การจำแนกกลุ่มจำกัดบางอันดับ

โดย

นายอัมรินทร์ อภิรักษ์มาศ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ

ภาควิชาคณิตศาสตร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2549

CLASSIFICATION OF FINITE GROUPS OF SOME ORDERS

By

Amarin Apirakmas

A Master's Report Submitted in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

Department of Mathematics

Graduate School

SILPAKORN UNIVERSITY

2006

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร อนุมัติให้สารนิพนธ์เรื่อง “การจำแนกกลุ่มจำกัดบางอันดับ” เสนอโดย นายอัมรินทร์ อภิรักษ์มาศ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ

.....
(รองศาสตราจารย์ ดร. ศิริชัย ชินะตังกูร)
คณบดีบัณฑิตวิทยาลัย
วันที่ ..... เดือน ..... พ.ศ. .....

ผู้ควบคุมสารนิพนธ์
รองศาสตราจารย์ ดร. ฉวีวรรณ รัตนประเสริฐ

คณะกรรมการตรวจสอบสารนิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร. สืบสกุล อยู่ยืนยง)
...…… / …… / ……..……

..... กรรมการ
(รองศาสตราจารย์ ดร. ฉวีวรรณ รัตนประเสริฐ)
...…… / …… / ……..……

..... กรรมการ
(รองศาสตราจารย์ วารี เกรอต)
...…… / …… / ……..……

K 46308315 : สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ
คำสำคัญ : แอคชันของกลุ่มบนเซต / ทฤษฎีบทของโคชี / ทฤษฎีบทซีโลว์

อัมรินทร์ อภิรักษ์มาศ : การจำแนกกลุ่มจำกัดบางอันดับ (CLASSIFICATION OF FINITE GROUPS OF SOME ORDERS) อาจารย์ผู้ควบคุมสารนิพนธ์ : รศ. ดร. ฉวีวรรณ รัตนประเสริฐ. 55 หน้า.

ในสารนิพนธ์นี้เราศึกษาแอคชันของกลุ่มบนเซต ซึ่งคือฟังก์ชันจาก $G\times X$ ไปยัง X เมื่อ G เป็นกลุ่ม และ X เป็นเซตที่ไม่ใช่เซตว่าง เราประยุกต์แอคชันของกลุ่มบนเซตพิสูจน์ทฤษฎีบทของโคชีและทฤษฎีบทซีโลว์ ซึ่งเป็นทฤษฎีบทสำคัญสำหรับการจำแนกกลุ่มจำกัด สุดท้ายเราประยุกต์ทฤษฎีบททั้งสองดังกล่าว จำแนกกลุ่มจำกัดอันดับไม่เกิน 15 และได้ผลดังต่อไปนี้ (ไม่นับการถอดแบบกัน)

1) กลุ่มที่มีเพียง 1 กลุ่ม คือกลุ่มขนาด 1, 15 และกลุ่มขนาดจำนวนเฉพาะ
2) กลุ่มที่มี 2 กลุ่ม คือกลุ่มขนาด 4, 6, 9, 10 และ 14
3) กลุ่มที่มี 5 กลุ่ม คือกลุ่มขนาด 8 และ 12

ภาควิชาคณิตศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ปีการศึกษา 2549

ลายมือชื่อนักศึกษา .....

ลายมือชื่ออาจารย์ผู้ควบคุมสารนิพนธ์ .....

K 46308315 : MAJOR : MATHEMATICS AND INFORMATION TECHNOLOGY
KEY WORD : GROUP ACTION ON A SET / CAUCHY'S THEOREM / SYLOW THEOREMS
AMARIN APIRAKMAS : CLASSIFICATION OF FINITE GROUPS OF SOME ORDERS. MASTER'S REPORT ADVISOR : ASSOC. PROF. CHAWEWAN RATANAPRASERT, Ph.D. 55 pp.

In the project, we studied a group action on a set which is a function from G×X to X where G is a group and X is a nonempty set. We applied an action to prove Cauchy's Theorem and Sylow Theorems which are important theorems for the classification of finite groups. Finally, we applied these to classify finite groups of orders less than or equal to 15 and the results (up to isomorphism) are in the following:

1) There is only 1 group of orders 1, 15 and of prime orders.
2) There are 2 groups of orders 4, 6, 9, 10, and 14.
3) There are 5 groups of orders 8 and 12.

Department of Mathematics Graduate School, Silpakorn University Academic Year 2006

Student's signature .....

Master's Report Advisor's signature .....

กิตติกรรมประกาศ

สารนิพนธ์นี้สำเร็จลุล่วงได้ด้วยคำปรึกษาที่มีประโยชน์อย่างดียิ่งจาก รองศาสตราจารย์ ดร. ฉวีวรรณ รัตนประเสริฐ อาจารย์ผู้ควบคุมสารนิพนธ์ ที่กรุณาให้ข้อแนะนำ แก้ไขข้อพกพร่องต่างๆ และช่วยเติมเติมความสมบูรณ์แห่งสารนิพนธ์นี้ จนทำให้สารนิพนธ์นี้สำเร็จบริบูรณ์ได้ด้วยดี

ข้าพเจ้าขอขอบพระคุณคณาจารย์ในภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร ตลอดจนคณาจารย์ทุกท่านที่กรุณาประสิทธิ์ประสาทวิชาความรู้ให้ลูกศิษย์คนนี้นับตั้งแต่อดีตจวบจนปัจจุบัน จนทำให้ลูกศิษย์คนนี้ประสบความสำเร็จ สามารถก้าวเดินอยู่บนถนนแห่งความสวยงามทางวิชาการสายนี้ได้อย่างเต็มภาคภูมิ

ข้าพเจ้าขอขอบคุณเพื่อนร่วมรุ่น ตลอดจนรุ่นพี่ในภาควิชาคณิตศาสตร์ สำหรับทุกกำลังใจที่มอบให้แก่ข้าพเจ้าเสมอมา

สุดท้ายนี้ข้าพเจ้าขอรำลึกถึงพระคุณอันเปี่ยมล้นแห่งบิดาและมารดา ตลอดจนญาติมิตรของข้าพเจ้าที่สนับสนุนการศึกษาและเฝ้าคอยเป็นกำลังใจให้ข้าพเจ้าประสบความสำเร็จทางการศึกษา จนข้าพเจ้าก้าวมาถึงวันแห่งความสำเร็จนี้ได้

สารบัญ

สารบัญตาราง

บทที่ 1
บทนำ
Introduction

ในสารนิพนธ์นี้ เราศึกษาทฤษฎีบทของโคชีและทฤษฎีบทซีโลว์ ซึ่งเป็นทฤษฎีบทสำคัญในทฤษฎีกลุ่มที่เป็นแขนงหนึ่งของวิชาพีชคณิตนามธรรม เราใช้มโนคติของแอคชันของกลุ่มบนเซตเป็นเครื่องมือในการพิสูจน์ทฤษฎีบททั้งหลาย จากนั้นเราประยุกต์ทฤษฎีบททั้งสองในการจำแนกกลุ่มอันดับ 1 – 15 โดยแบ่งการศึกษาออกเป็น 5 บทดังนี้

ในบทที่ 2 กล่าวถึงความรู้พื้นฐานในสาระต่างๆ ได้แก่ ทฤษฎีจำนวน ความสัมพันธ์สมมูล ทฤษฎีกลุ่ม กลุ่มการเรียงสับเปลี่ยน และกลุ่มสำคัญอื่นๆ ที่จะนำไปเป็นตัวอย่างในการศึกษาบทอื่นๆ โดยกล่าวถึงบทนิยาม และทฤษฎีบทที่สำคัญต่างๆ พอสังเขปโดยละการพิสูจน์ไว้

ในบทที่ 3 กล่าวถึงแอคชันของกลุ่มบนเซต ซึ่งใช้เป็นมโนคติพื้นฐานในการพิสูจน์ทฤษฎีบทต่างๆ เราศึกษาสมบัติของฟังก์ชันจาก $G\times X$ ไปยัง X เมื่อ G เป็นกลุ่ม และ X เป็นเซตที่ไม่ใช่เซตว่าง และเรียกฟังก์ชันดังกล่าวนี้ว่า “แอคชัน” เราประยุกต์แอคชันของกลุ่มบนเซตในการพิสูจน์ทฤษฎีบทของเบิร์นไซด์ ทฤษฎีบทของโคชี และนอร์มัลไลเซอร์ ซึ่งเป็นเครื่องมือสำหรับพิสูจน์ทฤษฎีบทซีโลว์ในบทที่ 4

ในบทที่ 4 ได้กล่าวถึงทฤษฎีบทซีโลว์ ซึ่งประกอบด้วย 3 ทฤษฎีบท พร้อมพิสูจน์โดยอาศัยมโนคติของแอคชันของกลุ่มบนเซตและนอร์มัลไลเซอร์ และประยุกต์ทฤษฎีบทซีโลว์เพื่อพิสูจน์ข้อคาดการณ์ที่ตั้งไว้ว่า “กลุ่มที่มีอันดับเป็น 6 เท่าของจำนวนเฉพาะไม่เป็นกลุ่มเชิงเดียว” และผลของการศึกษาพบว่าข้อคาดการณ์ดังกล่าวเป็นจริง

และในบทที่ 5 ได้แสดงการประยุกต์ทฤษฎีบทของโคชีและทฤษฎีบทซีโลว์ในอีกด้านหนึ่ง โดยนำความรู้จากทฤษฎีบททั้งสองไปใช้ในการจำแนกกลุ่มที่มีอันดับ 1 – 15 ว่ามีจำนวนกี่กลุ่ม เมื่อไม่นับการถอดแบบกัน

บทที่ 2
ความรู้พื้นฐาน
Basic Knowledge

การศึกษาของสารนิพนธ์นี้ ต้องอาศัยความรู้พื้นฐานเกี่ยวกับทฤษฎีจำนวนและพีชคณิตนามธรรม ในบทนี้จึงขอรวบรวมบทนิยามและทฤษฎีบทที่เกี่ยวข้องกับมโนคติของทฤษฎีจำนวน ความสัมพันธ์สมมูล ทฤษฎีกลุ่ม และกลุ่มการเรียงสับเปลี่ยนพอสังเขปโดยขอละการพิสูจน์ไว้

ตลอดสารนิพนธ์นี้ เราใช้สัญลักษณ์ $\mathbb{Z}$ แทนเซตของจำนวนเต็มทั้งหมด และใช้สัญลักษณ์ $\mathbb{Z}^+$ แทนเซตของจำนวนเต็มบวกทั้งหมด

2.1 ทฤษฎีจำนวน (Number Theory)

บ่อยครั้งที่การพิสูจน์ทฤษฎีบทต่างๆ ในสารนิพนธ์นี้ได้อ้างถึงความรู้พื้นฐานเกี่ยวกับทฤษฎีจำนวน ในหัวข้อนี้จึงขอกล่าวถึงบทนิยามและทฤษฎีบทที่สำคัญบางประการของทฤษฎีจำนวน

2.1.1 บทนิยาม ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ เรากล่าวว่า a **หาร** b **ลงตัว** และเขียนแทนด้วยสัญลักษณ์ $a|b$ ถ้า มีจำนวนเต็ม k ซึ่ง $b = ak$ ในกรณีนี้เราเรียก a ว่า **ตัวประกอบ (factor)** หรือ **ตัวหาร (divisor)** ของ b และเรียก b ว่า **พหุคูณ (multiple)** ของ a

2.1.2 ทฤษฎีบท ให้ a, b และ c เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$

ถ้า $a|b$ และ $b|c$ แล้ว $a|c$ ❐

2.1.3 ทฤษฎีบท ให้ a, b และ c เป็นจำนวนเต็ม โดยที่ $c \neq 0$

ถ้า $c|(a + b)$ และ $c|a$ แล้ว $c|b$ ❐

2.1.4 บทนิยาม ให้ a, b และ d เป็นจำนวนเต็ม โดยที่ $d \neq 0$ เรากล่าวว่า d เป็น **ตัวหารร่วม (common divisor)** ของ a และ b ถ้า $d|a$ และ $d|b$

ถ้า a และ b ไม่เป็นศูนย์พร้อมกันและ d เป็นจำนวนเต็มบวก เราเรียก d ว่า **ตัวหารร่วมมาก (greatest common divisor)** ของ a และ b เขียนแทนด้วยสัญลักษณ์ $d = (a, b)$ ถ้า d สอดคล้องกับสมบัติต่อไปนี้

(1) d เป็นตัวหารร่วมของ a และ b

(2) ถ้าจำนวนเต็มบวก c เป็นตัวหารร่วมของ a และ b แล้ว $c \leq d$

2.1.5 บทนิยาม เราเรียกจำนวนเต็มบวก p ว่า **จำนวนเฉพาะ (prime number)** ถ้า 1 และ p เท่านั้นซึ่งเป็นตัวหารที่เป็นจำนวนบวกของ p

2.1.6 ทฤษฎีบท ถ้า a เป็นจำนวนเต็ม ซึ่ง $a > 1$ แล้ว จะมีจำนวนเฉพาะ p ซึ่ง $p|a$ ❐

2.2 ความสัมพันธ์สมมูล (Equivalence Relation)

ความสัมพันธ์สมมูลเป็นมโนคติพื้นฐานสำคัญประการหนึ่งของการศึกษาคณิตศาสตร์ ในหัวข้อนี้จะขอกล่าวถึงบทนิยามและทฤษฎีบทที่เกี่ยวข้องกับความสัมพันธ์สมมูลและผลแบ่งกั้น ซึ่งจะนำไปประยุกต์ในการพิสูจน์ทฤษฎีบทและยกตัวอย่างประกอบการศึกษาในบทต่อๆ ไป

2.2.1 บทนิยาม ให้ X เป็นเซตที่ไม่ใช่เซตว่าง และ ~ เป็นความสัมพันธ์บน X (นั่นคือ $\sim \subseteq X \times X$) เรากล่าวว่า ~ เป็น **ความสัมพันธ์สมมูล (equivalence relation)** บน X ถ้า ~ สอดคล้องกับสมบัติต่อไปนี้

(1) **สมบัติการสะท้อน (reflexive property)** นั่นคือ $x \sim x$ สำหรับทุกๆ $x \in X$

(2) **สมบัติการสมมาตร (symmetric property)** นั่นคือ สำหรับทุกๆ $x_1, x_2 \in X$ ถ้า $x_1 \sim x_2$ แล้ว $x_2 \sim x_1$

(3) **สมบัติการถ่ายทอด (transitive property)** นั่นคือ สำหรับทุกๆ $x_1, x_2, x_3 \in X$ ถ้า $x_1 \sim x_2$ และ $x_2 \sim x_3$ แล้ว $x_1 \sim x_3$

2.2.2 บทนิยาม ให้ $\sim$ เป็นความสัมพันธ์สมมูลบนเซต X และให้ $a \in X$ เรานิยาม **คลาสสมมูล (equivalence class)** ของ a สัมพัทธ์กับ $\sim$ และเขียนแทนด้วยสัญลักษณ์ $\bar{a}$ ดังนี้

$$\bar{a} = \{x \in X \mid x \sim a\}$$

และเซตของคลาสสมมูลทั้งหมดซึ่งสัมพัทธ์กับความสัมพันธ์ $\sim$ เรียกว่า **เซตผลหาร (quotient set)** และเขียนแทนด้วยสัญลักษณ์ $X/_{\sim}$ นั่นคือ

$$X/_{\sim} = \{\bar{a} \mid a \in X\}$$

ถ้า n เป็นจำนวนเต็มบวก และ $\sim$ เป็นความสัมพันธ์บน $\mathbb{Z}$ ซึ่งกำหนดสำหรับทุกๆ $x_1, x_2 \in \mathbb{Z}$ โดย

$$x_1 \sim x_2 \text{ ก็ต่อเมื่อ } n \mid (x_1 - x_2)$$

แล้ว $\sim$ เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ ซึ่งนิยมเขียนแทนความสัมพันธ์นี้ด้วยสัญลักษณ์ $x_1 \equiv x_2 \pmod{n}$ และอ่านว่า "x_1 **คอนกรูเอนซ์** กับ x_2 **มอดูโล** n" และสำหรับแต่ละ $a \in \mathbb{Z}$ คลาสสมมูลของ a สัมพัทธ์กับ $\sim$ คือ

$$\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$$

เราเรียกคลาสสมมูลนี้ว่า **คอนกรูเอนซ์คลาสมอดูโล n (congruence class modulo n)** และในกรณีนี้จะเขียนแทนเซตผลหาร $Z/_{\sim} = \{\bar{a} \mid a \in \mathbb{Z}\}$ ด้วยสัญลักษณ์ $\mathbb{Z}_n$ และเรียก $\mathbb{Z}_n$ ว่า **เรซิดิวคลาสมอดูโล n (residue class modulo n)**

2.2.3 บทนิยาม ให้ X เป็นเซตที่ไม่ใช่เซตว่าง และ $\wp(X)$ เป็นสัญลักษณ์แทนเซตกำลัง (power set) ของ X เรากล่าวว่า $\varnothing \neq P \subseteq \wp(X)$ เป็น **ผลแบ่งกั้น (partition)** ของ X ถ้า

(1) $A \neq \varnothing$ สำหรับทุกๆ $A \in P$

(2) $A = B$ หรือ $A \cap B = \varnothing$ สำหรับทุกๆ $A, B \in P$

และ (3) $\bigcup_{A \in P} A = X$

2.2.4 ทฤษฎีบท ให้ X เป็นเซตที่ไม่ใช่เซตว่าง ถ้า $\sim$ เป็นความสัมพันธ์สมมูลบน X แล้ว $X/_{\sim}$ เป็นผลแบ่งกั้นของ X ❐

2.2.5 บทแทรก ให้ X เป็นเซตที่ไม่ใช่เซตว่าง และ $\sim$ เป็นความสัมพันธ์สมมูลบน X ถ้า $\bar{a}, \bar{b} \in X/_{\sim}$ แล้ว $\bar{a} = \bar{b}$ ก็ต่อเมื่อ $a \sim b$ ❐

ให้ S เป็นเซตที่ไม่ใช่เซตว่าง **การดำเนินการทวิภาคบน S (binary operation on S)** คือ ฟังก์ชันจาก $S \times S$ ไปยัง S

เราสามารถพิสูจน์ได้ไม่ยากว่าฟังก์ชัน $+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ ซึ่งนิยามโดย

$$+(\bar{a}, \bar{b}) = \bar{a} + \bar{b} = \overline{a+b}$$

เป็นการดำเนินการทวิภาคบน $\mathbb{Z}_n$

ให้ $n \in \mathbb{Z}$ โดยที่ $n \geq 2$ และ $a \in \mathbb{Z}$ แล้วจะมี $r \in \mathbb{Z}$ ซึ่ง $0 \leq r < n$ และ $\bar{a} = \bar{r}$ ซึ่งแสดงว่า $\mathbb{Z}_n$ มีคอนกรูเอนซ์คลาสมอดูโล n ที่แตกต่างกันทั้งหมด n คลาส ได้แก่

$$\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$$

ดังนั้น

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$$

2.3 ทฤษฎีกลุ่ม (Group Theory)

ทฤษฎีกลุ่มมีบทบาทสำคัญสำหรับการศึกษาสารนิพนธ์นี้ ในหัวข้อนี้จึงขอกล่าวถึงบทนิยามและทฤษฎีบทในทฤษฎีกลุ่มที่จะนำไปอ้างอิงในบทต่อๆ ไป

2.3.1 บทนิยาม ให้ G เป็นเซตที่ไม่ใช่เซตว่าง และ * เป็นการดำเนินการทวิภาคบน G เราเรียกโครงสร้าง (G ; *) ว่า **กลุ่ม (group)** ถ้า

(1) $a*(b*c) = (a*b)*c$ สำหรับทุกๆ $a, b, c \in G$

(2) มีสมาชิก $e \in G$ ซึ่ง $e*a = a = a*e$ สำหรับทุกๆ $a \in G$

(3) สำหรับแต่ละ $a \in G$ จะมี $b \in G$ ซึ่ง $a*b = e = b*a$

เรากล่าวว่ากลุ่ม (G ; *) เป็น **กลุ่มอาบีเลียน (abelian group)** ถ้า $a*b = b*a$ สำหรับทุกๆ $a, b \in G$ และเรียกกลุ่มที่ไม่เป็นกลุ่มอาบีเลียนว่า **กลุ่มนอนอาบีเลียน (non-abelian group)** เราใช้สัญลักษณ์ $|G|$ แทน **ขนาด (cardinality)** ของ G และเรียกว่า **อันดับ (order)** ของ G

2.3.2 หมายเหตุ (1) $(\mathbb{Z}_n ; +)$ โดยที่ + นิยามดังในหัวข้อ 2.2 เป็นตัวอย่างของกลุ่มอาบีเลียนสำหรับแต่ละจำนวนเต็มบวก n

(2) ถ้า G เป็นกลุ่มซึ่งอันดับ |G| ของ G เป็นจำนวนจำกัด จะกล่าวว่า G เป็น **กลุ่มจำกัด (finite group)** และเรากล่าวว่า G เป็น **กลุ่มอนันต์ (infinite group)** ถ้า |G| เป็นอนันต์

ให้ G เป็นกลุ่ม แล้ว สมาชิก $e \in G$ ที่กล่าวถึงในบทนิยาม 2.3.1 ข้อ (2) จะมีเพียงตัวเดียวเท่านั้น เราจึงจะเรียก e ว่า **เอกลักษณ์ (identity)** ของ G และในทำนองเดียวกัน สำหรับแต่ละ $a \in G$ สมาชิก $b \in G$ ที่สอดคล้องกับบทนิยาม 2.3.1 ข้อ (3) จะมีเพียงตัวเดียวเท่านั้น เราจึงเรียกสมาชิก b นี้ว่า **อินเวอร์ส (inverse)** ของ a และเราเขียนแทนอินเวอร์สของ a ด้วยสัญลักษณ์ a^{-1}

2.3.3 ข้อตกลง เราอาจกล่าวถึงกลุ่ม G โดยละการดำเนินการ * ในกรณีที่ไม่ทำให้เกิดการสับสน และสำหรับ $a, b \in G$ เรานิยมแทน $a*b$ ด้วย ab

2.3.4 ทฤษฎีบท ให้ G เป็นกลุ่ม แล้ว

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

(2) $(a^{-1})^{-1} = a$ สำหรับทุกๆ $a \in G$ ❐

โดยหลักอุปนัยเชิงคณิตศาสตร์ (Principle of Mathematical Induction) เราสามารถขยายทฤษฎีบท 2.3.4 ข้อ (1) สำหรับทุกๆ จำนวนเต็มบวก n ได้ดังนี้

ถ้า n เป็นจำนวนเต็มบวก และ $a_1, a_2, \ldots, a_n \in G$ แล้ว $(a_1a_2\ldots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\ldots a_1^{-1}$

2.3.5 บทนิยาม ให้ $(G ; *)$ เป็นกลุ่ม และ $H \subseteq G$ โดยที่ $H \neq \varnothing$ เราเรียก $(H ; *)$ ว่า **กลุ่มย่อย (subgroup)** ของ $(G ; *)$ ถ้า * เป็นการดำเนินการกำกัด (restriction operation) บน H และ $(H ; *)$ เป็นกลุ่ม

2.3.6 ทฤษฎีบท ให้ G เป็นกลุ่ม และ $H \subseteq G$ โดยที่ $H \neq \varnothing$ แล้ว H เป็นกลุ่มย่อยของ G ก็ต่อเมื่อ

(1) ถ้า $a, b \in H$ แล้ว $ab \in H$ และ

(2) ถ้า $a \in H$ แล้ว $a^{-1} \in H$

ถ้า G เป็นกลุ่ม และ $a \in G$ แล้ว $\{a^n \mid n \in \mathbb{Z}\}$ เป็นกลุ่มย่อยของ G เราเขียนแทนกลุ่มย่อยนี้ด้วยสัญลักษณ์ $< a >$ และเรียกว่า **กลุ่มย่อยวัฏจักรของ G ที่ก่อกำเนิดโดย a (cyclic subgroup of**

G **generated by** a) และถ้ามี $a \in G$ ซึ่ง $G = \langle a \rangle$ เรากล่าวว่า G เป็น **กลุ่มวัฏจักร (cyclic group)** และเรียก a ว่า **ตัวก่อกำเนิด (generator)** ของ G

ตัวอย่างเช่น สำหรับแต่ละจำนวนเต็มบวก n เราได้ว่า $\mathbb{Z}_n$ เป็นกลุ่มวัฏจักร โดยที่ $\mathbb{Z}_n = \langle \bar{1} \rangle$

2.3.7 บทนิยาม ให้ G เป็นกลุ่ม และ $a \in G$ ถ้ามีจำนวนเต็มบวก k ที่น้อยสุด ซึ่ง $a^k = e$ เราเรียก k ว่า **อันดับ (order)** ของ a เขียนแทนด้วยสัญลักษณ์ o(a) และถ้าไม่มีจำนวนเต็มบวก k ซึ่ง $a^k = e$ เรากล่าวว่า a มี **อันดับอนันต์ (infinite order)**

2.3.8 ข้อสังเกต (1) $o(a^{-1}) = o(a)$ สำหรับทุกๆ $a \in G$

(2) ให้ $m, n \in \mathbb{Z}^+$ ซึ่ง $(m, n) = 1$ ถ้า $a, b \in G$ โดยที่ $o(a) = m$ และ $o(b) = n$ แล้ว $a^i b^j$ สำหรับแต่ละ $0 \le i < m$ และ $0 \le j < n$ เป็นสมาชิกใน G ที่แตกต่างกันทั้งหมด

2.3.9 บทนิยาม ให้ G เป็นกลุ่ม และ H เป็นกลุ่มย่อยของ G และสำหรับแต่ละ $a \in G$ เรานิยามเซต

$$aH := \{ah \mid h \in H\}$$

และ $$Ha := \{ha \mid h \in H\}$$

เราเรียก aH และ Ha ว่า **โคเซตซ้าย (left coset)** และ **โคเซตขวา (right coset)** ของ H ใน G ตามลำดับ

2.3.10 ทฤษฎีบท ให้ G เป็นกลุ่ม และ H เป็นกลุ่มย่อยของ G แล้ว

(1) ถ้า $a \in G$ แล้ว $aH = H$ ก็ต่อเมื่อ $a \in H$

(2) ถ้า $a, b \in G$ แล้ว $aH = bH$ ก็ต่อเมื่อ $a^{-1}b \in H$

(3) ถ้า $a, b \in G$ แล้ว $Ha = Hb$ ก็ต่อเมื่อ $ab^{-1} \in H$

(4) ถ้า H เป็นกลุ่มจำกัด แล้ว $|H| = |aH| = |Ha|$ สำหรับทุกๆ $a \in G$ ❐

2.3.11 ทฤษฎีบท *ทฤษฎีบทของลากรองจ์ (Lagrange's Theorem)*

ถ้า G เป็นกลุ่มจำกัดและ H เป็นกลุ่มย่อยของ G แล้ว |H| เป็นตัวหารของ |G| ❐

2.3.12 บทแทรก ถ้า G เป็นกลุ่มจำกัดและ $a \in G$ แล้ว o(a) เป็นตัวหารของ |G| ❐

2.3.13 ทฤษฎีบท ให้ H เป็นกลุ่มย่อยของ G และให้ $\mathcal{A}$ = {Ha | a∈G} และ $\mathcal{B}$ = {aH | a∈G} แล้ว $|\mathcal{A}| = |\mathcal{B}|$ ❐

2.3.14 บทนิยาม ให้ G เป็นกลุ่มจำกัดและ H เป็นกลุ่มย่อยของ G เราเรียกจำนวนโคเซตซ้าย (หรือก็คือจำนวนโคเซตขวา) ของ H ใน G ที่แตกต่างกันทั้งหมดว่า **ดรรชนี (index)** ของ H ใน G และเขียนแทนด้วยสัญลักษณ์ [G : H]

2.3.15 บทแทรก ถ้า G เป็นกลุ่มจำกัดและ H เป็นกลุ่มย่อยของ G แล้ว |G| = |H|[G : H] ❐

2.3.16 ทฤษฎีบท ให้ H และ K เป็นกลุ่มย่อยอันดับจำกัดของกลุ่ม G ซึ่งต่างกัน ถ้า (|H|, |K|) = 1 หรือ |H| = |K| เป็นจำนวนเฉพาะ แล้ว H ∩ K = {e} ❐

2.3.17 บทนิยาม ให้ H เป็นกลุ่มย่อยของกลุ่ม G เรากล่าวว่า H เป็น **กลุ่มย่อยปรกติ (normal subgroup)** ของ G ถ้า aH = Ha สำหรับทุกๆ a∈G

2.3.18 บทนิยาม ให้ G เป็นกลุ่มและ H เป็นกลุ่มย่อยของ G และ a∈G เราเรียกสับเซตของ G ซึ่งนิยามดังนี้

$$aHa^{-1} \coloneqq \{aha^{-1} \mid h \in H\}$$

ว่า **สังยุค (conjugate)** ของ H ใน G

2.3.19 ทฤษฎีบท ให้ G เป็นกลุ่ม และ H เป็นกลุ่มย่อยของ G แล้ว ข้อความต่อไปนี้สมมูลกัน

(1) H เป็นกลุ่มย่อยปรกติของ G

(2) $xax^{-1} \in H$ สำหรับทุกๆ x∈G และ a∈H

(3) $aHa^{-1} = H$ สำหรับทุกๆ a∈G

(4) $aHa^{-1} \subseteq H$ สำหรับทุกๆ a∈G ❐

2.3.20 ทฤษฎีบท ให้ G เป็นกลุ่มจำกัด และ H เป็นกลุ่มย่อยของ G

ถ้า [G : H] = 2 แล้ว H เป็นกลุ่มย่อยปรกติของ G ❐

2.3.21 บทนิยาม ให้ G เป็นกลุ่ม และ H เป็นกลุ่มย่อยปรกติของ G เราเขียนแทนเซตของโคเซตทั้งหมดของ H ด้วยสัญลักษณ์ G/H นั่นคือ $G/H = \{aH \mid a \in G\} = \{Ha \mid a \in G\}$ และสัญลักษณ์ G/H อ่านว่า G **mod** H

ให้ G เป็นเป็นกลุ่ม และ H เป็นกลุ่มย่อยปรกติของ G เราสามารถพิสูจน์ได้ไม่ยากว่าฟังก์ชัน $* : G/H \times G/H \to G/H$ ที่นิยามโดย

$$* (aH, bH) = aH * bH = (a*b)H \quad \text{สำหรับทุกๆ } a, b \in G$$

เป็นการดำเนินการทวิภาคบน G/H และยิ่งไปกว่านั้น เราสามารถพิสูจน์ได้ว่า $(G/H, *)$ เป็นกลุ่ม และเรียกกลุ่ม G/H ว่า **กลุ่มผลหาร (quotient group)** ของ G โดย H

2.3.22 ทฤษฎีบท ให้ G เป็นกลุ่ม และ H เป็นกลุ่มย่อยปรกติของ G

(1) ถ้า G เป็นกลุ่มอาบีเลียน แล้ว G/H เป็นกลุ่มอาบีเลียน

(2) ถ้า G เป็นกลุ่มวัฏจักร แล้ว G/H เป็นกลุ่มวัฏจักร

(3) ถ้า G เป็นกลุ่มจำกัด แล้ว $\left| G/H \right| = \frac{|G|}{|H|} = [G : H]$ ❐

2.3.23 บทนิยาม ให้ $(G ; *)$ และ $(H ; \circ)$ เป็นกลุ่ม และ $f : G \to H$ เป็นฟังก์ชัน

เราเรียก f ว่า **ฟังก์ชันถ่ายแบบ (homomorphism)** จาก G ไปยัง H ถ้า $f(a*b) = f(a) \circ f(b)$ สำหรับทุกๆ $a, b \in G$

และเราเรียก f ว่า **ฟังก์ชันถอดแบบ (isomorphism)** ถ้า f เป็นฟังก์ชันถ่ายแบบชนิดหนึ่งต่อหนึ่งจาก G ไปบน H

ถ้ามีฟังก์ชันถอดแบบจาก G ไปยัง H เรากล่าวว่า G **ถอดแบบ (isomorphic)** กับ H เขียนแทนด้วยสัญลักษณ์ $G \cong H$

2.3.24 ทฤษฎีบท ให้ G_1, G_2 และ G_3 เป็นกลุ่ม แล้ว

(1) ฟังก์ชันเอกลักษณ์ (identity function) $1_{G_1} : G_1 \to G_1$ เป็นฟังก์ชันถอดแบบ

(2) ถ้า $f : G_1 \to G_2$ เป็นฟังก์ชันถอดแบบ แล้ว $f^{-1} : G_2 \to G_1$ เป็นฟังก์ชันถอดแบบ

(3) ถ้า $f : G_1 \to G_2$ และ $g : G_2 \to G_3$ เป็นฟังก์ชันถอดแบบ แล้ว $gof : G_1 \to G_3$ เป็นฟังก์ชันถอดแบบ ❐

2.3.25 บทแทรก ให้ G_1, G_2 และ G_3 เป็นกลุ่ม แล้ว

(1) $G_1 \cong G_1$

(2) ถ้า $G_1 \cong G_2$ แล้ว $G_2 \cong G_1$

(3) ถ้า $G_1 \cong G_2$ และ $G_2 \cong G_3$ แล้ว $G_1 \cong G_3$ ❐

2.3.26 ทฤษฎีบท ให้ p เป็นจำนวนเฉพาะ ถ้า G เป็นกลุ่มอันดับ p แล้ว G เป็นกลุ่มวัฏจักร ❐

2.3.27 ทฤษฎีบท ให้ n เป็นจำนวนเต็มบวก ถ้า G เป็นกลุ่มวัฏจักรอันดับ n แล้ว G จะถอดแบบกับกลุ่มคอนกรูเอนซ์คลาสมอดูโล n นั่นคือ $G \cong \mathbb{Z}_n$ ❐

2.3.28 ทฤษฎีบท ถ้า G เป็นกลุ่มวัฏจักรอันดับอนันต์ แล้ว G จะถอดแบบกับกลุ่มการบวกของจำนวนเต็มทั้งหมด $\mathbb{Z}$ นั่นคือ $G \cong \mathbb{Z}$ ❐

2.3.29 ทฤษฎีบท กลุ่มอันดับ p^2 เป็นกลุ่มอาบีเลียน สำหรับทุกๆ จำนวนเฉพาะ p ❐

2.3.30 ทฤษฎีบท ให้ p เป็นจำนวนเฉพาะ และ G เป็นกลุ่มอันดับ p^2 แล้ว $G \cong \mathbb{Z}_{p^2}$ หรือ $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ ❐

2.3.31 ทฤษฎีบท ให้ p เป็นจำนวนเฉพาะ และ G เป็นกลุ่มอันดับ 2p แล้ว $G \cong \mathbb{Z}_{2p}$ หรือ $G \cong D_p$ โดยที่ D_p คือกลุ่มไดฮิดรัล (dihedral group) (ดูหัวข้อ 2.5) ❐

2.3.32 ทฤษฎีบท ให้ p และ q เป็นจำนวนเฉพาะ ซึ่ง $p < q$ และ p ไม่เป็นตัวหารของ $q - 1$ แล้วทุกๆ กลุ่มอันดับ pq เป็นกลุ่มวัฏจักร ❐

2.4 กลุ่มการเรียงสับเปลี่ยน (Permutation Group)

กลุ่มการเรียงสับเปลี่ยนเป็นหมู่สำคัญของกลุ่มหมู่หนึ่ง ทั้งนี้เพราะทฤษฎีบทของเคย์เลย์ (Cayley's Theorem) ได้กล่าวไว้ว่า "กลุ่มจำกัดทุกกลุ่มจะถอดแบบกับกลุ่มการเรียงสับเปลี่ยน" นอกจากนี้กลุ่มการเรียงสับเปลี่ยนยังมีบทบาทสำคัญในการดำเนินการศึกษาสารนิพนธ์นี้ ในหัวข้อนี้จึงขอกล่าวถึงบทนิยามและทฤษฎีบทที่สำคัญของกลุ่มการเรียงสับเปลี่ยน ที่จะนำไปอ้างถึงในบทต่อๆ ไป

2.4.1 บทนิยาม สำหรับแต่ละจำนวนเต็มบวก n ให้ $X_n = \{1, 2, 3, \dots, n\}$ เราเรียกฟังก์ชัน $\sigma : X_n \to X_n$ ที่เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก X_n ไปบน X_n ว่า **การเรียงสับเปลี่ยน (permutation)** บน X_n และเขียนแทนเซตของการเรียงสับเปลี่ยนทั้งหมดบน X_n ด้วยสัญลักษณ์ S_n

ให้ n เป็นจำนวนเต็มบวก เรานิยมเขียนสมาชิกของ S_n ในรูปของเมทริกซ์ขนาด $2\times n$ กล่าวคือ ให้แถวแรกแทนสมาชิกใน X_n ทั้งหมด และในแถวที่สอง ณ ตำแหน่ง $2i$ $(1 \le i \le n)$ แทนค่า $\sigma(i)$ ของการเรียงสับเปลี่ยน นั่นคือถ้า $\sigma \in S_n$ แล้ว เราเขียนแทน σ ด้วยเมทริกซ์ได้ดังนี้

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

การเรียงสับเปลี่ยนเอกลักษณ์ (identity permutation) ใน S_n เขียนในรูปเมทริกซ์ได้ดังนี้

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

และเรานิยมแทนด้วยสัญลักษณ์สั้นๆ เป็น (1)

ตัวอย่างเช่น สมาชิกทั้งหมดของ S_3 ในรูปของเมทริกซ์เป็นดังนี้

$$(1) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

ถ้า n เป็นจำนวนเต็มบวก แล้ว $(S_n ; \circ)$ เป็นกลุ่ม เมื่อ $\circ$ คือการดำเนินการ “ผลประกอบ (composition) ของฟังก์ชัน” และเราเรียก S_n ว่า **กลุ่มสมมาตรดีกรี n (symmetric group of degree n)**

2.4.2 ทฤษฎีบท *ทฤษฎีบทของเคย์เลย์ (Cayley's Theorem)*

กลุ่มจำกัดทุกกลุ่มจะถอดแบบกับกลุ่มย่อยของกลุ่มสมมาตรดีกรี n สำหรับบางจำนวนเต็มบวก n ❐

ให้ n และ r เป็นจำนวนเต็มบวก และ $\{k_1, k_2, \dots, k_r\} \subseteq X_n$ เราใช้สัญลักษณ์

$$\sigma = (k_1\ k_2 \dots k_r)$$

แทนการเรียงสับเปลี่ยนซึ่งกำหนดโดย

$$\sigma(k_i) = k_{i+1} \quad \text{เมื่อ } i \in \{1, 2, \dots, r-1\}$$
$$\sigma(k_r) = k_1$$

และ $$\sigma(k) = k \quad \text{เมื่อ } k \notin \{k_1, k_2, \dots, k_r\}$$

และเรียกว่า **วัฏจักรความยาว r (cycle of length r)**

เช่น $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$ สามารถเขียน σ ในรูปของวัฏจักรความยาว 4 ได้ดังนี้

$$\sigma = (1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3)$$

และ $\sigma = (1\ 4\ 2\ 6) \in S_6$ หมายถึงการเรียงสับเปลี่ยน

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix}$$

2.4.3 ทฤษฎีบท ให้ n และ r เป็นจำนวนเต็มบวก ถ้า σ เป็นวัฏจักรความยาว r ใน S_n แล้ว σ^{-1} เป็นวัฏจักรความยาว r

ยิ่งไปกว่านั้น ถ้า $\sigma = (k_1\ k_2 \dots k_r)$ แล้ว $\sigma^{-1} = (k_r\ k_{r-1} \dots k_2\ k_1)$ ❐

เนื่องจากวัฏจักรคือการเรียงสับเปลี่ยน เราจึงมีผลประกอบของวัฏจักร 2 วัฏจักรใน S_n สำหรับทุกๆ จำนวนเต็มบวก n ซึ่งจะเรียกผลประกอบที่ได้ว่า **ผลคูณ** ของวัฏจักร เช่นถ้า $\sigma =$

(2 4 5) และ $\delta = (1\ 2\ 4)$ เป็นวัฏจักรใน S_5 เราจะได้ผลคูณ $\sigma\delta$ และ $\delta\sigma$ ดังนี้

$$\sigma\delta = (2\ 4\ 5)(1\ 2\ 4) = \begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\4&5&3&1&2\end{pmatrix}$$

และ

$$\delta\sigma = (1\ 2\ 4)(2\ 4\ 5) = \begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix}$$

และขอให้สังเกตว่าการคูณใน S_n ไม่สอดคล้องสมบัติการสลับที่ (commutative law)

2.4.4 บทนิยาม ให้ n, r และ s เป็นจำนวนเต็มบวก และให้ $\sigma = (k_1\ k_2\ \dots\ k_r)$ และ $\delta = (m_1\ m_2\ \dots\ m_s)$ เป็นวัฏจักรใน S_n เรากล่าวว่า σ และ δ เป็น **วัฏจักรต่างสมาชิก (disjoint cycles)** ถ้า $\{k_1, k_2, \dots, k_r\} \cap \{m_1, m_2, \dots, m_s\} = \varnothing$

2.4.5 ทฤษฎีบท ให้ n เป็นจำนวนเต็มบวก ถ้า σ และ δ เป็นวัฏจักรต่างสมาชิกใน S_n แล้ว $\sigma\delta = \delta\sigma$ ❐

2.4.6 ทฤษฎีบท ให้ n เป็นจำนวนเต็มบวก แล้วทุกการเรียงสับเปลี่ยนใน S_n จะเป็นการเรียงสับเปลี่ยนเอกลักษณ์ หรือวัฏจักร หรือสามารถเขียนได้ในรูปผลคูณของวัฏจักรต่างสมาชิกที่มีความยาวมากกว่า 1 ❐

2.4.7 บทนิยาม เราเรียกวัฏจักรความยาว 2 ว่า **ทรานสโพซิชัน** (**transposition**)

2.4.8 ทฤษฎีบท ให้ n เป็นจำนวนเต็มบวก แล้วแต่ละวัฏจักรความยาว $1 < r \le n$ ใน S_n เขียนได้ในรูปผลคูณของทรานสโพซิชันจำนวน $r - 1$ ทรานสโพซิชัน

ยิ่งไปกว่านั้น ถ้า $(k_1\ k_2\ \dots\ k_r)$ เป็นวัฏจักรความยาว $1 < r \le n$ ใน S_n แล้ว

$(k_1\ k_2\ \dots\ k_r) = (k_1\ k_r)(k_1\ k_{r-1}) \dots (k_1\ k_3)(k_1\ k_2)$ ❐

2.4.9 บทแทรก ทุกการเรียงสับเปลี่ยนสามารถเขียนได้ในรูปผลคูณของทรานสโพซิชัน ❐

2.5 ตัวอย่างกลุ่ม (Some Well-Known Groups)

ในหัวข้อนี้จะขอกล่าวถึงกลุ่มซึ่งเป็นที่รู้จักอื่นๆ เพื่อจะนำไปใช้เป็นตัวอย่างประกอบการศึกษาในบทต่อๆ ไป

กลุ่มสลับ (Alternating Groups)

2.5.1 บทนิยาม สำหรับแต่ละจำนวนเต็มบวก n ให้ $\sigma \in S_n$ โดยที่ $\sigma = \delta_1\delta_2\ldots\delta_r$ เมื่อ δ_i เป็นทรานสโพซิชัน เราเรียก σ ว่า **การเรียงสับเปลี่ยนคู่ (even permutation)** ถ้า r เป็นจำนวนคู่ และเราเรียก σ ว่า **การเรียงสับเปลี่ยนคี่ (odd permutation)** ถ้า r เป็นจำนวนคี่

2.5.2 ทฤษฎีบท ทุกการเรียงสับเปลี่ยนเป็นการเรียงสับเปลี่ยนคู่หรือการเรียงสับเปลี่ยนคี่ได้เพียงอย่างใดอย่างหนึ่งเท่านั้น ❐

2.5.3 ทฤษฎีบท การเรียงสับเปลี่ยนเอกลักษณ์ (1) เป็นการเรียงสับเปลี่ยนคู่ ❐

2.5.4 ทฤษฎีบท ให้ σ และ β เป็นการเรียงสับเปลี่ยน

(1) ถ้า σ เป็นการเรียงสับเปลี่ยนคู่ แล้ว σ^{-1} เป็นการเรียงสับเปลี่ยนคู่

(2) ถ้า σ เป็นการเรียงสับเปลี่ยนคี่ แล้ว σ^{-1} เป็นการเรียงสับเปลี่ยนคี่

(3) ถ้า σ และ β เป็นการเรียงสับเปลี่ยนคู่ทั้งคู่ หรือเป็นการเรียงสับเปลี่ยนคี่ทั้งคู่ แล้ว $\sigma\beta$ เป็นการเรียงสับเปลี่ยนคู่

(4) ถ้า σ หรือ β ตัวใดตัวหนึ่งเป็นการเรียงสับเปลี่ยนคู่ และอีกตัวหนึ่งเป็นการเรียงสับเปลี่ยนคี่ แล้ว $\sigma\beta$ เป็นการเรียงสับเปลี่ยนคี่ ❐

สำหรับแต่ละจำนวนเต็มบวก n เราให้ $A_n := \{\sigma \in S_n \mid \sigma \text{ เป็นการเรียงสับเปลี่ยนคู่}\}$ แล้ว A_n เป็นกลุ่มย่อยของ S_n เราเรียกกลุ่ม A_n นี้ว่า **กลุ่มสลับดีกรี n (alternating group of degree n)**

2.5.5 ทฤษฎีบท ให้ n เป็นจำนวนเต็มบวก แล้ว

(1) $|A_n| = \frac{n!}{2}$

(2) ถ้า $n \geq 2$ แล้ว $[S_n : A_n] = 2$

(3) A_n เป็นกลุ่มย่อยปรกติของ S_n ❐

เนื่องจาก A_4 เป็นตัวอย่างสำคัญในการศึกษาสารนิพนธ์นี้ จึงขอกล่าวถึงสมาชิกทั้งหมดของ A_4 พร้อมทั้งแสดงตารางการคูณ โดยเริ่มต้นด้วยการพิจารณาสมาชิกทั้งหมดของ S_4 ดังนี้

(1)	$\sigma_6 = (1\ 3\ 4\ 2)$	$\delta_3 = (1\ 3\ 4)$	$\alpha_1 = (1\ 2)$
$\sigma_1 = (1\ 2\ 3\ 4)$	$\sigma_7 = (1\ 3\ 2\ 4)$	$\delta_4 = (1\ 4\ 3)$	$\alpha_2 = (1\ 3)$
$\sigma_2 = (1\ 3)(2\ 4)$	$\sigma_8 = (1\ 2)(3\ 4)$	$\delta_5 = (1\ 2\ 4)$	$\alpha_3 = (1\ 4)$
$\sigma_3 = (1\ 4\ 3\ 2)$	$\sigma_9 = (1\ 4\ 2\ 3)$	$\delta_6 = (1\ 4\ 2)$	$\alpha_4 = (2\ 3)$
$\sigma_4 = (1\ 2\ 4\ 3)$	$\delta_1 = (2\ 3\ 4)$	$\delta_7 = (1\ 2\ 3)$	$\alpha_5 = (2\ 4)$
$\sigma_5 = (1\ 4)(2\ 3)$	$\delta_2 = (2\ 4\ 3)$	$\delta_8 = (1\ 3\ 2)$	$\alpha_6 = (3\ 4)$

จากสมาชิกทั้ง 24 ตัวของ S_4 จะมีสมาชิกที่เป็นการเรียงสับเปลี่ยนคู่ทั้งสิ้น 12 ตัว และสมาชิกทั้ง 12 ตัวนี้คือสมาชิกทั้งหมดของ A_4 ได้แก่ (1), σ_2, σ_5, σ_8, δ_1, δ_2, δ_3, δ_4, δ_5, δ_6, δ_7 และ δ_8

ต่อไปนี้เป็นตารางการคูณบน A_4

	(1)	**σ_2**	**σ_5**	**σ_8**	**δ_1**	**δ_2**	**δ_3**	**δ_4**	**δ_5**	**δ_6**	**δ_7**	**δ_8**
(1)	(1)	σ_2	σ_5	σ_8	δ_1	δ_2	δ_3	δ_4	δ_5	δ_6	δ_7	δ_8
σ_2	σ_2	(1)	σ_8	σ_5	δ_4	δ_7	δ_6	δ_1	δ_8	δ_3	δ_2	δ_5
σ_5	σ_5	σ_8	(1)	σ_2	δ_5	δ_3	δ_2	δ_8	δ_1	δ_7	δ_6	δ_4
σ_8	σ_8	σ_5	σ_2	(1)	δ_8	δ_6	δ_7	δ_5	δ_4	δ_2	δ_3	δ_1
δ_1	δ_1	δ_8	δ_4	δ_5	δ_2	(1)	σ_2	δ_6	δ_7	σ_5	σ_8	δ_3
δ_2	δ_2	δ_3	δ_6	δ_7	(1)	δ_1	δ_8	σ_5	σ_8	δ_4	δ_5	σ_2
δ_3	δ_3	δ_2	δ_7	δ_6	σ_5	δ_5	δ_4	(1)	σ_2	δ_8	δ_1	σ_8
δ_4	δ_4	δ_5	δ_1	δ_8	δ_7	σ_2	(1)	δ_3	δ_2	σ_8	σ_5	δ_6
δ_5	δ_5	δ_4	δ_8	δ_1	δ_3	σ_5	σ_8	δ_7	δ_6	(1)	σ_2	δ_2
δ_6	δ_6	δ_7	δ_2	δ_3	σ_8	δ_8	δ_1	σ_2	(1)	δ_5	δ_4	σ_5
δ_7	δ_7	δ_6	δ_3	δ_2	σ_2	δ_4	δ_5	σ_8	σ_5	δ_1	δ_8	(1)
δ_8	δ_8	δ_1	δ_5	δ_4	δ_6	σ_8	σ_5	δ_2	δ_3	σ_2	(1)	δ_7

ตาราง 2.1 : ตารางการคูณบน A_4

กลุ่มของเมทริกซ์ขนาด 2×2 เหนือจำนวนเชิงซ้อน
(Group of 2×2 Matrices Over the Complex Numbers)

ให้ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ เป็นเมทริกซ์ขนาด 2×2 โดยที่ a, b, c และ d เป็นจำนวนเชิงซ้อน แล้ว **ดีเทอร์มิแนนท์ (determinant)** ของ A เขียนแทนด้วยสัญลักษณ์ det(A) นิยามดังนี้

$$\det(A) := ad - bc$$

เมทริกซ์ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ เรียกว่า **เมทริกซ์เอกลักษณ์ (identity matrix)** เขียนแทนด้วยสัญลักษณ์ I

ให้ $\mathcal{M}$ แทนเซตของเมทริกซ์ขนาด 2×2 ทั้งหมดที่มีสมาชิก (entries) เป็นจำนวนเชิงซ้อน และมีดีเทอร์มิแนนท์ไม่เท่ากับศูนย์ แล้วเราสามารถพิสูจน์ได้ไม่ยากว่าโครงสร้างที่ประกอบด้วยเซต $\mathcal{M}$ กับการดำเนินการ “การคูณเมทริกซ์ (matrices multiplication)” บน $\mathcal{M}$ เป็นกลุ่ม และเราเรียก $\mathcal{M}$ ว่า **กลุ่มของเมทริกซ์ขนาด 2×2 เหนือจำนวนเชิงซ้อน (group of 2×2 matrices over the complex numbers)**

กลุ่มสมาชิก 4 ตัวของไคลน์ (Klien 4-Groups)

2.5.6 บทนิยาม ให้ G = {e, a, b, c} เป็นกลุ่มอันดับ 4 เราเรียก G ว่า **กลุ่มสมาชิก 4 ตัวของไคลน์ (Klien 4-group)** และเขียนแทนด้วยสัญลักษณ์ K_4 ถ้าการคูณบน G แสดงได้ดังตารางต่อไปนี้

	e	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

ตาราง 2.2 : ตารางการคูณของ K_4

ผลคูณตรง (Direct Product)

2.5.7 บทนิยาม ให้ H และ K เป็นเซต **ผลคูณคาร์ทีเซียน (Cartesian product)** ของ H และ K เขียนแทนด้วยสัญลักษณ์ $H \times K$ นิยามโดย $H \times K = \{ (h, k) \mid h \in H \text{ และ } k \in K \}$

ขอให้สังเกตว่า $H \times K = K \times H$ ก็ต่อเมื่อ K = H

ถ้า H และ K เป็นกลุ่ม และนิยามการดำเนินการบน $H \times K$ ดังนี้

$$(h_1, k_1)\cdot(h_2, k_2) = (h_1h_2, k_1k_2) \qquad \ldots (*)$$

สำหรับทุกๆ $(h_1, k_1), (h_2, k_2) \in H \times K$ โดยที่ h_1h_2 และ k_1k_2 คือผลคูณใน H และใน K ตามลำดับ แล้วเราสามารถพิสูจน์ได้ไม่ยากว่าเซต $H \times K$ กับการคูณซึ่งนิยามดัง (*) เป็นกลุ่ม ซึ่งเรียกกลุ่ม $H \times K$ ว่า **ผลคูณตรง (direct product)** ของ H และ K

2.5.8 ทฤษฎีบท ถ้า H และ K เป็นกลุ่มจำกัด แล้ว $| H \times K | = | H || K |$ ❐

2.5.9 ทฤษฎีบท ถ้า $G = H \times K$ เป็นผลคูณตรงของ H และ K และให้

$$H' = \{ (h, e) \mid h \in H \text{ และ } e \text{ เป็นเอกลักษณ์ของ } H \}$$
$$K' = \{ (e, k) \mid k \in K \text{ และ } e \text{ เป็นเอกลักษณ์ของ } K \}$$

แล้ว (1) H' และ K' เป็นกลุ่มย่อยปรกติของ G

(2) $H \cong H'$ และ $K \cong K'$

(3) ถ้า $h' \in H'$ และ $k' \in K'$ แล้ว $h'k' = k'h'$

(4) $G = H'K'$ และ $H' \cap K' = \{(e, e)\}$ ❐

2.5.10 บทแทรก ให้ $G = H \times K$ และ H', K' นิยามดังในทฤษฎีบท 2.5.9 แล้วแต่ละ $g \in G$ สามารถเขียนได้ในรูปผลคูณ $h'k'$ โดยที่ $h' \in H'$ และ $k' \in K'$ ได้แบบเดียวเท่านั้น ❐

2.5.11 บทนิยาม ให้ H และ K เป็นกลุ่มย่อยของกลุ่ม G เรานิยามสับเซต HK ของ G ดังนี้

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

2.5.12 ทฤษฎีบท ให้ H และ K เป็นกลุ่มย่อยของกลุ่ม G แล้ว HK เป็นกลุ่มย่อยของ G ก็ต่อเมื่อ $HK = KH$ ❐

2.5.13 ทฤษฎีบท ให้ G เป็นกลุ่ม ถ้า H เป็นกลุ่มย่อยของ G และ K เป็นกลุ่มย่อยปรกติของ G แล้ว HK เป็นกลุ่มย่อยปรกติของ G ❐

2.5.14 ทฤษฎีบท ให้ H และ K เป็นกลุ่มย่อยของกลุ่ม G ถ้า H และ K สอดคล้องกับเงื่อนไขต่อไปนี้

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

(2) $hk = kh$ สำหรับทุกๆ $h \in H$ และ $k \in K$

และ (3) $HK = G$

แล้ว $G \cong H \times K$ ❐

2.5.15 บทแทรก ให้ H และ K เป็นกลุ่มย่อยปรกติของกลุ่ม G ถ้า $H \cap K = \{e\}$และ $HK = G$ แล้ว $G \cong H \times K$ ❐

2.5.16 ทฤษฎีบท ให้ H และ K เป็นกลุ่มย่อยจำกัดของกลุ่ม G แล้ว $|HK| = \frac{|H||K|}{|H \cap K|}$ ❐

โดยทฤษฎีบท 2.5.16 เราสามารถเขียนทฤษฎีบท 2.5.14 ในกรณีที่ G เป็นกลุ่มจำกัด ได้ดังนี้

2.5.14′ ทฤษฎีบท ให้ H และ K เป็นกลุ่มย่อยจำกัดของกลุ่มจำกัด G โดยที่ $|H||K| = |G|$ ถ้า $H \cap K = \{e\}$ หรือ $HK = G$ แล้ว $G \cong H \times K$ ❐

กลุ่มไดฮิดรัลและกลุ่มควอเทอร์เนียน (Dihedral and Quaternion Groups)

2.5.17 บทนิยาม สำหรับแต่ละจำนวนเต็มบวก $n \geq 2$ **กลุ่มไดฮิดรัล (dihedral group)** D_n คือกลุ่มอันดับ 2n ซึ่งก่อกำเนิดด้วยสมาชิก 2 ตัว และนิยามดังนี้

$$D_n = \langle a, b \mid a^n = e, b^2 = e \text{ และ } bab = a^{-1} \rangle$$

2.5.18 ทฤษฎีบท $D_3 \cong S_3$ ❐

2.5.19 บทนิยาม **กลุ่มควอเทอร์เนียน (quaternion group)** เขียนแทนด้วยสัญลักษณ์ Q คือกลุ่มอันดับ 8 ซึ่งก่อกำเนิดด้วยสมาชิก 2 ตัว และนิยามดังนี้

$$Q = \langle a, b \mid a^4 = e, b^2 = a^2 \text{ และ } b^{-1}ab = a^{-1} \rangle$$

2.5.20 ทฤษฎีบท D_4 และ Q เป็นกลุ่มอันดับ 8 เพียงสองกลุ่มซึ่งเป็นกลุ่มนอนอาบีเลียน ❐

บทที่ 3
แอคชันของกลุ่มบนเซตและการประยุกต์
Group Action on a Set and Applications

ในบทนี้เราจะศึกษาแอคชันของกลุ่มบนเซต ซึ่งเป็นมโนคติสำคัญในการศึกษาทฤษฎีบทของโคชีและทฤษฎีบทซีโลว์ซึ่งจะกล่าวถึงในบทต่อไป สำหรับในบทนี้เราจะแสดงการประยุกต์แอคชันของกลุ่มบนเซตในการพิสูจน์ทฤษฎีบทของเบิร์นไซด์ซึ่งเป็นรากฐานสำคัญของการพัฒนาวิชาคอมบินาทอริกส์

ตลอดบทนี้ หากไม่มีการกำหนดเป็นอย่างอื่น เราให้ G แทนกลุ่มที่มี e เป็นเอกลักษณ์

3.1 แอคชันของกลุ่มบนเซต (Group Action on a Set)

ถ้า G และ X เป็นเซต ในหัวข้อนี้เราสนใจศึกษาฟังก์ชันจาก $G \times X$ ไปยัง X โดยเฉพาะเมื่อ G เป็นกลุ่มและ X ไม่เป็นเซตว่าง

3.1.1 บทนิยาม กำหนดให้ X เป็นเซตที่ไม่ใช่เซตว่าง และให้ G เป็นกลุ่ม เราเรียกฟังก์ชัน $* : G \times X \to X$ ว่า **แอคชันของ** G **บน** X **(action of** G **on** X**)** ถ้าเงื่อนไขต่อไปนี้เป็นจริง

(1) $*(e, x) = x$ สำหรับทุกๆ $x \in X$

(2) $*(g_1g_2, x) = *(g_1, *(g_2, x))$ สำหรับทุกๆ $x \in X$ และสำหรับทุกๆ $g_1, g_2 \in G$

และเราเรียก X ว่า G-**เซต (**G-**set)**

3.1.2 ทฤษฎีบทประกอบ ให้ G เป็นกลุ่มและ H เป็นกลุ่มย่อยของ G แล้วจะมีแอคชันของ H บน G

การพิสูจน์ ให้ $* : H \times G \to G$ นิยามสำหรับทุกๆ $g \in G$ และ $h \in H$ โดย

$$*(h, g) = hgh^{-1}$$

(1) ให้ $g \in G$ แล้ว $*(e, g) = ege^{-1} = g$

(2) ให้ $g \in G$ และ $h_1, h_2 \in H$ แล้ว $*(h_1h_2, g) = (h_1h_2)g(h_1h_2)^{-1} = (h_1h_2)g(h_2^{-1}h_1^{-1})$ $= h_1(h_2gh_2^{-1})h_1^{-1} = *(h_1, *(h_2, g))$

เพราะฉะนั้น * เป็นแอคชันของ H บน G ❐

3.1.3 ข้อตกลง ถ้า * เป็นแอคชันของกลุ่ม G บนเซต X แล้วสำหรับแต่ละ $g \in G$ และ $x \in X$ เราอาจเขียนแทน $*(g, x)$ ด้วย gx ในกรณีที่จะไม่ทำให้เกิดการสับสน

3.1.4 ทฤษฎีบทประกอบ ให้ G เป็นกลุ่มและ X เป็น G-เซต และนิยามความสัมพันธ์ ~ บน X โดย

$$x_1 \sim x_2 \text{ ก็ต่อเมื่อ มี } g \in G \text{ ซึ่ง } gx_1 = x_2$$

สำหรับแต่ละ $x_1, x_2 \in X$ แล้ว ~ เป็นความสัมพันธ์สมมูลบน X

การพิสูจน์ ให้ $x \in X$ เนื่องจาก X เป็น G-เซต จะได้ว่า $ex = x$ ซึ่งแสดงว่า $x \sim x$ ดังนั้น ~ สอดคล้องสมบัติการสะท้อน

ต่อไปให้ $x_1, x_2 \in X$ โดยที่ $x_1 \sim x_2$ แล้วจะมี $g \in G$ ซึ่ง $gx_1 = x_2$ ทำให้ได้ว่า $g^{-1} \in G$ และ $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1$ ดังนั้น $x_2 \sim x_1$ เพราะฉะนั้น ~ สอดคล้องสมบัติการสมมาตร

สุดท้ายให้ $x_1, x_2, x_3 \in X$ โดยที่ $x_1 \sim x_2$ และ $x_2 \sim x_3$ แล้วจะมี $g_1, g_2 \in G$ ซึ่ง $g_1x_1 = x_2$ และ $g_2x_2 = x_3$ ดังนั้น $g_2g_1 \in G$ และ $x_3 = g_2x_2 = g_2(g_1x_1) = (g_2g_1)x_1$ ดังนั้น $x_1 \sim x_3$ เพราะฉะนั้น ~ สอดคล้องสมบัติการถ่ายทอด

เพราะฉะนั้น ~ เป็นความสัมพันธ์สมมูลบน X ❐

ถ้า ~ เป็นความสัมพันธ์สมมูลที่กำหนดดังในทฤษฎีบทประกอบ 3.1.4 และ $a \in X$ แล้ว

$$\bar{a} = \{x \in X \mid a \sim x\} = \{x \in X \mid \text{มี } g \in G \text{ ซึ่ง } x = ga\}$$

เป็นเซตสมมูลสัมพัทธ์กับ ~ ซึ่งในกรณีนี้จะใช้สัญลักษณ์ G(a) แทน $\bar{a}$ และเรียกว่า **ออร์บิทของ** a **ใน** X **ภายใต้** G **(orbit of** a **in** X **under** G**)**

3.1.5 ทฤษฎีบท ให้ G เป็นกลุ่มจำกัดและ X เป็น G-เซต ที่เป็นเซตจำกัด และ $a \in X$ แล้ว

(1) $G_a := \{g \in G \mid ga = a\}$ เป็นกลุ่มย่อยของ G

(2) $|G(a)| = [G : G_a]$

การพิสูจน์ ให้ $a \in X$

(1) ให้ $g_1, g_2 \in G_a$ แล้ว $g_1a = a$ และ $g_2a = a$ ทำให้ได้ $a = g_1a = g_1(g_2a) = (g_1g_2)a$ ซึ่งแสดงว่า $g_1g_2 \in G_a$ ดังนั้น G_a มีสมบัติปิดภายใต้การดำเนินการของ G

เนื่องจาก $a = ea = (g_1^{-1}g_1)a = g_1^{-1}(g_1a) = g_1^{-1}a$ แสดงว่า $g_1^{-1} \in G_a$ เพราะฉะนั้น G_a เป็นกลุ่มย่อยของ G

(2) ให้ $H = \{gG_a \mid g \in G\}$ และสังเกตว่าถ้า $x \in G(a)$ แล้วจะมี $g \in G$ ที่ทำให้ $x = ga$ ต่อไปให้ $\varphi := \{(x, gG_a) \in G(a) \times H \mid x = ga\}$

ให้ $x_1, x_2 \in G(a)$ โดยที่ $x_1 = x_2$ แล้วจะมี $g_1, g_2 \in G$ ที่ทำให้ $x_1 = g_1a$ และ $x_2 = g_2a$ แต่ $x_1 = x_2$ จึงได้ $g_1a = g_2a$ ดังนั้น $g_1^{-1}(g_1a) = g_1^{-1}(g_2a)$ นั่นคือ $a = (g_1^{-1}g_2)a$ ซึ่งแสดงว่า $g_1^{-1}g_2 \in G_a$ ทำให้ได้ $g_1G_a = g_2G_a$ นั่นคือ $\varphi(x_1) = \varphi(x_2)$ เพราะฉะนั้น φ เป็นฟังก์ชัน

ต่อไปจะแสดงว่า φ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง ให้ $x_1, x_2 \in G(a)$ โดยที่ $g_1G_a = g_2G_a$ เมื่อ $x_1 = g_1a$ และ $x_2 = g_2a$ แล้ว $g_1^{-1}g_2 \in G_a$ ทำให้ได้ $a = (g_1^{-1}g_2)a = g_1^{-1}(g_2a)$ ดังนั้น $g_1a = g_2a$ นั่นคือ $x_1 = x_2$

สุดท้ายให้ $gG_a \in H$ แล้ว $ga \in G(a)$ และเลือก $x = ga$ ดังนั้นมี $x = ga \in G(a)$ ซึ่ง $\varphi(x) = gG_a$ เพราะฉะนั้น φ เป็นฟังก์ชันไปบน

แสดงว่า φ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก G(a) ไปบนเซตของโคเซตซ้าย H ของ G_a ใน G เพราะฉะนั้น $|G(a)| = |H| = [G : G_a]$ ❐

3.1.6 หมายเหตุ เราเรียกกลุ่มย่อย G_a ของ G ว่า **กลุ่มย่อยสเตบิไลเซอร์ (stabilizer subgroup)** ของ a

โดยผลของบทแทรก 2.2.5 ทำให้เราได้บทแทรกต่อไปนี้

3.1.7 บทแทรก ให้ n เป็นจำนวนเต็มบวก และ G เป็นกลุ่มย่อยของ S_n และให้ X เป็น G-เซต แล้ว $b \in G(a)$ ก็ต่อเมื่อ $G(a) = G(b)$ สำหรับทุกๆ $a,b \in X$ ❐

3.1.8 ตัวอย่าง ให้ $X = \{1, 2, 3, 4, 5, 6\}$ และ $G = \{(1), (1\ 2)(3\ 4\ 5\ 6), (3\ 5)(4\ 6), (1\ 2)(3\ 6\ 5\ 4)\}$ เป็นกลุ่มย่อยของ S_6

ให้ $* : G \times X \rightarrow X$ นิยามสำหรับทุกๆ $\sigma \in G$ และ $a \in X$ โดย $*(\sigma, a) = \sigma(a)$ แล้ว $*((1), a) = (1)(a) = a$ สำหรับทุกๆ $a \in X$ และถ้า $a \in X$ และ $\sigma_1, \sigma_2 \in G$ แล้ว $*(\sigma_1\sigma_2, a) = \sigma_1\sigma_2(a) = \sigma_1(\sigma_2(a)) = *(\sigma_1, \sigma_2(a)) = *(\sigma_1, *(\sigma_2, a))$ ดังนั้น $*$ เป็นแอคชันของ G บน X ทำให้ได้ว่า X เป็น G-เซต

ต่อไปเรานิยามความสัมพันธ์ $\sim$ บน X ตามทฤษฎีบทประกอบ 3.1.4 สำหรับทุกๆ $a,b \in X$ โดย

$$a \sim b \text{ ก็ต่อเมื่อ มี } \sigma \in G \text{ ซึ่ง } \sigma(a) = b$$

ซึ่งจะทำให้ได้ว่า $\sim$ เป็นความสัมพันธ์สมมูล ซึ่ง $\sim$ เขียนในรูปแจกแจงสมาชิกได้ดังนี้

$\sim$ = {(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 2), (2, 1), (3, 4), (4, 3), (3, 5), (5, 3), (3, 6), (6, 3), (4, 5), (5, 4), (4, 6), (6, 4), (5, 6), (6, 5)}

ต่อไปเราจะแสดงผลแบ่งกั้นของ X โดยการหาเซตผลหาร $X/_{\sim} = \{G(a) \mid a \in X\}$ เนื่องจากสำหรับแต่ละ $a \in X$ เราจะได้ออร์บิทของ a คือ $G(a) = \{b \in X \mid a \sim b\}$ แล้วโดยบทแทรก 3.1.7 เราจะได้ $G(1) = \{1, 2\} = G(2)$ และ $G(3) = \{3, 4, 5, 6\} = G(3) = G(4) = G(5) = G(6)$ เพราะฉะนั้น $X/_{\sim} = \{\{1, 2\}, \{3, 4, 5, 6\}\}$ ❐

3.2 ทฤษฎีบทของเบิร์นไซด์ (Burnside's Theorem)

ทฤษฎีบทของเบิร์นไซด์เป็นทฤษฎีบทที่ใช้ในการประยุกต์เรื่องการนับจำนวนออร์บิทใน G-เซตที่เป็นเซตจำกัด และ G เป็นกลุ่มจำกัด การนับดังกล่าวเป็นรากฐานของการพัฒนาวิชาคอมบินาทอริกส์ ในหัวข้อนี้เราจะแสดงการพิสูจน์ทฤษฎีบทของเบิร์นไซด์โดยใช้แอคชันของกลุ่มบนเซต และแสดงตัวอย่างการประยุกต์ทฤษฎีบทของเบิร์นไซด์

3.2.1 ทฤษฎีบท ให้ G เป็นกลุ่มและ X เป็น G-เซต และให้ $\sim$ เป็นความสัมพันธ์สมมูลบน X ซึ่งนิยามดังในทฤษฎีบทประกอบ 3.1.4 ถ้า $a \sim b$ แล้ว $G_a \cong G_b$ สำหรับทุกๆ $a, b \in X$

การพิสูจน์ ให้ $a, b \in X$ โดยที่ $a \sim b$ แล้วจะมี $g \in G$ ซึ่ง $ga = b$ เราจะแสดงก่อนว่าถ้า $x \in G_a$ แล้ว $gxg^{-1} \in G_b$

ให้ $x \in G_a$ แล้ว $x \in G$ และ $xa = a$ และเพราะว่า $(gxg^{-1})b = (gx)(g^{-1}b) = (gx)a = g(xa) = ga = b$ ดังนั้น $gxg^{-1} \in G_b$

ต่อไปเรานิยามฟังก์ชัน $\varphi : G_a \to G_b$ โดย $\varphi(x) = gxg^{-1}$ สำหรับทุกๆ $x \in G_a$

ให้ $x_1, x_2 \in G_a$ แล้ว $\varphi(x_1x_2) = gx_1x_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = \varphi(x_1)\varphi(x_2)$ ดังนั้น φ เป็นฟังก์ชันถ่ายแบบ

ให้ $x_1, x_2 \in G_a$ ซึ่ง $\varphi(x_1) = \varphi(x_2)$ จะได้ว่า $gx_1g^{-1} = gx_2g^{-1}$ ซึ่งทำให้ได้ว่า $x_1 = x_2$ ดังนั้น φ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ให้ $y \in G_b$ แล้ว $y \in G$ และ $yb = b$ เนื่องจาก $(g^{-1}yg)a = (g^{-1}y)(ga) = (g^{-1}y)b = g^{-1}(yb) = g^{-1}b = a$ ดังนั้น $g^{-1}yg \in G_a$ เราจึงเลือก $x = gyg^{-1}$ ทำให้ได้ว่า $\varphi(x) = \varphi(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y$ ดังนั้น φ เป็นฟังก์ชันไปบน

เพราะฉะนั้น φ เป็นฟังก์ชันถอดแบบจาก G_a ไปยัง G_b ทำให้เราสรุปได้ว่า $G_a \cong G_b$ ❐

หมายเหตุ ผลของทฤษฎีบท 3.2.1 ทำให้เราได้ว่า $|G_a| = |G_b|$ สำหรับทุกๆ $a, b \in X$

เราจะแสดงการประยุกต์ทฤษฎีบท 3.2.1 ในการพิสูจน์ทฤษฎีบทของเบิร์นไซด์ แต่ก่อนอื่นจะขอนิยามเซตจุดตรึงเสียก่อน

3.2.2 บทนิยาม ให้ X เป็น G-เซต และสำหรับแต่ละ $g \in G$ เรานิยาม $X_g := \{a \in X \mid ga = a\}$ และเรียกว่า **เซตจุดตรึง** (**fixed point set**) โดย g

3.2.3 ทฤษฎีบท *ทฤษฎีบทของเบิร์นไซด์ (Burnside's Theorem)*

ให้ G เป็นกลุ่มจำกัด และ X เป็น G-เซตที่เป็นเซตจำกัด ถ้า r เป็นจำนวนออร์บิททั้งหมดใน X ภายใต้ G แล้ว $r \cdot |G| = \sum_{g \in G} |X_g|$

การพิสูจน์ ให้ $\wp = \{(g, a) \in G \times X \mid ga = a\}$ ให้ $g \in G$ แล้วสำหรับแต่ละ $a \in X$ จะได้ว่า $ga = a$ ก็ต่อเมื่อ $a \in X_g$ ดังนั้นจำนวนคู่อันดับ (g, a) ใน $\wp$ สำหรับแต่ละ $a \in X$ เท่ากับ $|X_g|$ เพราะฉะนั้น $|\wp| = \sum_{g \in G} |X_g|$

ในทำนองเดียวกันให้ $a \in X$ แล้วสำหรับแต่ละ $g \in G$ จะได้ว่า $ga = a$ ก็ต่อเมื่อ $g \in G_a$ แล้วจำนวนคู่อันดับ (g, a) ใน $\wp$ สำหรับแต่ละ $g \in G$ เท่ากับ $|G_a|$ ดังนั้น $|\wp| = \sum_{a \in X} |G_a|$ ทำให้ได้ว่า $\sum_{g \in G} |X_g| = \sum_{a \in X} |G_a|$

ให้ $a \in X$ แล้ว $G(a)$ เป็นออร์บิทใน X ภายใต้ G และให้ $b \in G(a)$ แล้ว $b \in X$ และ $b \sim a$ จะได้ว่า $|G_b| = |G_a|$ ดังนั้น

$$\sum_{b \in G(a)} |G_b| = |G(a)|\,|G_a| = [G : G_a]\,|G_a| = |G|$$

ทำให้ได้ว่า $|X| = \sum_{a \in X} |G_a| = r \cdot |G|$

และเมื่อหาผลรวมของจำนวนออร์บิททั้งหมดที่แตกต่างกันใน X ภายใต้ G ทั้ง r ออร์บิท แล้วจะได้

$$\sum_{g \in G} |X_g| = \sum_{a \in X} |G_a| = r \cdot |G| \qquad \square$$

เราจะจบหัวข้อนี้ด้วยตัวอย่างการประยุกต์ทฤษฎีบทของเบิร์นไซด์ในการแก้ปัญหาการนับ

3.2.4 ตัวอย่าง เราต้องการหาจำนวนวิธีระบายสีแผ่นไม้กระดานรูปสี่เหลี่ยมจัตุรัสซึ่งแบ่งออกเป็นตาราง 4 ช่อง ตามหมายเลขดังนี้

1	2
4	3

(ก)

โดยใช้สี m สี โดยที่แต่ละช่องจะระบายสีได้เพียงสีเดียวเท่านั้น และเราจะระบายสีแผ่นไม้กระดานนี้เพียงหน้าเดียว

เนื่องจากแผ่นไม้กระดานนี้เป็นวัตถุแข็งเกร็งในระนาบซึ่งสามารถหมุนได้ เราจึงพิจารณาว่าการระบายสีในบางแบบเป็นการระบายสีแบบเดียวกัน เช่นการระบายสีตามรูปข้างล่างนี้

ถือว่าเป็นการระบายสีแบบเดียวกัน เพราะหากเราหมุนรูปใดรูปหนึ่งใน 4 รูปข้างต้นตามเข็มนาฬิกาหรือทวนเข็มนาฬิกาเป็นมุม 0° หรือ 90° หรือ 180° หรือ 270° ดังนี้เรื่อยไปแล้วจะได้รูปที่เป็นรูปใดรูปหนึ่งใน 4 รูปข้างต้น

ให้ X แทนเซตของภาพทั้งหมดที่เกิดจากการระบายสีลงในช่องหมายเลข 1 – 4 ช่องละสีจากสีที่มีอยู่ทั้งหมด m สี

เนื่องจากการหมุนภาพทำให้ภาพบางภาพซ้ำกัน เราจึงเลือกกลุ่ม G = < (1 2 3 4) > เพื่อนิยามแอคชันของ G บน X ซึ่งหากเราสามารถนิยามฟังก์ชันดังกล่าวได้แล้วโดยทฤษฎีบทประกอบ 3.1.4 เราจะได้ว่าความสัมพันธ์บน X ซึ่งกำหนดโดยเงื่อนไขของแอคชันดังกล่าวเป็นความสัมพันธ์สมมูลบน X ทำให้เราสามารถหาผลแบ่งกั้นของ X ได้ ซึ่งแต่ละคลาสสมมูลในผลแบ่งกั้นก็คือออร์บิท เพราะฉะนั้นจำนวนวิธีระบายสีที่ทำให้ได้ภาพที่แตกต่างกันทั้งหมดก็คือจำนวนออร์บิทที่แตกต่างกันทั้งหมดใน X นั่นเอง

เพื่อความสะดวกจะขอกำหนดสัญลักษณ์แทนภาพต่างๆ ดังต่อไปนี้

4	1
3	2

(ข)

3	4
2	1

(ค)

4	3
1	2

(ง)

ภาพ (ข), (ค) และ (ง) คือภาพที่ได้จากการหมุนภาพ (ก) ตามเข็มนาฬิกาเป็นมุม 90°, 180° และ 270° ตามลำดับ แล้วภาพ (ก) – (ง) เป็นสมาชิกในเซต X

นิยาม $\varphi : G \times X \to X$ สำหรับแต่ละ $\sigma \in G$ และ $f \in X$ ดังนี้

$\varphi((1), f)$ แทนภาพ f

$\varphi((1\ 2\ 3\ 4), f)$ แทนภาพที่ได้จากการหมุน f ตามเข็มนาฬิกาเป็นมุม 90°

$\varphi((1\ 3)(2\ 4), f)$ แทนภาพที่ได้จากการหมุน f ตามเข็มนาฬิกาเป็นมุม 180°

และ $\varphi((1\ 4\ 3\ 2), f)$ แทนภาพที่ได้จากการหมุน f ตามเข็มนาฬิกาเป็นมุม 270°

จากการนิยาม φ ข้างต้นจะเห็นว่า φ สอดคล้องกับเงื่อนไขของบทนิยาม 3.1.1 ข้อ (1) ต่อไปจะแสดงว่า φ สอดคล้องกับเงื่อนไขของบทนิยาม 3.1.1 ข้อ (2)

$\varphi((1)(1\ 2\ 3\ 4), f) = \varphi((1\ 2\ 3\ 4), f)$ ซึ่งก็คือภาพ (ข)

และเนื่องจาก $\varphi((1), \varphi((1\ 2\ 3\ 4), f)) = \varphi((1),$ ภาพ (ข)) ซึ่งก็คือภาพ (ข)

ดังนั้น $\varphi((1)(1\ 2\ 3\ 4), f) = \varphi((1), \varphi((1\ 2\ 3\ 4), f))$

ในทำนองเดียวกันจะได้ว่า

$\varphi((1)(1\ 3)(2\ 4), f) = \varphi((1), \varphi((1\ 3)(2\ 4), f))$

และ $\varphi((1)(1\ 4\ 3\ 2), f) = \varphi((1), \varphi((1\ 4\ 3\ 2), f))$

ต่อไปจะแสดงว่า $\varphi((1\ 2\ 3\ 4)(1\ 2\ 3\ 4), f) = \varphi((1\ 2\ 3\ 4), \varphi((1\ 2\ 3\ 4), f))$

เนื่องจาก $\varphi((1\ 2\ 3\ 4)(1\ 2\ 3\ 4), f) = \varphi((1\ 3)(2\ 4), f)$ ซึ่งก็คือภาพ (ค)

และเนื่องจาก $\varphi((1\ 2\ 3\ 4), \varphi((1\ 2\ 3\ 4), f)) = \varphi((1\ 2\ 3\ 4),$ ภาพ (ข)) ซึ่งก็คือภาพ (ค)

ดังนั้น $\varphi((1\ 2\ 3\ 4)(1\ 2\ 3\ 4), f\ ) = \varphi((1\ 2\ 3\ 4), \varphi((1\ 2\ 3\ 4), f\ ))$
และในทำนองเดียวกันจะได้ว่า

$\varphi((1\ 2\ 3\ 4)(1\ 3)(2\ 4), f\ ) = \varphi((1\ 2\ 3\ 4), \varphi((1\ 3)(2\ 4), f\ ))$
$\varphi((1\ 2\ 3\ 4)(1\ 4\ 3\ 2), f\ ) = \varphi((1\ 2\ 3\ 4), \varphi((1\ 4\ 3\ 2), f\ ))$
$\varphi((1\ 3)(2\ 4)(1\ 3)(2\ 4), f\ ) = \varphi((1\ 3)(2\ 4), \varphi((1\ 3)(2\ 4), f\ ))$
$\varphi((1\ 3)(2\ 4)(1\ 4\ 3\ 2), f\ ) = \varphi((1\ 3)(2\ 4), \varphi((1\ 4\ 3\ 2), f\ ))$

และ $\varphi((1\ 4\ 3\ 2)(1\ 4\ 3\ 2), f\ ) = \varphi((1\ 4\ 3\ 2), \varphi((1\ 4\ 3\ 2), f\ ))$
ดังนั้น X เป็น G-เซต

ต่อไปจะหาเซตจุดตรึงโดย σ เพื่อนับจำนวนออร์บิททั้งแตกต่างกันทั้งหมดใน X โดยประยุกต์ทฤษฎีบทของเบิร์นไซด์

สำหรับแต่ละ $\sigma \in G$ เราจะได้เซตจุดตรึงโดย σ คือ $X_\sigma = \{f \in X \mid \sigma f = f\}$ เพราะฉะนั้นสมาชิกใน X_σ ก็คือภาพ (ก) ใน X ซึ่งเมื่อหมุนในทิศทางที่กำหนดโดย σ แล้วยังคงได้ภาพเดิม

(1) เริ่มต้นจะหาจำนวนสมาชิกของ $X_{(1)}$:
เนื่องจาก $(1)f = f$ สำหรับทุกๆ $f \in X$ ดังนั้น $|X_{(1)}| = |X| = m^4$

(2) หาจำนวนสมาชิกของ $X_{(1\ 2\ 3\ 4)}$:

การที่เราจะระบายสีภาพ (ก) แล้วหมุนในทิศตามเข็มนาฬิกาเป็นมุม 90° เพื่อให้ได้ผลออกมาเป็นภาพเดิมนั้นเป็นไปได้เพียงกรณีเดียวคือทั้ง 4 ช่องจะต้องเป็นสีเดียวกัน เพราะหากทุกช่องไม่เป็นสีเดียวกันแล้วเมื่อเราหมุนภาพในทิศตามเข็มนาฬิกาเป็นมุม 90° จะทำให้ภาพเปลี่ยนไป ดังนั้นเราต้องเลือกสีระบายภาพ (ก) โดยให้ทั้ง 4 ช่องเป็นสีเดียวกัน ซึ่งเลือกได้ m วิธี นั่นคือ $|X_{(1\ 2\ 3\ 4)}| = m$

(3) หาจำนวนสมาชิกของ $X_{(1\ 3)(2\ 4)}$:

การที่เราจะระบายสีภาพ (ก) แล้วหมุนในทิศตามเข็มนาฬิกาเป็นมุม 180° เพื่อให้ได้ผลออกมาเป็นภาพเดิมนั้น เราต้องระบายช่องที่อยู่ในแนวเส้นทแยงมุมให้เป็นสีเดียวกัน นั่นคือเราต้องระบายสีช่องหมายเลข 1 และ 3 ให้เป็นสีเดียวกัน ซึ่งเลือกได้ m วิธี และระบายสีช่องหมายเลข 2 และ 4 ให้เป็นสีเดียวกัน ซึ่งเลือกได้ m วิธี ดังนั้นโดยหลักการนับเบื้องต้นเราได้ $|X_{(1\ 3)(2\ 4)}| = m^2$

(4) หาจำนวนสมาชิกของ $X_{(1\,4\,3\,2)}$:

การที่เราจะระบายสีภาพ (ก) แล้วหมุนในทิศตามเข็มนาฬิกาเป็นมุม 270° เพื่อให้ได้ผลออกมาเป็นภาพเดิมนั้นเป็นไปได้เพียงกรณีเดียวคือทั้ง 4 ช่องจะต้องเป็นสีเดียวกัน เพราะหากทุกช่องไม่เป็นสีเดียวกันแล้ว เมื่อเราหมุนภาพตามเข็มนาฬิกาเป็นมุม 270° จะทำให้ภาพเปลี่ยนไป ดังนั้นเราต้องเลือกสีระบายภาพ (ก) โดยให้ทั้ง 4 ช่องเป็นสีเดียวกัน ซึ่งเลือกได้ m วิธี นั่นคือ $|X_{(1\,4\,3\,2)}| = m$

โดยทฤษฎีบทของเบิร์นไซด์ จะได้

$$\begin{aligned}
\text{จำนวนวิธีระบายสีที่ต้องการ} &= \text{จำนวนออร์บิทใน } X \text{ ที่แตกต่างกันทั้งหมด} \\
&= \frac{1}{|G|}\sum_{\sigma\in G}|X_\sigma| \\
&= \frac{1}{|G|}\left(|X_{(1)}| + |X_{(1\,2\,3\,4)}| + |X_{(1\,3)(2\,4)}| + |X_{(1\,4\,3\,2)}|\right) \\
&= \frac{1}{4}\left(m^4 + m + m^2 + m\right) \\
&= \frac{1}{4}\left(m^4 + m^2 + 2m\right) \qquad \square
\end{aligned}$$

3.3 ทฤษฎีบทของโคชี (Cauchy's Theorem)

ในหัวข้อนี้เราจะประยุกต์แอคชันของกลุ่มบนเซตในการพิสูจน์ทฤษฎีบทของโคชี และแสดงตัวอย่างการประยุกต์ทฤษฎีบทของโคชีในการจำแนกกลุ่มที่มีอันดับ 6

ให้ G เป็นกลุ่มจำกัดและ X เป็น G-เซต แล้วสำหรับแต่ละ $a\in X$ จะได้ออร์บิทของ a ใน X คือ $G(a) = \{ga \mid g\in G\}$ และแต่ละสมาชิกของ X จะเป็นสมาชิกของออร์บิทใดออร์บิทหนึ่งเพียงออร์บิทเดียว ดังนั้นถ้ามีออร์บิทใน X ภายใต้ G จำนวน r เซต และสำหรับแต่ละ $i\in\{1, 2, \dots, r\}$ เลือก a_i เพียงตัวเดียวจากออร์บิท $G(a_i)$ แล้ว

$$|X| = \sum_{i=1}^{r}|G(a_i)| \qquad \dots (3.3.1)$$

ถ้าเรานิยามสับเซต X_G ของ X ดังนี้

$$X_G = \{a\in X \mid ga = a \text{ สำหรับทุกๆ } g\in G\}$$

แล้ว X_G เป็นยูเนียนของออร์บิทใน X ที่ประกอบด้วยสมาชิกเพียงหนึ่งตัว สมมติว่ามีออร์บิทใน X

ที่ประกอบด้วยสมาชิกเพียงตัวเดียวจำนวน s ออร์บิท โดยที่ $0 \le s \le r$ และ $G(a_{s+1}), G(a_{s+2}), \dots , G(a_r)$ เป็นออร์บิทใน X ที่ประกอบด้วยสมาชิกมากกว่าหนึ่งตัว จะได้ $|X_G| = s$ และเราสามารถเขียน (3.3.1) ได้ใหม่ดังนี้

$$|X| = |X_G| + \sum_{i=s+1}^{r} |G(a_i)| \qquad \dots (3.3.2)$$

3.3.1 ทฤษฎีบท ให้ p เป็นจำนวนเฉพาะและ G เป็นกลุ่มขนาด p^n เมื่อ $n \in \mathbb{Z}^+ \cup \{0\}$
ถ้า X เป็น G-เซต ที่เป็นเซตจำกัด แล้ว $|X| \equiv |X_G| \pmod p$

การพิสูจน์ ให้ X เป็น G-เซตที่เป็นเซตจำกัด แล้ว X สอดคล้องกับเงื่อนไข (3.3.2) ข้างต้น นั่นคือ $|X| = |X_G| + \sum_{i=s+1}^{r} |G(a_i)|$ แล้วโดยทฤษฎีบท 3.1.5 ถ้า $a \in X$ แล้ว $|G(a)| = [G : G_a]$ และเพราะ $[G : G_a]$ เป็นตัวหารของ $|G| = p^n$ ดังนั้น p เป็นตัวหารของ $|G(a)|$ ทำให้ได้ว่า p เป็นตัวหารของ $\sum_{i=s+1}^{r} |G(a_i)|$ นั่นคือ p หาร $(|X| - |X_G|)$ ลงตัว เพราะฉะนั้น $|X| \equiv |X_G| \pmod p$ ❐

3.3.2 บทนิยาม ให้ G เป็นกลุ่ม และ p เป็นจำนวนเฉพาะ เรากล่าวว่า G เป็น p-**กลุ่ม (p-group)** ถ้าสำหรับแต่ละ $g \in G$ ที่ $g \ne e$ จะมี $n \in \mathbb{Z}^+$ ซึ่ง $o(g) = p^n$ (นั่นคืออันดับของแต่ละสมาชิกใน G เป็นจำนวนในรูปกำลังของ p)

3.3.3 บทนิยาม ให้ G เป็นกลุ่ม และ H เป็นกลุ่มย่อยของ G เรากล่าวว่า H เป็น p-**กลุ่มย่อย (p-subgroup)** ของ G ถ้า H เป็น p-กลุ่ม

3.3.4 ทฤษฎีบท *ทฤษฎีบทของโคชี* (*Cauchy's Theorem*)

ให้ G เป็นกลุ่มจำกัดและ p เป็นจำนวนเฉพาะ ถ้า p เป็นตัวประกอบของ |G| แล้วจะมี $a \in G$ ซึ่ง $o(a) = p$

การพิสูจน์ ให้ $X := \{(g_1, g_2, \dots , g_p) \in G^p \mid g_i \in G \text{ และ } g_1g_2\dots g_p = e\}$
เราจะพิสูจน์ก่อนว่า p เป็นตัวหารของ |X|

ให้ $(g_1, g_2, \dots , g_p) \in X$ แล้ว $g_1g_2\dots g_p = e$ ดังนั้น $g_p = (g_1g_2\dots g_{p-1})^{-1}$ ในทางกลับกัน ถ้า $g_1, g_2, \dots , g_{p-1} \in G$ และเลือก $g_p = (g_1g_2\dots g_{p-1})^{-1}$ แล้ว $g_1g_2\dots g_p = e$ ดังนั้น

$|X|$ เท่ากับจำนวนวิธีเลือกสมาชิกใน G เพื่อวางลงใน $p-1$ ตำแหน่ง เพราะฉะนั้น $|X| = |G|^{p-1}$ และเพราะ p เป็นตัวหารของ $|G|$ ทำให้ได้ว่า p เป็นตัวหารของ $|G|^{p-1} = |X|$

ต่อไปเรานิยาม $* : S_p \times X \to X$ สำหรับ $(g_1, g_2, \dots, g_p) \in X$ และ $\sigma \in S_p$ โดย

$$*(\sigma,(g_1, g_2, \dots, g_p)) = (g_{\sigma(1)}, g_{\sigma(2)}, \dots, g_{\sigma(p)})$$

จะแสดงว่า * เป็นแอคชันของ S_p บน X ดังนี้

(1) ให้ $(g_1, g_2, \dots, g_p) \in X$ แล้ว

$$\begin{aligned} *((1),(g_1, g_2, \dots, g_p)) &= (g_{(1)(1)}, g_{(1)(2)}, \dots, g_{(1)(p)}) \\ &= (g_1, g_2, \dots, g_p) \end{aligned}$$

และ (2) ให้ $\sigma_1,\sigma_2 \in S_p$ และ $(g_1, g_2, \dots, g_p) \in X$ แล้ว

$$\begin{aligned} *(\sigma_1\sigma_2,(g_1, g_2, \dots, g_p)) &= (g_{\sigma_1\sigma_2(1)}, g_{\sigma_1\sigma_2(2)}, \dots, g_{\sigma_1\sigma_2(p)}) \\ &= (g_{\sigma_1(\sigma_2(1))}, g_{\sigma_1(\sigma_2(2))}, \dots, g_{\sigma_1(\sigma_2(p))}) \\ &= *(\sigma_1, (g_{\sigma_2(1)}, g_{\sigma_2(2)}, \dots, g_{\sigma_2(p)})) \\ &= *(\sigma_1, *(\sigma_2,(g_1, g_2, \dots, g_p)) \end{aligned}$$

ให้ $\sigma = (1\ 2\ \dots\ p) \in S_p$ แล้ว $o(\sigma) = p$ และพิจารณาออร์บิท

$$X_{<\sigma>} = \{(g_1, g_2, \dots, g_p) \in X \mid \sigma(g_1, g_2, \dots, g_p) = (g_1, g_2, \dots, g_p) \}$$

แล้วโดยทฤษฎีบท 3.3.1 จะได้ $|X| \equiv |X_{<\sigma>}| \pmod p$ แต่ p เป็นตัวหารของ $|X|$ ดังนั้น p เป็นตัวหารของ $|X_{<\sigma>}|$ ด้วย แสดงว่า $|X_{<\sigma>}| \geq p$ ดังนั้น $X_{<\sigma>} \neq \varnothing$

ให้ $(g_1, g_2, \dots, g_p) \in X_{<\sigma>}$ แล้ว $\sigma(g_1, g_2, \dots, g_p) = (g_1, g_2, \dots, g_p)$ แต่เนื่องจาก $\sigma(g_1, g_2, \dots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \dots, g_{\sigma(p)}) = (g_2, g_3, \dots, g_p, g_1)$ แสดงว่า $g_1 = g_2 = \dots = g_p$

ให้ $a := g_1 = g_2 = \dots = g_p$ จะได้ $g_1g_2\dots g_p = a^p = e$ เพราะฉะนั้น $o(a) = p$ ❐

3.3.5 บทแทรก ให้ G เป็นกลุ่มจำกัด และ p เป็นจำนวนเฉพาะ แล้ว G เป็น p-กลุ่ม ก็ต่อเมื่อ มี $n \in \mathbb{Z}^+$ ซึ่ง $|G| = p^n$

การพิสูจน์ ให้ G เป็น p-กลุ่ม แล้วจะมีจำนวนเฉพาะ q ที่เป็นตัวหารของ $|G|$ สมมติว่า $q \neq p$ แล้วโดยทฤษฎีบทของโคชี จะมี $a \in G$ ซึ่ง $o(a) = q$ แต่เนื่องจาก G เป็น p-กลุ่ม แสดงว่ามี $k \in \mathbb{Z}^+$ ซึ่ง $o(a) = p^k$ ทำให้ได้ $q = p^k$ เกิดขัดแย้งกับ q เป็นจำนวนเฉพาะ ดังนั้น $q = p$ นั่นคือมีจำนวนเฉพาะ p เพียงหนึ่งเดียวที่เป็นตัวหารของ $|G|$ ดังนั้นจะมี $n \in \mathbb{Z}^+$ ซึ่ง $|G| = p^n$

ในทางกลับกัน สมมติว่า มี $n\in\mathbb{Z}^+$ ซึ่ง $|G| = p^n$ และให้ $g\in G$ แล้วโดยบทแทรก 2.3.12 จะได้ว่า o(g) เป็นตัวหารของ $|G|$ นั่นคือ o(g) เป็นตัวหารของ p^n ดังนั้นจะมีจำนวนเต็ม k ซึ่ง $0 \le k \le n$ ที่ทำให้ $o(g) = p^k$ เพราะฉะนั้น G เป็น p-กลุ่ม ❐

เราจะจบหัวข้อนี้ด้วยตัวอย่างแสดงการประยุกต์ทฤษฎีบทของโคชี ในการวิเคราะห์หาจำนวนกลุ่มทั้งหมดที่มีอันดับ 6

3.3.6 ตัวอย่าง ให้ G เป็นกลุ่มซึ่ง $|G| = 6 = 2\cdot3$ แล้วโดยทฤษฎีบทของโคชี จะได้ว่า G มีสมาชิก a และ b ซึ่ง o(a) = 2 และ o(b) = 3 และโดยข้อสังเกต 2.3.7 ข้อ (2) จะได้ว่า e, a, b, b^2, ab, ab^2 เป็นสมาชิกของ G ที่แตกต่างกันทั้งหมด แต่เพราะ $|G| = 6$ ดังนั้น $G = \{e, a, b, b^2, ab, ab^2\}$ เนื่องจาก $ba \in G$ ดังนั้น $ba \in \{e, a, b, b^2, ab, ab^2\}$

ถ้า $ba = e$ แล้ว $b = a^{-1}$ เนื่องจาก $o(b) = 3$ แต่ $o(a^{-1}) = o(a) = 2$ เกิดเป็นข้อขัดแย้งกันเอง และถ้า $ba = a$ แล้ว $b = e$ จะเกิดข้อขัดแย้ง เพราะ b กับ e เป็นสมาชิกที่แตกต่างกัน และในทำนองเดียวกัน ถ้า $ba = b$ ก็จะเกิดข้อขัดแย้ง เพราะฉะนั้น $ba = ab$ หรือ $ba = ab^2$

กรณี $ba = ab$ แล้ว G เป็นกลุ่มอาบีเลียน เนื่องจาก $\mathbb{Z}_6$ เป็นกลุ่มอาบีเลียนอันดับ 6 ซึ่ง $o(\bar{3}) = 2$ และ $o(\bar{2}) = 3$ เราจึงนิยาม $f : G \to \mathbb{Z}_6$ ดังตาราง

x	e	a	b	b^2	ba	ab^2
f(x)	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{1}$

ตาราง 3.1 : ตารางการนิยามฟังก์ชันถอดแบบ $f : G \to \mathbb{Z}_6$

จากนิยามของ f เห็นได้ชัดว่า f เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งจาก G ไปบน $\mathbb{Z}_6$ ยิ่งไปกว่านั้น ตาราง 3.2 ตาราง 3.3 และตาราง 3.4 แสดงให้เห็นว่า $f(x*y) = f(x) + f(y)$ สำหรับทุกๆ $x,y\in G$ ดังนั้น f เป็นฟังก์ชันถ่ายแบบจาก G ไปบน $\mathbb{Z}_6$ ทำให้ได้ว่า $G \cong \mathbb{Z}_6$

*	**e**	**a**	**b**	**b^2**	**ba**	**ab^2**
e	e	a	b	b^2	ba	ab^2
a	a	e	ba	ab^2	b	b^2
b	b	ba	b^2	e	ab^2	a
b^2	b^2	ab^2	e	b	a	ba
ba	ba	b	ab^2	a	b^2	e
ab^2	ab^2	b^2	a	ba	e	b

ตาราง 3.2 : ตารางแสดงการดำเนินการ * บน G

	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{1}$
	$\bar{3}$	$\bar{0}$	$\bar{5}$	$\bar{1}$	$\bar{2}$	$\bar{4}$
	$\bar{2}$	$\bar{5}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{3}$
	$\bar{4}$	$\bar{1}$	$\bar{0}$	$\bar{2}$	$\bar{3}$	$\bar{5}$
	$\bar{5}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
	$\bar{1}$	$\bar{4}$	$\bar{3}$	$\bar{5}$	$\bar{0}$	$\bar{2}$

ตาราง 3.3 : ตารางแสดงค่าฟังก์ชัน f จากการดำเนินการ * บน G

		f(e) =	f(a) =	f(b) =	f(b^2) =	f(ba) =	f(ab^2) =
	+	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{1}$
f(e) =	$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{4}$	$\bar{5}$	$\bar{1}$
f(a) =	$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{5}$	$\bar{1}$	$\bar{2}$	$\bar{4}$
f(b) =	$\bar{2}$	$\bar{2}$	$\bar{5}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{3}$
f(b^2) =	$\bar{4}$	$\bar{4}$	$\bar{1}$	$\bar{0}$	$\bar{2}$	$\bar{3}$	$\bar{5}$
f(ba) =	$\bar{5}$	$\bar{5}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
f(ab^2) =	$\bar{1}$	$\bar{1}$	$\bar{4}$	$\bar{3}$	$\bar{5}$	$\bar{0}$	$\bar{2}$

ตาราง 3.4 : ตารางแสดงการดำเนินการ + บน $\mathbb{Z}_6$

กรณี ba = ab^2 เนื่องจากใน S_3 เป็นกลุ่มนอนอาบีเลียนอันดับ 6 ซึ่ง o((2 3)) = 2 และ o((1 2 3)) = 3 เราจึงนิยาม g : G $\rightarrow$ S_3 ดังตาราง

x	e	a	b	b^2	ab	ba
g(x)	(1)	(2 3)	(1 2 3)	(1 3 2)	(1 3)	(1 2)

ตาราง 3.5 : ตารางการนิยามฟังก์ชันถอดแบบ g : G $\rightarrow$ S_3

จากนิยามของ g เห็นได้ชัดว่า g เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งจาก G ไปบน S_3 ยิ่งไปกว่านั้น ตาราง 3.6 ตาราง 3.7 และตาราง 3.8 แสดงให้เห็นว่า g(x*y) = g(x)$\circ$g(y) สำหรับทุกๆ x,y$\in$G ดังนั้น g เป็นฟังก์ชันถ่ายแบบจาก G ไปบน S_3 ทำให้ได้ว่า G $\cong$ S_3

*	**e**	**a**	**b**	**b^2**	**ab**	**ba**
e	e	a	b	b^2	ab	ba
a	a	e	ab	ba	b	b^2
b	b	ba	b^2	e	a	ab
b^2	b^2	ab	e	b	ba	a
ab	ab	b^2	ba	a	e	b
ba	ba	b	a	ab	b^2	e

ตาราง 3.6 : ตารางแสดงการดำเนินการ * บน G

	(1)	(2 3)	(1 2 3)	(1 3 2)	(1 3)	(1 2)
	(2 3)	(1)	(1 3)	(1 2)	(1 2 3)	(1 3 2)
	(1 2 3)	(1 2)	(1 3 2)	(1)	(2 3)	(1 3)
	(1 3 2)	(1 3)	(1)	(1 2 3)	(1 2)	(2 3)
	(1 3)	(1 3 2)	(1 2)	(2 3)	(1)	(1 2 3)
	(1 2)	(1 2 3)	(2 3)	(1 3)	(1 3 2)	(1)

ตาราง 3.7 : ตารางแสดงค่าฟังก์ชัน g จากการดำเนินการ * บน G

		g(e) =	g(a) =	g(b) =	$g(b^2)$ =	g(ab) =	g(ba) =
	∘	(1)	(2 3)	(1 2 3)	(1 3 2)	(1 3)	(1 2)
g(e) =	(1)	(1)	(2 3)	(1 2 3)	(1 3 2)	(1 3)	(1 2)
g(a) =	(2 3)	(2 3)	(1)	(1 3)	(1 2)	(1 2 3)	(1 3 2)
g(b) =	(1 2 3)	(1 2 3)	(1 2)	(1 3 2)	(1)	(2 3)	(1 3)
$g(b^2)$ =	(1 3 2)	(1 3 2)	(1 3)	(1)	(1 2 3)	(1 2)	(2 3)
g(ab) =	(1 3)	(1 3)	(1 3 2)	(1 2)	(2 3)	(1)	(1 2 3)
g(ba) =	(1 2)	(1 2)	(1 2 3)	(2 3)	(1 3)	(1 3 2)	(1)

ตาราง 3.8 : ตารางแสดงการดำเนินการ ∘ บน S_3

เพราะฉะนั้นกลุ่มอันดับ 6 ที่แตกต่างกันทั้งหมดมีจำนวนทั้งสิ้น 2 กลุ่มเมื่อไม่นับการถอดแบบกัน ❐

3.4 นอร์มัลไลเซอร์ (Normalizer)

ให้ G เป็นกลุ่ม และ $\mathscr{S}$ = {H | H เป็นกลุ่มย่อยของ G} และนิยาม * : G × $\mathscr{S}$ → $\mathscr{S}$ สำหรับทุกๆ H∈$\mathscr{S}$ และ g∈G โดย *(g, H) = gHg^{-1} แล้วโดยทฤษฎีบทประกอบ 3.1.2 เราจะได้ $\mathscr{S}$ เป็น G-เซต

ให้ H ∈ $\mathscr{S}$ และ G_H = {g∈G | gHg^{-1} = H} แล้วโดยทฤษฎีบท 3.1.5 จะได้ว่า G_H เป็นกลุ่มย่อยของ G

ให้ g∈G_H แล้ว g∈G และ gHg^{-1} = H และโดยทฤษฎีบท 2.3.18 จะได้ว่า H เป็นกลุ่มย่อยปรกติของ G_H

ให้ K เป็นกลุ่มย่อยของ G ซึ่ง H เป็นกลุ่มย่อยปรกติของ K เราจะแสดงว่า K ⊆ G_H

ให้ g∈K เนื่องจาก K เป็นกลุ่มย่อยของ G จะได้ว่า g∈G และเนื่องจาก H เป็นกลุ่มย่อยปรกติของ K โดยทฤษฎีบท 2.3.18 จะได้ว่า aHa^{-1} = H สำหรับทุกๆ a∈K ทำให้ได้ gHg^{-1} = H ซึ่งแสดงว่า g∈G_H ดังนั้น K ⊆ G_H เพราะฉะนั้น G_H เป็นกลุ่มย่อยใหญ่สุดเฉพาะกลุ่ม (maximal subgroup)ของ G ซึ่งมี H เป็นกลุ่มย่อยปรกติ

3.4.1 บทนิยาม เราเรียกกลุ่มย่อย G_H ใน G ว่า **นอร์มัลไลเซอร์ (normalizer) ของ** H **ใน** G และเขียนแทนด้วยสัญลักษณ์ N[H]

3.4.2 ทฤษฎีบท ให้ p เป็นจำนวนเฉพาะ และ G เป็นกลุ่มจำกัด ถ้า H เป็น p-กลุ่มย่อย ของ G แล้ว [N[H] : H] ≡ [G : H] (mod p)

การพิสูจน์ ให้ $\mathscr{A}$ = {gH | g∈G} แล้ว |$\mathscr{A}$| = [G : H] และนิยาม φ : H × $\mathscr{A}$ → $\mathscr{A}$ สำหรับทุกๆ h∈H และ g∈G โดย φ(h, gH) = (hg)H

ให้ h_1, h_2∈H และ g_1, g_2∈G โดยที่ $(h_1, g_1H) = (h_2, g_2H)$ แล้ว $h_1 = h_2$ และ $g_1H = g_2H$ ดังนั้น $g_1^{-1}g_2$∈H แต่เนื่องจาก $(h_1g_1)^{-1}(h_2g_2) = (g_1^{-1}h_1^{-1})(h_2g_2) = g_1^{-1}(h_1^{-1}h_2)g_2 = g_1^{-1}eg_2 = g_1^{-1}g_2$ ∈ H ดังนั้น $(h_1g_1)H = (h_2g_2)H$ และทำให้ได้ $\varphi(h_1, g_1H) = \varphi(h_2, g_2H)$ เพราะฉะนั้น φ เป็นฟังก์ชัน

เราจะแสดงว่า $\mathscr{A}$ เป็น H-เซต ดังนี้

(1) ให้ g∈G แล้ว φ(e, gH) = (eg)H = gH

และ (2) ให้ h_1, h_2∈H และ gH ∈ $\mathscr{A}$ แล้ว $\varphi(h_1h_2, gH) = ((h_1h_2)g)H = (h_1(h_2g))H = \varphi(h_1, (h_2g)H) = \varphi(h_1, \varphi(h_2, gH))$

เพราะฉะนั้น φ เป็นแอคชันของ H บน $\mathscr{A}$

ต่อไปให้ $g \in G$ และนิยาม $\mathscr{A}_H = \{gH \in \mathscr{A} \mid gH = h(gH)$ สำหรับทุกๆ $h \in H\}$ (ดูวิธีการนิยามในหัวข้อ 3.3) และ $\mathscr{B} = \{gH \in \mathscr{A} \mid g \in N[H]\}$ แล้วจะแสดงว่า $\mathscr{A}_H = \mathscr{B}$

ให้ $gH \in \mathscr{A}_H$ แล้ว $gH \in \mathscr{A}$ และ $gH = h(gH)$ สำหรับทุกๆ $h \in H$ เราจะแสดงว่า $gH \in \mathscr{B}$ ให้ $h \in H$ แล้ว $gH = h(gH) = (hg)H$ ทำให้ได้ว่า $H = g^{-1}hgH$ และทำให้ได้ว่า $g^{-1}hg = g^{-1}h(g^{-1})^{-1} \in H$ แล้ว H เป็นกลุ่มย่อยปรกติของ G ดังนั้น $gHg^{-1} = H$ และได้ว่า $g \in N[H]$ เพราะฉะนั้น $gH \in \mathscr{B}$ ทำให้ได้ว่า $\mathscr{A}_H \subseteq \mathscr{B}$

บทกลับให้ $gH \in \mathscr{B}$ แล้ว $gH \in \mathscr{A}$ และ $g \in N[H]$ เราจะแสดงว่า $gH \in \mathscr{A}_H$ เนื่องจาก $g \in N[H]$ จะได้ว่า $gHg^{-1} = H$ ดังนั้น H เป็นกลุ่มย่อยปรกติของ G ให้ $h \in H$ แล้ว $g^{-1}h(g^{-1})^{-1} = g^{-1}hg \in H$ ทำให้ได้ $g^{-1}hgH = H$ และได้ว่า $h(gH) = (hg)H = gH$ ดังนั้น $gH \in \mathscr{A}_H$ ทำให้ได้ว่า $\mathscr{B} \subseteq \mathscr{A}_H$

ดังนั้น $\mathscr{A}_H = \mathscr{B}$ แต่ $|\mathscr{B}| = [N[H] : H]$ จะได้ว่า $|\mathscr{A}_H| = [N[H] : H]$ และเนื่องจาก H เป็น p-กลุ่ม โดยบทแทรก 3.3.5 จะมี $n \in \mathbb{Z}^+$ ซึ่ง $|H| = p^n$ และโดยทฤษฎีบท 3.3.1 จะได้ว่า $|\mathscr{A}| \equiv |\mathscr{A}_H| \pmod p$ เพราะฉะนั้น $[G : H] \equiv [N[H] : H] \pmod p$ ❐

3.4.3 บทแทรก ให้ p เป็นจำนวนเฉพาะและ G เป็นกลุ่มจำกัด ถ้า H เป็น p-กลุ่มย่อยของ G และ p เป็นตัวหารของ $[G : H]$ แล้ว $N[H] \neq H$

การพิสูจน์ ให้ H เป็น p-กลุ่มย่อย ของ G และ p เป็นตัวหารของ $[G : H]$ สมมติว่า $N[H] = H$ แล้ว $[N[H] : H] = 1$ โดยทฤษฎีบท 3.4.2 จะได้ว่า $1 \equiv [G : H] \pmod p$ นั่นคือ p เป็นตัวหารของ $1 - [G : H]$ เกิดข้อขัดแย้งกับสมมติฐานที่ว่า p เป็นตัวหารของ $[G : H]$ เพราะฉะนั้น $N[H] \neq H$ ❐

บทที่ 4
ทฤษฎีบทซีโลว์และการประยุกต์
Sylow Theorems and Applications

ในบทที่ผ่านมา เราได้ศึกษาแอคชันของกลุ่มบนเซตและได้ประยุกต์แอคชันของกลุ่มบนเซตในการพิสูจน์ทฤษฎีบทของโคชีและนอร์มัลไลเซอร์ ในบทนี้เราจะนำผลของการศึกษาดังกล่าวมาประยุกต์เพื่อการพิสูจน์ทฤษฎีบทซีโลว์ ซึ่งประกอบด้วย 3 ทฤษฎีบท ทฤษฎีบทซีโลว์เหล่านี้ได้รับการยกย่องว่าเป็นรากฐานของการศึกษากลุ่มจำกัด และในท้ายบทเราจะแสดงตัวอย่างการวิเคราะห์กลุ่มจำกัดด้วยการประยุกต์ทฤษฎีบทซีโลว์

4.1 ทฤษฎีบทซีโลว์ (Sylow Theorems)

ทฤษฎีบทของลากรองจ์ได้กล่าวว่า ถ้า G เป็นกลุ่มจำกัดและ H เป็นกลุ่มย่อยของ G แล้ว |H| จะเป็นตัวหารของ |G| ซึ่ง Peter Ludwig Sylow นักคณิตศาสตร์ชาวนอร์เวย์ ได้แสดงว่าบทกลับของทฤษฎีบทนี้อาจไม่เป็นจริง นั่นคือ ถ้าให้ $|G| = n$ และ $m|n$ แล้ว เราอาจหากลุ่มย่อยของ G ที่มีอันดับเท่ากับ m ไม่ได้ ตัวอย่างเช่น A_4 เป็นกลุ่มอันดับ 12 แต่ A_4 ไม่มีกลุ่มย่อยอันดับ 6 (ตัวอย่าง 4.2.1) เป็นต้น อย่างไรก็ตามท่านยังได้ศึกษาหาคำตอบที่ใกล้เคียงกับบทกลับของทฤษฎีบทลากรองจ์จนพิสูจน์ได้ทฤษฎีบทซีโลว์ 3 ทฤษฎีบทต่อไปนี้

4.1.1 ทฤษฎีบท *ทฤษฎีบทที่หนึ่งของซีโลว์ (The First Sylow's Theorem)*

ให้ G เป็นกลุ่มจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวกและ p เป็นจำนวนเฉพาะซึ่ง $(p, s) = 1$ แล้วจะมีกลุ่มย่อยของ G อันดับ p^k สำหรับแต่ละ k ซึ่ง $1 \le k \le m$ และแต่ละกลุ่มย่อยอันดับ p^k เมื่อ $k = 1, 2, \ldots, m - 1$ จะเป็นกลุ่มย่อยปรกติของกลุ่มย่อยอันดับ p^{k+1} อย่างน้อย 1 กลุ่มย่อย

การพิสูจน์ เริ่มต้นเราจะแสดงโดยอุปนัยเชิงคณิตศาสตร์ว่า G จะมีกลุ่มย่อยอันดับ p^k สำหรับแต่ละ k ซึ่ง $1 \le k \le m$ อย่างแรกโดยทฤษฎีบทของโคชี จะมี $a \in G$ ซึ่ง $o(a) = p$ แล้ว $\langle a \rangle$ เป็นกลุ่มย่อยของ G ซึ่ง $|\langle a \rangle| = p$ นั่นคือ G มีกลุ่มย่อยอันดับ p ต่อไปให้ H เป็นกลุ่มย่อยของ G ซึ่ง

$|H| = p^k$ โดยที่ $1 \le k < m$ แล้ว $m - k > 0$ แต่ $[G : H] = \frac{|G|}{|H|} = \frac{p^m s}{p^k} = p^{m-k}s = p(p^{m-k-1}s)$ ทำให้ได้ว่า p หาร $[G : H]$ ลงตัว ดังนั้นจะได้โดยทฤษฎีบท 4.2.2 ว่า $[N[H] : H] \equiv [G : H] \pmod p$ แต่ p หาร $[G : H]$ ลงตัว ดังนั้น p จึงหาร $[N[H] : H]$ ลงตัวด้วย และเนื่องจาก H เป็นกลุ่มย่อยปรกติของ $N[H]$ ดังนั้น $N[H]/H$ เป็นกลุ่มผลหารซึ่ง p เป็นตัวหารของ $\left| N[H]/H \right| = \frac{|N[H]|}{|H|}$ ทำให้ได้โดยทฤษฎีบทของโคชีว่า $N[H]/H$ มีกลุ่มย่อย K อันดับ p

เรานิยาม $\gamma : N[H] \to N[H]/H$ โดย $\gamma(g) = gH$ สำหรับทุกๆ $g \in N[H]$ แล้วจะแสดงว่า γ เป็นฟังก์ชันถ่ายแบบ

ให้ $g_1, g_2 \in N[H]$ โดยที่ $g_1 = g_2$ แล้ว $g_1H = Hg_1$ และ $g_2H = Hg_2$ แต่ $g_1 = g_2$ ทำให้ได้ $g_1H = Hg_2$ และ $g_2H = Hg_2$ ดังนั้น $g_1H = g_2H$ นั่นคือ $\gamma(g_1) = \gamma(g_2)$ เพราะฉะนั้น γ เป็นฟังก์ชัน และจาก $\gamma(g_1g_2) = (g_1g_2)H = (g_1H)(g_2H) = \gamma(g_1)\gamma(g_2)$ จะได้ว่า γ เป็นฟังก์ชันถ่ายแบบ

ต่อไปเราจะแสดงว่า $\gamma^{-1}(K) = \{x \in N[H] \mid \gamma(x) \in K\}$ เป็นกลุ่มย่อยของ $N[H]$ อย่างแรกเห็นได้ชัดว่า $e \in \gamma^{-1}(K)$ เพราะ $e \in G$ และ $eH = H = He$ ซึ่งแสดงว่า $e \in N[H]$ และ $\gamma(e) = eH = H \in K$

ให้ $x_1, x_2 \in \gamma^{-1}(K)$ แล้ว $x_1, x_2 \in N[H]$ และ $\gamma(x_1) \in K$ และ $\gamma(x_2) \in K$ ทำให้ได้ว่า $x_1H \in K$ และ $x_2H \in K$ เนื่องจาก $x_2 \in N[H]$ ดังนั้น $x_2 \in G$ และ $x_2H = Hx_2$ แต่ $x_1x_2^{-1} \in G$ และจาก K เป็นกลุ่มย่อยของ $N[H]/H$ ทำให้ได้ว่า $(x_2H)^{-1} = x_2^{-1}H \in K$ และ $(x_1H)(x_2^{-1}H) = (x_1x_2^{-1})H \in K$ นั่นคือ $\gamma(x_1x_2^{-1}) \in K$ และเพราะว่า $x_1 \in N[H]$ จะได้ $x_1H = Hx_1$ และเพราะว่า $(x_2H)^{-1} = (Hx_2)^{-1}$ จะได้ $x_2^{-1}H = Hx_2^{-1}$ ดังนั้น $(x_1H)(x_2^{-1}H) = (Hx_1)(Hx_2^{-1})$ นั่นคือ $(x_1x_2^{-1})H = H(x_1x_2^{-1})$ แสดงว่า $x_1x_2^{-1} \in N[H]$ ดังนั้น $x_1x_2^{-1} \in \gamma^{-1}[K]$ เพราะฉะนั้น $\gamma^{-1}(K)$ เป็นกลุ่มย่อยของ $N[H]$ จึงทำให้ $\gamma^{-1}(K)$ เป็นกลุ่มย่อยของ G ด้วย และสังเกตว่า $|\gamma^{-1}(K)| = p^{k+1}$ เราจึงสรุปได้ว่า G มีกลุ่มย่อยอันดับ p^n สำหรับแต่ละ n ซึ่ง $1 \le n \le m$

สุดท้ายเราจะแสดงว่าแต่ละกลุ่มย่อยอันดับ p^k ซึ่ง $k = 1, 2, \ldots, m - 1$ จะเป็นกลุ่มย่อยปรกติของกลุ่มย่อยอันดับ p^{k+1} อย่างน้อย 1 กลุ่มย่อย

เนื่องจาก H เป็นกลุ่มย่อยของ $\gamma^{-1}(K)$ ซึ่ง $|\gamma^{-1}(K)| = p^{k+1}$ และ $H \ne \gamma^{-1}(K)$ และ H เป็นกลุ่มย่อยปรกติของ $N[H]$ ดังนั้น H จึงเป็นกลุ่มย่อยปรกติของ $\gamma^{-1}(K)$ ❐

4.1.2 บทนิยาม ให้ G เป็นกลุ่มจำกัด และ p เป็นจำนวนเฉพาะ เรากล่าวว่า H เป็น **กลุ่มย่อย p-ซีโลว์ (p-Sylow subgroup)** ของ G ถ้า H เป็น p-กลุ่มย่อยใหญ่สุดเฉพาะกลุ่ม (maximal p-subgroup) ของ G (นั่นคือ ถ้า H เป็น p-กลุ่มย่อยของ G และ K เป็น p-กลุ่มย่อยของ G ซึ่ง $K \supset H$ แล้ว $K = H$)

ให้ G เป็นกลุ่มจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะซึ่ง (p, s) = 1 ทฤษฎีบทที่หนึ่งของซีโลว์ได้แสดงว่ากลุ่มย่อย p-ซีโลว์ของ G ล้วนเป็นกลุ่มย่อยอันดับ p^m ทฤษฎีบทต่อไปจะแสดงว่าถ้า H เป็นกลุ่มย่อย p-ซีโลว์ ของ G แล้ว ทุกๆ สังยุคของ H จะเป็นกลุ่มย่อย p-ซีโลว์ของ G ด้วย

4.1.3 ทฤษฎีบท ให้ G เป็นกลุ่มจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะซึ่ง (p, s) = 1 ถ้า H เป็นกลุ่มย่อย p-ซีโลว์ ของ G แล้ว gHg^{-1} เป็นกลุ่มย่อย p-ซีโลว์ ของ G สำหรับทุกๆ $g \in G$

การพิสูจน์ ให้ H เป็นกลุ่มย่อย p-ซีโลว์ของ G แล้วโดยทฤษฎีบท 4.1.1 จะได้ว่า H มีอันดับ p^m ต่อไปให้ $g \in G$ เราจะแสดงว่า $|gHg^{-1}| = |H|$ ด้วยการนิยาม $\alpha : H \rightarrow gHg^{-1}$ โดย $\alpha(h) = ghg^{-1}$ สำหรับทุกๆ $h \in H$ แล้วจะแสดงว่า α เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก H ไปบน gHg^{-1}

ให้ $h_1, h_2 \in H$ โดยที่ $h_1 = h_2$ และให้ $g \in G$ จะได้ $gh_1g^{-1} = gh_2g^{-1}$ นั่นคือ $\alpha(h_1) = \alpha(h_2)$ ดังนั้น α เป็นฟังก์ชัน

ต่อไปให้ $h_1, h_2 \in H$ โดยที่ $\alpha(h_1) = \alpha(h_2)$ แล้ว $gh_1g^{-1} = gh_2g^{-1}$ ทำให้ได้ $g^{-1}(gh_1g^{-1})g = g^{-1}(gh_2g^{-1})g$ นั่นคือ $(g^{-1}g)h_1(g^{-1}g) = (g^{-1}g)h_2(g^{-1}g)$ ดังนั้น $h_1 = h_2$ เพราะฉะนั้น α เป็นฟังก์ชันหนึ่งต่อหนึ่ง

สุดท้ายให้ $k \in gHg^{-1}$ แล้วเลือก $h = g^{-1}kg$ ทำให้ได้ $\alpha(h) = \alpha(g^{-1}kg) = g(g^{-1}kg)g^{-1} = k$ เพราะฉะนั้น α เป็นฟังก์ชันไปบน

เนื่องจาก α เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก H ไปบน gHg^{-1} ดังนั้น $|gHg^{-1}| = |H|$ ทำให้ได้ $|gHg^{-1}| = p^m$

ต่อไปให้ $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$ แล้ว $(gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = gh_1(g^{-1}g)h_2^{-1}g^{-1} = g(h_1h_2^{-1})g^{-1} \in gHg^{-1}$ ดังนั้น gHg^{-1} เป็นกลุ่มย่อยของ G

เนื่องจาก gHg^{-1} เป็นกลุ่มย่อยอันดับ p^m ของ G ดังนั้น gHg^{-1} เป็นกลุ่มย่อย p-ซีโลว์ของ G ❐

4.1.4 ทฤษฎีบท *ทฤษฎีบทที่สองของซีโลว์ (The Second Sylow's Theorem)*

ให้ G เป็นกลุ่มจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะซึ่ง (p, s) = 1 แล้วกลุ่มย่อย p-ซีโลว์ของ G เป็นสังยุคของกันและกัน

การพิสูจน์ ให้ H_1 และ H_2 เป็นกลุ่มย่อย p-ซีโลว์ ของ G แล้ว $|H_1| = |H_2| = p^m$ ให้ $S := \{xH_1 | x \in G\}$ และนิยาม $\varphi : H_2 \times S \to S$ โดย $\varphi(y, xH_1) = (yx)H_1$ สำหรับทุกๆ $y \in H_2$ และ $x \in G$

ให้ $y_1, y_2 \in H_2$ และ $x_1H_1, x_2H_1 \in S$ โดยที่ $(y_1, x_1H_1) = (y_2, x_2H_1)$ แล้ว $y_1 = y_2$ และ $x_1H_1 = x_2H_1$ ดังนั้น $x_1^{-1}x_2 \in H_1$ นั่นคือ $x_1^{-1}ex_2 \in H_1$ แต่ $y_1 = y_2$ จึงได้ว่า $x_1^{-1}y_1^{-1}y_2x_2 \in H_1$ นั่นคือ $(y_1x_1)^{-1}(y_2x_2) \in H_1$ แสดงว่า $(y_1x_1)H_1 = (y_2x_2)H_1$ ทำให้ได้ $\varphi(y_1, x_1H_1) = \varphi(y_2, x_2H_1)$ ดังนั้น φ เป็นฟังก์ชัน

ต่อไปจะแสดงว่า S เป็น H_2-เซต

(1) ให้ $x \in G$ แล้ว $\varphi(e, xH_1) = (ex)H_1 = xH_1$

และ (2) ให้ $xH_1 \in S$ และ $y_1, y_2 \in H_2$ แล้ว $\varphi(y_1y_2, xH_1) = ((y_1y_2)x)H_1 = (y_1(y_2x))H_1 = \varphi(y_1, (y_2x)H_1) = \varphi(y_1, \varphi(y_2, xH_1))$

จาก (1) และ (2) จะได้ว่า φ เป็นแอคชันของ H_2 บน S เพราะฉะนั้น S เป็น H_2-เซต

ให้ $x \in H_1$ แล้วโดยนิยามของ X_G (ดังกล่าวในหัวข้อ 3.3) เราจะได้

$$S_{H_2} = \{xH_1 \in S \mid \varphi(y, xH_1) = xH_1 \text{ สำหรับทุกๆ } y \in H_2\}$$
$$= \{xH_1 \in S \mid (yx)H_1 = xH_1 \text{ สำหรับทุกๆ } y \in H_2\}$$

ทำให้ได้โดยทฤษฎีบท 3.3.1 ว่า $|S_{H_2}| \equiv |S| \pmod p$ แต่เพราะ $|S| = [G : H_1] = \frac{|G|}{|H_1|} = \frac{p^m s}{p^m} = s$ และ (p, s) = 1 แล้ว p ไม่เป็นตัวหารของ |S| ทำให้ได้ว่า $|S_{H_2}| \neq 0$ นั่นคือ $S_{H_2} \neq \varnothing$

ให้ $xH_1 \in S_{H_2}$ แล้ว $yxH_1 = xH_1$ สำหรับทุกๆ $y \in H_2$ ซึ่งทำให้ $x^{-1}yxH_1 = H_1$ สำหรับทุกๆ $y \in H_2$ แสดงว่า $x^{-1}yx \in H_1$ สำหรับทุกๆ $y \in H_2$ ดังนั้น $x^{-1}H_2x$ เป็นกลุ่มย่อยของ H_1 แต่จาก $|H_1| = |H_2|$ เราจะได้ $H_1 = x^{-1}H_2x$ ❐

4.1.5 บทแทรก ให้ G เป็นกลุ่มจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะซึ่ง (p, s) = 1 ถ้า K เป็นกลุ่มย่อย p-ซีโลว์ ของ G แล้ว K เป็นกลุ่มย่อยปรกติของ G ก็ต่อเมื่อ K เป็นกลุ่มย่อย p-ซีโลว์เพียงกลุ่มย่อยเดียวของ G

การพิสูจน์ สมมติว่า K เป็นกลุ่มย่อยปรกติของ G และให้ P เป็นกลุ่มย่อย p-ซีโลว์ของ G แล้ว โดยทฤษฎีบทที่สองของซีโลว์ จะมี $x \in G$ ซึ่ง $P = x^{-1}Kx$ แต่ K เป็นกลุ่มย่อยปรกติของ G จะได้ว่า $P = x^{-1}Kx = K$ ดังนั้น K เป็นกลุ่มย่อย p-ซีโลว์เพียงกลุ่มย่อยเดียวของ G

ในทางกลับกัน สมมติว่า K เป็นกลุ่มย่อย p-ซีโลว์ เพียงหนึ่งเดียวของ G แล้ว $x^{-1}Kx = K$ สำหรับทุกๆ $x \in G$ ดังนั้น K เป็นกลุ่มย่อยปรกติของ G ❐

ต่อไปเราจะพิสูจน์ทฤษฎีบทที่สามของซีโลว์ซึ่งจะทำให้เราทราบถึงข้อมูลเกี่ยวกับจำนวนกลุ่มย่อย p-ซีโลว์ทั้งหมดของกลุ่มจำกัด G

4.1.6 ทฤษฎีบท *ทฤษฎีบทที่สามของซีโลว์ (The Third Sylow's Theorem)*

ให้ G เป็นกลุ่มจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวกและ p เป็นจำนวนเฉพาะซึ่ง $(p, s) = 1$ และให้ n_p เป็นจำนวนกลุ่มย่อย p-ซีโลว์ทั้งหมดของ G แล้ว $n_p \equiv 1 \pmod p$ และ n_p เป็นตัวหารของ $|G|$

การพิสูจน์ ให้ H เป็นกลุ่มย่อย p-ซีโลว์ ของ G แล้ว $|H| = p^m$ และให้ S เป็นเซตของกลุ่มย่อย p-ซีโลว์ทั้งหมดของ G แล้ว $n_p = |S|$

นิยาม $\varphi : H \times S \to S$ โดย $\varphi(x, T) = xTx^{-1}$ สำหรับทุกๆ $x \in H$ และ $T \in S$ แล้วจะแสดงว่า S เป็น H-เซต

(1) ให้ $T \in S$ แล้ว $\varphi(e, T) = eTe^{-1} = T$

(2) ให้ $T \in S$ แล้ว $x_1, x_2 \in H$ แล้ว $\varphi(x_1x_2, T) = (x_1x_2)T(x_1x_2)^{-1} = (x_1x_2)T(x_2^{-1}x_1^{-1})$ $= x_1(x_2 T x_2^{-1}) x_1^{-1} = \varphi(x_1, x_2 T x_2^{-1}) = \varphi(x_1, \varphi(x_2, T))$

จาก (1) และ (2) สรุปได้ว่า φ เป็นแอคชันของ H บน S เพราะฉะนั้น S เป็น H-เซต

โดยนิยามของ X_G (ดังกล่าวในหัวข้อ 3.3) เราจะได้

$S_H = \{T \in S \mid \varphi(x, T) = T$ สำหรับทุกๆ $x \in H\} = \{T \in S \mid xTx^{-1} = T$ สำหรับทุกๆ $x \in H\}$

แล้วโดยทฤษฎีบท 3.3.1 จะได้ว่า $|S_H| \equiv |S| \pmod p$

ให้ $T \in S_H$ แล้ว $xTx^{-1} = T$ สำหรับทุกๆ $x \in H$ ดังนั้น H เป็นกลุ่มย่อยของ N[T] และแน่นอนว่า T ก็เป็นกลุ่มย่อยของ N[T] จึงได้ว่า H และ T ต่างเป็นกลุ่มย่อย p-ซีโลว์ของ N[T] ดังนั้นโดยทฤษฎีบทที่สองของซีโลว์ จะมี $x \in N[T]$ ซึ่ง $H = x^{-1}Tx$ แต่ T เป็นกลุ่มย่อยปรกติของ N[T] ทำให้ได้ว่า $Tx = xT$ และได้ $H = x^{-1}Tx = x^{-1}xT = T$ ดังนั้น $S_H = \{T\}$ นั่นคือ $|S_H| = 1$ และโดยทฤษฎีบท 3.3.1 จะได้ว่า $|S| \equiv |S_H| \pmod p$ นั่นคือ $n_p \equiv 1 \pmod p$

ต่อไปเรานิยาม $* : G \times S \to S$ โดย $*(g, T) = gTg^{-1}$ สำหรับทุกๆ $g \in G$ และ $T \in S$ แล้ว G เป็น S-เซต ดังนั้นทุกๆ กลุ่มย่อย p-ซีโลว์ ของ G เป็นสังยุคซึ่งกันและกัน จึงทำให้มีออร์บิทใน S ภายใต้ G เพียง 1 ออร์บิทเท่านั้น

ให้ $H \in S$ แล้ว $G_H = \{g \in G \mid gHg^{-1} = H\} = N[H]$ โดยทฤษฎีบท 3.1.5 จะได้ n_p = ขนาดของออร์บิทใน H $= [G : G_H]$ เนื่องจาก $|G| = |G_H|[G : G_H]$ เพราะฉะนั้น $[G : G_H]$ หาร $|G|$ ลงตัว นั่นคือ n_p หาร $|G|$ ลงตัว ❐

4.2 ตัวอย่างการประยุกต์ทฤษฎีบทของซีโลว์

(Examples of Applications of Sylow Theorems)

ในหัวข้อนี้จะแสดงตัวอย่างการประยุกต์ทฤษฎีบทของซีโลว์ในการวิเคราะห์กลุ่มจำกัดบางกลุ่ม โดยขอเริ่มต้นด้วยตัวอย่างการประยุกต์ทฤษฎีบทของซีโลว์แสดงตัวอย่างค้านบทกลับของทฤษฎีบทของลากรองจ์

4.2.1 ตัวอย่าง จงแสดงว่า A_4 ไม่มีกลุ่มย่อยอันดับ 6

การพิสูจน์ เพื่อความสะดวกจะขอแสดงสมาชิกทั้งหมดของ A_4 อีกครั้งดังนี้

(1)	$\sigma_8 = (1\ 2)(3\ 4)$	$\delta_3 = (1\ 3\ 4)$	$\delta_6 = (1\ 4\ 2)$
$\sigma_2 = (1\ 3)(2\ 4)$	$\delta_1 = (2\ 3\ 4)$	$\delta_4 = (1\ 4\ 3)$	$\delta_7 = (1\ 2\ 3)$
$\sigma_5 = (1\ 4)(2\ 3)$	$\delta_2 = (2\ 4\ 3)$	$\delta_5 = (1\ 2\ 4)$	$\delta_8 = (1\ 3\ 2)$

สมมติว่า A_4 มีกลุ่มย่อยอันดับ 6 ให้ H เป็นกลุ่มย่อยของ A_4 ซึ่ง $|H| = 6$ เนื่องจาก $\sigma_2^2 = \sigma_5^2 = \sigma_8^2 = (1)$ ดังนั้น $o(\sigma_2) = o(\sigma_5) = o(\sigma_8) = 2$ และ $o(\delta_j) = 3$ สำหรับทุกๆ $j \in \{1, 2, \dots, 8\}$ เนื่องจาก $|H| = 6$ โดยทฤษฎีบทที่หนึ่งของซีโลว์ จะได้ว่า H มีกลุ่มย่อยอันดับ 3 ดังนั้นจะมี $i \in \{1, 2, \dots, 8\}$ ซึ่ง $\delta_i \in H$ เราสมมติให้ $\delta_1 \in H$ แล้ว $\{(1), \delta_1, \delta_2^2 = \delta_2\} \subseteq H$ โดยทฤษฎีบทที่หนึ่งของซีโลว์ จะได้ว่า H มีกลุ่มย่อยอันดับ 2 แล้วจะมี $k \in \{2, 5, 8\}$ ซึ่ง $\sigma_k \in H$ และถ้า $\sigma_2 \in H$ แล้ว $\sigma_2\delta_1 = \delta_4$ และ $\delta_1\sigma_2 = \delta_8$ ทำให้ได้ว่าถ้า $\sigma_2 \in H$ แล้ว $\delta_4 \in H$ ยิ่งไปกว่านั้น $\delta_4^2 = \delta_3$ และ $\delta_8^2 = \delta_7$ ซึ่งหมายความว่า H ประกอบด้วยสมาชิกที่แตกต่างกันอย่างน้อย 8 ตัว ซึ่งขัดแย้งกับ $|H| = 6$ ดังนั้น $\sigma_2 \notin H$ ในทำนองเดียวกัน $\sigma_5 \notin H$ และ $\sigma_8 \notin H$ ทำให้ H ไม่มีกลุ่มย่อยอันดับ 2 ซึ่งขัดแย้งกับทฤษฎีบทที่หนึ่งของซีโลว์ เพราะฉะนั้น A_4 ไม่มีกลุ่มย่อยอันดับ 6 ❐

4.2.2 บทนิยาม เรากล่าวว่ากลุ่ม G เป็น **กลุ่มเชิงเดียว (simple group)** ถ้า G มีเพียง {e} และ G เท่านั้นที่เป็นกลุ่มย่อยปรกติของ G นั่นคือ ถ้า H เป็นกลุ่มย่อยปรกติของ G แล้ว H = {e} หรือ H = G

เบิร์นไซด์ (ค.ศ. 1853 – 1927) นักคณิตศาสตร์ชาวอังกฤษ ผู้ซึ่งสนใจศึกษาทฤษฎีที่เกี่ยวกับกลุ่มจำกัดโดยเฉพาะกลุ่มเชิงเดียว ท่านเป็นผู้ตั้งข้อความคาดการณ์ว่า "กลุ่มเชิงเดียวที่เป็นกลุ่มนอนอาบีเลียนจะมีอันดับเป็นจำนวนคู่" และข้อคาดการณ์นี้ได้รับการพิสูจน์โดย J. Thomson และ W. Feit นักคณิตศาสตร์ชาวอเมริกัน ในปี ค.ศ. 1964

4.2.3 ทฤษฎีบท *ทฤษฎีบทของอาเบล (Abel's Theorem)*

A_n เป็นกลุ่มเชิงเดียว สำหรับทุกๆ จำนวนเต็มบวก $n \neq 4$ ❐

ต่อไปนี้เป็นตัวอย่างการประยุกต์ทฤษฎีบทของซีโลว์ ในการแสดงว่ากลุ่มอันดับ 12, 18 และ 30 ต่างไม่เป็นกลุ่มเชิงเดียว

4.2.4 ตัวอย่าง จงแสดงว่ากลุ่มอันดับ 12 ไม่เป็นกลุ่มเชิงเดียว

การพิสูจน์ ให้ G เป็นกลุ่ม ซึ่ง $|G| = 12 = 2^2 \cdot 3$ แล้ว G จะมีกลุ่มย่อย 2-ซีโลว์ อันดับ 4 และมีกลุ่มย่อย 3-ซีโลว์ อันดับ 3 และโดยทฤษฎีบทที่สามของซีโลว์ จะได้ว่า

$n_2 \equiv 1 (\text{mod } 2)$ และ $n_2 \mid 12$ ซึ่งทำให้ได้ $n_2 \in \{1, 3\}$

$n_3 \equiv 1 (\text{mod } 3)$ และ $n_3 \mid 12$ ซึ่งทำให้ได้ $n_3 \in \{1, 4\}$

สมมติว่า $n_2 \neq 1$ และ $n_3 \neq 1$ ดังนั้น $n_2 = 3$ และ $n_3 = 4$ ให้ H_1, H_2, H_3 และ H_4 เป็นกลุ่มย่อย 3-ซีโลว์ที่แตกต่างกันทั้งหมดของ G จะได้ว่า $H_i \cap H_j = \{e\}$ สำหรับทุกๆ $1 \leq i \neq j \leq 4$ ดังนั้นกลุ่มย่อย 3-ซีโลว์ ทั้ง 4 กลุ่มย่อยจะมีสมาชิกที่แตกต่างกันทั้งสิ้น 9 ตัว ให้ K_1, K_2 และ K_3 เป็นกลุ่มย่อย 2-ซีโลว์ ที่แตกต่างกันทั้งหมดของ G แล้ว $|K_i| = 4$ สำหรับทุกๆ $i \in \{1, 2, 3\}$ และ $K_i \cap K_j = \{e\}$สำหรับทุกๆ $1 \leq i \neq j \leq 3$ ดังนั้นกลุ่มย่อย 2-ซีโลว์ทั้ง 3 กลุ่มย่อยจะมีสมาชิกที่แตกต่างกันทั้งสิ้น 3 ตัว และเนื่องจาก $H_i \cap K_j = \{e\}$ สำหรับทุกๆ $i \in \{1, 2, 3\}$ และ $j \in \{1, 2, 3, 4\}$ ทำให้ได้ว่าจำนวนสมาชิกที่แตกต่างกันทั้งหมดในกลุ่มย่อย 2-ซีโลว์ และกลุ่มย่อย 3-ซีโลว์ ทุกกลุ่มของ G เท่ากับ 12 ซึ่งเท่ากับ |G| ทำให้ G ไม่สามารถมีกลุ่มย่อย 2-ซีโลว์ หรือกลุ่มย่อย 3-ซีโลว์ที่แตกต่างกันได้ เพราะฉะนั้น $n_2 = 1$ หรือ $n_3 = 1$ และโดยบทแทรก 4.1.5 สรุปได้ว่า G ไม่เป็นกลุ่มเชิงเดียว ❐

4.2.5 ตัวอย่าง จงแสดงว่ากลุ่มอันดับ 18 ไม่เป็นกลุ่มเชิงเดียว

การพิสูจน์ ให้ G เป็นกลุ่ม ซึ่ง $|G| = 18 = 2\cdot 3^2$ แล้ว G จะมีกลุ่มย่อย 2-ซีโลว์อันดับ 2 และมีกลุ่มย่อย 3-ซีโลว์อันดับ 9 และจะได้โดยทฤษฎีบทที่สามของซีโลว์ว่า

$n_2 \equiv 1(\text{mod } 2)$ และ $n_2 \mid 18$ ซึ่งทำให้ได้ $n_2 \in \{1, 3\}$

$n_3 \equiv 1(\text{mod } 3)$ และ $n_3 \mid 18$ ซึ่งทำให้ได้ $n_3 = 1$

ถ้า $n_2 = 1$ หรือ $n_3 = 1$ แล้ว โดยบทแทรก 4.1.5 จะได้ว่า G ไม่เป็นกลุ่มเชิงเดียว

ในกรณีที่ $n_2 = 3$ และ $n_3 = 1$ ใช้วิธีคิดเดียวกันกับตัวอย่าง 4.2.4 ทำให้สรุปได้ว่า G ไม่เป็นกลุ่มเชิงเดียว ❐

4.2.6 ตัวอย่าง จงแสดงว่ากลุ่มที่มีอันดับ 30 ไม่เป็นกลุ่มเชิงเดียว

การพิสูจน์ ให้ G เป็นกลุ่ม ซึ่ง $|G| = 30 = 2\cdot 3\cdot 5$ โดยทฤษฎีบทที่หนึ่งของซีโลว์ จะได้ว่า G มีกลุ่มย่อย 3-ซีโลว์ และกลุ่มย่อย 5-ซีโลว์ ให้ H เป็นกลุ่มย่อย 3-ซีโลว์ และ K เป็นกลุ่มย่อย 5-ซีโลว์ของ G โดยทฤษฎีบทที่สามของซีโลว์ จะได้ว่า

$n_2 \equiv 1(\text{mod } 2)$ และ $n_2 \mid 30$ ซึ่งจะได้ว่า $n_2 \in \{1, 3, 5, 15\}$

$n_3 \equiv 1(\text{mod } 3)$ และ $n_3 \mid 30$ ซึ่งจะได้ว่า $n_3 \in \{1, 10\}$

$n_5 \equiv 1(\text{mod } 5)$ และ $n_5 \mid 30$ ซึ่งจะได้ว่า $n_5 \in \{1, 6\}$

ถ้า $n_2 = 1$ หรือ $n_3 = 1$ หรือ $n_5 = 1$ แล้วจะได้โดยบทแทรก 4.1.5 ว่า G ไม่เป็นกลุ่มเชิงเดียว

สมมติว่า $n_p \neq 1$ สำหรับทุกๆ $p \in \{2, 3, 5\}$ แล้ว $n_3 = 10$ และ $n_5 = 6$ ให้ $H_1, H_2, \dots, H_6$ เป็นกลุ่มย่อย 5-ซีโลว์ ที่แตกต่างกันทั้งหมดของ G แล้ว $H_i \cap H_j = \{e\}$ สำหรับทุกๆ $1 \leq i \neq j \leq 6$ ดังนั้นแต่ละ H_i ซึ่ง $i \in \{1, 2, \dots, 6\}$ จะมีสมาชิกที่มีอันดับ 5 จำนวน 4 ตัว ทำให้ G มีสมาชิกที่มีอันดับ 5 จำนวนทั้งสิ้น 24 ตัว และในทำนองเดียวกัน เนื่องจาก $n_3 = 10$ จะได้ว่า G มีสมาชิกที่มีอันดับ 3 จำนวนทั้งสิ้น 20 ตัว แล้ว G มีสมาชิกอย่างน้อย 44 ตัว ซึ่งเป็นไปไม่ได้เพราะจำนวนสมาชิกดังกล่าวมากกว่า $|G| = 30$ ดังนั้นจะมี $p \in \{2, 3, 5\}$ ซึ่ง $n_p = 1$ จึงทำให้ได้ว่ากลุ่มย่อย p-ซีโลว์นั้นเป็นกลุ่มย่อยปรกติของ G ดังนั้น G ไม่เป็นกลุ่มเชิงเดียว ❐

จากตัวอย่าง 4.2.4 – 4.2.6 เราพบว่ากลุ่มอันดับ 12, 18 และ 30 ล้วนแต่ไม่เป็นกลุ่มเชิงเดียว จึงทำให้เกิดแนวคิดเป็นข้อคาดการณ์ว่า “กลุ่มที่มีอันดับเป็น 6 เท่าของจำนวนเฉพาะจะไม่เป็นกลุ่มเชิงเดียว” เราจะพิสูจน์ข้อคาดการณ์นี้ในทฤษฎีบทต่อไป

4.2.7 ทฤษฎีบท กลุ่มอันดับ 6p ไม่เป็นกลุ่มเชิงเดียว สำหรับทุกๆ จำนวนเฉพาะ p

การพิสูจน์ ให้ G เป็นกลุ่ม ซึ่ง |G| = 6p เมื่อ p เป็นจำนวนเฉพาะ แล้วในกรณีที่ $p \in \{2, 3, 5\}$ ทฤษฎีบทเป็นจริงดังแสดงในตัวอย่าง 4.2.4 – 4.2.6 เราจึงพิจารณากรณี $p \geq 7$

เนื่องจาก $|G| = 6p = 2 \cdot 3 \cdot p$ ดังนั้น G จะมีกลุ่มย่อย 3-ซีโลว์อันดับ 3 และมีกลุ่มย่อย p-ซีโลว์อันดับ p ให้ H เป็นกลุ่มย่อย 3-ซีโลว์ และ K เป็นกลุ่มย่อย p-ซีโลว์ของ G แล้ว |H| = 3 และ |K| = p ดังนั้น (|H|, |K|) = (3, p) = 1 และโดยทฤษฎีบท 2.3.16 จะได้ว่า $H \cap K = \{e\}$ ซึ่งแสดงว่า $| H \cap K | = 1$ ทำให้ได้โดยทฤษฎีบทที่สามของซีโลว์ว่า $n_p \equiv 1 \pmod{p}$ และ $n_p \mid 6p$

สมมติว่า $n_p \neq 1$ แล้วจะมีจำนวนเต็มบวก t ซึ่ง $n_p = tp + 1$ เนื่องจาก $(tp + 1) \mid 6p$ แล้วจะมีจำนวนเต็มบวก s ซึ่ง $6p = s(tp + 1)$ และเนื่องจาก $p \mid 6p$ ทำให้ได้ $p \mid s(tp + 1)$ แต่ $p \nmid (tp + 1)$ ทำให้ได้ว่า p|s แล้วจะมีจำนวนเต็มบวก k ซึ่ง $s = pk$ ดังนั้น $6p = pk(tp + 1)$ ทำให้ได้ว่า $6 = k(tp + 1) \geq tp + 1 \geq p + 1 > p \geq 7$ เกิดข้อขัดแย้ง ดังนั้น $n_p = 1$ ทำให้ได้ว่า K เป็นกลุ่มย่อย p-ซีโลว์เพียงหนึ่งเดียวของ G ดังนั้น K เป็นกลุ่มย่อยปรกติของ G โดยบทแทรก 4.1.5 และสรุปได้ว่า HK เป็นกลุ่มย่อยปรกติของ G โดยทฤษฎีบท 2.5.13 และเราได้จากทฤษฎีบท 2.5.16 ว่า $| HK | = \frac{| H || K |}{| H \cap K |} = 3p$ เพราะฉะนั้น HK เป็นกลุ่มย่อยปรกติอันดับ 3p ของ G เราจึงสรุปได้ว่ากลุ่มอันดับ 6p สำหรับ $p \geq 7$ ไม่เป็นกลุ่มเชิงเดียว ❐

บทที่ 5
การจำแนกกลุ่มจำกัดอันดับ 1 – 15
Classification of Groups of Orders 1 – 15

การศึกษาที่ผ่านมาเราได้ศึกษาทฤษฎีบทของโคชี และประยุกต์มโนคติของแอคชันของกลุ่มบนเซตและนอร์มัลไลเซอร์ในการพิสูจน์ทฤษฎีบทซีโลว์ และประยุกต์ทฤษฎีบทซีโลว์ในการพิสูจน์ว่ากลุ่มที่มีอันดับเป็น 6 เท่าของจำนวนเฉพาะไม่เป็นกลุ่มเชิงเดียว ในบทนี้เราจะประยุกต์ทฤษฎีบทของโคชีและทฤษฎีบทซีโลว์ในอีกด้านหนึ่ง กล่าวคือการวิเคราะห์เพื่อจำแนกกลุ่มจำกัดอันดับ 1 – 15 ว่าแต่ละอันดับจะมีจำนวนกี่กลุ่มที่แตกต่างกันเมื่อไม่นับการถอดแบบกัน

5.1 ตัวอย่าง ถ้า G เป็นกลุ่ม ซึ่ง $|G| = 1$ แล้ว $G \cong \{e\}$ ดังนั้นกลุ่มอันดับ 1 มีจำนวนทั้งสิ้น 1 กลุ่ม ❐

5.2 ตัวอย่าง *การจำแนกกลุ่มอันดับ 2, 3, 5, 7, 11, 13 (กลุ่มอันดับจำนวนเฉพาะ)*

โดยทฤษฎีบท 2.3.26 และ 2.3.27 จะได้ว่า $G \cong \mathbb{Z}_p$ สำหรับแต่ละจำนวนเฉพาะ p ดังนั้นกลุ่มอันดับ 2, 3, 5, 7, 11, 13 มีจำนวนทั้งสิ้น 1 กลุ่ม ❐

5.3 ตัวอย่าง *การจำแนกกลุ่มที่มีอันดับ 4 และอันดับ 9*

โดยทฤษฎีบท 2.3.30 จะได้ว่าถ้า G เป็นกลุ่มอันดับ p^2 เมื่อ p เป็นจำนวนเฉพาะ แล้ว $G \cong \mathbb{Z}_{p^2}$ หรือ $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ ดังนั้นกลุ่มอันดับ 4 และอันดับ 9 มีจำนวนทั้งสิ้น 2 กลุ่ม ❐

5.4 ตัวอย่าง *การจำแนกกลุ่มที่มีอันดับ 6, 10, 14*

โดยทฤษฎีบท 2.3.31 จะได้ว่า $G \cong \mathbb{Z}_{2p}$ หรือ $G \cong D_p$ สำหรับทุกแต่ละจำนวนเฉพาะ p และวิธีการจำแนกกลุ่มอันดับ 6 ได้แสดงไว้ในตัวอย่าง 3.3.6 ซึ่งเราสามารถจำแนกกลุ่มที่มีอันดับ 10 และ 14 ได้ด้วยวิธีการเดียวกัน ดังนั้นกลุ่มอันดับ 6, 10, 14 มีจำนวนทั้งสิ้น 2 กลุ่ม ❐

5.5 ตัวอย่าง *การจำแนกกลุ่มที่มีอันดับ 8*

ให้ G เป็นกลุ่ม ซึ่ง |G| = 8 แล้วโดยทฤษฎีบทของลากรองจ์ แต่ละสมาชิกใน G จะมีอันดับ 1, 2, 4 หรือ 8 (ตัวหารของ 8)

ถ้า G มีสมาชิกที่มีอันดับ 8 แล้ว $G \cong \mathbb{Z}_8$

ถ้า G ไม่มีสมาชิกที่มีอันดับ 8 แล้วทุกๆ สมาชิกใน G ที่ไม่ใช่เอกลักษณ์จะต้องมีอันดับ 2 หรือ 4

กรณีที่ 1 : ทุกสมาชิกใน G ที่ไม่ใช่เอกลักษณ์มีอันดับ 2

ให้ a, b และ c เป็นสมาชิกที่แตกต่างกัน 3 ตัวของ G แล้ว o(a) = o(b) = o(c) = 2 ทำให้ e, a, b, c, ab, ac, bc และ abc เป็นสมาชิกที่แตกต่างกันทั้งหมด 8 ตัว ดังนั้น G = {e, a, b, c, ab, ac, bc, abc} เราจะแสดงว่า $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

ให้ $f : G \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ กำหนดสำหรับทุกๆ $x \in G$ ดังตาราง 5.1

x	**f(x)**
e	$(\bar{0}, \bar{0}, \bar{0})$
a	$(\bar{0}, \bar{0}, \bar{1})$
b	$(\bar{0}, \bar{1}, \bar{0})$
c	$(\bar{1}, \bar{0}, \bar{0})$
ab	$(\bar{0}, \bar{1}, \bar{1})$
ac	$(\bar{1}, \bar{0}, \bar{1})$
bc	$(\bar{1}, \bar{1}, \bar{0})$
abc	$(\bar{1}, \bar{1}, \bar{1})$

ตาราง 5.1 : ตารางการนิยามฟังก์ชัน $f : G \to \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

แล้วโดยวิธีการพิสูจน์ทำนองเดียวกันกับตัวอย่าง 3.3.6 เราจะได้ว่า f เป็นฟังก์ชันถอดแบบ ดังนั้น $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

กรณีที่ 2 : มีสมาชิกใน G ที่มีอันดับ 4

ให้ $a \in G$ ซึ่ง o(a) = 4 และให้ $H = \langle a \rangle = \{e, a, a^2, a^3\}$

กรณีย่อยที่ 2.1 : มี $b \in G \setminus H$ ซึ่ง o(b) = 2

จะได้โคเซต $Hb = \{b, ab, a^2b, a^3b\}$ ดังนั้น $G = H \cup Hb = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$

ถ้า $ba = a^2b$ แล้ว $b^2a = ba^2b = (ba)(ab) = (a^2b)(ab) = a^2(ba)b = a^2(a^2b)b = a^4b^2$ แต่ $o(b) = 2$ ดังนั้น $a = a^4$ นั่นคือ $a^3 = e$ ซึ่งเกิดข้อขัดแย้ง ดังนั้น $ba \neq a^2b$ ทำให้ได้ว่า $ba = ab$ หรือ $ba = a^3b$

กรณี $ba = ab$ จะได้ว่า G เป็นกลุ่มอาบีเลียน เนื่องจาก $(\bar{3}, \bar{0})$ และ $(\bar{0}, \bar{1})$ เป็นสมาชิกของ $\mathbb{Z}_4 \times \mathbb{Z}_2$ ซึ่ง $o(\bar{3}, \bar{0}) = 4$ และ $o(\bar{0}, \bar{1}) = 2$ เรากำหนดให้ $f : G \to \mathbb{Z}_4 \times \mathbb{Z}_2$ กำหนดสำหรับทุกๆ $x \in G$ ดังตาราง 5.2

x	f(x)
e	$(\bar{0}, \bar{0})$
a	$(\bar{3}, \bar{0})$
a^2	$(\bar{2}, \bar{0})$
a^3	$(\bar{1}, \bar{0})$
b	$(\bar{0}, \bar{1})$
ab	$(\bar{3}, \bar{1})$
a^2b	$(\bar{2}, \bar{1})$
a^3b	$(\bar{1}, \bar{1})$

ตาราง 5.2 : ตารางการนิยามฟังก์ชัน $f : G \to \mathbb{Z}_4 \times \mathbb{Z}_2$

แล้วโดยวิธีการพิสูจน์ทำนองเดียวกันกับตัวอย่าง 3.3.6 เราจะได้ว่า f เป็นฟังก์ชันถอดแบบ ดังนั้น $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$

กรณี $ba = a^3b$ เนื่องจาก (1 2 3 4) และ (1 3) เป็นสมาชิกของ D_4 ซึ่ง $o((1\ 2\ 3\ 4)) = 4$ และ $o((1\ 3)) = 2$ เรากำหนดให้ $g : G \to D_4$ กำหนดสำหรับทุกๆ $x \in G$ ดังตาราง 5.3

x	g(x)
e	(1)
a	(1 2 3 4)
a^2	(1 3)(2 4)
a^3	(1 4 3 2)
b	(1 3)
ab	(1 4)(2 3)
a^2b	(2 4)
a^3b	(1 2)(3 4)

ตาราง 5.3 : ตารางการนิยามฟังก์ชัน $g : G \to D_4$

แล้วโดยวิธีการพิสูจน์ทำนองเดียวกันกับตัวอย่าง 3.3.6 เราจะได้ว่า g เป็นฟังก์ชันถอดแบบ ดังนั้น $G \cong D_4$

กรณีย่อยที่ 2.2 : ทุกสมาชิกของ G \ H มีอันดับ 4

ให้ $b \in G \setminus H$ แล้ว $b^4 = e$ ทำให้ได้ $b^2b^2 = (b^2)^2 = e$ แล้ว $o(b^2) = 2$ แต่มี a^2 เพียงตัวเดียวที่มีอันดับ 2 ใน H ดังนั้น $b^2 = a^2$

ถ้า $ba = ab$ แล้ว $(a^3b)^2 = (a^3b)(a^3b) = a^6b^2 = a^2b^2 = a^2a^2 = a^4 = e$ ดังนั้น $o(a^3b) = 2$ เกิดข้อขัดแย้งกับสมมติฐานของกรณีนี้

ถ้า $ba = a^2b$ แล้ว $b^4a = b^3a^2b = bb^2a^2b = ba^2a^2b = ba^4b = beb = b^2 = a^2$ ซึ่งจะได้ $b^4 = a$ แต่ $b^4 = e$ ดังนั้น $a = e$ เกิดข้อขัดแย้ง

เพราะฉะนั้น $ba = a^3b$ และ $a^4 = b^4 = e$ และ $a^2 = b^2$ ซึ่งภายใต้เงื่อนไขนี้เราสามารถสร้างตารางการคูณบน G ได้ดังตาราง 5.4

	e	**a**	**a^2**	**a^3**	**b**	**ab**	**a^2b**	**a^3b**
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

ตาราง 5.4 : ตารางการคูณบน G เมื่อ $ba = a^3b$ และ $a^4 = b^4 = e$ และ $a^2 = b^2$

ซึ่งแสดงว่า G เป็นกลุ่มควอเทอร์เนียน Q

เมื่อพิจารณาครบทุกกรณีแล้วเราสรุปได้ว่ามีกลุ่มอันดับ 8 ที่แตกต่างกัน (ไม่นับการถอดแบบ) ทั้งหมด 5 กลุ่ม ได้แก่ $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, D_4 และ Q ❐

5.6 ตัวอย่าง *การจำแนกกลุ่มที่มีอันดับ 12*

ให้ G เป็นกลุ่ม ซึ่ง $|G| = 12 = 2^2 \cdot 3$ แล้ว G มีกลุ่มย่อย 2-ซีโลว์ อันดับ 2^2 และมีกลุ่มย่อย 3-ซีโลว์ อันดับ 3 อย่างละอย่างน้อย 1 กลุ่มย่อย

ให้ n_2 และ n_3 แทนจำนวนกลุ่มย่อย 2-ซีโลว์ และกลุ่มย่อย 3-ซีโลว์ ของ G ตามลำดับ แล้วโดยทฤษฎีบทที่สามของซีโลว์จะได้ว่า $n_2 \equiv 1 (\mathrm{mod}\ 2)$ โดยที่ $n_2 \mid 12$ และ $n_3 \equiv 1 (\mathrm{mod}\ 3)$ โดยที่ $n_3 \mid 12$ ทำให้ได้ ($n_2 = 1$ หรือ $n_2 = 3$) และ ($n_3 = 1$ หรือ $n_3 = 4$) เนื่องจากกลุ่มย่อย 2-ซีโลว์ มีอันดับ 4 ดังนั้นกลุ่มย่อยเหล่านี้จะถอดแบบกับ $\mathbb{Z}_4$ หรือ K_4 และกลุ่มย่อย 3-ซีโลว์อันดับ 3 จะถอดแบบกับ $\mathbb{Z}_3$ เราจึงแยกการพิจารณาออกเป็น 4 กรณีดังนี้

กรณีที่ 1 : $n_2 = 1$ และ $n_3 = 1$

ให้ H เป็นกลุ่มย่อย 2-ซีโลว์ และ K เป็นกลุ่มย่อย 3-ซีโลว์ของ G แล้วโดยทฤษฎีบท 2.3.16 จะได้ว่า $H \cap K = \{e\}$ เนื่องจาก $n_2 = 1$ และ $n_3 = 1$ ดังนั้น H และ K ต่างเป็นกลุ่มย่อยปรกติของ G ทำให้ได้โดยทฤษฎีบท 2.5.14′ ว่า $G \cong H \times K$ เพราะฉะนั้น $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ หรือ $G \cong K_4 \times \mathbb{Z}_3$

ถ้า G เป็นกลุ่มอาบีเลียนแล้วทุกกลุ่มย่อยของ G เป็นกลุ่มย่อยปรกติ เราจะได้กรณี 1 ดังนั้นเราจึงจะพิจารณาเฉพาะกรณีที่ G เป็นกลุ่มนอนอาบีเลียน

ให้ H เป็นกลุ่มย่อย 2-ซีโลว์ และ K เป็นกลุ่มย่อย 3-ซีโลว์ของ G แล้ว $H \cap K = \{e\}$ ทำให้ได้ $|HK| = \frac{|H||K|}{|H \cap K|} = |H||K| = |G|$ ดังนั้น $G = HK$ สมมติว่า $hk = kh$ สำหรับทุกๆ $h \in H$ และ $k \in K$ แล้ว G เป็นกลุ่มอาบีเลียน (เพราะถ้า $g_1, g_2 \in G$ แล้วจะมี $h_1, h_2 \in H$ และ $k_1, k_2 \in K$ ซึ่ง $g_1 = h_1k_1$ และ $g_2 = h_2k_2$ ทำให้ได้ $g_1g_2 = h_1k_1h_2k_2 = h_2k_2h_1k_1 = g_2g_1$) เกิดข้อขัดแย้ง ดังนั้นถ้า H เป็นกลุ่มย่อย 2-ซีโลว์ และ K เป็นกลุ่มย่อย 3-ซีโลว์ของ G แล้วข้อความ “$hk = kh$ สำหรับทุกๆ $h \in H$ และ $k \in K$” ไม่เป็นจริง

กรณีที่ 2 : $n_2 = 1$ และ $n_3 = 4$

ให้ H เป็นกลุ่มย่อย 2-ซีโลว์ ของ G แล้ว $H \cong \mathbb{Z}_4$ หรือ $H \cong K_4$ และให้ K เป็นกลุ่มย่อย 3-ซีโลว์ ของ G เราแยกการพิจารณาออกเป็น 2 กรณีย่อยดังนี้

กรณีย่อยที่ 2.1 : $H \cong \mathbb{Z}_4$

ให้ $H = \langle a \rangle = \{e, a, a^2, a^3\}$ โดยที่ $a^4 = e$ และให้ $K = \langle b \rangle = \{e, b, b^2\}$ โดยที่ $b^3 = e$ เนื่องจาก H เป็นกลุ่มย่อยปรกติของ G เพียงหนึ่งเดียว ดังนั้น $b^{-1}ab \in H$ ถ้า $b^{-1}ab = a$ แล้ว $ab = ba$ แล้ว G เป็นกลุ่มอาบีเลียน เกิดข้อขัดแย้ง และเพราะ $o(a) = 4$ ดังนั้น $b^{-1}ab \neq a^2$ และ $b^{-1}ab \neq e$ ทำให้ $b^{-1}ab = a^3$ นั่นคือ $ab = ba^3$

เพราะว่า $(ba)^2 = b(ab)a = b(ba^3)a = b^2a^4 = b^2e = b^2$ ดังนั้น $(ba)^3 = (ba)^2ba = b^2ba = b^3a = ea = a$ และ $(ba)^4 = (ba)^2(ba)^2 = b^2b^2 = b^4 = b$ แสดงว่า $a, b \in \langle ba \rangle$ และได้ว่า $G = \langle ba \rangle$ นั่นคือ G เป็นกลุ่มวัฏจักร เกิดข้อขัดแย้ง เพราะฉะนั้นไม่มีกลุ่มอันดับ 12 ที่เป็นกลุ่มนอนอาบีเลียน ซึ่ง $n_2 = 1$ และ $n_3 = 4$ และ $H \cong \mathbb{Z}_4$

กรณีย่อยที่ 2.2 : $H \cong K_4$

ให้ $H = \{e, x, y, z\}$ เป็นกลุ่มที่มีสมาชิก 4 ตัวของไคลน์ และให้ $K = \{e, c, c^2\} \cong \mathbb{Z}_3$ แล้ว H เป็นกลุ่มย่อยปรกติเพียงหนึ่งเดียวของ G ทำให้ $c^{-1}hc \in H$ สำหรับทุกๆ $h \in H$ แต่จากข้อสมมติข้างต้นจะมี $h \in H$ ซึ่ง $c^{-1}hc \neq h$ โดยไม่เสียนัยทั่วไปให้ $c^{-1}xc \neq x$ และ $c^{-1}xc = y$

ต่อไปให้ $x = a$, $y = b$ และ $z = ab$ แล้ว $c^{-1}xc = y$ ทำให้ได้ว่า $x = cyc^{-1}$ นั่นคือ $a = cbc^{-1}$ เราจะแสดงว่า $c^{-1}bc \neq a$ โดยสมมติว่า $c^{-1}bc = a$ แล้ว $c^{-1}bc = cbc^{-1}$ หรือ $b = c^2bc^{-2}$ แต่ $c^2 = c^{-1}$ และ $c^{-2} = c$ ทำให้ได้ว่า $b = c^{-1}bc = a$ เกิดข้อขัดแย้ง เพราะฉะนั้น $c^{-1}bc \neq a$ และในทำนองเดียวกันเราสามารถแสดงได้ว่า $c^{-1}bc \neq b$ และ $c^{-1}bc \neq e$ แล้ว $c^{-1}bc = ab$ และ $c^{-1}(ab)c = (c^{-1}ac)(c^{-1}bc) = bab = b^2a = a$ เพราะฉะนั้น สมการต่อไปนี้เป็นจริงใน G

$$ac = cb,\ bc = cab,\ abc = ca,\ a^2 = b^2 = e,\ c^3 = e,\ ab = ba \qquad \ldots (*)$$

เนื่องจาก e, c และ c^2 กำหนดโคเซตของ H ใน G ที่แตกต่างกัน ดังนั้นสมาชิกทั้งหมดของ G ประกอบด้วย

$$e,\ c,\ c^2,\ a,\ b,\ ab,\ ca,\ cb,\ cab,\ c^2a,\ c^2b,\ c^2ab$$

จากสมการ (*) เราสามารถเขียนตารางการคูณสำหรับ G ได้ดังตาราง 5.5

	e	**c**	**c^2**	**a**	**b**	**ab**	**ca**	**cb**	**cab**	**c^2a**	**c^2b**	**c^2ab**
e	e	c	c^2	a	b	ab	ca	cb	cab	c^2a	c^2b	c^2ab
c	c	c^2	e	ca	cb	cab	c^2a	c^2b	c^2ab	a	b	ab
c^2	c^2	e	c	c^2a	c^2b	c^2ab	a	b	ab	ca	cb	cab
a	a	cb	c^2ab	e	ab	b	cab	c	ca	c^2b	c^2a	c^2
b	b	cab	c^2a	ab	e	a	cb	ca	c	c^2	c^2ab	c^2b
ab	ab	ca	c^2b	b	a	e	c	cab	cb	c^2ab	c^2	c^2a
ca	ca	c^2b	ab	c	cab	cb	c^2ab	c^2	c^2a	b	a	e
cb	cb	c^2ab	a	cab	c	ca	c^2b	c^2a	c^2	e	ab	b
cab	cab	c^2a	b	cb	ca	c	c^2	c^2ab	c^2b	ab	e	a
c^2a	c^2a	b	cab	c^2	c^2ab	c^2b	ab	e	a	cb	ca	c
c^2b	c^2b	ab	ca	c^2ab	c^2	c^2a	b	a	e	c	cab	cb
c^2ab	c^2ab	a	cb	c^2b	c^2a	c^2	e	ab	b	cab	c	ca

ตาราง 5.5 : ตารางการคูณสำหรับ G

เนื่องจาก A_4 เป็นกลุ่มนอนอาบีเลียนอันดับ 12 แล้ว A_4 จะถอดแบบกับกลุ่มซึ่งแสดงในตาราง 5.5 หรือตาราง 5.6 หรือถอดแบบกับ $D_3 \times \mathbb{Z}_2$ (ดูในการพิสูจน์กรณีที่ 3) จากตัวอย่าง 4.2.1 เราพบว่า A_4 มีสมาชิก 3 ตัวที่มีอันดับ 3 คือ σ_2, σ_5 และ σ_8 แต่จากตาราง 5.6 จะพบว่ามีสมาชิก a^2 เพียงตัวเดียวเท่านั้นที่มีอันดับ 2 ดังนั้น G ไม่ถอดแบบกับ A_4 และเนื่องจาก A_4 ไม่มี

กลุ่มย่อยอันดับ 6 และ D_3 ถอดแบบกับกลุ่มย่อยของ $D_3 \times \mathbb{Z}_2$ (โดยทฤษฎีบท 2.5.9) เพราะฉะนั้น A_4 จึงไม่ถอดแบบกับ $D_3 \times \mathbb{Z}_2$ ทำให้สรุปได้ว่า A_4 ต้องถอดแบบกับกลุ่มซึ่งแสดงในตาราง 5.5

กรณีที่ 3 : $n_2 = 3$ และ $n_3 = 1$

ให้ H เป็นกลุ่มย่อย 2-ซีโลว์ ของ G และ K เป็นกลุ่มย่อย 3-ซีโลว์ ของ G

กรณีย่อยที่ 3.1 : $H \cong \mathbb{Z}_4$

ให้ $H = \langle a \rangle = \{e, a, a^2, a^3\}$ โดยที่ $a^4 = e$ และให้ $K = \langle b \rangle = \{e, b, b^2\}$ โดยที่ $b^3 = e$ เนื่องจาก K เป็นกลุ่มย่อยปรกติเพียงหนึ่งเดียวของ G ดังนั้น $a^{-1}ba \in K$ แล้วจะมี c ซึ่ง $a^{-1}ca \neq b$ (มิฉะนั้นจะทำให้ G เป็นกลุ่มอาบีเลียนซึ่งขัดแย้งกับข้อสมมติข้างต้น) โดยการพิสูจน์ทำนองเดียวกันกับกรณีที่ 2 จะได้ว่า $a^{-1}ba = b^2$ และ $ba = ab^2$ และเช่นเดียวกันจะได้ว่า $b^2a = bab^2 = ab^4 = ab$ ทำให้เราได้สมการสำหรับกำหนดตารางการคูณสำหรับ G ดังนี้

$$ba = ab^2,\ b^2a = ab,\ a^4 = e,\ b^3 = e \qquad \ldots (**)$$

ทำให้สมาชิกทั้งหมดของ G ได้แก่ $e,\ a,\ a^2,\ a^3,\ b,\ b^2,\ ab,\ a^2b,\ a^3b,\ ab^2,\ a^2b^2,\ a^3b^2$

จากสมการ (**) เราสามารถเขียนตารางการคูณสำหรับ G ได้ดังตาราง 5.6

	e	**a**	**a^2**	**a^3**	**b**	**b^2**	**ab**	**a^2b**	**a^3b**	**ab^2**	**a^2b^2**	**a^3b^2**
e	e	a	a^2	a^3	b	b^2	ab	a^2b	a^3b	ab^2	a^2b^2	a^3b^2
a	a	a^2	a^3	e	ac	ab^2	a^2b	a^3b	b	a^2b^2	a^3b^2	c^2
a^2	a^2	a^3	e	a	a^2b	a^2b^2	a^3b	b	ab	a^3b^2	b^2	ab^2
a^3	a^3	e	a	a^2	a^3b	a^3b^2	b	ab	a^2b	b^2	ab^2	a^2b^2
b	b	ab^2	a^2b	a^3b^2	b^2	e	a	a^2b^2	a^3	ab	a^2	a^3b
b^2	b^2	ab	a^2b^2	a^3b	e	b	ab^2	a^2	a^3b^2	a	a^2b	a^3
ab	ab	a^3b^2	a^3b	b^2	ab^2	a	a^2	a^3b^2	e	a^2b	a^3	b
a^2b	a^2b	a^3b^2	b	ab^2	a^2b^2	a^2	a^3	b^2	a	a^3b	e	ab
a^3b	a^3b	b^2	ab	a^2b^2	a^3b^2	a^3	e	ab^2	a^2	b	a	a^2b
ab^2	ab^2	a^2b	a^3b^2	b	a	ab	a^2b^2	a^3	b^2	a^2	a^3b	e
a^2b^2	a^2b^2	a^3b	b^2	ab	a^2	a^2b	a^3b^2	e	ab^2	a^3	b	a
a^3b^2	a^3b^2	b	ab^2	a^2b	a^3	a^3b	b^2	a	a^2b^2	e	ab	a^2

ตาราง 5.6 : ตารางการคูณสำหรับ G

กลุ่มที่ถอดแบบกับ G ที่มีการคูณสมนัยกับตาราง 5.6 ได้แสดงไว้ในตัวอย่าง 5.7

กรณีย่อยที่ 3.2 : $H \cong K_4$

ให้ $H = \{e, x, y, z\}$ เป็นกลุ่มที่มีสมาชิก 4 ตัวของไคลน์ และให้ $K = \{e, c, c^2\}$ โดยที่ $c^3 = e$ เนื่องจาก K เป็นกลุ่มย่อยปรกติเพียงหนึ่งเดียวของ G ดังนั้น $k^{-1}ck \in K$ สำหรับทุกๆ $k \in K$ แล้วจะมี $k \in K$ ซึ่ง $k^{-1}ck \neq c$ โดยไม่เสียนัยทั่วไป เราสมมติว่า $x^{-1}cx = c^2$

ให้ x = a, y = b และ z = ab แล้วโดยการพิสูจน์ทำนองเดียวกับกรณีย่อยที่ 2.2 จะได้ว่า $ca = ac^2$ และ $c^2a = c(ca) = c(ac^2) = (ca)c^2 = ac^2c^2 = ac$ นั่นคือ $c^2a = ac$

เราจะพิสูจน์ว่า $S = \{e, c, c^2, a, ca, c^2a\}$ เป็นกลุ่มย่อยของ G ซึ่ง $|S| = 6$

S มีสมบัติปิด เพราะเอกลักษณ์ $ca = ac^2$ และ $c^2a = ac$ แล้ว $e \in S$ และอินเวอร์สของแต่ละสมาชิกใน S เป็นสมาชิกของ S และจากเอกลักษณ์ $c^{-1} = c^2$, $(c^2)^{-1} = c$, $a^{-1} = a$, $(ca)^{-1} = ca$ และ $(c^2a)^{-1} = c^2a$ ถ้า $ca = c^2a$ แล้ว $c = e$ เกิดข้อขัดแย้ง ดังนั้น $ca \neq c^2a$ และเพราะ $ac = c^2a \neq ca$ ดังนั้น S เป็นกลุ่มนอนอาบีเลียน ทำให้ S ถอดแบบกับ D_3 และเนื่องจาก $[\, G : S \,] = \frac{|G|}{|S|} = 2$ ดังนั้น S เป็นกลุ่มย่อยปรกติของ G ทำให้ได้ $b^{-1}cb \in S$ แต่ $o(b^{-1}cb) = 3$ จึงได้ว่า $b^{-1}cb = c$ หรือ $b^{-1}cb = c^2$ และเพราะสมาชิกตัวอื่นๆ ของ S ที่ไม่ใช่ e มีอันดับ 2 เราจะเลือกสมาชิก $h \in H \setminus S$ ซึ่ง $h^{-1}ch = c$ ถ้า $b^{-1}cb = c$ เราเลือก $h = b$ เช่นเดียวกัน ถ้า $b^{-1}cb = c^2$ เราเลือก $h = ab$ เนื่องจาก $a^{-1}ca = c^2$ จะได้ $(ab)^{-1}c(ab) = b^{-1}(a^{-1}ca)b = b^{-1}c^2b = (b^{-1}cb)(b^{-1}cb) = c^2c^2 = c$ เพราะฉะนั้นมีสมาชิก $h \notin S$ (ซึ่งก็คือ b หรือ ab) ที่ทำให้ $h^{-1}ch = c$

ต่อไปให้ $T = \langle h \rangle$ แล้ว $S \cap T = \{e\}$ และจากการตรวจสอบพบว่า $st = ts$ สำหรับทุกๆ $s \in S$ และ $t \in T$ และยิ่งไปกว่านั้น $|S|\,|T| = |G|$ โดยทฤษฎีบท 2.5.14′ สรุปได้ว่า $G \cong S \times T$ แต่เนื่องจาก $S \cong D_3$ และ $T \cong \mathbb{Z}_2$ เราจึงสรุปได้ว่ากลุ่ม G อันดับ 12 ที่มี $n_2 = 3$ และ $n_3 = 1$ และมีกลุ่มย่อย 2-ซีโลว์ ที่ถอดแบบกับ K_4 จะถอดแบบกับ $D_3 \times \mathbb{Z}_2$

สุดท้ายเราจะพิสูจน์ว่า $D_6 \cong D_3 \times \mathbb{Z}_2$

เนื่องจาก D_6 เป็นกลุ่มนอนอาบีเลียนอันดับ 12 ดังนั้นโดยทฤษฎีบทที่หนึ่งของซีโลว์ D_6 จะมีกลุ่มย่อยอันดับ 6 แสดงว่า D_6 ไม่ถอดแบบกับ A_4 และไม่ถอดแบบกับกลุ่มที่แสดงในตาราง 5.5 และเพราะ D_6 มีสมาชิกจำนวน 6 ตัว ที่มีอันดับ 2 ดังนั้น D_6 จึงไม่ถอดแบบกับกลุ่มที่แสดงในตาราง 5.6 เพราะกลุ่มดังกล่าวมีสมาชิกที่มีอันดับ 2 เพียงตัวเดียว เพราะฉะนั้นจึงเหลือกรณีที่เป็นไปได้เพียงกรณีเดียวคือ $D_6 \cong D_3 \times \mathbb{Z}_2$

กรณีที่ 4 : $n_2 = 3$ และ $n_3 = 4$

เนื่องจากกลุ่มวัฏจักรอันดับ 3 ที่แตกต่างกันจะมีสมาชิกร่วมกันเพียงตัวเดียวคือ e ดังนั้นยูเนียนของกลุ่มย่อย 3-ซีโลว์ ทั้ง 4 กลุ่มย่อย จะประกอบด้วยสมาชิกที่แตกต่างกัน 9 ตัว และเพราะ $|G| = 12 = 2^2 \cdot 3$ ดังนั้นกลุ่มย่อย 2-ซีโลว์ ของ G มีอันดับ 4 โดยที่อินเตอร์เซกชันของกลุ่มที่มีอันดับ 4 กับกลุ่มที่มีอันดับ 3 ประกอบด้วย e เพียงหนึ่งเดียว ทำให้ได้ว่าจำนวนสมาชิกที่แตกต่างกันทั้งหมดในกลุ่มย่อย 3-ซีโลว์ทั้ง 4 กลุ่มย่อย และกลุ่มย่อย 2-ซีโลว์ เท่ากับ 12 แต่ $|G| = 12$ ทำ

ให้ไม่สามารถมีกลุ่มย่อย 2-ซีโลว์ ที่แตกต่างกันได้ นั่นคือ $n_2 = 1$ เกิดข้อขัดแย้ง ดังนั้นจึงไม่มีกลุ่มอันดับ 12 ที่สอดคล้องกับเงื่อนไขของกรณีนี้

จากทั้ง 4 กรณี เราสามารถสรุปได้ว่ามีกลุ่มอันดับ 12 ที่ไม่ถอดแบบกันทั้งสิ้น 5 กลุ่ม ดังนี้

ถ้า $n_2 = 1$ และ $n_3 = 1$ แล้ว $G \cong \mathbb{Z}_{12}$ หรือ $G \cong K_4 \times \mathbb{Z}_3$

ถ้า $n_2 = 1$ และ $n_3 = 4$ แล้ว $G \cong A_4$

ถ้า $n_2 = 3$ และ $n_3 = 1$ แล้ว G ถอดแบบกับกลุ่มที่ของเมทริกซ์ขนาด 2×2 เหนือจำนวนเชิงซ้อน ซึ่งแสดงในตัวอย่าง 5.7

ถ้า $n_2 = 1$ และ $n_3 = 1$ แล้ว $G \cong D_3 \times \mathbb{Z}_2 \cong D_6$ ❐

5.7 ตัวอย่าง ให้ $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ และ $B = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^2 \end{pmatrix}$ โดยที่ $i^2 = -1$ และ ε เป็นรากที่สามของ 1 ที่ไม่ใช่ 1 นั่นคือ $\varepsilon^3 = 1$ และ $\varepsilon \neq 1$ ทำให้ได้ $\det(A) \neq 0$ และ $\det(B) \neq 0$ ดังนั้น $A,B \in \mathcal{M}$ โดยที่ $\mathcal{M}$ คือกลุ่มของเมทริกซ์ขนาด 2×2 เหนือจำนวนเชิงซ้อน เราจะแสดงว่า <A, B> เป็นกลุ่มอันดับ 12 ซึ่งถอดแบบกับตาราง 5.6

เริ่มต้นเราคำนวณผลคูณของเมทริกซ์ต่อไปนี้

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \qquad B^2 = \begin{pmatrix} \varepsilon^2 & 0 \\ 0 & \varepsilon \end{pmatrix} \qquad A^2B = \begin{pmatrix} -\varepsilon & 0 \\ 0 & -\varepsilon^2 \end{pmatrix} \qquad A^2B^2 = \begin{pmatrix} -\varepsilon^2 & 0 \\ 0 & -\varepsilon \end{pmatrix}$$

$$A^3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \qquad B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad A^3B = \begin{pmatrix} 0 & -i\varepsilon^2 \\ -i\varepsilon & 0 \end{pmatrix} \qquad A^2B^2 = \begin{pmatrix} 0 & -i\varepsilon \\ -i\varepsilon^2 & 0 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad AB = \begin{pmatrix} 0 & i\varepsilon^2 \\ i\varepsilon & 0 \end{pmatrix} \qquad AB^2 = \begin{pmatrix} 0 & i\varepsilon \\ i\varepsilon^2 & 0 \end{pmatrix}$$

ให้ $H = \{A, A^2, A^3, A^4, B, B^2, AB, A^2B, A^3B, AB^2, A^2B^2, A^3B^2\}$ เราจะแสดงว่า $H = \langle A, B \rangle$ ซึ่งเห็นได้ชัดว่า $H \subseteq \langle A, B \rangle$ ในการแสดงว่า $H = \langle A, B \rangle$ เราจะพิสูจน์ว่า H เป็นกลุ่มที่มี A และ B เป็นสมาชิก

เริ่มต้นสังเกตว่า $A^{-1}BA = B^2$ และ $(A^2B)(A^3B) = A^2A\cdot(A^{-1}BA)A^2B = A^3B^2A^2B = A^4(A^{-1}BA)(A^{-1}BA)AB = B^2B^2AB = BAB = AA^{-1}BAB = AB^2B = A$ แล้วโดยการตรวจสอบทุกคู่สมาชิกใน H จะได้ว่า H มีสมบัติปิดภายใต้การคูณเมทริกซ์

เนื่องจาก H เป็นสับเซตของเซตของเมทริกซ์ซึ่งมิใช่เอกฐาน (nonsingular matrices) ขนาด 2×2 ทั้งหมด ดังนั้นการคูณเมทริกซ์บน H จึงสอดคล้องกับสมบัติการเปลี่ยนกลุ่ม

ต่อไปเราจะแสดงว่าแต่ละสมาชิกของ H มีอินเวอร์สการคูณ ตัวอย่างเช่น อินเวอร์สการคูณของ A^3B กำหนดดังนี้

$(A^3B)^{-1} = B^2A = AA^{-1}B^2A = A(A^{-1}BA)(A^{-1}BA) = AB^2B^2 = AB \in H$

และจากการตรวจสอบทุกสมาชิกใน H จะได้ว่าสมาชิกของ H ทุกตัวมีอินเวอร์สการคูณ

ดังนั้น H เป็นกลุ่มอันดับ 12 ซึ่ง H = <A, B> และสอดคล้องเงื่อนไข $BA = AB^2$, $B^2A = AB$, $B^3 = I$ และ $A^4 = I$ เมื่อ I เป็นเมทริกซ์เอกลักษณ์ เราจึงนิยามการส่ง α โดย $\alpha(a) = A$ และ $\alpha(c) = B$ แล้ว α จะเป็นฟังก์ชันถอดแบบของกลุ่ม (พิจารณาตาราง 5.6 กับตารางการคูณของ H) ❐

5.8 ตัวอย่าง *การจำแนกกลุ่มที่มีอันดับ 15*

ให้ G เป็นกลุ่ม ซึ่ง $|G| = 15 = 3 \cdot 5$ แล้วโดยทฤษฎีบท 2.3.31 จะได้ว่า G เป็นกลุ่มวัฏจักร ดังนั้น $G \cong \mathbb{Z}_{15}$ ทำให้ได้ว่ากลุ่มอันดับ 15 มีจำนวนทั้งสิ้น 1 กลุ่มเมื่อไม่นับการถอดแบบกัน ❐

จากตัวอย่างที่แสดงทั้งหมดข้างต้น เราสามารถสรุปจำนวนกลุ่มอันดับ 1 – 15 ที่แตกต่างกันทั้งหมด โดยไม่นับการถอดแบบกันได้ดังตาราง 5.7 ต่อไปนี้

อันดับ	จำนวนกลุ่มที่แตกต่างกัน
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5
9	2
10	2
11	1
12	5
13	1
14	2
15	1

ตาราง 5.7 : ตารางแสดงการจำแนกจำนวนกลุ่มจำกัดอันดับ 1 – 15

บรรณานุกรม

อมรา เศวตะทัต. พีชคณิตนามธรรม. พิมพ์ครั้งที่ 2. ปัตตานี : ม.ป.ท., 2540.

Baumslag B. and Chandler B. SCHAUM'S OUTLINE OF THEORY AND PROBLEMS OF GROUP THEORY. New York : McGraw Hill, 1968.

Fraleigh, J.B. A First Course in Abstract Algebra. Fifth Edition. New York : Addison -Wesley, 1993.

Gallian, J.A. Contemporary Abstract Algebra. Boston : PWS Publishing, 1986.

Judson, T.W. Abstract Algebra : Theory and Applications. Boston : PWS Publishing, 1993.

Pinter, C.C. A Book of Abstract Algebra. New York : McGraw Hill, 1990.

Rotman, J.J. THE THEORY OF GROUPS : An Introduction. Second Edition. Boston : Allyn and Bacon, Inc., 1976.

ประวัติผู้วิจัย

ชื่อ-สกุล	นายอัมรินทร์ อภิรักษ์มาศ
ที่อยู่	80/71 หมู่ 2 ซอยเพชรเกษม 48 หมู่บ้านจันทร์ประดิษฐ์ เขตภาษีเจริญ กรุงเทพมหานคร 10160
ที่ทำงาน	โรงเรียนสอนคณิตศาสตร์ MATH HOUSE สาขาบางแค ชั้น 2 อาคารศูนย์การค้าเดอะมอลล์บางแค แขวงบางแคเหนือ เขตบางแค กรุงเทพมหานคร 10160 โรงเรียนสอนคณิตศาสตร์ MATH HOUSE สาขาเพชรเกษม (สำนักงานใหญ่) ซอยเพชรเกษม 84 แขวงบางแคเหนือ เขตบางแค กรุงเทพมหานคร 10160
ประวัติการศึกษา	
พ.ศ. 2545	สำเร็จการศึกษาระดับปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาคณิตศาสตร์ จากมหาวิทยาลัยหอการค้าไทย กรุงเทพมหานคร
พ.ศ. 2546	ศึกษาต่อระดับปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร วิทยาเขตพระราชวังสนามจันทร์ จังหวัดนครปฐม
ประวัติการทำงาน	
พ.ศ. 2549 - ปัจจุบัน	ครูประจำการวิชาคณิตศาสตร์ ระดับชั้นมัธยมศึกษาตอนปลาย โรงเรียนสอนคณิตศาสตร์ MATH HOUSE สาขาบางแค และสาขาเพชรเกษม (สำนักงานใหญ่)