสมาชิกใน $S_n$ ซึ่ง $\alpha = y_1y_2 \ldots y_k$ โดยที่ $y_i = (x_i\ \alpha(x_i) \ldots \alpha^{n_i-1}(x_i))$ สำหรับ $i = 1, 2, \ldots, k$

2. ให้ $\{\beta_1, \beta_2, \ldots, \beta_m\}$ เป็นชุดของวัฏจักรต่างสมาชิกที่มีผลคูณเป็น $\alpha$ โดยที่แต่ละ $\beta_i$ เป็นวัฏจักรที่มีความยาวอย่างน้อยสอง เนื่องจาก $A_1, A_2, \ldots, A_k$ เป็นวงโคจรของ $\alpha$ ดังนั้นถ้า $x_1 \in A_1$ แล้วจะมี $i \in \{1, 2, \ldots, m\}$ ซึ่ง $\beta_i(x_1) \neq x_1$ และเพราะว่า $\{\beta_1, \beta_2, \ldots, \beta_m\}$ เป็นชุดของวัฏจักรต่างสมาชิก ดังนั้น $\beta_j(x_1) = x_1$ สำหรับทุกๆ $j \neq i$ ซึ่งแสดงว่า $x_1$ อยู่ในวงโคจรที่มีสมาชิกมากกว่าหนึ่งตัวของ $\beta_i$ ดังนั้นวงโคจรนี้ของ $\beta_i$ จะมีสมาชิกทั้งหมดคือ $x_1, \alpha(x_1), \ldots, \alpha^{n_i-1}(x_1)$ ทำให้ได้ $\beta_i = (x_1\ \alpha(x_1) \ldots \alpha^{n_1-1}(x_1)) = y_1$ แล้วโดยทฤษฎีบท 4.2.9 ทำให้เขียนได้ดังนี้

$$\beta_1\beta_2\ldots\beta_{i-1}\beta_{i+1}\ldots\beta_m = \beta_i^{-1}y_1y_2\ldots y_k = y_2\ldots y_k$$

และโดยอุปนัยเชิงคณิตศาสตร์บน k เราสรุปได้ว่าทฤษฎีบทเป็นจริง ❐

4.2.12 **บทแทรก** แต่ละวิธีเรียงสับเปลี่ยนจะเป็นวิธีเรียงสับเปลี่ยนเอกลักษณ์ หรือวัฏจักร หรือเป็นผลคูณของวัฏจักรต่างสมาชิก ❐

**แบบฝึกหัด 4.2**

1. จงเขียนสมาชิกทั้งหมดในกรุป $S_6$ ในรูปผลคูณของวัฏจักรต่างสมาชิก
2. ให้ $\alpha$ และ $\beta$ เป็นวัฏจักรต่างสมาชิกใน $S_n$ ซึ่ง $\alpha\beta = (1)$ จงแสดงว่า $\alpha = \beta = (1)$
3. จงแสดงว่า $\alpha$ และ $\beta$ เป็นวัฏจักรต่างสมาชิกใน $S_n$ ก็ต่อเมื่อ $\alpha(i) \neq i$ เมื่อใดก็ตามที่ $\beta(i) = i$ สำหรับทุกๆ $i \in \{1, 2, \ldots, n\}$ และ $\beta(j) \neq j$ เมื่อใดก็ตามที่ $\alpha(j) = j$ สำหรับทุกๆ $j \in \{1, 2, \ldots, n\}$
4. ให้ $\alpha$ เป็นวัฏจักรที่มีความยาว $r > 1$ จงแสดงว่าถ้า $\alpha(x) \neq x$ แล้ว $\alpha(x) \neq \alpha^{m-1}(x)$ สำหรับทุกๆ จำนวนเต็มบวก m
5. จงหาผลคูณในข้อต่อไปนี้ใน $S_9$

| | |
|---|---|
| 5.1 (1 4 5)(3 7)(6 8 2) | 5.2 (1 2)(3 4 7) |
| 5.3 (1 4 7)(1 6 7 8)(7 4 1 3 2) | 5.4 (7 1 8 2 5)(3 6)(4 9) |
| 5.5 (1 7)(6 2 8)(9 3 5 4) | 5.6 (6 1 4 8)(2 3 4 5)(1 2 4 9 3) |

6. จงเขียนวิธีเรียงสับเปลี่ยนต่อไปนี้ในรูปผลคูณของวัฏจักรต่างสมาชิก

6.1 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & 3 & 6 & 8 & 7 & 5 \end{pmatrix}$ 6.2 (1 2 3 4) (1 2 3) (1 2)

6.3 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 2 & 5 & 1 & 7 & 6 & 8 & 3 \end{pmatrix}$ 6.4 (1 2 3) (4 6 7) (3 4 5)(1 4 6)

7. ให้ $\alpha$ = (3 7 1 4), $\beta$ = (1 2 3) และ $\gamma$ = (2 4 1 3 5) จงหาผลคูณต่อไปนี้และเขียนในรูปผลคูณของวัฏจักรต่างสมาชิก $\alpha^{-1}\beta, \gamma^{-1}\alpha, \alpha^{2}\beta, \beta^{2}\alpha\gamma^{-}, \gamma^{4}, \gamma^{3}\alpha^{-1}, \beta^{-1}\gamma$

8. จงเขียน (1 2 3 4 5) ใน $S_5$ ในรูปวัฏจักรที่แตกต่างกัน 5 แบบ

9. ให้ $\alpha \in S_n$ จงแสดงว่า

   9.1 มีจำนวนเต็มบวก m ตัวน้อยสุดซึ่ง $\alpha^m$ = (1)

   9.2 ถ้า $\alpha$ เป็นวัฏจักรความยาว r แล้ว r จะเป็นจำนวนเต็มบวกน้อยสุดซึ่ง $\alpha^r$ = (1)

   9.3 เราเรียกจำนวนเต็มบวกน้อยสุดในข้อ 7.1 ว่า *อันดับ(order)* ของวิธีเรียงสับเปลี่ยน จงแสดงว่าถ้า $\alpha$ และ $\beta$ เป็นวัฏจักรต่างสมาชิกที่มีอันดับ r และ s ตามลำดับแล้ว อันดับของ $\alpha\beta$ เท่ากับตัวคูณร่วมน้อยของ r และ s

   9.4 จงหาวิธีเรียงสับเปลี่ยนใน $S_n$ ที่มีอันดับเป็นจำนวนเฉพาะ

   9.5 ถ้า $\alpha$ = (1 2 . . . r) เป็นวัฏจักรความยาว r แล้ว $\alpha^{-1}$ เป็นวัฏจักรความยาว r และ $\alpha^{-1}$ = (r r–1 ... 2 1) = $\alpha^{r-1}$

10. ให้ $\alpha$ และ $\beta$ เป็นวิธีเรียงสับเปลี่ยนใน $S_n$ เมื่อ $n \geq 2$ จงพิสูจน์ว่า

   10.1 ถ้า $\alpha = (a_1\ a_2 \ldots a_s)$ แล้ว $\pi\alpha\pi^{-1} = (\pi(a_1)\ \pi(a_2)\ \cdots\ \pi(a_s))$ สำหรับทุกๆ วิธีเรียงสับเปลี่ยน $\pi$ ใน $S_n$

   10.2 ถ้า $\alpha$ และ $\beta$ เป็นวัฏจักรต่างสมาชิก แล้ว $\pi\alpha\pi^{-1}$ และ $\pi\beta\pi^{-1}$ เป็นวัฏจักรต่างสมาชิก สำหรับทุกๆ วิธีเรียงสับเปลี่ยน $\pi$ ใน $S_n$

   10.3 ถ้า $\alpha$ และ $\beta$ เป็นวัฏจักรที่มีอันดับเดียวกัน แล้วจะมีวิธีเรียงสับเปลี่ยน $\pi$ ใน $S_n$ ซึ่ง $\beta = \pi\alpha\pi^{-1}$

## 4.3 การแทนวิธีเรียงสับเปลี่ยนด้วยทรานโพสิชัน

ในหัวข้อ 4.2 ได้กล่าวถึงการแทนทุกๆ วิธีเรียงสับเปลี่ยนในรูปผลคูณของวัฏจักรต่างสมาชิกเพียงชุดเดียวซึ่งทำให้เราเขียนแต่ละวิธีเรียงสับเปลี่ยนในรูปที่ง่ายขึ้น อย่างไรก็ตามเราก็ยังต้องการเขียนหรือแทนวิธีเรียงสับเปลี่ยนในรูปที่ง่ายกว่ารูปผลคูณของวัฏจักรต่างสมาชิก ในหัวข้อนี้เราจึงจะศึกษาสมบัติของวัฏจักรที่มีความยาว 2 ซึ่งเรียกว่า "ทรานโพสิชัน" และแสดงให้เห็นว่าแต่ละวัฏจักร $(a_1\ a_2 \ldots a_m)$ สามารถกระจายได้ในรูปผลคูณของทรานโพสิชัน ดังนี้

$$(a_1\, a_2 \ldots a_m) = (a_m\ a_{m-1})\,(a_m\ a_{m-2}) \ldots (a_m\ a_1)$$

ซึ่งทำให้ได้ว่าทุกๆ วิธีเรียงสับเปลี่ยนเขียนได้ในรูปผลคูณของทรานโพสิชันเช่นกัน แต่เป็นที่น่าเสียดายว่าชุดของทรานโพสิชันในผลคูณดังกล่าวจะไม่เป็นชุดของวัฏจักรต่างสมาชิก และแม้ว่าชุดของทรานโพสิชันที่ให้ผลคูณเป็นแต่ละวิธีเรียงสับเปลี่ยนจะไม่ได้มีเพียงชุดเดียวก็ตาม แต่จำนวนของทรานโพสิชันในแต่ละชุดจะมีภาวะของการเป็นจำนวนคู่หรือจำนวนคี่เหมือนกัน

4.3.1 **บทนิยาม** สำหรับแต่ละจำนวนเต็ม $n \geq 2$ เราเรียก $\alpha \in S_n$ ว่า *ทรานโพสิชัน (transposition)* ถ้า $\alpha$ เป็นวัฏจักรที่มีความยาว 2

ตัวอย่างของทรานโพลิชันได้แก่ (1 2) หรือ (1 2) (3) เป็นต้น

ในการแสดงว่าแต่ละวิธีเรียงสับเปลี่ยนเขียนได้ในรูปผลคูณของทรานโพสิชัน เป็นการเพียงพอที่จะแสดงว่าแต่ละวัฏจักรเขียนได้ในรูปผลคูณของทรานโพสิชัน

4.3.2 **ทฤษฎีบท** ให้ n เป็นจำนวนเต็มซึ่ง $n \geq 2$ และ $\alpha$ เป็นวัฏจักรใน $S_n$ แล้ว $\alpha$ เขียนได้ในรูปผลคูณของทรานโพสิชัน

**บทพิสูจน์** เนื่องจาก (1) = (1 2) (2 1) ดังนั้นทฤษฎีบทเป็นจริงสำหรับวิธีเรียงสับเปลี่ยนเอกลักษณ์ จึงจะพิจารณากรณีที่ $\alpha$ เป็นวัฏจักรใน $S_n$ ที่ไม่ใช่เอกลักษณ์ โดยให้ $\alpha = (a_1\ a_2 \ldots a_r)$ เป็นวัฏจักรที่มีความยาว $r \geq 2$ และให้ $\beta = (a_r\ a_{r-1})(a_r\ a_{r-2}) \ldots (a_r\ a_1)$ แล้วขอให้สังเกตว่า $\alpha(x) = x = \beta(x)$ สำหรับทุกๆ $x \in S - \{a_1, a_2, \ldots, a_r\}$ เราจะแสดงว่า $\alpha$ เป็นวิธีเรียงสับเปลี่ยนเดียวกันกับ $\beta$

ให้ $x \in S$ ถ้า $x \in S - \{a_1, a_2, \ldots, a_r\}$ แล้วโดยข้อสังเกตในย่อหน้าก่อน จะได้ $\alpha(x) = \beta(x)$

เราจึงพิจารณากรณี $x \in \{a_1, a_2, \ldots, a_r\}$ แล้วจะมี $i \in \{1,2,\ldots,r\}$ ซึ่ง $x = a_i$ แล้ว $\alpha(x) = (a_1\, a_2 \ldots a_r)(a_i) = a_{i+1}$ และเพราะ $(a_r\, a_j)(a_k) = a_k$ สำหรับ $k \neq j$, $(a_r\, a_k)(a_k) = a_r$ และ $(a_r\, a_k)(a_r) = a_k$ ดังนั้น

$$\beta(x) = (a_r\, a_{r-1})(a_r\, a_{r-2}) \ldots (a_r\, a_1)(a_i) = (a_r\, a_{r-1})(a_r\, a_{r-2}) \ldots (a_r\, a_i)(a_i)$$
$$= (a_r\, a_{r-1})(a_r\, a_{r-2}) \ldots (a_r\, a_{i+1})(a_r) = a_{i+1} = \alpha(x)$$

จะเห็นว่าไม่ว่ากรณีใด เราได้ $\alpha(x) = \beta(x)$

โดยสมบัติการเท่ากันของฟังก์ชัน ทำให้สรุปได้ว่า $\alpha = \beta$ ดังนั้นทฤษฎีบทเป็นจริง ❐

โดยบทแทรก 4.2.12 และทฤษฎีบท 4.3.1 เราได้บทแทรกต่อไปนี้

4.3.2 **บทแทรก** ทุกๆ วิธีเรียงสับเปลี่ยนเขียนได้ในรูปผลคูณของทรานโพสิชัน ❐

ตัวอย่างเช่น (1 2 3 4 5) = (5 4)(5 3)(5 2)(5 1) เป็นต้น อย่างไรก็ตามเราอาจสังเกตจากการคำนวณได้ว่า

(1 2 3 4 5) = (1 5)(1 4)(5 1)(1 2)(2 1)(5 3)(5 2)(5 1)

หรือ (1 2 3 4 5) = (5 4)(5 2)(5 1)(1 4)(3 2)(4 1)

ซึ่งแสดงว่าการเขียนวิธีเรียงสับเปลี่ยนในรูปผลคูณของทรานโพสิชันทำได้หลายวิธีซึ่งต่างจากการเขียนวิธีเรียงสับเปลี่ยนในรูปผลคูณของวัฏจักรต่างสมาชิก อย่างไรก็ตามจากการสังเกตในกรณีเฉพาะพบว่าจำนวนของทรานโพลิชันที่มีผลคูณเป็นวิธีเรียงสับเปลี่ยนตัวหนึ่งจะเป็นจำนวนคู่หรือจำนวนคี่ อย่างใดอย่างหนึ่งเสมอ ต่อไปเราจึงจะแสดงว่าข้อสังเกตนี้ก็เป็นจริงในกรณีทั่วไป

4.3.3 **บทนิยาม** ให้ n เป็นจำนวนเต็มบวกและ $\alpha \in S_n$ เรากล่าวว่า $\alpha$ เป็น *วิธีเรียงสับเปลี่ยนคู่ (even permutation)* ถ้าชุดของทรานโพสิชันซึ่งมีผลคูณเป็น $\alpha$ ประกอบด้วยสมาชิกเป็นจำนวนคู่ (นั่นคือมีจำนวนเต็มบวก m และ $\alpha_1, \alpha_2, \ldots, \alpha_{2m}$ เป็นทรานโพสิชันซึ่ง $\alpha = \alpha_1\alpha_2 \ldots \alpha_{2m}$ และกล่าวว่า $\alpha$ เป็น *วิธีเรียงสับเปลี่ยนคี่ (odd permutation)* ถ้าชุดของทรานโพสิชันซึ่งมีผลคูณเป็น $\alpha$ ประกอบด้วยสมาชิกเป็นจำนวนคี่

ทฤษฎีบทต่อไปเราจะแสดงว่าชุดของทรานโพสิชันที่มีผลคูณเป็นวิธีเรียงสับเปลี่ยนเอกลักษณ์ประกอบด้วยสมาชิกเป็นจำนวนคู่เสมอ

4.3.4 **ทฤษฎีบท** ไม่ว่าจะเขียนวิธีเรียงสับเปลี่ยนเอกลักษณ์ในรูปผลคูณของทรานโพสิชันด้วยวิธีใด จำนวนของทรานโพสิชันในผลคูณเป็นจำนวนคู่เสมอ

**บทพิสูจน์** ให้ $\varepsilon$ เป็นวิธีเรียงสับเปลี่ยนเอกลักษณ์ จะแสดงก่อนว่าถ้า $t_1, t_2, \ldots, t_m$ เป็นทรานโพสิชันจำนวน m ฟังก์ชันซึ่ง $\varepsilon = t_1 t_2 \ldots t_m$ ..... (ก) แล้ว $\varepsilon$ จะเขียนได้ในรูปผลคูณของทรานโพสิชันจำนวน m – 2 ฟังก์ชัน

ให้ x เป็นสมาชิกของ S ซึ่งปรากฏในทรานโพสิชัน $t_2, \ldots, t_m$ ฟังก์ชันใดฟังก์ชันหนึ่ง และให้ $t_k = (x\ a)$ เป็นทรานโพสิชันตัวสุดท้ายใน (ก) เมื่ออ่านจากซ้ายไปขวาซึ่งมี x ปรากฏอยู่ แล้วใน $t_{k+1}, \ldots, t_m$ จะไม่มี x ปรากฏอยู่ ดังนี้

$$\varepsilon = t_1 \ldots t_{k-1} \underbrace{t_k}_{(xa)} \underbrace{t_{k+1} t_{k+2} \ldots t_m}_{\text{ไม่มี x ปรากฏ}}$$

เมื่อพิจารณา $t_{k-1}$ เราอาจได้ว่า $t_{k-1}$ คือ (x a) เช่นเดียวกับ $t_k$ หรือมีตัวหนึ่งหรือทั้งสองตัวที่ปรากฏใน $t_{k-1}$ ต่างจากของ $t_k$ เราจึงแบ่งกรณีของ $t_{k-1}$ ออกได้เป็น 4 กรณี ดังนี้

**กรณี 1 : $t_{k-1}$ = (x a)** แล้ว $t_{k-1}t_k = (x\ a)(x\ a)$ เป็นฟังก์ชันเอกลักษณ์ เราจึงอาจละไม่เขียน $t_{k-1}t_k$ ในผลคูณ (ก) ซึ่งทำให้ $\varepsilon = t_1 t_2 \ldots t_{k-2} t_{k+1} \ldots t_m$ เขียนได้ในรูปผลคูณของทรานโพสิชันจำนวน m – 2 ฟังก์ชันตามต้องการ

**กรณี 2 : $t_{k-1}$ = (x b)** โดยที่ $b \notin \{x, a\}$ แล้ว $t_{k-1}t_k = (x\ b)(x\ a) = (x\ a\ b) = (x\ a)(a\ b)$ ดังนั้นเมื่อแทน $t_{k-1}t_k$ ใน (ก) ด้วย (x a)(a b) จะทำให้ $\varepsilon$ เขียนได้ในรูปผลคูณของทรานโพสิชันจำนวน m ฟังก์ชันที่มี x ปรากฏอยู่ ณ ตำแหน่งทรานโพสิชันตัวสุดท้ายซึ่งเลื่อนไปทางซ้ายมากขึ้นอีก 1 ตำแหน่ง

**กรณี 3 : $t_{k-1}$ = (c a)** โดยที่ $c \notin \{x, a\}$ แล้ว $t_{k-1}t_k = (c\ a)(x\ a) = (x\ c\ a) = (x\ c)(c\ a)$ และเช่นเดียวกันเมื่อแทน $t_{k-1}t_k$ ใน (ก) ด้วย (x c)(c a) จะทำให้ $\varepsilon$ เขียนได้ในรูปผลคูณของทรานโพสิชันจำนวน m ฟังก์ชันที่มี x ปรากฏอยู่ ณ ตำแหน่งทรานโพสิชันตัวสุดท้ายซึ่งเลื่อนไปทางซ้ายมากขึ้น 1 ตำแหน่ง

**กรณี 4 : $t_{k-1}$ = (b c)** โดยที่ $b,c \notin \{x, a\}$ แล้ว $t_{k-1}t_k = (b\ c)(x\ a) = (x\ a)(b\ c)$ และเช่นเดียวกันเมื่อแทน $t_{k-1}t_k$ ใน (1) ด้วย (x a)(b c) จะทำให้ $\varepsilon$ เขียนได้ในรูปผลคูณของทรานโพสิชันจำนวน m ฟังก์ชันที่มี x ปรากฏอยู่ ณ ตำแหน่งทรานโพสิชันตัวสุดท้ายซึ่งเลื่อนไปทางซ้ายมากขึ้นอีก 1 ตำแหน่ง

ถ้าเกิดกรณี 1 เราจะได้ดังต้องการ แต่ถ้าเกิดกรณี 2 ถึง 4 เราจะดำเนินซ้ำกระบวนการเดิม และแต่ละครั้งจะเกิดกรณี 1 หรือ x ปรากฏอยู่ ณ ตำแหน่งทรานโพสิชันตัวสุดท้ายซึ่งเลื่อนไปทางซ้ายมากขึ้นอีก 1 ตำแหน่ง และเพราะว่า m เป็นจำนวนจำกัด ดังนั้นกระบวนการจะสิ้นสุดที่กรณี 1 หรือ

$t_1 = (x\ a)$ แต่กรณี $t_1 = (x\ a)$ จะเกิดขึ้นไม่ได้ เนื่องจาก x จะไม่ปรากฏในทรานโพสิชัน $t_2, \ldots, t_m$ ซึ่งทำให้ $\varepsilon$ ส่ง x ไป a ดังนั้น $\varepsilon$ ไม่ใช่ฟังก์ชันเอกลักษณ์ จะเกิดข้อขัดแย้งกันเอง

ต่อไปสมมติว่า $\varepsilon$ สามารถเขียนได้ในรูปผลคูณของทรานโพสิชันเป็นจำนวนคี่ฟังก์ชัน แล้วโดยการประยุกต์ผลของการพิสูจน์ในช่วงแรก ทำให้ได้ว่าเราสามารถเขียน $\varepsilon$ ได้ในรูปผลคูณของทรานโพสิชันเป็นจำนวนที่ลดลงทีละสองไปเรื่อยๆ ในที่สุด $\varepsilon = (a\ b)$ เป็นทรานโพสิชันเดี่ยวซึ่งจะไม่ใช่ฟังก์ชันเอกลักษณ์ ทำให้เกิดข้อขัดแย้งกันเอง ดังนั้น $\varepsilon$ ไม่สามารถเขียนได้ในรูปผลคูณของทรานโพสิชันเป็นจำนวนคี่ฟังก์ชันซึ่งเป็นอันจบการพิสูจน์ ❐

4.3.5 **ทฤษฎีบท** ให้ n เป็นจำนวนเต็มบวกและ $\alpha \in S_n$ แล้ว $\alpha$ ไม่สามารถเป็นได้ทั้งวิธีเรียงสับเปลี่ยนคู่และวิธีเรียงสับเปลี่ยนคี่พร้อมๆ กัน

**บทพิสูจน์** สมมติว่ามีวิธีเรียงสับเปลี่ยน $\alpha \in S_n$ ซึ่งเป็นทั้งวิธีเรียงสับเปลี่ยนคู่และวิธีเรียงสับเปลี่ยนคี่ แล้วจะมีจำนวนคู่ r จำนวนคี่ s และ $x_1, x_2, \ldots x_r, y_1, y_2, \ldots, y_s$ เป็นทรานโพสิชันซึ่ง $\alpha = x_1x_2\ldots x_r$ และ $\alpha = y_1y_2\ldots y_s$ แล้วให้ $\alpha^{-1}$ คือตัวผกผันของ $\alpha = y_1y_2\ldots y_s$ ซึ่งก็จะเป็นผลคูณของทรานโพสิชันจำนวน s ฟังก์ชันเช่นกัน (เพราะตัวผกผันของทรานโพสิชันคือทรานโพสิชันนั้นเอง) ทำให้ได้วิธีเรียงสับเปลี่ยน $\varepsilon = \alpha\alpha^{-1}$ เขียนได้ในรูปผลคูณของทรานโพสิชันเป็นจำนวนคี่ฟังก์ชันซึ่งจะขัดแย้งกับทฤษฎีบท 4.3.4 ❐

ขอให้สังเกตว่าผลคูณของวิธีเรียงสับเปลี่ยนคู่เป็นวิธีเรียงสับเปลี่ยนคู่ ผลคูณของวิธีเรียงสับเปลี่ยนคู่กับวิธีเรียงสับเปลี่ยนคี่เป็นวิธีเรียงสับเปลี่ยนคี่ และผลคูณของวิธีเรียงสับเปลี่ยนคี่กับวิธีเรียงสับเปลี่ยนคี่เป็นวิธีเรียงสับเปลี่ยนคู่ ดังนั้นถ้าให้ $A_n$ แทนเซตของวิธีเรียงสับเปลี่ยนคู่ทั้งหมดจาก $S_n$ แล้ว $A_n$ จะมีสมบัติปิดภายใต้การคูณของวิธีเรียงสับเปลี่ยน ทำให้ได้ว่า $A_n$ เป็นกรุปย่อยของ $S_n$ เราเรียกกรุป $A_n$ ว่า *กรุปสลับ (alternating group)*

4.3.6 **ทฤษฎีบท** $|A_n| = \frac{n!}{2}$ สำหรับแต่ละจำนวนเต็ม $n \geq 2$

**บทพิสูจน์** ให้ $B_n$ แทนเซตของวิธีเรียงสับเปลี่ยนคี่ทั้งหมดใน $S_n$ แล้ว $S_n = A_n \cup B_n$ และ $A_n \cap B_n = \phi$ นั่นคือ $\{A_n, B_n\}$ เป็นผลแบ่งกั้น $S_n$ เราจะแสดงว่า $|A_n| = |B_n|$ โดยการสร้างฟังก์ชันสมนัยหนึ่งต่อหนึ่งระหว่าง $A_n$ และ $B_n$

ให้ $\sigma : A_n \rightarrow B_n$ นิยามโดย $\sigma(\alpha) = \alpha(1\ 2)$ สำหรับแต่ละ $\alpha \in A_n$

ให้ $\alpha, \beta \in A_n$ โดยที่ $\sigma(\alpha) = \sigma(\beta)$ แล้ว $\alpha(1\ 2) = \beta(1\ 2)$ แต่ $(1\ 2)(1\ 2) = (1)$ ทำให้ได้ $\alpha = \beta$ เพราะฉะนั้น $\sigma$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ต่อไปให้ $\beta \in B_n$ แล้ว $\beta$ เป็นวิธีเรียงสับเปลี่ยนคี่ ทำให้ได้ $\beta(1\ 2)$ เป็นวิธีเรียงสับเปลี่ยนคู่ และ $\sigma(\beta(1\ 2)) = \beta(1\ 2)(1\ 2) = \beta$ เพราะฉะนั้น $\sigma$ เป็นฟังก์ชันทั่วถึง

เพราะฉะนั้น $|A_n| = |B_n|$ ซึ่งทำให้ได้ $n! = |S_n| = |A_n \cup B_n| = |A_n| + |B_n| = 2|A_n|$

ดังนั้น $|A_n| = \frac{n!}{2}$ ❐

## แบบฝึกหัด 4.3

1. ให้ n เป็นจำนวนเต็มซึ่ง $n \geq 2$ และ $(1\ 2 \ldots k)$ เป็นวัฏจักรความยาว $k > 1$ ใน $S_n$ จงแสดงว่า

   1.1 ถ้า $1 < j < k$ แล้ว $(1\ 2 \ldots k) = (1\ j+1 \ldots k)(1\ 2 \ldots j)$

   1.2 ถ้า $k \geq 2$ แล้ว $(1\ 2 \ldots k) = (1\ k)(1\ 2 \ldots k-1) = (1\ 2)(2\ 3)\ldots(k-1\ k)$

   1.3 $(k-1 \ldots 2\ 1)(1\ 2 \ldots k) = (1)$

2. จงเขียนวิธีเรียงสับเปลี่ยนในข้อต่อไปนี้ในรูปผลคูณของทรานโพสิชัน พร้อมทั้งบอกว่าเป็นวิธีเรียงสับเปลี่ยนคู่หรือคี่

   2.1 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 7 & 5 \end{pmatrix}$

   2.2 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 8 & 7 & 6 & 5 \end{pmatrix}$

   2.3 $(1\ 2\ 3)\ (2\ 4\ 5)\ (1\ 6\ 7)$

   2.4 $(1\ 3\ 7\ 4\ 2\ 8)$

   2.5 $(1\ 4\ 5\ 6\ 3)\ (1\ 4\ 6\ 5\ 3)\ (1\ 4\ 3\ 6\ 5)$

   2.6 $(1\ 2)\ (1\ 2\ 3)(1\ 3\ 5\ 7)$

3. จงเขียนวิธีเรียงสับเปลี่ยนในข้อ 2 ในรูปผลคูณของทรานโพสิชันที่แตกต่างกันมาวิธีเรียงสับเปลี่ยนละ 5 แบบ

4. ให้ $\beta = (1\ 2\ 3\ 4)$ จงแสดงว่าถ้า $\alpha \in S_n$ แล้ว $\alpha\beta\alpha^{-1} = (\alpha(1)\ \alpha(2)\ \alpha(3)\ \alpha(4))$

5. จงแสดงว่า $(1\ 2 \ldots n)$ เป็นวิธีเรียงสับเปลี่ยนคู่ ก็ต่อเมื่อ n เป็นจำนวนคี่

6. จงหาวิธีเรียงสับเปลี่ยนคู่ทั้งหมดใน $S_3$ และใน $S_4$

7. จงพิสูจน์ว่าข้อความในแต่ละข้อต่อไปนี้ เป็นจริง

   7.1 $A_n$ มีสมบัติปิดภายใต้การคูณและ $\iota_S \in A_n$ แต่ $B_n$ ไม่มีสมบัติปิดภายใต้การคูณ

   7.2 ถ้า $\alpha \in A_n$ แล้ว $\alpha^{-1} \in A_n$

   7.3 ถ้า $\alpha \in A_n$ และ $\beta \in S_n$ แล้ว $\beta\alpha\beta^{-1} \in A_n$

   7.4 ถ้า $\alpha, \beta \in S_n$ แล้ว $\beta\alpha\beta^{-1}$และ $\alpha$ เป็นวิธีเรียงสับเปลี่ยนคู่หรือคี่เหมือนๆ กัน

8. ให้ A เป็นเซตของวัฏจักรความยาว 3 ของ $S_4$ ทั้งหมด นั่นคือ

   A = {(1 2 3 ), (1 2 4 ), (1 3 2), (1 3 4 ), (1 4 2), (1 4 3), (2 3 4), (2 4 3)}

   จงแสดงว่า $A_4 = \langle A \rangle$

9. ทำเช่นข้อ 8 สำหรับ $n \geq 3$ [ข้อแนะนำ จงแสดงว่าผลคูณของทรานโพสิชันเป็นผลคูณของวัฏจักรความยาว 3 [ ตัวอย่างเช่น (1 3)(1 2) = (1 2 3), (1 2)(3 4) = (3 2 1)(1 3 4) เป็นต้น ]

10. จงแสดงว่า $\langle(1\ 2\ 3), (1\ 2\ 4), \ldots, (1\ 2\ n)\rangle = A_n$ สำหรับ $n \geq 3$ [ข้อแนะนำ จงแสดงว่า (a b c) = (1 c a)(1 a b), (1 a b) = (1 b 2)((1 2 a)(1 2 b) และ $(1\ b\ 2) = (1\ 2\ b)^2$ ]

11. จงแสดงว่าเซตของวิธีเรียงสับเปลี่ยนทั้งหมดใน $S_n$ ก่อกำเนิด $S_n$

12. จงแสดงว่า $\langle(1\ 2), (1\ 3), \ldots, (1\ n)\rangle = S_n$ สำหรับ $n \geq 3$

## 4.4 กรุปการสมมาตร

ในหัวข้อ 4.1 เราได้แนะนำว่าสัญลักษณ์ L(S) แทนหมู่หรือเซตของวิธีเรียงสับเปลี่ยนทั้งหมดบน S ซึ่งเราทราบแล้วว่า L(S) เป็นกรุปภายใต้การคูณของวิธีเรียงสับเปลี่ยน โดยเราเรียกกรุป (L(S); ∘ ) ว่ากรุปสมมาตรบน S อย่างไรก็ตามเราอาจสังเกตว่าสมาชิกของกรุปในตัวอย่าง 3.1.4 ก็เป็นวิธีเรียงสับเปลี่ยนบนเซตอนันต์ R เช่นกัน แต่จะมีบางวิธีเรียงสับเปลี่ยนบน R ที่ไม่เป็นสมาชิกของกรุปนี้ ดังนั้นกรุปในตัวอย่าง 3.1.4 จึงไม่ใช่กรุปสมมาตร โดยทั่วไปเราเรียกกรุปที่มีสมาชิกเป็นวิธีเรียงสับเปลี่ยนว่า *กรุปของวิธีเรียงสับเปลี่ยน (group of permutations)* ดังนั้นกรุปของวิธีเรียงสับเปลี่ยนจึงอาจไม่เป็นกรุปสมมาตร แต่กรุปสมมาตรทุกๆ กรุปเป็นกรุปของวิธีเรียงสับเปลี่ยน ในหัวข้อนี้เราจะศึกษาตัวอย่างของกรุปของวิธีเรียงสับเปลี่ยนที่สำคัญและมีประโยชน์ในวงวิชาการ ได้แก่กรุปที่บอกความสมมาตรของรูปทรงเรขาคณิตซึ่งเรียกว่า *กรุปการสมมาตร (group of symmetries)*

4.4.1 **บทนิยาม** ให้ G เป็นกรุปของวิธีเรียงสับเปลี่ยนบนเซต S ที่ไม่ใช่เซตว่าง และสำหรับ $T \subseteq S$ เรานิยามเซต $G_T$ และ $G_{(T)}$ ตามลำดับดังนี้

$$G_T = \{\alpha \in G \mid \alpha(t) = t \text{ สำหรับทุกๆ } t \in T\}$$

และ $$G_{(T)} = \{\alpha \in G \mid \alpha(T) = T\} \text{ เมื่อ } \alpha(T) = \{\alpha(t) \mid t \in T\}$$

นั่นคือ $G_T$ เป็น*เซตของวิธีเรียงสับเปลี่ยนยืนยง (preserve) สมาชิก*ใน T และ $G_{(T)}$ คือ*เซตของวิธีเรียงสับเปลี่ยนยืนยงเซต T*

ตัวอย่างเช่นถ้า $S = \{1, 2, 3, 4\}$, $G = S_4$ และ $T = \{1, 2\}$ แล้ว

$$G_T = \{(1), (3\ 4)\} \quad \text{และ} \quad G_{(T)} = \{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

เป็นต้น และเราสังเกตว่า $G_T$ และ $G_{(T)}$ ต่างเป็นกรุปย่อยของ G นอกจากนี้ $G_T \subseteq G_{(T)}$ เราจะพิสูจน์ว่าความจริงนี้ก็เกิดขึ้นในกรณีทั่วไป

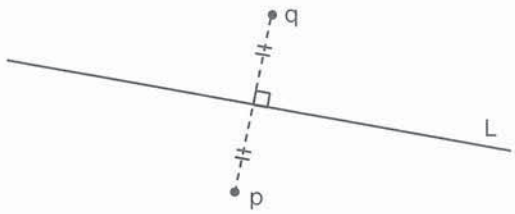
4.4.2 **ทฤษฎีบท** ให้ $G_T$ และ $G_{(T)}$ กำหนดดังบทนิยาม 4.4.1 แล้ว $G_T$ และ $G_{(T)}$ เป็นกรุปย่อยของ G และ $G_T \subseteq G_{(T)}$

**บทพิสูจน์** เราจะแสดงว่า $G_{(T)}$ เป็นกรุปย่อยของ G เท่านั้น สำหรับ $G_T$ เป็นกรุปย่อยของ G พิสูจน์ได้ในทำนองเดียวกัน

เนื่องจาก $\iota_S$ ยืนยงทุกๆ สมาชิกและทุกๆ เซตย่อยของ S ดังนั้น $\iota_S \in G_T$ และ $\iota_S \in G_{(T)}$ ซึ่งแสดงว่า $G_T \neq \phi$ และ $G_{(T)} \neq \phi$ ถ้า $\alpha, \beta \in G_{(T)}$ แล้ว $\alpha(T) = T$ และ $\beta(T) = T$ ซึ่งทำให้ $\alpha\beta(T) = \alpha(\beta(T)) = \alpha(T) = T$ ดังนั้น $\alpha\beta \in G_{(T)}$ และถ้า $\alpha \in G_{(T)}$ แล้ว $\alpha(T) = T$ ซึ่งทำให้ $T = \alpha^{-1}\alpha(T) = \alpha^{-1}(\alpha(T)) = \alpha^{-1}(T)$ ซึ่งแสดงว่า $\alpha^{-1} \in G_{(T)}$ เพราะฉะนั้นถ้า $\alpha, \beta \in G_{(T)}$ แล้ว $\beta^{-1} \in G$ และได้ $\alpha\beta^{-1} \in G_{(T)}$ ทำให้ได้โดยเกณฑ์การตรวจสอบกรุปย่อยว่า $G_{(T)}$ เป็นกรุปย่อยของ G ❐

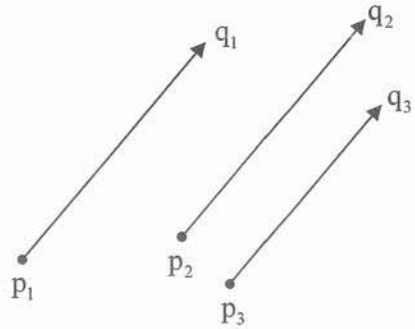
ให้ P แทนเซตของจุดทั้งหมดในระนาบและ M แทนเซตของวิธีเรียงสับเปลี่ยนบน P ซึ่งยืนยงระยะทางระหว่างจุด p และจุด q ใน P นั่นคือถ้า $p, q \in P$ และ $\mu \in M$ แล้ว $d(p, q) = d(\mu(p), \mu(q))$ เมื่อ $d(x, y)$ เป็นสัญลักษณ์แทนระยะทางระหว่างจุด x และจุด y เราเรียกสมาชิกของ M ว่า *โมชัน (motion)* หรือ *สมมิติ (isometry)* ของระนาบ และสมมิติที่พิจารณาเกี่ยวกับความสมมาตรมีอยู่ 3 ชนิด คือ

1. **การหมุน** (rotation) ระนาบรอบจุดคงที่จุดหนึ่ง ดังที่ได้กล่าวไว้ในตัวอย่าง 3.1.7
2. **การสะท้อน** (reflection) ของจุดในระนาบ P ข้ามเส้นตรงคงที่ $L \subseteq P$ เป็นโมชันที่ส่งแต่ละจุด $p \in P$ ไปยังจุด $q \in P$ โดยมี L เป็นเส้นแบ่งครึ่งและตั้งฉากเส้นตรงที่เชื่อมระหว่าง p และ q ดังรูป 4.4.1




**รูป** 4.4.1

3. **การเลื่อนทางขนาน** (translation) เป็นโมชันที่ส่งทุกจุดในระนาบไปด้วยระยะทางเท่าๆ กันและในทิศทางเดียวกัน เช่นในรูป 4.4.2 เป็นการเลื่อนทางขนานที่ส่ง $p_1$ไปยัง $q_1$ ส่ง $p_2$ ไปยัง $q_2$ และส่ง $p_3$ไปยัง $q_3$ เป็นต้น หรือในตัวอย่าง 3.1.4 ก็เป็นตัวอย่างของการเลื่อนทางขนานใน R




**รูป** 4.4.2

4.4.3 **ทฤษฎีบท** M เป็นกรุปย่อยของ L(P)

**บทพิสูจน์** เห็นได้ชัดว่า $\iota_P \in M$ ดังนั้น $M \neq \phi$ ให้ $\alpha, \beta \in M$ และ $p, q \in P$ แล้ว

$d(p, q) = d(\beta(p), \beta(q))$ แต่ $\beta(p), \beta(q) \in P$ และ $\alpha \in M$ จึงได้เช่นกันว่า

$$d(\beta(p), \beta(q)) = d(\alpha(\beta(p)), \alpha(\beta(q))) = d(\alpha\beta(p), \alpha\beta(q))$$

ซึ่งทำให้ได้ $d(p, q) = d(\alpha\beta(p), \beta\alpha(q))$ ซึ่งแสดงว่า $\alpha\beta \in M$

ต่อไปจะแสดงว่า $\alpha^{-1} \in M$ เนื่องจาก $\alpha \in M$ ดังนั้น $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก P ไปบน P ทำให้ได้ว่า $\alpha^{-1}(p)$ และ $\alpha^{-1}(q)$ เป็นจุดใน P ดังนั้น

$$d(\alpha^{-1}(p), \alpha^{-1}(q)) = d(\alpha(\alpha^{-1}(p)), \alpha(\alpha^{-1}(q))) = d(p, q)$$

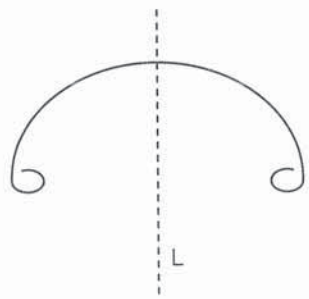
เพราะฉะนั้น $\alpha^{-1} \in M$

ถ้า $\alpha, \beta \in M$ แล้ว $\beta^{-1} \in M$ และทำให้ได้ $\alpha\beta^{-1} \in M$ ซึ่งโดยเกณฑ์การตรวจสอบกรุปย่อย ทำให้สรุปได้ว่า M เป็นกรุปย่อยของ L(P) ❐

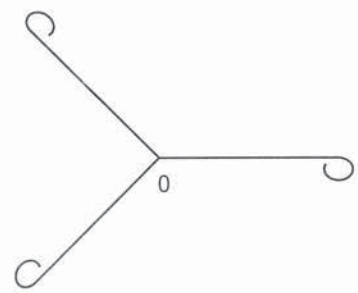
ให้ T แทนเซตของจุดในระนาบ นั่นคือ $T \subseteq P$ แล้ว $M_{(T)}$ จะเป็นกรุปของโมชันซึ่งยืนยงเซต T เราจะเรียกกรุปนี้ว่า *กรุปการสมมาตร (group of symmetries)* บน T

ถ้า T เป็นเซตของจุดบนรูปเรขาคณิตในระนาบ แล้วเราสามารถสร้างกรุปการสมมาตรซึ่งยืนยงรูปเรขาคณิตรูปนั้นๆ ได้ ซึ่งจะแสดงการสร้างพอเป็นตัวอย่างโดยสังเขปดังนี้

### 4.4.4 ตัวอย่าง




รูป 4.4.3




รูป 4.4.4

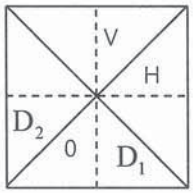
มีโมชันของรูป 4.4.3 อยู่ 2 โมชันคือฟังก์ชันเอกลักษณ์ กับการสะท้อนข้ามเส้นตรง L และในกรณีเช่นนี้ เราเรียกเส้นตรง L ว่า *แกนสมมาตร (axis of symmetry)* ของรูป หรือ *เส้นแบ่งครึ่งรูป (bisector)*

มีโมชันของรูป 4.4.4 อยู่ 3 โมชัน โมชันที่หนึ่งคือฟังก์ชันเอกลักษณ์ โมชันที่สองคือการหมุนระนาบรอบจุด O แบบตามเข็มนาฬิกาไปเป็นมุม 120 องศาและโมชันที่สามคือการหมุนระนาบรอบจุด O แบบตามเข็มนาฬิกาเป็นมุม 240 องศา ซึ่งจะเห็นว่าโมชันที่สองและโมชันสามต่างเป็นโมชันผกผัน

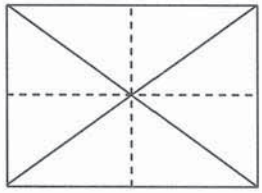
ของกันและกันในกรุปการสมมาตรของรูป 4.4.4 สำหรับกรณีเช่นเดียวกันกับรูป 4.4.3 จะเรียก O ในรูป 4.4.4 ว่า *จุดศูนย์กลาง (center)* ของรูป

**4.4.5 ตัวอย่าง** ในตัวอย่างนี้ เราจะพิจารณาการหาโมชันของรูปสี่เหลี่ยมจัตุรัส สี่เหลี่ยมผืนผ้าและสี่เหลี่ยมขนมเปียกปูน ดังในรูป 4.4.5 รูป 4.4.6 และรูป 4.4.7 ตามลำดับ

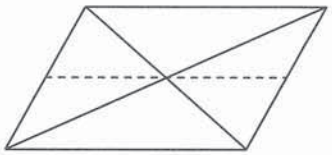
สังเกตว่าแต่ละโมชันของรูปใดรูปหนึ่ง จะเป็นวิธีเรียงสับเปลี่ยนจุดยอดและจุดบนด้านทั้งสี่ของรูปนั้นๆ และในทางกลับกันวิธีเรียงสับเปลี่ยนจุดยอดของรูปใด ก็จะกำหนดโมชันของรูปนั้นด้วย ซึ่งแสดงว่ากรุปการสมมาตรของแต่ละรูปเป็นกรุปย่อยของ L({a, b, c, d}) ดังนั้นกรุปการสมมาตรของแต่ละรูปจะมีอันดับไม่เกิน 4! = 24 แต่สังเกตว่ามีบางวิธีเรียงสับเปลี่ยนใน L({a, b, c, d}) ซึ่งไม่เป็นโมชัน เพราะฉะนั้นแต่ละกรุปย่อยดังกล่าวมีอันดับน้อยกว่า 24




รูป 4.4.5



รูป 4.4.6



รูป 4.4.7

กำหนดให้ H เป็นเส้นแบ่งครึ่งรูปตามแนวนอน V เป็นเส้นแบ่งครึ่งรูปตามแนวดิ่ง $D_1$ และ $D_2$ เป็นเส้นทแยงมุมและ O เป็นจุดศูนย์กลางของรูป แล้วโมชันของแต่ละรูปจะเป็นโมชันใดโมชันหนึ่งต่อไปนี้

e เป็นวิธีเรียงสับเปลี่ยนเอกลักษณ์บนระนาบ P,

$r_1$ เป็นการหมุนระนาบรอบจุด O แบบตามเข็มนาฬิกาเป็นมุม 90 องศา

$r_2$ เป็นการหมุนระนาบรอบจุด O แบบตามเข็มนาฬิกาเป็นมุม 180 องศา

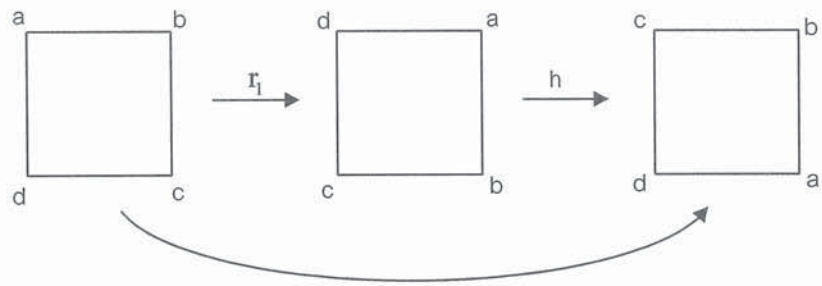
$r_3$ เป็นการหมุนระนาบรอบจุด O แบบตามเข็มนาฬิกาเป็นมุม 270 องศา

h เป็นการสะท้อนข้ามเส้น H

v เป็นการสะท้อนข้ามเส้น V

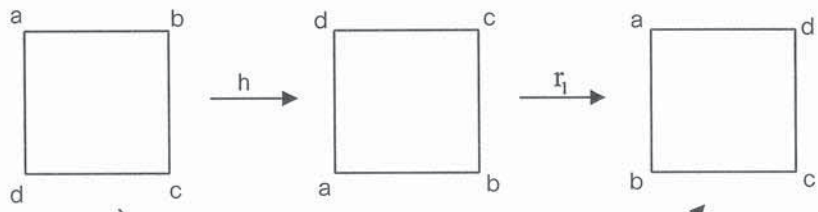
$d_1$ เป็นการสะท้อนข้ามเส้น $D_1$

$d_2$ เป็นการสะท้อนข้ามเส้น $D_2$




$hr_1 = d_1$

รูป 4.4.8




$r_1h = d_2$

รูป 4.4.9

| . | e | $r_1$ | $r_2$ | $r_3$ | h | v | $d_1$ | $d_2$ |
|---|---|---|---|---|---|---|---|---|
| e | e | $r_1$ | $r_2$ | $r_3$ | h | v | $d_1$ | $d_2$ |
| $r_1$ | $r_1$ | $r_2$ | $r_3$ | e | $d_1$ | $d_2$ | v | h |
| $r_2$ | $r_2$ | $r_3$ | e | $r_1$ | v | h | $d_2$ | $d_1$ |
| $r_3$ | $r_3$ | e | $r_1$ | $r_2$ | $d_2$ | $d_1$ | h | v |
| h | h | $d_2$ | v | $d_1$ | e | $r_2$ | $r_3$ | $r_1$ |
| v | v | $d_1$ | h | $d_2$ | $r_2$ | e | $r_1$ | $r_3$ |
| $d_1$ | $d_1$ | h | $d_2$ | v | $r_1$ | $r_3$ | e | $r_2$ |
| $d_2$ | $d_2$ | v | $d_1$ | h | $r_3$ | $r_1$ | $r_2$ | e |

ตาราง 4.4.1

1. โมชันที่ยืนยงรูป 4.4.5 คือทุกๆ โมชันที่กล่าวถึงข้างต้น นั่นคือ e ถึง $d_2$ ดังนั้นกรุปการสมมาตรของรูปสี่เหลี่ยมจัตุรัสคือ $G_S = \{e, r_1, r_2, r_3, h, v, d_1, d_2\}$ ซึ่งสามารถแสดงการคูณของ $r_1$ และ h ได้ $hr_1 = d_1$ และ $r_1h = d_2$ ดังรูป 4.4.8 และรูป 4.4.9 ตามลำดับ และสำหรับการคูณของสมาชิกคู่อื่นๆ ก็พิจารณาได้ในทำนองเดียวกัน ซึ่งได้แสดงผลคูณของทุกๆ คู่สมาชิกไว้ในตาราง 4.4.1 และขอให้สังเกตว่ากรุปการสมมาตรของรูปสี่เหลี่ยมจัตุรัสเป็นกรุปนอนอาบีเลียน
2. โมชันที่ยืนยงรูป 4.4.6 ได้แก่ e, $r_2$, h, v ซึ่งโดยทฤษฎีบท 4.4.2 จะได้ $G_R = \{e, r_2, h, v\}$ เป็นกรุปซึ่งเรียกว่ากรุปการสมมาตรของรูปสี่เหลี่ยมผืนผ้า และเพราะว่า $\{e, r_2, h, v\} = \langle r_2, h\rangle$ โดยที่ $r_2$, h และ v ต่างเป็นสมาชิกที่มีอันดับ 2 ดังนั้น $\langle r_2, h\rangle$ จึงไม่เป็นกรุปวัฏจักร ยิ่งไปกว่านั้น $\langle r_2, h\rangle$ เป็นกรุปที่มีลักษณะโครงสร้างเช่นเดียวกับกรุป $Z_2 \times Z_2$ ซึ่งเราเรียกกรุปที่มีลักษณะโครงสร้างเช่นนี้ว่า *กรุปไคลน์-4 (Klien – 4 group)* จะเห็นว่ากรุปไคลน์-4 เป็นกรุปซึ่งเป็นตัวแทนของกรุปอาบีเลียนอันดับ 4 ที่ไม่เป็นกรุปวัฏจักร และจะกล่าวถึงกรุปนี้อีกในการอ้างเป็นตัวอย่างต่อไปภายหลังและตารางการคูณของกรุป $G_R$ แสดงดังตาราง 4.4.2

| · | e | $r_2$ | h | v |
|---|---|---|---|---|
| e | e | $r_2$ | h | v |
| $r_2$ | $r_2$ | e | v | h |
| h | h | v | e | $r_2$ |
| v | v | h | $r_2$ | e |

**ตาราง 4.4.2**

3. โมชันที่ยืนยงรูป 4.4.7 คือ e และ $r_2$ ดังนั้นกรุปการสมมาตรของรูปสี่เหลี่ยมด้านขนาน $G_P = \{e, r_2\}$ เป็นกรุปวัฏจักรซึ่งมีตารางการคูณของกรุปแสดงดังตาราง 4.4.3

| · | e | $r_2$ |
|---|---|---|
| e | e | $r_2$ |
| $r_2$ | $r_2$ | e |

**ตาราง 4.4.3**

จากการพิจารณากรุปการสมมาตรของสี่เหลี่ยมทั้งสามรูปแบบในตัวอย่าง 4.4.5 ทำให้สังเกตได้ว่า ยิ่งรูปเรขาคณิตมีความสมมาตรมากเท่าใด กรุปการสมมาตรของรูปเรขาคณิตนั้นจะมีอันดับมากขึ้นด้วย เราจึงอาจเปรียบเทียบความสมมาตรของรูปเรขาคณิตด้วยอันดับของกรุปการสมมาตรของรูปเหล่านั้น

สำหรับแต่ละจำนวนเต็ม $n \geq 3$ เราใช้สัญลักษณ์ $D_n$ แทนกรุปการสมมาตรของรูป n เหลี่ยมปรกติ (regular polygon) นั่นคือรูป n เหลี่ยมด้านเท่า มุมเท่า และเราเรียกกรุปการสมมาตรของรูป n เหลี่ยมปรกติว่า *กรุปไดฮิดรัล (dihedral group)* ตัวอย่างเช่น $D_3 = S_3$ คือไดฮิดรัลกรุปของสามเหลี่ยมด้านเท่า $G_S = D_4$ คือไดฮิดรัลกรุปของสี่เหลี่ยมจัตุรัส และ $D_5$ คือไดฮิดรัลกรุปของห้าเหลี่ยมด้านเท่ามุมเท่า และอื่นๆ นอกจากนี้ขอให้สังเกตว่าอันดับของกรุปไดฮิดรัล $D_n$ เท่ากับ 2n สำหรับทุกๆ จำนวนเต็ม $n \geq 3$

**แบบฝึกหัด 4.4**

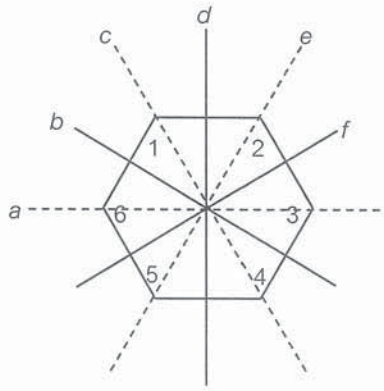
1. ให้ $G = \{\varepsilon, f, g, h\}$ เป็นเซตย่อยของ $S_4$ โดยที่ $\varepsilon = \iota_{S_4}$, $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ และ $h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ จงแสดงว่า Gเป็นกรุปย่อยของ $S_4$พร้อมทั้งแสดงตารางการคูณของ G
2. จงแจกแจงสมาชิกของกรุปย่อยวัฏจักรของ $S_6$ ซึ่งก่อกำเนิดโดย $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$
3. จงหากรุปย่อยอาบีเลียนของ $S_5$ ที่ประกอบด้วยสมาชิก 4 ตัว พร้อมทั้งเขียนตารางการคูณ
4. จงแสดงกรุปย่อย $\langle f, g \rangle$ ของ $S_5$ ซึ่งก่อกำเนิดโดย $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ และ $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$ พร้อมทั้งเขียนตารางการคูณของกรุปย่อย

5. จงเขียนสมาชิกของ $G_T$ และ $G_{<T>}$ เมื่อกำหนด G และ T ในข้อต่อไปนี้

   5.1 $G = S_3$ และ $T = \{1\}$ 5.2 $G = S_3$ และ $T = \{2, 3\}$

   5.3 $G = S_4$ และ $T = \{2, 3\}$ 5.4 $G = S_4$ และ $T = \{1, 2, 3\}$

6. ให้ $G = S_n$ เมื่อ n เป็นจำนวนเต็มบวก จงหาเงื่อนไขของ $T \subseteq \{1, 2, \ldots, n\}$ ที่ทำให้ $G_T = G_{<T>}$
7. จงหากรุปการสมมาตรของสามเหลี่ยมด้านเท่า พร้อมทั้งแสดงว่ากรุปการสมมาตรของสามเหลี่ยมด้านเท่าคือกรุปสมมาตร $S_6$
8. จงเปรียบเทียบกรุปการสมมาตรของสามเหลี่ยมหน้าจั่วและสามเหลี่ยมด้านเท่า
9. ให้ $S = \{a, b, c, d\}$ เป็นเซตของจุดยอดของสี่เหลี่ยมจัตุรัส จงแสดงว่า $\alpha = (a\ b)\ (c)(d) \in L(S)$ ไม่เป็นโมชันในระนาบ
10. ให้ $S = \{a, b, c, d\}$ เป็นเซตของจุดยอดของสี่เหลี่ยม จงหาสมาชิกของ L(S) ซึ่งสอดคล้องกับแต่ละ e, $r_1$, $r_2$, $r_3$, h, v, $d_1$ และ $d_2$ของตัวอย่าง 4.4.5
11. จงเขียนสมาชิกของกรุปย่อยของกรุปการสมมาตรของสี่เหลี่ยมจัตุรัสต่อไปนี้ $< r_1>$, $< r_2>$, $< r_3>$, $< r_1, h >$, $< r_2, v>$, $< v, d_1>$
12. ถ้า $H = \{e, r_2\}$ และ $K = \{e, d_1\}$ เป็นเซตย่อยของกรุปการสมมาตรของสี่เหลี่ยมจัตุรัสในตัวอย่าง 4.4.5 จงหากรุปย่อย $<H \cup K>$
13. จงหากรุปการสมมาตรของรูปหกเหลี่ยมด้านเท่า มุมเท่า พร้อมทั้งเขียนตารางการคูณ




14. จงแสดงการหาสมาชิกทั้งหมดของกรุปไดฮิดรัล $D_n$พร้อมกับสรุปว่าอันดับของกรุปไดฮิดรัล $D_n$ เท่ากับ 2n สำหรับทุกๆ จำนวนเต็ม $n \geq 3$

# บทที่ 5

# ทฤษฎีบทลากรองจ์และกรุปผลหาร

# LAGRANGE'S THEOREM AND QUOTIEN GROUPS

พิจารณากรุปจำกัด G ที่มีอันดับ p เมื่อ p เป็นจำนวนเฉพาะ นั่นคือ G ประกอบด้วยสมาชิกจำนวน p ตัว ดังนั้นจะมี $a \in G$ ซึ่ง $a \neq e$ แต่เพราะ G เป็นกรุปจำกัด ทำให้ได้ว่ามีจำนวนเต็ม $r > s$ ซึ่ง $a^r = a^s$ ดังนั้น $a^{r-s} = e$ เมื่อ $r - s$ เป็นจำนวนเต็มบวก ทำให้ได้โดยหลักการเป็นอันดับอย่างดีว่าจะมีจำนวนเต็มบวกตัวน้อยสุด n ซึ่ง $a^n = e$ ซึ่งเป็นการพิสูจน์ว่า a มีอันดับจำกัด ดังนั้นถ้าเราตั้งสมมติฐานที่กล่าวว่า

*"อันดับของสมาชิกในกรุปจำกัดเป็นตัวหารของอันดับของกรุปนั้น"*

เป็นจริง เราจะได้ว่า $n|p$ แต่ p เป็นจำนวนเฉพาะ และ $n > 1$ เราจึงสรุปได้ว่า $n = p$ เพราะฉะนั้นเซตย่อย $\{a, a^2, a^3, \ldots, a^{p-1}, a^p = e\}$ ของ G เป็นกรุปย่อยวัฏจักรและมีอันดับ p เท่ากันกับอันดับของ G ทำให้ได้ว่า G คือกรุปวัฏจักร $\{a, a^2, a^3, \ldots, a^{p-1}, a^p = e\}$

การวิเคราะห์ข้างต้นนี้เป็นจริงสำหรับทุกๆ กรุปที่มีอันดับเป็นจำนวนเฉพาะ เราจึงสรุปได้ภายใต้สมมติฐานข้างต้นว่า

*" ทุกๆ กรุปที่มีอันดับเป็นจำนวนเฉพาะเป็นกรุปวัฏจักร"* ..... (ก)

สังเกตว่าถ้า G เป็นกรุปซึ่งมี $e \neq a \in G$ เป็นสมาชิกที่มีอันดับ $n > 1$ แล้วเซตย่อย $\{a, a^2, \ldots, a^{n-1}, a^n = e\}$ เป็นกรุปย่อยวัฏจักรอันดับ n ของ G และทุกๆ กรุปย่อยวัฏจักรของ G จะอยู่ในรูปแบบนี้เช่นกัน ดังนั้นถ้าอันดับ n ของสมาชิก a ของกรุปจำกัด G เป็นตัวหารของอันดับของ G แล้วอันดับของกรุปย่อยวัฏจักรของ G ก็จะเป็นตัวหารของอันดับของ G และโดยกลับกัน ซึ่งแสดงว่าสมมติฐานที่เราตั้งไว้ข้างต้นสมมูลกับสมมติฐานเกี่ยวกับอันดับของกรุปย่อยวัฏจักรของ G ทำให้บังเกิดความคิดที่จะตั้งสมมติฐานที่เกี่ยวกับทุกๆ กรุปย่อยของ G ด้วย นั่นคือเราพยายามพิสูจน์ว่า

*"ถ้า H เป็นกรุปย่อยของกรุปจำกัด G แล้วอันดับของ H เป็นตัวหารของอันดับของ G"* ....(ข)

ในบทนี้เราจะศึกษาแนวคิดของท่าน โชแซฟ ลุยส์ ลากรองจ์ (Joseph Louis Lagrange) นักคณิตศาสตร์ชาวฝรั่งเศส ซึ่งท่านได้พิสูจน์ว่าข้อความ (ข) ข้างต้นเป็นจริง นอกจากนี้วิธีการของท่านยังทำให้เกิดกรุปย่อยชนิดพิเศษที่ทำให้สามารถสร้างกรุปใหม่ที่เรียกว่ากรุปผลหารซึ่งเป็นประโยชน์ต่อ

การศึกษาทฤษฎีกรุปเป็นอย่างมาก และจะได้กล่าวถึงกรุปผลหารนี้อีกในเรื่องทฤษฎีบทมูลฐานของสาทิสสัณฐาน นักคณิตศาสตร์ในยุคต่อมาจึงให้ชื่อทฤษฎีบทนี้ในนามของท่านเพื่อเป็นเกียรติและระลึกถึงผู้ริเริ่มแนวความคิดดังกล่าว

## 5.1 ทฤษฎีบทลากรองจ์และผลพลอยได้

แนวคิดของท่านลากรองจ์ในการพิสูจน์ข้อความ (ข) ข้างต้นก็คือพยายามหาผลแบ่งกั้นเซต G ออกเป็นเซตย่อยหลายๆ เซตโดยให้แต่ละคู่ของเซตย่อยเหล่านั้นไม่มีส่วนร่วมกันและแต่ละเซตย่อยประกอบด้วยสมาชิกจำนวนเท่ากันและเท่ากับจำนวนสมาชิกของ H เพื่อให้จำนวนสมาชิกของ G เป็นพหุคูณของจำนวนสมาชิกของ H ซึ่งจะทำให้เราได้ข้อความ (ข) ตามต้องการ และเพราะว่า H ก็เป็นเซตย่อยของ G ที่มีจำนวนสมาชิกตามต้องการแล้ว จึงหาทางที่จะสร้างเซตย่อยอื่นๆ ของ G ที่เป็นเซตต่างสมาชิกกันและเป็นเซตต่างสมาชิกของ H และวิธีหนึ่งซึ่งเป็นแนวคิดแบบธรรมชาติก็คือการคูณเซต H ด้วยสมาชิกต่างๆ ของ G

ให้ a เป็นสมาชิกคงตัวของ G แล้วพิจารณาเซต

$$Ha = \{ ha \mid h \in H \}$$

จะเห็นว่า $h_1a = h_2a$ ก็ต่อเมื่อ $h_1aa^{-1} = h_2aa^{-1}$ และก็ต่อเมื่อ $h_1 = h_2$ สำหรับทุกๆ สมาชิก $h_1$ และ $h_2$ ของ H ซึ่งแสดงว่าจำนวนสมาชิกทั้งหมดของเซต Ha เท่ากับจำนวนสมาชิกทั้งหมดของ H เราจะได้ทฤษฎีบทต่อไปนี้

5.1.1 **ทฤษฎีบท** ให้ G เป็นกรุปและ H เป็นกรุปย่อยของ G และสำหรับแต่ละ $a \in G$ นิยามเซต

$$Ha = \{ ha \mid h \in H \} \quad \text{และ} \quad aH = \{ ah \mid h \in H \}$$

แล้ว $|Ha| = |H| = |aH|$ สำหรับทุกๆ $a \in G$

**บทพิสูจน์** ให้ $a \in G$ และกำหนดฟังก์ชัน $f : H \longrightarrow Ha$ โดย $f(h) = ha$ สำหรับทุกๆ $h \in H$ แล้วโดยการวิเคราะห์ข้างต้น เราจะได้ว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง และเห็นได้ชัดจากนิยามของเซต Ha ว่า f เป็นฟังก์ชันทั่วถึง ดังนั้น $|H| = |Ha|$

สำหรับการพิสูจน์ว่า $|H| = |aH|$ ทำได้ในทำนองเดียวกัน $\square$

เนื่องจาก $a = ea \in Ha$ ทุกๆ $a \in G$ เราจะได้ว่า $\bigcup_{a \in G} Ha = G$ แต่เรายังไม่ทราบว่าเซตย่อยในรูป Ha เหล่านี้เป็นเซตต่างสมาชิกกันหรือไม่ เราจึงต้องการพิสูจน์ความจริงเหล่านี้

5.1.2 **ทฤษฎีบท** ให้ G เป็นกรุปและ H เป็นกรุปย่อยของ G แล้ว $\{Ha \mid a \in G\}$ เป็นผลแบ่งกั้น G

**บทพิสูจน์** เพราะว่า $a = ea \in Ha$ สำหรับทุกๆ $a \in G$ ดังนั้น Ha ไม่เป็นเซตว่างสำหรับแต่ละ $a \in G$

ให้ $a, a' \in G$ โดยที่ $Ha \cap Ha' \neq \phi$ และให้ $x \in Ha \cap Ha'$ แล้วจะมี $h_1, h_2 \in H$ ซึ่ง $x = h_1 a = h_2 a'$ ทำให้ได้ $a = h_1^{-1} h_2 a' \in Ha'$ และถ้า $y = ha$ เป็นสมาชิกของ Ha แล้ว $y = h(h_1^{-1} h_2)a' \in Ha'$ ดังนั้น $Ha \subseteq Ha'$ และในทำนองกลับกัน เราก็สามารถพิสูจน์ได้ว่า $Ha' \subseteq Ha$ เพราะฉะนั้น $Ha = Ha'$

การพิสูจน์ข้างต้นแสดงว่าเซตสองเซตใดๆ ในรูปแบบ Ha เมื่อ $a \in G$ จะเป็นเซตเดียวกันหรือเป็นเซตต่างสมาชิกกันอย่างใดอย่างหนึ่งเสมอ

นอกจากนี้ เราเห็นได้ชัดว่า $\bigcup_{a \in G} Ha = G$ ดังนั้น $\{Ha \mid a \in G\}$ เป็นผลแบ่งกั้น G ❐

ถ้า G เป็นกรุปจำกัด การพิสูจน์ในทฤษฎีบท 5.1.2 แสดงว่ามี $a_1 = e, a_2, \ldots, a_r$ เป็นสมาชิกที่แตกต่างกัน r ตัวของ G ที่ทำให้ $G = \bigcup_{i=1}^{r} Ha_i$ โดยที่ $H_{a_i} \cap H_{a_j} = \phi$ เมื่อ $i \neq j$ และจากผลแบ่งกั้น G ในรูปเซตย่อย Ha เมื่อ $a \in G$ ทั้งหมด r เซต โดยที่แต่ละเซตย่อยมีจำนวนสมาชิกเท่ากันและเท่ากับจำนวนสมาชิกของ H เราจะได้สมการ

$$|G| = r|H|$$

ซึ่งแสดงว่าอันดับของ H เป็นตัวหารของอันดับของ G

ผลของการพิสูจน์ทั้งหมดดังกล่าวข้างต้นรู้จักกันในชื่อว่า ทฤษฎีบทลากรองจ์ (Lagrange's Theorem) เป็นทฤษฎีบทซึ่งเป็นเกณฑ์ตัดสินว่าเซตย่อยใดของกรุปจำกัดจะไม่เป็นกรุปย่อยของกรุปจำกัดนั้นและยังเป็นต้นกำเนิดของทฤษฎีเกี่ยวกับการนับ

5.1.3 **ทฤษฎีบทของลากรองจ์** (Lagrange's Theorem)

ให้ G เป็นกรุปจำกัดและ H เป็นกรุปย่อยของ G แล้ว $|H|$ เป็นตัวหารของ $|G|$

**บทพิสูจน์** ให้ G เป็นกรุปจำกัดและ H เป็นกรุปย่อยของ G แล้วด้วยวิธีการหาผลแบ่งกั้น G ในรูปเซตย่อย Ha เมื่อ $a \in G$ ทั้งหมด r เซตดังกล่าวข้างต้น จะได้ว่าแต่ละเซตย่อยเป็นเซตจำกัดที่ไม่ใช่เซตว่าง เมื่อเลือกสมาชิกหนึ่งตัวจากแต่ละเซตย่อยและให้ชื่อแต่ละสมาชิกที่เลือกมาเป็น $a_1, a_2, \ldots, a_r$ ตามลำดับ แล้วโดยสมบัติของผลแบ่งกั้นจะได้

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_r$$

โดยที่ $H_{a_i} \cap H_{a_j} = \phi$ เมื่อ $i \neq j$ และโดยทฤษฎีบท 5.1.1 จะได้ว่า $|Ha_i| = |H|$ สำหรับทุกๆ $i = 1, 2, \ldots, r$ เพราะฉะนั้น

$$|G| = |Ha_1| + |Ha_2| + \ldots + |Ha_r| = |H| + |H| + \ldots + |H| \text{ (r ครั้ง)}$$
$$= r|H|$$

ซึ่งแสดงว่า $|H|$ เป็นตัวหารของ $|G|$ ❐

โดยทฤษฎีบทลากรองจ์ ถ้า G เป็นกรุปที่มีอันดับ 15 เราจะทราบว่ากรุปย่อยแท้ของ G **อาจ**มีอันดับ 3 หรือ 5 แต่จะไม่มีกรุปย่อยแท้ของ G ที่มีอันดับ 7 เป็นต้น หรือถ้า G เป็นกรุปที่มีอันดับ 7 แล้ว G มีเพียงกรุปย่อยอันดับ 1 และ 7 เท่านั้นซึ่งกรณีตัวอย่างหลังนี้ทำให้ได้ข้อสรุปในกรณีกรุปทั่วไปที่มีอันดับเป็นจำนวนเฉพาะ ดังจะพิสูจน์ให้เห็นจริงในบทแทรกต่อไป

5.1.4 **บทแทรก** ให้ G เป็นกรุปจำกัด แล้ว

1. $|a|$ เป็นตัวหารของ $|G|$ สำหรับทุกๆ $a \in G$ ยิ่งไปกว่านั้น $a^{|G|} = e$
2. ถ้า $|G|$ เป็นจำนวนเฉพาะแล้ว G เป็นกลุ่มวัฏจักร ยิ่งไปกว่านั้นทุกๆ สมาชิกของ G ที่ไม่ใช่เอกลักษณ์จะเป็นตัวก่อกำเนิด G
3. ถ้า $|G|$ เป็นจำนวนเฉพาะแล้ว $H = G$ หรือ $H = \{e\}$ สำหรับทุกๆ กรุปย่อย H ของ G

**บทพิสูจน์** ให้ G เป็นกรุปจำกัด

1. ให้ $a \in G$ แล้ว $<a>$ เป็นกรุปย่อยวัฏจักรของ G ที่มีอันดับเท่ากับ $|a|$ ดังนั้นโดยทฤษฎีบทลากรองจ์จะได้ $|<a>| = |a|$ เป็นตัวหารของ $|G|$ นั่นคือมีจำนวนเต็มบวก m ซึ่ง $|G| = m|a|$ ทำให้ได้ $a^{|G|} = a^{m|a|} = (a^{|a|})^m = e^m = e$

2. ให้ $|G|$ เป็นจำนวนเฉพาะ p แล้ว $|G| = p > 1$ ดังนั้นถ้า $e \neq a \in G$ แล้ว $<a>$ เป็นกรุปย่อยวัฏจักรของ G โดยที่ $|<a>| = |a|$ เป็นตัวหารของ $|G|$ ทำให้ได้ว่า $|a| = 1$ หรือ $|a| = |G| = p$ แต่ $a \neq e$ ดังนั้น $|<a>| = |a| = |G| = p$ โดยที่ $<a> \subseteq G$ เพราะฉะนั้น $G = <a>$ เป็นกรุปวัฏจักร

3. พิสูจน์ได้ในทำนองเดียวกับข้อ 2 ❐

**หมายเหตุ** ผลของทฤษฎีบทลากรองจ์ ทำให้เราสรุปเกี่ยวกับชนิดของกรุปอันดับ 1, 2, 3, 4 และ 5 ได้ดังนี้

1. โดยทฤษฎีบทลากรองจ์ ข้อ 3 จะได้ว่ากรุปอันดับ 1, 2, 3 และ 5 เป็นกรุปวัฏจักร
2. ถ้า G เป็นกรุปอันดับ 4 และมีสมาชิกตัวหนึ่งใน G ซึ่งมีอันดับ 4 แล้ว G เป็นกรุปวัฏจักร แต่ถ้าไม่มีสมาชิกตัวใดเลยใน G ที่มีอันดับ 4 แล้วโดยทฤษฎีบทลากรองจ์ ข้อ 2 จะได้ว่าทุกๆ สมาชิกของ G ซึ่งไม่ใช่เอกลักษณ์มีอันดับ 2 ดังนั้น $G = \{e, a, b, c\}$ โดยที่ $a^2 = b^2 = c^2 = e$ เพราะฉะนั้น $c = ab$ และ $c^2 = (ab)^2 = e$ ซึ่งทำให้ได้ $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ นั่นคือ

$$G = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle = K_4$$

5.1.5 **บทแทรก** ถ้า G เป็นกรุปนอนอาบีเลียน แล้ว $|G| \geq 6$ ❐

นอกจากนี้เรายังสามารถประยุกต์ทฤษฎีบทลากรองจ์ในการหากรุปย่อยทั้งหมดของ $S_3$ ซึ่งเป็นกรุปอันดับ 6 ได้ดังตัวอย่างต่อไปนี้

5.1.6 **ตัวอย่าง** ในตัวอย่างนี้ เราจะพิจารณาหากรุปย่อยทั้งหมดของกรุปสมมาตร $S_3$ บนเซตที่มี 3 สมาชิกซึ่งเขียนในรูปแจกแจงสมาชิกทั้งหมดได้เป็นดังนี้

$$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

และเราทราบแล้วว่า $S_3$ มีอันดับ $|S_3| = 6 = 2\times3$ แล้วโดยทฤษฎีบทลากรองจ์ข้อ 1 กรุปย่อยของ $S_3$ ต้องเป็นกรุปที่มีอันดับ 1, 2, 3 หรือ 6 เท่านั้น

กรุปย่อยอันดับ 1 และอันดับ 6 ต้องเป็น $\{(1)\}$ และ $S_3$ ตามลำดับ แต่โดยทฤษฎีบทลากรองจ์ ข้อ 3 กรุปย่อยอันดับ 2 และอันดับ 3 ทั้งหมดต้องเป็นกรุปย่อยวัฏจักรซึ่งก่อกำเนิดโดยสมาชิกที่มีอันดับ 2 และอันดับ 3 ตามลำดับ ดังนั้นกรุปย่อยเหล่านี้คือ

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

สังเกตว่า (1 2 3) และ (1 3 2) ต่างก่อกำเนิดกรุปย่อยเดียวกัน เนื่องจาก

$$\langle(1\ 2\ 3)\rangle = \{(1), (1\ 2\ 3), (1\ 3\ 2)\} = \langle(1\ 3\ 2)\rangle$$ ❍

คำถามสำคัญที่เกิดขึ้นขณะนี้ก็คือ "บทกลับของทฤษฎีบทลากรองจ์เป็นจริงด้วยหรือไม่" นั่นคือ "สำหรับแต่ละจำนวนเต็มบวก m ซึ่งเป็นตัวหารของกรุป G จะมีกรุปย่อย H ของ G ซึ่งมีอันดับ m หรือไม่" และในการพิจารณาหากรุปย่อยทั้งหมดของกรุปสลับ $A_4$ ซึ่งมีอันดับ $\frac{4!}{2} = 12$ ปรากฏว่า $A_4$

ไม่มีกรุปย่อยอันดับ 6 ซึ่งแสดงว่าบทกลับของทฤษฎีบทลากรองจ์ไม่เป็นจริง อย่างไรก็ตามทฤษฎีบทต่อไปนี้แสดงให้เห็นว่าบทกลับของทฤษฎีบทลากรองจ์เป็นจริงในกรณีของกรุปวัฏจักร

5.1.7 **ทฤษฎีบท** ถ้า G เป็นกรุปวัฏจักรอันดับจำกัดและ n เป็นจำนวนเต็มบวกซึ่งเป็นตัวหารของ $|G|$ แล้วจะมีกรุปย่อย H ของ G ซึ่ง $|H| = n$

**บทพิสูจน์** ให้ G เป็นกรุปวัฏจักรอันดับจำกัดและ n เป็นจำนวนเต็มบวกซึ่งเป็นตัวหารของ $|G|$ แล้วจะมี $a \in G$ และจำนวนเต็ม m ซึ่ง $a^{|G|} = e$ และ $|G| = mn$ ดังนั้น $(a^m)^n = e$ และเราสามารถพิสูจน์ได้ไม่ยากว่า $\left|a^m\right| = n$ ซึ่งทำให้ได้ว่า $H = \langle a^m \rangle$ เป็นกรุปย่อยของ G ที่มีอันดับ n ❐

## แบบฝึกหัด 5.1

1. จงแสดงว่า $Z_{12}$ มีกรุปย่อยอันดับ k สำหรับทุกๆ จำนวนเต็มบวก k ที่เป็นตัวหารของ 12
2. จงแสดงว่าถ้า p เป็นจำนวนเฉพาะ แล้วทุกๆ สมาชิกของ $Z_p \times Z_p$ ซึ่งไม่ใช่เอกลักษณ์มีอันดับ p
3. จงพิสูจน์ว่าถ้า G เป็นกรุปซึ่ง $|G| = n$ แล้ว $a^n = e$ สำหรับทุกๆ $a \in G$
4. จงพิสูจน์ว่าถ้า G เป็นกรุปซึ่ง $|G| = pq$ เมื่อ p และ q เป็นจำนวนเฉพาะแล้ว G เป็นกรุปวัฏจักร หรือทุกๆ สมาชิกที่ไม่ใช่เอกลักษณ์ของ G มีอันดับ p หรือ q
5. จงพิสูจน์ว่าถ้า G เป็นกรุปซึ่ง $|G| = 4$ แล้ว G เป็นกรุปวัฏจักร หรือทุกๆ สมาชิกของ G เป็นตัวผกผันของตัวเอง (ทำให้ได้ว่าทุกๆ กรุปอันดับ 4 เป็นกรุปอาบีเลียน)
6. จงพิสูจน์ว่าถ้า H และ K เป็นกรุปย่อยของกรุปจำกัด G แล้วอันดับของ $H \cap K$ เป็นตัวหารร่วมของอันดับ H และ K
7. ให้ H และ K เป็นกรุปย่อยที่ต่างกันของกรุปจำกัด G จงพิสูจน์ว่าถ้า $|H| = |K| = p$ เมื่อ p เป็นจำนวนเฉพาะแล้ว $H \cap K = \{e\}$
8. จงพิสูจน์ว่าถ้าในกรุปจำกัด G มีสมาชิกที่มีอันดับ m และอันดับ n แล้วอันดับของ G จะเป็นพหุคูณของตัวคูณร่วมน้อยของ m และ n
9. ให้ p เป็นจำนวนเฉพาะ จงพิสูจน์ว่าถ้า G เป็นกรุปจำกัด แล้วจำนวนสมาชิกของ G ที่มีอันดับ p จะเป็นพหุคูณของ $p-1$

## 5.2 โคเซตซ้ายและโคเซตขวา

การพิสูจน์ทฤษฎีบทลากรองจ์ได้มีการกำหนดเซตย่อยของกรุปจำกัด G ด้วยกรุปย่อย H ในรูปแบบ Ha สำหรับแต่ละ $a \in G$ และแสดงว่าเซตของเซตย่อยเหล่านั้นเป็นผลแบ่งกั้น G และโดยสมมาตรเราอาจกำหนดเซตย่อยของกรุปจำกัด G ด้วยกรุปย่อย H ในรูปแบบ aH สำหรับแต่ละ $a \in G$ และแสดงว่าผลที่ได้จะเป็นไปในทำนองเดียวกัน ในหัวข้อนี้ เราจึงจะศึกษาความสัมพันธ์ของผลแบ่งกั้นทั้งสองรูปแบบนี้

5.2.1 **บทนิยาม** ให้ H เป็นกรุปย่อยของกรุป G และ $a \in G$ เราเรียกเซต $Ha = \{ha \mid h \in H\}$ ว่า *โคเซตขวา (right coset)* ของ H ใน G และสำหรับเซต $aH = \{ah \mid h \in H\}$ ก็จะเรียกในทำนองเดียวกันว่า *โคเซตซ้าย (left coset)* ของ H ใน G โดยเรียก a ว่า *ตัวแทน (representative)* ของโคเซตขวาหรือโคเซตซ้ายซึ่ง a เป็นสมาชิก

สำหรับกรุปที่มีการดำเนินการคือ "การบวก + " จะแทนโคเซตขวาและโคเซตซ้ายที่มี a เป็นตัวแทนตามลำดับ ดังนี้

$$H+a = \{h+a \mid h \in H\} \quad \text{และ} \quad a+H = \{a+h \mid h \in H\}$$

**ข้อสังเกต** ขอให้สังเกตว่าโคเซตขวาหรือโคเซตซ้ายของกรุปย่อย H ใน G ที่ไม่ใช่ H จะเป็นเพียงเซตย่อยที่ไม่ใช่กรุปย่อยของ G เพราะเซตย่อยเหล่านั้นจะไม่มี e เป็นสมาชิก นอกจากนี้ในหัวข้อ 5.1 เราพิสูจน์แล้วว่า

$$|aH| = |H| = |Ha|$$

สำหรับทุกๆ $a \in G$ ยิ่งไปกว่านั้น เราได้ว่า

$$He = \{he \mid h \in H\} = \{h \mid h \in H\} = H = \{eh \mid h \in H\} = eH$$

**หมายเหตุ** ทฤษฎีบทและตัวอย่างทั้งหลายที่เกี่ยวกับโคเซตขวาจะเป็นจริงสำหรับโคเซตซ้ายด้วย โดยการพิสูจน์ในทำนองคู่กัน จึงจะแสดงการพิสูจน์สำหรับโคเซตขวาเท่านั้น

ตัวอย่างเช่น สำหรับกรุปย่อย <7> ของกรุป Z จะได้โคเซตขวาของ <7> ที่มี 3 เป็นสมาชิกคือ $3 + \langle 7 \rangle = 3 + \{\ldots, -14, -7, 0, 7, 14, \ldots\} = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$ เป็นต้น

ในการหาโคเซตขวาทั้งหมดของกรุปย่อย H ของกรุปจำกัด G เราอาจดำเนินการโดยอาศัยสมบัติการเป็นผลแบ่งกั้น G ได้ดังจะบรรยายในย่อหน้าต่อไปนี้

เนื่องจาก H = He เป็นกรุปย่อยของ G ซึ่งเป็นโคเซตขวาเซตหนึ่ง ดังนั้นโคเซตขวาของ G เซตอื่นๆ จะไม่มีสมาชิกร่วมกันกับ H ดังนั้นการหาโคเซตขวาเซตต่อไปทำได้โดยการเลือกสมาชิก a ตัวหนึ่งที่ไม่อยู่ใน H [แต่ถ้าไม่มีสมาชิกให้เลือก แสดงว่า G = H ในกรณีเช่นนี้จะมีโคเซตขวาของ H ใน G เพียงเซตเดียวคือ G ] และนำ a คูณทางขวากับทุกๆ สมาชิกของ H ก็จะได้โคเซตขวา Ha ต่อไปถ้ายังมีสมาชิกของ G เหลืออยู่ให้เลือก $b \in G$ ที่ไม่อยู่ใน $H \cup Ha$ แล้วสร้างโคเซตขวา Hb และดำเนินการเช่นนี้เรื่อยไปจนกระทั่งไม่มีสมาชิกของ G เหลืออยู่อีก

### 5.2.2 ตัวอย่าง

1. ในกรุปสมมาตร $S_3 = \{ (1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \}$ เราจะได้โคเซตขวาของ $H = \{(1), (1\ 2)\}$ ทั้งหมดใน $S_3$ ดังต่อไปนี้

$$H(1) = H = \{(1), (1\ 2)\},$$
$$H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\},$$
$$H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 3)\}$$

2. ในกรุปการสมมาตร $G_S$ ของสี่เหลี่ยมจัตุรัสในตัวอย่าง 4.4.5 เราจะได้โคเซตขวาของ $H = \{e, v\}$ ทั้งหมดใน $G_S$ ดังต่อไปนี้

$$He = H = \{ e^2, ev \} = \{ e, v \},$$
$$Hr_1 = \{ er_1, vr_1 \} = \{ r_1, d_1 \},$$
$$Hr_2 = \{ er_2, vr_2 \} = \{ r_2, h \},$$
$$Hr_3 = \{ er_3, vr_3 \} = \{ r_3, d_2 \}$$

3. ในกรุปวัฏจักร $Z_{12}$ ของความสัมพันธ์คอนกรูเอนซ์มอดูโล 12 เราจะได้โคเซตขวาของ $H = <\overline{4}>$ ทั้งหมดใน $Z_{12}$ ดังต่อไปนี้

$$<\overline{4}> = \{\overline{0}, \overline{4}, \overline{8}\},$$
$$<\overline{4}> \oplus \overline{1} = \{\overline{1}, \overline{5}, \overline{9}\},$$
$$<\overline{4}> \oplus \overline{2} = \{\overline{2}, \overline{6}, \overline{10}\},$$
$$<\overline{4}> \oplus \overline{3} = \{\overline{3}, \overline{7}, \overline{11}\}$$

ดังที่เราแสดงการพิสูจน์ไปแล้วว่าเซตของโคเซตขวาทั้งหมดของกรุปย่อย H ของกรุป G เป็นผลแบ่งกั้น G ดังนั้นจะมีความสัมพันธ์สมมูล $\sim$ ซึ่งกำหนดโดยผลแบ่งกั้นนี้ และในการหานิยามของ

ความสัมพันธ์ $\sim$ ดังกล่าวเราพิจารณาว่าถ้า $a, b \in G$ ซึ่ง $a \sim b$ แล้ว a และ b จะต้องเป็นสมาชิกในโคเซตขวาเซตเดียวกัน แต่โคเซตขวาที่มี a และ b เป็นสมาชิกคือ Ha และ Hb ตามลำดับ ดังนั้น

$$a \sim b \iff Ha = Hb$$

และเพราะว่า $b \in Hb = Ha$ ดังนั้นจะมี $h \in H$ ซึ่ง $b = ha$ ทำให้ได้ $ba^{-1} = h \in H$ เพราะฉะนั้น

$$a \sim b \iff ba^{-1} \in H$$

ในทำนองคู่กัน ความสัมพันธ์สมมูล $\sim$ ซึ่งกำหนดโดยผลแบ่งกั้นซึ่งคือเซตของโคเซตซ้ายทั้งหมดของกรุปย่อย H ของกรุป G นิยามโดย

$$a \sim b \iff aH = bH \iff a^{-1}b \in H$$

5.2.3 **ทฤษฎีบท** ให้ H เป็นกรุปย่อยของกรุป G และ $a, b \in G$ แล้ว

1. $Ha = Hb$ ก็ต่อเมื่อ $ba^{-1} \in H$
2. $aH = bH$ ก็ต่อเมื่อ $a^{-1}b \in H$
3. ยิ่งไปกว่านั้น $aH = H = Ha$ ก็ต่อเมื่อ $a \in H$ ❐

5.2.4 **ตัวอย่าง** ในกรุปวัฏจักร Z ซึ่งมีทุกๆ กรุปย่อยเป็นกรุปวัฏจักรในรูปแบบ $\langle n \rangle$ เมื่อ n เป็นจำนวนเต็ม เราสามารถนิยามความสัมพันธ์สมมูล $\sim$ ใน Z ซึ่งกำหนดโดย $\langle n \rangle$ สำหรับแต่ละจำนวนเต็มบวก n ได้ดังนี้

$$a \sim b \iff a - b \in \langle n \rangle$$

ซึ่งโดยความหมายนี้ก็คือ $a - b$ เป็นพหุคูณของ n หรือ n หาร $a - b$ ลงตัว นั่นคือ

$$a \sim b \iff a \equiv b \pmod{n}$$

เพาะฉะนั้นเซตของโคเซตขวาทั้งหมด (ซึ่งก็คือเซตของโคเซตซ้ายทั้งหมด) ของ $\langle n \rangle$ ใน Z ก็คือ $Z_n$ ❍

ขอให้สังเกตว่า ในกรณีเฉพาะคือกรุป Z ผลแบ่งกั้นที่กำหนดโดยเซตของโคเซตซึ่งกำหนดโดยกรุปย่อย $\langle n \rangle$ คือเซตของเรซิดิวมอดูโล n บางครั้งเราจึงเรียกความสัมพันธ์สมมูล $\sim$ ซึ่งกำหนดโดยเซตของโคเซตขวา (ซ้าย) ทั้งหมดของกรุปย่อย H ในกรุป G ว่า*ความสัมพันธ์คอนกรูเอนซ์มอดูโล* H

เราจะจบหัวข้อนี้ด้วยการแสดงว่าจำนวนโคเซตขวาทั้งหมดของกรุปย่อย H ในกรุป G เท่ากับจำนวนโคเซตขวาทั้งหมดของกรุปย่อย H ในกรุป G

5.2.5 **ทฤษฎีบท** ให้ H เป็นกรุปย่อยของกรุป G แล้วจำนวนโคเซตขวาทั้งหมดของ H ใน G เท่ากับจำนวนโคเซตขวาทั้งหมดของ H ใน G

**บทพิสูจน์** ให้ A และ B แทนเซตของโคเซตซ้ายทั้งหมดและโคเซตขวาทั้งหมดของ H ใน G ตามลำดับ แล้วจะแสดงว่า $|A| = |B|$ โดยการกำหนด $f : A \longrightarrow B$ โดย $f(aH) = Ha^{-1}$ สำหรับทุกๆ $a \in G$

เนื่องจาก $f(aH) = f(bH) \Leftrightarrow Ha^{-1} = Hb^{-1} \Leftrightarrow a^{-1}(b^{-1})^{-1} \in H \Leftrightarrow a^{-1}b \in H \Leftrightarrow aH = bH$ ดังนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่ง และโดยนิยามของโคเซตขวา Ha และโคเซตซ้าย Ha จะได้ว่า f เป็นฟังก์ชันทั่วถึง ซึ่งเป็นอันจบการพิสูจน์ ❐

โดยทฤษฎีบท 5.2.5 ทำให้กล่าวได้ถึงจำนวนโคเซตขวาทั้งหมดของ H ใน G ซึ่งเป็นจำนวนเดียวกับจำนวนโคเซตซ้ายทั้งหมดของ H ใน G เราจึงเรียกจำนวนนี้ว่า *ดรรชนี (index)* ของ H ใน G และเขียนแทนด้วยสัญลักษณ์ [G : H] และขอให้สังเกตว่าถ้า H = {e} แล้ว |G| = [G : {e}]

โดยบทพิสูจน์ทฤษฎีลากรองจ์ เราจะได้ว่า

$|G| = |H|\,[G : H]$

ซึ่งทำให้ได้ว่าทั้ง |H| และ [G : H] เป็นตัวหารของ |G|

## แบบฝึกหัด 5.2

1. จงหาโคเซตขวาและโคเซตซ้ายทั้งหมดของกรุปย่อย H ในกรุป G ที่กำหนดในแต่ละข้อต่อไปนี้

   1.1 $G = Z_{24}$ และ $H = \{\bar{0}, \bar{6}, \overline{12}, \overline{18}\}$

   1.2 $G = G_S$ และ $H = \{e, d_1\}$

   1.3 $G = S_4$ และ $H = \{ (1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \}$

   1.4 $G = Z$ และ $H = \langle 3 \rangle$

   1.5 $G = S_4$ และ $H = A_4$

   1.6 $G = R$ และ $H = Z$

   1.7 $G = R$ และ $H = \langle \frac{1}{2} \rangle$

   1.8 $G = R \times R$ และ $H = \{(x, y) \mid x = y\}$

   1.9 $G = Z_{24}$ และ $H = \langle 5 \rangle$

   1.10 $G = R^{*}$ และ $H = \{2^n \mid n \in Z\}$

2. ให้ H เป็นกรุปย่อยของกรุป G และ $a, b, c \in G$ จงพิสูจน์ข้อความในข้อต่อไปนี้

2.1 ถ้า $aH = Ha$ และ $bH = Hb$ แล้ว $(ab)H = H(ab)$

2.2 ถ้า $aH = Ha$ แล้ว $a^{-1}H = Ha^{-1}$

2.3 ถ้า $(ab)H = (ac)H$ แล้ว $bH = cH$

3. ให้ H เป็นกรุปย่อยของกรุป G จงพิสูจน์ข้อความในข้อต่อไปนี้

3.1 ถ้า $[G : H] = 2$ แล้ว $ab \in H$ สำหรับทุกๆ $a,b \notin H$

3.2 ถ้า $[G : H] = 2$ แล้วทุกๆ โคเซตซ้ายของ H ใน G จะเป็นโคเซตขวาของ H ใน G

4. จงหากรุปย่อย H ของ $R^*$ ซึ่ง $[R^* : H] = 2$

5. จงหาดรรชนีของ $<m>$ ใน Z สำหรับทุกๆ จำนวนเต็มบวก m

6. ให้ K และ H เป็นกรุปย่อยของกรุป G จงพิสูจน์ข้อความในข้อต่อไปนี้

6.1 ถ้า K เป็นกรุปย่อยของ H แล้ว $[G : K] = [G : H][H : K]$

6.2 ถ้า $H \cap K \neq \phi$ และ $|K|$ เป็นจำนวนเฉพาะ แล้ว K เป็นกรุปย่อยของ H

## 5.3 กรุปย่อยปรกติ

ในการพิสูจน์ความจริงว่า "อันดับของกรุปย่อยเป็นตัวหารของอันดับของกรุปจำกัด" เราได้สร้างเซตย่อยลักษณะเฉพาะขึ้นโดยนิยามชื่อเซตย่อยเหล่านั้นไว้ในหัวข้อ 5.2 ว่าโคเซตขวาและโคเซตซ้าย ดังนั้นเมื่อกำหนดกรุปย่อย H ของกรุป G เราก็จะได้เซตของโคเซตขวาทั้งหมด $\{Ha \mid a \in G\}$ และเซตของโคเซตซ้ายทั้งหมด $\{aH \mid a \in G\}$ ซึ่งเซตของโคเซตทั้งสองแบบต่างเป็นผลแบ่งกั้น G และแต่ละโคเซตจะมีจำนวนสมาชิกในแต่ละโคเซตเท่ากันคือเท่ากับอันดับของกรุปย่อย H นอกจากนี้เรายังได้แสดงการพิสูจน์ว่าจำนวนของโคเซตขวาทั้งหมดเท่ากับจำนวนของโคเซตซ้ายทั้งหมดซึ่งเท่ากับ $\frac{|G|}{|H|}$ โดยเรียกจำนวนนี้ว่าดรรชนีของ H ใน G แต่ยังคงมีคำถามที่น่าสนใจหาคำตอบว่า "ผลแบ่งกั้น G ที่เป็นเซตของโคเซตขวาทั้งหมดของ H ใน G และที่เป็นเซตของโคเซตซ้ายทั้งหมดของ H ใน G จะเป็นผลแบ่งกั้นเดียวกันหรือไม่" ถ้าคำตอบคือ "ไม่ใช่" แล้วภายใต้เงื่อนไขใดจึงจะทำให้เซตทั้งสองเป็นเซตเดียวกัน

เพื่อหาคำตอบของคำถามข้างต้น เราจะลองมาพิจารณาหาโคเซตขวาทั้งหมดและโคเซตซ้ายทั้งหมดของกรุปย่อย $H = \{(1), (1\ 2)\}$ ในกรุปสมมาตร $S_3$

โคเซตซ้ายทั้งหมดของ H ใน $S_3$ ที่ต่างกันทั้งหมดมีเพียง 3 โคเซต ได้แก่

$(1)\{(1), (1\ 2)\} = \{ (1), (1\ 2) \},$

$(1\ 3)\{(1), (1\ 2)\} = \{ (1\ 3), (1\ 2\ 3) \},$

$(2\ 3)\{(1), (1\ 2)\} = \{ (2\ 3), (1\ 3\ 2) \},$

ในทำนองเดียวกัน โคเซตขวาทั้งหมดของ H ใน $S_3$ ที่ต่างกันทั้งหมดก็จะมีเพียง 3 โคเซต ได้แก่

$\{(1), (1\ 2)\}(1) = \{ (1), (1\ 2) \},$

$\{(1), (1\ 2)\}(1\ 3) = \{ (1\ 3), (1\ 3\ 2) \},$

$\{(1), (1\ 2)\}(2\ 3) = \{ (2\ 3), (1\ 2\ 3)\}$

แต่เมื่อพิจารณาหาโคเซตขวาทั้งหมดและโคเซตซ้ายทั้งหมดของกรุปย่อย H = {(1), (1 2 3), (1 3 2) } ในกรุปสมมาตร $S_3$ เรากลับพบว่าโคเซตซ้ายทั้งหมดของ H ใน $S_3$ ที่ต่างกันทั้งหมดมีเพียง 2 โคเซต ได้แก่

$(1)\{ (1), (1\ 2\ 3), (1\ 3\ 2) \} = \{ (1), (1\ 2\ 3), (1\ 3\ 2) \},$

และ $(1\ 3)\{ (1), (1\ 2\ 3), (1\ 3\ 2) \} = \{ (1\ 2), (1\ 3), (2\ 3) \}$

ในทำนองเดียวกัน โคเซตขวาทั้งหมดของ H ใน $S_3$ ที่ต่างกันทั้งหมดก็จะมีเพียง 2 โคเซต ได้แก่

$\{ (1), (1\ 2\ 3), (1\ 3\ 2) \}(1) = \{ (1), (1\ 2\ 3), (1\ 3\ 2) \},$

และ $\{ (1), (1\ 2\ 3), (1\ 3\ 2) \}(1\ 3) = \{ (1\ 2), (1\ 3), (2\ 3) \}$

เพราะฉะนั้นโคเซตซ้ายของ H ใน $S_3$ อาจ "ใช่" หรือ "ไม่ใช่" โคเซตขวาของ H ใน $S_3$ ดังนั้นคำตอบของคำถามข้างต้นก็คือ "ไม่ใช่" เราจึงจะพิจารณาหาเงื่อนไขของกรุปหรือกรุปย่อยที่จะทำให้ได้ว่าเซตของโคเซตทั้งสองเป็นเซตเดียวกัน

ให้ H เป็นกรุปย่อยของกรุป G ถ้า $a \in G$ เราสามารถเขียน a = ae เมื่อ e เป็นเอกลักษณ์ของ G แล้วโคเซตซ้ายที่มี a เป็นสมาชิกคือ aH และทำนองเดียวกันโคเซตขวาที่มี a เป็นสมาชิกคือ Ha ทำให้ได้ว่าแต่ละโคเซตซ้ายของ H ใน G เป็นโคเซตขวาของ H ใน G ก็ต่อเมื่อ aH = Ha สำหรับทุกๆ $a \in G$ เราจึงกำหนดเรียกกรุปย่อย H ของกรุป G ที่มีลักษณะเช่นนี้ว่ากรุปย่อยปรกติ

5.3.1 **บทนิยาม** ให้ N เป็นกรุปย่อยของกรุป G จะเรียก N ว่า *กรุปย่อยปรกติ (normal subgroup)* ถ้าทุกๆ โคเซตซ้ายของ N ใน G เป็นโคเซตขวาของ N ใน G และโดยกลับกัน

ถ้า N เป็นกรุปย่อยปรกติของกรุป G และ aN เป็นโคเซตซ้ายของ N ใน G แล้วตามความหมายของบทนิยาม 5.3.1 จะได้ว่า aN เป็นโคเซตขวาของ N ใน G ด้วย นั่นคือมี $b \in G$ ซึ่ง $aN = Nb$ แต่ $a \in aN = Nb$ ทำให้มี $n \in N$ ซึ่ง $a = nb$ ซึ่งทำให้ได้ $ab^{-1} = n \in N$ แล้วโดยทฤษฎีบท 5.2.3 จะได้ $Na = Nb = aN$ เราจึงอาจกล่าวบทนิยาม 5.3.1 อีกแบบหนึ่งดังนี้

N เป็น *กรุปย่อยปรกติ* ของกรุป G ก็ต่อเมื่อ $Na = aN$ สำหรับทุกๆ $a \in G$

ถ้า G เป็นกรุป แล้ว {e} และ G จะเป็นกรุปย่อยปรกติของ G และถ้า G เป็นกรุปอาบีเลียนแล้วทุกๆ กรุปย่อยของ G เป็นกรุปย่อยปรกติ ดังนั้นทุกๆ กรุปย่อยของกรุปวัฏจักรเป็นกรุปย่อยปรกติ

**หมายเหตุ** ขอให้สังเกตว่า $Na = aN$ ในบทนิยามของกรุปย่อยปรกติ หมายความว่าสำหรับแต่ละ $n \in N$ จะมี $n' \in N$ ซึ่ง $an = n'a$ ไม่ใช่หมายความว่า $an = na$

ทฤษฎีบทต่อไปแสดงข้อความสมมูลกับการเป็นกรุปย่อยปรกติซึ่งสามารถนำไปประยุกต์เป็นเกณฑ์การตัดสินได้ว่ากรุปย่อยใดของกรุปเป็นกรุปย่อยปรกติ

5.3.2 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยของกรุป G แล้วข้อความต่อไปนี้สมมูลกัน

1. H เป็นกรุปย่อยปรกติของ G
2. $aH = Ha$ สำหรับทุกๆ $a \in G$
3. $a^{-1}Ha = H$ สำหรับทุกๆ $a \in G$
4. $a^{-1}Ha \subseteq H$ สำหรับทุกๆ $a \in G$
5. $a^{-1}ha \in H$ สำหรับทุกๆ $a \in G$ และทุกๆ $h \in H$

**บทพิสูจน์** (1) $\Rightarrow$ (2) โดยการวิเคราะห์ท้ายบทนิยามของกรุปย่อยปรกติ

(2) $\Rightarrow$ (3) ให้ $a \in G$ ถ้า $aH = Ha$ แล้ว $H = a^{-1}aH = a^{-1}Ha$

(3) $\Rightarrow$ (4) ให้ $a \in G$ ถ้า $a^{-1}Ha = H$ แล้ว $a^{-1}Ha \subseteq H$

(4) $\Rightarrow$ (5) ให้ $a \in G$ ถ้า $a^{-1}Ha \subseteq H$ แล้ว $a^{-1}ha \in a^{-1}Ha \subseteq H$ สำหรับทุกๆ $h \in H$

(5) $\Rightarrow$ (1) ถ้า $a^{-1}ha \in H$ สำหรับทุกๆ $a \in G$ และทุกๆ $h \in H$ แล้ว $a^{-1}Ha \subseteq H$ และ $(a^{-1})^{-1}Ha^{-1} \subseteq H$ (เพราะว่า $a^{-1}$ ก็เป็นสมาชิกของ G) ทำให้ได้ $aHa^{-1} \subseteq H$ และดังนั้น $H = a^{-1}aHa^{-1}a \subseteq a^{-1}Ha$

จาก $a^{-1}Ha \subseteq H$ และ $H \subseteq a^{-1}Ha$ เราจะได้ $a^{-1}Ha = H$ ซึ่งทำให้ได้ $aH = Ha$ ❐

5.3.3 **ทฤษฎีบท** 1. ถ้า G เป็นกรุปจำกัดและ H เป็นกรุปย่อยของ G ซึ่ง $[G : H] = 2$ แล้ว H เป็นกรุปย่อยปรกติ

2. กรุปสลับ $A_n$ เป็นกรุปย่อยปรกติของกรุปสมมาตร $S_n$ สำหรับทุกๆ จำนวนเต็มบวก n

**บทพิสูจน์** 1. ให้ G เป็นกรุปจำกัดและ H เป็นกรุปย่อยของ G ซึ่ง $[G : H] = 2$ นั่นคือเซตของโคเซตขวาทั้งหมดและเซตของโคเซตขวาทั้งหมดของ H ใน G มีเพียงเซตละ 2 โคเซต แล้วเราจะแสดงว่า $aH = Ha$ สำหรับทุกๆ $a \in G$

ให้ $a \in G$ ถ้า $a \in H$ แล้ว $aH = H = Ha$ และถ้า $a \notin H$ แล้ว $\{ H, Ha \}$ และ $\{ H, aH \}$ คือเซตของโคเซตขวาทั้งหมดและเซตของโคเซตขวาทั้งหมดของ H ใน G ดังนั้น $H \cup Ha = G = H \cup aH$ โดยที่ $H \cap Ha = \phi = H \cap aH$ ทำให้ได้ $aH = G - H = Ha$ ดังต้องการ

2. เพราะว่า $[G : H] = \frac{|G|}{|H|}$ สำหรับทุกๆ กรุปจำกัด G และทุกๆ กรุปย่อย H ของ G ดังนั้น สำหรับแต่ละจำนวนเต็มบวก n จะได้ว่า $[S_n : A_n] = \frac{|S_n|}{|A_n|} = \frac{n!}{n!/2} = 2$ ทำให้ได้โดยข้อ 1 ว่า $A_n$ เป็นกรุปย่อยปรกติของ $S_n$ ❐

## แบบฝึกหัด 5.3

1. จงแสดงว่าทุกๆ กรุปย่อยของกรุปอาบีเลียนเป็นกรุปย่อยปรกติ
2. ให้ G และ H เป็นกรุป จงพิสูจน์ว่า $G \times \{e_H\}$ และ $\{e_G\} \times H$ เป็นกรุปย่อยปรกติของ $G \times H$
3. ให้ H และ N เป็นกรุปย่อยและกรุปย่อยปรกติของกรุป G ตามลำดับ จงพิสูจน์ว่า
   3.1 NH เป็นกรุปย่อยของ G
   3.2 $H \cap N$ เป็นกรุปย่อยปรกติของ G
4. จงหากรุปย่อยปรกติทั้งหมดของกรุปต่อไปนี้ : $S_3$ และ $D_4$ ( $=G_S$)
5. จงยกตัวอย่างกรุป E, F และ G ซึ่ง $E \subset F \subset G$ โดยที่ E เป็นกรุปย่อยปรกติของ F และ F เป็นกรุปย่อยปรกติของ G แต่ E ไม่เป็นกรุปย่อยปรกติของ G
6. ให้ G เป็นกรุปและ $H = \{a \in G \mid ax = xa$ สำหรับทุกๆ $x \in G\}$ จงพิสูจน์ว่า H เป็นกรุปย่อยปรกติของ G และเราเรียกกรุปย่อยปรกติ H เช่นนี้ว่า *ศูนย์กลาง (center)* ของ G

7. ให้ G เป็นกรุปและ $a \in G$ ซึ่ง $|a| = 2$ จงพิสูจน์ว่า $\langle a \rangle$ เป็นกรุปย่อยปรกติของ G ก็ต่อเมื่อ a อยู่ในศูนย์กลางของ G [ดูนิยามในข้อ 6]

8. ให้ G เป็นกรุปและสำหรับแต่ละ $a \in G$ นิยามเซนทรัลไลเซอร์ของ a ใน G คือเซต

$$C_a = \{x \in G \mid ax = xa\} = \{x \in G \mid a = xax^{-1}\}$$

จงพิสูจน์ว่า

8.1 $C_a$ เป็นกรุปย่อยของกรุป G สำหรับทุกๆ $a \in G$

8.2 ข้อความต่อไปนี้สมมูลกันสำหรับทุกๆ $a, x, y \in G$

(ก) $xax^{-1} = y$ (ข) $axy^{-1} = xy^{-1}a$ (ค) $C_a x = C_a y$

8.3 สำหรับแต่ละ $a \in G$ จะมีสมนัยหนึ่งต่อหนึ่งระหว่างเซต $\{xax^{-1} \mid x \in G\}$ กับเซตของโคเซตทั้งหมดของ $C_a$ ใน G

8.3 สำหรับแต่ละ $a \in G$ จำนวนสมาชิกใน G ในรูปแบบ $xax^{-1}$ ที่แตกต่างกันทั้งหมดเท่ากับ $[G : C_a]$

9. ให้ G เป็นกรุปและ $\sim$ เป็นความสัมพันธ์ใน G กำหนดสำหรับทุกๆ $a,b \in G$ โดย

$$a \sim b \quad \text{ก็ต่อเมื่อ} \quad \text{มี } x \in G \text{ ซึ่ง } b = xax^{-1}$$

จงพิสูจน์ว่า $\sim$ เป็นความสัมพันธ์สมมูลซึ่ง $|\overline{a}| = [G : C_a]$ สำหรับแต่ละ $a \in G$

10. ให้ H เป็นกรุปย่อยของกรุป G จงพิสูจน์ว่าข้อความต่อไปนี้สมมูลกัน

(ก) H เป็นกรุปย่อยปรกติของ G

(ข) $ab \in H \Leftrightarrow ba \in H$ สำหรับทุกๆ $a, b \in G$

11. ให้ G เป็นกรุป เราเรียกสมาชิก $aba^{-1}b^{-1}$ สำหรับทุกๆ $a, b \in G$ ว่า *คอมมิวเทเตอร์ (commutator)* จงพิสูจน์ว่าถ้า H เป็นกรุปย่อยของกรุป G ซึ่งทุกๆ คอมมิวเทเตอร์ของ G เป็นสมาชิกของ H เป็นกรุปย่อยปรกติของ G

12. ให้ H เป็นกรุปย่อยของกรุป G และให้ S เป็นผลรวมของโคเซต Ha ทั้งหลายซึ่ง $Ha = aH$ จงพิสูจน์ว่า S เป็นกรุปย่อยของ G และ H เป็นกรุปย่อยปรกติของ S

## 5.4 กรุปผลหาร

เรารู้จักเซต aH และ Ha จากการพิสูจน์ทฤษฎีบทลากรองจ์ เมื่อ H เป็นกรุปย่อยของกรุป G และในหัวข้อก่อนเราได้เรียกเซตเหล่านี้ว่า "โคเซตซ้าย" และ "โคเซตขวา" ตามลำดับ อย่างไรก็ตามผลคูณตามบทนิยาม 3.4.19 ของเซตย่อยของกรุปเหล่านี้ยังคงเป็นเซตย่อยของกรุป จึงเกิดคำถามว่า "ผลคูณของโคเซตซ้ายยังคงเป็นโคเซตซ้าย" หรือ "ผลคูณของโคเซตขวายังคงเป็นโคเซตขวา" หรือไม่ หรือจะเป็นภายใต้เงื่อนไขใด ในหัวข้อนี้เราจะพิจารณาโคเซตซ้ายและโคเซตขวาของกรุปย่อยปรกติของกรุปซึ่งจากหัวข้อก่อน ทำให้เราทราบว่าเซตของโคเซตซ้ายก็คือเซตของโคเซตขวา ดังนั้นเราจึงอาจกล่าวโดยละคำว่า "ซ้าย" หรือ "ขวา" ได้ และจะเรียกรวมกันอย่างสั้นๆ ว่า "โคเซต" เราจะแสดงว่าผลคูณของโคเซตของกรุปย่อยปรกติของกรุปยังคงเป็นโคเซต ยิ่งไปกว่านั้น "การคูณ" ระหว่างโคเซตตามบทนิยาม 3.4.19 เป็นการดำเนินการบนเซตของโคเซตทั้งหมดที่สอดคล้องสมบัติการเป็นกรุป โดยเราเรียกกรุปที่สร้างจากเซตของโคเซตว่า "กรุปผลหาร" ซึ่งเป็นกรุปที่มีความสำคัญต่อการศึกษาทฤษฎีกรุปซึ่งเราจะศึกษากันในบทต่อไป

ขอทบทวนว่าถ้า G เป็นกรุปและ N เป็นกรุปย่อยของ G แล้วสำหรับทุกๆ $a, b \in G$ จะได้

$$(aN)(bN) = \{(an)(bn') \mid n, n' \in N\}$$

5.4.1 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยของกรุป G แล้ว N เป็นกรุปย่อยปรกติของ G ก็ต่อเมื่อ $(aN)(bN) = abN$ สำหรับทุกๆ $a, b \in G$

**บทพิสูจน์** ให้ N เป็นกรุปย่อยปรกติของกรุป G และ $a, b \in G$ แล้วจะพิสูจน์ว่า $(aN)(bN) = abN$ ให้ $n, n' \in N$ แล้วเพราะ $nb \in Nb$ และ $Nb = bN$ ดังนั้นจะมี $n_1 \in N$ ซึ่ง $nb = bn_1$ ทำให้ได้

$$(an)(bn') = a(nb)n' = a(bn_1)n' = (ab)(n_1n') \in abN$$

นอกจากนี้ $(ab)n = (ae)(bn) \in (aN)(bN)$ ซึ่งแสดงว่า $(aN)(bN) \subseteq abN$ และ $abN \subseteq (aN)(bN)$ ตามลำดับ เพราะฉะนั้น $(aN)(bN) = abN$

ในการพิสูจน์บทกลับ กำหนดให้ข้อความ "$(aN)(bN) = abN$ สำหรับทุกๆ $a, b \in G$" เป็นจริง และจะพิสูจน์ว่า $a^{-1}na \in H$ สำหรับทุกๆ $a \in G$ และทุกๆ $n \in N$ โดยให้ $n \in N$ และ $a \in G$ แล้ว $a^{-1}na = (a^{-1}n)(ae) \in (a^{-1}N)(aN)$ แต่โดยข้อความที่กำหนดให้เป็นจริงจะได้ว่า $(a^{-1}N)(aN) = a^{-1}aN = eN = N$ ดังนั้น $a^{-1}na \in N$ เพราะฉะนั้น N เป็นกรุปย่อยปรกติของ G ❐

แม้ว่าทฤษฎีบท 5.4.1 จะแสดงว่าผลคูณของโคเซตของกรุปย่อยปรกติของกรุปจะเป็นโคเซตของกรุปย่อยปรกติของกรุปก็ตาม แต่ก็เป็นการแสดงการคูณในรูปของตัวแทนของแต่ละโคเซต ดังนั้นการจะแสดงว่า "การคูณ" ระหว่างโคเซตดังกล่าวเป็นการดำเนินการบนเซตของโคเซตทั้งหมด เราจะต้องพิสูจน์ให้ได้ว่า ไม่ว่าตัวแทนของโคเซต aN และ bN จะเป็นตัวใดก็ตาม ผลคูณของโคเซตทั้งสองยังคงได้เป็นโคเซต abN

5.4.2 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยปรกติของกรุป G และให้ $\frac{G}{N}$ เป็นสัญลักษณ์แทนเซตของโคเซตของ N ใน Gทั้งหมด นั่นคือ

$$\frac{G}{N} = \{aN \mid a \in G\}$$

แล้ว "การคูณ" ระหว่างโคเซตตามบทนิยาม 3.4.19 เป็นการดำเนินการบน $\frac{G}{N}$

**บทพิสูจน์** ให้ $a, a', b, b' \in G$ โดยที่ $aN = a'N$ และ $bN = b'N$ แล้ว $a^{-1}a' \in N$ และ $b^{-1}b' \in N$ แต่ N เป็นกรุปย่อยปรกติ ดังนั้น $b^{-1}(a^{-1}a')b \in N$ ทำให้ได้ $[b^{-1}(a^{-1}a')b][b^{-1}b'] \in N$ และได้

$$(ab)^{-1}(a'b') = (b^{-1}a^{-1})(a'b') = b^{-1}(a^{-1}a')(bb^{-1})b' = [b^{-1}(a^{-1}a')b][b^{-1}b'] \in N$$

เพราะฉะนั้น $abN = a'b'N$ ซึ่งเป็นอันจบการพิสูจน์ ❐

5.4.3 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยปรกติของกรุป G แล้ว $\frac{G}{N}$ กับ "การคูณ" ระหว่างโคเซตตามบทนิยาม 3.4.19 เป็นกรุป

**บทพิสูจน์** ให้ $a, b, c \in G$ แล้ว $[(aN)(bN)](cN) = (abN)(cN) = ((ab)c)N = (a(bc)N = (aN)(bcN) = (aN)[(bN)](cN)]$ ซึ่งแสดงว่า "การคูณระหว่างโคเซต" สอดคล้องสมบัติการเปลี่ยนหมู่

เพราะว่า $(aN)N = (aN)(eN) = (ae)N = aN$ สำหรับทุกๆ $a \in G$ ดังนั้น $N = eN$ เป็นเอกลักษณ์ของ $\frac{G}{N}$ ภายใต้ "การคูณระหว่างโคเซต"

สุดท้ายให้ $a \in G$ แล้ว $a^{-1} \in G$ ซึ่งทำให้ได้ $(aN)(a^{-1}N) = (aa^{-1})N = eN = (a^{-1}a)N = (a^{1}N)(aN)$ ดังนั้น $a^{-1}N$ เป็นตัวผกผันของ aN ใน $\frac{G}{N}$ ภายใต้ "การคูณระหว่างโคเซต"

เพราะฉะนั้น $\frac{G}{N}$ เป็นกรุป ❐

5.4.3 **บทนิยาม** เราเรียกกรุปในทฤษฎีบท 5.4.3 ว่า *กรุปผลหาร (quotient group)* ของ N ใน G

**หมายเหตุ** 1. เพราะว่า $\frac{G}{N}$ คือเซตของโคเซตทั้งหมดของกรุปย่อยปรกติ N ในกรุป G ดังนั้นถ้า G เป็นกรุปจำกัด แล้วอันดับของกรุปผลหารเท่ากับดรรชนีของ N ใน G นั่นคือ $\left|\frac{G}{N}\right| = [G : N]$

2. เนื่องจากการดำเนินการบนกรุปใดๆ เราเรียกว่า "การคูณ" ดังนั้นจึงเรียกการดำเนินการบนกรุปผลหารว่า "การคูณระหว่างโคเซต" หรือเรียกสั้นๆ ว่า "การคูณ" แต่ถ้า G เป็น "กรุปการบวก" นั่นคือการดำเนินการของ G คือ + แล้วเพื่อให้สอดคล้องกับการดำเนินการของ G สัญลักษณ์แทนโคเซตของ N ใน G จึงเขียนเป็น a + N หรือ N + a และการดำเนินการบนกรุปผลหารก็จะเป็นการบวกเช่นเดียวกัน กล่าวคือสำหรับแต่ละ a, b $\in$G จะเขียนการบวกของโคเซตดังนี้

$$(a + N) + (b + N) = (a + b) + N$$

**5.4.5 ตัวอย่าง** พิจารณากรุปย่อยปรกติ N = $<r_2>$ ของกรุป $G_S$ แล้วโคเซตของ N ใน $G_S$ ที่ต่างกันทั้งหมดจะเป็นสมาชิกของกรุปผลหาร $\frac{G_S}{<r_2>}$ ทำให้ได้

$$\frac{G_S}{<r_2>} = \{\{e, r_2\}, \{r_1, r_3\}, \{h, v\}, \{d_1, d_2\}\}$$

ทำให้เขียนตารางการคูณของกรุปผลหารแสดงดังตารางข้างล่าง โดยจะแสดงตัวอย่างการคูณระหว่าง $\{d_1, d_2\}$ กับ $\{r_1, r_3\}$ ดังนี้

$$\{d_1, d_2\}\{r_1, r_3\} = (d_1N)(r_1N) = d_1r_1N = hN = \{h, v\}$$

| | $\{e, r_2\}$ | $\{r_1, r_3\}$ | $\{h, v\}$ | $\{d_1, d_2\}$ |
|---|---|---|---|---|
| $\{e, r_2\}$ | $\{e, r_2\}$ | $\{r_1, r_3\}$ | $\{h, v\}$ | $\{d_1, d_2\}$ |
| $\{r_1, r_3\}$ | $\{r_1, r_3\}$ | $\{e, r_2\}$ | $\{d_1, d_2\}$ | $\{h, v\}$ |
| $\{h, v\}$ | $\{h, v\}$ | $\{d_1, d_2\}$ | $\{e, r_2\}$ | $\{r_1, r_3\}$ |
| $\{d_1,d_2\}$ | $\{d_1, d_2\}$ | $\{h, v\}$ | $\{r_1, r_3\}$ | $\{e, r_2\}$ |

○

5.4.6 **ตัวอย่าง** พิจารณากรุปวัฏจักร Z ซึ่งเป็นกรุปการบวก จะได้ว่าทุกๆ กรุปย่อยของ Z เป็นกรุปวัฏจักรในรูปแบบ <n> เมื่อ n เป็นจำนวนเต็มบวก และเพราะกรุปวัฏจักรเป็นกรุปอาบีเลียน ดังนั้นทุกๆ กรุปย่อย <n> ของ Z เมื่อ n เป็นจำนวนเต็มบวก เป็นกรุปย่อยปรกติ

สำหรับ n > 1 โคเซตของ <n> ใน Z เขียนได้ในรูปแบบต่อไปนี้

$$a + \langle n \rangle = \{a + kn \mid k \in Z\}$$

สำหรับทุกๆ จำนวนเต็ม a แต่สมาชิกของ a + <n> ซึ่งอยู่ในรูปแบบ a + kn เป็นจำนวนเต็มซึ่งสัมพันธ์คอนกรูเอนซ์กับ a มอดูโล n ดังนั้น

$$a + \langle n \rangle = \bar{a}$$

สำหรับทุกๆ จำนวนเต็ม a ซึ่งแสดงว่ากรุปผลหาร $\frac{Z}{\langle n \rangle}$ ก็คือกรุป $Z_n$ นั่นเอง ○

5.4.7 **ตัวอย่าง** พิจารณากรุป $G = Z_{12} \times Z_4$ กับกรุปย่อย N ของ G ต่อไปนี้

$$N = \langle \bar{3} \rangle \times \langle \bar{2} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \times \{\bar{0}, \bar{2}\}$$
$$= \{(\bar{0},\bar{0}), (\bar{0},\bar{2}), (\bar{3},\bar{0}), (\bar{3},\bar{2}), (\bar{6},\bar{0}), (\bar{6},\bar{2}), (\bar{9},\bar{0}), (\bar{9},\bar{2})\}$$

แล้วพิสูจน์ได้ไม่ยากว่า N เป็นกรุปย่อยปรกติของ G และโดยวิธีการหาโคเซตทั้งหมดของ N ใน G ดังที่เคยกล่าวมา จะได้สมาชิกทั้งหมดของกรุปผลหาร $\frac{G}{N}$ ดังต่อไปนี้

$$N_{0,0} = N,$$
$$N_{0,1} = (\bar{0},\bar{1}) + N = \{(\bar{0},\bar{1}), (\bar{0},\bar{3}), (\bar{3},\bar{1}), (\bar{3},\bar{3}), (\bar{6},\bar{1}), (\bar{6},3), (\bar{9},\bar{1}), (\bar{9},\bar{3})\},$$
$$N_{1,0} = (\bar{1},\bar{0}) + N = \{(\bar{1},\bar{0}), (\bar{1},\bar{2}), (\bar{4},\bar{0}), (\bar{4},\bar{2}), (\bar{7},\bar{0}), (\bar{7},\bar{2}), (\overline{10},\bar{0}), (\overline{10},\bar{2})\},$$
$$N_{1,1} = (\bar{1},\bar{1}) + N = \{(\bar{1},\bar{1}), (\bar{1},\bar{3}), (\bar{4},1), (\bar{4},\bar{3}), (\bar{7},\bar{1}), (\bar{7},\bar{3}), (\overline{10},\bar{1}), (\overline{10},\bar{3})\},$$
$$N_{2,0} = (\bar{2},\bar{0}) + N = \{(\bar{2},\bar{0}), (\bar{2},\bar{2}), (\bar{5},\bar{0}), (\bar{5},\bar{2}), (\bar{8},\bar{0}), (\bar{8},\bar{2}), (\overline{11},\bar{0}), (\overline{11},\bar{2})\},$$
$$N_{2,1} = (\bar{2},\bar{1}) + N = \{(\bar{2},\bar{1}), (\bar{2},\bar{3}), (\bar{5},1), (\bar{5},\bar{3}), (\bar{8},\bar{1}), (\bar{8},\bar{3}), (\overline{11},\bar{1}), (\overline{11},\bar{3})\},$$

ซึ่งมีตารางการคูณของกรุปผลหาร แสดงในตารางข้างล่างนี้

| + | $N_{0,0}$ | $N_{0,1}$ | $N_{1,0}$ | $N_{1,1}$ | $N_{2,0}$ | $N_{2,1}$ |
|---|---|---|---|---|---|---|
| $N_{0,0}$ | $N_{0,0}$ | $N_{0,1}$ | $N_{1,0}$ | $N_{1,1}$ | $N_{2,0}$ | $N_{2,1}$ |
| $N_{0,1}$ | $N_{0,1}$ | $N_{0,0}$ | $N_{1,1}$ | $N_{1,0}$ | $N_{2,1}$ | $N_{2,0}$ |
| $N_{1,0}$ | $N_{1,0}$ | $N_{1,1}$ | $N_{2,0}$ | $N_{2,1}$ | $N_{0,0}$ | $N_{0,1}$ |
| $N_{1,1}$ | $N_{1,1}$ | $N_{1,0}$ | $N_{2,1}$ | $N_{2,0}$ | $N_{0,1}$ | $N_{0,0}$ |
| $N_{2,0}$ | $N_{2,0}$ | $N_{2,1}$ | $N_{0,0}$ | $N_{0,1}$ | $N_{1,0}$ | $N_{1,1}$ |
| $N_{2,1}$ | $N_{2,1}$ | $N_{2,0}$ | $N_{0,1}$ | $N_{0,0}$ | $N_{1,1}$ | $N_{1,0}$ |

○

## แบบฝึกหัด 5.4

1. จงเขียนสมาชิกทั้งหมดของกรุปผลหารในข้อต่อไปนี้ พร้อมบอกอันดับของกรุป

   1.1 $\dfrac{Z_8}{<\bar{3}>}$ 1.2 $\dfrac{Z_8}{<\bar{2}>}$ 1.3 $\dfrac{Z_{12}\times Z_4}{<(\bar{3},\bar{2})>}$

   1.4 $\dfrac{<3>}{<6>}$ เมื่อ $<6>\subseteq<3>\subseteq Z$

   1.5 $\dfrac{Z_4\times Z_2}{<(0,1)>}$ เมื่อ $<(0,1)>$ เป็นกรุปย่อยของ $Z_4\times Z_2$ ซึ่งก่อกำเนิดโดย (0, 1)

   1.6 $\dfrac{R\times R}{H}$ เมื่อ $H=\{(x,0)\mid x\in R\}$

   1.7 $\dfrac{R\times R}{H}$ เมื่อ $H=\{(x,y)\mid y=-x\}$

   1.8 $\dfrac{R\times R}{H}$ เมื่อ $H=\{(x,y)\mid y=2x\}$

2. ให้ N เป็นกรุปย่อยปรกติของกรุป G จงพิสูจน์ว่าข้อความต่อไปนี้สมมูลกัน

   (ก) G เป็นกรุปอาบีเลียน

   (ข) $\dfrac{G}{N}$ เป็นกรุปอาบีเลียน

   (ค) $aba^{-1}b^{-1}\in N$ สำหรับทุกๆ $a, b\in G$

3. ให้ N เป็นกรุปย่อยปรกติของกรุป G จงพิสูจน์ว่าข้อความต่อไปนี้

   3.1 ถ้าทุกๆ สมาชิกของ $\dfrac{G}{N}$ มีอันดับจำกัดและทุกๆ สมาชิกของ N มีอันดับจำกัด แล้ว ทุกๆ สมาชิกของ G มีอันดับจำกัด

   3.2 อันดับของ aN ใน $\dfrac{G}{N}$ เป็นตัวหารของอันดับของ a ใน G สำหรับทุกๆ $a\in G$

   3.3 ถ้า $[G:N]=m$ เมื่อ m เป็นจำนวนเต็มบวก แล้ว $a^m\in N$ สำหรับทุกๆ $a\in G$

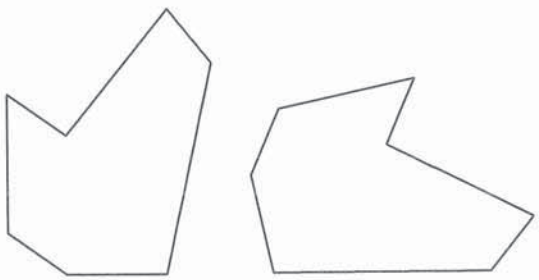
   3.4 ถ้า $[G:N]=p$ เมื่อ p เป็นจำนวนเฉพาะ แล้ว G มีสมาชิกอันดับ p

4. จงพิสูจน์ว่าทุกๆ สมาชิกใน $\dfrac{Q}{Z}$ มีอันดับจำกัด

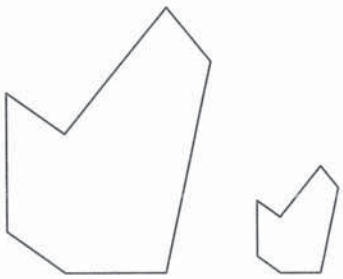
5. ให้ K เป็นกรุปย่อยปรกติของกรุป G และ H เป็นกรุปย่อยปรกติของกรุป K จงพิสูจน์ว่าถ้า $\dfrac{G}{H}$ เป็นกรุปอาบีเลียน แล้ว $\dfrac{G}{K}$ และ $\dfrac{K}{H}$ ต่างเป็นกรุปอาบีเลียน

# บทที่ 6
# กรุปสมสัณฐาน
# ISOMORPHISM OF GROUPS

ความเข้าใจได้ของมนุษย์เกิดจากความฉลาดหรือความสามารถในการแยกแยะ จดจำความเหมือน ความแตกต่าง และความสัมพันธ์กันของสรรพสิ่ง ในพจนานุกรมบอกเราว่า สิ่งสองสิ่งสมสัณฐานกันถ้าสองสิ่งนั้นมีโครงสร้างเหมือนกัน สมสัณฐานในวิชาเรขาคณิตมีหลายชนิด ชนิดง่ายที่สุดและคุ้นเคยกันเป็นอย่างดีก็คือ "การเท่ากันทุกประการ (congruence)" และ "ความคล้าย (similarity)" รูปเรขาคณิตสองรูปเท่ากันทุกประการถ้ามีโมชันบนระนาบส่งรูปหนึ่งไปบนอีกรูปหนึ่ง และรูปเรขาคณิตสองรูปคล้ายกันถ้ามีการเลื่อนทางขนานบนระนาบส่งรูปหนึ่งไปบนอีกรูปหนึ่งในลักษณะ "หด" หรือ "ยืด" ด้วย อัตราส่วนคงตัว ดังรูปข้างล่างนี้



**รูปเท่ากันทุกประการ**



**รูปคล้ายกัน**

ความหมายของสมสัณฐานเป็นศูนย์กลางของการศึกษาในหลายๆ สาขาของวิชาคณิตศาสตร์และซึมแทรกอยู่ในทุกๆการให้เหตุผลเชิงนามธรรม ในบทนี้เราจะศึกษาการสมสัณฐานของกรุป จำแนกกรุปต่างๆ ด้วยสมสัณฐาน ตลอดจนศึกษาการแทนกรุปนามธรรมด้วยกรุปที่รู้จัก

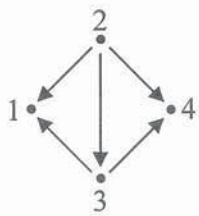
## 6.1 สมสัณฐาน

ก่อนจะให้นิยามสมสัณฐานระหว่างกรุปสองกรุป เราลองพิจารณาความหมายของสมสัณฐานทั่วๆ ไปเสียก่อน

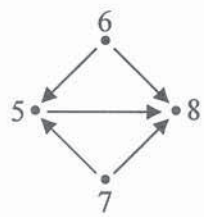
| | | |
|---|---|---|
| MADAM | | ROTOR |
| A | และ | O |
| MAD | | ROT |

ตัวอย่างแรกเราพิจารณาการเรียงกันของอักษรในแผนภาพข้างบน จะเห็นว่าแผนภาพทั้งสองข้างต้นเป็นการวางเรียงอักษรที่แตกต่างกัน แต่ความคิดเชิงนามธรรมบอกเราว่าการเรียงทั้งสองเป็นสมสัณฐานกันเพราะว่าการเรียงอันแรกจะกลายเป็นการเรียงอันที่สองถ้าเราแทนที่ M ด้วย R แทนที่ A ด้วย O และแทนที่ D ด้วย T

อีกตัวอย่างหนึ่งเช่น การไหลของข่ายงานสองข่ายงานที่ต่างกันที่มีแผนภาพแสดงดังข้างล่างนี้ ซึ่งอาจเป็นตัวอย่างของข่ายงานการเงินกับข่ายงานการขนส่งสินค้าที่แทนหน่วยงานด้วยจุดและแทนการไหลด้วยลูกศร




**ข่ายงาน (ก)**




**ข่ายงาน (ข)**

แม้ว่าข่ายงานทั้งสองเป็นข่ายงานที่ต่างกัน แต่ก็สมสัณฐานกัน เพราะว่าข่ายงาน (ก) จะกลายเป็นข่ายงาน (ข) ถ้าเราแทนจุด 1 ด้วย 6 แทนจุด 2 ด้วย 5 แทนจุด 3 ด้วย 8 และแทนจุด 4 ด้วย 7

ขอให้สังเกตว่า "การแทน" ที่กล่าวถึงในทั้งสองตัวอย่างข้างต้น ก็คือการมีฟังก์ชันระหว่างเซตสองเซตที่เป็นแบบหนึ่งต่อหนึ่งและทั่วถึงซึ่งยืนยงโครงสร้างตามลำดับ ดังต่อไปนี้

$$\begin{pmatrix} M & A & D \\ \downarrow & \downarrow & \downarrow \\ R & O & T \end{pmatrix} \quad \text{และ} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 5 & 8 & 7 \end{pmatrix}$$

พิจารณาในเรื่องกรุป ให้ $G_1 = \{0, 1, 2\}$ และ $G_2 = \{e, a, b\}$ เป็นกรุปสองกรุปภายใต้การดำเนิน การ + บน $G_1$ และการดำเนินการ · บน $G_2$ แสดงดังตารางข้างล่างนี้

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

**ตารางของ $G_1$**

| · | e | a | b |
|---|---|---|---|
| e | e | a | b |
| a | a | b | e |
| b | b | e | a |

**ตารางของ $G_2$**

แม้ว่า $G_1$ และ $G_2$ ไม่ใช่กรุปเดียวกันแต่สมสัณฐานกัน และโดยความเป็นจริง มีฟังก์ชันจาก $G_1$ ไปยัง $G_2$ ที่เป็นแบบหนึ่งต่อหนึ่งและทั่วถึงซึ่งยืนยงการดำเนินการของทั้งสองกรุป ดังนี้

$$\begin{pmatrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ e & a & b \end{pmatrix}$$

โดยทั่วไป การสมสัณฐานกันของกรุปสองกรุป จะต้องมีฟังก์ชัน $\theta$ ชนิดหนึ่งต่อหนึ่งและทั่วถึงระหว่างกรุปทั้งสองในลักษณะที่ยืนยงการดำเนินการของทั้งสองกรุป กล่าวคือสำหรับทุกๆ คู่ $a, b \in G_1$ ถ้า $\theta(a) = a'$ และ $\theta(b) = b'$ แล้ว $\theta(ab) = a'b'$ นั่นคือถ้า $\theta$ ส่ง a ไปยัง $a'$ และส่ง b ไปยัง $b'$ แล้ว $\theta$ ต้องส่ง ab ไปยัง $a'b'$ เพราะจะทำให้ $\theta$ แปลงตารางการคูณของ $G_1$ เป็นตารางการคูณของ $G_2$ ดังนี้

| $G_1$ | b | | $G_2$ | $b'$ |
|---|---|---|---|---|
| | $\vdots$ | | | $\vdots$ |
| a | $\cdots$ ab | $\xrightarrow[\text{แทน x ด้วย } \theta(x) \text{ สำหรับทุกๆ x}]{}$ | $a'$ | $\cdots$ $a'b'$ |

เราอาจกล่าวสถานการณ์ของการสมสัณฐานกันของกรุปได้อีกอย่างหนึ่งว่า กรุปสองกรุปจะสมสัณฐานกัน ถ้ากรุปทั้งสองเป็นเสมือนกรุปเดียวกัน ต่างกันเฉพาะชื่อของสมาชิกในแต่ละกรุป ดังนั้นถ้าเปลี่ยนชื่อสมาชิกในกรุปหนึ่งให้เหมือนกับของอีกกรุปหนึ่ง แล้วกรุปทั้งสองจะเป็นกรุปเดียวกันและฟังก์ชันที่ส่งแบบยืนยงการดำเนินการก็คือเครื่องมือการเปลี่ยนชื่อนั่นเอง

6.1.1 **บทนิยาม** ให้ G และ H เป็นกรุปและ $\theta : G \longrightarrow H$ เราจะเรียก $\theta$ ว่า *สมสัณฐาน (isomorphism)* ถ้า $\theta$ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึงและ $\theta(ab) = \theta(a)\theta(b)$ สำหรับทุกๆ $a, b \in G$

ถ้ามีสมสัณฐานจาก G ไปยัง H เราจะกล่าวว่า G *สมสัณฐานกับ (isomorphic)* H และเขียนแทนด้วยสัญลักษณ์ $G \cong H$

ขอให้สังเกตว่าในสมการ $\theta(ab) = \theta(a)\theta(b)$ นั้น ab เป็นผลการดำเนินการของ G ส่วน $\theta(a)\theta(b)$ เป็นผลการดำเนินการใน H

ปัญหาต่อไปก็คือ เราจะทราบได้อย่างไร หรือแสดงได้อย่างไร ว่ากรุปสองกรุป G และ H เป็นสมสัณฐานกันหรือไม่ สำหรับในกรณีที่กรุปสองกรุปเป็นสมสัณฐานกันอาจจะแสดงได้ไม่ยากเพราะตามความหมายหรือบทนิยามบอกให้เรากระทำตามขั้นตอนต่อไปนี้

1. "หา" หรือ "สร้าง" ฟังก์ชัน $\theta : G \rightarrow H$ (ในการสร้าง เราอาจคาดเดามาก่อนแล้วว่า $\theta$ น่าจะเป็นสมสัณฐาน)
2. ตรวจสอบหรือพิสูจน์ว่า $\theta$ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึง
3. ตรวจสอบหรือพิสูจน์ว่า $\theta$ สอดคล้องสมการ $\theta(ab) = \theta(a)\theta(b)$ สำหรับทุกๆ $a, b \in G$

6.1.2 **ตัวอย่าง** ให้ R แทนกรุปของจำนวนจริงทั้งหมดภายใต้ "การบวก + " ของจำนวนจริงและ $R^{pos}$ แทนกรุปของจำนวนจริงบวกทั้งหมดภายใต้ "การคูณ ·" ของจำนวนจริง แล้วเป็นที่น่าสนใจว่ากรุปทั้งสองนี้สมสัณฐานกันหรือไม่ ซึ่งเราอาจเดาว่ากรุปทั้งสองสมสัณฐานกัน ทำให้เราต้องพิสูจน์ข้อคาดเดานี้ด้วยขั้นตอนที่กล่าวไว้ในย่อหน้าก่อน ดังนี้

1. เราคาดเดาด้วยสมบัติของฟังก์ชันเชิงกำลังจากที่เคยศึกษามาว่า $f : R \rightarrow R^{pos}$ ซึ่งนิยามโดย $f(x) = e^x$ สำหรับทุกๆ จำนวนจริง x **อาจ**เป็นสมสัณฐานที่ต้องการ

2. ตรวจสอบว่า f ที่คาดเดาในข้อ 1 เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งโดยให้ a และ b เป็นจำนวนจริงซึ่ง $f(a) = f(b)$ นั่นคือ $e^a = e^b$ แล้วโดยการหาภาพของฟังก์ชันลอการิทึมธรรมชาติของ $e^a = e^b$ จะได้ $a = b$

   ต่อไปตรวจสอบว่า f เป็นฟังก์ชันชนิดทั่วถึงโดยให้ y เป็นจำนวนจริงบวกแล้ว $y = e^{\ln y} = f(\ln y)$ ดังนั้นมีจำนวนจริง $x = \ln y$ ซึ่ง $f(x) = y$

   เพราะฉะนั้น f ที่คาดเดาไว้เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึง

3. ตรวจสอบหรือพิสูจน์ว่า f สอดคล้องสมการ $f(a+b) = f(a)f(b)$ สำหรับทุกๆ $a, b \in R$ ซึ่งการตรวจสอบนี้ เราประยุกต์ความจริงที่รู้จักกันเป็นอย่างดีว่า $e^{a+b} = e^a e^b$ (และด้วยเหตุผลนี้ จึงอาจตอบคำถามว่าทำไมจึงเลือกฟังก์ชันเชิงกำลังเป็นสมสัณฐาน)

เพราะฉะนั้น $(R; +) \cong (R^{pos}; \cdot)$ ○

**6.1.3 ตัวอย่าง** สำหรับกรณีกรุปจำกัด เราอาจบอกความเป็นสมสัณฐานกันโดยดูง่ายๆ จากตารางการดำเนินการของทั้งสองกรุป เช่นกรุป $G = \{1,-1, i ,-i\}$ ซึ่งมีตารางการคูณแสดงดังในตัวอย่าง 3.1.9 กับกรุป $Z_4 = \{\bar{0},\bar{1},\bar{2},\bar{3}\}$ ซึ่งมีตารางการบวกแสดงดังตารางข้างล่างนี้

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

จะเห็นว่าถ้าเราแทน $\bar{0}$ ด้วย 1 แทน $\bar{1}$ ด้วย i แทน $\bar{2}$ ด้วย –1 และแทน $\bar{3}$ ด้วย –i แล้วตารางการดำเนินการทั้งสองจะเป็นตารางเดียวกัน นั่นคือเราได้มีการกำหนดฟังก์ชัน $\theta : Z_4 \longrightarrow G$ โดย $\theta(\bar{0}) = 1$, $\theta(\bar{1}) = i$, $\theta(\bar{2}) = -1$ และ $\theta(\bar{3}) = -i$ แล้วเห็นได้ชัดว่า $\theta$ เป็นสมสัณฐาน

ขอให้สังเกตว่า ฟังก์ชัน $\overline{\theta} : Z_4 \longrightarrow G$ ซึ่งกำหนดโดย $\overline{\theta}(\bar{0}) = 1$, $\overline{\theta}(\bar{1}) = -i$, $\overline{\theta}(\bar{2}) = -1$ และ $\overline{\theta}(\bar{3}) = i$ ก็เป็นสมสัณฐานเช่นเดียวกัน ❍

ถ้า G เป็นกรุป แล้วเห็นได้ชัดว่าฟังก์ชันเอกลักษณ์ $\iota_G$ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก G ไปทั่วถึง G และ $\iota_G(ab) = ab = \iota_G(a)\iota_G(b)$ สำหรับทุกๆ $a, b \in G$ ดังนั้น $G \cong G$

ถ้า G และ H เป็นกรุปซึ่ง $G \cong H$ แล้วจะมีสมสัณฐาน $\theta : G \longrightarrow H$ เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง ดังนั้น $\theta^{-1}$ ก็จะเป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงจาก H ไปยัง G ยิ่งไปกว่านั้นสำหรับแต่ละ $c, d \in H$ จะมี $a, b \in G$ ซึ่ง $\theta^{-1}(c) = a$ และ $\theta^{-1}(d) = b$ ทำให้ได้ $ab = \theta^{-1}(c)\theta^{-1}(d)$ และได้

$$\theta(ab) = \theta(\theta^{-1}(c)\theta^{-1}(d)) = \theta(\theta^{-1}(c))\,\theta(\theta^{-1}(d)) = cd$$

ดังนั้น $\theta^{-1}(cd) = ab = \theta^{-1}(c)\theta^{-1}(d)$ ซึ่งแสดงว่า $\theta^{-1}$ ก็เป็นสมสัณฐานด้วย ทำให้ได้ $H \cong G$

ถ้า G, H และ K เป็นกรุปซึ่ง $G \cong H$ และ $H \cong K$ แล้วจะมี $\theta : G \longrightarrow H$ และ $\varphi : H \longrightarrow K$ เป็นสมสัณฐาน ดังนั้นฟังก์ชันประกอบ $\varphi \circ \theta$ ของ $\theta$ และ $\varphi$ จะเป็นสมสัณฐานจาก G ไปยัง K เพราะว่า $\varphi \circ \theta$ จะเป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึงและถ้า $a, b \in G$ แล้ว $\theta(ab) = \theta(a)\theta(b)$ โดยที่ $\theta(a)$ และ $\theta(b)$ เป็นสมาชิกของกรุป H ทำให้ได้

$$\varphi(\theta(a)\theta(b)) = \varphi(\theta(a))\,\varphi(\theta(b)) = (\varphi \circ \theta)(a)\,(\varphi \circ \theta)(b)$$

ดังนั้น $(\varphi \circ \theta)(ab) = \varphi(\theta(ab)) = \varphi(\theta(a)\theta(b)) = (\varphi \circ \theta)(a)\,(\varphi \circ \theta)(b)$
เราจึงสรุปได้เป็นทฤษฎีบทต่อไปนี้

6.1.4 **ทฤษฎีบท** ให้ G, H และ K เป็นกรุป แล้ว

1. $G \cong G$
2. ถ้า $G \cong H$ แล้ว $H \cong G$
3. ถ้า $G \cong H$ และ $H \cong K$ แล้ว $G \cong H$ ❐

**หมายเหตุ** โดยทฤษฎีบท 6.1.4 อาจกล่าวได้ว่า "สมสัณฐาน" เป็นความสัมพันธ์สมมูลในหมู่ของกรุป

ในกรณีกรุปสองกรุปไม่สมสัณฐานกัน เราจะต้องแสดงว่าทุกๆ ฟังก์ชันที่ส่งจากกรุปหนึ่งไปยังอีกกรุปหนึ่งไม่เป็นสมสัณฐาน นั่นคือไม่ใช่ฟังก์ชันหนึ่งต่อหนึ่ง หรือไม่ใช่ฟังก์ชันทั่วถึง หรือมีคู่สมาชิกในกรุปซึ่งเป็นโดเมนที่ทำให้ฟังก์ชันไม่สอดคล้องสมการในบทนิยาม 5.1.1 จะเห็นว่าอาจเป็นการยากมากในทางปฏิบัติที่จะแสดงให้ครบทุกๆ ฟังก์ชันได้ เราจึงต้องหาวิธีการอื่นเพื่อแสดงว่ากรุปสองกรุปไม่สมสัณฐานกัน

เมื่อพิจารณาความหมายของการเป็นกรุปที่สมสัณฐานกันซึ่งดังกล่าวไว้แล้วว่ากรุปทั้งสองนั้นจะเป็นเสมือนกรุปเดียวกัน ต่างกันเฉพาะชื่อของสมาชิกในแต่ละกรุปเท่านั้น แสดงว่ากรุปทั้งสองต้องมีสมบัติต่างๆ เหมือนๆ กัน ดังนั้นถ้ากรุปหนึ่งมีสมบัติอย่างหนึ่งที่อีกกรุปหนึ่งไม่มีสมบัตินั้น ก็จะแสดงว่ากรุปทั้งสองไม่สมสัณฐานกัน และตัวอย่างของสมบัติที่เรานิยมมองหาเพื่อแสดงว่ากรุปสองกรุปไม่สมสัณฐานกัน ตัวอย่างเช่น

1. กรุปหนึ่งเป็นอาบีเลียนกรุป แต่อีกกรุปหนึ่งไม่เป็น
2. แต่ละสมาชิกในกรุปหนึ่งเป็นตัวผกผันของตัวเอง แต่สมาชิกของอีกกรุปหนึ่งไม่เป็นเช่นนั้น
3. กรุปหนึ่งก่อกำเนิดโดยสมาชิก 2 ตัว แต่สมาชิก 2 ตัวใดๆ ในอีกกรุปหนึ่งจะไม่ก่อกำเนิดกรุปนั้น

6.1.5 **ตัวอย่าง** ให้ $R^*$ แทนเซตของจำนวนจริงที่ไม่ใช่ศูนย์ทั้งหมด แล้ว $R^*$ กับการคูณของจำนวนจริงเป็นกรุปซึ่งไม่สมสัณฐานกับกรุป R กับการบวกของจำนวนจริง เพราะว่า 1 เป็นเอกลักษณ์ของ $R^*$ และมี $-1 \in R^*$ ซึ่ง $(-1)(-1) = 1$ ในขณะที่ 0 เป็นเอกลักษณ์ของ R แต่ไม่มีสมาชิก x ใดๆ ใน R ซึ่ง $x + x = 0$

อย่างไรก็ตามสำหรับตัวอย่างนี้ เราอาจแสดงว่า R ไม่สมสัณฐานกับ $R^*$ อีกอย่างหนึ่งโดยสมมติว่ามีสมสัณฐาน $\theta : R \rightarrow R^*$ และขอให้สังเกตว่าสมสัณฐานต้องส่งเอกลักษณ์ไปยังเอกลักษณ์ ดังนั้น $\theta(0) = 1$ และเพราะ $-1 \in R^*$ และ $\theta$ เป็นฟังก์ชันไปบน ดังนั้นจะมี $x \in R$ ซึ่ง $\theta(x) = -1$ ทำให้ได้ $\theta(2x) = \theta(x + x) = \theta(x)\theta(x) = (-1)(-1) = 1 = \theta(0)$ และเพราะ $\theta$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ทำให้ได้ $2x = 0$ นั่นคือ $x = 0$ ดังนั้น $\theta(0) = -1$ และ $\theta(0) = 1$ ทำให้ $\theta$ ไม่เป็นฟังก์ชัน เกิดเป็นข้อขัดแย้งกันเอง เพราะฉะนั้นไม่มีสมสัณฐานจาก R ไปยัง $R^*$ ❍

## แบบฝึกหัด 6.1

1. ให้ G และ H เป็นกรุปและ $\theta : G \rightarrow H$ เป็นสมสัณฐาน จงพิสูจน์ว่า
   1.1 $\theta(e_G) = e_H$ [นั่นคือสมสัณฐานส่งเอกลักษณ์ไปยังเอกลักษณ์]
   1.2 $\theta(a^{-1}) = \theta(a)^{-1}$ สำหรับทุกๆ $a \in G$ [นั่นคือสมสัณฐานส่งตัวผกผันของ $a \in G$ ไปยังตัวผกผันของ $\theta(a) \in H$ หรือกล่าวอีกนัยหนึ่งว่า $\theta(a) = b$ ก็ต่อเมื่อ $\theta(a^{-1}) = b^{-1}$]
   1.3 ถ้า $G = \langle a \rangle$ เป็นกรุปวัฏจักรแล้ว H เป็นกรุปวัฏจักรซึ่ง $H = \langle \theta(a) \rangle$ [นั่นคือสมสัณฐานส่งตัวก่อกำเนิดไปยังตัวก่อกำเนิด]

2. จงแสดงว่ากรุปสองกรุปที่กำหนดในแต่ละข้อต่อไปนี้สมสัณฐานกันหรือไม่
   2.1 $Z_6$ และ $Z_2 \times Z_3$ 2.2 $Z_2 \times Z_2 \times Z_2$ และ $D_4$
   2.3 $S_3$ และ กรุป $G = \{e, a, a^2, b, c, d\}$ ซึ่งมีตารางการคูณแสดงได้ดังนี้

| . | e | a | $a^2$ | b | c | d |
|---|---|---|---|---|---|---|
| e | e | a | $a^2$ | b | c | d |
| a | a | $a^2$ | e | c | d | b |
| $a^2$ | $a^2$ | e | a | d | b | c |
| b | b | d | c | e | $a^2$ | a |
| c | c | b | d | a | e | $a^2$ |
| d | d | c | b | $a^2$ | a | e |

[หมายเหตุ ขอให้สังเกตว่า $c = ab$ และ $d = a^2b$ เราจึงอาจเขียนเซต G ได้ใหม่เป็น $G = \{e, a, a^2, b, ab, a^2b\}$ ซึ่งแสดงว่า G ก่อกำเนิดโดยเซต $\{a, b\}$ โดยที่ a และ b สอดคล้องความสัมพันธ์ $a^3 = e = b^2$ เราจึงนิยมเขียนแทน G ในอีกรูปแบบหนึ่งดังนี้

$$G = \langle a,b \mid a^3 = e = b^2 \rangle \text{ ]}$$

2.4 กรุปของจำนวนเต็มทั้งหมด Z กับกรุปของจำนวนตรรกยะทั้งหมด Q ภายใต้การบวก

2.5 กรุปของจำนวนตรรกยะทั้งหมด Q กับการบวก และกรุปของจำนวนตรรกยะบวกทั้งหมด $Q^*$ กับการคูณ

3. ให้ $G = \{x \in R \mid x \neq -1\}$ และ $*$ เป็นการดำเนินการบน G ซึ่งนิยามสำหรับทุกๆ $x, y \in G$ โดย $x * y = x + y + xy$ จงแสดงว่า $\theta : R^* \longrightarrow G$ นิยามโดย $\theta(x) = x - 1$ สำหรับทุกๆ $x \in R^*$ เป็นสมสัณฐาน

4. ให้ G เป็นกรุปของจำนวนจริงทั้งหมดกับการดำเนินการ $*$ ซึ่งนิยามโดย $x * y = x + y + 1$ สำหรับทุกๆ $x, y \in G$ จงแสดงว่ากรุป R สมสัณฐานกับ G

5. ให้ G, H, K และ T เป็นกรุป จงพิสูจน์ว่า

5.1 $G \times H \cong H \times G$ และถ้า $G \cong H$ และ $K \cong T$ แล้ว $G \times K \cong H \times T$

5.2 $G \cong G \times \{e_H\}$ และ $H \cong e_G \times H$

5.3 G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ $\theta : G \longrightarrow G$ นิยามโดย $\theta(x) = x^{-1}$ สำหรับทุกๆ $x \in G$ เป็นสมสัณฐาน

6. ให้ G และ H เป็นกรุปและ $\theta : G \longrightarrow H$ เป็นสมสัณฐาน จงพิสูจน์ว่า

6.1 $|a| = |\theta(a)|$ สำหรุบทุกๆ $a \in G$

6.2 G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ H เป็นกรุปอาบีเลียน

6.3 G เป็นกรุปวัฏจักร ก็ต่อเมื่อ H เป็นกรุปวัฏจักร

6.4 G เป็นกรุปก่อกำเนิดแบบจำกัด ก็ต่อเมื่อ H เป็นกรุปก่อกำเนิดแบบจำกัด

6.5 G เป็นกรุปอย่างง่าย ก็ต่อเมื่อ H เป็นกรุปอย่างง่าย

[**บทนิยาม** เรากล่าวว่า G เป็น *กรุปอย่างง่าย (simple group)* ถ้า G และ {e} เท่านั้นที่เป็นกรุปย่อยของ G]

## 6.2 การจำแนกกรุปวัฏจักร

ในบทที่ 3 เราได้แนะนำกรุปวัฏจักรว่าเป็นกรุปที่มีตัวก่อกำเนิด 1 ตัวเขียนได้ในรูป <a> นั่นคือกรุปซึ่งทุกๆ สมาชิกเขียนได้ในรูปกำลังต่างๆ ของ a และได้พิสูจน์ว่ากรุปวัฏจักรเป็นกรุปอาบีเลียน และทุกๆ กรุปย่อยของกรุปวัฏจักรเป็นกรุปวัฏจักร ในหัวข้อนี้เราจะประยุกต์สมสัณฐานเพื่อแสดงกรุปวัฏจักรทั้งหมด ดังนั้นอย่างแรกเราจึงต้องหาตัวอย่างของกรุปวัฏจักรทั้งอันดับจำกัดและอันดับอนันต์เสียก่อน

เราได้ยกตัวอย่างในบทที่ 3 ว่ากรุปของจำนวนเต็มทั้งหมด Z ก่อกำเนิดโดย 1 นั่นคือ Z = <1> กรุปของจำนวนเต็มคู่ทั้งหมด $Z^e$ ก่อกำเนิดโดย 2 นั่นคือ Z = <2> และทุกๆ กรุปย่อยของ Z เขียนได้ในรูป <n> เมื่อ n เป็นจำนวนเต็ม จึงกล่าวได้ว่ากรุป Z และทุกๆ กรุปย่อยของ Z เป็นตัวอย่างของกรุปวัฏจักรอันดับอนันต์ นอกจากนี้บทแทรก 3.4.13 ยังกล่าวว่า "มีกรุปวัฏจักรอันดับ n สำหรับทุกๆ จำนวนเต็มบวก n" โดยยกตัวอย่างกรุปวัฏจักร $Z_n$ เมื่อ n เป็นจำนวนเต็มบวกซึ่งแสดงว่า $Z_n$ เมื่อ n เป็นจำนวนเต็มบวก เป็นตัวอย่างของกรุปวัฏจักรอันดับจำกัด

ต่อไปถ้า n เป็นจำนวนเต็มบวกและ G เป็นกรุปวัฏจักรอันดับ n แล้วจะมี $a \in G$ ซึ่ง $G = \langle a \rangle = \{e, a, a^2, \ldots, a^n\}$ ซึ่งเมื่อเปรียบเทียบกับกรุป $Z_n$ เราก็จะเห็นความเป็นสมนัยหนึ่งต่อหนึ่งของสมาชิกในทั้งสองกรุปดังต่อไปนี้

$$\begin{array}{rcl} \langle a \rangle = & \{a^0, & a^1, & a^2, & \ldots, & a^{n-1}\} \\ & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ Z_n = & \{0, & 1, & 2, & \ldots, & n-1\} \end{array}$$

นอกจากนี้การสมนัยหนึ่งต่อหนึ่งดังกล่าวยังยืนยงการดำเนินการบวกของสมาชิกใน $Z_n$ และการดำเนินการของ G ทฤษฎีบทแรกของหัวข้อนี้ เราจึงจะพิสูจน์ว่า ภายใต้การเป็นสมสัณฐาน จะมีเพียง $Z_n$ ที่เป็นกรุปวัฏจักรอันดับ n สำหรับแต่ละจำนวนเต็มบวก n

6.2.1 **ทฤษฎีบท** ให้ n เป็นจำนวนเต็มบวก แล้ว G เป็นกรุปวัฏจักรอันดับ n ก็ต่อเมื่อ $G \cong Z_n$

**บทพิสูจน์** ให้ n เป็นจำนวนเต็มบวกและให้ G เป็นกรุปวัฏจักรอันดับ n แล้วจะมี $a \in G$ ซึ่ง

$G = \langle a \rangle = \{e, a, a^2, \ldots, a^n\}$

ให้ $f : Z_n \rightarrow G$ กำหนดโดย $f(\bar{k}) = a^k$ สำหรับทุกๆ $\bar{k} \in Z_n$ แล้วเพราะ $e, a, a^2, \ldots, a^n$ เป็นสมาชิกที่ต่างกันทั้งหมดและโดยบทแทรก 3.4.9 ข้อ 4 จะได้ว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง และ

ถ้า $\bar{r}$ และ $\bar{s}$ เป็นสมาชิกของ $Z_n$ แล้ว $f(\bar{r} \oplus \bar{s}) = a^{r+s} = a^r a^s = f(\bar{r})f(\bar{s})$ เพราะฉะนั้น f เป็นสมสัณฐาน

สำหรับบทกลับ เราเห็นได้ชัดโดยความหมายของสมสัณฐานและ $Z_n$ เป็นกรุปวัฏจักรอันดับ n เราจึงได้ว่า G เป็นกรุปวัฏจักรอันดับ n ❐

ในทำนองเดียวกันถ้า G เป็นกรุปวัฏจักรอันดับอนันต์แล้วจะมี $a \in G$ ซึ่ง

$$G = \langle a \rangle = \{ \ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots \}$$

และเมื่อเปรียบเทียบกับกรุป Z เราก็จะเห็นความเป็นสมนัยหนึ่งต่อหนึ่งของสมาชิกในทั้งสองกรุปทำนอง เดียวกันดังต่อ ไปนี้

$$\begin{array}{lcccccccc} \langle a \rangle = & \{\ldots, & a^{-2}, & a^{-1}, & a^{0}, & a^{1}, & a^{2}, & \ldots\} \\ & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ Z_n = & \{\ldots & -2, & -1, & 0, & 1, & 2, & \ldots\} \end{array}$$

แล้วเห็นได้ชัดเช่นเดียวกันว่า $f : Z \rightarrow G$ ซึ่งกำหนดโดย $f(k) = a^k$ สำหรับทุกๆ $k \in Z_n$ เป็นสมสัณฐาน เราจึงได้ทฤษฎีบทการจำแนกกรุปวัฏจักรอันดับอนันต์ต่อไปนี้

6.2.2 **ทฤษฎีบท** G เป็นกรุปวัฏจักรอันดับอนันต์ ก็ต่อเมื่อ $G \cong Z$ ❐

และโดยทฤษฎีบท 6.1.4 เราจะได้บทแทรกต่อไปนี้

6.2.3 **บทแทรก** ทุกๆ กรุปวัฏจักรอันดับเดียวกันจะสมสัณฐานกัน ❐

## แบบฝึกหัด 6.2

1. จงพิสูจน์ทฤษฎีบท 6.2.2 และบทแทรก 6.2.3
2. จงแจกแจงสมาชิกทั้งหมดของกรุปวัฏจักร $\langle 6 \rangle$ และ $Z_{16}$
3. จงแจกแจงสมาชิกทั้งหมดของกรุปวัฏจักร $\langle f \rangle$ ใน $S_6$ เมื่อ

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

4. จงแจกแจงสมาชิกของกรุปย่อยวัฏจักร $<\frac{1}{2}>$ ของ $R^*$ และกรุปย่อยวัฏจักร $<\frac{1}{2}>$ ของ R
5. จงแสดงว่า $R^*$ เป็นกรุปวัฏจักรหรือไม่ [ข้อแนะนำ : สมมติว่ามีจำนวนจริง k ซึ่ง $R^* = <k>$ แล้วจะได้ $k > k^2 > k^3 > \ldots$ ถ้า $k > 1$ และ $k < k^2 < k^3 < \ldots$ ถ้า $k < 1$ แล้วพิจารณา $k+1$ และ $k-1$ ]
6. ให้ G และ H เป็นกรุป จงพิสูจน์ว่าถ้า $G \times H$ เป็นกรุปวัฏจักรแล้ว G และ H ต่างเป็นกรุปวัฏจักร แต่บทกลับไม่เป็นจริง
7. ให้ G และ H เป็นกรุป $a \in G$ และ $b \in H$ จงแสดงว่า
   7.1 $|(a,b)|$ สำหรับ $(a, b) \in G \times H$ เท่ากับตัวคูณร่วมน้อยของ $|a|$ และ $|b|$
   7.2 ถ้า $(a, b) \in G \times H$ และ $(|a|, |b|) = 1$ แล้ว $|(a,b)| = |a|\,|b|$
   7.3 ถ้า $G = <a>$ เป็นกรุปวัฏจักรอันดับ mn โดยที่ $(m, n) = 1$ แล้ว $G \cong <a^m> \times <a^n>$

## 6.3 ทฤษฎีบทของเคย์เลย์

ในหัวข้อ 6.2 เราได้แสดงให้เห็นแล้วว่า กรุปวัฏจักรไม่ใช่กรุปนามธรรมภายใต้การเป็นสมสัณฐาน หรือกล่าวอีกนัยหนึ่งได้ว่า แม้จะกำหนดกรุปวัฏจักรนามธรรม เราก็จะทราบโครงสร้างของกรุปนั้น ในสมัยเมื่อเริ่มต้นกำเนิดทฤษฎีกรุปนั้น ได้นิยามว่า กรุปก็คือกรุปของวิธีเรียงสับเปลี่ยน และได้มีการศึกษาสมบัติของกรุปเหล่านั้นกันมาอย่างยาวนาน จนทำให้เรารู้จักกรุปของวิธีเรียงสับเปลี่ยนกันเป็นอย่างดี และต่อมาเมื่อขยายนิยามกรุปในเชิงนามธรรมมากขึ้น เราก็ยังต้องการเห็นตัวอย่างของกรุปนามธรรมเหล่านั้น เพื่อให้เข้าใจโครงสร้างของกรุปนามธรรมเหล่านั้น จนกระทั่งเมื่อประมาณ100 ปีที่แล้ว นักคณิตศาสตร์ชาวอังกฤษ ที่มีชื่อว่า อาร์เทอร์ เคย์เลย์ (Arthur Cayley) ได้พิสูจน์ทฤษฎีบทตัวแทนของกรุปนามธรรมทั้งหลายว่า "ทุกๆ กรุปจะสมสมสัณฐานกับกรุปของวิธีเรียงสับเปลี่ยน" ทำให้เห็นว่าแม้จะนิยามกรุปเชิงนามธรรมอย่างไร กรุปทั้งหมดก็คือกรุปของวิธีเรียงสับเปลี่ยน ดังที่ศึกษากันมาแต่เดิม ทำให้สมบัติต่างๆของกรุปที่ศึกษากันมาอย่างยาวนานก็จะเป็นสมบัติของกรุปนามธรรมด้วย

ในหัวข้อนี้ เราจะแสดงการพิสูจน์ทฤษฎีบทของเคย์เลย์ และแสดงตัวอย่างการประยุกต์ทฤษฎีบทของเคย์เลย์ ในการหากรุปของวิธีเรียงสับเปลี่ยนซึ่งเป็นตัวแทนของกรุปที่กำหนด

6.3.1 **ทฤษฎีบทของเคย์เลย์ (Cayley's Theorem)** สำหรับแต่ละกรุป G จะมีกรุปย่อย A ของกรุปสมมาตร L(G) ซึ่ง $G \cong A$

**บทพิสูจน์** ให้ G เป็นกรุป แล้วเราต้องการหา A ซึ่งเป็นกรุปย่อยของ L(G) ซึ่ง $G \cong A$ ดังนั้นขนาดของ A จะต้องสมนัยหนึ่งต่อหนึ่งกับ G และสมาชิกของ A ต้องเป็นวิธีเรียงสับเปลี่ยนบน G นั่นคือ สำหรับแต่ละ $a \in G$ เราต้องสร้างฟังก์ชัน (ซึ่งขึ้นกับ a) จาก G ไปยัง G ให้เป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง และเคย์เลย์ให้สัญลักษณ์ $\pi_a$ แทนฟังก์ชันที่จะสร้างซึ่งขึ้นกับ a ดังกล่าว และนิยามโดย $\pi_a(x) = ax$ สำหรับทุกๆ $x \in G$ นั่นคือ

1. สำหรับแต่ละ $a \in G$ ให้ $\pi_a : G \longrightarrow G$ นิยามโดย $\pi_a(x) = ax$ สำหรับทุกๆ $x \in G$ แล้วจะแสดงว่า $\pi_a \in L(G)$

1.1 $\pi_a$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง : ให้ $x_1, x_2 \in G$ โดยที่ $\pi_a(x_1) = \pi_a(x_2)$ แล้วโดยนิยามของ $\pi_a$ จะได้ $ax_1 = ax_2$ ซึ่งทำให้ได้โดยกฎการตัดออกในกรุปว่า $x_1 = x_2$

1.2 $\pi_a$ เป็นฟังก์ชันทั่วถึง : ให้ $y \in G$ แล้ว $y = ey = (aa^{-1})y = a(a^{-1}y)$ และเพราะ $a^{-1}y \in G$ ดังนั้นมี $x = a^{-1}y \in G$ ซึ่ง $\pi_a(x) = ax = a(a^{-1}y) = (aa^{-1})y = ey = y$

เมื่อทราบว่า $\pi_a \in L(G)$ สำหรับทุกๆ $a \in G$ เราจึงให้ $A = \{\pi_a \mid a \in G\}$ แล้วจะแสดงก่อนว่า A เป็นกรุปย่อยของ L(G)

2. จะแสดงว่า A เป็นกรุปย่อยของ L(G)

2.1 จะแสดงอย่างแรกว่า $\pi_a \circ \pi_b$ และ $\pi_{ab}$ เป็นฟังก์ชันเดียวกัน สำหรับทุกๆ $a, b \in G$

ให้ $a, b \in G$ และให้ $x \in G$ แล้ว $(\pi_a \circ \pi_b)(x) = \pi_a(\pi_b(x)) = \pi_a(bx) = a(bx) = (ab)x = \pi_{ab}(x)$ เพราะฉะนั้น $\pi_a \circ \pi_b = \pi_{ab} \in L(G)$ ซึ่งแสดงว่าเซต A มีสมบัติปิดภายใต้การคูณของ L(G)

2.2 อย่างที่สองจะแสดงว่า $\pi_e \in A$ เป็นเอกลักษณ์ของ L(G) โดยให้ $x \in G$ แล้ว $\pi_e(x) = ex = x$ เพราะฉะนั้น $\pi_e$ เป็นเอกลักษณ์ของ L(G) ดังต้องการ

2.3 อย่างที่สามจะแสดงว่า $\pi_a^{-1} = \pi_{a^{-1}}$ สำหรับทุกๆ $a \in G$ โดยให้ $a \in G$ แล้วโดย 2.1 ข้างต้นจะได้ว่า $\pi_a \circ \pi_{a^{-1}} = \pi_{aa^{-1}} = \pi_e$ ดังนั้น $\pi_{a^{-1}}$ เป็นตัวผกผันของ $\pi_a$

2.4 อย่างที่สี่ $\pi_a \circ \pi_b^{-1} \in A$ สำหรับทุกๆ a, b∈G โดยให้ a, b∈G แล้วโดยข้อ 2.3 ข้างต้นจะได้ $\pi_b^{-1} = \pi_{b^{-1}}$ ดังนั้น $\pi_a \circ \pi_b^{-1} = \pi_a \circ \pi_{b^{-1}} = \pi_{ab^{-1}} \in A$ แล้วโดยเกณฑ์การตรวจสอบกรุปย่อย จะได้ว่า A เป็นกรุปย่อยของ L(G)

3. จะแสดงว่า A เป็นสมสัณฐานกับ G โดยให้ f : G⟶A นิยามโดย $f(a) = \pi_a$ สำหรับทุกๆ a∈G

3.1 f เป็นฟังก์ชันหนึ่งต่อหนึ่ง : ให้ a, b∈G โดยที่ f(a) = f(b) แล้วโดยนิยามของ f จะได้ $\pi_a = \pi_b$ นั่นคือ $\pi_a(x) = \pi_b(x)$ สำหรับทุกๆ x∈G และเพราะ e∈G ดังนั้น $\pi_a(e) = \pi_b(e)$ จึงได้ $a = \pi_a(e) = \pi_b(e) = b$

3.2 f เป็นฟังก์ชันทั่วถึง : ให้ $\pi \in A$ แล้วโดยนิยามของ A จะมี a∈G ซึ่ง $\pi = \pi_a$

3.3 ให้ a, b∈G แล้ว $f(ab) = \pi_{ab} = \pi_a \circ \pi_b = f(a)\, f(b)$

เพราะฉะนั้น f เป็นสมสัณฐาน ซึ่งเป็นอันจบการพิสูจน์ ❐

6.3.2 **บทแทรก** ถ้า G เป็นกรุปจำกัด แล้วจะมีจำนวนเต็มบวก n ซึ่ง G เป็นสมสัณฐานกับกรุปย่อยของ $S_n$

**บทพิสูจน์** ให้ n = |G| และ $L(G) = S_n$ แล้วดำเนินการพิสูจน์เช่นเดียวกับทฤษฎีบทของเคย์เลย์ ❐

6.3.3 **ตัวอย่าง** เราจะแสดงว่ากรุปไคลน์ -4 $K_4 = \{e, a, b, c\}$ ซึ่งมีตารางการคูณแสดงดังตารางข้างล่างนี้ เป็นสมสัณฐานกับกรุปย่อยของกรุปสมมาตร $S_4$

| • | E | a | b | c |
|---|---|---|---|---|
| e | E | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

เราจะสร้างกรุปย่อย A ของ $S_4$ โดยดำเนินการเช่นเดียวกับการสร้างในบทพิสูจน์ของทฤษฎีบทของเคย์เลย์ นั่นคือแต่ละ $x \in K_4$ เราสร้าง $\pi_x : K_4 \longrightarrow K_4$ ด้วยการคูณทางซ้ายด้วย x กับทุกสมาชิกในโดเมน ซึ่งจะทำให้ได้

$$\pi_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} = \iota_{K_4}, \qquad \pi_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} = (e\ a)(b\ c)$$

$$\pi_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} = (e\ b)(a\ c), \quad \pi_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} = (e\ c)(a\ b)$$

โดยผลการพิสูจน์ของทฤษฎีบทของเคย์เลย์ จะได้ว่า $A = \{\pi_e, \pi_a, \pi_b, \pi_c\}$ เป็นกรุปย่อยของ $S_4$ ซึ่งสมสัณฐานกับ $K_4$ แต่

$\{\pi_e, \pi_a, \pi_b, \pi_c\} = \{\iota_{K_4}, (e\ a)(b\ c), (e\ b)(a\ c), (e\ c)(a\ b)\}$

สมสัณฐานกับกรุปย่อย $\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ ของ $S_4$ ดังนั้น

$K_4 \cong \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ ❍

6.3.4 **ตัวอย่าง** พิจารณากรุปของเซตกำลัง $P(\{a, b, c\})$ ภายใต้การดำเนินการผลต่างสมมาตร (ดังกล่าวไว้ในตัวอย่าง 3.1.3) และเราต้องการหา n และกรุปย่อย H ของ $S_n$ ซึ่ง $H \cong P(\{a, b, c\})$

โดยทฤษฎีบทของเคย์เลย์ เราจะทราบว่า n คือขนาดของกรุป $P(\{a, b, c\})$ ซึ่งเท่ากับ $2^3 = 8$ ดังนั้นเราจะหากรุปย่อย H ของ $S_8$ ซึ่ง $H \cong P(\{a, b, c\})$

ให้ $G = P(\{a, b, c\}) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ แล้วโดยดำเนินการเช่นเดียวกับการสร้างในบทพิสูจน์ของทฤษฎีบทของเคย์เลย์ เราจะได้

$$\pi_\phi = \iota_G,$$

$$\pi_{\{a\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{a\} & \phi & \{a,b\} & \{a,c\} & \{b\} & \{c\} & \{a,b,c\} & \{b,c\} \end{pmatrix},$$

$$\pi_{\{b\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{b\} & \{a,b\} & \phi & \{b,c\} & \{a\} & \{a,b,c\} & \{c\} & \{a,c\} \end{pmatrix}$$

$$\pi_{\{c\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{c\} & \{a,c\} & \{b,c\} & \phi & \{a,b,c\} & \{a\} & \{b\} & \{a,b\} \end{pmatrix},$$

$$\pi_{\{a,b\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{a,b\} & \{b\} & \{a\} & \{a,b,c\} & \phi & \{b,c\} & \{a,c\} & \{c\} \end{pmatrix},$$

$$\pi_{\{a,c\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{a,c\} & \{c\} & \{a,b,c\} & \{a\} & \{b,c\} & \phi & \{a,b\} & \{b\} \end{pmatrix},$$

$$\pi_{\{b,c\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{b,c\} & \{a,b,c\} & \{c\} & \{b\} & \{a,c\} & \{a,b\} & \phi & \{a\} \end{pmatrix},$$

$$\pi_{\{a,b,c\}} = \begin{pmatrix} \phi & \{a\} & \{b\} & \{c\} & \{a,b\} & \{a,c\} & \{b,c\} & \{a,b,c\} \\ \{a,b,c\} & \{b,c\} & \{a,c\} & \{a,b\} & \{c\} & \{b\} & \{a\} & \phi \end{pmatrix}$$

ถ้าเราแทน $\phi \leftrightarrow 1$, $\{a\} \leftrightarrow 2$, $\{b\} \leftrightarrow 3$, $\{c\} \leftrightarrow 4$, $\{a, b\} \leftrightarrow 5$, $\{a, c\} \leftrightarrow 6$, $\{b, c\} \leftrightarrow 7$ และ $\{a, b, c\} \leftrightarrow 8$ เราจะได้

$$\pi_{\phi} = \iota_G = (1),$$

$$\pi_{\{a\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 6 & 3 & 4 & 8 & 7 \end{pmatrix} = (1\ 2)(3\ 5)(4\ 6)(7\ 8),$$

$$\pi_{\{b\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 1 & 7 & 2 & 8 & 4 & 6 \end{pmatrix} = (1\ 3)(2\ 5)(4\ 7)(6\ 8),$$

$$\pi_{\{c\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 7 & 1 & 8 & 2 & 3 & 5 \end{pmatrix} = (1\ 4)(2\ 6)(3\ 7)(5\ 8),$$

$$\pi_{\{a,b\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 8 & 1 & 7 & 6 & 4 \end{pmatrix} = (1\ 5)(2\ 3)(4\ 8)(6\ 7),$$

$$\pi_{\{a,c\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 8 & 2 & 7 & 1 & 5 & 3 \end{pmatrix} = (1\ 6)(2\ 4)(3\ 8)(5\ 7),$$

$$\pi_{\{b,c\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix} = (1\ 7)(2\ 8)(3\ 4)(5\ 6),$$

และ $\pi_{\{a,b,c\}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 8)(2\ 7)(3\ 6)(4\ 5)$

ดังนั้นกรุปย่อย H ของ $S_8$ ซึ่ง $H \cong P(\{a, b, c\})$ คือ

$$H = \{\pi_\phi, \pi_{\{a\}}, \pi_{\{b\}}, \pi_{\{c\}}, \pi_{\{a,b\}}, \pi_{\{a,c\}}, \pi_{\{b,c\}}, \pi_{\{a,b,c\}}\}$$
$$= \{(1), (1\ 2)(3\ 5)(4\ 6)(7\ 8), (1\ 3)(2\ 5)(4\ 7)(6\ 8), (1\ 4)(2\ 6)(3\ 7)(5\ 8), (1\ 5)(2\ 3)(4\ 8)(6\ 7),$$
$$(1\ 6)(2\ 4)(3\ 8)(5\ 7), (1\ 7)(2\ 8)(3\ 4)(5\ 6), (1\ 8)(2\ 7)(3\ 6)(4\ 5)\}$$

และเราสังเกตว่าทุกๆ สมาชิกของ H มีอันดับ 2 เราจึงสามารถพิสูจน์ได้ไม่ยากว่า H สมสัณฐานกับกรุป $Z_2 \times Z_2 \times Z_2$ ❍

## แบบฝึกหัด 6.3

1. ในการพิสูจน์ทฤษฎีบทของเคย์เลย์ เราจับคู่สำหรับสมาชิก a ในกรุป G ด้วยวิธีเรียงสับเปลี่ยน $\pi_a$ บน G ซึ่งนิยามโดย $\pi_a(x) = ax$ สำหรับทุกๆ $x \in G$ นั่นคือกำหนดด้วยกฎการคูณทางซ้ายกับทุกๆ สมาชิกของ G ด้วย a ซึ่งเราจะเรียก $A = \{\pi_a \mid a \in G\}$ ว่า "*การแทนทางซ้าย (the left representation)* ของ G"

   ในทำนองเดียวกันเราอาจกำหนดเซตของวิธีเรียงสับเปลี่ยน $\pi_a$ บน G ซึ่งนิยามโดย $\rho_a(x) = xa$ สำหรับทุกๆ $x \in G$ นั่นคือกำหนดด้วยกฎการคูณทางขวากับทุกๆ สมาชิกของ G ด้วย a ซึ่งเราจะเรียก $A^* = \{\rho_a \mid a \in G\}$ ว่า "*การแทนทางขวา (the right representation)* ของ G" และขอให้สังเกตว่าสำหรับกรุปอาบีเลียน การแทนทั้งสองเป็นการแทนเดียวกัน

   จงพิสูจน์ทฤษฎีบทของเคย์เลย์ด้วยการแทนทางขวา

2. จงหาการแทนทางซ้ายและการแทนทางขวาของกรุปในข้อต่อไปนี้

   2.1 กรุป $Z_3$, $Z_4$, $Z_6$ และ $Z_2 \times S_3$

   2.2 กรุป $P_2$ ของเซตย่อยทั้งหมดบนเซต 2 สมาชิก (การดำเนินการเป็นดังนิยามไว้ในตัวอย่าง 3.1.3)

2.3 กรุป G ซึ่งประกอบด้วยเมทริกซ์ 6 ตัวคือ $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$,

$B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $C = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$, $D = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ และ $K = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

ซึ่งมีตารางการคูณดังนี้

| | I | A | B | C | D | K |
|---|---|---|---|---|---|---|
| I | I | A | B | C | D | K |
| A | A | I | C | B | K | D |
| B | B | K | D | A | I | C |
| C | C | D | K | I | A | B |
| D | D | C | I | K | B | A |
| K | K | B | A | D | C | I |

3. จงพิสูจน์ว่ากรุป H ในตัวอย่าง 3.3.4 สมสัณฐานกับกรุป $Z_2 \times Z_2 \times Z_2$
4. จงบอกจำนวนเต็มบวก n และแสดงการหากรุปย่อยของ $S_n$ ซึ่งสมสัณฐานกับกรุปในข้อต่อไปนี้

   4.1 $Z_7^{\cdot}$ (นั่นคือกรุป $Z_7^* - \{\overline{0}\}$)  4.2 $Z_2 \times S_3$

## 6.4 กรุปอัตสัณฐาน

สมสัณฐานชนิดสำคัญและเป็นประโยชน์ต่อการศึกษาพีชคณิตนามธรรมคืออัตสัณฐาน ซึ่งเป็นสมสัณฐานจากกรุปหนึ่งไปยังกรุปนั้นเอง เราเห็นได้ชัดว่าฟังก์ชันเอกลักษณ์เป็นตัวอย่างของอัตสัณฐานบนกรุปใดๆ อย่างไรก็ตามตัวอย่าง 5.1.3 ได้แสดงให้เห็นว่าในบางกรุปอาจมีอัตสัณฐานบนกรุปที่ไม่ใช่ฟังก์ชันเอกลักษณ์ และอาจมีอัตสัณฐานเหล่านี้ได้มากกว่าหนึ่งฟังก์ชัน นอกจากนี้อัตสัณฐานบนกรุปใดๆ จะเป็นวิธีเรียงสับเปลี่ยนบนกรุปนั้น แต่เป็นที่ทราบกันดีว่า ไม่ใช่ทุกๆ วิธีเรียงสับเปลี่ยนจะเป็นอัตสัณฐาน ดังนั้นเซตของอัตสัณฐานทั้งหมดบนกรุปๆ หนึ่ง จึงไม่เป็นกรุปสมมาตรบนกรุปนั้น เราอาจตั้งคำถามว่าเซตของอัตสัณฐานทั้งหมดบนกรุปๆ หนึ่ง จะเป็นกรุปหรือไม่ และจะเป็นกรุปย่อยของกรุปสมมาตรบนกรุปนั้นหรือไม่ ในหัวข้อนี้เราจะพิสูจน์ว่าเซตของอัตสัณฐาน

ทั้งหมดบนกรุปๆ หนึ่งจะกรุปย่อยของกรุปสมมาตรบนกรุปนั้น และจะแนะนำหมู่พิเศษของอัตสัณฐานบนกรุปซึ่งเป็นประโยชน์ต่อการศึกษาพีชคณิตนามธรรม

6.4.1 **บทนิยาม** ให้ G เป็นกรุป ถ้า $\theta : G \longrightarrow G$ เป็นสมสัณฐาน เราจะเรียก $\theta$ ว่า *อัตสัณฐาน (automorphism)* บน G และใช้สัญลักษณ์ A(G) แทนเซตของอัตสัณฐานทั้งหมดบน G

เพราะว่าฟังก์ชันเอกลักษณ์ $\iota_G$ เป็นอัตสัณฐานบน G ดังนั้น $A(G) \neq \phi$ และเห็นได้ชัดว่าฟังก์ชันประกอบของทุกๆ คู่อัตสัณฐานบน G เป็นอัตสัณฐานบน G และแต่ละอัตสัณฐานบน G มีฟังก์ชันผกผันเป็นอัตสัณฐานบน G จึงทำให้ได้ว่า A(G) เป็นกรุปย่อยของ L(G)

6.4.2 **ทฤษฎีบท** A(G) เป็นกรุปย่อยของ L(G) ❐

6.4.3 **ทฤษฎีบท** ให้ G เป็นกรุปและสำหรับแต่ละ $a \in G$ นิยาม $T_a : G \longrightarrow G$ โดย $T_a(x) = axa^{-1}$ สำหรับทุกๆ $a \in G$ แล้ว $T_a$ เป็นอัตสัณฐานบน G สำหรับทุกๆ $a \in G$

**บทพิสูจน์** ให้ $a \in G$

1. $T_a$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง : ให้ $x, y \in G$ ซึ่ง $T_a(x) = T_a(y)$ แล้ว $axa^{-1} = aya^{-1}$ ทำให้ได้ $x = exe = (a^{-1}a)x(a^{-1}a) = a^{-1}(axa^{-1})a = a^{-1}(aya^{-1})a = (a^{-1}a)y(a^{-1}a) = eye = y$
2. $T_a$ เป็นฟังก์ชันทั่วถึง : ให้ $y \in G$ แล้ว $y = eye = (aa^{-1})y(aa^{-1}) = a(a^{-1}ya)a^{-1}$ ดังนั้นเลือก $x = a^{-1}ya \in G$ จะทำให้ได้ $T_a(x) = axa^{-1} = a(a^{-1}ya)a^{-1} = y$
3. $T_a$ เป็นสมสัณฐาน : ให้ $x, y \in G$ แล้ว $T_a(xy) = axya^{-1} = axeya^{-1} = (axa^{-1})(aya^{-1}) = T_a(x)T_a(y)$ ❐

สังเกตว่าถ้า $|G| = 2$ แล้วเพราะอัตสัณฐานต้องเป็นฟังก์ชันหนึ่งต่อหนึ่งซึ่งส่งเอกลักษณ์ของกรุปไปยังเอกลักษณ์ ดังนั้นอัตสัณฐานจึงมีเพียงฟังก์ชันเอกลักษณ์จึงทำให้ได้ $A(G) = \{\iota_G\}$ นั่นคือ $|A(G)| = 1$ และถ้า G เป็นกรุปอาบีเลียนแล้วอัตสัณฐาน $T_a$ ซึ่งนิยามดังในทฤษฎีบท 5.4.3 จะเป็นฟังก์ชันเอกลักษณ์สำหรับทุกๆ $a \in G$ แต่ถ้า G เป็นกรุปอาบีเลียนที่มี $a \in G$ ซึ่ง $a \neq a^{-1}$ และกำหนด $T : G \longrightarrow G$ โดย $T(x) = x^{-1}$ สำหรับทุกๆ $x \in G$ แล้ว T จะเป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง นอกจากนี้ถ้า

$x, y \in G$ แล้ว $T(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = T(x)T(y)$ ทำให้ได้ว่า T เป็นอัตสัณฐานซึ่ง $T \neq T_a$ สำหรับทุกๆ $a \in G$ แสดงว่าโดยทั่วไป $|A(G)| > 1$ และอัตสัณฐานอาจไม่ได้อยู่ในรูปแบบ $T_a$

6.4.4 **บทนิยาม** ให้ G เป็นกรุป เราเรียกอัตสัณฐานที่นิยามดังในทฤษฎีบท 5.4.3 ว่า *อัตสัณฐานภายใน (inner automorphism)* และใช้สัญลักษณ์ $\mathrm{I}(G)$ แทนเซตของอัตสัณฐานภายในทั้งหมดของ G

เรียกอัตสัณฐานที่ไม่ใช่อัตสัณฐานภายในว่า *อัตสัณฐานภายนอก(outer automorphism)*

6.4.5 **ทฤษฎีบท** ให้ G เป็นกรุป แล้ว $\mathrm{I}(G)$ เป็นกรุปย่อยปรกติของ A(G)

**บทพิสูจน์** ให้ $a, b, x \in G$ แล้ว $(T_aT_b)(x) = T_a(T_b(x)) = T_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(a^{-1}b^{-1}) = (ab)x(ab)^{-1} = T_{ab}(x)$ ดังนั้น $T_aT_b = T_{ab} \in \mathrm{I}(G)$ ซึ่งทำให้ได้ $T_aT_{a^{-1}} = T_{aa^{-1}} = T_e = \iota_G$ ซึ่งแสดงว่า $T_a^{-1} = T_{a^{-1}} \in \mathrm{I}(G)$ เพราะฉะนั้น $T_aT_b^{-1} = T_aT_{b^{-1}} = T_{ab^{-1}} \in \mathrm{I}(G)$ ทำให้ได้โดยเกณฑ์การตรวจสอบกรุปย่อยว่า $\mathrm{I}(G)$ เป็นกรุปย่อยของ Aut(G)

ต่อไปให้ $a \in G$ และ $\tau \in \mathrm{Aut}(G)$ แล้วจะแสดงว่า $\tau T_a \tau^{-1} \in \mathrm{I}(G)$ โดยให้ $x \in G$ แล้ว

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

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

ซึ่งแสดงว่า $\tau T_a \tau^{-1} = T_{\tau(a)} \in \mathrm{I}(G)$ ดังนั้น $\mathrm{I}(G)$ เป็นกรุปย่อยปรกติของ A(G) ❐

6.4.6 **บทนิยาม** ให้ G เป็นกรุปและ $a, b, x \in G$ เราเรียกสมาชิก $xax^{-1}$ ใน G ว่า *สังยุค (conjugate)* ของ a และถ้ามี $y \in G$ ซึ่ง $b = yay^{-1}$ จะกล่าวว่า a และ b เป็น *คู่สังยุค (conjugacy pair))*

ถ้า $a \in G$ เป็นคู่สังยุคของตัวเองเท่านั้น เราจะได้ว่า $a = xax^{-1}$ สำหรับทุกๆ $x \in G$ ซึ่งสมมูลกับ $ax = xa$ สำหรับทุกๆ $x \in G$ นั่นคือ a สลับที่ได้กับทุกๆ สมาชิกของ G เราจะเรียกสมาชิกของ G ซึ่งเป็นคู่สังยุคของตัวเองเท่านั้นว่า *สมาชิกเชิงศูนย์กลาง (central element)* และให้ C(G) แทนเซตของสมาชิกเชิงศูนย์กลางทั้งหมดใน G โดยเรียก C(G) ว่า *ศูนย์กลาง (center)* ของ G

ขอให้สังเกตโดยนิยามของเซตศูนย์กลางของ G ว่า ถ้า $x \in G$ และ $a \in \mathbf{C}(G)$ แล้ว $xax^{-1} = axx^{-1} = a \in C(G)$ ทำให้เห็นได้ชัดว่า $\mathbf{C}(G)$ เป็นกรุปย่อยปรกติของ G ยิ่งไปกว่านั้นสำหรับทุกๆ $x \in G$ เราจะได้ว่า $x\mathbf{C}(G)x^{-1} = \mathbf{C}(G)$ และถ้าเราเรียกกรุปย่อย N ของ G ซึ่ง $xNx^{-1} = N$ ว่า *กรุปย่อยเชิงศูนย์กลาง (central subgroup)* ใน G แล้วทฤษฎีบทต่อไปจะแสดงว่ากรุปย่อยเชิงศูนย์กลางใน G ไม่ใช่เรื่องใหม่

6.4.7 **ทฤษฎีบท** ให้ G เป็นกรุปแล้ว

1. $\mathbf{C}(G)$ เป็นกรุปย่อยเชิงศูนย์กลางใน G
2. N เป็นกรุปย่อยเชิงศูนย์กลางใน G ก็ต่อเมื่อ N เป็นกรุปย่อยปรกติของ G

**บทพิสูจน์** ข้อ 1 เห็นได้ชัดจึงจะพิสูจน์เฉพาะข้อ 2 ให้ N กรุปย่อยเชิงศูนย์กลางใน G และให้ $n \in N$ และ $a \in G$ แล้วเพราะ $ana^{-1} \in aNa^{-1}$ โดยที่ $aNa^{-1} = N$ ดังนั้น $ana^{-1} \in N$ ซึ่งแสดงว่า N เป็นกรุปย่อยปรกติของ G และในการพิสูจน์บทกลับให้ N เป็นกรุปย่อยปรกติของ G และ $a \in G$ แล้วโดยทฤษฎีบท 5.3.2 เราเหลือเพียงการพิสูจน์ว่า $N \subseteq aNa^{-1}$ ให้ $n \in N$ แล้ว $a^{-1}n \in a^{-1}N$ โดยที่ $a^{-1}N = Na^{-1}$ ดังนั้น $a^{-1}n \in Na^{-1}$ จึงมี $n' \in N$ ซึ่ง $a^{-1}n = n'a^{-1}$ ทำให้ได้ว่า $n = en = aa^{-1}n = an'a^{-1} \in aNa^{-1}$ ซึ่งแสดงว่า $N \subseteq aNa^{-1}$ ตามต้องการ ❐

ขอให้สังเกตจากทฤษฎีบท 6.4.3 ว่าแต่ละอัตสัณฐานภายในจะส่งแต่ละสมาชิกของกรุปไปยังคู่สังยุคในกรุปนั้น ยิ่งไปกว่านั้นถ้าเรากำหนดความสัมพันธ์ในกรุปโดยให้แต่ละคู่สมาชิกที่สัมพันธ์กันต้องเป็นคู่สังยุคกัน แล้วความสัมพันธ์นี้จะเป็นความสัมพันธ์สมมูลซึ่งจะกำหนดผลแบ่งกั้นกรุปที่มีประโยชน์ต่อสาขาวิชาที่ประยุกต์ทฤษฎีบทเชิงการนับ

6.4.8 **ทฤษฎีบท** ให้ G เป็นกรุปและนิยามความสัมพันธ์ $R \subseteq G \times G$ สำหรับทุกๆ $a, b \in G$ โดย

$$aRb \iff a \text{ และ } b \text{ เป็นคู่สังยุค}$$

แล้ว R เป็นความสัมพันธ์สมมูล

**บทพิสูจน์** ถ้า $a \in G$ แล้ว $a = ae = a(aa^{-1}) = aaa^{-1}$ นั่นคือ aRa สำหรับทุกๆ $a \in G$ หรือก็คือ R มีสมบัติสะท้อน

ให้ $a, b \in G$ โดยที่ $aRb$ แล้วจะมี $x \in G$ ซึ่ง $b = xax^{-1}$ ทำให้ได้ $a = eae = (x^{-1}x)a(x^{-1}x) = x^{-1}(xax^{-1})x = x^{-1}bx = x^{-1}b(x^{-1})^{-1}$ นั่นคือมี $y = x^{-1} \in G$ ซึ่ง $a = yby^{-1}$ ซึ่งแสดงว่า $bRa$ เพราะฉะนั้น R มีสมบัติสมมาตร

สุดท้ายให้ $a, b, c \in G$ ซึ่ง $aRb$ และ $bRc$ แล้วจะมี $x,y \in G$ ซึ่ง $b = xax^{-1}$ และ $c = yby^{-1}$ ทำให้ได้ $c = yby^{-1} = y(xax^{-1})y^{-1} = (yx)a(x^{-1}y^{-1}) = (yx)a(yx)^{-1}$ นั่นคือมี $z = yx \in G$ ซึ่ง $a = zcz^{-1}$ ซึ่งแสดงว่า $aRc$ เพราะฉะนั้น R มีสมบัติถ่ายทอด ❐

เราเรียกความสัมพันธ์สมมูลซึ่งนิยามดังในทฤษฎีบท 6.4.8 ว่า "ความสัมพันธ์คู่สังยุค" และเรียกแต่ละเซตสมมูลในผลแบ่งกั้นซึ่งสมนัยกับความสัมพันธ์สมมูลนี้ว่า "*เซตสมมูลสังยุค (conjugate class) ของ G*" เซตสมมูลเหล่านี้ต่างจาก "โคเซต" ที่เป็นเซตสมมูลซึ่งกำหนดโดยความสัมพันธ์มอดูโล H เมื่อ H เป็นกรุปย่อยของ G กล่าวคือขนาดของแต่ละโคเซตในผลแบ่งกั้นจะเท่ากัน ในขณะที่ขนาดของแต่ละเซตสมมูลสังยุคจะไม่เท่ากัน เซตสมมูลของเอกลักษณ์ของ G และของสมาชิกเชิงศูนย์กลางใน G จะประกอบด้วยสมาชิกเพียงหนึ่งเดียว เพราะถ้า $a \in C(G)$ และ $b \in G$ ซึ่ง $a \sim b$ แล้ว b เป็นคู่สังยุคกับ a ดังนั้นจะมี $c \in G$ ซึ่ง $b = cac^{-1}$ แต่โดยนิยามของ a จะได้ว่า $a = xax^{-1}$ สำหรับทุกๆ $x \in G$ ดังนั้น $b = cac^{-1} = a$ และสำหรับเซตสมมูลสังยุคของสมาชิกที่ไม่ใช่สมาชิกเชิงศูนย์กลางใน G จะประกอบด้วยสมาชิกมากกว่า 1 ตัว

สังเกตว่า $\{xax^{-1} \mid x \in G\}$ เป็นเซตสมมูลสังยุคซึ่งมี $a \in G$ เป็นสมาชิกซึ่งเป็นเซตย่อยของ G แต่สำหรับ $a \in G$ และเซตย่อย A ของ G เราจะเรียกเซต

$$C_G(a) = \{x \in G \mid xax^{-1} = a\}$$

ว่า *เซตกำหนดเชิงศูนย์กลาง (centralizer)* ของ a ใน G และเรียกเซต

$$N_G(A) = \{x \in G \mid xAx^{-1} = A\}$$

ว่า *เซตกำหนดปรกติ (normalizer)* ของ A ใน G

ขอให้สังเกตว่า a เป็นสมาชิกเชิงศูนย์กลางใน G ก็ต่อเมื่อ $C_G(a) = G$ และ A เป็นกรุปย่อยปรกติของ G ก็ต่อเมื่อ $N_G(A) = G$

ทฤษฎีบทต่อไปจะแสดงการประยุกต์มโนมติเหล่านี้ กับการนับจำนวนสมาชิกในกรุป

**6.4.9 ทฤษฎีบท** ให้ n เป็นจำนวนเต็มบวก ให้ G เป็นกรุปจำกัดและให้ $\{A_i \mid i = 1, 2, \ldots, n\}$ เป็นผลแบ่งกั้น G ซึ่งกำหนดโดยความสัมพันธ์คู่สังยุคแล้ว $|A_i| = [G : C_G(a)]$ เมื่อ $a \in A_i$ สำหรับแต่ละ $i = 1, 2, \ldots, n$

**บทพิสูจน์** เราเห็นได้ชัดว่า $C_G(a)$ เป็นกรุปย่อยของ G สำหรับทุกๆ $a \in G$ ดังนั้นสำหรับแต่ละ $i = 1, 2, \ldots, n$ และ $a \in A_i$ จะได้ว่า $[G : C_G(a)]$ เป็นดรรชนีของ $C_G(a)$ ใน G ซึ่งก็คือจำนวนโคเซตซ้ายทั้งหมดของ $C_G(a)$ ใน G ในการพิสูจน์ทฤษฎีบทเราจึงจะสร้างฟังก์ชันสมนัยหนึ่งต่อหนึ่งจาก $A_i$ สำหรับแต่ละ $i = 1, 2, \ldots, n$ ไปยังเซตของโคเซตซ้ายทั้งหมดของ $C_G(a)$ ใน G

สำหรับแต่ละ $i = 1, 2, \ldots, n$ ให้ $a \in A_i$ และนิยาม $f : A_i = \{xax^{-1} \mid x \in G\} \rightarrow \{xC_G(a) \mid x \in G\}$ โดย $f(xax^{-1}) = xC_G(a)$ สำหรับทุกๆ $x \in G$

ให้ $x_1, x_2 \in G$ แล้ว $x_1ax_1^{-1} = x_2ax_2^{-1}$ ก็ต่อเมื่อ $a = x_1^{-1}x_2ax_2^{-1}x_1$ ซึ่งก็ต่อเมื่อ $x_1^{-1}x_2 \in C_G(a)$ นั่นคือก็ต่อเมื่อ $x_1C_G(a) = x_2C_G(a)$ ซึ่งแสดงว่า f เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง และโดยนิยามของ f เห็นได้ชัดว่า f เป็นฟังก์ชันทั่วถึง ❐

**6.4.10 บทแทรก** ให้เงื่อนไขของทฤษฎีบท 6.4.9 เป็นจริง แล้ว $|A_i|$ เป็นตัวหารของ $|G|$ สำหรับแต่ละ $i = 1, 2, \ldots, n$

**บทพิสูจน์** เนื่องจาก $G = A_1 \cup A_2 \cup \ldots \cup A_n$ โดยที่ $A_i \cap A_j = \phi$ เมื่อ $i \neq j$ ดังนั้น $|G| = |A_1| + |A_2| + \ldots + |A_n|$ และโดยทฤษฎีบทลากรองจ์ สำหรับแต่ละ $i = 1, 2, \ldots, n$ และ $a \in A_i$ จะได้ว่า $[G : C_G(a)]$ เป็นตัวหารของ $|G|$ ทำให้ได้โดยทฤษฎีบท 6.4.9 ว่า $|A_i|$ เป็นตัวหารของ $|G|$ สำหรับแต่ละ $i = 1, 2, \ldots, n$ ❐

**6.4.11 ทฤษฎีบท** ให้ n เป็นจำนวนเต็มบวกและ p เป็นจำนวนเฉพาะ ถ้า G เป็นกรุปที่มีอันดับ $p^n$ แล้ว $|C(G)| \geq p$

**บทพิสูจน์** ให้ k เป็นจำนวนเต็มบวกและ $\{A_i \mid i = 1, 2, \ldots, k\}$ เป็นผลแบ่งกั้น G ซึ่งกำหนดโดยความสัมพันธ์คู่สังยุค และสำหรับแต่ละ $i = 1, 2, \ldots, k$ ให้ $|A_i| = \alpha_i$ แล้ว

$$p^n = |G| = |A_1| + |A_2| + \ldots + |A_k| = \alpha_1 + \ldots + \alpha_k$$

แต่โดยบทแทรก 6.4.10 จะได้ $\alpha_i$ เป็นตัวหารของ $p^n$ สำหรับแต่ละ $i = 1, 2, \ldots, k$

ถ้า $C(G) = \{e\}$ เมื่อ e เป็นเอกลักษณ์ของ G แล้วจะมี $i \in \{1, 2, \ldots, k\}$ ซึ่ง $A_i = \{e\}$ และ

โดยไม่เสียนัยทั่วไป ขอกำหนดให้ $A_1 = \{e\}$ ดังนั้น $|A_1| = \alpha_1 = 1$ และสำหรับ $i \geq 2$ จะได้ $\alpha_i > 1$ ทำให้ได้ว่า $|A_i|$ เป็นตัวหารของ $p^n$ สำหรับทุกๆ $i \geq 2$ แสดงว่า p เป็นตัวหารของ $\alpha_i$ สำหรับทุกๆ $i \geq 2$ ดังนั้น p จะเป็นตัวหารของ $p^n - (\alpha_2 + \ldots + \alpha_k) = \alpha_1 = 1$ ซึ่งเป็นไปไม่ได้ เพราะฉะนั้น $|C(G)| > 1$ แต่โดยทฤษฎีบทลากรองจ์และ C(G) เป็นกรุปย่อยของ G จะได้ว่า $|C(G)|$ เป็นตัวหารของ $|G| = p^n$ ดังนั้น p จะเป็นตัวหารของ $|C(G)|$ ทำให้ได้ว่า $|C(G)| \geq p$ ❐

6.4.12 **บทแทรก** ให้ p เป็นจำนวนเฉพาะและให้ G เป็นกรุปอันดับ $p^2$ แล้ว G เป็นกรุปอาบีเลียน

**บทพิสูจน์** โดยทฤษฎีบท 6.4.11 จะได้ว่า $|C(G)| \geq p$ สมมติว่า $|C(G)| = p$ แล้ว C(G) เป็นกรุปย่อยแท้ของ G ดังนั้นจะมี $a \in G$ ซึ่ง $a \notin C(G)$ ซึ่งทำให้ได้ $C(G) \subseteq C_G(a)$ และ $a \in C_G(a)$ จึงได้ว่า $|C_G(a)| > p$ แต่ $|C_G(a)|$ เป็นตัวหารของ $p^2$ เพราะ $C_G(a)$ เป็นกรุปย่อยของ G เราจึงสรุปได้ว่า $|C_G(a)| = p^2$ นั่นคือ $C_G(a) = G$ ซึ่งแสดงว่า $ax = xa$ สำหรับทุกๆ สมาชิก x ใน G ทำให้ได้ $a \in C(G)$ เกิดเป็นข้อขัดแย้งกันเอง

ดังนั้น $|C(G)| > p$ ทำให้ได้ว่า $|C(G)|$ เป็นตัวหารของ $p^2$ ซึ่งมากกว่า p ซึ่งแสดงว่า $|C(G)| = p^2$ เพราะฉะนั้น $C_G(a) = G$ ทำให้ได้ว่า G เป็นกรุปอาบีเลียน ❐

## แบบฝึกหัด 6.4

1. จงแสดงว่า G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ $\mathrm{I}(G) = \{\iota_G\}$
2. ให้ G เป็นกรุปและสำหรับแต่ละ $a, b \in G$ นิยาม $\lambda_a : G \to G$ และ $\tau_b : G \to G$ โดย $\lambda_a(x) = ax$ และ $\tau_b(x) = xb$ สำหรับทุกๆ $x \in G$ จงแสดงว่า
   2.1 $\lambda_a$ และ $\tau_b$ ต่างเป็นวิธีเรียงสับเปลี่ยนบน G
   2.2 ถ้า $\theta$ เป็นวิธีเรียงสับเปลี่ยนบน G ซึ่ง $\lambda_a\theta = \theta\lambda_a$ สำหรับทุกๆ $a \in G$ แล้วจะมี $b \in G$ ซึ่ง $\theta = \tau_b$
3. จงหา A(G) และ $\mathrm{I}(G)$ สำหรับกรุป G ต่อไปนี้คือ กรุปไคลน์ $K_4$ กรุป $S_3$ และกรุป $Z_m$ สำหรับแต่ละจำนวนเต็มบวก m
4. สำหรับแต่ละกรุป G จงแสดงว่า $T_a = T_b$ ก็ต่อเมื่อ $a \in bC(G)$ สำหรับทุกๆ $T_a$ และ $T_b$ ใน $\mathrm{I}(G)$

5. ให้ H เป็นกรุปย่อยของกรุป G และสำหรับแต่ละ $a \in G$ นิยามเซต $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ จงแสดงว่า

   5.1 $aHa^{-1}$ เป็นกรุปย่อยของ G สำหรับทุกๆ $a \in G$

   5.2 ถ้า $W = \bigcap_{a \in G} aHa^{-1}$ แล้ว W เป็นกรุปย่อยของ G ซึ่ง $xwx^{-1} \in W$ สำหรับทุกๆ $x \in G$ และทุกๆ $w \in W$

6. จงหาคู่สังยุคใน $S_5$ ซึ่งไม่เป็นคู่สังยุคใน $A_5$

7. จงเขียนผลแบ่งกั้น $A_5$ ซึ่งกำหนดโดยความสัมพันธ์สมมูลที่กำหนดดังในทฤษฎีบท 6.4.8 พร้อมทั้งบอกจำนวนสมาชิกในแต่ละเซตสมมูลที่เป็นสมาชิกในผลแบ่งกั้น

8. จงหา $C_G(a)$ สำหรับ $G = S_n$ เมื่อ $n \geq 4$ และ $a = (1\ 2)(3\ 4)$

9. ให้ A และ B เป็นกรุปย่อยของกรุป G จงแสดงว่าถ้า A เป็นกรุปย่อยปรกติของ B แล้ว $B \subseteq N_G(A)$

# บทที่ 7

# สาทิสสัณฐาน

# HOMOMORPHISM

การศึกษาโครงสร้างพีชคณิตของระบบคณิตศาสตร์ที่มีขนาดใหญ่แต่ซับซ้อนวิธีหนึ่ง คือศึกษาโครงสร้างพีชคณิตของระบบคณิตศาสตร์ที่มีขนาดเล็กกว่าและซับซ้อนน้อยกว่า เพื่อให้เห็นสมบัติที่ต้องการศึกษานั้นชัดเจนขึ้น สาทิสสัณฐานเป็นเครื่องมืออย่างหนึ่งของวิธีการดังกล่าว เพราะสาทิสสัณฐานเป็นฟังก์ชันจากระบบคณิตศาสตร์ระบบหนึ่งไปยังอีกระบบหนึ่งที่มีสมบัติยืนยงหรือไม่แปรเปลี่ยนโครงสร้างของการดำเนินการและไม่จำเป็นต้องเป็นฟังก์ชันหนึ่งต่อหนึ่ง ดังนั้นภาพของสาทิสสัณฐานจะมีขนาดเล็กกว่าหรือเท่ากับโดเมนแต่จะสะท้อนโครงสร้างบางโครงสร้างของโดเมนโดยเฉพาะเมื่อต้องการศึกษาสมบัติใดของกรุปโดเมน เราจะหาภาพสาทิสสัณฐานของโดเมนที่มีสมบัตินั้นๆ และศึกษากับสาทิสสัณฐานแทน ในบทนี้เราจะกล่าวถึงสาทิสสัณฐานระหว่างกรุป สมบัติที่ถ่ายทอดผ่านทางสาทิสสัณฐาน พิสูจน์ทฤษฎีบทหลักมูลของพีชคณิตและทฤษฎีบทสมสัณฐานสามทฤษฎีบท

## 7.1 สาทิสสัณฐาน

เราได้เห็นแล้วว่ากรุปสองกรุปจะสมสัณฐานกันถ้ามีฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึงซึ่งแปลงสมาชิกของกรุปหนึ่งไปทั่วถึงอีกกรุปหนึ่ง ในลักษณะที่ทำให้เห็นว่าโครงสร้างของทั้งสองกรุปเหมือนกัน ซึ่งเราอาจพิจารณาว่าภายใต้การแปลงดังกล่าวจะไม่แปรเปลี่ยนโครงสร้างของกรุปทั้งสอง ดังนั้นสำหรับกรุปสองกรุปใดๆ ที่อาจจะไม่สมสัณฐานกัน เราก็อาจเห็นการแปลงที่ไม่แปรเปลี่ยนโครงสร้างระหว่างกรุปทั้งสองโดยที่การแปลงนั้นอาจไม่เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งหรือเป็นฟังก์ชันทั่วถึง ตัวอย่างเช่นการแปลง $\theta$ จากกรุป $Z_6$ ไปยังกรุป $Z_3$ ซึ่งกำหนดดังนี้

$$\theta = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \overline{0} & \overline{1} & \overline{2} & \overline{0} & \overline{1} & \overline{2} \end{pmatrix}$$

จะเห็นว่า แม้ว่า $\theta$ จะเป็นฟังก์ชันทั่วถึงแต่ก็ไม่ใช่ฟังก์ชันหนึ่งต่อหนึ่ง และถ้าเราเปรียบเทียบตารางการคูณของ $Z_6$ กับภาพของ $Z_6$ ภายใต้ $\theta$ ดังตารางต่อไปนี้

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |

$\xrightarrow[x \text{ ด้วย } f(x)]{\text{แทนที่}}$

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

$\xrightarrow[\text{เช่น } 2+2=1 \text{ ปรากฏ 4 ครั้ง}]{\text{กำจัดตัวซ้ำ}}$

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

เราอาจสังเกตว่าตารางของภาพของ $Z_6$ ภายใต้ $\theta$ จะเป็นตารางการคูณของ $Z_3$ ปรากฏซ้ำ 4 ครั้ง ซึ่งแสดงว่า $\theta$ ยืนยงการดำเนินการของ $Z_6$ และ $Z_3$ ทำให้เห็นว่า $Z_3$ เป็นโครงสร้างบางส่วนของ $Z_6$

โดยทั่วไปถ้า G และ $\overline{G}$ เป็นกรุปและมีฟังก์ชัน $\theta$ ซึ่งแปลง G ไปยัง $\overline{G}$ ในลักษณะยืนยงหรือไม่แปรเปลี่ยนโครงสร้างบางส่วนของ G เราหมายความว่า f ต้องแปลงตารางการคูณของ G ไปยังตารางการคูณของ $\overline{G}$ ในลักษณะที่ถ้า a และ b เป็นสมาชิกใดๆ ใน G ซึ่ง $\theta(a) = a'$ และ $\theta(b) = b'$ แล้ว $\theta(ab) = a'b' = \theta(a)\theta(b)$ ใน $\overline{G}$ เช่นเดียวกับการแปลงของสมสัณฐาน

7.1.1 **บทนิยาม** ให้ G และ $\overline{G}$ เป็นกรุป เรากล่าวว่า $\theta : G \rightarrow \overline{G}$ เป็น *สาทิสสัณฐาน (homomorphism)* ถ้า $\theta(ab) = \theta(a)\theta(b)$ สำหรับทุกๆ $a, b \in G$

สังเกตว่า ab ในสมการ $\theta(ab) = \theta(a)\theta(b)$ เป็นผลคูณของสมาชิกในกรุป G ในขณะที่ $\theta(a)\theta(b)$ เป็นผลคูณของสมาชิกในกรุป $\overline{G}$ ดังนั้นสมการ $\theta(ab) = \theta(a)\theta(b)$ แสดงให้ทราบว่าภาพภายใต้สาทิสสัณฐาน $\theta$ ของผลคูณใน G เป็นผลคูณของภาพภายใต้ $\theta$ ใน $\overline{G}$ เราจึงเรียกสมบัตินี้ของ $\theta$ ว่า "สมบัติยืนยงการดำเนินการ" ความสัมพันธ์ของสาทิสสัณฐาน $\theta$ กับการดำเนินการของ G และ $\overline{G}$ อาจแสดงได้ด้วยแผนภาพต่อไปนี้

$$\begin{tikzcd}
(a,b) \arrow[r, "\cdot"] \arrow[d, "\theta"'] & a\cdot b \arrow[d, "\theta"] \\
(\theta(a),\theta(b) \arrow[r, "\cdot"'] & \theta(a)\theta(b) = \theta(ab)
\end{tikzcd}$$

จากแผนภาพจะเห็นว่า ถ้าเราเริ่มต้นที่คู่อันดับ (a, b) แล้วไม่ว่าเราจะไปทางซ้ายหรือทางขวาของแผนภาพ เราจะไปสิ้นสุดด้วยผลเดียวกันโดยสมบัติยืนยงการดำเนินการ และเราจะเรียกแผนภาพในลักษณะเช่นนี้ว่า *แผนภาพสลับที่ (commutative diagram)*

ขอให้สังเกตว่าทุกๆ สมสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ จะเป็นสาทิสสัณฐาน ดังนั้นทุกๆ ตัวอย่างของสมสัณฐานในบทที่ 6 ก็เป็นตัวอย่างของสาทิสสัณฐาน

ถ้า G และ $\overline{G}$ เป็นกรุปใดๆ ที่มี e และ $\overline{e}$ เป็นเอกลักษณ์ของกรุปตามลำดับ แล้วจะมีฟังก์ชัน $\theta : G \rightarrow \overline{G}$ ซึ่งนิยามโดย $f(a) = \overline{e}$ สำหรับทุกๆ $a \in G$ เป็นสาทิสสัณฐานเสมอ [เพราะว่า $\theta(ab) = \overline{e} = \overline{e}\cdot\overline{e} = \theta(a)\theta(b)$ สำหรับทุกๆ a, b $\in G$] ยิ่งไปกว่านั้นฟังก์ชันนี้จะเป็นฟังก์ชันคงตัวเพียงฟังก์ชันเดียวที่เป็นสาทิสสัณฐาน เราจะเรียกฟังก์ชันนี้ว่า *สาทิสสัณฐานคงตัว (constant homomorphism)*

7.1.2 **ตัวอย่าง** พิจารณากรุปการบวก Z ของจำนวนเต็มทั้งหมดและกรุปการบวก $Z_n$ ของเรซิดิวคลาส มอดูโล n เมื่อ n เป็นจำนวนเต็มบวก ถ้าเรานิยาม $\theta : Z \rightarrow Z_n$ โดย $\theta(a) = \overline{a}$ สำหรับทุกๆ จำนวนเต็ม a [นั่นคือ $\theta$ ส่งแต่ละจำนวนเต็มไปยังเซตสมมูลที่มี a เป็นสมาชิกอยู่] แล้ว $\theta$ เป็นสาทิสสัณฐานเพราะ

$$\theta(a+b) = \overline{a+b} = \overline{a} \oplus \overline{b} = \theta(a) \oplus \theta(b)$$

สำหรับทุกๆ จำนวนเต็ม a และ b ❍

เนื่องจากสาทิสสัณฐานมีสมบัติยืนยงการดำเนินการ ดังนั้นสาทิสสัณฐานจะไม่แปรเปลี่ยนโครงสร้างบางส่วนของ G ทฤษฎีบทต่อไปจะแสดงโครงสร้างที่จะไม่แปรเปลี่ยนภายใต้สาทิสสัณฐาน

7.1.3 ทฤษฎีบท ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้ว

1. $\theta(e) = \overline{e}$ เมื่อ e และ $\overline{e}$ เป็นเอกลักษณ์ของ G และ $\overline{G}$ ตามลำดับ
2. $\theta(a^{-1}) = \theta(a)^{-1}$ สำหรับแต่ละ $a \in G$

**บทพิสูจน์** 1. เนื่องจาก $\theta(e)\overline{e} = \theta(e) = \theta(e \cdot e) = \theta(e)\theta(e)$ ดังนั้นโดยกฎการตัดออกในกรุป $\overline{G}$ จะได้ $\theta(e) = \overline{e}$

2. ให้ $a \in G$ แล้ว $\theta(a)\theta(a^{-1}) = \theta(aa^{-1}) = \theta(e) = \overline{e}$ ซึ่งแสดงว่า $\theta(a^{-1})$ เป็นตัวผกผันของ $\theta(a)$ แต่ตัวผกผันของ $\theta(a)$ มีเพียงหนึ่งเดียว จึงสรุปได้ว่า $\theta(a^{-1}) = \theta(a)^{-1}$ □

7.1.4 **ตัวอย่าง** เพื่อให้เห็นการประยุกต์ของทฤษฎีบท 7.1.3 จะแสดงว่าสำหรับแต่ละจำนวนจริง $r \neq 0$ จะมีสาทิสสัณฐาน $\theta$ จากกรุปการบวก Z ไปยังกรุปการคูณ $R^{pos}$ เพียงฟังก์ชันเดียวซึ่ง $\theta(1) = r$

**วิธีทำ** ให้ r เป็นจำนวนจริงซึ่ง $r \neq 0$ และให้ $\theta$ คือสมสัณฐานในตัวอย่าง 6.1.2 ที่กำกัดลงบน Z แล้ว $\theta$ เป็นสาทิสสัณฐาน

ส่วนการพิสูจน์ว่า $\theta$ เป็นเพียงฟังก์ชันเดียวซึ่ง $\theta(1) = r$ จะสมมติให้ $\psi : Z \rightarrow R^{pos}$ เป็นสาทิสสัณฐานซึ่ง $\psi(1) = r$ และจะแสดงว่า $\theta = \psi$

ให้ n เป็นจำนวนเต็ม ถ้า n เป็นจำนวนเต็มบวก แล้ว $n = \underbrace{1+1+\ldots+1}_{n\text{ ครั้ง}}$ และด้วยสมบัติยืนยงการดำเนินการของ $\theta$ และ $\psi$ จะได้

$$\theta(n) = \theta(1)^n = r^n = \psi(1)^n = \psi(n)$$

ถ้า n เป็นจำนวนเต็มลบ แล้ว -n เป็นจำนวนเต็มบวก จะทำให้ได้โดยกรณี n เป็นจำนวนเต็มบวกว่า $\theta(-n) = \psi(-n)$ ดังนั้น

$$\theta(n) = \theta(-(-n)) = -\theta(-n) = -\psi(-n) = \psi(-(-n)) = \psi(n)$$

และโดยทฤษฎีบท 7.1.3 ข้อ 1 จะได้ $\theta(0) = 1 = \psi(0)$

จากทั้งสามกรณีที่กล่าวมา สรุปว่า $\theta(n) = \psi(n)$ สำหรับทุกๆ จำนวนเต็ม n ทำให้ได้ว่า $\theta = \psi$ ○

ทฤษฎีบทต่อไป จะแสดงว่าภาพของสาทิสสัณฐานเป็นกรุป ยิ่งไปกว่านั้นสาทิสสัณฐานยังส่งโครงสร้างบางส่วนของโดเมนไปยังภาพของสาทิสสัณฐานและโดยกลับกัน

7.1.5 **ทฤษฎีบท** ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้ว

1. ถ้า H เป็นกรุปย่อยของ G แล้ว $\theta(H)$ เป็นกรุปย่อยของ $\overline{G}$
2. ถ้า $\overline{H}$ เป็นกรุปย่อยของ $\overline{G}$ แล้ว $\theta^{-1}(H)$ เป็นกรุปย่อยของ G

**บทพิสูจน์** 1. ให้ H เป็นกรุปย่อยของกรุป G และให้ x และ y เป็นสมาชิกใดๆ ใน $\theta(H)$ และขอทบทวนว่า $\theta(H) = \{\theta(h) \mid h \in H\}$ ดังนั้นจะมี $h_1, h_2 \in H$ ซึ่ง $x = \theta(h_1)$ และ $y = \theta(h_2)$ เนื่องจาก H เป็นกรุปย่อยของ G เพราะฉะนั้น $h_1h_2^{-1} \in H$ และ $xy^{-1} = \theta(h_1)\theta(h_2^{-1}) = \theta(h_1h_2^{-1}) \in \theta(H)$ ซึ่งแสดงว่า $\theta(H)$ เป็นกรุปย่อยของ $\overline{G}$

2. ให้ $\overline{H}$ เป็นกรุปย่อยของกรุป $\overline{G}$ และขอทบทวนว่า $\theta^{-1}(\overline{H}) = \{a \in G \mid \theta(a) \in \overline{H}\}$ ให้ $a, b \in \theta^{-1}(H)$ แล้ว $\theta(a), \theta(b) \in \overline{H}$ และเพราะว่า $\overline{H}$ เป็นกรุปย่อยของ $\overline{G}$ ดังนั้น

$$\theta(ab^{-1}) = \theta(a)\theta(b^{-1}) = \theta(a)\theta(b)^{-1} \in \overline{H}$$

ซึ่งแสดงว่า $ab^{-1} \in \theta^{-1}(\overline{H})$ นั่นคือ $\theta^{-1}(\overline{H})$ เป็นกรุปย่อยของ G ❐

7.1.6 **บทแทรก** ถ้า $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้วพิสัย $\theta(G)$ เป็นกรุปย่อยของ $\overline{G}$ ❐

7.1.7 **บทแทรก** ถ้า $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้ว

1. ถ้า $\overline{N}$ เป็นกรุปย่อยปรกติของ $\overline{G}$ แล้ว $\theta^{-1}(\overline{N})$ เป็นกรุปย่อยปรกติของ G
2. ถ้า $\theta(G) = \overline{G}$ แล้ว $\theta(N)$ เป็นกรุปย่อยปรกติของ $\overline{G}$ สำหรับแต่ละกรุปย่อยปรกติ N ของ G

**บทพิสูจน์** 1. ให้ n และ a เป็นสมาชิกใดๆ ใน $\theta^{-1}(\overline{N})$ และ G ตามลำดับแล้ว $\theta(n) \in \overline{N}$ และเพราะ $\overline{N}$ เป็นกรุปย่อยปรกติของ $\overline{G}$ เราจะได้ว่า $\theta(ana^{-1}) = \theta(a)\theta(n)\theta(a^{-1}) \in \overline{N}$ นั่นคือ $ana^{-1} \in \theta^{-1}(\overline{N})$ ซึ่งแสดงว่า $\theta^{-1}(\overline{N})$ เป็นกรุปย่อยปรกติของ G

2. ให้ $\theta(G) = \overline{G}$ และให้ $n' \in \theta(N)$ และ $x \in \overline{G} = \theta(G)$ แล้วจะมี $n \in N$ และ $a \in G$ ซึ่ง $\theta(n) = n'$ และ $\theta(a) = x$ ถ้า N เป็นกรุปย่อยปรกติ แล้ว $ana^{-1} \in N$ และ

$$xn'x^{-1} = \theta(a)\theta(n)\theta(a)^{-1} = \theta(ana^{-1}) \in \theta(N)$$

จึงได้ว่า $\theta(N)$ เป็นกรุปย่อยปรกติของ $\overline{G}$ ❐

## แบบฝึกหัด 7.1

1. จงแสดงว่าฟังก์ชันซึ่งนิยามระหว่างกรุป ในแต่ละข้อต่อไปนี้เป็นสาทิสสัณฐานหรือไม่

1.1 $f : Z_8 \rightarrow Z_4$ กำหนดโดย $f = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} & \overline{7} \\ \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \end{pmatrix}$

1.2 $f : R \rightarrow R^{*}$ กำหนดโดย $f(a) = 2^{a}$

1.3 $f : R^{*} \rightarrow R^{pos}$ กำหนดโดย $f(a) = |a|$

1.4 $f : R \times R \rightarrow R$ กำหนดโดย $f(a, b) = a + b$

2. ให้ $\mathfrak{I}(R)$ แทนเซตของฟังก์ชันค่าจริงทั้งหมด

2.1 จงแสดงว่า $\mathfrak{I}(R)$ เป็นกรุปภายใต้การบวกของฟังก์ชันเป็นกรุป

2.2 จงแสดงว่า $\varphi : \mathfrak{I}(R) \rightarrow R$ กำหนดโดย $\varphi(f) = f(0)$ สำหรับทุกๆ $f \in \mathfrak{I}(R)$ เป็นสาทิสสัณฐาน

3. ให้ A และ B เป็นเซตซึ่ง $A \subset B$ และให้ $h : P(A) \rightarrow P(B)$ กำหนดโดย $h(C) = C \cap B$ สำหรับทุกๆ $C \subset A$

3.1 สำหรับ $A = \{1, 2, 3\}$ และ $B = \{1, 2\}$ จงเติมตารางการส่งของ h ข้างล่างนี้

$$h = \begin{pmatrix} \phi & \{1\} & \{2\} & \{3\} & \{1,2\} & \{1,3\} & \{2,3\} & \{1,2,3\} \\ & & & & & & & \end{pmatrix}$$

3.2 จงพิสูจน์ว่า h เป็นสาทิสสัณฐานสำหรับทุกๆ เซต A และ B ซึ่ง $A \subset B$

4. จงแสดงว่าถ้า G และ $\overline{G}$ เป็นกรุปและ $\varphi_1 : G \times \overline{G} \rightarrow G$ และ $\varphi_2 : G \times \overline{G} \rightarrow \overline{G}$ นิยามตามลำดับโดย $\varphi_1(a, b) = a$ และ $\varphi_2(a, b) = b$ แล้ว $\varphi_1$ และ $\varphi_2$ ต่างเป็นสาทิสสัณฐาน

5. ให้ G, H และ K เป็นกรุป และ $\theta : G \rightarrow H$ และ $\varphi : H \rightarrow K$ เป็นสาทิสสัณฐาน จงพิสูจน์ว่าฟังก์ชันประกอบ $\varphi \circ \theta$ เป็นสาทิสสัณฐาน

6. ให้ G เป็นกรุป จงพิสูจน์ว่าข้อความต่อไปนี้สมมูลกัน

(ก) G เป็นกรุปอาบีเลียน

(ข) $\theta : G \rightarrow G$ นิยามโดย $\theta(a) = a^{-1}$ เป็นสาทิสสัณฐาน

(ค) $\theta : G \rightarrow G$ นิยามโดย $\theta(a) = a^{2}$ เป็นสาทิสสัณฐาน

7. ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ และ $S \subseteq G$ จงพิสูจน์ว่าถ้า $G = \langle S \rangle$ แล้ว $\overline{G} = \langle \theta(S) \rangle$

8. ให้ G เป็นกรุปวัฏจักรอันดับจำกัด n และ k เป็นจำนวนเต็มบวกซึ่ง (n, k) = 1 จงพิสูจน์ว่า $\theta : G \rightarrow G$ นิยามโดย $\theta(x) = x^k$ สำหรับทุกๆ $x \in G$ เป็นสาทิสสัณฐาน

## 7.2 ความสัมพันธ์ของสาทิสสัณฐานและกรุปย่อยปรกติ

สำหรับแต่ละกรุป G ที่มี e เป็นเอกลักษณ์ เราสามารถพิสูจน์ได้อย่างง่ายๆ ว่า $a\{e\}a^{-1} = \{e\}$ และ $aGa^{-1} = G$ ซึ่งแสดงว่า {e} และ G เป็นกรุปย่อยปรกติของ G เราจึงเรียก {e} และ G ว่า *กรุปย่อยขัด (trivial subgroup)* และ *กรุปย่อยปรกติขัด (trivial normal subgroup)* ของ G นอกจากนี้เรายังเห็นได้ชัดว่าฟังก์ชันเอกลักษณ์และฟังก์ชันคงตัวซึ่งส่งทุกสมาชิกไปยังเอกลักษณ์ดังกล่าวไว้ในหัวข้อ 7.1 เป็นสาทิสสัณฐาน ทำให้เราอาจตั้งคำถามในกรณีทั่วไปว่าถ้า $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้วเซตย่อยของสมาชิกใน G ซึ่งถูกส่งโดย $\theta$ ไปยังเอกลักษณ์ $\overline{e}$ ของ $\overline{G}$ หรือก็คือภาพผกผันของ $\overline{e}$ จะเป็นกรุปย่อยและเป็นกรุปย่อยปรกติของ G หรือไม่ ในหัวข้อนี้ เราจะพิสูจน์คำตอบเชิงบวกของคำถามดังกล่าว กล่าวคือจะมีกรุปย่อยปรกติของกรุป G ซึ่งกำหนดโดยแต่ละสาทิสสัณฐานจาก G และโดยกลับกันเราจะแสดงด้วยว่า แต่ละกรุปย่อยปรกติ N ของ G จะมีกรุป $\overline{G}$ และสาทิสสัณฐานจาก G ไปยัง $\overline{G}$ ที่ทำให้ภาพผกผันของ $\overline{e}$ ใน $\overline{G}$ คือ N

7.2.1 **บทนิยาม** ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ จะเรียกเซตของสมาชิกใน G ซึ่งถูกส่งโดย $\theta$ ไปยังเอกลักษณ์ $\overline{e}$ ของ $\overline{G}$ ว่า *ส่วนกลาง(kernel)* ของ $\theta$ และเขียนแทนเซตนี้ด้วย $\ker\theta$ นั่นคือ

$$\ker\theta = \{x \in G \mid \theta(x) = \overline{e}\} = \theta^{-1}(\{\overline{e}\})$$

โดยทฤษฎีบท 7.1.3 จะเห็นว่า $\ker\theta$ ไม่เป็นเซตว่าง เพราะเอกลักษณ์ของกรุป G จะเป็นสมาชิกของ $\ker\theta$ และเนื่องจาก $\{\overline{e}\}$ เป็นกรุปย่อยปรกติของ $\overline{G}$ ดังนั้นบทแทรก 7.1.7 ทำให้เราสรุปได้ว่า $\ker\theta = \theta^{-1}(\{\overline{e}\})$ เป็นกรุปย่อยปรกติของ G

7.2.1 **ทฤษฎีบท** ถ้า $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้ว $\ker\theta$ เป็นกรุปย่อยปรกติของ G ❐

เพราะว่าเอกลักษณ์ $\overline{e}$ ของกรุป $\overline{G}$ เป็นสมาชิกของทุกๆ กรุปย่อย $\overline{H}$ ของ $\overline{G}$ ดังนั้น $\theta^{-1}(\{\overline{e}\})$ จะเป็นเซตย่อยของ $\theta^{-1}(\overline{H})$ เราจะได้บทแทรกต่อไปนี้

7.2.2 **บทแทรก** ถ้า $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้ว $\theta^{-1}(\overline{H})$ เป็นกรุปย่อยของ G ซึ่ง $\ker\theta \subseteq \theta^{-1}(H)$ สำหรับทุกๆ กรุปย่อย $\overline{H}$ ของ $\overline{G}$ ❐

7.2.3 **ตัวอย่าง** ให้ $\theta : Z \longrightarrow R^{*}$ นิยามโดย $\theta(n) = \begin{cases} 1 & \text{ถ้า } n \text{ เป็นจำนวนคู่} \\ -1 & \text{ถ้า } n \text{ เป็นจำนวนคี่} \end{cases}$ สำหรับทุกๆ $n \in Z$

แล้วสำหรับแต่ละคู่ของจำนวนเต็ม m และ n เราจะได้ $\theta(mn) = 1 = (1)(1) = \theta(m)\theta(n)$ [เมื่อ m และ n ต่างเป็นจำนวนคู่] หรือ $\theta(mn) = -1 = (1)(-1) = \theta(m)\theta(n)$ [เมื่อ m เป็นจำนวนคู่และ n เป็นจำนวนคี่] หรือ $\theta(mn) = -1 = (-1)(1) = \theta(m)\theta(n)$ [เมื่อ m เป็นจำนวนคี่และ n เป็นจำนวนคู่] หรือ $\theta(mn) = 1 = (-1)(-1) = \theta(m)\theta(n)$ [เมื่อ m และ n ต่างเป็นจำนวนคี่] ซึ่งแสดงว่า $\theta$ เป็นสาทิสสัณฐาน ทำให้ได้โดยทฤษฎีบท 7.2.1 ว่า

$$\ker\theta = \{ n \in Z \mid \theta(n) = 1 \} = \text{เซตของจำนวนเต็มคู่ทั้งหมด}$$

เป็นกรุปย่อยปรกติของ Z ❍

ถ้า $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ และ $y \in \theta(G)$ แล้วจะมี $x \in G$ ซึ่ง $\theta(x) = y$ และเป็นที่ทราบกันดีว่าเราเรียก x ว่าภาพผกผันของ y ภายใต้ $\theta$ และถ้า y คือเอกลักษณ์ $\overline{e}$ ของ $\overline{G}$ เราก็ทราบจากทฤษฎีบท 7.2.1 แล้วว่า $K = \ker\theta = \theta^{-1}(\{\overline{e}\})$ เป็นกรุปย่อยปรกติของ G ดังนั้นเซตของโคเซตซ้ายทั้งหมดของ K ใน G เป็นเซตเดียวกับเซตของโคเซตขวาทั้งหมดของ K ใน G ทำให้เรากล่าวถึงเซตนี้ได้อย่างสั้นๆ ว่าเซตของโคเซตทั้งหมดของ K ใน G จึงเกิดคำถามว่าแต่ละโคเซตของ K ใน G จะเป็นภาพผกผันของสมาชิกใน $\overline{G}$ เช่นเดียวกับ K หรือไม่ ทฤษฎีบทต่อไปจะแสดงความจริงนี้

7.2.4 **ทฤษฎีบท** ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ และให้ $K = \ker\theta$ แล้วโคเซต xK จะเป็นภาพผกผันของ $\theta(x) \in \theta(G)$ สำหรับทุกๆ $x \in G$

**บทพิสูจน์** ให้ $x \in G$ แล้ว $\theta(x) \in \theta(G)$ ให้ $y = \theta(x)$ และ $t \in \theta^{-1}(\{y\})$ แล้ว $\theta(t) = y = \theta(x)$ ทำให้ได้ $\overline{e} = \theta(x)^{-1}\theta(t) = \theta(x^{-1}t)$ ซึ่งแสดงว่า $x^{-1}t \in K$ นั่นคือ $xK = tK$ ดังนั้น $t \in xK$ ทำให้ได้ว่า $\theta^{-1}(\{y\}) \subseteq xK$

ในทางกลับกัน ให้ $t \in xK$ แล้วจะมี $k \in K$ ซึ่ง $t = xk$ ทำให้ได้ $\theta(t) = \theta(xk) = \theta(x)\theta(k) = \theta(x)\overline{e} = \theta(x) = y$ ดังนั้น $t \in \theta^{-1}(\{y\})$ ซึ่งแสดงว่า $xK \subseteq \theta^{-1}(\{y\})$

เพราะฉะนั้น xK เป็นภาพผกผันของ $\theta(x)$ ❐

ในหัวข้อโคเซตซ้ายและโคเซตขวา ได้มีการแสดงว่าทุกๆ โคเซต (ซ้ายหรือขวาก็ตาม) ของ K ใน G จะมีขนาดเท่ากันและเท่ากับของ K ดังนั้นโดยทฤษฎีบท 7.2.3 ถ้า K = {e} นั่นคือ K เป็นเซตโทนที่ประกอบด้วยเอกลักษณ์ของ G เพียงหนึ่งเดียว แล้วภาพผกผันของแต่ละสมาชิกใน $\theta(G)$ จะประกอบด้วยสมาชิกเพียงหนึ่งเดียวด้วย ซึ่งแสดงว่า $\theta$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

7.2.5 **บทแทรก** ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้ว $\theta$ เป็นฟังก์ชันหนึ่งต่อหนึ่งก็ต่อเมื่อ $\ker\theta = \{e\}$ ❐

ในบทที่ 5 เราได้แสดงแล้วว่า สำหรับแต่ละกรุปย่อยปรกติ N ของกรุป G เราสามารถกำหนดกรุปผลหาร $\frac{G}{N}$ ซึ่งเป็นกรุปที่ประกอบด้วยโคเซตทั้งหมดของ N ใน G และเมื่อพิจารณากรุป G และ $\frac{G}{N}$ เราอาจถามว่าจะมีสาทิสสัณฐานระหว่างกรุปสองกรุปนี้หรือไม่ และเพื่อจะหาคำตอบ ใครสักคนอาจคิดแบบเป็นธรรมชาติว่า ลองส่งแต่ละสมาชิกใน G ไปยังโคเซตที่สมาชิกนั้นอยู่ ทฤษฎีบทต่อไปนี้จะแสดงว่าการส่งดังกล่าวเป็นสาทิสสัณฐาน ซึ่งจะทำให้เราได้ด้วยว่าทุกๆ กรุปย่อยปรกติของกรุป G จะเป็นส่วนกลางของสาทิสสัณฐาน

7.2.6 **ทฤษฎีบท** สำหรับแต่ละกรุปย่อยปรกติ N ของกรุป G จะมีกรุป $\overline{G}$ และสาทิสสัณฐาน $\theta$ จาก G ไปบน $\overline{G}$ ที่ทำให้ N เป็นส่วนกลางของ $\theta$

**บทพิสูจน์** ให้ N เป็นกรุปย่อยปรกติ N ของ G แล้วจะมี $\frac{G}{N}$ เป็นกรุปผลหาร ให้ $\eta : G \rightarrow \frac{G}{N}$ กำหนดโดย $\eta(a) = aN$ สำหรับทุกๆ $a \in G$ แล้วเราจะแสดงว่า $\eta$ เป็นสาทิสสัณฐาน

เนื่องจากกรุปผลหาร $\frac{G}{N}$ เป็นผลแบ่งกั้น G ดังนั้น $\eta$ เป็นฟังก์ชัน และเราเห็นได้ชัดโดยบทนิยามของโคเซตว่า $\eta$ เป็นฟังก์ชันทั่วถึง นอกจากนี้ถ้า $a, b \in G$ เราจะได้โดยนิยามการคูณของโคเซตว่า $\eta(ab) = abN = (aN)(bN) = \eta(a)\eta(b)$ เพราะฉะนั้น $\eta$ เป็นสาทิสสัณฐาน

สุดท้ายเพราะว่าโคเซต N = eN เป็นเอกลักษณ์ของกรุปผลหาร $\frac{G}{N}$ เราจะได้ว่า

$$a \in \ker\eta \Leftrightarrow \eta(a) = N \Leftrightarrow aN = N \Leftrightarrow a \in N$$

เพราะฉะนั้น $N = \ker\eta$ ❐

เราเรียกฟังก์ชัน $\eta$ ซึ่งกำหนดดังในทฤษฎีบท 7.2.5 ว่า *สาทิสสัณฐานธรรมชาติ (natural homomorphism)* นอกจากนี้ทฤษฎีบท 7.2.5 ยังแสดงว่าแต่ละกรุปย่อยปรกติของกรุปจะกำหนดกรุปผลหารซึ่งเป็นภาพสาทิสสัณฐานของกรุปนั้น

**แบบฝึกหัด 7.2**

จงหาส่วนกลางของสาทิสสัณฐานในข้อ 1 ข้อ 2 และข้อ 3 ของแบบฝึกหัด 7.1

## 7.3 ทฤษฎีบทหลักมูลของสาทิสสัณฐาน

ในหัวข้อ 7.2 เราได้แสดงแล้วว่า แต่ละกรุปผลหารเป็นภาพของกรุปภายใต้สาทิสสัณฐาน เราอาจมีคำถามว่า แล้วภาพของกรุปภายใต้สาทิสสัณฐานดีอย่างไร เราจะลองมาพิจารณาจากตัวอย่างต่อไปนี้

ให้ P = {e, o} แล้ว P เป็นกรุปภายใต้การดำเนินการกำหนดบน P แสดงดังตารางข้างล่างนี้

| + | e | o |
|---|---|---|
| e | e | o |
| o | o | e |

ให้ $f : Z \longrightarrow P$ โดย f ส่งทุกๆ จำนวนคู่ไปยัง e และส่งทุกๆ จำนวนคี่ไปยัง o [นั่นคือเราให้ e แทน "คู่ (even)" และให้ o แทน "คี่ (odd)"] เราจึงเรียกกรุป P ว่า *กรุปภาวะคู่หรือคี่ (parity group)* แล้วโดยการพิสูจน์ในทำนองเดียวกับตัวอย่าง 7.2.2 จะได้ว่า f เป็นสาทิสสัณฐาน และเห็นได้ชัดว่า f เป็นฟังก์ชันทั่วถึง ดังนั้น P เป็นภาพภายใต้สาทิสสัณฐานของกรุป Z เราจะเห็นว่า P เป็นกรุปที่มีขนาดเล็กกว่า Z มากและ P เป็นกรุปที่มีความซับซ้อนน้อยกว่า Z อย่างไรก็ตาม P และ Z มีสมบัติที่เหมือนกันอย่างหนึ่งคือภาวะแสดงความเป็นจำนวนคู่และจำนวนคี่ แสดงให้เห็นว่าสาทิสสัณฐานจะแปลงสมบัติจากกรุปที่เป็นโดเมน (ซึ่งอาจมีความยุ่งยากซับซ้อน) มายังกรุปซึ่งเป็นภาพของสาทิสสัณฐานที่จะมีขนาดเล็กกว่าหรือเท่ากับโดเมน และจะสะท้อนโครงสร้างที่เราอาจกำลังพิจารณาศึกษาในกรุปโดเมนแต่ไม่ค่อยชัดเจนเนื่องจากความซับซ้อน

เราจึงต้องการหาภาพภายใต้สาทิสสัณฐานทั้งหมดของแต่ละกรุป และทฎษฎีบท 7.2.5 ได้พิสูจน์แล้วว่าทุกๆ กรุปผลหารของกรุปเป็นภาพภายใต้สาทิสสัณฐานของกรุปนั้น เราจึงต้องการทราบ

ว่าจะมีภาพภายใต้สาทิสสัณฐานของกรุปที่นอกเหนือจากกรุปผลหารหรือไม่ ในหัวข้อนี้เราจะแสดงการพิสูจน์ว่าจะไม่มีภาพภายใต้สาทิสสัณฐานของกรุปที่นอกเหนือจากกรุปผลหาร ทฤษฎีบทนี้จึงสำคัญในสาขาวิชาพีชคณิต จึงเรียกทฤษฎีบทที่แสดงผลดังกล่าวนี้ว่า "ทฤษฎีบทหลักมูลของสาทิสสัณฐาน"

7.3.1 **ทฤษฎีบทหลักมูลของสาทิสสัณฐาน** (The fundamental homomorphism theorem)

ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ และ $K = \ker\theta$ ถ้า $\theta$ เป็นฟังก์ชันทั่วถึง แล้ว $\overline{G}$ สมสัณฐานกับ $\frac{G}{K}$

**บทพิสูจน์** ในการแสดงว่า $\overline{G} \cong \frac{G}{K}$ เราต้องพิจารณาหาฟังก์ชันซึ่งส่งจาก $\frac{G}{K}$ ไปยัง $\overline{G}$ ที่จะเป็นสมสัณฐาน และฟังก์ชันที่น่าจะเป็นไปได้ เราพิจารณาจากข้อกำหนดว่า $\theta$ เป็นสาทิสสัณฐานชนิดทั่วถึงจากกรุป G ไปยังกรุป $\overline{G}$ ซึ่งแสดงว่าแต่ละสมาชิก y ใน $\overline{G}$ จะกำหนดสมาชิก x ใน G ซึ่ง $y = \theta(x)$ นอกจากนี้เรายังมีสาทิสสัณฐานธรรมชาติ $\eta$ ซึ่งส่งแต่ละสมาชิก x จาก G ไปยังโคเซต xK ใน $\frac{G}{K}$

เราจึงนิยาม $\sigma : \frac{G}{K} \rightarrow \overline{G}$ โดย $\sigma(xK) = \theta(x)$ สำหรับทุกๆ $x \in G$ เราต้องแสดงก่อนอื่นว่า $\sigma$ เป็นฟังก์ชัน โดยให้ $x_1, x_2 \in G$ ซึ่ง $x_1K = x_2K$ แล้วโดยทฤษฎีบท 7.2.3 เราจะได้ว่า $\theta(x_1) = \theta(x_1K) = \theta(x_2K) = \theta(x_2)$ แต่ $\sigma(x_1K) = \theta(x_1)$ และ $\sigma(x_2K) = \theta(x_2)$ ดังนั้น $\sigma(x_1K) = \sigma(x_2K)$

อย่างที่สองจะแสดงว่า $\sigma$ เป็นสาทิสสัณฐาน โดยให้ $x_1, x_2 \in G$ แล้ว $\sigma((x_1K)(x_2K)) = \sigma(x_1x_2K) = \theta(x_1x_2) = \theta(x_1)\theta(x_2) = \sigma(x_1K)\sigma(x_2K)$

อย่างที่สามจะแสดงว่า $\sigma$ เป็นฟังก์ชันชนิดทั่วถึง โดยให้ $y \in \overline{G}$ แล้วเพราะ $\theta$ เป็นฟังก์ชันชนิดทั่วถึง จะมี $x \in G$ ซึ่ง $y = \theta(x)$ แต่โดยนิยามของ $\sigma$ ทำให้ได้ $\sigma(xK) = \theta(x) = y$

สุดท้ายจะแสดงว่า $\sigma$ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง โดยให้ $x_1, x_2 \in G$ ซึ่ง $\sigma(x_1K) = \sigma(x_2K)$ หรือสมมูลกับ $\theta(x_1) = \theta(x_2)$ ทำให้ได้ $\overline{e} = \theta(x_1)^{-1}\theta(x_2) = \theta(x_1^{-1}x_2)$ ซึ่งแสดงว่า $x_1^{-1}x_2 \in K$ นั่นคือ $x_1K = x_2K$ ❐

7.3.2 **บทแทรก** ถ้า $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ และ $K = \ker\theta$ แล้ว

$\theta(G) \cong \frac{G}{K}$ ❐

7.3.3 **ตัวอย่าง** เราอาจแสดงว่าทุกๆ กรุปวัฏจักร จะสมสัณฐานกับ Z หรือ $Z_n$ เมื่อ n เป็นจำนวนเต็ม

บวกดังแสดงในทฤษฎีบท 6.2.1 และ 6.2.2 อีกวิธีหนึ่งโดยประยุกต์ทฤษฎีบทหลักมูลของสาทิสสัณฐาน ดังนี้

ให้ G เป็นกรุปและ $a \in G$ และนิยาม $\theta : Z \rightarrow G$ โดย $\theta(n) = a^n$ สำหรับทุกๆ จำนวนเต็ม n แล้วเราจะละการพิสูจน์ว่า $\theta$ เป็นสาทิสสัณฐาน ดังนั้นโดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ $\theta(G) \cong \frac{Z}{K}$ เมื่อ $K = \ker\theta$ และขอให้สังเกตว่า $\theta(G) = \{a^n \mid n \in Z\} = \langle a \rangle$ เป็นกรุปวัฏจักรก่อกำเนิดโดย a

เพราะว่า $K = \ker\theta = \{n \in Z \mid a^n = e\}$ ดังนั้น ถ้า $K = \ker\theta = \{0\}$ แล้ว $Z \cong \frac{Z}{\{0\}} = \frac{Z}{K} \cong \langle a \rangle$ เป็นกรุปวัฏจักรอันดับอนันต์ และถ้า $K = \ker\theta \neq \{0\}$ แล้วจะมีจำนวนต็มบวก n ตัวน้อยสุดซึ่ง $a^n = e$ ซึ่งในกรณีเช่นนี้ $K = \ker\theta = \langle n \rangle$ ทำให้ได้ว่า $\frac{Z}{K} = \frac{Z}{\langle n \rangle} = Z_n$ เพราะฉะนั้น $\langle a \rangle \cong Z_n$ ❍

7.3.4 **ตัวอย่าง** ในตัวอย่างนี้ เราจะแสดงว่าขนาดของกรุปสลับเป็นครึ่งหนึ่งของกรุปสมมาตรอีกวิธีหนึ่งโดยประยุกต์ทฤษฎีบทหลักมูลของสาทิสสัณฐาน

ให้ P เป็นกรุปภาวะคู่หรือคี่และ n เป็นจำนวนเต็มบวก และนิยาม $\theta : S_n \rightarrow P$ โดย

$$\theta(\alpha) = \begin{cases} e & \text{ถ้า } \alpha \in A_n' \\ o & \text{ถ้า } \alpha \in B_n' \end{cases}$$ แล้วโดยการพิสูจน์อย่างง่ายๆ จะได้ว่า $\theta$ เป็นสาทิสสัณฐานจาก $S_n$ ไปทั่วถึง P ดังนั้นโดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ $P \cong \frac{S_n}{K}$ เมื่อ $K = \ker\theta = \{\alpha \in S_n \mid \theta(\alpha) = e\} = A_n$ เพราะฉะนั้น

$$2 = |P| = \left|\frac{S_n}{K}\right| = \left|\frac{S_n}{A_n}\right| = \frac{|S_n|}{|A_n|} \qquad \text{ซึ่งสมมูลกับ} \qquad |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$ ❍

7.3.5 **ตัวอย่าง** ให้ G เป็นกรุปของการหมุนระนาบรอบจุดคงที่ p และสำหรับแต่ละจำนวนจริง r ให้ $\theta(r)$ เป็นสมาชิกใน G ซึ่งแทนการหมุนรอบ p ตามเข็มนาฬิกาไป r เรเดียน แล้ว $\theta$ เป็นสาทิสสัณฐานจากกรุปการบวก R ไปทั่วถึง G ดังนั้นโดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ $G \cong \frac{R}{K}$ เมื่อ $K = \ker\theta = \{2k\pi \mid k \in Z\} = \langle 2\pi \rangle$ เพราะฉะนั้น $G \cong \frac{R}{\langle 2\pi \rangle}$ ❍

7.3.6 **ทฤษฎีบท** $\frac{G}{C(G)} \cong I(G)$ สำหรับทุกๆ กรุป G

**บทพิสูจน์** ให้ G เป็นกรุปและให้ $\theta : G \rightarrow I(G)$ นิยามโดย $\theta(a) = T_a$ สำหรับทุกๆ $a \in G$ แล้วเพราะ $a = b$ ก็ต่อเมื่อ $T_a = T_b$ สำหรับทุกๆ $a, b \in G$ ดังนั้น $\theta$ เป็นฟังก์ชันและโดยนิยามของ $I(G)$ จะได้ $\theta$ เป็นฟังก์ชันไปบน จึงเหลือเพียงการพิสูจน์ว่า $\theta$ เป็นสาทิสสัณฐาน

ให้ $a, b \in G$ แล้ว $\theta(ab) = T_{ab} = T_aT_b = \theta(a)\theta(b)$ ดังนั้น $\theta$ เป็นสาทิสสัณฐาน โดยที่

$$a \in \ker\theta \Leftrightarrow \iota_G = \theta(a) = T_a \Leftrightarrow axa^{-1} = x \text{ สำหรับทุกๆ } x \in G$$

$$\Leftrightarrow ax = xa \text{ สำหรับทุกๆ } x \in G \Leftrightarrow a \in C(G)$$

ซึ่งแสดงว่า $\ker\theta = C(G)$ เพราะฉะนั้นโดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ $\frac{G}{C(G)} \cong I(G)$ ❐

ถ้า $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป $\overline{G}$ แล้วโดยทฤษฎีบท 7.1.5 แต่ละกรุปย่อย H ของ G จะกำหนดกรุปย่อยกรุปย่อย $\theta(H)$ ของ $\overline{G}$ และถ้า H และ K เป็นกรุปย่อยของ G ซึ่ง $H \subseteq K \subseteq \ker\theta$ แล้ว $\theta(H) = \theta(K)$ นั่นคือทุกๆ กรุปย่อยของ G ซึ่งเป็นเซตย่อยของส่วนกลางของสาทิสสัณฐานจะกำหนดกรุปย่อยของ $\overline{G}$ กรุปย่อยเดียวกัน ทำให้เราได้ว่าจะไม่มีฟังก์ชันสมนัยหนึ่งต่อหนึ่งระหว่างเซตของกรุปย่อยทั้งหมดของ G กับเซตของกรุปย่อยทั้งหมดของ $\overline{G}$ แต่ทฤษฎีบทต่อไป เราจะแสดงว่า ถ้าสาทิสสัณฐานเป็นฟังก์ชันทั่วถึงแล้วจะมีฟังก์ชันสมนัยหนึ่งต่อหนึ่งระหว่างเซตของกรุปย่อยทั้งหลายของ G ที่มีส่วนกลางของสาทิสสัณฐานเป็นเซตย่อยกับเซตของกรุปย่อยทั้งหมดของ $\overline{G}$

7.3.7 **ทฤษฎีบท** ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปทั่วถึงกรุป $\overline{G}$

1. ถ้า H เป็นกรุปย่อยของ G ซึ่ง $\ker\theta \subseteq H$ แล้ว $H = \theta^{-1}(\theta(H))$
2. $|A| = |B|$ ถ้า A เป็นเซตของกรุปย่อย H ของ G ซึ่ง $\ker\theta \subseteq H$ และ B เป็นเซตของกรุปย่อยทั้งหมดของ $\overline{G}$

**บทพิสูจน์** 1. โดยสมบัติของฟังก์ชันทั่วไป จะได้ $H \subseteq \theta^{-1}(\theta(H))$ จึงเหลือเพียงแสดงว่า $\theta^{-1}(\theta(H)) \subseteq H$ โดยให้ $a \in \theta^{-1}(\theta(H))$ แล้ว $\theta(a) \in \theta(H)$ ดังนั้นจะมี $h \in H$ ซึ่ง $\theta(a) = \theta(h)$ ทำให้ได้ว่า $\overline{e} = \theta(a)\theta(h^{-1}) = \theta(ah^{-1})$ ซึ่งแสดงว่า $ah^{-1} \in \ker\theta \subseteq H$ นั่นคือมี $h' \in H$ ที่ทำให้ $ah^{-1} = h'$ ซึ่งสมมูลกับ $a = h'h$ โดยที่ $h'h \in H$ ดังนั้น $a \in H$

2. ให้ $\sigma : A \rightarrow B$ นิยามโดย $\sigma(H) = \theta(H)$ สำหรับทุกๆ $H \in A$ เราจะแสดงก่อนว่า $\sigma$ เป็นฟังก์ชันทั่วถึง โดยให้ $\overline{H}$ เป็นกรุปย่อยของ $\overline{G}$ แล้วโดยทฤษฎีบท 7.1.5 จะได้ $\theta^{-1}(\overline{H})$ เป็นกรุปย่อยของ G

และเพราะ $\bar{e} \in \bar{H}$ ดังนั้น $\ker\theta = \theta^{-1}(\{\bar{e}\}) \subseteq \theta^{-1}(\bar{H})$ ให้ $H = \theta^{-1}(\bar{H})$ แล้ว H เป็นกรุปย่อยของ G ซึ่ง $\ker\theta \subseteq H$ ทำให้ได้โดยผลของข้อ 1 ว่า $H = \theta^{-1}(\theta(H))$ ดังนั้น $\sigma(H) = \theta(H) = \theta(\theta^{-1}(\bar{H})) = \bar{H}$

ต่อไปจะแสดงว่า $\sigma$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง โดยให้ H และ K เป็นกรุปย่อยของ G ซึ่ง $\ker\theta \subseteq H$, $\ker\theta \subseteq K$ และ $\theta(H) = \theta(K)$ แล้วโดยผลของข้อ 1 จะได้ว่า $H = \theta^{-1}(\theta(H)) = \theta^{-1}(\theta(K)) = K$ ❐

โดยผลของทฤษฎีบท 7.3.7 เมื่อประยุกต์สาทิสสัณฐานธรรมชาติกับกรุปผลหารซึ่งกำหนดโดยแต่ละกรุปย่อยปรกติของกรุป เราจะได้บทแทรกต่อไปนี้

7.3.8 **บทแทรก** ให้ N เป็นกรุปย่อยปรกติของกรุป G

1. $|A| = |B|$ ถ้า A เป็นเซตของกรุปย่อย H ทั้งหมดของ G ซึ่ง $N \subseteq H$ และ B เป็นเซตของกรุปย่อยทั้งหมดของ $\frac{G}{N}$
2. ถ้า K กรุปย่อยของ $\frac{G}{N}$ แล้วจะมีกรุปย่อย H ของ G ซึ่ง $N \subseteq H$ และ $K = \frac{H}{N}$ ❐

**แบบฝึกหัด** 7.3

1. จงประยุกต์ทฤษฎีบทหลักมูลของสาทิสสัณฐาน เพื่อแสดงข้อต่อไปนี้เป็นจริง

   1.1 $Z_5 \cong \frac{Z_{20}}{<\bar{5}>}$ 1.2 $Z_3 \cong \frac{Z_{18}}{<\bar{3}>}$

   1.3 $Z_k \cong \frac{Z_n}{<\bar{k}>}$ ถ้า k เป็นตัวหารของ n 1.4 $Z_2 \times Z_2 \cong \frac{G_S}{<r_2>}$

   1.5 $Z_3 \cong \frac{Z_3 \times Z_3}{K}$ เมื่อ $K = \{(0, 0), (1, 1), (2, 2)\}$ [**ข้อแนะนำ** : พิจารณาฟังก์ชันจาก $Z_3 \times Z_3$ ไปยัง $Z_3$ ซึ่งกำหนดโดย $h(a,b) = a - b$]

   1.6 $P_2 \cong \frac{P_3}{K}$ เมื่อ $P_2$ และ $P_3$ คือเซตกำลังของ {1, 2} และ {1, 2, 3} ตามลำดับและ $K = \{\phi, \{c\}\}$ [**ข้อแนะนำ** : พิจารณาฟังก์ชันซึ่งกำหนดโดย $h(C) = C \cap \{1,2\}$]

2. จงหาภาพภายใต้สาทิสสัณฐานทั้งหมดของกรุปในข้อต่อไปนี้

2.1 $S_3$ 2.2 $S_3$ 2.3 $Z_n$ เมื่อ n เป็นจำนวนเต็มบวก

3. ให้ $\alpha : \mathfrak{I}(R) \to R$ และ $\beta : \mathfrak{I}(R) \to R$ นิยามตามลำดับโดย $\alpha(f) = f(1)$ และ $\beta(f) = f(2)$ จงพิสูจน์ว่า

3.1 $\alpha$ และ $\beta$ เป็นสาทิสสัณฐาน

3.2 ถ้า J เป็นเซตของฟังก์ชันทั้งหลายจาก R ไปยัง R ที่มีกราฟผ่านจุด (1, 0) และ K เป็นเซตของฟังก์ชันทั้งหลายจาก R ไปยัง R ที่มีกราฟผ่านจุด (2, 0) แล้ว

$$\frac{\mathfrak{I}(R)}{J} \cong R \cong \frac{\mathfrak{I}(R)}{K}$$

## 7.4 ทฤษฎีบทสมสัณฐาน

ในหัวข้อนี้ เราจะแสดงการประยุกต์ทฤษฎีบทหลักมูลของสาทิสสัณฐาน ในการพิสูจน์ทฤษฎีบทสำคัญเกี่ยวกับสมสัณฐานที่รู้จักกันเป็นอย่างดี

7.4.1 **ทฤษฎีบท** ให้ G เป็นกรุป N เป็นกรุปย่อยปรกติของ G และ H เป็นกรุปย่อยของ G

1. NH เป็นกรุปย่อยของ G
2. $H \cap N$ เป็นกรุปย่อยปรกติของ H
3. N เป็นกรุปย่อยปรกติของ NH

**บทพิสูจน์** 1. โดยทฤษฎีบท 3.4.20 เพียงพอที่จะแสดงว่า NH = HN ให้ $n \in N$ และ $h \in H$ แล้ว เพราะ $h^{-1} \in H \subseteq G$ และ N เป็นกรุปย่อยปรกติของ G จะได้ว่า $h^{-1}nh = h^{-1}n(h^{-1})^{-1} \in N$ ทำให้ได้ $nh = h(h^{-1}nh) \in HN$ ดังนั้น $NH \subseteq HN$ และโดยการพิสูจน์ในทำนองคล้ายกัน เราก็จะได้ $HN \subseteq NH$

2. เราเห็นได้ชัดว่า $H \cap N$ เป็นกรุปย่อยของ H จึงให้ $t \in H \cap N$ และ $h \in H$ แล้ว $t \in H$ ทำให้ได้ $hth^{-1} \in H$ และเพราะว่า $t \in N$, $h \in H \subseteq G$ และ N เป็นกรุปย่อยปรกติของ G ดังนั้น $hth^{-1} \in N$ เพราะฉะนั้น $hth^{-1} \in H \cap N$

3. เพราะว่า N เป็นกรุปย่อยปรกติของ G ดังนั้น $ana^{-1} \in N$ สำหรับทุกๆ $n \in N$ และ $a \in G$ แต่ $NH \subseteq G$ ทำให้ได้ $ana^{-1} \in N$ สำหรับทุกๆ $n \in N$ และ $a \in NH$ เพราะฉะนั้น N เป็นกรุปย่อยปรกติของ NH ❐

### 7.4.2 **ทฤษฎีบทที่หนึ่งของสมสัณฐาน** (The First Isomorphism Theorem)

ถ้า N เป็นกรุปย่อยปรกติและ H เป็นกรุปย่อยของกรุป G แล้ว $\frac{H}{H\cap N} \cong \frac{NH}{N}$

**บทพิสูจน์** โดยทฤษฎีบท 7.4.1 เราได้ว่า NH เป็นกรุปย่อยของ G, $H\cap N$ เป็นกรุปย่อยปรกติของ H และ N เป็นกรุปย่อยปรกติของ NH ดังนั้น $\frac{H}{H\cap N}$ และ $\frac{NH}{N}$ เป็นกรุปผลหาร

ต่อไปเราจะสร้างสาทิสสัณฐานจาก H ไปทั่วถึง $\frac{NH}{N}$ โดยมีส่วนกลางคือ $H\cap N$ เพื่อจะประยุกต์ทฤษฎีบทหลักมูลของสาทิสสัณฐานได้ว่า $\frac{H}{H\cap N} \cong \frac{NH}{N}$ ในการสร้าง เราต้องส่งแต่ละสมาชิก $h\in H$ ไปยังโคเซตใน $\frac{NH}{N}$ แต่เพราะ $H\subseteq NH$ และเรามีสาทิสสัณฐานธรรมชาติ $\eta$ จาก NH ไปทั่วถึง $\frac{NH}{N}$ เราจึงให้ $\theta$ เป็นฟังก์ชันประกอบของฟังก์ชันเอกลักษณ์ $\iota_H$ ซึ่งกำกัดลงบน H กับ $\eta$ นั่นคือ

$\theta = \eta \circ \iota_H$ โดยมีแผนภาพการส่งแสดงดังนี้

$$\begin{tikzcd} H \arrow[rr, "\iota_H"] \arrow[dr, "\theta"'] & & HK \arrow[dl, "\eta"] \\ & HK/H & \end{tikzcd}$$

แล้ว $\theta$ สาทิสสัณฐานชนิดทั่วถึง และ

$$\begin{aligned} a\in\ker\theta &\Leftrightarrow a\in H \text{ และ } \theta(a) = N \\ &\Leftrightarrow a\in H \text{ และ } N = (\eta\circ\iota_H)(a) = (\eta(\iota_H(a) = \eta(a) = aN \\ &\Leftrightarrow a\in H \text{ และ } a\in N \Leftrightarrow a\in H\cap N \end{aligned}$$

ทำให้ได้ส่วนกลาง $\ker\theta = H\cap N$ ตามต้องการ ❐

### 7.4.3 **ทฤษฎีบท** ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปทั่วถึงกรุป $\overline{G}$

1. ถ้า N เป็นกรุปย่อยปรกติของ G ซึ่ง $\ker\theta \subseteq N$ แล้ว $\frac{G}{N} \cong \frac{\overline{G}}{\theta(N)}$
2. ถ้า $\overline{N}$ เป็นกรุปย่อยปรกติของ $\overline{G}$ แล้ว $\frac{G}{\theta^{-1}(\overline{N})} \cong \frac{\overline{G}}{\overline{N}}$

**บทพิสูจน์** 1. โดยบทแทรก 7.1.7 เราจะได้ว่า $\theta(N)$ เป็นกรุปย่อยปรกติของ $\overline{G}$ และให้ $\overline{\eta}$ เป็นสาทิสสัณฐานธรรมชาติจาก $\overline{G}$ ไปทั่วถึง $\frac{\overline{G}}{\theta(N)}$ และให้ $\sigma$ เป็นฟังก์ชันประกอบของ $\theta$ และ $\overline{\eta}$ ซึ่งมีแผนภาพของฟังก์ชันประกอบดังต่อไปนี้

$$\begin{tikzcd} G \arrow[r, "\theta"] \arrow[dr, "\sigma"'] & \overline{G} \arrow[d, "\overline{\eta}"] \\ & \overline{G}/\sigma(N) \end{tikzcd}$$

แล้วเพราะ $\theta$ และ $\overline{\eta}$ ต่างเป็นสาทิสสัณฐานดังนั้น $\sigma$ เป็นสาทิสสัณฐาน และเพราะ $\overline{\eta}$ เป็นฟังก์ชันทั่วถึง ดังนั้น $\sigma$ เป็นฟังก์ชันทั่วถึง ทำให้ได้โดยทฤษฎีบทหลักมูลของสาทิสสัณฐานว่า $\frac{G}{\ker\sigma} \cong \frac{\overline{G}}{\theta(N)}$ เราจึงจะแสดงว่า $\ker\sigma = N$

เนื่องจากเอกลักษณ์ของกรุปผลหาร $\frac{\overline{G}}{\theta(N)}$ คือโคเซต $\overline{e}\theta(N) = \theta(N)$ เราจะได้

$$a \in \ker\sigma \iff \sigma(a) = \theta(N) \iff \theta(N) = (\overline{\eta}(\theta(a)) = (\overline{\eta} \circ \theta)(a)\ \theta(a)\theta(N)$$

(โดยนิยามของ $\overline{\eta}$)

$$\iff \theta(a) \in \theta(N) \iff a \in \theta^{-1}(\theta(N)) = N \text{ (เพราะว่า } \ker\theta \subseteq N)$$

ดังนั้น $\ker\sigma = N$ และได้ $\frac{G}{N} \cong \frac{\overline{G}}{\theta(N)}$ ตามต้องการ

2. ให้ $\overline{N}$ เป็นกรุปย่อยปรกติของกรุป $\overline{G}$ แล้วโดยบทแทรก 7.1.7 จะได้ว่า $\theta^{-1}(\overline{N})$ เป็นกรุปย่อยปรกติของ G ยิ่งไปกว่านั้นบทแทรก 7.3.8 กล่าวว่า $\ker\theta \subseteq \theta^{-1}(\overline{N})$ ดังนั้นโดยผลของข้อ 1 จะได้

$$\frac{G}{\theta^{-1}(\overline{N})} \cong \frac{\overline{G}}{\theta(\theta^{-1}(\overline{N}))} = \frac{\overline{G}}{\overline{N}}$$ ❐

### 7.4.4 ทฤษฎีบทที่สองของสมสัณฐาน (The Second Isomorphism Theorem)

ถ้า N และ H เป็นกรุปย่อยปรกติของกรุป G ซึ่ง $N \subseteq H$ แล้ว $\frac{G/N}{H/N} \cong \frac{G}{H}$

**บทพิสูจน์** ให้ N และ H เป็นกรุปย่อยปรกติของกรุป G ซึ่ง $N \subseteq H$ และให้ $\eta$ เป็นสาทิสสัณฐานธรรมชาติจาก G ไปทั่วถึง $\frac{G}{N}$ แล้วเพราะ H เป็นกรุปย่อยปรกติของ G ดังนั้นโดยบทแทรก 7.1.7 จะได้ว่า $\eta(H)$ เป็นกรุปย่อยปรกติของ $\frac{G}{N}$ และโดยบทแทรก 7.3.8 จะได้ว่า $\eta(H) = \frac{H}{N}$ และเพราะว่า $\ker\eta = N \subseteq H$ เราจะได้โดยทฤษฎีบท 7.4.3 ว่า $\frac{G}{H} \cong \frac{G/N}{\eta(H)} = \frac{G/N}{H/N}$ ดังต้องการ $\square$

## แบบฝึกหัด 7.4

1. ให้ G และ H เป็นกรุป J และ K เป็นกรุปย่อยปรกติของ G และ H ตามลำดับ จงพิสูจน์ว่า
   1.1 ฟังก์ชัน f ซึ่งกำหนดการส่งโดย $f(x, y) = (xJ, yK)$ เป็นสาทิสสัณฐานจาก $G \times H$ ไปทั่วถึง $\frac{G}{J} \times \frac{H}{K}$
   1.2 $\frac{G \times H}{J \times K} \cong \frac{G}{J} \times \frac{H}{K}$

2. ให้ H และ K เป็นกรุปย่อยปรกติของกรุป G โดยที่ $H \subseteq K$ และนิยาม $\alpha : \frac{G}{H} \to \frac{G}{K}$ โดย $\alpha(aH) = aK$ จงพิสูจน์ว่า
   2.1 $\alpha$ เป็นฟังก์ชันและเป็นสาทิสสัณฐานชนิดทั่วถึง
   2.2 $\ker\alpha = \frac{K}{H}$
   2.3 สรุปผลที่ได้จากการพิสูจน์ข้อ 2.1 และ 2.2

3. ให้ G และ H เป็นกรุป จงพิสูจน์ว่าถ้า J เป็นกรุปย่อยปรกติของ G และ K เป็นกรุปย่อยปรกติของ H แล้ว $\frac{G \times H}{J \times K} \cong \frac{G}{J} \times \frac{H}{K}$ [ข้อแนะนำ : พิสูจน์ว่าฟังก์ชัน $f : (x, y) \to (Jx, Ky)$ เป็นสาทิสสัณฐาน พร้อมกับหาส่วนกลางของ f ]

4. ให้ G เป็นกรุป H, $H_1$, K และ $K_1$ เป็นกรุปย่อยของ G จงพิสูจน์ว่าถ้า $H_1$ เป็นกรุปย่อยปรกติของ H และ $K_1$ เป็นกรุปย่อยปรกติของ K แล้ว $\frac{(H \cap K)H_1}{(H \cap K_1)H_1} \cong \frac{(H \cap K)K_1}{(H_1 \cap K)K_1}$

# บทที่ 8

# กรุปผลคูณตรง

# DIRECT PRODUCT OF GROUPS

การศึกษาโครงสร้างของกรุปโดยผ่านทางกรุปผลคูณตรงเป็นวิธีการศึกษาโครงสร้างเชิงพีชคณิตอีกวิธีหนึ่งซึ่งแตกต่างจากที่ศึกษามาในบทก่อนๆ กรุปผลคูณตรงที่เราจะศึกษาในบทนี้มีการสร้างอยู่สองลักษณะ กรุปผลคูณตรงแบบที่หนึ่งเป็นกรุปซึ่งเราสร้างขึ้นให้สมสัณฐานกับกรุปที่กำหนดให้โดยสร้างจากกรุปย่อยของกรุปที่กำหนดนั้นในลักษณะแบบเดียวกันกับการกระจายจำนวนเต็มออกในรูปผลคูณของตัวประกอบหรือตัวหารของจำนวนนั้น ทำให้เราเห็นโครงสร้างของกรุปได้ง่ายขึ้น กรุปผลคูณตรงแบบที่สองเป็นกรุปที่สร้างจากผลคูณคาร์ทีเซียนของกรุปซึ่งได้แนะนำกรุปผลคูณตรงแบบที่สองของกรุปสองกรุปไว้แล้วในตัวอย่าง 3.1.12 ในบทนี้เราจะศึกษาสมบัติของกรุปผลคูณตรงทั้งสองแบบ และแสดงความสัมพันธ์กันของกรุปผลคูณตรงทั้งสองแบบ

## 8.1 กรุปผลคูณตรงภายใน

พิจารณากรุปย่อย H และ K ของกรุป G โดยบทนิยาม 3.4.19 จะได้ว่า HK เป็นเซตที่ประกอบด้วยสมาชิกของ G ในรูป hk เมื่อ $h \in H$ และ $k \in K$ ตามลำดับ แต่ HK อาจจะเป็นหรือไม่เป็นกรุปย่อยของ G ก็ได้ แต่ถ้าทั้ง H และ K เป็นกรุปย่อยปรกติของ G แล้ว HK จะเป็นกรุปย่อยปรกติของ G ด้วย ในหัวข้อนี้เราสนใจศึกษาผลคูณ HK ในกรณีที่ $G = HK$ และ $H \cap K = \{e\}$

8.1.1 **บทนิยาม** ให้ H และ K เป็นกรุปย่อยปรกติของกรุป G เรากล่าวว่า G เป็น *กรุปผลคูณตรงภายใน (internal direct product)* ของ H และ K ถ้า $G = HK$ และ $H \cap K = \{e\}$ เมื่อ e แทนเอกลักษณ์ของ G และเขียนแทนด้วยสัญลักษณ์ $H \otimes K$

8.1.2 **ตัวอย่าง** กรุปไคลน์-4 $K_4 = \left\langle a,b \middle| a^2 = b^2 = e, ab = ba \right\rangle = \{e, a, b, ab\}$ เป็นกรุปอาบีเลียน ดังนั้นกรุปย่อย $H = \langle a \rangle$ และ $K = \langle b \rangle$ ต่างเป็นกรุปย่อยปรกติของ $K_4$ โดยที่ $K_4 = HK$ และ $H \cap K = \{e\}$ ดังนั้น $K_4 = H \otimes K$ เป็นกรุปผลคูณตรงภายในของกรุปย่อยวัฏจักรอันดับสอง

○

8.1.3 **ตัวอย่าง** ให้ $G = \langle a \rangle$ เป็นกรุปวัฏจักรอันดับอนันต์และ H และ K เป็นกรุปย่อย H ของ G ซึ่งไม่ใช่ G และ {e} แล้ว H และ K เป็นกรุปย่อยวัฏจักร H ของ G ดังนั้นจะมีจำนวนเต็ม $m > 1$ และ $n > 1$ ซึ่ง $H = \langle a^m \rangle$ และ $K = \langle a^n \rangle$ ทำให้ได้ $a^{mn} \in H \cap K$ ทั้งนี้เพราะ $a^{mn} = (a^m)^n \in H$ และ $a^{mn} = (a^n)^m \in K$ แต่เพราะ $G = \langle a \rangle$ เป็นกรุปอันดับอนันต์ ดังนั้น $a^k \neq e$ สำหรับทุกๆ จำนวนเต็ม k ทำให้ $a^{mn} \neq e$ ซึ่งแสดงว่า $H \cap K \neq \{e\}$

เพราะฉะนั้น $G \neq H \otimes K$ ไม่ว่า H และ K จะเป็นกรุปย่อยใดๆ ของ G นั่นคือ G ไม่เป็นกรุปผลคูณภายใน ❍

เมื่อมีทั้งตัวอย่างของกรุปผลคูณภายในและกรุปที่ไม่เป็นกรุปผลคูณภายใน เราจึงควรมีเกณฑ์สำหรับพิจารณาว่ากรุปใดเป็นกรุปผลคูณภายใน

8.1.4 **ทฤษฎีบท** ให้ H และ K เป็นกรุปย่อยของกรุป G แล้ว G เป็นกรุปผลคูณตรงภายในของ H และ K ก็ต่อเมื่อ

1. แต่ละสมาชิก x ใน G เขียนได้เพียงวิธีเดียวในรูป $x = hk$ เมื่อ $h \in H$ และ $k \in K$ และ
2. $hk = kh$ สำหรับทุกๆ $h \in H$ และ $k \in K$

**บทพิสูจน์** ให้ $G = H \otimes K$ แล้ว $G = HK$ ดังนั้นแต่ละสมาชิก x ใน G เขียนได้ในรูป $x = hk$ เมื่อ $h \in H$ และ $k \in K$ จึงเหลือการพิสูจน์ข้อ 1 เพียงแสดงว่าแต่ละสมาชิก x ใน G เขียนได้ในรูปนี้เพียงวิธีเดียว โดยสมมติให้ $x \in G$ โดยที่ $x = hk$ และ $x = h_1k_1$ เมื่อ $h, h_1 \in H$ และ $k, k_1 \in K$ แล้ว $hk = h_1k_1$ ซึ่งสมมูลกับ $h^{-1}h_1 = kk_1^{-1}$ และเราสังเกตว่า $h^{-1}h_1 \in H$ และ $kk_1^{-1} \in K$ ดังนั้น $h^{-1}h_1 = kk_1^{-1} \in H \cap K = \{e\}$ ซึ่งทำให้ได้ $h^{-1}h_1 = kk_1^{-1} = e$ นั่นคือ $h = h_1$ และ $k = k_1$

ในการพิสูจน์ข้อ 2 ให้ $h \in H$ และ $k \in K$ แล้วเพราะ H และ K เป็นกรุปย่อยปรกติของกรุป G ดังนั้น $hkh^{-1} \in K$ และ $kh^{-1}k^{-1} \in H$ ทำให้ได้ $(hkh^{-1})k^{-1} \in K$ และ $h(kh^{-1}k^{-1}) \in H$ ซึ่งแสดงว่า $hkh^{-1}k^{-1} \in H \cap K = \{e\}$ จึงได้ $hkh^{-1}k^{-1} = e$ ซึ่งสมมูลกับ $hk = kh$

สำหรับการพิสูจน์บทกลับสมมติให้เงื่อนไขข้อ 1 และข้อ 2 ของทฤษฎีบทเป็นจริง แล้วโดยข้อ 1 จะได้ว่า $G = HK$ เราจึงจะแสดงว่า H เป็นกรุปย่อยปรกติของกรุป G โดยให้ $h \in H$ และ $x \in G$ แล้วจะมี $h_1 \in H$ และ $k_1 \in K$ ซึ่ง $x = h_1k_1$ และโดยเงื่อนไขข้อ 2 จะได้ว่า

$$xhx^{-1} = (h_1k_1)h(h_1k_1)^{-1} = (h_1k_1)(hk_1^{-1})h_1^{-1} = h_1(k_1k_1^{-1})(hh_1^{-1}) = h_1hh_1^{-1} \in H$$

และเราสามารถแสดงในทำนองเดียวกันได้ว่า K เป็นกรุปย่อยปรกติของกรุป G สุดท้ายเราจะแสดงว่า $H \cap K = \{e\}$ โดยให้ $x \in H \cap K$ แต่เพราะว่า $x \in HK$ ดังนั้น x เขียนได้เพียงวิธีเดียวในรูป $x = hk$ เมื่อ $h \in H$ และ $k \in K$ แต่ $ex = x = xe$ เป็นวิธีเขียนในรูปดังกล่าว จึงทำให้ได้ว่า $x = e$ ❐

ทฤษฎีบทต่อไป เราจะแสดงความสัมพันธ์ของกรุปผลคูณตรงภายในกับกรุปผลหาร

8.1.5 **ทฤษฎีบท** ให้ H และ K เป็นกรุปย่อยปรกติของกรุป G ถ้า $G = H \otimes K$ แล้ว $\frac{G}{H} \cong K$ และ $\frac{G}{K} \cong H$

**บทพิสูจน์** เราจะพิสูจน์ว่า $\frac{G}{H} \cong K$ เท่านั้น สำหรับ $\frac{G}{K} \cong H$ พิสูจน์ในทำนองเดียวกัน

ให้ $\theta : G \longrightarrow K$ นิยามโดย $\theta(x) = k$ สำหรับทุกๆ $x \in G$ โดยที่ $x = hk$ เมื่อ $h \in H$ และ $k \in K$ เนื่องจากแต่ละ $x \in G$ เขียนได้เพียงวิธีเดียวในรูป $x = hk$ ดังนั้น $\theta$ เป็นฟังก์ชันและเพราะว่าแต่ละ $k \in K$ เขียนได้ในรูป $k = ek$ โดยพิจารณาว่า $e \in H$ จึงได้ว่า $\theta$ เป็นฟังก์ชันทั่วถึง ต่อไปจะแสดงว่า $\theta$ เป็นสาทิสสัณฐาน ให้ $x, y \in G$ แล้วจะมี $h, h_1 \in H$ และ $k, k_1 \in K$ ซึ่ง $x = hk$ และ $y = h_1k_1$ ทำให้ได้ $xy = (hk)(h_1k_1) = h(kh_1)k_1 = h(h_1k)k_1 = (hh_1)(kk_1)$ เพราะฉะนั้น

$$\theta(xy) = kk_1 = \theta(x)\,\theta(y)$$

และสุดท้าย เราจะได้ว่า

$$x = hk \in \ker\theta \iff \theta(x) = k = e \iff x = h \in H$$

ซึ่งแสดงว่า $\ker\theta = H$ ดังนั้นโดยทฤษฎีบทหลักมูลของสาทิสสัณฐาน จะได้ $\frac{G}{H} \cong K$ ❐

8.1.6 **บทแทรก** ให้ G เป็นกรุปจำกัดและ H และ K เป็นกรุปย่อยปรกติของ G ถ้า $G = H \otimes K$ แล้ว $|G| = |H||K|$

**บทพิสูจน์** โดยทฤษฎีบทลากรองจ์และทฤษฎีบท 8.1.5 จะได้ว่า $|K| = \left|\frac{G}{H}\right| = [G : H] = \frac{|G|}{|H|}$ ทำให้ได้ $|G| = |H||K|$ ❐

8.1.7 **บทแทรก** ถ้า H และ K เป็นกรุปย่อยจำกัดของกรุป G แล้ว $|HK| = \frac{|H||K|}{|H \cap K|}$

**บทพิสูจน์** เนื่องจากแต่ละครั้งของการนำสมาชิกใน H มาคูณกับสมาชิกใน K จะได้สมาชิกใน HK และโดยกลับกัน ดังนั้นจำนวนสมาชิกของ HK จะไม่เกิน $|H||K|$ แต่สำหรับแต่ละ $x \in H \cap K$ จะได้ว่า $hk = (hx)(x^{-1}k)$ สำหรับทุกๆ $hk \in HK$ โดยสังเกตต่อได้ว่า $hx \in H$ และ $x^{-1}k \in K$ ซึ่งแสดงว่าการนับจำนวนสมาชิกใน HK เกิดการนับซ้ำไม่น้อยกว่า $|H \cap K|$ ครั้ง และถ้า hk และ $h_1k_1$ เป็นสมาชิกใน HK ที่เกิดการนับซ้ำโดยที่ $h \neq h_1$ และ $k \neq k_1$ ก็จะได้ว่า $h^{-1}h_1 = kk_1^{-1} \in H \cap K$ นั่นคือการนับซ้ำเกิดขึ้นเฉพาะกับสมาชิกของ $H \cap K$ ซึ่งแสดงว่าจำนวนครั้งของการนับซ้ำจะไม่เกิน $|H \cap K|$ จึงสรุปได้ว่าจำนวนครั้งของการนับซ้ำเท่ากับ $|H \cap K|$ เพราะฉะนั้นจำนวนสมาชิกของ HK ที่ต่างกันทั้งหมดเท่ากับจำนวนสมาชิกที่นับได้หารด้วยจำนวนสมาชิกที่ถูกนับซ้ำ ทำให้ได้ $|HK| = \dfrac{|H||K|}{|H \cap K|}$ ❐

8.1.8 **บทแทรก** ให้ G เป็นกรุปจำกัด H และ K เป็นกรุปย่อยปรกติของ G ซึ่ง $|G| = |H||K|$ ถ้า $G = HK$ หรือ $H \cap K = \{e\}$ แล้ว $G = H \otimes K$

**บทพิสูจน์** สมมติให้เงื่อนไขของทฤษฎีบทเป็นจริงและเกิดกรณี $G = HK$ แล้วโดยบทแทรก 8.1.7 จะได้ว่า $|H||K| = |G| = |HK| = \dfrac{|H||K|}{|H \cap K|}$ ทำให้ได้ $|H \cap K| = 1$ นั่นคือ $H \cap K = \{e\}$ ดังนั้นเราจะได้เงื่อนไขของบทนิยาม 8.1.1 ทำให้ได้ว่า $G = H \otimes K$

สำหรับกรณีที่เกิด $H \cap K = \{e\}$ เราก็จะได้ว่า $|H \cap K| = 1$ ทำให้ได้โดยบทแทรก 8.1.7 ว่า $|HK| = \dfrac{|H||K|}{|H \cap K|} = |H||K| = |G|$ แต่ G เป็นกรุปจำกัดและ HK เป็นกรุปย่อยของ G ดังนั้น $G = HK$ เราจึงได้เงื่อนไขของบทนิยาม 8.1.1 ทำให้ได้ว่า $G = H \otimes K$ ❐

8.1.9 **ตัวอย่าง** ในกรุป $Z_{10}$ จะมีกรุปย่อยปรกติซึ่งไม่ใช่ $\{e\}$ และ $Z_{10}$ อยู่เพียง 2 กรุปย่อยเท่านั้น คือ $H = \{\bar{0}, \bar{5}\}$ และ $K = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ ซึ่งเราสังเกตว่า $|Z_{10}| = 10 = (2)(5) = |H||K|$ นอกจากนี้ $H \cap K = \{\bar{0}\}$ ทำให้เราสรุปได้โดยบทแทรก 8.1.8 ว่า $Z_{10} = H \otimes K$ ❍

ต่อไปเราจะกล่าวถึงกรุปผลคูณตรงภายในของกรุปย่อยปรกติจำนวน n กรุปย่อยเมื่อ n เป็นจำนวนนับใดๆ ซึ่งจะเป็นการวางนัยทั่วไปของผลการศึกษาในกรณีกรุปผลคูณตรงภายในของกรุปย่อยปรกติ 2 กรุปย่อย

8.1.10 **บทนิยาม** ให้ n เป็นจำนวนเต็มบวกและ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปรกติของกรุป G เรากล่าวว่า G เป็น *กรุปผลคูณตรงภายใน ( internal direct product )* ของ $G_1, G_2, ..., G_n$ และเขียนแทนด้วยสัญลักษณ์ $G_1 \otimes G_2 \otimes ... \otimes G_n$ ถ้า

1. $G = G_1G_2 ...G_n$ [นั่นคือสำหรับแต่ละ $x \in G$ เขียนได้ในรูปผลคูณ $x = g_1g_2 \cdots g_n$ โดยที่ $g_i \in G_i$ ทุกๆ $i = 1, 2, \ldots, n$ ]

และ 2. $G_i \cap \left(G_1G_2 ...G_{i-1}G_{i+1}...G_n\right) = \{e\}$ สำหรับแต่ละ $1 \le i \le n$

8.1.11 **ทฤษฎีบท** ให้ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปกติของกรุป G แล้ว G เป็นผลคูณตรงภายในของ $G_1, G_2, ..., G_n$ ก็ต่อเมื่อ

1. $G_i \cap G_j = \{e\}$ สำหรับทุกๆ $1 \le i \ne j \le n$
2. $g_ig_j = g_jg_i$ สำหรับทุกๆ $g_i \in G_i$ และ $g_j \in G_j$ และ $1 \le i \ne j \le n$

**บทพิสูจน์** ให้ G เป็นผลคูณภายในของกรุปย่อยปกติ $G_1, G_2, ..., G_n$ ของ G

1. ให้ $1 \le i < j \le n$ และให้ $k \in G_i \cap G_j$ แล้ว $k \in G_i$ และ $k \in G_j$ ให้ $e_s = e$ ทุกๆ $s = 1,2,...,n$ แล้ว $k = e_1e_2...e_{i-1}e_{i+1}...e_{j-1}ke_{j+1}...e_n \in G_1G_2...G_{i-1}G_{i+1}...G_n$ ดังนั้น $k \in G_i \cap \left(G_1G_2...G_{i-1}G_{i+1}...G_n\right)$ ทำให้ได้ $k = e$

2. ให้ $1 \le i, j \le n$ และให้ $g_i \in G_i$ และ $g_j \in G_j$ แล้วเพราะว่า $g_i^{-1} \in G_i$ และ $g_j, g_j^{-1} \in G$ และ $G_i$ เป็นกรุปย่อยปรกติของ G ดังนั้น $g_jg_i^{-1}g_j^{-1} \in G_i$ ให้ $s_i = g_jg_i^{-1}g_j^{-1} \in G_i$ แล้ว $g_ig_jg_i^{-1}g_j^{-1} = g_i\left(g_jg_i^{-1}g_j^{-1}\right) = g_is_i \in G_i$ และโดยการพิสูจน์ในทำนองเดียวกันจะได้ $g_ig_jg_i^{-1}g_j^{-1} \in G_j$ ทำให้ได้ $g_ig_jg_i^{-1}g_j^{-1} \in G_i \cap G_j = \{e\}$ ดังนั้น $g_ig_jg_i^{-1}g_j^{-1} = e$ ซึ่งทำให้ได้ $g_ig_j = g_jg_i$

สำหรับการพิสูจน์บทกลับ จะขอละไว้เป็นแบบฝึกหัด ❐

ต่อไปจะแสดงว่าแต่ละสมาชิกของกรุปผลคูณตรงภายในของ $G_1, G_2, ..., G_n$ เขียนได้ในรูปผลคูณ $g = g_1g_2 ...g_n$ โดยที่ $g_i \in G_i$ สำหรับทุกๆ $1 \le i \le n$ ได้เพียงแบบเดียวเท่านั้น

**8.1.12 บทแทรก** ถ้า G เป็นกรุปผลคูณตรงภายในของกรุปย่อยปกติ $G_1, G_2, \ldots, G_n$ ของ G แล้วแต่ละสมาชิก x ใน G เขียนได้เพียงวิธีเดียวในรูป $x = g_1 g_2 \ldots g_n$ เมื่อ $g_i \in G_i$ สำหรับทุกๆ $i = 1, 2, \ldots, n$

**บทพิสูจน์** ให้ G เป็นกรุปผลคูณตรงภายในของกรุปย่อยปกติ $G_1, G_2, \ldots, G_n$ ของ G และให้ $x \in G$ และสมมติมี $g_i, h_i \in G_i$ เมื่อ $i = 1, 2, \ldots, n$ ซึ่ง $x = g_1 g_2 \ldots g_n = h_1 h_2 \ldots h_n$ แล้ว

$$\begin{aligned} g_i &= (g_1 g_2 \ldots g_{i-1})^{-1}(h_1 h_2 \ldots h_n)(g_{i+1} g_{i+2} \ldots g_n)^{-1} \\ &= g_{i-1}^{-1} g_{i-2}^{-1} \ldots g_1^{-1} h_1 h_2 \ldots h_n g_n^{-1} g_{n-1}^{-1} \ldots g_{i+1}^{-1} \\ &= h_i \left(h_1 g_1^{-1}\right)\left(h_2 g_2^{-1}\right) \ldots \left(h_{i-1} g_{i-1}^{-1}\right)\left(h_{i+1} g_{i+1}^{-1}\right) \ldots \left(h_n g_n^{-1}\right) \end{aligned}$$

ทำให้ได้ว่า $g_i h_i^{-1} = \left(h_1 g_1^{-1}\right)\left(h_2 g_2^{-1}\right) \ldots \left(h_{i-1} g_{i-1}^{-1}\right)\left(h_{i+1} g_{i+1}^{-1}\right) \ldots \left(h_n g_n^{-1}\right)$ ซึ่งแสดงว่า $g_i h_i^{-1} \in G_1 G_2 \ldots G_{i-1} G_{i+1} \ldots G_n$ และ $g_i h_i^{-1} \in G_i$ เพราะฉะนั้น $g_i h_i^{-1} \in G_i \cap (G_1 G_2 \ldots G_{i-1} G_{i+1} \ldots G_n)$ ดังนั้น $g_i h_i^{-1} = e$ เพราะฉะนั้น $g_i = h_i$ ❐

## แบบฝึกหัด 8.1

1. จงแสดงว่ากรุป $Z_{15}$ เป็นกรุปผลคูณตรงภายใน แต่กรุป $G_S$ ไม่เป็นกรุปผลคูณตรงภายใน
2. จงแสดงว่ากรุป $S_3$ ไม่เป็นกรุปผลคูณตรงภายใน [ข้อแนะนำ : แสดงว่าผลคูณตรงภายในของกรุปอันดับ 2 กับกรุปอันดับ 3 จะเป็นกรุปวัฏจักร ]
3. จงแสดงว่าถ้า H และ K เป็นกรุปย่อยปรกติของกรุป G ซึ่ง $|G| = |H||K|$ และ $(|H|, |K|) = 1$ แล้ว $G = H \otimes K$
4. ให้ $\theta$ เป็นสาทิสสัณฐานจากกรุป G ไปทั่วถึงกรุป $\overline{G}$ และ H เป็นกรุปย่อยปรกติของ G จงแสดงว่าถ้าฟังก์ชันกำกัดของ $\theta$ ลงบน H เป็นสมสัณฐานจาก H ไปทั่วถึง $\overline{G}$ แล้ว $G = H \otimes \ker\theta$
5. ให้ H และ K เป็นกรุปย่อยปรกติของกรุป G โดยที่ $G = H \otimes K$ จงพิสูจน์ว่าถ้า N เป็นกรุปย่อยปรกติของ H (หรือของ K) แล้ว N เป็นกรุปย่อยปรกติของ G
6. จงพิสูจน์บทกลับของทฤษฎีบท 8.1.11

## 8.2 กรุปผลคูณตรงภายนอก

ถ้า G และ H เป็นกรุปแล้วตัวอย่าง 3.1.12 ได้แสดงการนิยามการดำเนินการตามองค์ประกอบบนผลคูณคาร์ทีเซียนของ G และ H และพิสูจน์ได้ว่า G×H เป็นกรุปภายใต้การดำเนินการตามองค์ประกอบนั้น และเรียกว่ากรุปผลคูณตรงของ G และ H ในหัวข้อนี้เราจะขยายแนวคิดนี้ในกรณีทั่วไป กล่าวคือจะสร้างกรุปใหม่จากกรุปจำนวนจำกัดกรุป $G_1, G_2, \ldots, G_n$ บนผลคูณคาร์ทีเซียน $G_1 \times G_2 \times \ldots \times G_n$ โดยการดำเนินการตาม

**8.2.1 ทฤษฎีบท** ให้ $G_1, G_2, \ldots, G_n$ เป็นกรุปและ *ผลคูณคาร์ทีเซียน (cartesian product)* $G_1 \times G_2 \times \ldots \times G_n$ ของ $G_1, G_2, \ldots, G_n$ นิยามโดย

$$G_1 \times G_2 \times \ldots \times G_n = \left\{ \left( g_1, g_2, \ldots, g_n \right) \middle| \, g_i \in G_i ; i = 1,2,\ldots,n \right\}$$

และให้ $\circ : \left( G_1 \times G_2 \times \ldots \times G_n \right) \times \left( G_1 \times G_2 \times \ldots \times G_n \right) \to G_1 \times G_2 \times \ldots \times G_n$ นิยามโดย

$$\left( g_1, g_2, \ldots, g_n \right) \circ \left( h_1, h_2, \ldots, h_n \right) = \left( g_1 h_1, g_2 h_2, \ldots, g_n h_n \right)$$

สำหรับทุกๆ $\left( g_1, g_2, \ldots, g_n \right)$ และ $\left( h_1, h_2, \ldots, h_n \right)$ ใน $G_1 \times G_2 \times \ldots \times G_n$ ซึ่งจะเรียก $\circ$ ว่า *การดำเนินการตามองค์ประกอบ(componentwise operation)* แล้ว $\left( G_1 \times G_2 \times \ldots \times G_n ; \circ \right)$ เป็นกรุป

**บทพิสูจน์** ให้ $G_1, G_2, \ldots, G_n$ เป็นกรุป

1. ให้ $\left( g_1, g_2, \ldots, g_n \right), \left( h_1, h_2, \ldots, h_n \right)$ และ $\left( k_1, k_2, \ldots, k_n \right)$ เป็นสมาชิกของ $G_1 \times G_2 \times \ldots \times G_n$ แล้ว

$$\begin{aligned}
&\left( \left( g_1, g_2, \ldots, g_n \right) \circ \left( h_1, h_2, \ldots, h_n \right) \right) \circ \left( k_1, k_2, \ldots, k_n \right) \\
&\qquad = \left( g_1 h_1, g_2 h_2, \ldots, g_n h_n \right) \circ \left( k_1, k_2, \ldots, k_n \right) \\
&\qquad = \left( \left( g_1 h_1 \right) k_1, \left( g_2 h_2 \right) k_2, \ldots, \left( g_n h_n \right) k_n \right) \\
&\qquad = \left( g_1 \left( h_1 k_1 \right), g_2 \left( h_2 k_2 \right), \ldots, g_n \left( h_n k_n \right) \right)
\end{aligned}$$

$$=\left(g_1, g_2, \ldots, g_n\right) \circ \left(h_1k_1, h_2k_2, \ldots, h_nk_n\right)$$
$$=\left(g_1, g_2, \ldots, g_n\right) \circ \left(\left(h_1, h_2, \ldots, h_n\right) \circ \left(k_1, k_2, \ldots, k_n\right)\right)$$

ดังนั้น $\circ$ สอดคล้องสมบัติการเปลี่ยนหมู่บน $G_1 \times G_2 \times \ldots \times G_n$

2. ให้ $e_i$ เป็นเอกลักษณ์ของ $G_i$ สำหรับ $i = 1, 2, \ldots, n$ แล้ว $\left(e_1, e_2, \ldots, e_n\right)$ $\in G_1 \times G_2 \times \ldots \times G_n$ ให้ $\left(g_1, g_2, \ldots, g_n\right) \in G_1 \times G_2 \times \ldots \times G_n$ แล้ว

$$\left(g_1, g_2, \ldots, g_n\right) \circ \left(e_1, e_2, \ldots, e_n\right) = \left(g_1e_1, g_2e_2, \ldots, g_ne_n\right) = \left(g_1, g_2, \ldots, g_n\right)$$
$$= \left(e_1g_1, e_2g_2, \ldots, e_ng_n\right) = \left(e_1, e_2, \ldots, e_n\right) \circ \left(g_1, g_2, \ldots, g_n\right)$$

ดังนั้น $\left(e_1, e_2, \ldots, e_n\right)$ เป็นเอกลักษณ์ของ $G_1 \times G_2 \times \ldots \times G_n$ ภายใต้ $\circ$

3. ให้ $\left(g_1, g_2, \ldots, g_n\right) \in G_1 \times G_2 \times \ldots \times G_n$ แล้ว $g_i \in G_i$ ทุกๆ $i = 1, 2, \ldots, n$ ทำให้ $g_i^{-1} \in G_i$ ทุกๆ $i = 1, 2, \ldots, n$ ดังนั้น $\left(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}\right) \in G_1 \times G_2 \times \ldots \times G_n$ โดยที่

$$\left(g_1, g_2, \ldots, g_n\right) \circ \left(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}\right) = \left(g_1g_1^{-1}, g_2g_2^{-1}, \ldots, g_ng_n^{-1}\right)$$
$$= \left(e_1, e_2, \ldots, e_n\right) = \left(g_1^{-1}g_1, g_2^{-1}g_2, \ldots, g_n^{-1}g_n\right)$$
$$= \left(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}\right) \circ \left(g_1, g_2, \ldots, g_n\right)$$

ดังนั้น $\left(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}\right)$ เป็นตัวผกผันของ $\left(g_1, g_2, \ldots, g_n\right)$

เพราะฉะนั้น $\left(G_1 \times G_2 \times \ldots \times G_n ; \circ\right)$ เป็นกรุป $\square$

8.2.2 **บทนิยาม** เราเรียกกรุป $\left(G_1 \times G_2 \times \ldots \times G_n ; \circ\right)$ ในทฤษฎีบท 8.2.1 ว่า *ผลคูณตรง (direct product )* ของกรุป $G_1, G_2, \ldots, G_n$ และกรุปซึ่งสมสัณฐานกับผลคูณตรงของกรุป $G_1, G_2, \ldots, G_n$ ว่า *กรุปผลคูณตรงภายนอก (external direct product )* ของ $G_1, G_2, \ldots, G_n$

**ข้อสังเกต** ขอให้สังเกตว่ากรุปผลคูณตรงภายนอก $G_1 \times G_2 \times \ldots \times G_n$ สมสัณฐานกับกรุปผลคูณตรงภายนอก $G_{\sigma(1)} \times G_{\sigma(2)} \times \ldots \times G_{\sigma(n)}$ ไม่ว่า $\sigma$ จะเป็นวิธีเรียงสับเปลี่ยนใดๆ บนเซต $\{1, 2, \ldots, n\}$ ตัวอย่างเช่นในกรณี n =2 เราจะได้ $G_1 \times G_2 \cong G_2 \times G_1$ หรือกรณี n =3 เราจะได้ $G_1 \times G_2 \times G_3 \cong G_2 \times G_1 \times G_3 \cong G_3 \times G_2 \times G_1 \cong G_1 \times G_3 \times G_2 \cong G_2 \times G_3 \times G_1 \cong G_3 \times G_1 \times G_2$ เป็นต้น ดังนั้นเราจึงกล่าวถึงกรุปผลคูณตรงภายนอกของ $G_1, G_2, \ldots, G_n$ โดยไม่กล่าวถึงอันดับของกรุป $G_1, G_2, \ldots, G_n$

เราจะมีคำถามเกิดขึ้นในขณะนี้ก็คือ สำหรับกรุป $G_1, G_2, \ldots, G_n$ จะมีกรุป G หรือไม่ ซึ่ง G เป็นกรุปผลคูณตรงภายในของกรุปย่อยปรกติ $H_1, H_2, \ldots, H_n$ ของ G โดยที่ $H_i \cong G_i$ สำหรับทุกๆ $1 \le i \le n$ ทฤษฎีบทต่อไปจะตอบคำถามเหล่านี้

8.2.3 **ทฤษฎีบท** ให้ n เป็นจำนวนเต็มบวกและให้ $G_1, G_2, \ldots, G_n$ เป็นกรุป แล้วสำหรับแต่ละ $1 \le i \le n$ จะมีกรุปย่อยปรกติ $\overline{G_i}$ ของกรุป $G_1 \times G_2 \times \ldots \times G_n$ ซึ่ง

1. $\overline{G_i}$ สมสัณฐานกับ $G_i$ ทุกๆ $1 \le i \le n$
2. $\overline{G_i} \cap \left(\overline{G_1}\,\overline{G_2} \ldots \overline{G_{i-1}}\,\overline{G_{i+1}} \ldots \overline{G_n}\right) = \left\{\left(e_1, e_2, \ldots, e_n\right)\right\}$ สำหรับแต่ละ $1 \le i \le n$
3. $G_1 \times G_2 \times \ldots \times G_n = \overline{G_1}\,\overline{G_2} \ldots \overline{G_n}$

**บทพิสูจน์** สำหรับแต่ละ $i = 1, 2, \ldots, n$ ให้ $\overline{G_i} = \left\{\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right) \middle| g_i \in G_i\right\}$ แล้วสำหรับทุกๆ $i = 1, 2, \ldots, n$ จะได้ว่า $\overline{g_i} \in \overline{G_i}$ ก็ต่อเมื่อ $\overline{g_i} = \left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right)$ สำหรับบาง $g_i \in G_i$ เราจะพิสูจน์ว่า $\overline{G_i}$ เป็นกรุปย่อยปรกติของ $G_1 \times G_2 \times \ldots \times G_n$ สำหรับทุกๆ $i = 1, 2, \ldots, n$

ให้ $e_i$ เป็นเอกลักษณ์ของ $G_i$ สำหรับแต่ละ $i = 1, 2, \ldots, n$ แล้ว $\left(e_1, e_2, \ldots, e_n\right) \in \overline{G_i}$ ทำให้ $\overline{G_i} \ne \phi$ สำหรับทุกๆ $i = 1, 2, \ldots, n$

ให้ $i \in \{1, 2, \ldots, n\}$ และ $\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right), \left(e_1, e_2, \ldots, h_i, e_{i+1}, \ldots, e_n\right) \in \overline{G_i}$ แล้ว $\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right)\left(e_1, e_2, \ldots, h_i, e_{i+1}, \ldots, e_n\right) = \left(e_1, e_2, \ldots, g_i h_i, e_{i+1}, \ldots, e_n\right)$

$\in \overline{G_i}$ ดังนั้น $\overline{G_i}$ มีสมบัติปิดภายใต้การดำเนินการของ $G_1 \times G_2 \times \ldots \times G_n$ และเพราะว่า $g_i^{-1} \in G_i$ ทำให้มี $\left(e_1, e_2, \ldots, g_i^{-1}, e_{i+1}, \ldots, e_n\right) \in \overline{G_i}$ ซึ่งทำให้

$$\begin{aligned}
&\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right)\left(e_1, e_2, \ldots, g_i^{-1}, e_{i+1}, \ldots, e_n\right) \\
&\qquad = \left(e_1, e_2, \ldots, g_i g_i^{-1}, e_{i+1}, \ldots, e_n\right) = \left(e_1, e_2, \ldots, e_n\right) \\
&\qquad = \left(e_1, e_2, \ldots, g_i^{-1} g_i, e_{i+1}, \ldots, e_n\right) \\
&\qquad = \left(e_1, e_2, \ldots, g_i^{-1}, e_{i+1}, \ldots, e_n\right)\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right)
\end{aligned}$$

ดังนั้น $\left(e_1, e_2, \ldots, g_i^{-1}, e_{i+1}, \ldots, e_n\right)$ เป็นตัวผกผันของ $\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right)$ เพราะฉะนั้น $\overline{G_i}$ เป็นกรุปย่อยของ $G_1 \times G_2 \times \ldots \times G_n$

ต่อไปให้ $\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right) \in \overline{G_i}$ และให้ $\left(g_1, g_2, \ldots, g_n\right) \in G_1 \times G_2 \times \ldots \times G_n$ แล้ว

$$\begin{aligned}
&\left(g_1, g_2, \ldots, g_n\right)\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right)\left(g_1, g_2, \ldots, g_n\right)^{-1} \\
&\quad = \left(g_1, g_2, \ldots, g_n\right)\left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right)\left(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}\right) \\
&\quad = \left(g_1 e_1 g_1^{-1}, g_2 e_2 g_2^{-1}, \ldots, g_{i-1} e_{i-1} g_{i-1}^{-1}, g_i e_i g_i^{-1}, g_{i+1} e_{i+1} g_{i+1}^{-1}, \ldots, g_n e_n g_n^{-1}\right) \\
&\quad = \left(g_1 g_1^{-1}, g_2 g_2^{-1}, \ldots, g_{i-1} g_{i-1}^{-1}, g_i g_i^{-1}, g_{i+1} g_{i+1}^{-1}, \ldots, g_n g_n^{-1}\right) \\
&\quad = \left(e_1, e_2, \ldots, g_i, e_{i+1}, \ldots, e_n\right) \in \overline{G_i}
\end{aligned}$$

ดังนั้น $\left(g_1, g_2, \ldots, g_n\right)\overline{G_i}\left(g_1, g_2, \ldots, g_n\right)^{-1} \subseteq \overline{G_i}$ สำหรับทุกๆ $\left(g_1, g_2, \ldots, g_n\right) \in G_1 \times G_2 \times \ldots \times G_n$ เพราะฉะนั้น $\overline{G_i}$ เป็นกรุปย่อยปรกติของ $G_1 \times G_2 \times \ldots \times G_n$

1. เราจะพิสูจน์ว่า $\overline{G_i}$ สมสัณฐานกันกับ $G_i$ ทุกๆ $1 \le i \le n$

ให้ $i = 1, 2, \ldots, n$ และนิยาม $\alpha : \overline{G_i} \to G_i$ โดย $\alpha\left(e_1, e_2, \ldots, a_i, e_{i+1}, \ldots, e_n\right) = a_i$ สำหรับทุกๆ $a_i \in G_i$ แล้วเห็นได้ชัดว่า $\alpha$ เป็นฟังก์ชันและเป็นฟังก์ชันหนึ่งต่อหนึ่งและทั่วถึง นอกจากนี้

$$\alpha\left(\left(e_1,e_2,\ldots,a_i,e_{i+1},\ldots,e_n\right)\left(e_1,e_2,\ldots,b_i,e_{i+1},\ldots,e_n\right)\right)$$
$$=\left(e_1,e_2,\ldots,a_ib_i,e_{i+1},\ldots,e_n\right)=a_ib_i$$
$$=\alpha\left(e_1,e_2,\ldots,a_i,e_{i+1},\ldots,e_n\right)\alpha\left(e_1,e_2,\ldots,b_i,e_{i+1},\ldots,e_n\right)$$

สำหรับทุกๆ $\left(e_1,e_2,\ldots,a_i,e_{i+1},\ldots,e_n\right),\left(e_1,e_2,\ldots,b_i,e_{i+1},\ldots,e_n\right)\in\overline{G_i}$ ซึ่งแสดงว่า $\alpha$ เป็นสาทิสสัณฐาน เพราะฉะนั้น $\alpha$ เป็นสมสัณฐาน

2. $\overline{G_i}\cap\left(\overline{G_1}\,\overline{G_2}\ldots\overline{G_{i-1}}\,\overline{G_{i+1}}\ldots\overline{G_n}\right)=\left\{\left(e_1,e_2,\ldots,e_n\right)\right\}$ สำหรับแต่ละ $1\le i\le n$

ให้ $\left(g_1,g_2,\ldots,g_n\right)\in\overline{G_i}\cap\left(\overline{G_1}\,\overline{G_2}\ldots\overline{G_{i-1}}\,\overline{G_{i+1}}\ldots\overline{G_n}\right)$ แล้ว $\left(g_1,g_2,\ldots,g_n\right)\in\overline{G_i}$ ทำให้ $\left(g_1,g_2,\ldots,g_n\right)=\left(e_1,e_2,\ldots,g_i,e_{i+1},\ldots,e_n\right)$ ดังนั้น $g_k=e_k$ สำหรับทุกๆ $1\le k\ne i\le n$ และเพราะ $\left(g_1,g_2,\ldots,g_n\right)=\left(e_1,e_2,\ldots,g_i,e_{i+1},\ldots,e_n\right)\in\overline{G_1}\,\overline{G_2}\ldots\overline{G_{i-1}}\,\overline{G_{i+1}}\ldots\overline{G_n}$ ดังนั้น สำหรับแต่ละ $1\le k\ne i\le n$ จะมี $\overline{g_k}=\left(e_1,e_2,\ldots,e_{k-1},g_k,e_{k+1},\ldots,e_n\right)\in\overline{G_k}$ ซึ่ง

$$\left(e_1,e_2,\ldots,g_i,e_{i+1},\ldots,e_n\right)=\overline{g_1}\,\overline{g_2}\ldots\overline{g_{i-1}}\,\overline{g_{i+1}}\ldots\overline{g_n}=\overline{g_1}\,\overline{g_2}\ldots\overline{g_{i-1}}\,\overline{e_i}\,\overline{g_{i+1}}\ldots\overline{g_n}$$
$$=\left(g_1,g_2,\ldots,g_{i-1},e_i,g_{i+1},\ldots,g_n\right)$$

ดังนั้น $g_k=e_k$ สำหรับทุกๆ $1\le k\le n$ ทำให้ได้ $\left(g_1,g_2,\ldots,g_n\right)=\left(e_1,e_2,\ldots,e_n\right)$

ซึ่งแสดงว่า $\overline{G_i}\cap\left(\overline{G_1}\,\overline{G_2}\ldots\overline{G_{i-1}}\,\overline{G_{i+1}}\ldots\overline{G_n}\right)=\left\{\left(e_1,e_2,\ldots,e_n\right)\right\}$ ทุกๆ $i=1,2,\ldots,n$

3. $G_1\times G_2\times\ldots\times G_n=\overline{G_1}\,\overline{G_2}\ldots\overline{G_n}$ เพราะว่า

$\left(g_1,g_2,\ldots,g_n\right)\in G_1\times G_2\times\ldots\times G_n\iff$

$$\left(g_1,g_2,\ldots,g_n\right)=\left(g_1,e_2,\ldots,e_n\right)\left(e_1,g_2,e_3,\ldots,e_n\right)\ldots\left(e_1,e_2,\ldots,g_n\right)=\overline{g_1}\,\overline{g_2}\ldots\overline{g_n}$$
$$\in\overline{G_1}\,\overline{G_2}\ldots\overline{G_n}\qquad\square$$

## แบบฝึกหัด 8.2

1. ให้ n เป็นจำนวนเต็มบวกและ $G_1, G_2, \ldots, G_n$ เป็นกรุป จงพิสูจน์ว่า
   1.1 $\left|\left(g_1, g_2, \ldots, g_n\right)\right|$ เท่ากับตัวคูณร่วมน้อยของ $\left|g_1\right|, \left|g_1\right|, \ldots, \left|g_1\right|$ สำหรับทุกๆ $\left(g_1, g_2, \ldots, g_n\right)$ ในกรุป $G_1 \times G_2 \times \ldots \times G_n$
   1.2 $G_1 \times G_2 \times \ldots \times G_n$ เป็นกรุปวัฏจักร ก็ต่อเมื่อ $\left|g_1\right|, \left|g_1\right|, \ldots, \left|g_1\right|$ เป็นจำนวนเฉพาะสัมพัทธ์
2. จงพิสูจน์ข้อสังเกตท้ายบทนิยาม 8.2.2
3. ให้ H และ K เป็นกรุปย่อยปรกติของกรุป G โดยที่ $G = H \otimes K$ จงพิสูจน์ว่าถ้า N เป็นกรุปย่อยปรกติของ H แล้ว $\frac{G}{N} \cong \frac{H}{N} \times K$ เป็นกรุปย่อยปรกติของ G

## 8.3 ความสัมพันธ์ของกรุปผลคูณตรงภายนอกและกรุปผลคูณตรงภายใน

เราควรจะมีคำถามว่า กรุปผลคูณตรงภายนอกและกรุปผลคูณตรงภายในมีความสัมพันธ์กันหรือไม่ อย่างไร ในหัวข้อนี้เราจะศึกษาเพื่อตอบคำถามนี้ว่า กรุปทั้งสองเป็นสมสัณฐานกัน

8.3.1 **ทฤษฎีบท** ให้ $G, G_1, G_2, \ldots, G_n$ เป็นกรุปแล้ว G เป็นกรุปผลคูณตรงภายนอกของ $G_1, G_2, \ldots, G_n$ ก็ต่อเมื่อ มีกรุปย่อยปรกติ $N_1, N_2, \ldots, N_n$ ของ G ซึ่ง $G_i \cong N_i$ สำหรับแต่ละ $1 \leq i \leq n$ และ G เป็นกรุปผลคูณตรงภายในของ $N_1, N_2, \ldots, N_n$

**บทพิสูจน์** ให้ G เป็นกรุปผลคูณตรงภายนอกของ $G_1, G_2, \ldots, G_n$ แล้วจะมีสมสัณฐาน $\alpha : G \rightarrow G_1 \times G_2 \times \ldots \times G_n$ และโดยทฤษฎีบท 8.2.3 จะมีกรุปย่อยปรกติ $\overline{G_i}$ ของ $G_1 \times G_2 \times \ldots \times G_n$ ซึ่ง $\overline{G_i} \cong G_i$ สำหรับแต่ละ $1 \leq i \leq n$ และเพราะภาพผกผันภายใต้สาทิสสัณฐานของกรุปย่อยปรกติเป็นกรุปย่อยปรกติ ทำให้ได้ $\alpha^{-1}\left(\overline{G_i}\right)$ เป็นกรุปย่อยปรกติของ G สำหรับแต่ละ $1 \leq i \leq n$

สำหรับแต่ละ $1 \leq i \leq n$ ให้ $N_i = \alpha^{-1}\left(\overline{G_i}\right)$ แล้ว $\alpha\left(N_i\right) = \overline{G_i} \cong G_i$ ทำให้ได้ $N_i \cong \alpha\left(N_i\right) = \overline{G_i} \cong G_i$ สำหรับแต่ละ $1 \leq i \leq n$

ต่อไปจะแสดงว่า G เป็นผลคูณภายในของ $N_1, N_2, \ldots, N_n$

1. ให้ $g \in G$ แล้ว $\alpha(g) \in G_1 \times G_2 \times \ldots \times G_n$ และโดยทฤษฎีบท 8.2.3 ข้อ 3 จะมี $\overline{g_i} \in \overline{G_i}$ สำหรับแต่ละ $1 \le i \le n$ ที่ทำให้ $\alpha(g) = \overline{g_1}\,\overline{g_2} \ldots \overline{g_n}$ แต่ $\overline{g_i} \in \overline{G_i} = \alpha(N_i)$ สำหรับแต่ละ $1 \le i \le n$ ดังนั้นจะมี $x_i \in N_i$ ซึ่ง $\overline{g_i} = \alpha(x_i)$ สำหรับทุกๆ $1 \le i \le n$ ทำให้ได้ $\alpha(g) = \overline{g_1}\,\overline{g_2} \ldots \overline{g_n} = \alpha(x_1)\alpha(x_2)\ldots\alpha(x_n) = \alpha(x_1 x_2 \ldots x_n)$ และเพราะ $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ดังนั้น $g = x_1 x_2 \ldots x_n$ เพราะฉะนั้น $G = N_1 N_2 \ldots N_n$

2. ให้ $1 \le i \le n$ และให้ $y \in N_i \cap (N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_n)$ แล้ว $y \in N_i$ ทำให้ได้ว่ามี $x_i \in N_i$ ซึ่ง $y = x_i$ ดังนั้น $\alpha(y) = \alpha(x_i) = \overline{g_i} \in \overline{G_i}$ และ $y \in N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_n$ ทำให้ได้ว่ามี $x_j \in N_j$ สำหรับแต่ละ $1 \le j \ne i \le n$ ซึ่ง $y = x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n$ ดังนั้น

$$\begin{aligned}
\alpha(y) &= \alpha(x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n) \\
&= \alpha(x_1)\alpha(x_2)\ldots\alpha(x_{i-1})\alpha(x_{i+1})\ldots\alpha(x_n) \\
&= \overline{g_1}\,\overline{g_2} \ldots \overline{g_{i-1}}\,\overline{g_{i+1}} \ldots \overline{g_n} \qquad \in \quad \overline{G_1}\,\overline{G_2} \ldots \overline{G_{i-1}}\,\overline{G_{i+1}} \ldots \overline{G_n}
\end{aligned}$$

ทำให้ได้ว่า $\alpha(y) \in \overline{G_i} \cap (\overline{G_1}\,\overline{G_2} \ldots \overline{G_{i-1}}\,\overline{G_{i+1}} \ldots \overline{G_n}) = \{(e_1, e_2, \ldots, e_n)\}$ โดยที่ $e_i \in G_i$ สำหรับแต่ละ $1 \le i \le n$ ดังนั้น $\alpha(y) = (e_1, e_2, \ldots, e_n)$ เป็นเอกลักษณ์ใน $G_1 \times G_2 \times \ldots \times G_y$ แต่ $\alpha$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น $y = e$

ในทางกลับกันเพราะว่า $N_1, N_2, \ldots, N_n$ เป็นกรุปย่อยปรกติของ $G$ ดังนั้นเซตผลคูณ $N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_n$ เป็นกรุปย่อยของ $G$ ทำให้ได้ $e \in N_i$ และ $e \in N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_n$ เพราะฉะนั้น $N_i \cap (N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_n) = \{e\}$ ดังนั้น $G$ เป็นกรุปผลคูณภายในของ $N_1, N_2, \ldots, N_n$

ในการพิสูจน์บทกลับให้ $N_1, N_2, \ldots, N_n$ เป็นกรุปย่อยปรกติของ $G$ ซึ่ง $G_i \cong N_i$ โดยสมสัณฐาน $\alpha_i$ สำหรับแต่ละ $1 \le i \le n$ และให้ $G$ เป็นกรุปผลคูณภายในของ $N_1, N_2, \ldots, N_n$ แล้วจะแสดงว่า $G$ เป็นผลคูณภายนอกของ $G_1, G_2, \ldots, G_n$

ให้ $\alpha : G \to G_1 \times G_2 \times \ldots \times G_n$ นิยามโดย $\alpha(g) = (g_1, g_2, \ldots, g_n)$ สำหรับแต่ละ $g \in G$ โดยที่ $g = x_1 x_2 \ldots x_n$ ซึ่ง $x_i \in N_i$ และ $\alpha_i(x_i) = g_i$ ทุกๆ $1 \le i \le n$ แล้วเพราะว่า $\alpha_i$ เป็นสมสัณฐานสำหรับแต่ละ $1 \le i \le n$ และแต่ละ $g \in G$ เขียนได้วิธีเดียวในรูปผลคูณ $g = x_1 x_2 \ldots x_n$ สำหรับทุกๆ $1 \le i \le n$ ดังนั้น $\alpha$ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึง

ให้ $g,h \in G$ แล้ว $g = x_1x_2...x_n$ และ $h = y_1y_2...y_n$ โดยที่ $x_i, y_i \in N_i$ และ $\alpha_i(x_i) = g_i$ และ $\alpha_i(y_i) = h_i$ ทุกๆ $1 \le i \le n$ ดังนั้น

$$\begin{aligned}\alpha(gh) &= \alpha(x_1x_2...x_ny_1y_2...y_n) = \alpha(x_1y_1x_2y_2...x_ny_n)\\ &= (\alpha_1(x_1y_1), \alpha_2(x_2y_2), ..., \alpha_n(x_ny_n))\\ &= (\alpha_1(x_1)\alpha_1(y_1), \alpha_2(x_2)\alpha_2(y_2), ..., \alpha_n(x_n)\alpha_n(y_n))\\ &= (x_1y_1, x_2y_2, ..., x_ny_n) = (x_1, x_2, ..., x_n)(y_1, y_2, ..., y_n) = \alpha(g)\alpha(h)\end{aligned}$$

ดังนั้น $\alpha$ เป็นสาทิสสัณฐาน เพราะฉะนั้น $G \cong G_1 \times G_2 \times ... \times G_n$ ❐

8.3.2 **ทฤษฎีบท** ให้กรุป G เป็นกรุปผลคูณตรงภายในของกรุปย่อยปรกติ $G_1, G_2, ..., G_n$ ถ้า $N_1, N_2, ..., N_n$ เป็นกรุปซึ่ง $G_i \cong N_i$ สำหรับทุกๆ $i = 1, 2, ..., n$ และ N เป็นกรุปผลคูณตรงภายนอกของ $N_1, N_2, ..., N_n$ แล้ว $G \cong N$

**บทพิสูจน์** สำหรับแต่ละ $i = 1, 2, ..., n$ ให้ $f_i : N_i \to G_i$ เป็นสมสัณฐานและให้ $f : N \to G$ นิยามโดย $f(x_1, x_2, ..., x_n) = f_1(x_1)f_2(x_2)...f_n(x_n)$ สำหรับทุกๆ $x_i \in N_i$ และ $i = 1, 2, ..., n$

1. ให้ $(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_n) \in N_1 \times N_2 \times ... \times N_n$ แล้ว $x_i = y_i$ สำหรับแต่ละ $i = 1, 2, ..., n$ ทำให้ได้

$$\begin{aligned}f(x_1, x_2, ..., x_n) &= f_1(x_1)\, f_2(x_2)...f_n(x_n)\\ &= f_1(y_1)f_2(y_2)...f_n(y_n) = f(y_1, y_2, ..., y_n)\end{aligned}$$

เพราะฉะนั้น f เป็นฟังก์ชัน

2. ให้ $(x_1, x_2, ..., x_n), (y_1, y_2, ..., y_n) \in N_1 \times N_2 \times ... \times N_n$ แล้ว

$$\begin{aligned}f((x_1, x_2, ..., x_n)(y_1, y_2, ..., y_n)) &= f(x_1y_1, x_2y_2, ..., x_ny_n)\\ &= f_1(x_1y_1)f_2(x_2y_2)...f_n(x_ny_n)\\ &= f_1(x_1)f_1(y_1)f_2(x_2)f_2(y_2)...f_n(x_n)f_n(y_n)\end{aligned}$$

$$=\left(f_1(x_1)f_2(x_2)\ldots f_n(x_n)\right)\left(f_1(y_1)\,f_2(y_2)\ldots f_n(y_n)\right)$$
$$=f(x_1,x_2,\ldots,x_n)f(y_1,y_2,\ldots,y_n)$$

เพราะฉะนั้น f เป็นสาทิสสัณฐาน

3. ให้ $(x_1,x_2,\ldots,x_n)\in N_1\times N_2\times\ldots\times N_n$ ซึ่ง $f(x_1,x_2,\ldots,x_n)=e$ แล้ว $(x_1,x_2,\ldots,x_n)\in\ker(f)$ แต่ $f(x_1,x_2,\ldots,x_n)=f_1(x_1)f_2(x_2)\ldots f_n(x_n)=e_1e_2\ldots e_n$ จะได้ $f(x_i)=e_i$ สำหรับทุกๆ $i=1,2,\ldots,n$ และเพราะว่า $f_i$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ทุกๆ $i=1,2,\ldots,n$ ดังนั้น $x_i=e_i$ สำหรับทุกๆ $i=1,2,\ldots,n$ ทำให้ได้ เพราะฉะนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่ง

4. ให้ $g=g_1g_2\ldots g_n\in G$ โดยที่ $g_i\in G_i$ เนื่องจากแต่ละ $f_i$ เป็นฟังก์ชันทั่วถึง ดังนั้นแต่ละ $i=1,2,\ldots,n$ จะมี $x_i\in N_i$ ซึ่ง $f_i(x_i)=g_i$ ทำให้ได้ว่ามี $(x_1,x_2,\ldots,x_n)\in N$ ซึ่ง $f(x_1,x_2,\ldots,x_n)=f_1(x_1)f_2(x_2)\ldots f_n(x_n)=g_1g_2\ldots g_n=g$ ซึ่งแสดงว่า f เป็นฟังก์ชันทั่วถึง

เพราะฉะนั้น f เป็นสมสัณฐาน ดังนั้น $G\cong N$ ❐

8.3.3 **ทฤษฎีบท** ให้ G เป็นกรุปและให้ $G_1,G_2,\ldots,G_n$ เป็นกรุปย่อยปรกติของ G แล้ว G เป็นกรุปผลคูณตรงภายนอกของ $G_1,G_2,\ldots,G_n$ ก็ต่อเมื่อ G เป็นกรุปผลคูณตรงภายในของ $G_1,G_2,\ldots,G_n$ ❐

จากแนวคิดเรื่องการสมสัณฐานกันของกรุปผลคูณตรงภายนอกและกรุปผลคูณตรงภายในทำให้เราประยุกต์แยกกรุปเรซิดิวคลาสมอดูโล n เช่นเดียวกับการแยกตัวประกอบของจำนวนเต็มดังจะแสดงในทฤษฎีบทต่อไปนี้

8.3.4 **ทฤษฎีบท** ถ้า m และ n เป็นจำนวนเต็มบวกซึ่ง (m, n) = 1 แล้ว $Z_{mn}\cong Z_m\times Z_n$

**บทพิสูจน์** ให้ $H=\{\bar{0},\bar{n},\overline{2n},\ldots,\overline{(m-1)n}\}$ และ $K=\{\bar{0},\bar{m},\overline{2m},\ldots,\overline{(n-1)m}\}$ แล้ว H และ K เป็นกรุปย่อยของ $Z_{mn}$ และดังนั้นเป็นกรุปย่อยปรกติของ $Z_{mn}$ โดยที่ $|H|=n$ และ $|K|=m$ เพราะฉะนั้น $|Z_{mn}|=mn=|H|\,|K|$

ถ้า $a \in H \cap K$ แล้วทั้ง m และ n จะต่างเป็นตัวหารของ a และเพราะ (m, n) = 1 เราจึงได้ว่า mn จะเป็นตัวหารของ a ดังนั้น $\bar{a} = \bar{0}$ ซึ่งแสดงว่า $H \cap K = \{\bar{0}\}$

ทำให้ได้โดยบทแทรก 8.1.8 ว่า $Z_{mn} = H \otimes K \cong H \times K$ แต่ $H \cong Z_m$ และ $K \cong Z_n$ ดังนั้น $Z_{mn} \cong Z_m \times Z_n$ ❐

โดยทฤษฎีบทหลักมูลของเลขคณิตซึ่งกล่าวว่า สำหรับแต่ละจำนวนเต็ม n > 1 จะเขียนได้ในรูปผลคูณของจำนวนเฉพาะ ทำให้เรากล่าวบทแทรกซึ่งเป็นการวางนัยของทฤษฎีบท 8.3.4 ได้ดังต่อไปนี้ ซึ่งจะขอละการพิสูจน์ไว้เป็นแบบฝึกหัด

8.3.5 **บทแทรก** ให้ n > 1 เป็นจำนวนเต็มซึ่ง $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ โดยที่ r, $k_1, \ldots, k_r$ เป็นจำนวนเต็มบวก $p_1, p_2, \ldots p_r$ เป็นจำนวนเฉพาะที่ต่างกันทั้งหมด แล้ว

$$Z_n \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$$

เมื่อ $n_i = p_i^{k_i}$ สำหรับทุกๆ i = 1, 2, . . . , r ❐

**แบบฝึกหัด 8.3**

จงพิสูจน์ทฤษฎีบท 8.3.3 และบทแทรก 8.3.5

# บรรณานุกรม
# REFERENCES


1. ฉวีวรรณ รัตนประเสริฐ *พีชคณิตแผนใหม่* ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร 2527
2. Burton, D.M., *Abstract Algebra and Linear Algebra*, Addison Wesley Series In Mathematics, Reading, Mass., 1971.
3. Dummit, D.S., *Abstract Algebra*, New Jersey : Prentice-Hall, Inc., 1991.
4. Durbin J. R., *Modern Algebra*, John Wiley & Son, New York, 1979.
5. Hall, M., *The Theory of Group*, New York : The Macmillan Company, 1959.
6. Hungerford, T.W., *Abstract Algebra : An Introduction*, Sauders College Publishing, 1990.
7. Kochendorffer, R., *Group*, London : Mcgraw-Hill Publishing Company Limited, 1970
8. Malik, D.S., *Fundamentals of Abstract Algebra*, New York : The McGraw-Hill Companies, Inc., 1997.
9. Zassenhans, H.J., *The Theory of Groups*, New York : Dover Publications, Inc.,1999.

# บัญชีศัพท์
# INDEX

ก

ข



ค



จ



ช

ซ



ด



ต



ท

## ผ



## พ



## ฟ



## ภ



## ม



## ร

ล



ว



ศ



ส

อ