กรุปซึ่งทุกกรุปย่อยเป็นกรุปย่อยปกติ

โดย
นางสาวพัชยา สบบง

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ
ภาควิชาคณิตศาสตร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2552

กรุปซึ่งทุกกรุปย่อยเป็นกรุปย่อยปกติ

โดย
นางสาวพัชยา สบบง

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ
ภาควิชาคณิตศาสตร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2552

GROUPS WHOSE ALL SUBGROUPS ARE NORMAL

By

Patchaya Sobbong

An Independent Study Submitted in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

Department of Mathematics

Graduate School

SILPAKORN UNIVERSITY

2009

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร อนุมัติให้การค้นคว้าอิสระเรื่อง " กรุปซึ่งทุกกรุปย่อยเป็นกรุปย่อยปกติ " เสนอโดย นางสาวพัชยา สบบง เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ

.....

(รองศาสตราจารย์ ดร.ศิริชัย ชินะตังกูร)

คณบดีบัณฑิตวิทยาลัย

วันที่.....เดือน..... พ.ศ.....

อาจารย์ที่ปรึกษาการค้นคว้าอิสระ

ศาสตราจารย์ ดร.ฉวีวรรณ รัตนประเสริฐ

คณะกรรมการตรวจสอบการค้นคว้าอิสระ

..... ประธานกรรมการ

(อาจารย์ ดร.สมเจตน์ ชัยยะ)

...../...../.....

..... กรรมการ

(อาจารย์ ดร.จิตติ รักบุตร)

...../...../.....

..... กรรมการ

(ศาสตราจารย์ ดร.ฉวีวรรณ รัตนประเสริฐ)

...../...../.....

49308303 : สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ
คำสำคัญ : กรุปย่อยปกติ / กรุปย่อยคอมมิวเตเตอร์ / ทฤษฎีบทของโคชี / ทฤษฎีบทซีโลว์ /
ผลคูณตรง / กรุปอาบีเลียนขนาดจำกัด / กรุปฮามิลทอเนียน
พัชยา สบบง : กรุปซึ่งทุกกรุปย่อยเป็นกรุปย่อยปกติ. อาจารย์ที่ปรึกษาการค้นคว้าอิสระ: ศ.ดร. ฉวีวรรณ รัตนประเสริฐ. 59 หน้า.

ในการค้นคว้าอิสระนี้เราศึกษากรุปซึ่งทุกกรุปย่อยเป็นกรุปย่อยปกติ โดยแบ่งการศึกษาออกเป็นสองส่วน คือ กรุปอาบีเลียนขนาดจำกัดและกรุปฮามิลทอเนียน ในกรณีของกรุปอาบีเลียนขนาดจำกัด เราประยุกต์ทฤษฎีบทของซีโลว์ช่วยในการพิสูจน์ว่ากรุปอาบีเลียนอันดับจำกัด เขียนได้ในรูปผลคูณตรงของกรุปวัฏจักรขนาดจำกัด และกรณีของกรุปฮามิลทอเนียนเราแสดงว่ากรุปฮามิลทอเนียนสามารถเขียนในรูปผลคูณตรงของกรุปย่อยควอเทอร์เนียนกับกรุปย่อยอาบีเลียนซึ่งทุกสมาชิก มีอันดับเป็นจำนวนเต็มคี่ และกรุปย่อยอาบีเลียนที่ทุกสมาชิกมีอันดับสอง

ภาควิชาคณิตศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ปีการศึกษา 2552
ลายมือชื่อนักศึกษา.....
ลายมือชื่ออาจารย์ที่ปรึกษาการค้นคว้าอิสระ.....

49308303 : MAJOR : MATHEMATICS AND INFORMATION TECHNOLOGY
KEY WORDS : NORMAL SUBGROUPS / CAUCHY'S THEOREM / SYLOW THEOREMS /
DIRECT PRODUCT / FINITE ABELIAN GROUPS / HAMILTONIAN GROUPS
PATCHAYA SOBBONG : GROUPS WHOSE ALL SUBGROUPS ARE NORMAL.
INDEPENDENT STUDY ADVISOR : PROF.CHAWEWAN RATANAPRASERT, Ph.D.. 59 pp.

In the independent study, we study groups whose all subgroups are normal. We investigate on finite abelian groups and Hamiltonian groups. For finite abelian groups, we apply the Sylow theorems to prove that all finite abelian groups are the finite direct product of cyclic groups. For Hamiltonian groups, we show that all Hamiltonian groups can be written as the direct product of a Quaternion group, a finite abelian group of odd order and an elementary abelian group.

Department of Mathematics Graduate School, Silpakorn University Academic Year 2009
Student's signature…….
Independent Study Advisor's signature…….

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยดี เพราะความกรุณาและความเมตตาจาก ศาสตราจารย์ ดร.ฉวีวรรณ รัตนประเสริฐ ที่ได้ให้คำปรึกษา คำแนะนำ ทำให้โลกทัศน์ทางวิชาการของข้าพเจ้ากว้างขึ้น ช่วยเติมเต็มและแก้ไขส่วนที่บกพร่อง จนทำให้การค้นคว้าอิสระฉบับนี้สำเร็จด้วยดี

ขอกราบขอบพระคุณ คณาจารย์ของภาควิชาคณิตศาสตร์ ภาควิชาสถิติ และภาควิชาคอมพิวเตอร์ มหาวิทยาลัยศิลปากรทุกท่าน ที่ได้ประสิทธิ์ประสาทวิชา พร้อมทั้งหยิบยื่นโอกาสทางการศึกษา จนทำให้ข้าพเจ้าได้พบความสำเร็จ สามารถนำความรู้ที่ได้ไปใช้ให้ก่อประโยชน์ได้อย่างถูกต้อง

ขอขอบคุณเพื่อนๆ สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ สำหรับความช่วยเหลือและมิตรภาพอันดีงามระหว่างการศึกษา

สุดท้ายขอขอบคุณ ครอบครัวของข้าพเจ้าที่ได้ให้กำลังใจ มอบความรัก ดูแลและให้การสนับสนุนทางการศึกษา จนทำให้ข้าพเจ้าประสบผลสำเร็จได้ในวันนี้

สารบัญ

บทที่ 1

บทนำ

ในการค้นคว้าอิสระนี้ เราศึกษาเรื่องราวของกรุปซึ่งทุกกรุปย่อยเป็นกรุปย่อยปกติ และเขียนกรุปเหล่านั้นให้อยู่ในรูปผลคูณตรงของกรุปย่อยบางกรุป โดยเราใช้ทฤษฎีบทเกี่ยวกับผลคูณตรงของกรุปวัฏจักรมาช่วยในการพิสูจน์ เราแบ่งกรุปที่ศึกษาออกเป็นสองชนิดคือกรุปอาบีเลียนและกรุปนอนอาบีเลียน ในกรณีของกรุปอาบีเลียนเราศึกษาโครงสร้างของกรุปอาบีเลียนขนาดจำกัด และพิสูจน์ทฤษฎีบทหลักมูลของกรุปอาบีเลียนขนาดจำกัด และในกรณีของกรุปนอนอาบีเลียนเราศึกษาสมบัติของกรุปฮามิลทอเนียน

ในบทที่ 2 กล่าวถึงความรู้พื้นฐานซึ่งประกอบด้วยบทนิยามและทฤษฎีบทเบื้องต้นเกี่ยวกับกรุป ได้แก่ การนิยามกรุป กรุปอาบีเลียน กรุปนอนอาบีเลียน กรุปย่อยปกติ อันดับของกรุป และทฤษฎีบทที่สำคัญต่างๆ ของกรุป พอสังเขปโดยละการพิสูจน์ไว้

ในบทที่ 3 กล่าวถึงบทนิยามและทฤษฎีบทของนอร์มัลไลเซอร์ ศูนย์กลางของกรุป ทฤษฎีบทเกี่ยวกับศูนย์กลางของกรุป บทนิยามและทฤษฎีบทเกี่ยวกับกรุปย่อยคอมมิวเตเตอร์

ในบทที่ 4 เราสร้างกรุปใหม่จากกรุปเดิมที่มีสมาชิกจำนวนจำกัด แล้วเรียกกรุปนั้นว่าผลคูณตรง ศึกษาความสัมพันธ์ระหว่างผลคูณภายนอกและผลคูณภายใน ศึกษาทฤษฎีบทของโคชีและใช้เป็นเครื่องมือในการพิสูจน์ทฤษฎีบทของซีโลว์ แล้วใช้ทฤษฎีบทเหล่านี้ศึกษาโครงสร้างของกรุปอาบีเลียนที่มีขนาดจำกัด ผลที่ได้จากการศึกษาโครงสร้างนี้สรุปได้เป็นทฤษฎีบทหลักมูลของกรุปอาบีเลียนขนาดจำกัดคือ ทุกกรุปอาบีเลียนขนาดจำกัดเป็นผลคูณตรงของกรุปวัฏจักรที่มีอันดับเป็นกำลังของจำนวนเฉพาะ

ในบทที่ 5 เราได้แสดงว่านอกจากกรุปอาบีเลียนที่มีกรุปย่อยทุกกรุปเป็นกรุปย่อยปกติ และสามารถเขียนกรุปอาบีเลียนให้อยู่ในรูปผลคูณตรงได้แล้ว ยังมีกรุปนอนอาบีเลียนที่มีกรุปย่อยทุกกรุปเป็นกรุปย่อยปกติซึ่งเรียกว่ากรุปฮามิลทอเนียน เราพิสูจน์ว่ากรุปฮามิลทอเนียนคือผลคูณตรงของกรุปย่อยควอเทอร์เนียน กับกรุปย่อยอาบีเลียนซึ่งทุกสมาชิกมีอันดับเป็นจำนวนคี่ และกรุปย่อยอาบีเลียนที่มีทุกสมาชิกมีอันดับสอง

บทที่ 2

ความรู้พื้นฐาน

2.1 สมบัติเบื้องต้นของกรุป

คำว่า “กรุป” กำหนดขึ้นเป็นครั้งแรกโดย กาลัวส์ (Galois) ราวปี ค.ศ.1830 ซึ่งเขาได้อธิบายเกี่ยวกับเซตของฟังก์ชันหนึ่งต่อหนึ่งบนเซตจำกัด ต่อมาในปี ค.ศ.1852 ได้มีนักคณิตศาสตร์สองท่านคือ Heinrich Weber และ Walter von Dyck ให้ความหมายของกรุปในเชิงนามธรรม ในหัวข้อนี้จะกล่าวถึงบทนิยามของกรุป และทฤษฎีกรุปที่สำคัญโดยจะขอละการพิสูจน์ไว้

2.1.1 บทนิยาม กรุป (group) คือโครงสร้าง $(G,\circ)$ ที่ประกอบด้วยเซต $G \neq \varnothing$ กับการดำเนินการทวิภาค $\circ$ ซึ่งสอดคล้องสมบัติ ดังนี้

1. การดำเนินการ $\circ$ สอดคล้องสมบัติการเปลี่ยนหมู่ (association)
2. มีสมาชิก $e \in G$ ซึ่ง $e \circ a = a = a \circ e$ สำหรับทุกสมาชิก $a \in G$ เรียก e ว่าสมาชิกเอกลักษณ์ (identity) ของ G ภายใต้ $\circ$
3. แต่ละสมาชิก $a \in G$ มี $b \in G$ ซึ่ง $a \circ b = e = b \circ a$ เรียก b ว่าตัวผกผัน (inverse) ของ a ภายใต้ $\circ$ และจะแทนตัวผกผันของ a ด้วยสัญลักษณ์ a^{-1}

ต่อไปในกรณีที่จะไม่ทำให้เกิดการสับสนเราอาจจะการเขียนกรุป $(G, \circ)$ เพียง G และอาจเขียน ab แทน $a \circ b$

2.1.2 บทนิยาม กรุป G เป็น **กรุปอาบีเลียน** (abelian group) ถ้าการดำเนินการ $\circ$ สอดคล้องสมบัติสลับที่ (commutative) นั่นคือ $ab = ba$ สำหรับทุกสมาชิก $a, b \in G$

ถ้ามีสมาชิก a และ b ใน G ซึ่ง $ab \neq ba$ จะเรียก G ว่า**กรุปนอนอาบีเลียน** (non-abelian group)

2.1.3 ทฤษฎีบท กำหนดให้ G เป็นกรุป แล้ว

1. $\left(a^{-1}\right)^{-1} = a$ สำหรับทุกสมาชิก $a \in G$

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

2.1.4 บทนิยาม ให้ G เป็นกรุป และสำหรับแต่ละจำนวนเต็มบวก n เราจะใช้สัญลักษณ์ $\prod_{i=1}^{n} a_i$ แทนผลคูณ $a_1 a_2 \ldots a_n$ ของสมาชิก $a_1, a_2, \ldots, a_n$ ใน G และกำหนดผลคูณในรูปอุปนัยดังนี้

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

จากบทนิยาม 2.1.4 จะได้ว่า $\prod_{i=1}^{1} a_i = a_1$, $\prod_{i=1}^{2} a_i = a_1 a_2$, $\prod_{i=1}^{3} a_i = (a_1 a_2) a_3$, $\prod_{i=1}^{4} a_i = ((a_1 a_2) a_3) a_4, \ldots$ เป็นต้น

เนื่องจากการดำเนินการของ G สอดคล้องกฎการเปลี่ยนหมู่ ซึ่งแสดงว่าสัญลักษณ์ $(a_1 a_2) a_3$ และ $a_1 (a_2 a_3)$ แทนสมาชิกตัวเดียวกันในกรุปนั้น ทำให้เราอาจละวงเล็บในการเขียนผลคูณของ 3 สมาชิก แล้วการเขียนผลคูณ $\prod_{i=1}^{n} a_i$ เมื่อ $n \geq 3$ อาจจะละวงเล็บได้เช่นเดียวกับกรณี $n = 3$ หรือไม่ เราจะแสดงความจริงนี้ในชื่อว่า “การวางนัยทั่วไปของกฎการเปลี่ยนหมู่”

2.1.5 ทฤษฎีบทการวางนัยทั่วไปของกฎการเปลี่ยนหมู่

ให้ G เป็นกรุป ถ้า $a_1, a_2, \ldots, a_n$ เป็นสมาชิก n ตัวใน G สำหรับจำนวนเต็มบวก n แล้วการเปลี่ยนหมู่ในอันดับ $a_1, a_2, \ldots, a_n$ จะเป็นเช่นใดก็ตาม ผลคูณของสมาชิก n ตัวจะเท่ากันและเท่ากับ $\prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n$

โดยหลักอุปนัยเชิงคณิตศาสตร์และทฤษฎีบทการวางนัยทั่วไปของกฎการเปลี่ยนหมู่ เราสามารถขยายทฤษฎีบท 2.1.3 ข้อ 2 สำหรับทุกจำนวนเต็มบวก n ได้ดังนี้

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

2.1.7 บทนิยาม ให้ G เป็นกรุป จะเรียก**ขนาด** (cardinality) ของเซต G ว่า**อันดับ** (order) ของกรุป และเขียนแทนด้วย $|G|$

ถ้าอันดับของกรุป G เป็นจำนวนจำกัดแล้วอันดับของ G เท่ากับจำนวนสมาชิกของ G จะเรียก G ว่า**กรุปจำกัด** (finite group) แต่ถ้า G ไม่เป็นกรุปจำกัด จะเรียก G ว่า**กรุปอนันต์** (infinite group)

2.1.8 **บทนิยาม** ให้ G เป็นกรุปที่มี e เป็นเอกลักษณ์ และ $a \in G$ จะใช้สัญลักษณ์ a^0 แทน e และสำหรับจำนวนเต็มบวก n จะแทน aa^{n-1} ด้วย a^n และอ่านว่า กำลัง n ของ a หรือ a ยกกำลัง n และจะใช้สัญลักษณ์ a^{-n} แทนตัวผกผันของ a^n

2.1.9 **ทฤษฎีบท** กำหนด $a \in G$ และ m และ n เป็นจำนวนเต็ม แล้ว

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

2.1.10 **ทฤษฎีบท** ถ้า G เป็นกรุปจำกัดและ $a \in G$ แล้วจะมีจำนวนเต็มบวก k ซึ่ง $a^k = e$

2.1.11 **บทนิยาม** ให้ A เป็นเซตที่ไม่ใช่เซตว่าง เรากล่าวว่า σ เป็น**การเรียงสับเปลี่ยน** (permutation) บน A ถ้า σ เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก A ไป A

2.1.12 **ทฤษฎีบท** สำหรับแต่ละจำนวนเต็มบวก n ให้ $A = \{1, 2, 3, ..., n\}$ และให้ S_n แทนเซตของวิธีเรียงสับเปลี่ยนทั้งหมดบน A และให้ o แทน**การประกอบ** (composition) ระหว่างฟังก์ชันแล้ว $(S_n; o)$ เป็นกรุป และเราเรียก $(S_n; o)$ ว่า**กรุปสมมาตร** (symmetric group) ขนาด n

ให้ n เป็นจำนวนเต็มบวก และ $A = \{1, 2, 3, ..., n\}$ เรานิยมเขียนสมาชิกของ S_n ในรูปของเมทริกซ์ขนาด $2 \times n$ กล่าวคือ ให้แถวแรกแทนสมาชิกใน A ทั้งหมด และในแถวที่สองตำแหน่งที่ 2i เมื่อ $1 \le i \le n$ แทนค่า $\sigma(i)$ ของการเรียงสับเปลี่ยน นั่นคือถ้า $\sigma \in S_n$ เราเขียนแทน σ ด้วยเมทริกซ์ได้ดังนี้

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

การเรียนสับเปลี่ยนเอกลักษณ์ (identity permutation) ใน S_n เขียนได้ในรูปของเมทริกซ์ได้ดังนี้

$$\begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$$

และนิยมเขียนแทนด้วยสัญลักษณ์สั้นๆ เป็น (1)

2.2 กรุปย่อย

ในหัวข้อนี้เราจะกล่าวถึงเซตย่อยของกรุปที่มีสมบัติแบบเดียวกับกรุป ซึ่งเราจะเรียกกรุปนั้นว่ากรุปย่อย โดยมีการให้บทนิยามและกล่าวถึงทฤษฎีบทที่จำเป็นที่จะนำไปใช้ช่วยในการพิสูจน์ทฤษฎีบทในบทต่อไป

2.2.1 **บทนิยาม** ให้ G เป็นกรุป และ $\varnothing \neq H \subseteq G$ จะเรียก H ว่า**กรุปย่อย** (subgroup) ของ G ถ้า H เป็นกรุปภายใต้การดำเนินการทวิภาคของ G ซึ่งกำกัดลงบน H เขียนแทนด้วยสัญลักษณ์ $H \leq G$ และถ้า $H \neq \{e\}$ และ $H \neq G$ เราจะเรียก H ว่า**กรุปย่อยแท้** (proper subgroup) ของ G เขียนแทนด้วยสัญลักษณ์ $H < G$

2.2.2 **ทฤษฎีบท** กำหนด G เป็นกรุปและ $\varnothing \neq H \subseteq G$ แล้ว H เป็นกรุปย่อยของ G ก็ต่อเมื่อ $x^{-1} \in H$ และ $xy \in H$ สำหรับทุกๆ $x, y \in H$

2.2.3 **ทฤษฎีบท** กำหนด G เป็นกรุปและ $\varnothing \neq H \subseteq G$ แล้ว H เป็นกรุปย่อยของ G ก็ต่อเมื่อ $xy^{-1} \in H$ สำหรับทุกๆ $x, y \in H$

2.3 กรุปวัฏจักร

ในหัวข้อนี้เราจะกล่าวถึงบทนิยามและทฤษฎีบทเกี่ยวกับกรุปย่อยวัฏจักร เรากล่าวว่า G เป็นกรุปวัฏจักร เมื่อแต่ละสมาชิกของ G เขียนได้ในรูปกำลังต่างๆ ของ $a \in G$ ซึ่งเป็นตัวก่อกำเนิดของ G และเรายังได้ว่ากรุปวัฏจักรเป็นกรุปอาบีเลียนดังบทนิยามและทฤษฎีบทต่อไปนี้

2.3.1 **บทนิยาม** ให้ G เป็นกรุปและ $a \in G$ ถ้ามี n เป็นจำนวนเต็มบวกตัวน้อยสุดซึ่ง $a^n = e$ เรากล่าวว่า n เป็น**อันดับ** (order) ของ a และจะแทนอันดับของ a ด้วยสัญลักษณ์ $o(a) = n$ และในกรณีที่ไม่มีจำนวนเต็มบวก n ใด ๆ ที่ทำให้ $a^n = e$ เราจะกล่าวว่า a มี**อันดับอนันต์** (infinite order)

2.3.2 **ทฤษฎีบท** ให้ G เป็นกรุป และ $a \in G$ ให้ m และ n เป็นจำนวนเต็มบวก ถ้า $o(a) = n$ แล้ว $a^m = e$ ก็ต่อเมื่อ $n|m$

2.3.3 **ทฤษฎีบท** ให้ G เป็นกรุบและ $a \in G$ แล้ว $\{ a^n \mid n$ เป็นจำนวนเต็ม $\}$ เป็นกรุปย่อยของ G

2.3.4 **บทนิยาม** ให้ G เป็นกรุปและ $a \in G$ จะเขียนแทนกรุปย่อย $\{ a^n \mid n$ เป็นจำนวนเต็ม $\}$ ด้วยสัญลักษณ์ $\langle a \rangle$ และเรียกว่า**กรุปย่อยวัฏจักรของ G ที่ก่อกำเนิดโดย** a (cyclic subgroup of G generated by a)

2.3.5 **บทแทรก** ให้ G เป็นกรุปวัฏจักรจำกัดที่มีอันดับ n ถ้า a เป็นตัวก่อกำเนิดของ G แล้ว $e = a^0, a^1, a^2, \ldots, a^{n-1}$ เป็นสมาชิกที่ต่างกันทั้งหมดของ G และ $\langle a \rangle = \{ a^0, a^1, a^2, ..., a^{n-1} \}$

2.3.6 **ทฤษฎีบท** ให้ G เป็นกรุปและ $a \in G$ แล้ว $o(a) = |\langle a \rangle|$

2.3.7 **ทฤษฎีบท** ให้ G เป็นกรุปและ $\varnothing \neq A \subseteq G$ กำหนด $\langle A \rangle = \cap H$ เมื่อ $H \in \{ K \leq G \mid A \subseteq K \}$ แล้ว $\langle A \rangle$ เป็นกรุปย่อยของ G ที่ก่อกำเนิดโดย A และได้ว่า $\langle A \rangle$ เป็นกรุปย่อยเล็กสุด ของ G ที่มี A เป็นเซตย่อย

ในกรณีเฉพาะถ้า $A = \{a_1, a_2, \ldots, a_n\}$ แล้วเราจะเขียน $\langle A \rangle$ ด้วย $\langle a_1, a_2, \ldots, a_n \rangle$

2.3.8 **ทฤษฎีบท** ให้ G เป็นกรุปและ $\varnothing \neq A \subseteq G$ แล้ว $\langle A \rangle = \{ a_1{}^{\alpha_1} a_2{}^{\alpha_2} \ldots a_n{}^{\alpha_n} \mid a_i \in A, a_i \neq a_{i+1}, \alpha_i$ เป็นจำนวนเต็ม สำหรับ $1 \leq i \leq n$ และ n เป็นจำนวนเต็มบวก $\}$

2.3.9 **บทแทรก** ให้ G เป็นกรุปและ $a_1, a_2, \ldots, a_n \in G$ แล้ว $\langle a_1, a_2, \ldots, a_n \rangle = \{ b_1^{\alpha_1} b_2^{\alpha_2} \ldots b_m^{\alpha_m} \mid b_i \in \{a_1, a_2, \ldots, a_n\}, b_i \neq b_{i+1}, \alpha_i$ เป็นจำนวนเต็ม สำหรับ $1 \leq i \leq m$ และ m เป็นจำนวนเต็มบวก $\}$

2.3.10 **บทแทรก** ให้ G เป็นกรุปอาบีเลียนและ $a_1, a_2, \ldots, a_n \in G$ แล้ว $\langle a_1, a_2, \ldots, a_n \rangle = \{ a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} \mid \alpha_i$ เป็นจำนวนเต็ม สำหรับ $1 \leq i \leq n \}$

2.3.11 **บทนิยาม** ให้ G เป็นกรุป เราจะเรียก G ว่า**กรุปวัฏจักร** (cyclic group) ถ้ามี $a \in G$ ซึ่ง $G = \langle a \rangle$ และเรียก a ว่า**ตัวก่อกำเนิด** (generator) ของ G

2.3.12 **ทฤษฎีบท** ถ้า G เป็นกรุปวัฏจักร แล้ว G เป็นกรุปอาบีเลียน

2.3.13 **ทฤษฎีบท** ถ้า G เป็นกรุปวัฏจักรและ $H \leq G$ แล้ว H เป็นกรุปวัฏจักร

2.3.14 **บทนิยาม** ให้ G เป็นกรุป $H \leq G$ และ $a \in G$ จะเรียกเซต

$$aH = \{ ah \mid h \in H \}$$ ว่า **โคเซตซ้าย** (left coset) ของ H ใน G

และจะเรียกเซต $Ha = \{ ha \mid h \in H \}$ ว่า **โคเซตขวา** (rigth coset) ของ H ใน G

จำนวนโคเซตซ้ายทั้งหมดของ H ใน G เท่ากับจำนวนโคเซตขวาทั้งหมดของ H ใน G และจะเรียกจำนวนเต็มนี้ว่า**ดรรชนี** (index) ของ H ใน G เขียนแทนด้วยสัญลักษณ์ $[G : H]$

2.3.15 **ทฤษฎีบทลากรองจ์** (Lagrange's Theorem)

ให้ m และ n เป็นจำนวนเต็มบวก ถ้า G เป็นกรุปที่มีขนาดเท่ากับ n และ $H \leq G$ ซึ่ง $|H| = m$ แล้ว $m \mid n$

2.3.16 **ทฤษฎีบท** ให้ G เป็นกรุปซึ่ง $|G| = p$ เมื่อ p เป็นจำนวนเฉพาะแล้ว G เป็นกรุปวัฏจักร

2.3.17 **ทฤษฎีบท** ให้ G เป็นกรุปและให้ H และ K เป็นกรุปย่อยอันดับจำกัดของ G ซึ่งต่างกัน ถ้า $(|H|, |K|) = 1$ หรือ $|H|$ และ $|K|$ เป็นจำนวนเฉพาะสัมพัทธ์ แล้ว $H \cap K = \{e\}$

2.3.18 **บทนิยาม** ให้ G เป็นกรุป และ $H, K \subseteq G$ ซึ่ง H และ K ไม่เป็นเซตว่าง กำหนด HK เป็นเซตนิยามโดย $HK = \{ab \mid a \in H, b \in K\}$

โดยทั่วไป $HK \neq KH$

2.3.19 **ทฤษฎีบท** ให้ H และ K เป็นกรุปย่อยของ G แล้ว HK เป็นกรุปย่อยของ G ก็ต่อเมื่อ $HK = KH$

2.3.20 **บทแทรก** ให้ G เป็นกรุป ถ้า H และ K เป็นกรุปย่อยอันดับจำกัดของ G ซึ่ง $H \cap K = \{e\}$ แล้ว $|HK| = |H||K|$

2.4 กรุปย่อยปกติและกรุปผลหาร

ในหัวข้อนี้เรากล่าวถึงกรุบย่อยที่มีโคเซตซ้ายเท่ากับโคเซตขวาซึ่งกรุบย่อยที่มีลักษณะเช่นนี้เราให้ชื่อว่ากรุปย่อยปกติ และกล่าวถึงกรุปผลหาร ซึ่งมีบทนิยามและทฤษฎีบทดังนี้

2.4.1 **บทนิยาม** ให้ G เป็นกรุป และ N เป็นกรุปย่อยของ G จะกล่าวว่า N เป็น**กรุปย่อยปกติ** (normal subgroup) ของ G ก็ต่อเมื่อ $aN = Na$ สำหรับทุกสมาชิก a ใน G

2.4.2 **บทนิยาม** ให้ G เป็นกรุป และ N เป็นกรุปย่อยของ G และ $a \in G$ เราเรียกเซตย่อยของ G ซึ่งนิยามดังนี้

$$aNa^{-1} = \{aha^{-1} \mid h \in N\}$$

ว่า **สังยุค** (conjugate) ของ N

2.4.3 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยของ G ข้อความต่อไปนี้สมมูลกัน

1. N เป็นกรุปย่อยปกติของ G
2. $aNa^{-1} \subseteq N$ สำหรับสมาชิกทุกๆ a ใน G
3. $aNa^{-1} = N$ สำหรับสมาชิกทุกๆ a ใน G

2.4.4 **ทฤษฎีบท** ให้ G เป็นกรุป และ N เป็นกรุปย่อยของ G ถ้า $[G : N] = 2$ แล้ว N เป็นกรุปย่อยปกติของ G

2.4.5 **ทฤษฎีบท** ถ้า G เป็นกรุปอาบีเลียนและ N เป็นกรุปย่อยของ G แล้ว N เป็นกรุปย่อยปกติของ G

2.4.6 **ทฤษฎีบท** ให้ G เป็นกรุป จะได้ว่า ถ้า N_1 และ N_2 เป็นกรุปย่อยปกติของ G แล้ว $N_1 \cap N_2$ เป็นกรุปย่อยปกติของ G

2.4.7 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยของ G แล้ว N เป็นกรุบย่อยปกติของ G ก็ต่อเมื่อ สำหรับสมาชิก a และ b ใน G จะได้ $(aN)(bN) = (ab)N$

ถ้ากำหนดสัญลักษณ์ G/N แทนเซตของโคเซตซ้ายทั้งหมดของ N ใน G นั่นคือ $G/N = \{aN \mid a \in G\}$ และกำหนดการดำเนินการระหว่างเซตนี้โดยการคูณดังทฤษฎีบท 2.4.7 แล้ว G/N เป็นกรุป และทำให้ได้ทฤษฎีบทต่อไปนี้

2.4.8 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยปกติของ G แล้ว G/N เป็นกรุปภายใต้การคูณระหว่างโคเซต ซึ่งนิยามดังนี้ $(aN)(bN) = (ab)N$ เมื่อ a และ b เป็นสมาชิกใน G

2.4.9 **บทนิยาม** เรียกกรุป G/N ว่า**กรุปผลหาร** (factor group) ของ N ใน G

2.4.10 **ทฤษฎีบท** ถ้า G เป็นกรุปอาบีเลียนและ N เป็นกรุปย่อยของ G แล้ว G/N เป็นกรุปอาบีเลียน

2.4.11 **ทฤษฎีบท** ถ้า G เป็นกรุปวัฏจักรและ N เป็นกรุปย่อยของ G แล้ว G/N เป็นกรุปย่อยวัฏจักรของ

2.4.12 **ทฤษฎีบท** ถ้า G เป็นกรุปจำกัด แล้ว $\left|G/H\right| = \frac{|G|}{|H|} = [G : H]$

2.5 สาทิสสัณฐานและสมสัณฐาน

ในหัวข้อนี้เราศึกษาความสัมพันธ์ระหว่างกรุปสองกรุป แต่เนื่องจากกรุปคือ เซตกับการ

ดำเนินการทวิภาค ดังนั้น การศึกษาความสัมพันธ์ระหว่างกรุปทั้งสองก็คือ การศึกษาฟังก์ชันจากกรุปหนึ่งไปยังอีกกรุปหนึ่ง โดยที่ฟังก์ชันนั้นรักษาสมบัติของการดำเนินการทวิภาคของกรุปทั้งสอง

2.5.1 **บทนิยาม** ให้ G และ H เป็นกรุป และให้ $f : G \to H$ เรากล่าวว่า f เป็น**สาทิสสัณฐาน** (homomorphism) จาก G ไปยัง H ถ้า $f(ab) = f(a)f(b)$ สำหรับทุก $a, b \in G$

2.5.2 **บทนิยาม** ให้ G และ H เป็นกรุป และให้ $f : G \to H$ เป็นสาทิสสัณฐาน ถ้า f เป็นเป็นฟังก์ชันหนึ่งต่อหนึ่งจาก G ไปทั่วถึง H เรากล่าวว่า f เป็น**สมสัณฐาน** (isomorphism) จาก G ไป H และเรียกว่า G **สมสัณฐานกัน** (isomorphic) กับ H ถ้ามีฟังก์ชันสมสัณฐานจาก G ไป H เขียนแทนด้วยสัญลักษณ์ $G \cong H$

2.5.3 **ทฤษฎีบท** ให้ f เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป H แล้ว

1. $f(e) = e'$ เมื่อ e และ e' เป็นสมาชิกเอกลักษณ์ใน G และ H ตามลำดับ
2. $f\left(g^{-1}\right) = \left(f(g)\right)^{-1}$ สำหรับทุก $g \in G$
3. $f(G) = \{f(g) \mid g \in G\} \leq H$

2.5.4 **ทฤษฎีบท** ให้ G, H และ K เป็นกรุป แล้ว

1. $G \cong G$
2. ถ้า $G \cong H$ แล้ว $H \cong G$
3. ถ้า $G \cong H$ และ $H \cong K$ แล้ว $G \cong H$

2.5.5 **ทฤษฎีบท** ถ้า G และ H เป็นกรุปวัฏจักรซึ่ง $|G| = |H|$ แล้ว $G \cong H$

2.5.6 **ทฤษฎีบท** ให้ f เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป H และ n เป็นจำนวนเต็มบวก แล้ว $f(g_1 g_2 \cdots g_n) = f(g_1)f(g_2)\cdots f(g_n)$ สำหรับ $g_1, g_2, ..., g_n \in G$

2.5.7 **บทนิยาม** ให้ f เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป H ถ้า S เป็นกรุปย่อยของ H นิยาม $f^{-1}(S) = \{x \in S \mid f(x) \in S\}$ และเรียกว่า**ภาพผกผันสาทิสสัณฐาน** (homomorphic inverse image) ของ S

2.5.8 **ทฤษฎีบท** ถ้า f เป็นสาทิสสัณฐานจากกรุป G ไปยังกรุป H และ K เป็นกรุปย่อยของ H แล้ว $f^{-1}(K)$ เป็นกรุปย่อยของ G

2.5.9 **บทนิยาม** ให้ G และ H เป็นกรุป และ e_H เป็นเอกลักษณ์ของ H และให้ $f : G \to H$ เป็นสาทิสสัณฐาน และให้

$$\ker f = \{x \in G \mid f(x) = e_H\}$$

เราเรียก $\ker f$ ว่า**แก่นกลาง** (kernel) ของ f

2.5.10 **ทฤษฎีบท** ให้ G และ H เป็นกรุป ถ้า $f : G \to H$ เป็นสาทิสสัณฐาน แล้ว $\ker f$ เป็นกรุปย่อยปกติของ G

2.5.11 **ทฤษฎีบท** ให้ N เป็นกรุปย่อยปกติของกรุป G แล้วจะมีฟังก์ชันสมนัยหนึ่งต่อหนึ่งระหว่างเซตของกรุปย่อย H ของ G ซึ่ง $N \subseteq H$ และเซตของกรุปย่อย K ของกรุปผลหาร G/N

2.5.12 **บทแทรก**

1. H เป็นกรุปย่อยของ G ซึ่ง $N \subseteq H$ ก็ต่อเมื่อ H/N เป็นกรุปย่อยของ G/N
2. $\eta^{-1}(H/N) = H$ เมื่อ η เป็นสาทิสสัณฐานธรรมชาติของ G ไปบน G/N

2.6 ความสัมพันธ์สมมูลและเซตอันดับ

หัวข้อนี้เราศึกษาความสัมพันธ์สมมูลซึ่งจะขอกล่าวถึงบทนิยามความสัมพันธ์สมมูลและผลแบ่งกั้น และศึกษาความสัมพันธ์ที่เป็นอันดับและเซตอันดับ ซึ่งเป็นความสัมพันธ์ที่มีสมบัติสะท้อน สมบัติปฏิสมมาตร และสมบัติถ่ายทอด

2.6.1 **บทนิยาม** ให้ X เป็นเซตที่ไม่ใช่เซตว่าง และ $\sim$ เป็นความสัมพันธ์ (relation) บน X เราเรียก $\sim$ ว่า**ความสัมพันธ์สมมูล** (equivalence relation) บน X ถ้า $\sim$ สอดคล้องกับสมบัติต่อไปนี้

1. สมบัติสะท้อน (reflexive) นั่นคือ $a \sim a$ สำหรับทุกๆ $\in X$
2. สมบัติสมมาตร (symmetric) นั่นคือ สำหรับทุกๆ $a, b \in X$ ถ้า $a \sim b$ แล้ว $b \sim a$

3. สมบัติถ่ายทอด (transitive) นั่นคือ สำหรับทุกๆ $a, b, c \in X$ ถ้า $a \sim b$ และ $b \sim c$ แล้ว $a \sim c$

2.6.2 **บทนิยาม** ให้ a และ b เป็นจำนวนเต็ม และ m เป็นจำนวนเต็มบวก เรากล่าวว่า a **สมภาค** (congruence) **กับ** b **มอดุโล** m ถ้า m เป็นตัวหารของ $a-b$ และเขียนแทนด้วยสัญลักษณ์ $a \equiv b(\mathrm{mod}\, m)$

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

1. $\varnothing \notin P$
2. $A = B$ หรือ $A \cap B = \varnothing$ สำหรับทุกๆ $A, B \in P$

และ 3. $\bigcup_{A \in P} A = X$

2.6.4 **บทนิยาม** กำหนด S เป็นเซตและ $\leq$ เป็นความสัมพันธ์บน S เราเรียก $\leq$ ว่า**อันดับ** (order) บน S ถ้า $\leq$ สอดคล้องสมบัติต่อไปนี้

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

และเรียกโครงสร้าง $(S, \leq)$ ว่า **เซตอันดับ** (ordered set)

โดยทั่วไปอันดับบนเซต S เขียนแทนด้วยสัญลักษณ์ $\leq$ และสัญลักษณ์ $(a, b) \in \leq$ จะเขียนแทนด้วย $a \leq b$

2.6.5 **ตัวอย่าง** ให้ R เป็นความสัมพันธ์บนเซตของจำนวนเต็ม Z ซึ่งนิยามโดย

$$R = \{(a, b) \in Z \times Z \mid b - a \geq 0\}$$

แล้ว R เป็นอันดับบน Z

2.6.6 **ตัวอย่าง** ให้ S เป็นเซตและให้ $P(S)$ เป็นเซตกำลังของ S ให้ R เป็นความสัมพันธ์บน $P(S)$ ซึ่งนิยามโดย $R = \{(A, B) \in P(S) \times P(S) \mid A \subseteq B\}$ แล้ว R เป็นอันดับบน $P(S)$

2.6.7 **บทนิยาม** เรากล่าวว่าเซตย่อย H ของเซตอันดับ $(S,\leq)$ เป็น**เซตย่อยอันดับเชิงเส้น** (linearly ordered set) **หรือ โซ่** (chain) ถ้า $x \leq y$ หรือ $y \leq x$ สำหรับทุกๆ สมาชิก $x, y \in H$

เซตอันดับในตัวอย่าง 2.6.5 เป็นเซตย่อยอันดับเชิงเส้น แต่เซตอันดับในตัวอย่าง 2.6.6 ไม่เป็นเซตย่อยอันดับเชิงเส้น เพราะว่าถ้า S มีสมาชิกที่แตกต่างกัน คือ a และ b แล้ว $\{a\}$ และ $\{b\}$ ไม่เปรียบเทียบกัน

2.6.8 **บทนิยาม** กำหนด $(S,\leq)$ เป็นเซตอันดับ และ $H \subseteq S$ ถ้า $c \in S$ และ $a \leq c$ สำหรับทุกๆ $a \in H$ เราจะเรียก c ว่า**ขอบเขตบน** (upper bound) ของ H ใน S

ถ้ามี d เป็นขอบเขตบนของ H ซึ่ง $d \leq c$ สำหรับทุกๆ ขอบเขตบน c ของ H จะเรียก d ว่า**ขอบเขตบนน้อยสุด** (least upper bound) ของ H

ในทางกลับกันถ้า $l \in S$ และ $l \leq a$ สำหรับทุกๆ $a \in H$ เราจะเรียก l ว่า**ขอบเขตล่าง** (Lower bound) ของ H ใน S

และถ้ามี s เป็นขอบเขตล่างของ H ซึ่ง $l \leq s$ สำหรับทุกๆ ขอบเขตล่าง l ของ H แล้วจะเรียก s ว่า**ขอบเขตล่างมากสุด** (greatest lower bound) ของ H

2.6.9 **บทนิยาม** กำหนด $(S,\leq)$ เป็นเซตอันดับและ $P \subseteq S$ เราเรียก $u \in P$ ว่า**สมาชิกใหญ่สุดเฉพาะกลุ่ม** (maximal element) ของ P ถ้า $u = v$ เมื่อ $u \leq v \in P$

และจะเรียกสมาชิก $s \in P$ ว่า **สมาชิกน้อยสุดเฉพาะกลุ่ม** (minimal element) ของ P ถ้า $s = v$ เมื่อ $s \geq v \in P$

2.6.10 Zorn's Lemma: ถ้าทุกๆ เซตย่อยอันดับเชิงเส้นในเซตอันดับ $(S,\leq)$ มีขอบเขตบนใน S แล้ว S มีสมาชิกใหญ่สุดเฉพาะกลุ่ม

บทที่ 3

กรุปย่อยนอร์มัลไลเซอร์และคอมมิวเตเตอร์

ในบทนี้เรากล่าวถึงบทนิยามและทฤษฎีบทของกรุปย่อยนอร์มัลไลเซอร์ และบทนิยามและทฤษฎีบทเกี่ยวกับกรุปย่อยคอมมิวเตเตอร์

3.1 กรุปย่อยนอร์มัลไลเซอร์

ในหัวข้อนี้เรากล่าวถึงบทนิยามและทฤษฎีบทของกรุปย่อยนอร์มัลไลเซอร์ และกล่าวถึงศูนย์กลางของกรุป

3.1.1 **ทฤษฎีบท** ให้ G เป็นกรุป และ $H \leq G$ แล้วเซต $N[H] = \left\{ g \in G \,\middle|\, g^{-1}Hg = H \right\}$ เป็นกรุปย่อยของ G และ H เป็นกรุปย่อยปกติของ $N[H]$

บทพิสูจน์ ให้ G เป็นกรุป และ $H \leq G$ และให้เซต $N[H] = \left\{ g \in G \,\middle|\, g^{-1}Hg = H \right\}$

ต้องการแสดงว่า $N[H] \leq G$ เนื่องจาก $e \in G$ และ $e^{-1}He = H$ ดังนั้น $e \in N[H]$ ซึ่งแสดงว่า $N[H] \neq \varnothing$ ให้ $a, b \in N[H]$ แล้ว $a, b \in G$ ซึ่ง $a^{-1}Ha = H$ และ $b^{-1}Hb = H$ ฉะนั้น $a^{-1}Ha = b^{-1}Hb$ ทำให้ได้ $H = ba^{-1}Hab^{-1} = \left(ab^{-1}\right)^{-1}Hab^{-1}$ นั่นคือ $\left(ab^{-1}\right)^{-1}Hab^{-1} = H$ เนื่องจาก $ab^{-1} \in G$ ดังนั้น $ab^{-1} \in N[H]$ เพราะฉะนั้น $N[H]$ เป็นกรุปย่อยของ G

ต่อไปจะแสดงว่า H เป็นกรุปย่อยปกติของ $N[H]$ ให้ $h \in H$ แล้ว $h^{-1}Hh = H$ ซึ่งแสดงว่า $h \in N[H]$ ดังนั้น $H \subseteq N[H]$ เนื่องจาก $H \leq G$ และ $N[H] \leq G$ ดังนั้น $H \leq N[H]$ และจากบทนิยามของ $N[H]$ จะได้ว่า $g^{-1}Hg = H$ สำหรับทุกๆ $g \in N[H]$ ดังนั้น H เป็นกรุปย่อยปกติของ $N[H]$ ∎

3.1.2 **บทนิยาม** เราเรียกกรุปย่อย $N[H] = \left\{ g \in G \,\middle|\, g^{-1}Hg = H \right\}$ ว่า**นอร์มัลไลเซอร์** (normalizer) ของ H ใน G

3.1.3 **ทฤษฎีบท** ให้ K และ H เป็นกรุปย่อยของ G และ H เป็นกรุปย่อยปกติของ K แล้ว K เป็นกรุปย่อยของ $N[H]$

บทพิสูจน์ ให้ K และ H เป็นกรุปย่อยของ G และให้ H เป็นกรุปย่อยปกติของ K เราจะแสดงว่า $K \leq N[H]$ ให้ $k \in K$ แล้ว $k^{-1}Hk = H$ ฉะนั้น $k \in N[H]$ ทำให้ได้ว่า $K \subseteq N[H]$ เนื่องจาก $K \leq G$ และ $N[H] \leq G$ ดังนั้น $K \leq N[H]$ ∎

โดยทฤษฎีบท 3.1.1 และ 3.1.3 ทำให้ได้ว่า $N[H]$ เป็นกรุปย่อยที่ใหญ่ที่สุดของ G ซึ่งมี H เป็นกรุปย่อยปกติ

3.1.4 **ทฤษฎีบท** ให้ G เป็นกรุป แล้วเซต $Z(G) = \{a \in G \mid ax = xa \text{ สำหรับทุก } x \text{ ใน } G\}$ เป็นกรุปย่อยปกติของ G

บทพิสูจน์ เนื่องจากเอกลักษณ์ $e \in G$ สอดคล้องสมบัติ $ex = xe$ สำหรับทุกๆ $x \in G$ ดังนั้น $e \in Z(G)$ ซึ่งทำให้ได้ว่า $Z(G) \neq \varnothing$ ให้ $a, b \in Z(G)$ จะได้ว่า $ax = xa$ และ $bx = xb$ สำหรับ $x \in G$ ดังนั้น $abx = axb = xab$ ทำให้ได้ว่า $ab \in Z(G)$ และเนื่องจาก $a \in Z(G)$ ดังนั้น $a^{-1} \in Z(G)$ เพราะฉะนั้น $Z(G)$ เป็นกรุปย่อยของ G ต่อไปจะแสดงว่า $gZ(G) = Z(G)g$ ให้ $g \in G$ ถ้า $x \in gZ(G)$ แล้วจะมี $a \in Z(G)$ ซึ่ง $ga = ag$ และ $x = ga$ ฉะนั้น $x = ag \in Z(G)g$ ดังนั้น $gZ(G) \subseteq Z(G)g$ ถ้า $x \in Z(G)g$ แล้วจะมี $a \in Z(G)$ ซึ่ง $ga = ag$ และ $x = ag$ ฉะนั้น $x = ga \in gZ(G)$ ดังนั้น $Z(G)g \subseteq gZ(G)$ ทำให้ได้ว่า $gZ(G) = Z(G)g$ เพราะฉะนั้น $Z(G)$ เป็นกรุปย่อยปกติของ G ∎

3.1.5 **บทนิยาม** เราเรียก $Z(G) = \{a \in G \mid ax = xa \text{ สำหรับทุก } x \text{ ใน } G\}$ ว่า**ศูนย์กลาง** (center) ของ G

3.1.6 **ทฤษฎีบท** ให้ G เป็นกรุป แล้ว

1. $Z(G)$ เป็นกรุปอาบีเลียน
2. G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ $G = Z(G)$

บทพิสูจน์ 1. ให้ $a,b \in Z(G)$ แล้ว $a, b \in G$ ทำให้ได้ว่า $ab = ba$ ดังนั้น $Z(G)$ เป็นกรุปอาบีเลียน

2. $(\rightarrow)$ สมมติ G เป็นกรุปอาบีเลียน และให้ $a \in G$ แล้ว $ax = xa$ สำหรับทุก $x \in G$ ดังนั้น $a \in Z(G)$ นั่นคือ $G \subseteq Z(G)$ เนื่องจาก $Z(G) \subseteq G$ ดังนั้น $G = Z(G)$

$(\leftarrow)$ ให้ $G = Z(G)$ แล้วโดยข้อ 1. จะได้ว่า G เป็นกรุปอาบีเลียน ∎

3.2 กรุปย่อยคอมมิวเตเตอร์

ในหัวข้อนี้เราจะให้บทนิยามของคอมมิวเตเตอร์ของสมาชิกและกรุปย่อยคอมมิวเตเตอร์ รวมทั้งแสดงความสัมพันธ์ของสมาชิกคอมมิวเตเตอร์ในกรุปดังทฤษฎีบทต่อไปนี้

3.2.1 **บทนิยาม** กำหนด G เป็นกรุป และ $a, b \in G$ จะเรียก $aba^{-1}b^{-1}$ ว่า**คอมมิวเตเตอร์** (commutator) ของ a และ b และเขียนแทนด้วยสัญลักษณ์ (a,b)

3.2.2 **ทฤษฎีบท** ให้ G เป็นกรุป และ $a,b,c \in G$

1. ถ้า $(a,b) = e$ แล้ว $ab = ba$
2. ถ้า $(a,c) \in Z(G)$ แล้ว $(a, bc) = (a, b)(a, c)$
3. ถ้า $(b,c) \in Z(G)$ แล้ว $(ab,c) = (a,c)(b,c)$
4. ถ้า $(a,b) \in Z(G)$ แล้ว $(a,b)^n = (a,b^n)$ และ $(a,b)^n = (a^n,b)$ สำหรับทุกจำนวนเต็มบวก n
5. ถ้า $(a,b) \in Z(G)$ แล้ว $(ab)^n = (b,a)^{\frac{1}{2}n(n-1)}a^n b^n$ สำหรับทุกจำนวนเต็มบวก n

บทพิสูจน์ ให้ $a, b, c \in G$

1. ให้ $(a,b) = e$ แล้ว $aba^{-1}b^{-1} = e$ ดังนั้น $ab = ba$

2. ให้ $(a,c) \in Z(G)$ แล้ว $(a, bc) = a(bc)a^{-1}(bc)^{-1} = abca^{-1}c^{-1}b^{-1} = ab\left(a^{-1}a\right)ca^{-1}c^{-1}b^{-1} = aba^{-1}\left(aca^{-1}c^{-1}\right)b^{-1} = aba^{-1}(a,c)b^{-1} = aba^{-1}b^{-1}(a,c) = (a,b)(a,c)$
ดังนั้น $(a, bc) = (a, b)(a, c)$

3. ให้ $(b, c) \in Z(G)$ แล้ว $(ab, c) = abc(ab)^{-1}c^{-1} = abcb^{-1}a^{-1}c^{-1} = abcb^{-1}\left(c^{-1}c\right)a^{-1}c^{-1} = a\left(bcb^{-1}c^{-1}\right)ca^{-1}c = a(b, c)ca^{-1}c^{-1} = ac(b, c)a^{-1}c^{-1} = aca^{-1}(b,c)c^{-1} = aca^{-1}c^{-1}(b,c) = (a,c)(b,c)$ ดังนั้น $(ab,c) = (a, c)(b, c)$

4. ให้ $(a, b) \in Z(G)$ สำหรับแต่ละจำนวนเต็มบวก n ให้ $P(n)$ แทนข้อความ $(a, b)^n = \left(a, b^n\right)$

ขั้นที่ 1 เพราะว่า $(a, b)^1 = (a, b) = \left(a, b^1\right)$ ดังนั้น $P(1)$ เป็นจริง

ขั้นที่ 2 ให้ k เป็นจำนวนเต็มบวกซึ่ง $P(k)$ เป็นจริง แล้ว $(a, b)^k = \left(a, b^k\right)$ ทำให้ได้ $(a, b)^{k+1} = (a, b)^k(a, b) = \left(a, b^k\right)(a, b) = \left(ab^k a^{-1}b^{-k}\right)(a, b) = ab^k a^{-1}(a, b)b^{-k} = ab^k a^{-1}aba^{-1}b^{-1}b^{-k} = ab^k ba^{-1}b^{-1}b^{-k} = ab^{k+1}a^{-1}b^{-(k+1)} = \left(a, b^{k+1}\right)$ ดังนั้น $P(k+1)$ เป็นจริง โดยอุปนัยเชิงคณิตศาสตร์จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n ดังนั้น $(a,b)^n = \left(a, b^n\right)$ สำหรับทุกจำนวนเต็มบวก n

โดยการพิสูจน์ทำนองเดียวกันเราได้ว่า $(a,b)^n = \left(a^n, b\right)$ สำหรับทุกจำนวนเต็มบวก n

5. ให้ $(a,b) \in Z(G)$ สำหรับแต่ละจำนวนเต็มบวก n ให้ $P(n)$ แทนข้อความ $(ab)^n = (b,a)^{\frac{1}{2}n(n-1)}a^n b^n$

ขั้นที่ 1 เพราะว่า $(ab)^1 = (b,a)^{\frac{1}{2}\cdot 1\cdot(1-1)}a^1 b^1$ ดังนั้น $P(1)$ เป็นจริง

ขั้นที่ 2 ให้ k เป็นจำนวนเต็มบวกซึ่ง $P(k)$ เป็นจริง แล้ว $(ab)^k = (b,a)^{\frac{1}{2}k(k-1)}a^k b^k$ ทำให้ได้

$$
\begin{aligned}
(ab)^{k+1} &= (ab)^k ab \\
&= (b,a)^{\frac{1}{2}k(k-1)}a^k b^k ab \\
&= (b,a)^{\frac{1}{2}k(k-1)}a^k b^k a\left(b^{-k}a^{-1}ab^k\right)b \\
&= (b,a)^{\frac{1}{2}k(k-1)}a^k \left(b^k ab^{-k}a^{-1}\right)ab^k b \\
&= (b,a)^{\frac{1}{2}k(k-1)}a^k (b,a)^k ab^k b \\
&= (b,a)^{\frac{1}{2}k(k-1)}(b,a)^k a^k ab^k b \\
&= (b,a)^{\frac{1}{2}k(k-1)+k}a^{k+1}b^{k+1} \\
&= (b,a)^{\frac{1}{2}(k+1)k}a^{k+1}b^{k+1}
\end{aligned}
$$

ดังนั้น $P(k+1)$ เป็นจริง โดยอุปนัยเชิงคณิตศาสตร์จะได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนเต็มบวก n เพราะฉะนั้น $(ab)^n = (b,a)^{\frac{1}{2}n(n-1)}a^n b^n$ สำหรับทุกจำนวนเต็มบวก n ∎

บทที่ 4

กรุปอาบีเลียนขนาดจำกัด

ในบทนี้เราศึกษาผลคูณตรงของกรุป ทฤษฎีบทของโคชีและนำทฤษฎีบทของโคชีมาช่วยพิสูจน์ทฤษฎีบทซีโลว์ แล้วประยุกต์ทฤษฎีบทของซีโลว์ในการพิสูจน์ว่ากรุปอาบีเลียนอันดับจำกัดเขียนได้ในรูปผลคูณตรงของกรุปวัฏจักรขนาดจำกัด

4.1 ผลคูณตรงของกรุป

ในหัวข้อนี้เราศึกษาการนำกรุปจำนวนจำกัดกรุปมาสร้างกรุปขึ้นใหม่ เราเรียกว่ากรุปผลคูณตรง ตลอดจนศึกษาทฤษฎีบทต่าง ๆ ที่สำคัญของผลคูณตรง

4.1.1 **ทฤษฎีบท** ให้ $G_1, G_2, ..., G_n$ เป็นกรุป และ **ผลคูณคาทีเซียน** (cartesian product) ของ $G_1, G_2, ..., G_n$ เขียนแทนด้วย $G_1 \times G_2 \times ... \times G_n$ นิยามโดย

$$G_1 \times G_2 \times ... \times G_n = \{(g_1, g_2, ..., g_n) \mid g_i \in G_i \ ; i = 1,2,...,n\}$$

และให้ $\circ : (G_1 \times G_2 \times ... \times G_n) \times (G_1 \times G_2 \times ... \times G_n) \to (G_1 \times G_2 \times ... \times G_n)$ นิยามโดย

$$(g_1, g_2, ..., g_n) \circ (h_1, h_2, ..., h_n) = (g_1h_1, g_2h_2, ..., g_nh_n)$$

สำหรับทุกๆ $(g_1, g_2, ..., g_n)$ และ $(h_1, h_2, ..., h_n)$ ใน $G_1 \times G_2 \times ... \times G_n$ แล้ว $(G_1 \times G_2 \times ... \times G_n \ ; \circ)$ เป็นกรุป

บทพิสูจน์ ให้ $G_1, G_2, ..., G_n$ เป็นกรุป

1. ให้ $(g_1, g_2, ..., g_n), (h_1, h_2, ..., h_n)$ และ $(i_1, i_2, ..., i_n)$ เป็นสมาชิกของ $G_1 \times G_2 \times ... \times G_n$ แล้ว

$$\begin{aligned}((g_1, g_2, ..., g_n) \circ (h_1, h_2, ..., h_n)) \circ (i_1, i_2, ..., i_n) &= (g_1h_1, g_2h_2, ..., g_nh_n) \circ (i_1, i_2, ..., i_n) \\ &= ((g_1h_1)i_1, (g_2h_2)i_2, ..., (g_nh_n)i_n) \\ &= (g_1(h_1i_1), g_2(h_2i_2), ..., g_n(h_ni_n)) \\ &= (g_1, g_2, ..., g_n) \circ (h_1i_1, h_2i_2, ..., h_ni_n)\end{aligned}$$

$$= (g_1, g_2, ..., g_n) \circ ((h_1, h_2, ..., h_n) \circ (i_1, i_2, ..., i_n))$$

ดังนั้น $\circ$ สอดคล้องสมบัติการเปลี่ยนหมู่บน $G_1 \times G_2 \times ... \times G_n$

2. ให้ e_i เป็นเอกลักษณ์ของ G_i สำหรับ $i = 1, 2, ..., n$ แล้ว

$(e_1, e_2, ..., e_n) \in G_1 \times G_2 \times ... \times G_n$ ให้ $(g_1, g_2, ..., g_n) \in G_1 \times G_2 \times ... \times G_n$ แล้ว

$$\begin{aligned}(g_1, g_2, ..., g_n) \circ (e_1, e_2, ..., e_n) &= (g_1 e_1, g_2 e_2, ..., g_n e_n) \\ &= (g_1, g_2, ..., g_n) \\ &= (e_1 g_1, e_2 g_2, ..., e_n g_n) \\ &= (e_1, e_2, ..., e_n) \circ (g_1, g_2, ..., g_n)\end{aligned}$$

ดังนั้น $(e_1, e_2, ..., e_n)$ เป็นเอกลักษณ์ของ $G_1 \times G_2 \times ... \times G_n$ ภายใต้ $\circ$

3. ให้ $(g_1, g_2, ..., g_n) \in G_1 \times G_2 \times ... \times G_n$ แล้ว $g_i \in G_i$ สำหรับ $i = 1, 2, ..., n$

เพราะว่าแต่ละ $G_1, G_2, ..., G_n$ เป็นกรุป ดังนั้น ${g_i}^{-1} \in G_i$ สำหรับทุกๆ $i = 1, 2, ..., n$ ทำให้ได้ว่า $\left({g_1}^{-1}, {g_2}^{-1}, ..., {g_n}^{-1}\right) \in G_1 \times G_2 \times ... \times G_n$ โดยที่

$$\begin{aligned}(g_1, g_2, ..., g_n) \circ \left({g_1}^{-1}, {g_2}^{-1}, ..., {g_n}^{-1}\right) &= \left(g_1 {g_1}^{-1}, g_2 {g_2}^{-1}, ..., g_n {g_n}^{-1}\right) \\ &= (e_1, e_2, ..., e_n) \\ &= \left({g_1}^{-1} g_1, {g_2}^{-1} g_2, ..., {g_n}^{-1} g_n\right) \\ &= \left({g_1}^{-1}, {g_2}^{-1}, ..., {g_n}^{-1}\right) \circ (g_1, g_2, ..., g_n)\end{aligned}$$

ดังนั้น $\left({g_1}^{-1}, {g_2}^{-1}, ..., {g_n}^{-1}\right)$ เป็นตัวผกผันของ $(g_1, g_2, ..., g_n) \in G_1 \times G_2 \times ... \times G_n$ ภายใต้ $\circ$

เพราะฉะนั้น $(G_1 \times G_2 \times ... \times G_n ; \circ)$ เป็นกรุป ∎

4.1.2 **บทนิยาม** เราเรียกกรุป $(G_1 \times G_2 \times ... \times G_n ; \circ)$ ในทฤษฎีบท 4.1.1 ว่า**ผลคูณตรง** (direct product) ของกรุป $G_1, G_2, ..., G_n$

4.1.3 **บทนิยาม** ให้ $G_1, G_2, ..., G_n$ เป็นกรุป เรากล่าวว่า G เป็น **ผลคูณภายนอก** (external direct product) ของ $G_1, G_2, ..., G_n$ ถ้า G สมสัณฐานกันกับผลคูณตรงของ $G_1, G_2, ..., G_n$

4.1.4 **ทฤษฎีบท** ให้ n เป็นจำนวนเต็มบวก และให้ $G_1, G_2, ..., G_n$ เป็นกรุป แล้วสำหรับแต่ละ $1 \le i \le n$ จะมีกรุปย่อยปกติ $\overline{G_i}$ ของกรุป $G_1 \times G_2 \times ... \times G_n$ ซึ่ง

1. $\overline{G_i}$ สมสัณฐานกันกับ G_i ทุกๆ $1 \le i \le n$
2. $\overline{G_i} \cap \left(\overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}\right) = \{(e_1, e_2, ..., e_n)\}$ สำหรับแต่ละ $1 \le i \le n$
3. $G_1 \times G_2 \times ... \times G_n = \overline{G_1}\overline{G_2}...\overline{G_n}$ สำหรับแต่ละ $1 \le i \le n$

บทพิสูจน์ ให้ n เป็นจำนวนเต็มบวก และให้ $G_1, G_2, ..., G_n$ เป็นกรุป สำหรับแต่ละ $i = 1,2,...,n$ ให้ $\overline{G_i} = \{(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n) \mid g_i \in G_i\}$ แล้ว $\overline{g_i} \in \overline{G_i}$ ก็ต่อเมื่อ $\overline{g_i} = (e_1, e_2, ..., g_i, e_{i+1}, ..., e_n)$ สำหรับบาง $g_i \in G_i$ เราจะพิสูจน์ว่า $\overline{G_i}$ เป็นกรุปย่อยปกติของกรุป $G_1 \times G_2 \times ... \times G_n$ สำหรับแต่ละ $i = 1,2,...,n$

เพราะว่า $G_1, G_2, ..., G_n$ เป็นกรุป แล้วแต่ละ G_i จะมี e_i เป็นเอกลักษณ์ สำหรับแต่ละ $i = 1,2,...,n$ ดังนั้น $(e_1, e_2, ..., e_n) \in \overline{G_i}$ เป็นเอกลักษณ์ของ $G_1 \times G_2 \times ... \times G_n$ ทำให้ $\overline{G_i} \neq \varnothing$ สำหรับทุกๆ $i = 1,2,...,n$

i) ให้ $i \in \{1,2,...,n\}$ และ $(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n), (e_1, e_2, ..., h_i, e_{i+1}, ..., e_n) \in \overline{G_i}$ แล้ว $(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n)(e_1, e_2, ..., h_i, e_{i+1}, ..., e_n) = (e_1, e_2, ..., g_i h_i, e_{i+1}, ..., e_n) \in \overline{G_i}$ ดังนั้น $\overline{G_i}$ มีสมบัติปิดภายใต้การดำเนินการของ $G_1 \times G_2 \times ... \times G_n$

ii) ให้ $(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n) \in \overline{G_i}$ แล้ว $g_i \in G_i$ ดังนั้นมี $g_i^{-1} \in G_i$ ทำให้มี $\left(e_1, e_2, ..., g_i^{-1}, e_{i+1}, ..., e_n\right) \in \overline{G_i}$ ซึ่งทำให้

$$\begin{aligned}(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n)\left(e_1, e_2, ..., g_i^{-1}, e_{i+1}, ..., e_n\right) &= \left(e_1, e_2, ..., g_i g_i^{-1}, e_{i+1}, ..., e_n\right) \\ &= (e_1, e_2, ..., e_n) \\ &= \left(e_1, e_2, ..., g_i^{-1} g_i, e_{i+1}, ..., e_n\right) \\ &= \left(e_1, e_2, ..., g_i^{-1}, e_{i+1}, ..., e_n\right)(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n)\end{aligned}$$

ดังนั้น $\left(e_1, e_2, ..., g_i^{-1}, e_{i+1}, ..., e_n\right)$ เป็นตัวผกผันของ $(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n)$ เพราะฉะนั้น $\overline{G_i}$ เป็นกรุปย่อยของกรุป $G_1 \times G_2 \times ... \times G_n$

iii) ให้ $(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n) \in \overline{G_i}$ และให้ $(g_1, g_2, ..., g_n) \in G_1 \times G_2 \times ... \times G_n$ แล้ว $(g_1, g_2, ..., g_n)(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n)(g_1, g_2, ..., g_n)^{-1}$

$$\begin{aligned}&= (g_1, g_2, ..., g_n)(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n)\left(g_1^{-1}, g_2^{-1}, ..., g_n^{-1}\right) \\ &= \left(g_1 e_1 g_1^{-1}, g_2 e_2 g_2^{-1}, ..., g_{i-1} e_{i-1} g_{i-1}^{-1}, g_i e_i g_i^{-1}, g_{i+1} e_{i+1} g_{i+1}^{-1}, ..., g_n e_n g_n^{-1}\right) \\ &= \left(g_1 g_1^{-1}, g_2 g_2^{-1}, ..., g_{i-1} g_{i-1}^{-1}, g_i g_i^{-1}, g_{i+1} g_{i+1}^{-1}, ..., g_n g_n^{-1}\right) \\ &= (e_1, e_2, ..., g_i, e_{i+1}, ..., e_n) \in \overline{G_i}\end{aligned}$$

ดังนั้น $(g_1, g_2, ..., g_n)\overline{G_i}(g_1, g_2, ..., g_n)^{-1} \subseteq \overline{G_i}$ ทุกๆ $(g_1, g_2, ..., g_n) \in G_1 \times G_2 \times ... \times G_n$ เพราะฉะนั้น $\overline{G_i}$ เป็นกรุปย่อยปกติของกรุป $G_1 \times G_2 \times ... \times G_n$

ต่อไปเราจะพิสูจน์ว่า

1. $\overline{G_i}$ สมสัณฐานกันกับ G_i ทุกๆ $1 \le i \le n$
2. $\overline{G_i} \cap \left(\overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}\right) = \{(e_1, e_2, ..., e_n)\}$ สำหรับแต่ละ $1 \le i \le n$
3. $G_1 \times G_2 \times ... \times G_n = \overline{G_1}\overline{G_2}...\overline{G_n}$ สำหรับแต่ละ $1 \le i \le n$

1. ให้ $i = 1,2,...,n$ และให้ $\alpha : \overline{G_i} \to G_i$ นิยามโดย $\alpha(e_1, e_2, ..., a_i, e_{i+1}, ..., e_n) = a_i$ สำหรับทุกๆ $a_i \in G_i$ จะได้ว่า α เป็นฟังก์ชัน

1.1 ให้ $(e_1, e_2, ..., a_i, e_{i+1}, ..., e_n), (e_1, e_2, ..., b_i, e_{i+1}, ..., e_n) \in \overline{G_i}$ แล้วจะได้ว่า

$$\begin{aligned}\alpha((e_1, e_2, ..., a_i, e_{i+1}, ..., e_n)(e_1, e_2, ..., b_i, e_{i+1}, ..., e_n)) &= (e_1, e_2, ..., a_i b_i, e_{i+1}, ..., e_n) \\ &= a_i b_i \\ &= \alpha(e_1, e_2, ..., a_i, e_{i+1}, ..., e_n)\alpha(e_1, e_2, ..., b_i, e_{i+1}, ..., e_n)\end{aligned}$$

เพราะฉะนั้น α เป็นสาทิสสัณฐาน

1.2 ให้ $(e_1, e_2, ..., a_i, e_{i+1}, ..., e_n) \in \overline{G_i}$ และ $(e_1, e_2, ..., b_i, e_{i+1}, ..., e_n) \in \overline{G_i}$ ซึ่ง $\alpha(e_1, e_2, ..., a_i, e_{i+1}, ..., e_n) = \alpha(e_1, e_2, ..., b_i, e_{i+1}, ..., e_n)$ แล้ว $a_i = b_i$

ดังนั้น $(e_1, e_2, ..., a_i, e_{i+1}, ..., e_n) = (e_1, e_2, ..., b_i, e_{i+1}, ..., e_n)$

เพราะฉะนั้น α เป็นฟังก์ชันหนึ่งต่อหนึ่ง

1.3 ให้ $a_i \in G_i$ แล้ว $(e_1, e_2, ..., a_i, e_{i+1}, ..., e_n) \in \overline{G_i}$ ซึ่ง

$\alpha(e_1, e_2, ..., a_i, e_{i+1}, ..., e_n) = a_i$ เพราะฉะนั้น α เป็นฟังก์ชันทั่วถึง

ดังนั้น $\overline{G_i}$ สมสัณฐานกันกับ G_i ทุกๆ $1 \le i \le n$

2. ให้ $(g_1, g_2, ..., g_n) \in \overline{G_i} \cap \left(\overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}\right)$ แล้ว $(g_1, g_2, ..., g_n) \in \overline{G_i}$ และ $(g_1, g_2, ..., g_n) \in \overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}$ เพราะว่า $(g_1, g_2, ..., g_n) \in \overline{G_i}$ แล้ว $(g_1, g_2, ..., g_n) = (e_1, e_2, ..., g_i, e_{i+1}, ..., e_n)$ ดังนั้น $g_k = e_k$ ทุกๆ $1 \le k \ne i \le n$

เพราะว่า $(g_1, g_2, ..., g_n) \in \overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}$ แล้วจะมี $\overline{g_k} = \overline{G_k}$ สำหรับ $1 \le k \ne i \le n$ ซึ่ง $(g_1, g_2, ..., g_n) = \overline{g_1}\overline{g_2}...\overline{g_{i-1}}\overline{g_{i+1}}...\overline{g_n} = \overline{g_1}\overline{g_2}...\overline{g_{i-1}}\overline{e_i}\overline{g_{i+1}}...\overline{g_n}$

$(g_1, g_2, ..., g_n) = (g_1, g_2, ..., g_{i-1}, e_i, g_{i+1}, ..., g_n)$

เพราะฉะนั้น $(e_1, e_2, ..., g_i, e_{i+1}, ..., e_n) = (g_1, g_2, ..., g_{i-1}, e_i, g_{i+1}, ..., g_n)$

จะได้ว่า $g_i = e_i$ เพราะฉะนั้น $(g_1, g_2, ..., g_n) = (e_1, e_2, ..., e_n)$

และในทางกลับกัน $(e_1,e_2,...,e_n)\in\overline{G_i}$ และ $(e_1,e_2,...,e_n)\in\overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}$
จะได้ว่า $(e_1,e_2,...,e_n)\in\overline{G_i}\cap\left(\overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}\right)$
เพราะฉะนั้น $\overline{G_i}\cap\left(\overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}\right)=\{(e_1,e_2,...,e_n)\}$ โดยที่ $i=1,2,...,n$
3. ให้ $(g_1,g_2,...,g_n)\in G_1\times G_2\times...\times G_n$ แล้ว

$$(g_1,g_2,...,g_n)=(g_1,e_2,...,e_n)(e_1,g_2,e_3,...,e_n)...(e_1,e_2,...,g_n)=\overline{g_1}\overline{g_2}...\overline{g_n}$$

เพราะฉะนั้น $(g_1,g_2,...,g_n)\in\overline{G_1}\overline{G_2}...\overline{G_n}$
และในทางกลับกันให้ $\overline{g_1}\overline{g_2}...\overline{g_n}\in\overline{G_1}\overline{G_2}...\overline{G_n}$ แล้ว $\overline{g_1}\overline{g_2}...\overline{g_n}=(g_1,e,...,e)(e,g_2,e,...,e)$
$...(e,e,...,g_n)=(g_1,g_2,...,g_n)\in G_1\times G_2\times...\times G_n$ เพราะฉะนั้น $G_1\times G_2\times...\times G_n=$
$\overline{G_1}\overline{G_2}...\overline{G_n}$ สำหรับแต่ละ $1\le i\le n$ ∎

เมื่อเราศึกษาผลคูณภายนอกและทฤษฎีบทเกี่ยวกับผลคูณภายนอกแล้วต่อไปเราจะศึกษาผลคูณของกรุปซึ่งเรียกว่าผลคูณภายในและศึกษาทฤษฎีบทที่เกี่ยวข้องกับผลคูณภายใน

4.1.5 **บทนิยาม** ให้ G เป็นกรุปที่มี e เป็นเอกลักษณ์ และ $G_1,G_2,...,G_n$ เป็นกรุปย่อยปกติของ G เรากล่าวว่า G เป็น**ผลคูณภายใน** (internal direct product) ของ $G_1,G_2,...,G_n$ ถ้า

1. $G=G_1G_2...G_n$
2. $G_i\cap(G_1G_2...G_{i-1}G_{i+1}...G_n)=\{e\}$ สำหรับแต่ละ $1\le i\le n$

4.1.6 **ทฤษฎีบท** ให้ $G_1,G_2,...,G_n$ เป็นกรุปย่อยปกติของกรุป G ที่มี e เป็นเอกลักษณ์ ถ้า G เป็นผลคูณภายในของ $G_1,G_2,...,G_n$ แล้ว

1. $G_i\cap G_j=\{e\}$ สำหรับทุกๆ $1\le i\ne j\le n$
2. $h_ih_j=h_jh_i$ สำหรับทุกๆ $h_i\in G_i$ และ $h_j\in G_j$ และ $1\le i,j\le n$

บทพิสูจน์ ให้ $G_1,G_2,...,G_n$ เป็นกรุปย่อยปกติของกรุป G ที่มี e เป็นเอกลักษณ์ และให้ G เป็นผลคูณภายในของ $G_1,G_2,...,G_n$
1. ให้ $1\le i<j\le n$ และให้ $k\in G_i\cap G_j$ แล้ว $k\in G_i$ และ $k\in G_j$ ให้ $e_s=e$ ทุกๆ $s=1,2,...,n$ แล้ว

$$k=e_1e_2...e_{i-1}e_{i+1}...e_{j-1}ke_{j+1}...e_n\in G_1G_2...G_{i-1}G_{i+1}...G_n$$

เพราะฉะนั้น $k \in G_i \cap (G_1G_2...G_{i-1}G_{i+1}...G_n)$ ทำให้ได้ $k = e$

2. ให้ $1 \le i, j \le n$ และให้ $h_i \in G_i$ และ $h_j \in G_j$ แล้วเพราะว่า $h_i{}^{-1} \in G_i$ และ $h_j, h_j^{-1} \in G$ และ G_i เป็นกรุปย่อยปกติของกรุป G ดังนั้น $h_j h_i{}^{-1} h_j{}^{-1} \in G_i$ ให้ $s_i = h_j h_i{}^{-1} h_j{}^{-1} \in G_i$ ทำให้ได้ $h_i h_j h_i{}^{-1} h_j{}^{-1} = h_i\left(h_j h_i{}^{-1} h_j{}^{-1}\right) = h_i s_i \in G_i$ แล้วเพราะว่า $h_j \in G_j$ และ $h_i, h_i{}^{-1} \in G$ และ G_j เป็นกรุปย่อยปกติของกรุป G ดังนั้น $h_i h_j h_i{}^{-1} \in G_j$ ให้ $t_j = h_i h_j h_i{}^{-1} \in G_j$ ทำให้ได้ $h_i h_j h_i{}^{-1} h_j{}^{-1} = \left(h_i h_j h_i{}^{-1}\right) h_j{}^{-1} = t_j h_j{}^{-1} \in G_j$ แล้ว $h_i h_j h_i{}^{-1} h_j{}^{-1} \in G_i \cap G_j = \{e\}$ เพราะฉะนั้น $h_i h_j h_i{}^{-1} h_j{}^{-1} = e$ แล้ว $h_i h_j = h_j h_i$ ∎

จากบทนิยาม 4.1.5 แสดงให้เห็นว่า G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$ แล้ว $G = G_1G_2 ...G_n$ ทำให้ได้ว่าแต่ละ $g \in G$ ยังเขียนได้ในรูป $g = g_1g_2 ...g_n$ โดยที่ $g_i \in G_i$ ต่อไปจะแสดงให้เห็นว่าแต่ละ $g \in G$ เขียนในรูป $g = g_1g_2 ...g_n$ ได้เพียงแบบเดียวเท่านั้น

4.1.7 **ทฤษฎีบท** ให้ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปกติของกรุป G ถ้า G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$ แล้วแต่ละ $g \in G$ เขียนได้ในรูป $g = g_1g_2 ...g_n$ โดยที่ $g_i \in G_i$ สำหรับแต่ละ $i = 1,2,...,n$ ได้เพียงแบบเดียวเท่านั้น

บทพิสูจน์ ให้ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปกติของกรุป G และให้ G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$

ให้ $g \in G$ และสมมติมี $g_i \in G_i$ และ $h_i \in G_i$ เมื่อ $i = 1,2,...,n$ ซึ่ง $g = g_1g_2 ...g_n$ และ $g = h_1h_2 ...h_n$ แล้ว $g_1g_2 ...g_n = h_1h_2...h_n$ จะแสดงว่า $g_i = h_i$ ทุกๆ $i = 1,2,...,n$

ให้ $i \in \{1,2,...,n\}$ แล้วจะได้ว่า $g_1g_2 ...g_n = h_1h_2...h_n$ ดังนั้น

$$\begin{aligned} g_i &= (g_1g_2 ...g_{i-1})^{-1}(h_1h_2...h_n)(g_{i+1}g_{i+2} ...g_n)^{-1} \\ &= g_{i-1}^{-1}g_{i-2}^{-1} ...g_1^{-1}h_1h_2...h_ng_n^{-1}g_{n-1}^{-1} ...g_{i+1}^{-1} \\ &= h_i\left(h_1g_1^{-1}\right)\left(h_2g_2^{-1}\right)...\left(h_{i-1}g_{i-1}^{-1}\right)\left(h_{i+1}g_{i+1}^{-1}\right)...\left(h_ng_n^{-1}\right) \end{aligned}$$

ทำให้ได้ว่า $g_ih_i^{-1} = \left(h_1g_1^{-1}\right)\left(h_2g_2^{-1}\right)...\left(h_{i-1}g_{i-1}^{-1}\right)\left(h_{i+1}g_{i+1}^{-1}\right)...\left(h_ng_n^{-1}\right)$

ซึ่งแสดงว่า $g_ih_i^{-1} \in G_1G_2 ...G_{i-1}G_{i+1}...G_n$ และ $g_ih_i^{-1} \in G_i$

เพราะฉะนั้น $g_ih_i^{-1} \in G_i \cap (G_1G_2 ...G_{i-1}G_{i+1}...G_n)$

ดังนั้น $g_i h_i^{-1} = e$ เพราะฉะนั้น $g_i = h_i$ ∎

ต่อไปเราจะแสดงความสัมพันธ์ระหว่างผลคูณภายนอกและผลคูณภายใน

4.1.8 **ทฤษฎีบท** ให้ $G, G_1, G_2, ..., G_n$ เป็นกรุป แล้ว G เป็นผลคูณภายนอกของ $G_1, G_2, ..., G_n$ ก็ต่อเมื่อ มีกรุปย่อยปกติ $N_1, N_2, ..., N_n$ ของ G ซึ่ง $G_i \cong N_i$ สำหรับแต่ละ $1 \le i \le n$ และ G เป็นผลคูณภายในของ $N_1, N_2, ..., N_n$

บทพิสูจน์ ให้ $G, G_1, G_2, ..., G_n$ เป็นกรุป

$(\rightarrow)$ ให้ G เป็นผลคูณภายนอกของ $G_1, G_2, ..., G_n$ แล้วจะมี $\alpha : G \rightarrow G_1 \times G_2 \times ... \times G_n$ เป็นสมสัณฐาน และโดยทฤษฎีบท 4.1.4 จะมี $\overline{G_i}$ เป็นกรุปย่อยปกติของ $G_1 \times G_2 \times ... \times G_n$ ซึ่ง $\overline{G_i} \cong G_i$ สำหรับแต่ละ $1 \le i \le n$ และเพราะอิมเมจผกผันภายใต้สาทิสสัณฐานของกรุปย่อยปกติเป็นกรุปย่อยปกติ เราจะได้ว่า $\alpha^{-1}(\overline{G_i})$ เป็นกรุปย่อยปกติของ G สำหรับแต่ละ $1 \le i \le n$

สำหรับแต่ละ $1 \le i \le n$ ให้ $N_i = \alpha^{-1}(\overline{G_i})$ แล้ว $\alpha(N_i) = \overline{G_i} \cong G_i$ และจะได้ $N_i \cong \alpha(N_i) = \overline{G_i} \cong G_i$ ดังนั้น $G_i \cong N_i$ สำหรับแต่ละ $1 \le i \le n$

ต่อไปจะแสดงว่า G เป็นผลคูณภายในของ $N_1, N_2, ..., N_n$

1. ให้ $g \in G$ แล้ว $\alpha(g) \in G_1 \times G_2 \times ... \times G_n$ และโดยทฤษฎีบท 4.1.4(3) จะมี $\overline{g_i} \in \overline{G_i}$ สำหรับแต่ละ $1 \le i \le n$ ที่ทำให้ $\alpha(g) = \overline{g_1}\overline{g_2}...\overline{g_n}$ แต่ $\overline{g_i} \in \overline{G_i} = \alpha(N_i)$ สำหรับแต่ละ $1 \le i \le n$ ดังนั้นจะมี $x_i \in N_i$ ซึ่ง $\overline{g_i} = \alpha(x_i)$ สำหรับทุกๆ $1 \le i \le n$ ทำให้ได้ $\alpha(g) = \overline{g_1}\overline{g_2}...\overline{g_n} = \alpha(x_1)\alpha(x_2)...\alpha(x_n)$ เพราะว่า α เป็นสาทิสสัณฐาน ดังนั้น $\alpha(g) = \alpha(x_1 x_2 ... x_n)$ และเพราะ α เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น $g = x_1 x_2 ... x_n$ เพราะฉะนั้น $G = N_1 N_2 ... N_n$

2. ให้ $1 \le i \le n$ และให้ $y \in N_i \cap (N_1 N_2 ... N_{i-1} N_{i+1} ... N_n)$ แล้ว $y \in N_i$ และ $y \in N_1 N_2 ... N_{i-1} N_{i+1} ... N_n$ เพราะว่า $y \in N_i$ แล้วจะมี $x_i \in N_i$ ที่ทำให้ $y = x_i$ ดังนั้น $\alpha(y) = \alpha(x_i) = \overline{g_i}$ เพราะฉะนั้น $\alpha(y) \in \overline{G_i}$ และเพราะว่า $y \in N_1 N_2 ... N_{i-1} N_{i+1} ... N_n$ แล้วจะมี $x_j \in N_j$ สำหรับ $1 \le j \ne i \le n$ ที่ทำให้ $y = x_1 x_2 ... x_{i-1} x_{i+1} ... x_n$ ดังนั้น

$$\begin{aligned}\alpha(y) &= \alpha(x_1 x_2 ... x_{i-1} x_{i+1} ... x_n) \\ &= \alpha(x_1)\alpha(x_2)...\alpha(x_{i-1})\alpha(x_{i+1})...\alpha(x_n) \\ &= \overline{g_1}\overline{g_2}...\overline{g_{i-1}}\overline{g_{i+1}}...\overline{g_n}\end{aligned}$$

$\in \overline{G_1}\,\overline{G_2}...\overline{G_{i-1}}\,\overline{G_{i+1}}...\overline{G_n}$

ดังนั้น $\alpha(y) \in \overline{G_i} \cap \left(\overline{G_1}\,\overline{G_2}...\overline{G_{i-1}}\,\overline{G_{i+1}}...\overline{G_n}\right) = \{(e_1, e_2, ..., e_n)\}$ โดยที่ $e_i \in G_i$ สำหรับ $1 \le i \le n$ เพราะฉะนั้น $\alpha(y) = (e_1, e_2, ..., e_n)$ เป็นเอกลักษณ์ใน $G_1 \times G_2 \times ... \times G_n$ ทำให้ได้ $\alpha(y) = \alpha(e)$ แต่ α เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น $y = e$

ในทางกลับกัน เพราะว่า $N_1, N_2, ..., N_n$ เป็นกรุปย่อยปกติของ G ดังนั้น $N_1N_2...N_{i-1}N_{i+1}...N_n$ เป็นกรุปย่อยของ G ทำให้ได้ $e \in N_i$ และ $e \in N_1N_2...N_{i-1}N_{i+1}...N_n$ เพราะฉะนั้น $N_i \cap (N_1N_2...N_{i-1}N_{i+1}...N_n) = \{e\}$ ดังนั้น G เป็นผลคูณภายในของ $N_1, N_2, ..., N_n$

$(\leftarrow)$ ให้ $N_1, N_2, ..., N_n$ เป็นกรุปย่อยปกติของ G ซึ่ง $G_i \cong N_i$ โดยสาทิสสัณฐาน α_i สำหรับแต่ละ $1 \le i \le n$ และให้ G เป็นผลคูณภายในของ $N_1, N_2, ..., N_n$ จะแสดงว่า G เป็นผลคูณภายนอกของ $G_1, G_2, ..., G_n$ นั่นคือจะแสดงว่า $G \cong G_1 \times G_2 \times ... \times G_n$

ให้ $\alpha : G \to G_1 \times G_2 \times ... \times G_n$ นิยามโดย $\alpha(g) = (g_1, g_2, ..., g_n)$ สำหรับแต่ละ $g \in G$ โดยที่ $g = x_1x_2...x_n$ ซึ่ง $x_i \in N_i$ และ $\alpha_i(x_i) = g_i$ ทุกๆ $1 \le i \le n$

1. ให้ $g, h \in G$ ซึ่ง $g = h$ เมื่อ $g = x_1x_2...x_n$ โดยที่ $x_i \in N_i$ และ $\alpha_i(x_i) = g_i$ ทุกๆ $1 \le i \le n$ และ $h = y_1y_2...y_n$ โดยที่ $y_i \in N_i$ และ $\alpha_i(y_i) = h_i$ ทุกๆ $1 \le i \le n$ แล้ว $g = x_1x_2...x_n = h = y_1y_2...y_n$ จากทฤษฎีบท 4.1.7 จะได้ว่า $x_i = y_i$ ทุกๆ $1 \le i \le n$

แล้ว
$$\begin{aligned}\alpha(g) &= \alpha(x_1x_2...x_n)\\ &= (\alpha_1(x_1), \alpha_2(x_2), ..., \alpha_n(x_n))\\ &= (\alpha_1(y_1), \alpha_2(y_2), ..., \alpha_n(y_n))\\ &= \alpha(y_1y_2...y_n)\\ &= \alpha(h)\end{aligned}$$

เพราะฉะนั้น α เป็นฟังก์ชัน

2. ให้ $g, h \in G$ เมื่อ $g = x_1x_2...x_n$ โดยที่ $x_i \in N_i$ และ $\alpha_i(x_i) = g_i$ ทุกๆ $1 \le i \le n$ และ $h = y_1y_2...y_n$ โดยที่ $y_i \in N_i$ และ $\alpha_i(y_i) = h_i$ ทุกๆ $1 \le i \le n$

แล้ว
$$\begin{aligned}\alpha(gh) &= \alpha(x_1x_2...x_ny_1y_2...y_n)\\ &= \alpha(x_1y_1x_2y_2...x_ny_n)\\ &= (\alpha_1(x_1y_1), \alpha_2(x_2y_2), ..., \alpha_n(x_ny_n))\\ &= (\alpha_1(x_1)\alpha_1(y_1), \alpha_2(x_2)\alpha_2(y_2), ..., \alpha_n(x_n)\alpha_n(y_n))\\ &= (x_1y_1, x_2y_2, ..., x_ny_n)\end{aligned}$$

และ $\alpha(g)\alpha(h)=(x_1,x_2,...,x_n)(y_1,y_2,...,y_n)=(x_1y_1,x_2y_2,...,x_ny_n)$
ดังนั้น α เป็นสาทิสสัณฐาน
3. ให้ $g,h\in G$ ซึ่ง $\alpha(g)=\alpha(h)$ เมื่อ $g=x_1x_2...x_n$ โดยที่ $x_i\in N_i$ และ $\alpha_i(x_i)=g_i$ ทุกๆ $1\le i\le n$ และ $h=y_1y_2...y_n$ โดยที่ $y_i\in N_i$ และ $\alpha_i(y_i)=h_i$ ทุกๆ $1\le i\le n$ แล้ว $\alpha_i(x_i)=\alpha_i(y_i)$ ทุกๆ $1\le i\le n$ ทำให้ $x_i=y_i$ ทุกๆ $1\le i\le n$ จะได้ $g=h$ เพราะฉะนั้น α เป็นฟังก์ชันหนึ่งต่อหนึ่ง

4. ให้ $(g_1,g_2,...,g_n)\in G_1\times G_2\times...\times G_n$ แล้ว $g_i\in G_i$ ทำให้ $\alpha_i(g_i)=x_i\in N_i$ สำหรับแต่ละ $1\le i\le n$ เลือก $g=x_1x_2...x_n$ แล้ว

$$\alpha(g)=\alpha(x_1x_2...x_n)=(\alpha_1(x_1),\alpha_2(x_2),...,\alpha_n(x_n))=(g_1,g_2,...,g_n)$$

ดังนั้น α เป็นฟังก์ชันทั่วถึง
เพราะฉะนั้น α เป็นสาทิสสัณฐาน ดังนั้น $G\cong G_1\times G_2\times...\times G_n$ ∎

4.1.9 **ทฤษฎีบท** ให้ G เป็นกรุปและให้ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยของ G ซึ่ง G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$ ถ้า $N_1, N_2, ..., N_n$ เป็นกรุปซึ่ง $G_i\cong N_i$ สำหรับแต่ละ $i=1,2,...,n$ และ N เป็นผลคูณภายนอกของ $N_1, N_2, ..., N_n$ แล้ว $G\cong N$

บทพิสูจน์ ให้ G เป็นกรุปและให้ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยของ G ซึ่ง G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$ และให้ $N_1, N_2, ..., N_n$ เป็นกรุปซึ่ง $G_i\cong N_i$ สำหรับแต่ละ $i=1,2,...,n$ และ N เป็นผลคูณภายนอกของ $N_1, N_2, ..., N_n$

ให้ $f_i:N_i\to G_i$ เป็นสมสัณฐานจาก N_i ไปยัง G_i และให้ $f:N\to G$ นิยามโดย

$$f((x_1,x_2,...,x_n))=f_1(x_1)f_2(x_2)...f_n(x_n)$$

1. ให้ $(x_1,x_2,...,x_n),(y_1,y_2,...,y_n)\in N_1\times N_2\times...\times N_n$ ซึ่ง $(x_1,x_2,...,x_n)=(y_1,y_2,...,y_n)$ แล้ว $x_i=y_i$ สำหรับแต่ละ $i=1,2,...,n$ แล้ว $f((x_1,x_2,...,x_n))=f_1(x_1)f_2(x_2)...f_n(x_n)=f_1(y_1)f_2(y_2)...f_n(y_n)=f(y_1,y_2,...,y_n)$ เพราะฉะนั้น f เป็นฟังก์ชัน
2. ให้ $(x_1,x_2,...,x_n),(y_1,y_2,...,y_n)\in N_1\times N_2\times...\times N_n$ แล้ว

$$\begin{aligned}f((x_1,x_2,...,x_n)(y_1,y_2,...,y_n))&=f((x_1y_1,x_2y_2,...,x_ny_n))\\&=f_1(x_1y_1)f_2(x_2y_2)...f_n(x_ny_n)\\&=f_1(x_1)f_1(y_1)f_2(x_2)f_2(y_2)...f_n(x_n)f_n(y_n)\end{aligned}$$

$$= (f_1(x_1)f_2(x_2)...f_n(x_n))(f_1(y_1)f_2(y_2)...f_n(y_n))$$
$$= f(x_1, x_2, ..., x_n)f(y_1, y_2, ..., y_n)$$

เพราะฉะนั้น f เป็นสาทิสสัณฐาน

3. ให้ $(x_1, x_2, ..., x_n) \in N_1 \times N_2 \times ... \times N_n$ ซึ่ง $f((x_1, x_2, ..., x_n)) = e$ แล้ว $(x_1, x_2, ..., x_n) \in \ker(f)$ แล้ว $f((x_1, x_2, ..., x_n)) = e$ แล้ว $f_1(x_1)f_2(x_2)...f_n(x_n) = e_1e_2...e_n$ จะได้ $f(e_i) = e_i$ สำหรับ $i = 1,2,..., n$ เพราะว่า f_i เป็นฟังก์ชันหนึ่งต่อหนึ่ง ดังนั้น $a_i = e_i$ สำหรับ $i = 1,2,..., n$ แล้ว $(x_1, x_2, ..., x_n) = (e_1, e_2, ..., e_n)$ ซึ่งก็คือเอกลักษณ์ของ N เพราะฉะนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่ง

4. ให้ $g \in G$ ซึ่ง $g = g_1g_2 ...g_n$ โดยที่ $g_i \in G_i$ เนื่องจาก f_i เป็นฟังก์ชันทั่วถึง จะมี $x_i \in N_i$ ซึ่ง $f_i(x_i) = g_i$ แล้ว $(x_1, x_2, ..., x_n) \in N$ ซึ่ง $f((x_1, x_2, ..., x_n)) = f_1(x_1)f_2(x_2)...f_n(x_n)$ $= g_1g_2...g_n = g$ เพราะฉะนั้น f เป็นฟังก์ชันทั่วถึง

เพราะฉะนั้น f เป็นสมสัณฐาน ดังนั้น $G \cong N$ ∎

4.1.10 บทแทรก ให้ G เป็นกรุปและให้ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปกติของ G แล้ว G เป็นผลคูณภายนอกของ $G_1, G_2, ..., G_n$ ก็ต่อเมื่อ G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$

บทพิสูจน์ ให้ G เป็นกรุปและให้ $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปกติของ G

$(\rightarrow)$ ให้ G เป็นผลคูณภายนอกของ $G_1, G_2, ..., G_n$

เราจะแสดงว่า G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$

1. ให้ $g \in G_1 \times G_2 \times ... \times G_n$ โดยทฤษฎีบท 4.1.4(3) จะมี $\overline{g_i} \in \overline{G_i}$ สำหรับแต่ละ $1 \le i \le n$ ที่ทำให้ $g = \overline{g_1}\overline{g_2}...\overline{g_n}$ แต่ $\overline{g_i} \in \overline{G_i}$ และ $\overline{G_i} \cong G_i$ สำหรับแต่ละ $1 \le i \le n$ ทำให้ได้ $g = g_1g_2 ...g_n$ เพราะฉะนั้น $G = G_1 G_2 ...G_n$

2. ให้ $1 \le i \le n$ และให้ $k \in G_i \cap (G_1G_2...G_{i-1}G_{i+1}...G_n)$ แล้ว $k \in G_i$ และ $k \in G_1G_2...G_{i-1}G_{i+1}...G_n$ เพราะว่า $k \in G_i$ ทำให้ได้ว่า $g_i \in G_i$ ที่ทำให้ $k = g_i = \overline{g_i}$ เพราะฉะนั้น $k \in \overline{G_i}$ และเพราะว่า $k \in G_1G_2...G_{i-1}G_{i+1}...G_n$ ดังนั้นจะมี $g_j \in G_j$ สำหรับ $1 \le i \ne j \le n$ ที่ทำให้ $k = g_1g_2 ...g_{i-1}g_{i+1}... g_n = \overline{g_1}\overline{g_2}...\overline{g_{i-1}}\overline{g_{i+1}}...\overline{g_n}$ เพราะฉะนั้น $k \in \overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}$ เพราะฉะนั้น $k \in \overline{G_i} \cap (\overline{G_1}\overline{G_2}...\overline{G_{i-1}}\overline{G_{i+1}}...\overline{G_n}) = \{(e_1, e_2, ..., e_n)\}$ โดยที่ $e_i \in G_i$ สำหรับ $1 \le i \le n$ เพราะฉะนั้น $k = (e_1, e_2, ..., e_n)$ เป็นเอกลักษณ์ใน $G_1 \times G_2 \times ... \times G_n$ เพราะฉะนั้น $k = e$

ในทางกลับกัน เพราะว่า $G_1, G_2, ..., G_n$ เป็นกรุปย่อยปกติของ G ดังนั้น $k \in G_i \cap (G_1G_2...G_{i-1}G_{i+1}...G_n)$ เป็นกรุปย่อยของ G ทำให้ได้ $e \in G_i$ และ $e \in G_1G_2...G_{i-1}G_{i+1}...G_n$ เพราะฉะนั้น $G_i \cap (G_1G_2...G_{i-1}G_{i+1}...G_n) = e$ ดังนั้น G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$

$(\leftarrow)$ ให้ G เป็นผลคูณภายในของ $G_1, G_2, ..., G_n$ เราจะแสดงว่า G เป็นผลคูณภายนอกของ $G_1, G_2, ..., G_n$ นั่นคือจะแสดงว่า $G = G_1 \times G_2 \times ... \times G_n$

ให้ $g \in G_1\, G_2\, ...G_n$ โดยทฤษฎีบท 4.1.4(1) ทำให้ได้ $g \in \overline{G_1}\,\overline{G_2}...\overline{G_n}$ และ $G_1 \times G_2 \times ... \times G_n = \overline{G_1}\,\overline{G_2}...\overline{G_n}$ ดังนั้น $g \in G_1 \times G_2 \times ... \times G_n$ เพราะฉะนั้น $G = G_1 \times G_2 \times ... \times G_n$ ดังนั้น G เป็นผลคูณภายนอกของ $G_1, G_2, ..., G_n$ ∎

4.2 ทฤษฎีบทของโคชี

ในหัวข้อนี้เราจะศึกษาแอคชันของกรุปบนเซต บทนิยามของ G – เซต และออร์บิท แล้วเราจะประยุกต์แอคชันของกรุปบนเซตในการพิสูจน์ทฤษฎีบทของโคชี

4.2.1 **บทนิยาม** กำหนดให้ X เป็นเซตที่ไม่ใช่เซตว่าง และให้ G เป็นกรุป 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)

4.2.2 **ข้อตกลง** ถ้า $*$ เป็นแอคชันของกรุป G บนเซต X แล้วสำหรับแต่ละ $g \in G$ และ $x \in X$ เราอาจขียน $*(g, x)$ ด้วย gx

4.2.3 **บทนิยาม** ให้ G เป็นกรุปจำกัดและ X เป็น G – เซต สำหรับแต่ละ $a \in X$ นิยาม $G(a) = \{x \in X \mid \text{มี } g \in G \text{ ซึ่ง } x = ga\}$ และเรียก $G(a)$ ว่า **ออร์บิทของ a ใน X ภายใต้ G** (orbit of a in X under G)

4.2.4 **ทฤษฎีบท** ให้ G เป็นกรุปจำกัดและ X เป็น G – เซต ที่เป็นเซตจำกัด และ $a \in X$ แล้ว

1. $G_a = \{g \in G \mid ga = a\}$ เป็นกรุปย่อยของ G

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

บทพิสูจน์ ให้ $a \in X$

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

เนื่องจาก $a = ea = \left(g_1^{-1} g_1\right)a = g_1^{-1}(g_1 a) = g_1^{-1} a$ แสดงว่า $g_1^{-1} \in G_a$ เพราะฉะนั้น G_a เป็นกรุปย่อยของ G

2. ให้ $H = \{gG_a \mid g \in G\}$ และสังเกตว่าถ้า $x \in G(a)$ แล้วจะมี $g \in G$ ที่ทำให้ $x = ga$

ต่อไปให้ $\varphi = \{(x, gG_a) \in G(a) \times H \mid x = ga\}$ สมมติมี $g_1, g_2 \in G$ ซึ่ง $g_1 a = g_2 a$ ดังนั้น $a = \left(g_1^{-1} g_2\right)a$ ซึ่งแสดงว่า $g_1^{-1} g_2 \in G_a$ แล้ว $g_1 G_a = g_2 G_a$ ฉะนั้น $\varphi(x_1) = \varphi(x_2)$ เพราะฉะนั้น φ เป็นฟังก์ชัน ต่อไปจะแสดงว่า φ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง ให้ $x_1, x_2 \in G_a$ โดยที่ $g_1 G_a = g_2 G_a$ เมื่อ $x_1 = g_1 a$ และ $x_2 = g_2 a$ แล้ว $g_1^{-1} g_2 \in G_a$ ทำให้ได้ $a = \left(g_1^{-1} g_2\right)a = g_1^{-1}(g_2 a)$ ดังนั้น $g_1 a = g_2 a$ นั่นคือ $x_1 = x_2$

สุดท้ายให้ $gG_a \in H$ และเลือก $x = ga$ ดังนั้นมี $x = ga \in G(a)$ ซึ่ง $\varphi(x) = gG_a$ เพราะฉะนั้น φ เป็นฟังก์ชันไปบน H แสดงว่า φ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก $G(a)$ ไปบนเซตของโคเซตซ้าย H ของ G_a ใน G เพราะฉะนั้น $|G(a)| = [G : G_a]$ ∎

จากบทนิยาม 4.2.3 สำหรับแต่ละ $a \in X$ เราจะเขียนออร์บิทของ a ใน X ด้วย $G(a) = \{ga \mid g \in G\}$ และแต่ละสมาชิกของ X จะเป็นสมาชิกของออร์บิทใดออร์บิทหนึ่งเพียงออร์บิทเดียว ดังนั้นถ้ามีออร์บิทใน X ภายใต้ G จำนวน r เซต และสำหรับแต่ละ $i \in \{1, 2, ..., r\}$ เลือก a_i เพียงตัวเดียวจากออร์บิท $G(a_i)$ แล้ว

$$|X| = \sum_{i=1}^{r} |G(a_i)| \qquad ...(4.2.1)$$

ถ้าเรานิยามเซตย่อย 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 $G(a_{s+1})$, $G(a_{s+2})$, ..., $G(a_r)$ เป็นออร์บิทใน X ที่ประกอบด้วยสมาชิกมากกว่าหนึ่งตัว จะได้ $|X_G| = s$ และสามารถเขียน(4.2.1) ได้ใหม่ดังนี้

$$|X| = |X_G| + \sum_{i=s+1}^{r} |G(a_i)| \qquad \text{...(4.2.2)}$$

4.2.5 **ทฤษฎีบท** ให้ p เป็นจำนวนเฉพาะและ G เป็นกรุปขนาด p^n เมื่อ n เป็นจำนวนเต็มที่ไม่ใช่จำนวนเต็มลบ ถ้า X เป็น $G-$เซต ที่เป็นเซตจำกัด แล้ว $|X| \equiv |X_G| \pmod{p}$

บทพิสูจน์ ให้ X เป็น $G-$เซต ที่เป็นเซตจำกัด แล้ว X สอดคล้องกับเงื่อนไข (4.2.2) นั่นคือ $|X| = |X_G| + \sum_{i=s+1}^{r} |G(a_i)|$ แล้วโดยทฤษฎีบท 4.2.4 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 $|X| \equiv |X_G| \pmod{p}$ ∎

4.2.6 **บทนิยาม** ให้ G เป็นกรุป และ p เป็นจำนวนเฉพาะ เรากล่าวว่า G เป็น $p-$**กรุป** (p-group) ถ้าสำหรับแต่ละ $g \in G$ ที่ $g \neq e$ จะมีจำนวนเต็มบวก n ซึ่ง $o(g) = p^n$ (นั่นคืออันดับของแต่ละสมาชิกใน G เป็นจำนวนในรูปกำลังของ p)

4.2.7 **บทนิยาม** ให้ G เป็นกรุป และ H เป็นกรุปย่อยของ G เรากล่าวว่า H เป็น $p-$**กรุปย่อย** (p-subgroup) ของ G ถ้า H เป็น $p-$กรุป

4.2.8 **ทฤษฎีบทของโคชี** (Cauchy's Theorem)

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

บทพิสูจน์ ให้ $X = \{(g_1, g_2, ..., g_p) \in G^p \mid g_i \in G \text{ และ } g_1 g_2 ... g_p = e\}$ เราจะพิสูจน์ว่า p เป็นตัวหารของ $|X|$

ให้ $(g_1, g_2, ..., g_p) \in X$ แล้ว $g_1 g_2 ... g_p = e$ ดังนั้น $g_p = (g_1 g_2 ... g_{p-1})^{-1}$ ในทางกลับกัน ถ้า $g_1, g_2, ..., g_{p-1} \in G$ และเลือก $g_p = (g_1 g_2 ... g_{p-1})^{-1}$ แล้ว $g_1 g_2 ... g_p = e$ 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 $(g_1, g_2, ..., g_p) \in X$ และ $\sigma \in S_p$ โดย

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

จะแสดงว่า * เป็นแอคชันของ S_p บน X ดังนี้

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

$$*(1, (g_1, g_2, ..., g_p)) = (g_{(1)(1)}, g_{(1)(2)}, ..., g_{(1)(p)})$$
$$= (g_1, g_2, ..., g_p)$$

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

$$*(\sigma_1\sigma_2, (g_1, g_2, ..., g_p)) = (g_{\sigma_1\sigma_2(1)}, g_{\sigma_1\sigma_2(2)}, ..., g_{\sigma_1\sigma_2(p)})$$
$$= (g_{\sigma_1(\sigma_2(1))}, g_{\sigma_1(\sigma_2(2))}, ..., g_{\sigma_1(\sigma_2(p))})$$
$$= *(\sigma_1, (g_{\sigma_2(1)}, g_{\sigma_2(2)}, ..., g_{\sigma_2(p)},))$$
$$= *(\sigma_1, *(\sigma_2, (g_1, g_2, ..., g_p)))$$

จาก 1. และ 2. จะได้ว่า * เป็นแอคชัน

ให้ $\sigma = (1\ 2\ ...\ p) \in S_p$ แล้ว $o(\sigma) = p$ และพิจารณายูเนียนของออร์บิท

$$X_{\langle\sigma\rangle} = \{ (g_1, g_2, ..., g_p) \in X \mid \sigma(g_1, g_2, ..., g_p) = (g_1, g_2, ..., g_p) \}$$

แล้วโดยทฤษฎีบท 4.2.5 จะได้ $|X| \equiv |X_{\langle\sigma\rangle}| \pmod p$ แต่ p เป็นตัวหารของ $|X|$ ดังนั้น p เป็นตัวหารของ $|X_{\langle\sigma\rangle}|$ ด้วย และเนื่องจาก $(e_1, e_2, ..., e_p) \in X_{\langle\sigma\rangle}$ ดังนั้น $X_{\langle\sigma\rangle} \neq \varnothing$ แสดงว่า $|X_{\langle\sigma\rangle}| \geq p$

ให้ $(g_1, g_2, ..., g_p) \in X_{\langle\sigma\rangle}$ ที่ $g_k \neq e$ สำหรับ $1 \leq k \leq p$ แล้ว $\sigma(g_1, g_2, ..., g_p) = (g_1, g_2, ..., g_p)$ แต่ $\sigma(g_1, g_2, ..., g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, ..., g_{\sigma(p)}) = (g_2, g_3, ..., g_p, g_1)$ แสดงว่า $g_1 = g_2 = ... = g_p$

ให้ $a = g_1 = g_2 = ... = g_p$ จะได้ $g_1g_2...g_p = a^p = e$ เพราะฉะนั้น $o(a) = p$ ∎

4.2.9 **บทแทรก** ให้ G เป็นกรุป และ p เป็นจำนวนเฉพาะ แล้ว G เป็น $p-$กรุป ก็ต่อเมื่อ มี n เป็นจำนวนเต็มบวก ซึ่ง $|G| = p^n$

บทพิสูจน์ ให้ G เป็น $p-$กรุป สมมติมีจำนวนเฉพาะ q ที่เป็นตัวหารของ $|G|$ ที่ $q \neq p$ แล้วโดยทฤษฎีบทของโคชี จะมี $a \in G$ ซึ่ง $o(a) = q$ แต่เนื่องจาก G เป็น $p-$กรุป แสดงว่ามี k เป็นจำนวนเต็มบวกซึ่ง $o(a) = p^k$ ทำให้ได้ $q = p^k$ เกิดข้อขัดแย้งกับ q เป็นจำนวนเฉพาะดังนั้น

$q = p$ นั่นคือ มีจำนวนเฉพาะ p เพียงหนึ่งเดียวที่เป็นตัวหารของ $|G|$ ดังนั้นจะมี n เป็นจำนวนเต็มบวก ซึ่ง $|G| = p^n$

ในทางกลับกันให้ n เป็นจำนวนเต็มบวก ซึ่ง $|G| = p^n$ และให้ $g \in G$ เนื่องจาก $o(g)$ เป็นตัวหารของ $|G|$ ดังนั้น $o(g)$ เป็นตัวหารของ p^n นั่นคือจะมีจำนวนเต็ม k ซึ่ง $0 \le k \le n$ ที่ทำให้ $o(g) = p^k$ เพราะฉะนั้น G เป็น $p-$กรุป ∎

4.2.10 **ทฤษฎีบท** ให้ p เป็นจำนวนเฉพาะ และ G เป็นกรุปจำกัด ถ้า H เป็น $p-$กรุปย่อยของ G แล้ว $[N[H]:H] \equiv [G:H] \pmod p$

บทพิสูจน์ ให้ $A = \{gH \mid g \in G\}$ แล้ว $|A| = [G:H]$ และนิยาม $\varphi : H \times A \to A$ โดย

$$\varphi(h, gH) = (hg)H \text{ สำหรับทุกๆ } h \in H \text{ และ } g \in G$$

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

ต่อไปจะแสดงว่า A เป็น $H-$เซต ดังนี้

1. ให้ $g \in G$ แล้ว $\varphi(e, gH) = (eg)H = gH$

และ 2. ให้ $h_1, h_2 \in H$ และ $gH \in A$ 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 A

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

ให้ $gH \in A_H$ แล้ว $gH \in A$ และ $gH = h(gH)$ สำหรับทุกๆ $h \in H$ เราจะแสดงว่า $gH \in B$ 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 เป็นกรุปย่อยปกติของ G โดยทฤษฎีบท 2.4.4 จะได้ $gHg^{-1} = H$ และได้ว่า $g \in N[H]$ เพราะฉะนั้น $gH \in B$ ทำให้ได้ว่า $A_H \subseteq B$

ในทางกลับกันให้ $gH \in B$ แล้ว $gH \in A$ และ $g \in N[H]$ เราจะแสดงว่า $gH \in A_H$ เนื่องจาก $g \in N[H]$ จะได้ว่า $gHg^{-1} = H$ ดังนั้น H เป็นกรุปย่อยปกติของ G ให้ $h \in H$ แล้ว

$g^{-1}h\left(g^{-1}\right)^{-1}= g^{-1}hg \in H$ ทำให้ได้ $g^{-1}hgH = H$ และได้ว่า $h(gH) = (hg)H = gH$ ดังนั้น $gH \in A_H$ ทำให้ได้ว่า $B \subseteq A_H$

ดังนั้น $A_H = B$ แต่ $|B| = [N[H]: H]$ จะได้ว่า $|A_H| = [N[H]: H]$ และเนื่องจาก H เป็น $p-$กรุปย่อย โดยบทแทรก 4.2.9 จะมี จำนวนเต็มบวก n ซึ่ง $|H| = p^n$ และโดยทฤษฎีบท 4.2.5 จะได้ว่า $|A| \equiv |A_H| \pmod p$ เพราะฉะนั้น $[G : H] \equiv [N[H]: H] \pmod p$ ∎

4.3 ทฤษฎีบทซีโลว์

ในหัวข้อนี้เราจะศึกษาทฤษฎีบทซีโลว์ ซึ่งประกอบด้วย 3 ทฤษฎีบท ซึ่งได้รับการยกย่องว่าเป็นรากฐานของการศึกษากรุปจำกัด

ทฤษฎีบทที่หนึ่งของซีโลว์แสดงว่า บทกลับของลากรองจ์เป็นจริงในกรณีที่ตัวหารของขนาดของกรุปอยู่ในรูปเลขยกกำลังของจำนวนเฉพาะจำนวนหนึ่ง

ทฤษฎีบทที่สองและที่สามของซีโลว์กล่าวถึงการหาจำนวนกรุปย่อยของกรุปจำกัดที่กำหนด นั่นคือ ทฤษฎีบทของซีโลว์ได้แสดงให้เห็นความสัมพันธ์ของขนาดของกรุปที่กำหนดกับลักษณะของ กรุปย่อยที่เกิดขึ้น

4.3.1 ทฤษฎีบทที่หนึ่งของซีโลว์ (The First Sylow's Theorem)

ให้ G เป็นกรุปจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวกและ p เป็นจำนวนเฉพาะซึ่ง $(p,s)=1$ แล้วจะมีกรุปย่อยของ G อันดับ p^k สำหรับแต่ละ k ซึ่ง $1 \le k \le m$ และแต่ละกรุปย่อยอันดับ p^k เมื่อ $k = 1,2,...,m-1$ จะเป็นกรุปย่อยปกติของกรุปย่อยอันดับ p^{k+1} อย่างน้อย 1 กรุปย่อย

บทพิสูจน์ เราจะแสดงโดยอุปนัยเชิงคณิตศาสตร์ว่า G จะมีกรุปย่อยอันดับ p^k สำหรับแต่ละ k ซึ่ง $1 \le k \le m$ อย่างแรกโดยทฤษฎีบทของโคชี จะมี $a \in G$ ซึ่ง $o(a) = p$ แล้ว $\langle a \rangle$ เป็นกรุปย่อยของ G ซึ่ง $|\langle a \rangle| = p$ นั่นคือ G มีกรุบย่อยอันดับ p ต่อไปให้ H เป็นกรุบย่อยของ G ซึ่ง $|H| = p^k$ โดยที่ $1 \le k \le m-1$ แล้ว $m-k>0$ แต่ $[G : H] = \dfrac{|G|}{|H|} = \dfrac{p^m s}{p^k} = p^{m-k}s =$ $p\left(p^{m-k-1}s\right)$ ทำให้ได้ว่า p หาร $[G : H]$ ลงตัว และโดยทฤษฎีบท 4.2.จ เราได้ว่า $[N[H]: H]$ $\equiv [G : H] \pmod p$ แต่ p หาร $[G : H]$ ดังนั้น p หาร $[N[H]: H]$ ลงตัวด้วย เนื่องจาก H เป็น

กรุปย่อยปกติของ $N[H]$ ดังนั้น $N[H]/H$ เป็นกรุปผลหารซึ่ง p เป็นตัวหารของ $\left|N[H]/H\right| = [N[H]:H]$ โดยทฤษฎีบทของโคชีจะได้ว่า $N[H]/H$ มีกรุปย่อย K อันดับ p

เนื่องจาก H เป็นกรุปย่อยปกติของ $N[H]$ ดังนั้นโดยทฤษฎีบท 2.5.11 จะมีฟังก์ชันสมนัยหนึ่งต่อหนึ่งระหว่างเซตของกรุปย่อยของ $N[H]$ ซึ่งมี H เป็นกรุปย่อยกับเซตของกรุปย่อยของ $N[H]$ โดยเฉพาะอย่างยิ่งจะมีกรุปย่อย $S = \eta^{-1}(K)$ ของ $N[H]$ เมื่อ η เป็นสาทิสสัณฐานธรรมชาติจาก $N[H]$ ไปยัง $N[H]/H$ ซึ่ง $H \subseteq S$ และ $S/H = K$ จะได้ $|S| = \left|S/H\right||H| = |K||H| = pp^k = p^{k+1}$

สุดท้ายเราจะแสดงว่าแต่ละกรุปย่อยอันดับ p^k ซึ่ง $k = 1, 2, ..., m-1$ จะเป็นกรุปย่อยปกติของกรุปย่อยอันดับ p^{k+1} อย่างน้อย 1 กรุปย่อย

ให้ $a \in S$ เนื่องจาก $S \subseteq N[H]$ ดังนั้น $a \in N[H]$ ทำให้ได้ว่า $aHa^{-1} = H$ ดังนั้น H เป็นกรุปย่อยปกติอันดับ p^k ของ S ∎

4.3.2 **บทนิยาม** ให้ G เป็นกรุปจำกัด และ p เป็นจำนวนเฉพาะ เรากล่าวว่า H เป็น**กรุปย่อย $p-$ซีโลว์** (p-Sylow subgroup) ของ G ถ้า H เป็น **$p-$กรุปย่อยใหญ่สุดเฉพาะกลุ่ม** (maximal p-subgroup) ของ G (นั่นคือ ถ้า K เป็น $p-$กรุปย่อยของ G ซึ่ง $K \supseteq H$ แล้ว $K = H$)

ให้ G เป็นกรุปจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะซึ่ง $(p,s) = 1$ ทฤษฎีบทที่หนึ่งของซีโลว์ได้แสดงว่ากรุปย่อย $p-$ซีโลว์ ของ G เป็นกรุปย่อยอันดับ p^m ทฤษฎีบทต่อไปจะแสดงว่าถ้า H เป็นกรุปย่อย $p-$ซีโลว์ ของ G แล้วทุกๆ สังยุคของ H จะเป็นกรุปย่อย $p-$ซีโลว์ ของ G ด้วย

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

บทพิสูจน์ ให้ H เป็นกรุปย่อย $p-$ซีโลว์ ของ G โดยทฤษฎีบท 4.3.1 จะได้ว่า H มีอันดับ p^m ต่อไปให้ $g \in G$ เราจะแสดงว่า $\left|gHg^{-1}\right| = |H|$ ด้วยการนิยาม $\alpha : H \to gHg^{-1}$ โดย

$\alpha(h)=ghg^{-1}$ สำหรับทุก $h\in H$ แล้วจะแสดงว่า α เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก H ไปบน gHg^{-1}

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

ให้ $k\in gHg^{-1}$ เลือก $h=g^{-1}kg$ ทำให้ได้ $\alpha(h)=\alpha\left(g^{-1}kg\right)=g\left(g^{-1}kg\right)g^{-1}=k$ เพราะฉะนั้น α เป็นฟังก์ชันไปทั่วถึง gHg^{-1}

เนื่องจาก α เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก H ไปทั่วถึง gHg^{-1} ดังนั้น $\left|gHg^{-1}\right|=|H|$ ทำให้ได้ $\left|gHg^{-1}\right|=p^m$ ให้ $gh_1g^{-1},gh_2g^{-1}\in gHg^{-1}$ แล้วจะได้ว่า $\left(gh_1g^{-1}\right)\left(gh_2g^{-1}\right)^{-1}$ $=\left(gh_1g^{-1}\right)\left(gh_2^{-1}g^{-1}\right)=gh_1\left(g^{-1}g\right)h_2^{-1}g^{-1}=g\left(h_1h_2^{-1}\right)g^{-1}\in gHg^{-1}$ ดังนั้น gHg^{-1} เป็นกรุปย่อยของ G เนื่องจาก gHg^{-1} เป็นกรุปย่อยอันดับ p^m ของ G ดังนั้น gHg^{-1} เป็นกรุปย่อย $p-$ซีโลว์ ของ G ∎

4.3.4 **ทฤษฎีบทที่สองของซีโลว์** (The Second Sylow's Theorem)

ให้ G เป็นกรุปจำกัดอันดับ $n=p^ms$ โดยที่ m และ s เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะซึ่ง $(p,s)=1$ แล้วกรุปย่อย $p-$ซีโลว์ ของ G เป็นสังยุคของกันและกัน

บทพิสูจน์ ให้ H_1 และ H_2 เป็นกรุปย่อย $p-$ซีโลว์ ของ G แล้ว $|H_1|=|H_2|=p^m$ ให้ $S=\left\{xH_1\,\middle|\,x\in G\right\}$ 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 $x_1H_1=x_2H_2$ 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 $\varphi(y_1y_2,xH_1)=((y_1y_2)x)H_1=$ $(y_1(y_2x))H_1=\varphi(y_1,(y_2x)H_1)=\varphi(y_1,\varphi(y_2,xH_1))$

จากข้อหนึ่งและข้อสองจะได้ว่า φ เป็นแอคชันของ H_2 บน S ฉะนั้น S เป็น H_2-เซต

ให้ $x \in H_1$ แล้วโดยนิยามของ X_G 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 4.2.5 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 $x^{-1}H_2x$ เป็นกรุปย่อยของ H_1 แต่ $|H_1| = |H_2| = |x^{-1}H_2x|$ เราจะได้ $H_1 = x^{-1}H_2x$ ∎

4.3.5 **บทแทรก** ให้ G เป็นกรุปจำกัดอันดับ $n = p^m s$ โดยที่ m และ s เป็นจำนวนเต็มบวก และ p เป็นจำนวนเฉพาะซึ่ง $(p,s) = 1$ ถ้า K เป็นกรุปย่อย $p-$ซีโลว์ ของ G แล้ว K เป็นกรุปย่อยปกติของ G ก็ต่อเมื่อ K เป็นกรุปย่อย $p-$ซีโลว์เพียงกรุปเดียวของ G

บทพิสูจน์ สมมติว่า K เป็นกรุปย่อยปกติของ G และให้ P เป็นกรุปย่อย $p-$ซีโลว์ ของ G แล้วโดยทฤษฎีบทที่สองของซีโลว์ จะมี $x \in G$ ซึ่ง $P = x^{-1}Kx$ แต่ K เป็นกรุปย่อยปกติของ G จะได้ว่า $P = x^{-1}Kx = K$ ดังนั้น K เป็นกรุปย่อย $p-$ซีโลว์เพียงกรุปเดียวของ G

ในทางกลับกัน สมมติว่า K เป็นกรุปย่อย $p-$ซีโลว์เพียงกรุปเดียวของ G แล้ว $x^{-1}Kx = K$ สำหรับทุกๆ $x \in G$ ดังนั้น K เป็นกรุปย่อยปกติของ G ∎

4.3.6 **ทฤษฎีบทที่สามของซีโลว์** (The Third Sylow's Theorem)

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

บทพิสูจน์ ให้ H เป็นกรุปย่อย $p-$ซีโลว์ ของ G แล้ว $|H| = p^m$ และให้ S เป็นเซตของกรุปย่อย $p-$ซีโลว์ทั้งหมดของ G แล้ว $n_p = |S|$

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

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

และ 2. ให้ $T \in S$ แล้ว $x_1, x_2 \in H$ แล้ว $\varphi(x_1x_2, T) = (x_1x_2)T(x_1x_2)^{-1} = (x_1x_2)T\left(x_1^{-1}x_2^{-1}\right) = \varphi\left(x_1, x_2Tx_2^{-1}\right) = \varphi(x_1, \varphi(x_2, T))$

จากทั้งข้อ 1. และ 2. จะได้ว่า φ เป็นแอคชันของ H บน S ฉะนั้น S เป็น $H-$เซต โดยนิยามของ X_G 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 4.2.5 ว่า $|S_H| \equiv |S| \pmod p$ ให้ $T \in S_H$ แล้ว $xTx^{-1} = T$ สำหรับทุกๆ $x \in H$ ดังนั้น H เป็นกรุปย่อยของ $N[T]$ และแน่นอนว่า T เป็นกรุปย่อยของ $N[T]$ จึงได้ว่า H และ T ต่างเป็นกรุปย่อย $p-$ซีโลว์ของ $N[T]$ ดังนั้นโดยทฤษฎีบทที่สองของซีโลว์ จะมี $x \in N[T]$ ซึ่ง $H = x^{-1}Tx$ แต่ T เป็นกรุปย่อยปกติของ $N[T]$ ทำให้ได้ว่า $Tx = xT$ และได้ $H = x^{-1}Tx = x^{-1}xT = T$ ดังนั้น $S_H = \{T\}$ นั่นคือ $|S_H| = 1$ และโดยทฤษฎีบท 4.2.5 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 กรุปย่อย $p-$ซีโลว์ ของ G เป็นสังยุคซึ่งกันและกัน จึงทำให้มีออร์บิทใน S ภายใต้ G เพียง 1 ออร์บิทเท่านั้น

ให้ $T \in S$ แล้ว $G_H = \left\{g \in G \;\middle|\; gHg^{-1} = H\right\} = N[H]$ โดยทฤษฎีบท 4.2.4 จะได้ n_p เท่ากับขนาดของออร์บิทใน $H = [G : G_H]$ เนื่องจาก $|G| = |G_H|[G : G_H]$ เพราะฉะนั้น $[G : G_H]$ หาร $|G|$ ลงตัว นั่นคือ n_p หาร $|G|$ ลงตัว ∎

4.4 กรุปอาบีเลียนขนาดจำกัด

ในหัวข้อนี้จะศึกษาเกี่ยวกับโครงสร้างของกรุปอาบีเลียนขนาดจำกัด และแสดงว่ากรุปอาบีเลียนขนาดจำกัดเป็นผลคูณตรงของกรุปวัฏจักร

4.4.1 ทฤษฎีบท ถ้า G เป็นกรุปอาบีเลียนขนาดจำกัดแล้ว G เป็นสมสัณฐานกันกับผลคูณตรงของกรุปย่อยซีโลว์ของ G

บทพิสูจน์ ให้ G เป็นกรุปอาบีเลียนขนาดจำกัด และให้ $|G| = p_1^{k1}\ p_2^{k2}...p_m^{km}$ เมื่อ m เป็นจำนวนนับ และ k_i เป็นจำนวนเต็มบวก และแต่ละ p_i เป็นจำนวนเฉพาะที่แตกต่างกันทั้งหมด สำหรับ $1 \le i \le m$ แล้ว $(p_i, p_j) = 1$ ถ้า $1 \le i \ne j \le m$ ทำให้ได้โดยทฤษฎีบท 4.3.1 ว่ามีกรุปย่อย p_i – ซีโลว์ของ G ที่มีอันดับ $p_i^{k_i}$ เมื่อ $1 \le i \le m$ ให้ S_i เป็นกรุปย่อยของ G ซึ่ง $|S_i| = {p_i}^{k_i}$ สำหรับแต่ละ $1 \le i \le m$ แล้วโดยบทแทรก 4.3.5 จะได้ว่า S_i เป็นกรุปย่อย p_i – ซีโลว์เพียงกรุบย่อยเดียว G สำหรับทุก ๆ $1 \le i \le m$ นอกจากนี้ $S_i \cap S_j = \{e\}$

ต่อไปให้ $a_i \in S_i$ และ $a_j \in S_j$ สำหรับแต่ละ $1 \le i, j \le m$ แล้ว $a_i a_j = a_j a_i$ เราจะแสดงว่า $S_i \cap (S_1 S_2 ... S_{i-1} S_{i+1} ... S_m) = \{e\}$ ให้ $a \in S_i \cap (S_1 S_2 ... S_{i-1} S_{i+1} ... S_m)$ แล้ว $a \in S_i$ และ $a \in S_1 S_2 ... S_{i-1} S_{i+1} ... S_m$ ทำให้ได้ว่า $a_i \in S_j$ สำหรับ $1 \le i \ne j \le m$ ซึ่ง $a = a_1 a_2 ... a_{i-1} a_{i+1} ... a_m$ และเพราะว่า $|S_1 S_2 ... S_{i-1} S_{i+1} ... S_m| = p_1^{k1} p_2^{k2} ... p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} ... p_m^{km}$ ดังนั้น $o(a) \mid p_1^{k1} p_2^{k2} ... p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} ... p_m^{km}$ แต่ $o(a) \mid p_i^{k_i}$ ดังนั้น $o(a) = 1$ ฉะนั้น $a = e$ ทำให้ได้ $S_i \cap (S_1 S_2 ... S_{i-1} S_{i+1} ... S_m) = \{e\}$

ต่อไปจะแสดงว่า $G = S_1 S_2 ... S_m$ เนื่องจาก $p_i \ne p_j$ สำหรับ $1 \le i \ne j \le m$ และ p_i หาร $|G|$ ลงตัว สำหรับแต่ละ $1 \le i \le m$ และเพราะว่า $S_i \ne S_j$ และ $(|S_i|, |S_j|) = 1$ เมื่อ $1 \le i \ne j \le m$ โดยบทแทรก 2.3.20 จะได้ $|S_1 S_2 ... S_m| = |S_1 \| S_2| ... |S_m| = p_1^{k1} p_2^{k2} ... p_m^{km} = |G|$ และเนื่องจาก $S_1 S_2 ... S_m \subseteq G$ ดังนั้น $G = S_1 S_2 ... S_m$ ฉะนั้น G เป็นผลคูณภายในของ $S_1, S_2, ..., S_m$

แล้วโดยบทแทรกที่ 4.1.10 จะได้ว่า G เป็นผลคูณภายนอกของ $S_1, S_2, ..., S_m$ นั่นคือ $G \cong S_1 \times S_2 \times ... \times S_m$ ∎

ในทฤษฎีบท 4.4.1 เราได้แสดงว่ากรุบอาบีเลียนขนาดจำกัดสมสัณฐานกันกับผลคูณตรงของกรุปย่อย p – ซีโลว์ ต่อไปเราจะแสดงว่าแต่ละกรุปย่อย p – ซีโลว์ สมสัณฐานกันกับผลคูณตรง ของกรุปย่อยวัฏจักร

4.4.2 **ทฤษฎีบท** ให้ G เป็นกรุปอาบีเลียนขนาดจำกัดและเป็น p – กรุป เมื่อ p เป็นจำนวนเฉพาะ แล้วจะมี $a \in G$ และกรุปย่อยแท้ H ของ G ซึ่ง $G \cong \langle a \rangle \times H$

บทพิสูจน์ ให้ p เป็นจำนวนเฉพาะและ G เป็นกรุปอาบีเลียนขนาดจำกัดและเป็น p – กรุป แล้วโดยทฤษฎีบทโคชี จะมี $a \in G$ ซึ่ง $o(a) = p$ ดังนั้นให้ $a \in G$ เป็นสมาชิกที่มีอันดับมากสุดใน

บรรดาเหล่าสมาชิกของ G แล้วจะมีจำนวนเต็มบวก k ซึ่ง $o(a)=p^k$ ถ้า $\langle a\rangle = G$ แล้ว $\langle a\rangle \times \{e\} \cong G = \langle a\rangle\{e\}$ เราจึงพิจารณากรณี ถ้า $\langle a\rangle \subset G$ ให้ $\bar{a} \in G - \langle a\rangle$ และให้ $\overline{A} = \langle \bar{a}\rangle$ แล้ว $\overline{A} \cap \langle a\rangle = \{e\}$ โดย Zorn's Lemma สมมติว่า H เป็นกรุปย่อยใหญ่สุดเฉพาะกลุ่มของ G ซึ่ง $\langle a\rangle \cap H = \{e\}$ เนื่องจาก G เป็นกรุปอาบีเลียน ดังนั้น H เป็นกรุปย่อยปกติ แล้วต้องการแสดงว่า $G = \langle a\rangle H$ โดยสมมติ $G \neq \langle a\rangle H$

ให้ $x \in G - \langle a\rangle H$ เนื่องจาก a เป็นสมาชิกที่มีอันดับมากสุดในบรรดาเหล่าสมาชิกของ G และ $o(a)=p^k$ ดังนั้น $x^{p^k} = e$ ทำให้ได้ $x^{p^k} \in \langle a\rangle H$ ให้ r เป็นจำนวนนับน้อยสุดซึ่ง $x^{p^r} \in \langle a\rangle H$ แล้ว $r \leq k$ ให้ $g = x^{p^{r-1}}$ จะได้ว่า $g \notin \langle a\rangle H$ แต่ $g^p = x^{p^r} \in \langle a\rangle H$ ดังนั้นจะมีจำนวนเต็ม q และ $h \in H$ ซึ่ง $g^p = a^q h$ ทำให้ได้ว่า $e = g^{p^k} = \left(g^p\right)^{p^{k-1}} = \left(a^q h\right)^{p^{k-1}} = a^{qp^{k-1}} h^{p^{k-1}}$ ดังนั้น $a^{qp^{k-1}} = h^{-p^{k-1}} \in H$ เพราะว่า $a^{qp^{k-1}} \in \langle a\rangle$ ฉะนั้น $a^{qp^{k-1}} = \langle a\rangle \cap H = \{e\}$ จะได้ว่า $a^{qp^{k-1}} = e$ ดังนั้น $o(a) \mid qp^{k-1}$ ทำให้ได้ $p^k \mid qp^{k-1}$ ดังนั้น $p \mid q$ ให้ s เป็นจำนวนเต็มซึ่ง $q = ps$ เนื่องจาก $g \notin \langle a\rangle H$ ดังนั้น $ga^{-s} \notin H$ แต่ $\left(ga^{-s}\right)^p = g^p a^{-ps} = g^p a^{-q} = h \in H$ ให้ $K = \left\langle ga^{-s}\right\rangle H$ เนื่องจาก $H \subseteq K$ จะได้ $ga^{-s} \in K$ แต่ $ga^{-s} \notin H$ ดังนั้น $H \neq K$ เนื่องจาก H เป็นกรุปย่อยใหญ่สุดเฉพาะกลุ่มของ G ซึ่ง $\langle a\rangle \cap H = \{e\}$ และ $H \subseteq K$ จึงได้ว่า $K \cap \langle a\rangle \neq \{e\}$

ให้ $e \neq b \in \langle a\rangle \cap K$ แล้วจะมี เป็นจำนวนเต็ม t และ u และให้ $h_1 \in H$ ซึ่ง $b = a^t = \left(ga^{-s}\right)^u h_1$ สมมติ $p \mid u$ แล้วจะมีจำนวนเต็ม v ซึ่ง $u = pv$ และทำให้ได้ $b = \left(ga^{-s}\right)^u h_1 = \left(ga^{-s}\right)^{pv} h_1 = \left(\left(ga^{-s}\right)^p\right)^v h_1$ เพราะว่า $\left(ga^{-s}\right)^p \in H$ จึงได้ว่า $\left(\left(ga^{-s}\right)^p\right)^v h_1 \in H$ ฉะนั้น $b \in H$ เนื่องจาก $b \in \langle a\rangle$ ดังนั้น $b \in \langle a\rangle \cap H = \{e\}$ เกิดข้อขัดแย้งกับ $b \neq e$ เพราะฉะนั้น p ไม่เป็นตัวหารของ u เนื่องจาก p เป็นจำนวนเฉพาะ ดังนั้น $(p, u) = 1$ แล้วจะมีจำนวนเต็ม c และ d ซึ่ง $1 = pc + ud$ ทำให้ได้ว่า $g = g^{pc+ud} = \left(g^p\right)^c \left(g^u\right)^d$ เพราะว่า $g^p \in \langle a\rangle H$ ทำให้ได้ $\left(g^p\right)^c \in \langle a\rangle H$ และเนื่องจาก $a^t = \left(ga^{-s}\right)^u h_1$ ดังนั้น $g^u = a^t a^{su} h_1^{-1} \in \langle a\rangle H$ ทำให้ได้ว่า $g \in \langle a\rangle H$ เกิดข้อขัดแย้งกับที่สมมติว่า $g \notin \langle a\rangle H$ ดังนั้น $G = \langle a\rangle H$ เพราะฉะนั้น G เป็นผลคูณภายในของ $\langle a\rangle$ และ H

โดยทฤษฎีบท 4.1.10 เราได้ว่า G เป็นผลคูณตรงของ $\langle a\rangle$ และ H ดังนั้น $G \cong \langle a\rangle \times H$

∎

4.4.3 บทแทรก ถ้า G เป็นกรุปอาบีเลียนขนาดจำกัดและเป็น $p-$กรุป เมื่อ p เป็นจำนวนเฉพาะ แล้ว G เป็นผลคูณตรงของกรุปย่อยวัฏจักรที่มีอันดับเป็นกำลังของ p

บทพิสูจน์ ให้ G เป็นกรุปอาบีเลียนขนาดจำกัดและเป็น $p-$กรุป เมื่อ p เป็นจำนวนเฉพาะ แล้วจะมีจำนวนเต็มบวก k ซึ่ง $|G|=p^k$ ดังนั้นโดยทฤษฎีบท 4.4.2 จะมี $a\in G$ และมีกรุปย่อย H ของ G ซึ่ง $G\cong\langle a\rangle\times H$ ให้ $a_1\in G$ เป็นสมาชิกที่มีอันดับมากสุดที่ทำให้มี $H_1\leq G$ ซึ่ง $G\cong\langle a_1\rangle\times H_1$ ให้ $o(a_1)=p^{k1}$ เมื่อ k_1 เป็นจำนวนเต็มบวก แล้ว $|H_1|=p^{k-k1}$ ดังนั้น H_1 เป็นกรุปอาบีเลียนขนาดจำกัดและเป็น $p-$กรุป สมมติให้ $a_k\in H_{k-1}$ เป็นสมาชิกที่มีอันดับมากสุดที่ทำให้มี $H_k\leq G$ ซึ่ง $G\cong\langle a_1\rangle\times\langle a_2\rangle\times\ldots\times\langle a_k\rangle\times H_k$ และ $o(a_i)=p^{k_i}$ เมื่อ k_i เป็นจำนวนเต็มบวก ซึ่ง $1\leq i\leq k$ เนื่องจาก $|G|=p^k$ ดังนั้น $|H_k|=p^{k-k_1-\ldots-k_k}$ ทำให้ได้ว่า H_k เป็นกรุปอาบีเลียนขนาดจำกัดและเป็น $p-$กรุป แล้วโดยทฤษฎีบท 4.4.2 ทำให้ได้ว่ามี $a_{k+1}\in H_k$ เป็นสมาชิกที่มีอันดับมากสุดที่ทำให้มี $H_{k+1}\leq H_k$ ซึ่ง $H_k\cong\langle a_{k+1}\rangle\times H_{k+1}$ ดังนั้น $G\cong\langle a_1\rangle\times\langle a_2\rangle\times\ldots\times\langle a_k\rangle\times\langle a_{k+1}\rangle\times H_{k+1}$ โดยอุปนัยเชิงคณิตศาสตร์เราได้ว่า $G\supseteq H_1\supseteq H_2\supseteq\ldots\supseteq\{e\}$ ทำให้ได้ $|G|\geq|H_1|\geq|H_2|\geq\ldots\geq 1$ แต่ $|G|$ เป็นจำนวนจำกัด ดังนั้นจะมีจำนวนเต็มบวก n ซึ่ง $H_n=\{e\}$ และ $a_n\in H_{n-1}$ ดังนั้น $G\cong\langle a_1\rangle\times\langle a_2\rangle\times\ldots\times\langle a_n\rangle\times\{e\}$ เพราะฉะนั้น G เป็นผลคูณตรงของกรุปย่อยวัฏจักรที่มีอันดับเป็นกำลังของ p ∎

ต่อไปเราจะกล่าวทฤษฎีบทหลักมูลของกรุปอาบีเลียนขนาดจำกัดซึ่งเป็นผลโดยตรงของทฤษฎีบท 4.4.1 และบทแทรก 4.4.3

4.4.4 ทฤษฎีบทหลักมูลของกรุปอาบีเลียนขนาดจำกัด (The Fundamental Theorem of Finite Abelian Groups)

ทุกกรุปอาบีเลียนขนาดจำกัดเป็นผลคูณตรงของกรุปวัฏจักรที่มีอันดับเป็นกำลังของจำนวนเฉพาะ

บทที่ 5

กรุปฮามิลทอเนียน

ในการศึกษาสมบัติของกรุปในบทที่ 4 ได้มีการพิสูจน์ว่ากรุปอาบีเลียนสามารถเขียนได้ในรูปผลคูณตรงของกรุปย่อยวัฏจักรและแต่ละกรุปย่อยของกรุปวัฏจักรเป็นกรุปย่อยปกติ แต่กรุปโดยทั่วไปที่ไม่ใช่กรุปอาบีเลียนอาจไม่มีสมบัติเช่นนี้ และการศึกษาลักษณะเฉพาะของกรุปที่ไม่ใช่กรุปอาบีเลียนยังคงเป็นปัญหาเปิดอยู่ อย่างไรก็ตามได้มีการศึกษาเพื่อหาลักษณะเฉพาะสำหรับกรุปนอนอาบีเลียนที่มีสมบัติเช่นเดียวกับกรุปอาบีเลียน นั่นคือกรุปที่มีกรุปย่อยทุกกรุปเป็นกรุปย่อยปกติและเรียกกรุปนั้นว่า กรุปฮามิลทอเนียน ในบทนี้เราศึกษาลักษณะเฉพาะของกรุปฮามิลทอเนียน

5.1 กรุปควอเทอร์เนียน

ให้ $Q = \{1,-1,i,-i,j,-j,k,-k\}$ และนิยามการดำเนินการทวิภาคบน Q คือการคูณ โดยมี 1 เป็นสมาชิกเอกลักษณ์การคูณ และกำหนด $(-1)^2 = 1$ และ $i^2 = j^2 = k^2 = ijk = -1$ แล้วตารางการคูณบน Q แสดงดังตารางข้างล่างนี้

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	I	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	J	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	K	-j	j	i	-i	1	-1

ตาราง 1

จากตารางการคูณของ Q เห็นได้ว่า Q ไม่เป็นกรุปอาบีเลียนเพราะมี $i, j \in Q$ ซึ่ง $ij = k$ และ $ji = -k$ นั่นคือ $ij \neq ji$ หรือ $ij = -ji$

ถ้าแทนสมาชิกของ Q ใหม่โดยให้ $i = a, j = b$ และ $k = ab$ แล้ว $a^2 = -1, a^3 = -a,$ $a^4 = 1$ และจะได้ $b^2 = -1 = a^2, a^2b = b^3 = ba^2,\ b^4 = a^2b^2 = a^4 = 1$ และ $ba = -k = -1ab = a^2ab = a^3b$ ทำให้ได้ตารางการคูณในตัวแปร a และ b แสดงดังตาราง 2 ข้างล่างนี้

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	1	a^3	a^2

ตาราง 2

จะเห็นว่ากรุป Q เป็นกรุปที่ก่อกำเนิดโดยสมาชิก 2 ตัว คือ a และ b ซึ่งมีความสัมพันธ์ $o(a) = 4, a^2 = b^2$ และ $ba = a^3b$

5.1.1 **บทนิยาม** เรียกกรุป G ว่า **กรุปควอเทอร์เนียน** (quaternion group) ถ้า G มีตัวก่อกำเนิด 2 ตัว คือ a และ b ซึ่งมีความสัมพันธ์ $a^4 = 1, a^2 = b^2$ และ $ba = a^3b$

เพื่อความสะดวกถ้า Q เป็นกรุปควอเทอร์เนียนเราจะใช้สัญลักษณ์แทน ดังนี้ $Q = \langle a, b \rangle$

5.2 กรุปฮามิลทอเนียน

ในหัวข้อนี้ศึกษาสมบัติของกรุปฮามิลทอเนียนและพิสูจน์ทฤษฎีบทที่แสดงเงื่อนไขจำเป็นของกรุปฮามิลทอเนียน

5.2.1 **บทนิยาม** เราเรียกกรุปนอนอาบีเลียนที่มีกรุบย่อยทุกกรุบเป็นกรุบย่อยปกติ ว่า**กรุปฮามิลทอเนียน** (Hamiltonion group)

ขอทบทวนว่า สัญลักษณ์ (a,b) หมายถึงคอมมิวเตเตอร์ของ a และ b นั่นคือ $(a,b)=aba^{-1}b^{-1}$

5.2.2 **ทฤษฎีบทประกอบ** ถ้า G เป็นกรุปฮามิลทอเนียน แล้ว $(a,b)\in\langle a\rangle\cap\langle b\rangle$ สำหรับทุกๆ $a, b \in G$

บทพิสูจน์ ให้ $a,b\in G$ ถ้า $ab=ba$ แล้ว $(a,b)=aba^{-1}b^{-1}=e\in\langle a\rangle\cap\langle b\rangle$ เราจึงพิจารณากรณี $ab\neq ba$ ให้ $c=(a,b)=aba^{-1}b^{-1}$ เนื่องจาก G เป็นกรุปฮามิลทอเนียน และ $\langle a\rangle$ กับ $\langle b\rangle$ เป็นกรุบย่อยของ G ดังนั้น $\langle a\rangle$ และ $\langle b\rangle$ เป็นกรุปย่อยปกติของ G ทำให้ได้ว่า $aba^{-1}\in\langle b\rangle$ ดังนั้น $aba^{-1}b^{-1}=\left(aba^{-1}\right)b^{-1}\in\langle b\rangle b^{-1}\subseteq\langle b\rangle$ ซึ่งแสดงว่า $c\in\langle b\rangle$ โดยการพิสูจน์ในทำนองเดียวกัน เราจะได้ว่า $c\in\langle a\rangle$ เพราะฉะนั้น $c\in\langle a\rangle\cap\langle b\rangle$ ∎

สำหรับกรุปนอนอาบีเลียน G ที่ไม่เป็นกรุปฮามิลทอเนียนแล้วอาจจะมี $a,b\in G$ ซึ่ง $ab\neq ba$ ที่ทำให้ $(a,b)\notin\langle a\rangle\cap\langle b\rangle$ ตัวอย่างเช่น กรุป $\left\langle a,b\,\middle|\, a^4=e, b^2=e, ba=a^3b\right\rangle$ เห็นได้ว่า $ab\neq ba$ และ $\langle b\rangle=\{e,b\}$ เป็นกรุปย่อยของ $\left\langle a,b\,\middle|\, a^4=e, b^2=e, ba=a^3b\right\rangle$ เนื่องจาก $(a,b)=aba^{-1}b^{-1}=aba^3b=abba=a^2\notin\langle b\rangle$ ดังนั้น $(a,b)\notin\langle a\rangle\cap\langle b\rangle$

5.2.3 **ทฤษฎีบท** ถ้า H เป็นกรุปย่อยนอนอาบีเลียนของกรุปฮามิลทอเนียน G แล้วจะมีกรุปย่อย Q ของ H ซึ่ง Q เป็นกรุปควอเทอร์เนียน

บทพิสูจน์ ให้ G เป็นกรุปฮามิลทอเนียน และ H เป็นกรุปย่อยนอนอาบีเลียนของ G แล้วจะมี $a,b \in H$ ซึ่ง $ab \neq ba$ และโดยทฤษฎีบทประกอบ 5.2.2 จะได้ว่า $(a,b) \in \langle a \rangle \cap \langle b \rangle$

ให้ $c = (a,b) = aba^{-1}b^{-1}$ แล้ว $c \neq e$ และจะมีจำนวนเต็มที่ไม่เท่ากับศูนย์ r และ s ซึ่ง $a^r = c = b^s$

ให้ Q เป็นกรุปย่อยของ H ซึ่งก่อกำเนิดโดย a และ b นั่นคือ $Q = \langle a,b \rangle$

1. จะแสดงว่า $\langle c \rangle$ เป็นกรุปย่อยแท้ของ $\langle a \rangle$ และของ $\langle b \rangle$

1.1 จะแสดงว่า $c \in Z(Q)$

ให้ $x \in Q$ แล้วจะมีจำนวนเต็มบวก n และจำนวนเต็ม k_i สำหรับ $i = 1,2,3,...,n$ ซึ่ง $x = a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}$ ทำให้ได้ว่า

$$\begin{aligned}
cx &= c\left(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= \left(a^r a^{k1}\right)\left(b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= a^{r+k1}\left(b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= a^{k1+r}\left(b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= a^{k1}\left(a^r b^{k2}\right)\left(a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= a^{k1}\left(b^s b^{k2}\right)\left(a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= a^{k1}b^{s+k2}\left(a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= \left(a^{k1}b^{k2}\right)a^r\left(a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= ..... \\
&= \left(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right)b^s \\
&= \left(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right)c \quad = \quad xc
\end{aligned}$$

ดังนั้น $xc = cx$ สำหรับทุกๆ $x \in Q$ เพราะฉะนั้น $c \in Z(Q)$

1.2 จะแสดงว่า $a \notin \langle c \rangle$ และ $b \notin \langle c \rangle$

สมมติให้ $a \in \langle c \rangle$ แล้วจะมีจำนวนเต็ม k ซึ่ง $a = c^k$ เนื่องจาก $c \in Z(Q)$ ทำให้ได้ว่า $ab = c^k b = c^{k-1}cb = c^{k-1}bc = c^{k-2}cbca = c^{k-3}cbc^2 = ... = cbc^{k-1} = bc^k = ba$ เกิดข้อขัดแย้ง ดังนั้น $a \notin \langle c \rangle$ ในทำนองเดียวกัน เราสามารถสรุปได้ว่า $b \notin \langle c \rangle$ เพราะฉะนั้น $\langle c \rangle$ เป็นกรุปย่อยแท้ของ $\langle a \rangle$ และของ $\langle b \rangle$

2. จะแสดงว่าทุก ๆ สมาชิกของ H มีอันดับจำกัด

2.1 จะแสดงว่า a และ b มีอันดับจำกัด

เพราะว่า $(a,b^s) = ab^s a^{-1}b^{-s} = aa^r a^{-1}\left(b^s\right)^{-1} = a^{r+1}a^{-1}\left(a^r\right)^{-1} = a^{r+1}a^{-(1+r)}$

$= a^0 = e$ และ $c^s = (a,b)^s = (a,b^s)$ จะได้ $c^s = e$ และจากกำหนดให้ $c = a^r$ จะได้ $(a^r)^s = e$ โดยที่ rs เป็นจำนวนเต็มซึ่งไม่เท่ากับศูนย์ แสดงว่ามีจำนวนเต็มบวก m ซึ่ง $a^m = e$ และจากกำหนดให้ $c = b^s$ ทำให้ได้ $(b^s)^s = e$ โดยที่ s^2 เป็นจำนวนเต็มซึ่งไม่เท่ากับศูนย์ แสดงว่ามีจำนวนเต็มบวก n ซึ่ง $b^n = e$ ดังนั้น a และ b ต่างมีอันดับจำกัด

2.2 จะแสดงว่า $h \in H$ ซึ่ง $h \notin \{a, b\}$ มีอันดับจำกัด

ให้ $h \in H$ ถ้า $ha \neq ah$ หรือ $hb \neq bh$ แล้วโดยการพิสูจน์ในทำนองเดียวกับ 2.1 จะได้ว่า h มีอันดับจำกัด ถ้า $ah = ha$ และ $bh = hb$ สมมติว่า $(ah)b = b(ah)$ จะได้ $hab = bha = hba$ ทำให้ได้ $ab = ba$ เกิดข้อขัดแย้ง ดังนั้น $(ah)b \neq b(ah)$ และในทำนองเดียวกันจะได้ $a(bh) \neq (bh)a$ โดยการพิสูจน์ในทำนองเดียวกับ 2.1 จะได้ ah มีอันดับจำกัด ให้ m เป็นจำนวนเต็มบวก ซึ่ง $a^m = e$ และให้ s เป็นจำนวนเต็มบวกซึ่ง $(ah)^s = e$ พิจารณา $h^{ms} = (a^m)h^{ms}$ $= (a^m)^s h^{ms} = (ah)^{ms} = ((ah)^s)^m = e$ ดังนั้น $h^{ms} = e$ ฉะนั้น h มีอันดับจำกัด

ให้ a และ b เป็นสมาชิกที่มีอันดับน้อยสุดในเหล่าสมาชิก f, g ใน H ซึ่ง $fg \neq gf$ ให้ $m = o(a)$ และ $n = o(b)$ และให้ p เป็นจำนวนเฉพาะซึ่ง $p|m$ ดังนั้นจะมีจำนวนเต็ม s ซึ่ง $ps = m$ และได้ว่า $e = a^m = a^{ps} = (a^p)^s$ ดังนั้น $o(a^p) \leq s < m$ ในทำนองเดียวกัน ให้ q เป็นจำนวนเฉพาะซึ่ง $q|n$ ดังนั้นจะมีจำนวนเต็ม t ซึ่ง $qt = n$ ดังนั้น $o(a^q) \leq t < n$

สมมติ $a^p b \neq ba^p$ เนื่องจาก a และ b เป็นสมาชิกที่มีอันดับน้อยสุดในเหล่าสมาชิก f, g ใน H ซึ่ง $fg \neq gf$ เพราะฉะนั้น $o(a^p) \geq m$ ทำให้เกิดข้อขัดแย้ง ดังนั้น $a^p b = ba^p$ ทำให้ได้ว่า $(a^p, b) = e$ โดยการพิสูจน์ทำนองเดียวกัน จะได้ว่า $(a, b^q) = e$ เนื่องจาก $c^p = (a,b)^p = (a^p, b) = e = (a, b^q) = (a, b)^q = c^q$ ทำให้ได้ว่า $o(c) | p$ และ $o(c) | q$ ดังนั้น $o(c) = 1$ หรือ $o(c) = p = q$ เพราะว่า $c \neq e$ ดังนั้น $o(c) = p = q$

เนื่องจาก m สามารถเขียนได้ในรูปผลคูณจำกัดของกำลังของจำนวนเฉพาะต่างๆ นั่นคือ มีจำนวนเต็มบวก $M, t_1, \ldots, t_M$ และจำนวนเฉพาะ $p_1, \ldots, p_M$ ที่ทำให้ $m = {p_1}^{t_1} {p_2}^{t_2} \ldots {p_M}^{t_M}$ และโดยใช้การพิสูจน์ในทำนองเดียวกับก่อนหน้านี้ เราจะได้ $c^{p1} = c^{p2} = \ldots = e$ จึงทำให้ได้ว่า $p_1 = p_2 = \ldots = p_M = p$ ทำให้เราสรุปได้ว่า จะมีจำนวนเต็มบวก u ซึ่ง $m = p^u$ และโดยการพิสูจน์ในทำนองเดียวกัน จะได้ว่า มีจำนวนเต็มบวก v ซึ่ง $n = p^v$

ต่อไปจะแสดงว่า $p^2 | m$ และ $p^2 | n$ โดยการแสดงว่า $u \geq 2$ และ $v \geq 2$

สมมติให้ $u=1$ จะได้ว่า $m=p$ เนื่องจาก $c^p=e$ และ $c\neq e$ ดังนั้น $|\langle c\rangle|=|\langle a\rangle|=p$ ซึ่งแสดงว่า $\langle c\rangle=\langle a\rangle$ และเกิดข้อขัดแย้งกับที่แสดงไว้ว่า $\langle c\rangle$ เป็นกรุปย่อยแท้ของ $\langle a\rangle$ ดังนั้น $u\geq 2$ ในทำนองเดียวกันเราได้ว่า $v\geq 2$

ต่อไปจะแสดงว่า a^p อยู่ใน $Z(Q)$ ให้ $x\in Q$ ถ้า $x=a^i$ สำหรับ i ที่เป็นจำนวนเต็ม เราได้ว่า $a^px=a^pa^i=a^{p+i}=a^ia^p=xa^p$ ถ้า $x=b^j$ สำหรับ j ที่เป็นจำนวนเต็มและจาก $(a^p,b)=e$ เราได้ว่า $a^px=a^pb^j=(a^pb)b^{i-1}=(ba^p)b^{i-1}=...=b^{i-1}(a^pb)=b^ia^p=xa^p$ ถ้า $x=a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}$ สำหรับจำนวนเต็มบวก n และ k_i เป็นจำนวนเต็ม ซึ่ง $i=1,2,3,...,n$ โดยการแสดงกรณีที่ $x=a^i$ และ $x=b^j$ เราจะได้

$$\begin{aligned}
a^px &= a^p(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn})\\
&= (a^{k1}a^p)(b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn})\\
&= a^{k1}(b^{k2}a^p)(a^{k3}b^{k4}....a^{kn-1}b^{kn})\\
&= \ \ldots\\
&= a^{k1}\ldots a^{kn-1}(a^pb^{kn})\\
&= a^{k1}b^{k2}\ldots a^{kn-1}b^{kn}a^p\\
&= xa^p
\end{aligned}$$

จากกรณีทั้งหมดเราได้ว่า $a^px=xa^p$ สำหรับทุกๆ $x\in Q$ ดังนั้น a^p อยู่ใน $Z(Q)$ และโดยการพิสูจน์ในทำนองเดียวกัน เราจะได้ว่า b^p อยู่ใน $Z(Q)$

เนื่องจาก $c=a^r$, $a^{rp}=(a^r)^p=c^p=e$ และจาก $o(a)=p^u$ เราจะได้ $p^u|rp$ ดังนั้นจะมีจำนวนเต็มบวก j ซึ่ง $rp=jp^u$ และได้ว่า $r=jp^{u-1}$ ถ้า p เป็นตัวหารของ j แล้วจะมีจำนวนเต็มบวก t ซึ่ง $j=pt$ และจาก $r=jp^{u-1}$ เราจะได้ว่า $r=ptp^{u-1}=tp^u$ และ $c=a^r=a^{tp^u}=\left(a^{p^u}\right)^t=e$ เกิดข้อขัดแย้งกับ $c\neq e$ ดังนั้น p ไม่เป็นตัวหารของ j และ $c=a^{jp^{u-1}}$ โดยการพิสูจน์ในทำนองเดียวกัน จะได้ว่ามีจำนวนเต็มบวก k ซึ่ง p ไม่เป็นตัวหารของ k ที่ทำให้ $c=b^{kp^{v-1}}$

โดยไม่เสียนัยสมมติ $u\geq v$ เนื่องจาก $c^k=(a,b)^k=(a,b^k)=ab^ka^{-1}b^{-k}$ และ p ไม่เป็นตัวหารของ k ดังนั้น $e\neq c^k=ab^ka^{-1}b^{-k}$ ซึ่งแสดงว่า $ab^k\neq b^ka$

ให้ $b_1=a^{-jp^{u-v}}b^k$ จะแสดงว่า $ab_1=b_1a$ เนื่องจาก $ab_1=a\left(a^{-jp^{u-v}}b^k\right)=$

$a^{1-jp^{u-v}}b^k=\left(a^{-jp^{u-v}}a\right)b^k$ และ $b_1a=\left(a^{-jp^{u-v}}b^k\right)a$ ดังนั้น $a^{-jp^{u-v}}ab^k=$ $a^{-jp^{u-v}}b^ka$ ทำให้ได้ว่า $ab^k=b^ka$ เกิดข้อขัดแย้ง ดังนั้น $ab_1\neq b_1a$ และจะได้ว่า b_1 มีอันดับจำกัด และจากการสมมติว่าสมาชิก a และ b เป็นสมาชิกที่มีอันดับน้อยสุดในเหล่าสมาชิก f,g ใน H ซึ่ง $fg\neq gf$ ดังนั้น $o(b_1)\geq o(b)$ ทำให้ได้ ${b_1}^{p^{v-1}}\neq e$

เนื่องจาก ${b_1}^p=\left(a^{-jp^{u-v}}b^k\right)^p$

$$=\left(a^{-jp^{u-v}}\right)^p\left(b^k\right)^p\left(b^k,a^{-jp^{u-v}}\right)^{p(p-1)/2}$$

$$=\left(a^p\right)^{-jp^{u-v}}\left(b^p\right)^k(a,b)^{jkp^{u-v}(p(p-1)/2)}$$

$$=\left(a^p\right)^{-jp^{u-v}}\left(b^p\right)^kc^{jkp^{u-v}(p(p-1)/2)}$$

ทำให้ได้ว่า

$${b_1}^{p^{v-1}}=\left({b_1}^p\right)^{p^{v-2}}$$

$$=\left(\left(a^p\right)^{-jp^{u-v}}\left(b^p\right)^kc^{jkp^{u-v}(p(p-1)/2)}\right)^{p^{v-2}}$$

$$=\left(a^{p^{v-1}}\right)^{-jp^{u-v}}\left(b^{p^{v-1}}\right)^kc^{jkp^{u-v}((p-1)/2)p^{v-1}}\quad(\because a^p,b^p,c\in Z(Q))$$

$$=a^{-jp^{u-1}}\left(b^{kp^{v-1}}\right)c^{jkp^{u-1}(p-1)/2}$$

$$=b^{-kp^{v-1}}b^{kp^{v-1}}c^{jkp^{u-1}(p-1)/2}$$

$$=c^{jkp^{u-1}(p-1)/2}$$

ดังนั้น $c^{jkp^{u-1}(p-1)/2}\neq e$ สมมติ p เป็นจำนวนเฉพาะคี่ แล้วจะมีจำนวนเต็มบวก t ซึ่ง $p=2t+1$ หรือก็คือ $p-1=2t$ ทำให้ได้ว่า $c^{jkp^{u-1}(p-1)/2}=c^{jkp^{u-1}(2t)/2}=c^{p^{u-1}jkt}$ $=\left(c^p\right)^{p^{u-2}jkt}=e$ เกิดข้อขัดแย้งกับ $c^{jkp^{u-1}(p-1)/2}={b_1}^{p^{v-1}}\neq e$ ดังนั้น $p=2$

สมมติให้ $u>2$ แล้ว $u-2\geq1$ ซึ่งทำให้ได้ $c^{jkp^{u-1}(p-1)/2}=c^{jk2^{u-1}(2-1)/2}$

$= c^{jk2^{u-1-1}} = \left(c^2\right)^{jk2^{u-3}} = e$ เพราะว่า $c^p = c^2 = e$ ซึ่งเกิดข้อขัดแย้งในทำนองเดียวกับข้างต้น ดังนั้น $u = 2$ และเนื่องจาก $c = a^{jp^{u-1}}$ และ $p = 2$ ทำให้ได้ว่า $c = a^{2j}$ เนื่องจาก 2 ไม่เป็นตัวหารของ j ดังนั้น j เป็นจำนวนคี่ แล้วจะมีจำนวนเต็ม t ซึ่ง $j = 2t+1$ ทำให้ได้ว่า $c = a^{(2t+1)2} = \left(a^4\right)^t a^2 = a^2$ เนื่องจาก $u \geq v \geq 2$ และ $u = 2$ จึงได้ว่า $v = 2$ และโดยการพิสูจน์ในทำนองเดียวกัน จะได้ว่า $c = b^2$ ทำให้ได้ว่า $a^2 = b^2,\ c = a^{-1}b^{-1}ab$ และ $c^2 = e$

เนื่องจาก $a^2 = c = a^{-1}b^{-1}ab$ และ $a^2b = ba^2$ จะได้ว่า $a^3b = aa^{-1}b^{-1}abb$

$= b^{-1}ab^2 = b^{-1}b^2a = ba$ ดังนั้น $ba = a^3b$

เพราะฉะนั้น $Q = \langle a, b \rangle$ เป็นกรุปควอเทอร์เนียน ∎

5.2.4 **ทฤษฎีบท** ถ้า G เป็นกรุปฮามิลทอเนียน แล้วจะมีกรุปย่อยควอเทอร์เนียน Q ของ G ซึ่ง $G = QC$ โดยที่ C เป็นเซตกำหนดเชิงศูนย์กลางของ Q ใน G

บทพิสูจน์ ให้ G เป็นกรุปฮามิลทอเนียน แล้วโดยทฤษฎีบท 5.2.3 จะมีสมาชิก a และ b ใน G เป็นสมาชิกที่มีอันดับน้อยสุดในเหล่าสมาชิก $x, y \in G$ ซึ่ง $xy \neq yx$ ซึ่ง $Q = \langle a, b \rangle$ เป็นกรุปย่อยควอเทอร์เนียนของ G ให้ C เป็นเซตกำหนดเชิงศูนย์กลางของ Q ใน G หรือ $C = Z(Q)$ เนื่องจาก Q และ C เป็นกรุปย่อยของ G ดังนั้น $QC \subseteq G$

ให้ $x \in G$ ถ้า $x \in C$ และเพราะว่าเอกลักษณ์ e ของ G เป็นสมาชิกของ Q ที่ทำให้ $x = ex$ ดังนั้น $x \in QC$ ถ้า $x \notin C$ แล้วมี $t \in Q$ ซึ่ง $xt \neq tx$ สมมติว่า $xa = ax$ และ $xb = bx$ เนื่องจาก $t \in Q$ ดังนั้น มีจำนวนเต็มบวก n และจำนวนเต็ม k_i เมื่อ $i = 1,2,3,..,n$ ซึ่ง $t = a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}$ แล้วโดย $xa = ax$ และ $xb = bx$ เราจะได้ว่า

$$\begin{aligned} xt &= x\left(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\ &= \left(a^{k1}x\right)b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn} \\ &= a^{k1}\left(b^{k2}x\right)a^{k3}b^{k4}....a^{kn-1}b^{kn} \\ &= ..... \\ &= a^{k1}....a^{kn-1}\left(xb^{kn}\right) \\ &= a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}x \\ &= tx \end{aligned}$$

เกิดข้อขัดแย้ง เพราะฉะนั้น $xa \neq ax$ หรือ $xb \neq bx$

1. สมมติว่า $xa \neq ax$ และ $xb = bx$ โดยทฤษฎีบทประกอบ 5.2.2 จะได้ว่า $axa^{-1}x^{-1} \in \langle a \rangle \cap \langle x \rangle$ เนื่องจาก $o(a) = 4$ ดังนั้น $\langle a \rangle = \{e, a, a^2, a^3\}$ ถ้า $axa^{-1}x^{-1} = a$ แล้ว $ax = axa$ ทำให้ได้ว่า $a = (ax)^{-1}(axa) = (ax)^{-1}ax = e$ เกิดข้อขัดแย้งเนื่องจาก $a \neq e$ ถ้า $axa^{-1}x^{-1} = a^3$ แล้ว $xa^{-1}x^{-1} = a^2$ ทำให้ได้ $x = a^2xa = b^2xa = xb^2a$ ดังนั้น $b^2a = e$ นั่นคือ $a^3 = e$ เกิดข้อขัดแย้ง ดังนั้น $axa^{-1}x^{-1} = a^2$ จะได้ว่า $xa^{-1}x^{-1} = a$ นั่นคือ $xa^{-1} = ax$ ให้ $c = a^{-1}b^{-1}ab$ ดังนั้น $xc = xa^{-1}b^{-1}ab = xbb = xb^2$ จะได้ว่า $xb = xa^{-1}b^{-1}a$ ทำให้ได้ $(xb)a = xa^{-1}b^{-1}aa = xa^{-1}b^{-1}a^2 = xa^{-1}b^{-1}b^2 = xa^{-1}b = a(xb)$ นั่นคือ $(xb)a = a(xb)$ ต่อไปจะแสดงว่า $xbt = txb$ สำหรับทุก $t \in Q$ ให้ $t \in Q$ แล้วจะมีจำนวนเต็มบวก n และจำนวนเต็ม k_i เมื่อ $i = 1,2,3,...,n$ ซึ่ง $t = a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}$ แล้วโดย $xb = bx$ และ $(xb)a = a(xb)$ เราจะได้ว่า

$$\begin{aligned}
xbt &= xb\left(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\
&= \left(a^{k1}xb\right)b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn} \\
&= a^{k1}(bx)b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn} \\
&= a^{k1}b\left(xb^{k2}\right)a^{k3}b^{k4}....a^{kn-1}b^{kn} \\
&= a^{k1}b^{k2}(xb)a^{k3}b^{k4}....a^{kn-1}b^{kn} \\
&= .... \\
&= a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}(xb)b^{kn} \\
&= \left(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right)xb \\
&= txb
\end{aligned}$$

นั่นคือ $xb \in C$ จะได้ว่า มี $t \in C$ ซึ่ง $xb = t$ ทำให้ได้ว่า $x = tb^{-1} = b^{-1}t \in QC$

2. สมมติว่า $xa = ax$ และ $xb \neq bx$ โดยทฤษฎีบทประกอบ 5.2.2 จะได้ว่า $bxb^{-1}x^{-1} \in \langle b \rangle \cap \langle x \rangle$ เนื่องจาก $o(b) = 4$ ดังนั้น $\langle b \rangle = \{e, b, b^2, b^3\}$ โดยการพิสูจน์ในทำนองเดียวกันเราจะได้ว่า $bxb^{-1}x^{-1} = b^2$ และได้ว่า $bx = xb^{-1}$

ต่อไปจะแสดงว่า $(xa)b = b(xa)$ จาก $a^2 = c = a^{-1}b^{-1}ab$ จะได้ว่า $a^3 = aa^{-1}b^{-1}ab = b^{-1}ab$ และได้ $xa^3 = xb^{-1}ab$ และ $xa^3a^2 = xb^{-1}aba^2$ ดังนั้น $xa = xb^{-1}ab^3$ หรือ $xab = xb^{-1}ab^3b = xb^{-1}a = bxa = xb^{-1}a$ โดยการพิสูจน์ในทำนองเดียวกันกับการพิสูจน์ว่า $xbt = txb$ สำหรับทุก $t \in Q$ เราจะได้ว่า $xat = txa$ สำหรับทุก $t \in Q$ นั่นคือ $xa \in C$ จะได้ว่ามี $t \in C$ ซึ่ง $xa = t$ ทำให้ได้ว่า $x = ta^{-1} = a^{-1}t \in QC$

3. สมมติว่า $xa \neq ax$ โดยทฤษฎีบทประกอบ 5.2.2 จะได้ว่า $axa^{-1}x^{-1} \in \langle a \rangle \cap \langle x \rangle$ และโดยการพิสูจน์แบบเดียวกันกับทฤษฎีบท 5.2.3 ข้อ 1.2 เราจะได้ว่า $axa^{-1}x^{-1} = a^2$ ทำให้ได้ $xa^{-1} = ax$ และเพราะว่า $o(a) = o(b) = 4$ และ $ba = a^3b$ ดังนั้น $a(xab) = xa^{-1}ab = xb = xa^4b = xaa^3b = (xab)a$ ฉะนั้น $a(xab) = (xab)a$ ในทำนองเดียวกันสมมติ $xb \neq bx$ จะได้ $b(xab) = (xab)b$

ต่อไปจะแสดงว่า $xabt = txab$ สำหรับทุก $t \in Q$ ให้ $t \in Q$ แล้วจะมีจำนวนเต็มบวก n และจำนวนเต็ม k_i เมื่อ $i = 1,2,3,...,n$ ซึ่ง $t = a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}$ แล้วโดย $(xab)a = a(xab)$ และ $(xab)b = b(xab)$ จะได้ว่า

$$\begin{aligned} xabt &= xab\left(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right) \\ &= a^{k1}(xab)b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn} \\ &= a^{k1}b^{k2}(xab)a^{k3}b^{k4}....a^{kn-1}b^{kn} \\ &= .... \\ &= a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}(xab)b^{kn} \\ &= \left(a^{k1}b^{k2}a^{k3}b^{k4}....a^{kn-1}b^{kn}\right)xab \\ &= txab \end{aligned}$$

นั่นคือ $xab \in C$ จะได้ว่ามี $t \in C$ ซึ่ง $xab = t$ ทำให้ได้ว่า $x = tb^{-1}a^{-1} = \left(b^{-1}a^{-1}\right)t \in QC$

ไม่ว่ากรณีใดๆ ได้ว่า $x \in QC$ ทำให้ได้ว่า $G \subseteq QC$ นั่นคือ $G = QC$ ∎

5.2.5 **ทฤษฎีบท** ถ้า G เป็นกรุปฮามิลทอเนียน แล้วจะมี Q ซึ่งเป็นกรุปย่อยควอเทอร์เนียน มี Z เป็นกรุปย่อยอาบีเลียนซึ่งทุกสมาชิกมีอันดับเป็นจำนวนคี่ และมี U เป็นกรุปย่อยอาบีเลียนที่มีทุกสมาชิกมีอันดับสอง ที่ทำให้ $G \cong Q \times U \times Z$

บทพิสูจน์ ให้ G เป็นกรุปฮามิลทอเนียน และให้ a และ b เป็นสมาชิกที่มีอันดับน้อยสุดในเหล่าสมาชิก f, g ใน G ซึ่ง $fg \neq gf$ แล้วโดยทฤษฎีบท 5.2.3 จะได้ว่ามี $Q = \langle a, b \rangle$ เป็นกรุปย่อยควอเทอร์เนียนของ G และโดยทฤษฎีบท 5.2.4 จะได้ว่า $G = QC$ เมื่อ $C = Z(Q)$

1. จะแสดงว่าทุกสมาชิกใน G มีอันดับจำกัด ให้ $g \in G$ ถ้า $g \notin C(G)$ แล้วจะมี $h \in G$ ซึ่ง $gh \neq hg$ แล้วโดยใช้การพิสูจน์ในทฤษฎีบท 5.2.3 จะได้ว่า g มีอันดับจำกัด และถ้า $g \in C(G)$ แล้ว $ga = ag$ สมมติ $bga = gab$ แล้ว $gba = gab$ ทำให้ได้ $\left(g^{-1}\right)gba = \left(g^{-1}\right)gab$ นั่นคือ $ba = ab$ เกิดข้อขัดแย้ง ดังนั้น $bga \neq gab$ แล้วโดยการพิสูจน์ในทฤษฎีบท 5.2.3 ทำให้ได้

ว่า b และ ga มีอันดับจำกัด ให้ d เป็นจำนวนเต็มบวกซึ่ง $(ga)^d = e$ เนื่องจาก $a^4 = e$ จึงได้ว่า $e = \left((ga)^d\right)^4 = \left(g^{4d}\right)\left(a^{4d}\right) = \left(g^{4d}\right)e = g^{4d}$ ซึ่งแสดงว่า g มีอันดับจำกัด

2. จะแสดงว่า C ไม่มีสมาชิกที่มีอันดับ 4 สมมติว่ามี $x \in C$ ซึ่ง $x^4 = e$ จาก $xa = ax$ ทำให้ได้ $b(ax) \neq (xa)b$ เนื่องจาก $xab = axb = abx$ ดังนั้น $(bx)a \neq a(bx)$ และ เนื่องจาก a และ b เป็นสมาชิกที่มีอันดับน้อยสุดในเหล่าสมาชิก f, g ใน G ซึ่ง $fg \neq gf$ ดังนั้น $o(bx) \geq o(b) = 4$ และ $x^4 = e$ ฉะนั้น $(bx)^4 = b^4x^4 = e$ นั่นแสดงว่า $o(bx) \leq 4$ เพราะฉะนั้น $o(bx) = 4 = o(b)$ โดยการพิสูจน์ในทฤษฎีบท 5.2.3 จะได้ว่า $\langle a, bx\rangle$ เป็นกรุปย่อยควอเทอร์เนียนของ G ทำให้ได้ว่า $e = a^4 = a^2a^2 = a^2(bx)^2 = a^2b^2x^2 = a^2a^2x^2 = a^4x^2 = x^2$ ฉะนั้น $o(x) \leq 2$ เกิดข้อขัดแย้งกับ $o(x) = 4$ ดังนั้น C ไม่มีสมาชิกที่มีอันดับ 4 เพราะฉะนั้น C ไม่มีกรุปย่อยควอเทอร์เนียน ทำให้ได้ว่า C เป็นกรุปอาบีเลียน

3. ให้ $Z = \{ x \in C \mid$ อันดับของ x เป็นจำนวนคี่ $\}$ และ $Z_1 = \left\{ x \in C \,\middle|\, x^2 = e \right\}$ จะแสดงว่า Z และ Z_1 เป็นกรุปย่อยของ C ให้ $x, y \in Z$ แล้วจะมีจำนวนเต็มบวก m และ n ที่น้อยสุดซึ่ง $x^{2m+1} = e$ และ $y^{2n+1} = e$ จะได้ว่า $(xy)^{(2m+1)(2n+1)} = x^{(2m+1)(2n+1)}$ $y^{(2m+1)(2n+1)} = \left(x^{(2m+1)}\right)^{(2n+1)}\left(y^{(2n+1)}\right)^{(2m+1)} = e$ ดังนั้น xy มีอันดับเป็นจำนวนคี่ ฉะนั้น $xy \in Z$ เพราะว่า $e = x^{(2m+1)}x^{-(2m+1)} = ex^{-(2m+1)} = x^{(-1)(2m+1)} = \left(x^{-1}\right)^{2m+1}$ จะได้ว่า x^{-1} มีอันดับเป็นจำนวนคี่ ดังนั้น $x^{-1} \in Z$ ทำให้ได้ว่า Z เป็นกรุปย่อยของ C ให้ $x, y \in Z_1$ แล้ว $x^2 = e$ และ $y^2 = e$ จะได้ว่า $x^2y^2 = (xy)^2 = e$ ฉะนั้น $xy \in Z_1$ และจะได้ $e = x^{2-2} = x^2\left(x^{-2}\right) = e\left(x^{-2}\right)$ ทำให้ได้ $e = x^{-2} = \left(x^{-1}\right)^2$ ซึ่งแสดงว่า $x^{-1} \in Z_1$ ดังนั้น Z_1 เป็นกรุปย่อยของ C

4. จะแสดงว่า $C = ZZ_1$ ให้ $x \in C$ แล้วเพราะว่าทุกสมาชิกใน G มีอันดับจำกัด จะได้ว่า x มีอันดับจำกัด ถ้าอันดับของ x เป็นจำนวนคี่แล้ว $x \in Z$ และเพราะ $e \in Z_1$ ทำให้ $x = xe \in ZZ_1$ ถ้าอันดับของ x เป็นจำนวนคู่ แล้วจะมีจำนวนเต็มบวก m ซึ่ง $o(x) = 2m$ สมมติ m เป็นจำนวนคู่ จะได้ว่ามีจำนวนเต็มบวก k ซึ่ง $m = 2k$ ที่ทำให้ $x^{2m} = x^{2(2k)} = e$ นั่นคือ $\left(x^k\right)^4 = e$ แต่จากการพิสูจน์ในข้อ 2 เราได้ว่าทุกสมาชิก x ใน C ถ้า $x^4 = e$ แล้ว $x^2 = e$ จะได้ว่า $\left(x^k\right)^2 = e$ นั่นคือ $x^{2k} = e$ เกิดข้อขัดแย้งกับ $o(x) = 2m$ เนื่องจาก $2k < 2m$ ดังนั้น m เป็นจำนวนคี่ ฉะนั้นมีจำนวนเต็มบวก k ซึ่ง $m = 2k + 1$ ดังนั้น $\left(x^{2k+1}\right)^2 = x^{2(2k+1)} = e$ ทำให้ได้ว่า $x^{2k+1} \in Z_1$ หรือ $\left(x^2\right)^{2k+1} = e$ แสดงว่า $x^2 \in Z$ และเนื่องจาก $x = ex = x^{2m}x =$

$x^{2(2k+1)}x = x^{4k+2}x = x^{2(k+1)}x^{2k}x = \left(x^2\right)^{k+1}\left(x^{2k+1}\right)$ ดังนั้น $x \in ZZ_1$ ฉะนั้น $C \subseteq ZZ_1$ เนื่องจาก Z และ Z_1 เป็นกรุปย่อยของ C ดังนั้น $ZZ_1 \subseteq C$ เพราะฉะนั้น $C = ZZ_1$ เนื่องจาก C เป็นกรุปอาบีเลียน ดังนั้น Z และ Z_1 เป็นกรุปย่อยปกติของ C เนื่องจาก $C = ZZ_1$ และ $Z \cap Z_1 = \{e\}$ จึงได้ว่า $C \cong Z \times Z_1$

5. เพราะว่า $c^2 = e$ ดังนั้น $c \in Z_1$ จะแสดงว่าเซตอันดับ $H = \{D | D$ เป็นกรุปย่อยของ Z_1 และ $c \notin D\}$ มีสมาชิกใหญ่สุดเฉพาะกลุ่ม ให้ P เป็นเซตย่อยอันดับเชิงเส้นของ H

สมมติ $c \in \left\langle \bigcup_{K \in P} K \right\rangle$ แล้วจะมีจำนวนเต็มบวก n และ $D_1, D_2, \ldots, D_n \in P$ ซึ่ง $c = x_1 \ldots x_n$ โดยที่ $x_i \in D_i$ เมื่อ $1 \le i \le n$ และเพราะ P เป็นอันดับเชิงเส้น เราอาจสมมติให้ $D_1 \subseteq D_2 \subseteq \ldots \subseteq D_n$ แล้ว $x_i \in D_n$ สำหรับทุกๆ $1 \le i \le n$ จะได้ $c = x_1 x_2 \ldots x_n \in D_n$ เกิดข้อขัดแย้งเพราะว่า $D_n \in H$ และ $c \notin D$ ทุกๆ $D \in H$ เพราะฉะนั้น $c \notin \left\langle \bigcup_{K \in P} K \right\rangle$ ทำให้ได้ว่า $\left\langle \bigcup_{K \in P} K \right\rangle \in H$

เนื่องจาก D เป็นกรุปย่อยของ $\left\langle \bigcup_{K \in P} K \right\rangle$ สำหรับทุกๆ $D \in P$ ดังนั้น $\left\langle \bigcup_{K \in P} K \right\rangle$ เป็นขอบเขตบนของ P ใน H ทำให้โดย Zorn's Lemma เราได้ว่า H จะมีสมาชิกใหญ่สุดเฉพาะกลุ่ม ให้ U เป็นสมาชิกใหญ่สุดเฉพาะกลุ่มของ H แล้ว U เป็นกรุปย่อยใหญ่สุดเฉพาะกลุ่มของ Z_1 ซึ่ง $c \notin U$

6. จะแสดงว่า $\langle U, c\rangle = \langle U, x\rangle$ สำหรับทุกสมาชิก $x \in Z_1 - U$

ให้ $x \in Z_1 - U$ แล้ว $xc \in Z_1$ ถ้า $c \in \langle U, xc\rangle$ แล้วจะมี $t \in U$ ซึ่ง $t(xc) = c$ จะได้ว่า $x = t^{-1} \in U$ เกิดข้อขัดแย้ง ดังนั้น $c \notin \langle U, xc\rangle$ ทำให้ได้ $\langle U, xc\rangle$ เป็นกรุปย่อยของ Z_1 ซึ่ง $c \notin \langle U, xc\rangle$ ดังนั้น $\langle U, xc\rangle \neq Z_1$ แต่ U เป็นกรุปย่อยใหญ่สุดเฉพาะกลุ่มของ Z_1 ซึ่ง $c \notin U$ และ $U \subseteq \langle U, xc\rangle \subset Z_1$ ดังนั้น $U = \langle U, xc\rangle$ ทำให้ได้ว่า $xc \in U$ ดังนั้นจะมี $u \in U$ ซึ่ง $xc = u$ หรือ $x = uc^{-1} = cu$ นั่นแสดงว่า $x \in \langle U, c\rangle$ และทำให้ได้ว่า $c = x^{-1}u = ux$ หรือ $c \in \langle U, x\rangle$ ดังนั้น $\langle U, c\rangle \subseteq \langle U, x\rangle$ และโดยการพิสูจน์ในทำนองเดียวกันจะได้ $\langle U, c\rangle = \langle U, x\rangle$

7. จะแสดงว่า $C \cong Z \times U \times \langle c\rangle$

เนื่องจาก $U \subset Z_1$ และ $\langle c\rangle \subset Z_1$ ดังนั้น $\langle U, c\rangle \subseteq Z_1$ ให้ $t \in Z_1$ ถ้า $t \in U$ จะได้ว่า $t \in \langle U, c\rangle$ ถ้า $t \notin U$ จะได้ว่า $t \in Z_1 - U$ โดยข้อ 6 เราได้ว่า $\langle U, c\rangle = \langle U, t\rangle$ และ $t \in \langle U, c\rangle$

จากทั้งสองกรณีทำให้ได้ว่า $Z_1 \subseteq \langle U,c\rangle$ ฉะนั้น $Z_1 = \langle U,c\rangle$ เพราะว่า $U \cap \langle c\rangle = \{e\}$ ดังนั้น $Z_1 \cong U \times \langle c\rangle$ และเนื่องจาก $C \cong Z \times Z_1$ ดังนั้น $C \cong Z \times U \times \langle c\rangle$

8. จะแสดงว่า $Q \cap C = \langle c\rangle$

ให้ $t \in Q \cap C$ แล้ว $t \in Q$ และ $t \in C$ เนื่องจาก $Q = \{e, a, a^2, a^3, b, b^3, ab, ab^3\}$ และ $a, b \notin C$ ดังนั้น $t \neq a$ และ $t \neq b$ ถ้า $t = a^3$ แล้วจะได้ว่า $a^3b = ba^3 = ba^2a = a^3b = ba^3 = ba^2a = bb^2a = b^2ba = a^2ba$ ทำให้ได้ว่า $ab = ba$ เกิดข้อขัดแย้ง ดังนั้น $t \neq a^3$ ถ้า $t = b^3$ แล้วจะได้ $b^3a = ab^3 = ab^2b = aa^2b = a^2ab = b^2ab$ ทำให้ได้ว่า $ab = ba$ เกิดข้อขัดแย้ง ดังนั้น $t \neq b^3$ ถ้า $t = ab$ แล้ว $aba = aab$ หรือ $ba = ab$ เกิดข้อขัดแย้ง ดังนั้น $t \neq ab$ ถ้า $t = ab^3$ แล้ว $ab^3a = aab^3 = b^2b^3 = b$ ทำให้ได้ว่า $ab = a(ab^3a) = a(ab^2ba) = aa^3ba = ba$ เกิดข้อขัดแย้ง ดังนั้น $t \neq ab^3$ เพราะฉะนั้น $t = e$ หรือ $t = a^2 = c$ ทำให้ได้ว่า $Q \cap C \subseteq \langle c\rangle$

โดยการพิสูจน์ในทฤษฎีบท 5.2.3 เราได้ว่า $a^2 = c \in Z(Q) = C$ ดังนั้น $c \in Q \cap C$ และทำให้ได้ว่า $\langle c\rangle \subseteq Q \cap C$ ดังนั้น $Q \cap C = \langle c\rangle$

9. จะแสดงว่า $G \cong Q \times U \times Z$

เนื่องจาก Q, Z และ U เป็นกรุปย่อยของ G ดังนั้น $Q(Z \times U) \subseteq G$ เนื่องจาก $(Q \cap (Z \times U)) \subseteq (Q \cap C)$ และ $Q \cap C = \langle c\rangle$ ดังนั้น $Q \cap (Z \times U) \subseteq \langle c\rangle$ สมมติให้ $c \in ZU$ แล้วจะมี $z \in Z$ และ $u \in U$ ซึ่ง $c = zu$ ทำให้ได้ว่า $z = cu$ หรือ $z^2 = (cu)^2 = e$ เกิดข้อขัดแย้ง และเนื่องจาก z มีอันดับเป็นจำนวนคี่ ดังนั้น $c \notin ZU$ ฉะนั้น $c \notin Q \cap (Z \times U) \subseteq \langle c\rangle$ เพราะฉะนั้น $Q \cap (Z \times U) \subseteq \{e\}$

ให้ $g \in G$ แล้วเพราะว่า $G = QC$ จะมี $q \in Q$ และ $y \in C$ ซึ่ง $g = qy$ เนื่องจาก $C \cong Z \times U \times \langle c\rangle$ ดังนั้นมี $z \in Z$ และ $u \in U$ และ $c \in \langle c\rangle$ ซึ่ง $g = qzuc = qczu$ และเนื่องจาก $q, c \in Q$ ดังนั้นมี $\bar{q} \in Q$ ซึ่ง $\bar{q} = qc$ ทำให้ได้ว่า $g = \bar{q}zu$ ดังนั้น $g \in Q(Z \times U)$ ฉะนั้น $G \subseteq Q(Z \times U)$ ทำให้ได้ว่า $G = Q(Z \times U)$ และเนื่องจาก $Q \cap (Z \times U) \subseteq \{e\}$ และ $G = Q(Z \times U)$ ดังนั้น $G \cong Q \times U \times Z$ ∎

5.2.6 **ทฤษฎีบท** ถ้า $G = Z \times U \times Q$ โดยที่ Z เป็นกรุปย่อยอาบีเลียนซึ่งทุกสมาชิกมีอันดับเป็นจำนวนคี่ U เป็นกรุปย่อยอาบีเลียนที่ทุกสมาชิกมีอันดับสองและ Q เป็นกรุปย่อยควอเทอร์เนียน แล้ว G เป็นกรุปฮามิลทอเนียน

บทพิสูจน์ ให้ $G = Z \times U \times Q$ โดยที่ Z เป็นกรุปย่อยอาบีเลียนซึ่งทุกสมาชิกมีอันดับเป็นจำนวนคี่ U เป็นกรุปย่อยอาบีเลียนที่ทุกสมาชิกมีอันดับสองและ Q เป็นกรุปย่อยควอเทอร์เนียน ต้องการแสดงว่า G เป็นกรุปฮามิลทอเนียน นั่นคือต้องแสดงว่า กรุปย่อยใด ๆ ของ G เป็นกรุปย่อยปกติ ให้ H เป็นกรุปย่อยของ G ถ้า $H = \{e\}$ แล้ว H เป็นกรุปย่อยปกติของ G จึงพิจารณากรณี $H \neq \{e\}$

เราจะพิสูจน์ว่า $g^{-1}Hg \subseteq G$ สำหรับทุกๆ $g \in G$

ให้ $g \in G$ และให้ $h \in H$ แล้วจะมี $a \in Z, b \in U$ และ $q \in Q$ ซึ่ง $h = (a, b, q)$ และจะมี $\alpha \in Z, \beta \in U$ และ $\gamma \in Q$ ซึ่ง $g = (\alpha, \beta, \gamma)$ ทำให้ได้

$$\begin{aligned} g^{-1}hg &= (\alpha, \beta, \gamma)^{-1}(a, b, q)(\alpha, \beta, \gamma) \\ &= \left(\alpha^{-1}a\alpha, \beta^{-1}b\beta, \gamma^{-1}q\gamma\right) \\ &= \left(a, b, \gamma^{-1}q\gamma\right) \quad \text{(เพราะว่า } Z \text{ และ } U \text{ เป็นกรุปอาบีเลียน)} \end{aligned}$$

ดังนั้น $g^{-1}hg = \left(a, b, \gamma^{-1}q\gamma\right)$ ..... (5.2.1)

เราต้องการแสดงว่า $g^{-1}hg \in H$ ซึ่งสมมูลกับการแสดงว่า $\left(a, b, \gamma^{-1}q\gamma\right) \in H$ พิจารณา $\gamma^{-1}q\gamma$ เนื่องจาก $q \in Q$ ดังนั้น $q^4 = e$ เพราะว่ากรุปย่อย $\langle q \rangle$ เป็นกรุปย่อยปกติของ Q เนื่องจาก $\gamma \in Q$ และ $q \in \langle q \rangle$ ดังนั้น $\gamma^{-1}q\gamma \in \langle q \rangle$ ฉะนั้น $\gamma^{-1}q\gamma = e, q, q^2$ หรือ q^3 ถ้า $\gamma^{-1}q\gamma = e$ แล้ว $q\gamma = \gamma$ ทำให้ได้ว่า $q = \gamma\gamma^{-1} = e$ นั่นแสดงว่า $h = (a, b, e)$ และได้สมการ (5.2.1) เป็น $g^{-1}hg = \left(a, b, \gamma^{-1}q\gamma\right) = (a, b, e) = h$ ดังนั้น $g^{-1}hg \in H$ ถ้า $\gamma^{-1}q\gamma = q$ แล้ว $g^{-1}hg = \left(a, b, \gamma^{-1}q\gamma\right) = (a, b, q) = h$ ดังนั้น $g^{-1}hg \in H$ ถ้า $\gamma^{-1}q\gamma = q^2$ แล้ว $\left(\gamma^{-1}q\gamma\right)^2 = \left(q^2\right)^2 = e$ ฉะนั้น $\left(\gamma^{-1}q\gamma\right)\left(\gamma^{-1}q\gamma\right) = e$ หรือ $\gamma^{-1}q^2\gamma = e$ ดังนั้น $q^2 = e$ เพราะฉะนั้น $\langle q \rangle = \{e, q\}$ ทำให้ได้ว่า $\gamma^{-1}q\gamma = e$ หรือ $\gamma^{-1}q\gamma = q$ ดังนั้น $g^{-1}hg \in H$ และถ้า $\gamma^{-1}q\gamma = q^3$ เราจะได้ว่า $g^{-1}hg = \left(a, b, \gamma^{-1}q\gamma\right) = \left(a, b, q^3\right) = (a, b, q)\left(e, e, q^2\right) = h\left(e, e, q^2\right)$

ต่อไปจะแสดงว่า $\left(e, e, q^2\right)$ เป็นสมาชิกของ H เนื่องจาก $a \in Z$ จึงได้ว่ามีจำนวนเต็มบวก n ซึ่ง $o(a) = 2n+1$ ให้ $o(q) = 4$ ให้ $k = 2n+1$ จะได้ว่า

$$a^k = e \qquad \text{.....(5.2.2)}$$

และเนื่องจาก $o(q) = 4$ จึงได้ว่า

$$q^{2k} = q^{2(2n+1)} = q^{4n+2} = \left(q^4\right)^n (q)^2 = e^n q^2 = q^2 \qquad \text{.....(5.2.3)}$$

และเนื่องจาก U เป็นกรุปอาบีเลียนซึ่ง $U = C_2 \times C_2 \times ... \times C_2$ จำนวน m ครั้ง เมื่อ C_2 คือ กรุปย่อยวัฏจักรที่ทุกสมาชิกมีอันดับสอง ดังนั้น สำหรับแต่ละสมาชิก b ใด ๆ ใน U จะได้ว่า

$$b^2 = e \qquad \text{.....(5.2.4)}$$

เนื่องจาก $h = (a, b, q)$ เป็นสมาชิกของกรุปย่อย H ดังนั้น h^{2k} เป็นสมาชิกของกรุปย่อย H โดยสมการ (5.2.2), (5.2.3) และ (5.2.4) จะได้ $h^{2k} = (a, b, q)^{2k} = \left(a^{2k}, b^{2k}, q^{2k}\right) = \left(e, e, q^2\right)$ ดังนั้น $\left(e, e, q^2\right) = h^{2k} \in H$

ฉะนั้น $g^{-1}hg = h\left(e, e, q^2\right) \in H$ ดังนั้น H เป็นกรุปย่อยปกติของ G เพราะฉะนั้น G เป็นกรุปฮามิลทอเนียน ∎

บรรณานุกรม

ภาษาไทย

ฉวีวรรณ รัตนประเสริฐ. พีชคณิตแผนใหม่. ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากร, 2527.

ภาษาอังกฤษ

Dummit, D.S. Abstract Algebra. New Jersey : Prentice-Hall, Inc., 1991.

Hall, M. The Theory of Group. New York : The Macmillan Company, 1959.

Hungerford, T.W. Abstract Algebra : An Introduction. Philadelphia : Saunders College Publishing, 1990.

Kochendorffer, R. Group. London : Mcgraw-Hill Publishing Company Limited, 1970.

Malik, D.S. Fundamentals of Abstract Algebra. New York : The McGraw-Hill Companies, Inc., 1997.

Zassenhans, H.J. The Theory of Groups. New York : Dover Publications, Inc., 1999.

ประวัติผู้วิจัย

ชื่อ-สกุล	นางสาวพัชยา สบบง
ที่อยู่	41 ถ.หน้าโรงไฟฟ้า ต.พระปฐมเจดีย์ อ.เมือง จ.นครปฐม 73000
ประวัติการศึกษา	
พ.ศ. 2547	สำเร็จการศึกษาปริญญาวิทยาศาสตรบัณฑิต สาขาคณิตศาสตร์ มหาวิทยาลัยนเรศวร จังหวัดพิษณุโลก
พ.ศ. 2548	สำเร็จการศึกษาประกาศนียบัณฑิต ทางการสอน มหาวิทยาลัยนเรศวร จังหวัดพิษณุโลก
พ.ศ. 2549	ศึกษาต่อระดับปริญญามหาบัณฑิต สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ประวัติการทำงาน	
พ.ศ. 2548	พนักงานครูเทศบาล ตำแหน่งครูผู้ช่วย สังกัดโรงเรียนเทศบาล๑ วัดพระงาม(สามัคคีพิทยา) เทศบาลนครนครปฐม
พ.ศ. 2550-ปัจจุบัน	พนักงานครูเทศบาล ตำแหน่งครู คศ.1 สังกัดโรงเรียนเทศบาล๑ วัดพระงาม(สามัคคีพิทยา) เทศบาลนครนครปฐม