



ผลคูณตรงและผลคูณอิสระของกรุป

มหาวิทยาลัยศิลปากร โดย สงวนลิขสิทธ์
นายไอลัน น้าวไกรศร

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ
ภาควิชาคณิตศาสตร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2551
ลิขสิทธ์ของบัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ผลคูณตรงและผลคูณอิสระของกรุป

โดย
นายไอลัน น้าวไกรสร

มหาวิทยาลัยศิลปากร สงวนลิขสิทธิ์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ
ภาควิชาคณิตศาสตร์
บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ปีการศึกษา 2551
ลิขสิทธิ์ของบัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

DIRECT PRODUCTS AND FREE PRODUCTS OF GROUPS

By

Olan Naowkraisorn

มหาวิทยาลัยศิลปากร สงวนลิขสิทธิ์

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

MASTER OF SCIENCE

Department of Mathematics

Graduate School

SILPAKORN UNIVERSITY

2008

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร อนุมัติให้การค้นคว้าอิสระเรื่อง “ ผลคุณตรงและ
ผลคุณอิสระของกรุป ” เสนอโดย นายโอดัน น้าวไกรสร เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ

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

อาจารย์ที่ปรึกษาการค้นคว้าอิสระ
ศาสตราจารย์ ดร.ฉวีวรรณ รัตนประเสริฐ

คณะกรรมการตรวจสอบการค้นคว้าอิสระ

มหาวิทยาลัยศิลปากร ส่วนวนลิขสิทธิ์
..... ประธานกรรมการ

(รองศาสตราจารย์ ดร.สีบสกุล อยู่ยืนยง)
...../...../.....

..... กรรมการ

(อาจารย์ ดร.จิตติ รักบุตร)
...../...../.....

..... กรรมการ

(ศาสตราจารย์ ดร.ฉวีวรรณ รัตนประเสริฐ)
...../...../.....

47308308 : สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ

คำสำคัญ : กรุป / ผลคูณตรง / ผลคูณอิสระ

ไอฉันทัน น้าวไกรศร : ผลคูณตรงและผลคูณอิสระของกรุป. อาจารย์ที่ปรึกษาการค้ันคว้าอิสระ : ศ.ดร.ฉวีวรรณ รัตนประเสริฐ. 40 หน้า.

ให้ G_1, G_2, \dots, G_n เป็นกรุป เราจะสร้างกรุปผลคูณตรงขึ้นจากผลคูณคาร์ทีเซียนของกรุปเหล่านี้ เราศึกษาผลคูณภายนอกและผลคูณภายในของกรุปตลอดจนความสัมพันธ์ของผลคูณทั้งสองแบบ

ต่อจากนั้นเราศึกษาเพื่อขยายการสร้างผลคูณตรงของกรุปจำนวนจำกัดไปยังกรุปจำนวนอนันต์ ทำให้พบว่าผลคูณตรงของกรุปจำนวนอนันต์เป็นผลคูณในคะติโกรีของกรุป และสุดท้ายเราสร้างกรุปซึ่งเป็นอิสระในคะติโกรีของกรุปจึงเป็นผลคูณอิสระของกรุปด้วย

มหาวิทยาลัยศิลปากร สงวนลิขสิทธ์

ภาควิชาคณิตศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ปีการศึกษา 2551

ลายมือชื่อนักศึกษา.....

ลายมือชื่ออาจารย์ที่ปรึกษาการค้ันคว้าอิสระ

47308308 : MAJOR : MATHEMATICS AND INFORMATION TECHNOLOGY

KEY WORDS : GROUP / DIRECT PRODUCTS / FREE PRODUCTS

OLAN NAOWKRAISORN : DIRECT PRODUCTS AND FREE PRODUCTS OF GROUPS. INDEPENDENT STUDY ADVISOR : PROF.CHAWEWAN RATANAPRASERT,Ph.D..
40 pp.

Let G_1, G_2, \dots, G_n be groups . We construct the direct product on the cartesian product of these groups . We study external direct product , internal direct product and theirs relationships .

Then we extend the result from finite direct product to infinite case . We found that the direct product of infinite groups is the product in category . Finally , we construct a group which is free in category of groups and so , it is a free product of groups .

มหาวิทยาลัยศิลปากร สงวนลิขสิทธิ์

Department of Mathematics Graduate School, Silpakorn University Academic Year 2008
Student's signature
Independent Study Advisor's signature

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยดี เพราะความกรุณาและความเมตตาจาก ศาสตราจารย์ ดร.ฉวีวรรณ รัตนประเสริฐ ที่ได้ให้คำปรึกษา คำแนะนำ ทำให้โลกทัศน์ทางวิชาการ ของข้าพเจ้ากว้างขึ้น ช่วยเติมเต็มและแก้ไขส่วนที่บกพร่อง จนทำให้การค้นคว้าอิสระฉบับนี้สำเร็จ ด้วยดี

ขอกราบขอบพระคุณ คณาจารย์ของภาควิชาคณิตศาสตร์ ภาควิชาสถิติ และ ภาควิชาคอมพิวเตอร์ มหาวิทยาลัยศิลปากรทุกท่าน ที่ได้ประสิทธิ์ประสาทวิชา พร้อมทั้งหยิบยื่น โอกาสทางการศึกษา จนทำให้ข้าพเจ้าได้พบความสำเร็จ สามารถนำความรู้ที่ได้ไปใช้ให้ก่อ ประโยชน์ได้อย่างถูกต้อง

ขอกราบขอบพระคุณ รองศาสตราจารย์ช่อฟ้า นิลรัตน์ ภาควิชาคณิตศาสตร์ คณะ วิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ ที่ได้มอบพื้นฐานที่ดีแก่ข้าพเจ้าตลอดความห่วงใยที่มี ต่อข้าพเจ้าเสมอมา

ขอขอบคุณเพื่อนๆ สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ สำหรับความ ช่วยเหลือและมีมิตรภาพอันดีงามระหว่างการศึกษา
สุดท้ายขอขอบคุณ ครอบครัวของข้าพเจ้าที่ได้ให้กำลังใจ มอบความรัก ดูแลและให้ การสนับสนุนทางการศึกษา จนทำให้ข้าพเจ้าประสบผลสำเร็จได้ในวันนี้

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	จ
กิตติกรรมประกาศ	ฉ
บทที่	
1 บทนำ	1
2 ความรู้พื้นฐาน.....	2
3 ผลคุณภายนอกและผลคุณภายใน.....	12
4 ผลคุณอนันต์และผลคุณอิสระของกรุป.....	26
บรรณานุกรม.....	39
ประวัติผู้วิจัย	40

มหาวิทยาลัยศิลปากร สงวนลิขสิทธิ์

บทที่ 1

บทนำ

เราศึกษาผลคุณภายนอกและผลคุณภายในของกรุปต่างๆ โดยเริ่มจากกรุปบนผลคูณคาร์ทีเซียนที่เรารู้จักกันเป็นอย่างดี จากการศึกษาทำให้เราพบว่าผลคุณภายนอกและผลคุณภายในมีความสัมพันธ์กัน อีกทั้งยังทำให้มีการศึกษาค้นคว้าต่อยอดออกไปในกรุปจำนวนอนันต์ ทำให้ได้กรุปที่เรียกว่ากรุปอิสระและผลคูณอิสระของกรุป ในการค้นคว้าอิสระนี้แบ่งการศึกษาออกเป็น 4 บท ดังนี้

บทที่ 2 ศึกษาทบทวนความรู้พื้นฐานที่ควรทราบซึ่งความรู้เหล่านี้จะถูกอ้างอิงหรือนำไปใช้ประกอบการพิสูจน์ในบทอื่นๆต่อไป

ในบทที่ 3 ศึกษาการสร้างกรุปบนผลคูณคาร์ทีเซียนจำกัดที่เรียกว่าผลคูณตรงหรือผลคูณภายนอกและศึกษาความสัมพันธ์ระหว่างผลคุณภายนอกและผลคุณภายในของกรุปและสมบัติที่สำคัญต่างๆที่เกี่ยวข้องกับผลคุณภายนอกและผลคุณภายใน

ในบทที่ 4 ศึกษาขยายการสร้างผลคูณตรงไปยังผลคูณตรงของกรุปจำนวนอนันต์และสร้างเซตของคำลดทอนขึ้นเพื่อให้เป็นเอกภาพของกรุปอิสระและศึกษาทฤษฎีบทสำคัญที่เกี่ยวข้องกับกรุปอิสระ ศึกษาผลคูณอิสระของกรุปตลอดจนสมบัติของผลคูณอิสระ

บทที่ 2 ความรู้พื้นฐาน

ก่อนจะเริ่มต้นศึกษาเนื้อหาของผลคูณตรง ขอทบทวนความรู้พื้นฐานที่จำเป็นต่อการค้นคว้าอิสระฉบับนี้โดยขอละการพิสูจน์ไว้ และความรู้เหล่านี้จะถูกอ้างอิงหรือนำไปใช้ประกอบการพิสูจน์ในหัวข้อต่อไป

ตลอดการค้นคว้าอิสระนี้ จะขอใช้สัญลักษณ์ Z แทนเซตของจำนวนเต็มทั้งหมด

2.1 บทนิยาม ให้ $a, b \in Z$ เรากล่าวว่า a หาร b ลงตัว (a divides b) ถ้ามี $k \in Z$ ซึ่ง $b = ka$ และเราแทนความหมายนี้ด้วยสัญลักษณ์ $a|b$

ถ้า $a|b$ เราเรียก b ว่า **พหุคูณ** (multiple) ของ a และเรียก a ว่า **ตัวหาร** (divisor) ของ b

2.2 ทฤษฎีบท ให้ $a, b, c \in Z$ ถ้า $a|b$ และ $b|c$ แล้ว $a|c$

2.3 บทนิยาม ให้ $a, b \in Z$ และ d เป็นจำนวนเต็มบวก เรากล่าวว่า d เป็น **ตัวหารร่วมมาก** (greatest common divisor) ของ a และ b และเขียนแทน d ด้วยสัญลักษณ์ $\gcd(a, b)$ ถ้า 1. $d|a$ และ $d|b$
และ 2. ถ้า c เป็นจำนวนเต็มบวกซึ่ง $c|a$ และ $c|b$ แล้ว $c \leq d$

2.4 บทนิยาม ให้ a และ b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์ เรากล่าวว่า a และ b เป็น **จำนวนเฉพาะสัมพัทธ์** (relatively prime) ถ้า $\gcd(a, b) = 1$

2.5 บทนิยาม ให้ $a, b \in Z$ และ c เป็นจำนวนเต็มบวก เรากล่าวว่า c เป็น **ตัวคูณร่วมน้อย** (least common multiple) ของ a และ b และเขียนแทน c ด้วยสัญลักษณ์ $\text{lcm}(a, b)$ ถ้า 1. $a|c$ และ $b|c$
และ 2. ถ้า d เป็นจำนวนเต็มซึ่ง $a|d$ และ $b|d$ แล้ว $c \leq d$

2.6 **ทฤษฎีบท** ให้ m และ n เป็นจำนวนเต็มบวก ถ้า $\text{lcm}(m, n) = c$ และ $\text{gcd}(m, n) = d$ แล้ว $mn = cd$

2.7 **บทนิยาม** ให้ A เป็นเซตที่ไม่ใช่เซตว่าง เรากล่าวว่า σ เป็นกาธิยงสับเปลี่ยน (permutation) บน A ถ้า σ เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก A ไป A

ถ้า A เป็นเซตจำกัดและ $B = \{x_1, x_2, \dots, x_k\}$ เป็นเซตย่อยของ A และ σ เป็นวิธีเรียงสับเปลี่ยนของ B ซึ่ง $\sigma: x_1 \rightarrow x_2, \sigma: x_2 \rightarrow x_3, \dots, \sigma: x_{k-1} \rightarrow x_k, \sigma: x_k \rightarrow x_1$ เรากล่าวว่า σ เป็นวัฏจักรที่มีความยาวเท่ากับ k และในกรณีเช่นนี้จะเขียนแทน σ ด้วยสัญลักษณ์ $(x_1 x_2 \dots x_k)$

2.8 **ตัวอย่าง** ให้ $A = \{1, 2, 3\}$ และให้ $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ แล้ว

σ_1 และ σ_2 เป็นวิธีเรียงสับเปลี่ยนบน A โดยที่ $\sigma_1: 1 \rightarrow 2, \sigma_1: 2 \rightarrow 3, \sigma_1: 3 \rightarrow 1$ และ

$\sigma_2: 1 \rightarrow 3, \sigma_2: 2 \rightarrow 1, \sigma_2: 3 \rightarrow 2$ เราจึงแทน σ_1 ได้ด้วย (123) และแทน σ_2 ได้ด้วย (132)

2.9 **บทนิยาม** ให้ m เป็นจำนวนเต็มบวก และให้ a และ b เป็นจำนวนเต็ม เรากล่าวว่า a สมภาคกับ b มอดุโล m (a is congruence to b modulo m) ถ้า m เป็นตัวหารของ $a - b$ และเขียนแทนความหมายนี้ด้วยสัญลักษณ์ $a \equiv b \pmod{m}$

ขอให้สังเกตว่าการสมภาค (congruence) เป็นความสัมพันธ์สมมูล (equivalence relations) บน Z นั่นคือสำหรับแต่ละ $m \in Z$

1. $a \equiv a \pmod{m}$ สำหรับทุกๆ $a \in Z$
2. ถ้า $a \equiv b \pmod{m}$ แล้ว $b \equiv a \pmod{m}$ สำหรับทุกๆ $a, b \in Z$
3. ถ้า $a \equiv b \pmod{m}$ และ $b \equiv c \pmod{m}$ แล้ว $a \equiv c \pmod{m}$ สำหรับทุกๆ $a, b, c \in Z$

ดังนั้น “การสมภาค” จะทำให้เกิดผลแบ่งกัน (partition) บน Z

2.10 **บทนิยาม** ให้ m เป็นจำนวนเต็มบวก และให้ k เป็นจำนวนเต็ม เราใช้สัญลักษณ์ \bar{k} แทนเซตของจำนวนเต็มทั้งหมดที่ลงรอยกันกับ k มอดุโล m นั่นคือ

$$\bar{k} = \{x \in Z \mid x \equiv k \pmod{m}\}$$

เราเรียกเซต $\{\bar{k} \mid 0 \leq k < n\}$ ซึ่งเป็นผลแบ่งกันหนึ่งของ Z ว่า **ชั้นสมมูลมอดุโล n**
(equivalence class modulo n)

สังเกตว่า ชั้นสมมูลมอดุโล n ประกอบด้วยสมาชิก n ตัว คือ $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$
และเรานิยมเขียนแทนชั้นสมมูลมอดุโล n ด้วย Z_n ดังนั้น

$$Z_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

2.11 บทนิยาม ให้ G เป็นเซตที่ไม่ใช่เซตว่าง และ $O: G \times G \rightarrow G$ เรากล่าวว่าโครงสร้าง
($G; O$) เป็น **กรุป (Group)** ถ้า

1. O มีสมบัติการเปลี่ยนหมู่ (associative law) บน G นั่นคือ $(a Ob) Oc = a O (b Oc)$
สำหรับทุก $a, b, c \in G$

2. มี $e \in G$ เป็นเอกลักษณ์ (identity) ของ G ภายใต้ O นั่นคือ $a O e = a = e O a$
สำหรับทุก $a \in G$

3. สำหรับแต่ละสมาชิกของ G มีตัวผกผัน (inverse) ภายใต้ O นั่นคือแต่ละ $a \in G$ มี
 $b \in G$ ซึ่ง $a Ob = e \equiv b Oa$ และตัวผกผันของแต่ละ $a \in G$ มีเพียงตัวเดียวจึงนิยมใช้
สัญลักษณ์ a^{-1} แทนตัวผกผันของ a

เรากล่าวว่ากรุป ($G; O$) เป็น **กรุปสลับที่ (abelian group)** ถ้า O มีสมบัติการสลับ
ที่บน G นั่นคือ $a Ob = b Oa$ สำหรับทุก $a, b \in G$

2.12 บทนิยาม ให้ ($G; O$) เป็นกรุป เราเรียกจำนวนสมาชิกทั้งหมดในกรุป G ว่าขนาดของ G
และแทนขนาดของ G ด้วยสัญลักษณ์ $|G|$ เรากล่าวว่ากรุป ($G; O$) เป็น **กรุปจำกัด (finite
group)** ถ้าขนาดของเซต G เป็นจำนวนจำกัด และกล่าวว่า ($G; O$) เป็น **กรุปอนันต์ (infinite
group)** ถ้า ($G; O$) ไม่เป็นกรุปจำกัด

หมายเหตุ : ในการกล่าวถึงกรุป ($G; O$) บางครั้งเราจะละการดำเนินการ O บน G
โดยกล่าวเพียงว่า G เป็นกรุปและ $a Ob$ แทนด้วย ab ทุกๆ $a, b \in G$

2.13 ตัวอย่าง ให้ n เป็นจำนวนเต็มบวก และให้ $Z_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ และให้
 $+: Z_n \times Z_n \rightarrow Z_n$ นิยามโดย $\bar{a} + \bar{b} = \overline{a+b}$ สำหรับทุก $\bar{a}, \bar{b} \in Z_n$ แล้ว ($Z_n; +$) เป็นกรุป
สลับที่และเป็นกรุปจำกัด

บทพิสูจน์

1. ให้ $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in Z_n$ ซึ่ง $\bar{a} = \bar{c}$ และ $\bar{b} = \bar{d}$ แล้วจะมี $s, t \in Z$ ที่ทำให้ $a = c + ns$ และ $b = d + nt$ แล้ว $\bar{a} + \bar{b} = \overline{a+b} = \overline{c+ns+d+nt} = \overline{c+d+n(s+t)} = \overline{c+d} = \bar{c} + \bar{d}$ ดังนั้น $+$ เป็นฟังก์ชัน

2. ให้ $\bar{a}, \bar{b}, \bar{c} \in Z_n$ แล้ว

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

ดังนั้น $+$ มีสมบัติการเปลี่ยนหมู่บน Z_n

3. มี $\bar{0} \in Z_n$ ซึ่ง $\bar{a} + \bar{0} = \overline{a+0} = \bar{a} = \bar{0} + \bar{a} = \overline{0+a}$ สำหรับทุก $\bar{a} \in Z_n$

ดังนั้น $\bar{0}$ เป็นเอกลักษณ์ของ Z_n ภายใต้ $+$

4. ให้ $\bar{a} \in Z_n$ เลือก $\bar{b} = \overline{n-a} \in Z_n$ ซึ่งทำได้

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{a+(n-a)} = \bar{0} = \bar{e} = \bar{0} = \overline{(n-a)+a} = \bar{b} + \bar{a} = \bar{b} + \bar{a}$$

ดังนั้น \bar{b} เป็นตัวผกผันของ \bar{a} ภายใต้ $+$

5. ให้ $\bar{a}, \bar{b} \in Z_n$ แล้ว $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$ นั่นคือ $+$ มีสมบัติการสลับที่บน Z_n

เพราะฉะนั้น Z_n เป็นกรุปสลับที่

บททฤษฎีบทเกี่ยวกับพีลากร ส่วนวนลิขสิทธิ์

เพราะว่า $Z_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ มีสมาชิกจำนวน n ตัว เพราะฉะนั้น Z_n เป็นกรุปจำกัด ■

2.14 ตัวอย่าง ให้ $A = \{1, 2, \dots, n\}$ และให้ S_n แทนเซตของวิธีเรียงสับเปลี่ยนทั้งหมดบน A และให้ \circ แทนการประกอบ (composition) ระหว่างฟังก์ชันแล้ว $(S_n; \circ)$ เป็นกรุป เราเรียก $(S_n; \circ)$ ว่ากรุปสมมาตร (symmetric group) ขนาด n

บทพิสูจน์

1. เป็นที่ทราบกันดีว่า ผลประกอบระหว่างฟังก์ชันเป็นการดำเนินการซึ่งสอดคล้องสมบัติการเปลี่ยนหมู่ ดังนั้น \circ มีสมบัติการเปลี่ยนหมู่บน S_n ด้วย

2. ให้ α เป็นฟังก์ชันเอกลักษณ์ นั่นคือ $\alpha: A \rightarrow A$ นิยามโดย $\alpha(a) = a$ สำหรับทุก $a \in A$ แล้ว $\alpha \in S_n$ และให้ $\sigma \in S_n$ แล้ว

$$(\sigma \circ \alpha)(a) = \sigma(\alpha(a)) = \sigma(a) \text{ และ } (\alpha \circ \sigma)(a) = \alpha(\sigma(a)) = \sigma(a)$$

ทำให้ได้ $\sigma \circ \alpha = \sigma = \alpha \circ \sigma$ ดังนั้น α เป็นเอกลักษณ์ของ S_n ภายใต้ \circ

3. ให้ $\sigma \in S_n$ และให้ $\delta: A \rightarrow A$ นิยามโดย $\sigma(a) = b \leftrightarrow \delta(b) = a$ สำหรับ
 ทุกๆ $a, b \in A$

ให้ $a, b \in A$ โดยที่ $\sigma(a) = b$ แล้ว $\delta(b) = a$ ทำให้ได้

$$(\delta \circ \sigma)(a) = \delta(\sigma(a)) = \delta(b) = a = \alpha(a) \text{ และ}$$

$$(\sigma \circ \delta)(b) = \sigma(\delta(b)) = \sigma(a) = b = \alpha(b)$$

ดังนั้น $\delta \circ \sigma = \alpha = \sigma \circ \delta$

เพราะฉะนั้น δ เป็นตัวผกผันของ σ ภายใต้ α

เพราะฉะนั้น $(S_n; \alpha)$ เป็นกรุป

2.15 **บทนิยาม** ให้ $(G; \alpha)$ เป็นกรุป และให้ $a \in G$ ถ้ามี n เป็นจำนวนเต็มบวกตัวน้อยที่สุด
 ซึ่ง $a^n = e$ เราเรียกว่า n เป็น**อันดับของ a** (order of a) และจะแทนอันดับของ a ด้วย
 สัญลักษณ์ $o(a)$ และในกรณีที่ไม่มีจำนวนเต็มบวก m ใดๆ ซึ่ง $a^m = e$ เราจะกล่าวว่า
 a มี**อันดับอนันต์** (infinite order)

2.16 **ตัวอย่าง** กรุปสมมาตรบนเซตขนาด 3 คือ S_3 ซึ่งเขียนแจกแจงสมาชิกทั้งหมดของ S_3
 ได้ดังนี้

$$S_3 = \{ (1), (12), (13), (23), (123), (132) \}$$

แล้วเห็นได้ชัดว่าอันดับของ (1) เท่ากับ 1

เนื่องจาก $(123)^2 = (123)(123) = (132)$ และ

$$(123)^3 = (123)^2(123) = (132)(123) = (1)$$

ดังนั้นอันดับของ (123) เท่ากับ 3

2.17 **ทฤษฎีบท** ให้ G เป็นกรุป $a \in G$ ให้ n และ s เป็นจำนวนเต็มบวก ถ้า n เป็นอันดับของ a
 แล้ว $a^s = e$ ก็ต่อเมื่อ $n|s$

2.18 **บทนิยาม** ให้ $(G; \alpha)$ เป็นกรุป ถ้ามี $a \in G$ ซึ่ง $G = \{a^r \mid r \in \mathbb{Z}\}$ เราเรียก G ว่า

กรุปวัฏจักร (cyclic group) และเรียก a ว่า**ตัวก่อกำเนิด** (generator) สำหรับ G และเขียน
 แทน G ด้วยสัญลักษณ์ $\langle a \rangle$

ตัวอย่างเช่น $(Z_n; +)$ เป็นกรุปวัฏจักร โดยมี 1 เป็นตัวก่อกำเนิด เพราะว่า $Z_n = \langle 1 \rangle$ แต่ $(S_n; \circ)$ ไม่เป็นกรุปวัฏจักร เมื่อ $n > 2$ เป็นต้น

2.19 ทฤษฎีบท $(G; \circ)$ เป็นกรุปวัฏจักรขนาดจำกัด ก็ต่อเมื่อมี $a \in G$ ซึ่ง $o(a) = |G|$

2.20 ทฤษฎีบท ถ้า $(G; \circ)$ เป็นกรุปวัฏจักร แล้ว $(G; \circ)$ เป็นกรุปสลับที่

2.21 บทนิยาม ให้ $(G; \circ)$ เป็นกรุป และให้ $H \subseteq G$ โดยที่ $H \neq \emptyset$ เรากล่าวว่า H เป็นกรุปย่อย (subgroup) ของ G ถ้า $(H; \circ)$ เป็นกรุป

2.22 ทฤษฎีบท ให้ $(G; \circ)$ เป็นกรุป และให้ $H \subseteq G$ โดยที่ $H \neq \emptyset$ แล้ว H เป็นกรุปย่อยของ G ถ้า

1. H มีคุณสมบัติปิดภายใต้ \circ นั่นคือ $h \circ k \in H$ สำหรับทุกๆ $h, k \in H$

2. สำหรับแต่ละ $a \in H$ มี $a^{-1} \in H$ เป็นตัวผกผัน ภายใต้ \circ

2.23 ตัวอย่าง พิจารณากรุปชั้นสมมูลมอดุโล 5 ซึ่งคือ $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ แล้ว

$H = \{\bar{0}, \bar{1}, \bar{4}\}$ เป็นกรุปย่อยของ Z_5

บทพิสูจน์ พิจารณาตารางเคย์เลย์ของ H ดังนี้

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

จะเห็นว่า $\bar{0}$ เป็นเอกลักษณ์ของ H ภายใต้ $+$ นอกจากนั้น $\bar{0}, \bar{1}$ และ $\bar{4}$ เป็นตัวผกผันของ $\bar{0}, \bar{4}$ และ $\bar{1}$ ตามลำดับ ดังนั้นแต่ละ $\bar{a} \in Z_5$ มีตัวผกผันเพราะฉะนั้น $(H; +)$ เป็นกรุป ดังนั้น $(H; +)$ เป็นกรุปย่อยของ $(Z_5; +)$ ■

2.24 **บทนิยาม** ให้ G เป็นกรุป n เป็นจำนวนเต็มบวกและ G_1, G_2, \dots, G_n เป็นกรุปย่อยของ G จะใช้สัญลักษณ์ $G_1 G_2 \dots G_n$ แทนเซตย่อยของ G ซึ่งกำหนดโดย

$$G_1 G_2 \dots G_n = \{g_1 g_2 \dots g_n \mid g_i \in G_i \text{ สำหรับแต่ละ } i = 1, 2, \dots, n\}$$

ตัวอย่างเช่น ในกรุป S_3 ให้ $H = \{(1), (12)\}$ และ $K = \{(1), (13)\}$ แล้ว H และ K เป็นกรุปย่อยของ S_3 และทำให้ได้

$$HK = \{(1), (12), (13), (12)(13)\} = \{(1), (12), (13), (132)\}$$

ขอให้สังเกตว่า HK ไม่เป็นกรุปย่อยของ S_3

2.25 **บทนิยาม** ให้ G เป็นกรุป H เป็นกรุปย่อยของ G และ $a \in G$ เราเรียก

$aH = \{ah \mid h \in H\}$ ว่าเซตร่วมทางซ้ายของ H ใน G (left coset of H in G) และเรียก

$Ha = \{h \mid h \in H\}$ ว่าเซตร่วมทางขวาของ H ใน G (right coset of H in G)

2.26 **บทนิยาม** ให้ G เป็นกรุป ให้ H เป็นกรุปย่อยของ G เรากล่าวว่า $(H; \circ)$ เป็นกรุปย่อยปกติ (normal subgroup) ถ้า $aH = Ha$ สำหรับทุกๆ $a \in G$

2.27 **ทฤษฎีบท** ให้ G เป็นกรุป และ H เป็นกรุปย่อยของ G แล้ว H เป็นกรุปย่อยปกติก็ต่อเมื่อ $aHa^{-1} \subseteq H$ สำหรับทุกๆ $a \in G$

2.28 **ทฤษฎีบท** ให้ G เป็นกรุป ถ้า G_1 และ G_2 เป็นกรุปย่อยปกติของ G แล้ว $G_1 G_2$ เป็นกรุปย่อยของ G

2.29 **ทฤษฎีบท** ให้ G เป็นกรุป และ n เป็นจำนวนเต็มบวก ถ้า G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของ G สำหรับทุกๆ $i = 1, 2, \dots, n$ แล้ว $G_1 G_2 \dots G_n$ เป็นกรุปย่อยของ G

2.30 **บทนิยาม** ให้ $(G; *)$ และ $(H; \circ)$ เป็นกรุป และให้ $\phi: G \rightarrow H$ เรากล่าวว่า ϕ เป็น **สัทิสต์ฐาน** (homomorphism) จาก G ไปยัง H ถ้า $\phi(x * y) = \phi(x) \circ \phi(y)$ สำหรับทุก $x, y \in G$

ถ้า ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่งจะเรียก ϕ ว่า **เอกสัฐาน** (monomorphism)

ถ้า ϕ เป็นฟังก์ชันทั่วถึงจะเรียก ϕ ว่า **อุปรีฐาน** (epimorphism)

ถ้า ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่งและเป็นฟังก์ชันทั่วถึงจะเรียก ϕ ว่า **สมสัณฐาน** (isomorphism)

ถ้ามี $\phi: G \rightarrow H$ เป็นสัทิสสัณฐาน ชนิดหนึ่งต่อหนึ่งแบบทั่วถึง เราจะกล่าวว่า G **สมสัณฐานกัน** (isomorphic) กับ H และแทนความหมายนี้ด้วยสัญลักษณ์ $G \cong H$

2.31 **บทนิยาม** ให้ G และ H เป็นกรุป ถ้ามีสัทิสสัณฐาน ชนิดทั่วถึงจาก G ไปยัง H เรากล่าวว่า H เป็น **ภาพสัทิสสัณฐาน** (homomorphic image) ของ G

2.32 **บทนิยาม** ให้ G และ H เป็นกรุป และ $\phi: G \rightarrow H$ เป็นสัทิสสัณฐาน ถ้า S เป็นกรุปย่อยของ H เรานิยาม $\phi^{-1}(S) = \{x \in G \mid \phi(x) \in S\}$ และเรียกว่า **ภาพผกผันสัทิสสัณฐาน** (homomorphic inverse image) ของ S

2.33 **ทฤษฎีบท** ถ้า G และ H เป็นกรุป และ ϕ เป็นสัทิสสัณฐาน จาก G ไปยัง H และ K เป็นกรุปย่อยของ H แล้ว $\phi^{-1}(K)$ เป็นกรุปย่อยของ G

2.34 **บทนิยาม** ให้ G เป็นกรุป ให้ H เป็นกรุปที่มี e_H เป็นเอกลักษณ์ และให้ $\phi: G \rightarrow H$ เป็นสมสัณฐาน ให้

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

เราเรียก $\ker \phi$ ว่า **แก่นกลาง** (kernel) ของ ϕ

2.35 **ทฤษฎีบท** ให้ G และ H เป็นกรุป และให้ $\phi: G \rightarrow H$ เป็นสมสัณฐาน แล้วแก่นกลางของ ϕ เป็นกรุปย่อยปกติของ G

2.36 **ทฤษฎีบท** ให้ G เป็นกรุปที่มี e_G เป็นเอกลักษณ์ และให้ H เป็นกรุปและให้ $\phi: G \rightarrow H$ เป็นสมสัณฐาน แล้ว ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่งก็ต่อเมื่อ $\ker \phi = \{e_G\}$

2.37 **บทนิยาม** **คะติโกรี** (category) ประกอบด้วย

1) กลุ่มของ **วัตถุ** (object)

2) สำหรับแต่ละคู่ของวัตถุ A และ B จะมี $f: A \rightarrow B$ เราเรียกว่า **สัณฐาน** (morphism) จาก A ไปยัง B

3) สำหรับแต่ละคู่ของสัจฐาน u และ v จะมี \circ เป็นการดำเนินการทวิภาค (binary operation) ระหว่าง u และ v เราเรียกว่าการประกอบ (composition) ของสัจฐาน และสัจฐานจะสอดคล้องกฎต่อไปนี้

1) ถ้า u เป็นสัจฐานจาก A ไปยัง B และ v เป็นสัจฐานจาก B ไปยัง C จะมีสัจฐาน $u \circ v$ เป็นสัจฐานจาก A ไปยัง C

2) ถ้า u เป็นสัจฐานจาก A ไปยัง B v เป็นสัจฐานจาก B ไปยัง C และ w เป็นสัจฐานจาก C ไปยัง D แล้ว $(u \circ v) \circ w = u \circ (v \circ w)$ นั่นคือสัจฐานมีสมบัติการเปลี่ยนหมู่

3) ถ้า u เป็นสัจฐานจาก A ไปยัง B แล้วจะมีสัจฐานจาก A ไปยัง A เขียนแทนด้วยสัญลักษณ์ I_a และสัจฐานจาก B ไปยัง B เขียนแทนด้วยสัญลักษณ์ I_b ซึ่ง $I_a \circ u = u$ และ $u \circ I_b = u$ เราเรียก I_a และ I_b ว่าเอกลักษณ์สัจฐานของ A และ เอกลักษณ์สัจฐานของ B ตามลำดับ

2.38 ทฤษฎีบท ให้ $\{A_i | i \in I\}$ เป็นวงศ์ของวัตถุในคตโกรี \mathcal{G} แล้วจะมี P เป็นวัตถุในคตโกรี

\mathcal{G} และ $\{\pi_i : P \rightarrow A_i | i \in I\}$ เป็นวงศ์ของสัจฐานที่ทำให้ ถ้า B เป็นวัตถุในคตโกรี \mathcal{G}

และ $\{\varphi_i : B \rightarrow A_i | i \in I\}$ เป็นวงศ์ของสัจฐานแล้วจะมีสัจฐาน $\varphi : B \rightarrow P$ เพียงหนึ่งเดียวซึ่ง

$$\pi_i \circ \varphi = \varphi_i \text{ สำหรับทุกๆ } i \in I$$

เรากล่าวว่า P เป็นผลคูณ (product) ของวงศ์ $\{A_i | i \in I\}$

2.39 บทแทรก ให้ \mathcal{G} เป็นคตโกรีของกรุป ให้ X เป็นเซตไม่ว่างแล้วจะมี F เป็นกรุปในคตโกรี

\mathcal{G} และ $i : X \rightarrow F$ เป็นการส่งของเซตที่ทำให้ ถ้า A เป็นกรุปและ f เป็นการส่งจาก X ไปยัง A

แล้วจะมีสัจฐาน $\bar{f} : F \rightarrow A$ เพียงหนึ่งเดียวซึ่ง $\bar{f} \circ i = f$ สำหรับทุกๆ $i \in I$ เรากล่าวว่า F เป็นผลคูณ

2.40 ทฤษฎีบท ให้ $\{A_i | i \in I\}$ เป็นวงศ์ของวัตถุในคตโกรี \mathcal{G} แล้วจะมี S เป็นวัตถุในคตโกรี

\mathcal{G} และ $\{i_i : A_i \rightarrow S | i \in I\}$ เป็นวงศ์ของสัจฐานที่ทำให้ ถ้า B เป็นวัตถุในคตโกรี \mathcal{G}

และ $\{\Psi_i : A_i \rightarrow B | i \in I\}$ เป็นวงศ์ของสัจฐานแล้วจะมีสัจฐาน $\Psi : S \rightarrow B$ เพียงหนึ่งเดียวซึ่ง

$$\Psi_i \circ i_i = \Psi_i \text{ สำหรับทุกๆ } i \in I$$

เรากล่าวว่า S เป็นผลคูณอิสระ (free product) ของวงศ์ $\{A_i | i \in I\}$

2.41 บทแทรก ให้ $\{G_i | i \in I\}$ เป็นวงศ์ของกรุปในคะติโกรี \mathcal{G} จะมี S เป็นกรุปใน \mathcal{G} และ $\{\iota_i : G_i \rightarrow S | i \in I\}$ เป็นวงศ์ของสัณฐานแล้วจะมีกรุป B และวงศ์ของสัณฐาน $\{\Psi_i : G_i \rightarrow B | i \in I\}$ ซึ่ง $\Psi : S \rightarrow B$ เป็นสัณฐานเพียงหนึ่งเดียวซึ่ง $\Psi \iota_i = \Psi_i$ สำหรับทุกๆ $i \in I$ เรากล่าวว่า S เป็นผลคูณอิสระของวงศ์ $\{G_i | i \in I\}$
 เราเรียกกรุป S ซึ่งเป็นผลคูณอิสระว่ากรุปอิสระ

มหาวิทยาลัยศิลปากร สงวนลิขสิทธิ์

บทที่ 3
ผลคูณภายนอกและผลคูณภายใน

ในบทนี้จะกล่าวถึงการนำกรุปจำนวนจำกัดกรุปมาสร้างกรุปขึ้นใหม่ เราเรียกว่ากรุปผลคูณตรงและยกตัวอย่างกรุปผลคูณตรงตลอดจนศึกษาทฤษฎีบทต่างที่สำคัญของผลคูณตรง

3.1 ทฤษฎีบท ให้ G_1, G_2, \dots, G_n เป็นกรุป และ **ผลคูณคาร์ทีเซียน** (cartesian product) ของ G_1, G_2, \dots, G_n เขียนแทนด้วย $G_1 \times G_2 \times \dots \times G_n$ นิยามโดย

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

และให้ $\circ: (G_1 \times G_2 \times \dots \times G_n) \times (G_1 \times G_2 \times \dots \times G_n) \rightarrow (G_1 \times G_2 \times \dots \times G_n)$

นิยามโดย $(g_1, g_2, \dots, g_n) \circ (h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n)$

สำหรับทุก (g_1, g_2, \dots, g_n) และ (h_1, h_2, \dots, h_n) ใน $G_1 \times G_2 \times \dots \times G_n$

แล้ว $(G_1 \times G_2 \times \dots \times G_n; \circ)$ เป็นกรุป

บทพิสูจน์ ให้ G_1, G_2, \dots, G_n เป็นกรุป

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

$$\begin{aligned} &\text{แล้ว} \quad ((g_1, g_2, \dots, g_n) \circ (h_1, h_2, \dots, h_n)) \circ (i_1, i_2, \dots, i_n) \\ &= (g_1 h_1, g_2 h_2, \dots, g_n h_n) \circ (i_1, i_2, \dots, i_n) \\ &= ((g_1 h_1) i_1, (g_2 h_2) i_2, \dots, (g_n h_n) i_n) \\ &= (g_1 (h_1 i_1), g_2 (h_2 i_2), \dots, g_n (h_n i_n)) \\ &= (g_1, g_2, \dots, g_n) \circ (h_1 i_1, h_2 i_2, \dots, h_n i_n) \\ &= (g_1, g_2, \dots, g_n) \circ ((h_1, h_2, \dots, h_n) \circ (i_1, i_2, \dots, i_n)) \end{aligned}$$

ดังนั้น \circ มีสมบัติการเปลี่ยนหมู่บน $G_1 \times G_2 \times \dots \times G_n$

2. ให้ e_i เป็นเอกลักษณ์บน G_i สำหรับ $i=1,2,\dots,n$ แล้ว

$$(e_1, e_2, \dots, e_n) \in G_1 \times G_2 \times \dots \times G_n \text{ ให้ } (g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n \text{ แล้ว}$$

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

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

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

เพราะว่าแต่ละ G_1, G_2, \dots, G_n เป็นกรุป ดังนั้น $g_i^{-1} \in G_i$ สำหรับทุกๆ $i=1, 2, \dots, n$

ทำให้ได้ว่า $(g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}) \in G_1 \times G_2 \times \dots \times G_n$ โดยที่

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

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

มหาวิทยาลัยศิลปากร ส่วนวนลิขสิทธิ์

3.2 บทนิยาม เราเรียกกรุป $(G_1 \times G_2 \times \dots \times G_n; \circ)$ ในทฤษฎีบท 3.1 ว่าผลคูณตรง (direct product) ของกรุป G_1, G_2, \dots, G_n

3.3 ตัวอย่าง พิจารณากรุปสมมาตร $S_2 = \{(1), (12)\}$ และ

$S_3 = \{(1), (12), (13), (23), (123), (132)\}$ แล้วผลคูณตรงของ S_2 กับ S_3 คือกรุปบนเซต

$$S_2 \times S_3 = \left\{ \begin{aligned} &((1), (1)), ((1), (12)), ((1), (13)), ((1), (23)), \\ &((1), (123)), ((1), (132)), ((12), (1)), ((12), (12)), \\ &((12), (13)), ((12), (23)), ((12), (123)), ((12), (132)) \end{aligned} \right\}$$

ที่มีการคูณ $\cdot : (S_2 \times S_3) \times (S_2 \times S_3) \rightarrow (S_2 \times S_3)$ กำหนดโดย

$(\sigma, \tau) \cdot (\alpha, \delta) = (\sigma\alpha, \tau\delta)$ เมื่อ $\sigma\alpha$ และ $\tau\delta$ คือผลประกอบระหว่างฟังก์ชันใน S_2 และ S_3 ตามลำดับ ตัวอย่างเช่น

$$((12), (123)) \cdot ((1), (132)) = ((12)(1), (123)(132)) = ((12), (1)) \text{ เป็นต้น} \blacksquare$$

3.4 ตัวอย่าง ผลคูณตรงของกลุ่ม $Z_2 = \{\bar{0}, \bar{1}\}$ และ $Z_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ คือกลุ่ม

$$Z_2 \times Z_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}$$

ที่มีการบวก $+$: $(Z_2 \times Z_3) \times (Z_2 \times Z_3) \rightarrow (Z_2 \times Z_3)$ กำหนดโดย

$(a, b) + (c, d) = (a+c, b+d)$ เมื่อ $a+c$ และ $b+d$ เป็นการบวกใน Z_2 และ Z_3 ตามลำดับ ตัวอย่างเช่น $(\bar{1}, \bar{1}) \cdot (\bar{1}, \bar{2}) = (\bar{1}+\bar{1}, \bar{1}+\bar{2}) = (\bar{0}, \bar{0})$ เป็นต้น \blacksquare

สังเกตว่าจำนวนสมาชิกในผลคูณตรงเท่ากับผลคูณของสมาชิกในกลุ่มที่นำมาสร้างเป็นผลคูณตรงนั้นๆ เช่นตัวอย่างที่ 3.3 จำนวนสมาชิกของ S_2 เท่ากับ 2 และจำนวนสมาชิกของ S_3 เท่ากับ 6 ดังนั้นจำนวนสมาชิกของผลคูณตรงของ S_2 กับ S_3 เท่ากับ $2 \times 6 = 12$ เป็นต้น

นอกจากนี้ขอให้สังเกตว่าการดำเนินการระหว่างสมาชิกในผลคูณตรงสอดคล้องกับการดำเนินการของกลุ่มที่นำมาสร้างเป็นผลคูณตรงนั้นๆ ดังตัวอย่างที่ 3.5

3.5 ตัวอย่าง ให้ m และ n เป็นจำนวนเต็มบวก แล้วผลคูณตรงของกลุ่ม Z_m และ S_n คือกลุ่ม

$$Z_m \times S_n = \{(\bar{a}, \alpha) \mid \bar{a} \in Z_m; \alpha \in S_n\}$$

ที่มีการดำเนินการ \cdot : $(Z_m \times S_n) \times (Z_m \times S_n) \rightarrow (Z_m \times S_n)$ กำหนดโดย

$(\bar{a}, \alpha) \cdot (\bar{b}, \sigma) = (\overline{a+b}, \alpha\sigma)$ เมื่อ $\overline{a+b}$ และ $\alpha\sigma$ เป็นการดำเนินการใน Z_m และ S_n ตามลำดับ \blacksquare

3.6 บทนิยาม ให้ G, G_1, G_2, \dots, G_n เป็นกลุ่ม เรากล่าวว่า G เป็น **ผลคูณภายนอก**

(external direct product) ของ G_1, G_2, \dots, G_n ถ้า G สมมูลฐานกับผลคูณตรงของ

$$G_1, G_2, \dots, G_n$$

เพราะว่าผลคูณตรงเป็นกลุ่ม เราจึงจะศึกษาต่อไปถึงการหาอันดับของสมาชิกในผลคูณตรง $G_1 \times G_2 \times \dots \times G_n$ ว่ามีความสัมพันธ์กับสมาชิกในแต่ละกลุ่ม G_1, G_2, \dots, G_n อย่างไร

3.7 ทฤษฎีบท ให้ G_1, G_2, \dots, G_n เป็นกรุปจำกัดจำนวน n กรุป ($n \geq 1$) แล้ว

$$o(g_1, g_2, \dots, g_n) = \text{lcm}(o(g_1), o(g_2), \dots, o(g_n)) \text{ สำหรับทุกๆ}$$

$$(g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n$$

บทพิสูจน์ ให้ G_1, G_2, \dots, G_n เป็นกรุปจำกัด และ $(g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n$

ให้ t_i เป็นอันดับของ g_i สำหรับ $i = 1, 2, \dots, n$ และให้ t เป็นอันดับของ (g_1, g_2, \dots, g_n) แล้ว

$$(g_1, g_2, \dots, g_n)^t = (e_1, e_2, \dots, e_n)$$

ให้ s เป็นตัวคูณร่วมน้อยของ t_1, t_2, \dots, t_n แล้วสำหรับแต่ละ $1 \leq i \leq n$ จะมี $m_i \in \mathbb{Z}^+$ ซึ่ง $s = t_i m_i$

$$\text{ดังนั้น } (g_1, g_2, \dots, g_n)^s = (g_1^s, g_2^s, \dots, g_n^s) = (g_1^{t_1 m_1}, g_2^{t_2 m_2}, \dots, g_n^{t_n m_n}) = (e_1, e_2, \dots, e_n)$$

จะได้ว่า t เป็นตัวหารของ s ดังนั้น $t \leq s$ แต่

$$(g_1^t, g_2^t, \dots, g_n^t) = (g_1, g_2, \dots, g_n)^t = (e_1, e_2, \dots, e_n)$$

ดังนั้น $g_i^t = e_i$ สำหรับทุกๆ $1 \leq i \leq n$ ทำให้ได้ว่า t_i เป็นตัวหารของ t สำหรับทุก $i = 1, 2, \dots, n$

จะได้ว่า t เป็นพหุคูณของ t_1, t_2, \dots, t_n แต่ s เป็นตัวคูณร่วมน้อยของ t_1, t_2, \dots, t_n เพราะฉะนั้น $s \leq t$

จาก $t \leq s$ และ $s \leq t$ ดังนั้น $s = t$

มหาวิทยาลัยศิลปากร สงวนลิขสิทธิ์

ตัวอย่างเช่น ในกรุปของผลคูณตรง $S_2 \times S_3$ ของตัวอย่าง 2.3 เพราะว่า $o(12) = 2$

และ $o(123) = 3$ ใน S_2 และ S_3 ตามลำดับและตัวคูณร่วมน้อยของ $o(12)$ และ $o(123)$

เท่ากับ ตัวคูณร่วมน้อยของ 2 และ 3 ซึ่งเท่ากับ 6 เพราะฉะนั้น $o((12), (123)) = 6$

ตัวอย่างการหาอันดับของสมาชิกในผลคูณตรง โดยประยุกต์ทฤษฎีบท 3.7

3.8 ตัวอย่าง จงหาจำนวนสมาชิกทั้งหมดในผลคูณตรง $Z_{25} \times Z_5$ ที่มีอันดับ 5

วิธีทำ ให้ $(a, b) \in Z_{25} \times Z_5$ โดยที่ $o(a, b) = 5$ แล้วเพราะเราต้องการ $o(a, b) = 5$ และ

$o(a, b)$ คือตัวคูณร่วมน้อยของ $o(a)$ และ $o(b)$ โดยที่ $a \in Z_{25}$ และ $b \in Z_5$

ดังนั้น $o(a) \mid 5$ และ $o(b) \mid 5$ จะได้ว่า $o(a) \in \{1, 5\}$ และ $o(b) \in \{1, 5\}$ เพราะฉะนั้น

$a \in Z_{25}$ ที่เป็นไปได้คือ 0, 5, 10, 15 และ 20 และ $b \in Z_5$ ที่เป็นไปได้คือ 0, 1, 2, 3 และ 4

แต่ $(0, 0)$ มีอันดับ 1 ดังนั้น (a, b) ที่เป็นไปได้คือ

$$\begin{aligned} & (0,1), (0,2), (0,3), (0,4), \\ & (5,0), (5,1), (5,2), (5,3), (5,4), \\ & (10,0), (10,1), (10,2), (10,3), (10,4), \\ & (15,0), (15,1), (15,2), (15,3), (15,4), \\ & (20,0), (20,1), (20,2), (20,3) \text{ และ } (20,4) \end{aligned}$$

เมื่อตรวจสอบแล้วพบว่าสมาชิกทุกตัว ดังกล่าวนี้ ทั้งหมดมีอันดับ 5 ดังนั้น จำนวนสมาชิกใน $Z_{25} \times Z_5$ ที่มีอันดับ 5 ทั้งหมดเท่ากับ 24 จำนวน ■

3.9 ทฤษฎีบท ให้ G และ H เป็นกรุปจำกัด ถ้า $G \times H$ เป็นกรุปวัฏจักร แล้ว $|G|$ และ $|H|$ เป็นจำนวนเฉพาะสัมพัทธ์

บทพิสูจน์ ให้ G และ H เป็นกรุปจำกัด โดยที่ $|G| = m$ และ $|H| = n$ แล้ว $|G \times H| = mn$

ให้ $G \times H$ เป็นกรุปวัฏจักร แล้วจะมี $(g, h) \in G \times H$ ซึ่ง $o(g, h) = mn$

แต่จากทฤษฎีบท 3.7 จะได้ $o(g, h) = \text{lcm}(o(g), o(h))$ ดังนั้น $mn = \text{lcm}(o(g), o(h))$

เนื่องจาก $|G| = m$ และ $|H| = n$ และ $g \in G$ และ $h \in H$ ดังนั้น $o(g) | m$ และ $o(h) | n$

ให้ $s = \text{lcm}(m, n)$ แล้ว $m | s$ และ $n | s$ เพราะฉะนั้น $o(g) | s$ และ $o(h) | s$

เพราะฉะนั้น s เป็นพหุคูณของ $o(g)$ และ $o(h)$ ดังนั้น $mn = \text{lcm}(o(g), o(h)) \leq s$

แต่ mn เป็นพหุคูณของ m และ n ดังนั้น $s = \text{lcm}(m, n) \leq mn$ เพราะฉะนั้น $mn = s$

ให้ $d = \text{gcd}(m, n)$ แล้ว $mn = ds = d(mn)$ เพราะฉะนั้น $d = 1$

ดังนั้น m และ n เป็นจำนวนเฉพาะสัมพัทธ์ ●

สังเกตว่า บทกลับของทฤษฎีบท 3.9 ไม่เป็นจริง ตัวอย่างเช่น ผลคูณตรงของ $Z_5 \times S_3$ ซึ่ง $|Z_5| = 5$ และ $|S_3| = 6$ และ 5 และ 6 เป็นจำนวนเฉพาะสัมพัทธ์กัน แต่ $Z_5 \times S_3$ ไม่เป็นกรุปวัฏจักรเพราะไม่มีสมาชิกใน $Z_5 \times S_3$ ที่มีอันดับ 30 (ดูทฤษฎีบท 3.7)

ต่อไปจะสร้างกรุป \bar{G}_i สำหรับแต่ละ $1 \leq i \leq n$ ขึ้นจากกรุป G_1, G_2, \dots, G_n โดยที่ \bar{G}_i เป็นกรุปย่อยปกติของกรุป $G_1 \times G_2 \times \dots \times G_n$ และแสดงว่า \bar{G}_i สมสัณฐานกันกับ G_i ทุกๆ

$$1 \leq i \leq n$$

3.10 ทฤษฎีบท ให้ n เป็นจำนวนเต็มบวก และให้ G_1, G_2, \dots, G_n เป็นกรุป แล้วสำหรับแต่ละ $1 \leq i \leq n$ จะมีกรุปย่อยปกติ \overline{G}_i ของกรุป $G_1 \times G_2 \times \dots \times G_n$ ซึ่ง

1. \overline{G}_i สมมูลฐานกันกับ G_i ทุกๆ $1 \leq i \leq n$
2. $\overline{G}_i \cap (\overline{G}_1 \overline{G}_2 \dots \overline{G}_{i-1} \overline{G}_{i+1} \dots \overline{G}_n) = \{(e_1, e_2, \dots, e_n)\}$ สำหรับแต่ละ $1 \leq i \leq n$
3. $G_1 \times G_2 \times \dots \times G_n = \overline{G}_1 \overline{G}_2 \dots \overline{G}_n$ สำหรับแต่ละ $1 \leq i \leq n$

บทพิสูจน์ ให้ n เป็นจำนวนเต็มบวก และให้ G_1, G_2, \dots, G_n เป็นกรุป สำหรับแต่ละ $i = 1, 2, \dots, n$

ให้ $\overline{G}_i = \{(e_1, e_2, \dots, g_i, e_{i+1}, \dots, e_n) \mid g_i \in G_i\}$ และให้ $g_i \in G_i$ โดยที่

$\overline{g}_i = (e_1, e_2, \dots, g_i, e_{i+1}, \dots, e_n)$ สำหรับแต่ละ $g_i \in G_i$ เราจะพิสูจน์ว่า \overline{G}_i เป็นกรุปย่อยปกติของกรุป $G_1 \times G_2 \times \dots \times G_n$ สำหรับแต่ละ $i = 1, 2, \dots, n$

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

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

2. ให้ $(e_1, e_2, \dots, g_i, e_{i+1}, \dots, e_n) \in \overline{G}_i$ แล้ว $g_i \in G_i$ ดังนั้นมี $g_i^{-1} \in G_i$ ทำให้มี $(e_1, e_2, \dots, g_i^{-1}, e_{i+1}, \dots, e_n) \in \overline{G}_i$ ซึ่งทำให้

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

ดังนั้น $(e_1, e_2, \dots, g_i^{-1}, e_{i+1}, \dots, e_n)$ เป็นตัวผกผันของ $(e_1, e_2, \dots, g_i, e_{i+1}, \dots, e_n)$

เพราะฉะนั้น \overline{G}_i เป็นกรุปย่อยของกรุป $G_1 \times G_2 \times \dots \times G_n$

3. ให้ $(e_1, e_2, \dots, g_i, e_{i+1}, \dots, e_n) \in \overline{G}_i$ และให้ $(g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n$ แล้ว

$$\begin{aligned} & (g_1, g_2, \dots, g_n)(e_1, e_2, \dots, g_i, e_{i+1}, \dots, e_n)(g_1, g_2, \dots, g_n)^{-1} \\ &= (g_1, g_2, \dots, g_n)(e_1, e_2, \dots, g_i, e_{i+1}, \dots, e_n)(g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}) \\ &= (g_1 e_1 g_1^{-1}, g_2 e_2 g_2^{-1}, \dots, g_{i-1} e_{i-1} g_{i-1}^{-1}, g_i g_i^{-1}, g_{i+1} e_{i+1} g_{i+1}^{-1}, \dots, g_n e_n g_n^{-1}) \end{aligned}$$

$$\begin{aligned}
&= (g_1 g_1^{-1}, g_2 g_2^{-1}, \dots, g_{i-1} g_{i-1}^{-1}, g_i, g_{i+1} g_{i+1}^{-1}, \dots, g_n g_n^{-1}) \\
&= (e_1, e_2, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_n) \in \overline{G}_i
\end{aligned}$$

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

ต่อไปเราจะพิสูจน์ว่า

1. \overline{G}_i สมสัณฐานกันกับ G_i สำหรับทุก $1 \leq i \leq n$
2. $\overline{G}_i \cap (\overline{G}_1 \overline{G}_2 \dots \overline{G}_{i-1} \overline{G}_{i+1} \dots \overline{G}_n) = \{(e_1, e_2, \dots, e_n)\}$ สำหรับแต่ละ $1 \leq i \leq n$
3. $G_1 \times G_2 \times \dots \times G_n = \overline{G}_1 \overline{G}_2 \dots \overline{G}_n$ สำหรับแต่ละ $1 \leq i \leq n$

1. ให้ $i = 1, 2, \dots, n$ และให้ $\alpha_i : \overline{G}_i \rightarrow G_i$ นิยามโดย $\alpha_i(e_1, e_2, \dots, a_i, e_{i+1}, \dots, e_n) = a_i$
 สำหรับทุกๆ $a_i \in G_i$ แล้วเห็นได้ชัดว่า α_i เป็นฟังก์ชัน

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

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

เพราะฉะนั้น α_i เป็นสัทิสถ์ฐาน

1.2 ให้ $(e_1, e_2, \dots, a_i, e_{i+1}, \dots, e_n) \in \overline{G}_i$ และ $(e_1, e_2, \dots, b_i, e_{i+1}, \dots, e_n) \in \overline{G}_i$ ซึ่ง

$$\alpha_i(e_1, e_2, \dots, a_i, e_{i+1}, \dots, e_n) = \alpha_i(e_1, e_2, \dots, b_i, e_{i+1}, \dots, e_n) \text{ แล้ว } a_i = b_i$$

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

เพราะฉะนั้น α_i เป็นฟังก์ชันหนึ่งต่อหนึ่ง

1.3 ให้ $a_i \in G_i$ แล้ว $(e_1, e_2, \dots, a_i, e_{i+1}, \dots, e_n) \in \overline{G}_i$ ซึ่ง $\alpha_i(e_1, e_2, \dots, a_i, e_{i+1}, \dots, e_n) = a_i$

เพราะฉะนั้น α_i เป็นฟังก์ชันทั่วถึง

ดังนั้น \overline{G}_i สมสัณฐานกันกับ G_i ทุกๆ $1 \leq i \leq n$

2. ให้ $(g_1, g_2, \dots, g_n) \in \overline{G}_i \cap (\overline{G}_1 \overline{G}_2 \dots \overline{G}_{i-1} \overline{G}_{i+1} \dots \overline{G}_n)$ แล้ว $(g_1, g_2, \dots, g_n) \in \overline{G}_i$

และ $(g_1, g_2, \dots, g_n) \in \overline{G}_1 \overline{G}_2 \dots \overline{G}_{i-1} \overline{G}_{i+1} \dots \overline{G}_n$

เพราะว่า $(g_1, g_2, \dots, g_n) \in \overline{G}_i$ แล้ว $(g_1, g_2, \dots, g_n) = (e_1, e_2, \dots, g_i, e_{i+1}, \dots, e_n)$ ดังนั้น

$g_k = e_k$ ทุกๆ $k \in \{1, 2, \dots, n\} - \{i\}$

เพราะว่า $(g_1, g_2, \dots, g_n) \in \overline{G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n}$ แล้วจะมี $g_k \in \overline{G_k}$ สำหรับ $1 \leq k \neq i \leq n$

ซึ่ง $(g_1, g_2, \dots, g_n) = \overline{g_1 g_2 \dots g_{i-1} g_{i+1} \dots g_n} = \overline{g_1 g_2 \dots g_{i-1}} \overline{e_i} \overline{g_{i+1} \dots g_n}$

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

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

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

และในทางกลับกัน $(e_1, e_2, \dots, e_n) \in \overline{G_i}$ และ $(e_1, e_2, \dots, e_n) \in \overline{G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n}$

จะได้ว่า $(e_1, e_2, \dots, e_n) \in \overline{G_i} \cap (\overline{G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n})$

เพราะฉะนั้น $\overline{G_i} \cap (\overline{G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n}) = \{(e_1, e_2, \dots, e_n)\}$ โดยที่ $i=1, 2, \dots, n$

3. ให้ $(g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n$ แล้ว

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

เพราะฉะนั้น $(g_1, g_2, \dots, g_n) \in \overline{G_1 G_2 \dots G_n}$

และในทางกลับกันให้ $\overline{g_1 g_2 \dots g_n} \in \overline{G_1 G_2 \dots G_n}$ แล้ว

$$\overline{g_1 g_2 \dots g_n} = (g_1, e, \dots, e)(e, g_2, e, \dots, e) \dots (e, e, \dots, g_n) = (g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n$$

เพราะฉะนั้น $G_1 \times G_2 \times \dots \times G_n = \overline{G_1 G_2 \dots G_n}$ สำหรับแต่ละ $1 \leq i \leq n$

มหาวิทยาลัยศิลปากร สงวนลิขสิทธิ์

เมื่อศึกษาผลคูณภายนอกและทฤษฎีบทที่เกี่ยวข้องกับผลคูณภายนอกแล้วต่อไปเรา

จะศึกษาผลคูณของกรุปซึ่งเรียกว่าผลคูณภายในและศึกษาทฤษฎีบทที่เกี่ยวข้องกับผลคูณภายใน

3.11 บทนิยาม ให้ G เป็นกรุปที่มี e เป็นเอกลักษณ์ และ G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของ G เรากล่าวว่า G เป็นผลคูณภายใน (internal direct product) ของ G_1, G_2, \dots, G_n ถ้า

$$1. G = G_1 G_2 \dots G_n$$

$$2. G_i \cap (G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n) = \{e\} \text{ สำหรับแต่ละ } 1 \leq i \leq n$$

3.12 ทฤษฎีบท ให้ G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของกรุป G ที่มี e เป็นเอกลักษณ์ ถ้า G เป็นผลคูณภายในของ G_1, G_2, \dots, G_n แล้ว

$$1. G_i \cap G_j = \{e\} \text{ สำหรับทุกๆ } 1 \leq i \neq j \leq n$$

$$2. h_i h_j = h_j h_i \text{ สำหรับทุกๆ } h_i \in G_i \text{ และ } h_j \in G_j \text{ และ } 1 \leq i, j \leq n$$

บทพิสูจน์ ให้ G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของกรุป G ที่มี e เป็นเอกลักษณ์ และให้ G เป็นผลคูณภายในของ G_1, G_2, \dots, G_n

1. ให้ $1 \leq i < j \leq n$ และให้ $k \in G_i \cap G_j$ แล้ว $k \in G_i$ และ $k \in G_j$

ให้ $e_s = e$ ทุกๆ $s = 1, 2, \dots, n$ แล้ว

$$k = e_1 e_2 \dots e_{i-1} e_{i+1} \dots e_{j-1} k e_{j+1} \dots e_n \in G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n$$

เพราะฉะนั้น $k \in G_i \cap (G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n)$ ทำให้ได้ $k = e$

2. ให้ $1 \leq i, j \leq n$ 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 $h_i h_j h_i^{-1} h_j^{-1} = h_i (h_j h_i^{-1} h_j^{-1}) = h_i s_i \in G_i$

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 $h_i h_j h_i^{-1} h_j^{-1} = (h_i h_j h_i^{-1}) h_j^{-1} = t_j h_j^{-1} \in G_j$

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 3.11 แสดงให้เห็นว่าถ้า G เป็นผลคูณภายในของ G_1, G_2, \dots, G_n

แล้ว $G = G_1 G_2 \dots G_n$ ทำให้ได้ว่าแต่ละ $g \in G$ ยังเขียนได้ในรูป $g = g_1 g_2 \dots g_n$ โดยที่ $g_i \in G_i$

ต่อไปจะแสดงให้เห็นว่าแต่ละ $g \in G$ เขียนในรูป $g = g_1 g_2 \dots g_n$ ได้เพียงแบบเดียวเท่านั้น

3.13 ทฤษฎีบท ให้ G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของ G ถ้า G เป็นผลคูณภายใน

ของ G_1, G_2, \dots, G_n แล้ว แต่ละ $g \in G$ เขียนได้ในรูป $g = g_1 g_2 \dots g_n$ โดยที่ $g_i \in G_i$

สำหรับแต่ละ $i = 1, 2, \dots, n$ ได้เพียงแบบเดียวเท่านั้น

บทพิสูจน์ ให้ G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของ G และให้ G เป็นผลคูณภายใน

ของ G_1, G_2, \dots, G_n

ให้ $g \in G$ และสมมติมี $g_i \in G_i$ และ $h_i \in G_i$ เมื่อ $i = 1, 2, \dots, n$ ซึ่ง

$g = g_1 g_2 \dots g_n$ และ $g = h_1 h_2 \dots h_n$ แล้ว $g_1 g_2 \dots g_n = h_1 h_2 \dots h_n$ จะแสดงว่า $g_i = h_i$

ทุกๆ $i = 1, 2, \dots, n$

ให้ $i \in \{1, 2, \dots, n\}$ แล้วเพราะว่า $g_1 g_2 \dots g_n = h_1 h_2 \dots h_n$ ดังนั้น

$$\begin{aligned} g_i &= (g_1 g_2 \dots g_{i-1})^{-1} (h_1 h_2 \dots h_n) (g_{i+1} g_{i+2} \dots g_n)^{-1} \\ &= g_{i-1}^{-1} g_{i-2}^{-1} \dots g_1^{-1} h_1 h_2 \dots h_n g_n^{-1} g_{n-1}^{-1} \dots g_{i+1}^{-1} \\ &= h_i (h_1 g_1^{-1}) (h_2 g_2^{-1}) \dots (h_{i-1} g_{i-1}^{-1}) (h_{i+1} g_{i+1}^{-1}) \dots (h_n g_n^{-1}) \end{aligned}$$

ทำให้ได้ $g_i h_i^{-1} = (h_1 g_1^{-1})(h_2 g_2^{-1}) \dots (h_{i-1} g_{i-1}^{-1})(h_{i+1} g_{i+1}^{-1}) \dots (h_n g_n^{-1})$
 ซึ่งแสดงว่า $g_i h_i^{-1} \in G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n$ และ $g_i h_i^{-1} \in G_i$
 เพราะฉะนั้น $g_i h_i^{-1} \in G_i \cap (G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n)$
 ดังนั้น $g_i h_i^{-1} = e$ เพราะฉะนั้น $g_i = h_i$

หลังจากทราบดีถึงผลคูณภายนอกและผลคูณภายในแล้ว ต่อไปเราจะแสดงให้เห็นว่า
 ผลคูณภายนอกและผลคูณภายในนั้นมีความสัมพันธ์กัน

3.14 ทฤษฎีบท ให้ G, G_1, G_2, \dots, G_n เป็นกรุป แล้ว G เป็นผลคูณภายนอกของ
 G_1, G_2, \dots, G_n ก็ต่อเมื่อ มีกรุปย่อยปกติ H_1, H_2, \dots, H_n ของ G ซึ่ง G_i สมมูลฐานกับ H_i
 สำหรับแต่ละ $1 \leq i \leq n$ และ G เป็นผลคูณภายในของ H_1, H_2, \dots, H_n

บทพิสูจน์ ให้ G, G_1, G_2, \dots, G_n เป็นกรุป

(\rightarrow) ให้ G เป็นผลคูณภายนอกของ G_1, G_2, \dots, G_n แล้วจะมี

$\alpha: G \rightarrow G_1 \times G_2 \times \dots \times G_n$ เป็นสมมูลฐาน และโดยทฤษฎีบท 2.10 จะมี $\overline{G_i}$ เป็นกรุปย่อย
 ปกติของ $G_1 \times G_2 \times \dots \times G_n$ ซึ่ง $\overline{G_i}$ สมมูลฐานกับ G_i สำหรับแต่ละ $1 \leq i \leq n$ และเพราะ
 อิมเมจผกผันภายใต้สัทิสต์ฐานของกรุปย่อยปกติเป็นกรุปย่อยปกติ เราจะได้ว่า $\alpha^{-1}(\overline{G_i})$
 เป็นกรุปย่อยปกติของ G สำหรับแต่ละ $1 \leq i \leq n$

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

ต่อไปเราจะแสดงว่า G เป็นผลคูณภายในของ H_1, H_2, \dots, H_n

1. ให้ $g \in G$ แล้ว $\alpha(g) \in G_1 \times G_2 \times \dots \times G_n$ และโดยทฤษฎีบท 3.10(3) จะมี $\overline{g_i} \in \overline{G_i}$ สำหรับ
 แต่ละ $1 \leq i \leq n$ ที่ทำให้ $\alpha(g) = \overline{g_1} \overline{g_2} \dots \overline{g_n}$ แต่ $\overline{g_i} \in \overline{G_i} = \alpha(H_i)$ สำหรับแต่ละ $1 \leq i \leq n$
 ดังนั้นจะมี $h_i \in H_i$ ซึ่ง $\overline{g_i} = \alpha(h_i)$ สำหรับทุกๆ $1 \leq i \leq n$ ทำให้ได้

$$\alpha(g) = \overline{g_1} \overline{g_2} \dots \overline{g_n} = \alpha(h_1) \alpha(h_2) \dots \alpha(h_n)$$

เพราะว่า α เป็นสัทิสต์ฐาน ดังนั้น $\alpha(g) = \alpha(h_1 h_2 \dots h_n)$ และเพราะ α เป็น
 ฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น $g = h_1 h_2 \dots h_n$ เพราะฉะนั้น $G = H_1 H_2 \dots H_n$

2. ให้ $1 \leq i \leq n$ และให้ $k \in H_i \cap (H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n)$ แล้ว $k \in H_i$ และ

$$k \in H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n$$

เพราะว่า $k \in H_i$ แล้วจะมี $h_i \in H_i$ ที่ทำให้ $k = h_i$ ดังนั้น $\alpha(k) = \alpha(h_i) = \overline{g_i}$

เพราะฉะนั้น $\alpha(k) \in \overline{G_i}$

และเพราะว่า $k \in H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n$ แล้วจะมี $h_j \in H_j$ สำหรับ $1 \leq j \neq i \leq n$ ที่ทำให้

$$\begin{aligned} k &= h_1 h_2 \dots h_{i-1} h_{i+1} \dots h_n \quad \text{ดังนั้น} \quad \alpha(k) = \alpha(h_1 h_2 \dots h_{i-1} h_{i+1} \dots h_n) \\ &= \alpha(h_1) \alpha(h_2) \dots \alpha(h_{i-1}) \alpha(h_{i+1}) \dots \alpha(h_n) \\ &= \overline{g_1 g_2 \dots g_{i-1} g_{i+1} \dots g_n} \end{aligned}$$

เพราะฉะนั้น $\alpha(k) \in \overline{G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n}$

เพราะฉะนั้น $\alpha(k) \in \overline{G_i} \cap (\overline{G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n}) = \{(e_1, e_2, \dots, e_n)\}$ โดยที่ e_i

เป็นเอกลักษณ์ของ G_i สำหรับ $1 \leq i \leq n$

เพราะฉะนั้น $\alpha(k) = (e_1, e_2, \dots, e_n)$ เป็นเอกลักษณ์ใน $G_1 \times G_2 \times \dots \times G_n$

ทำให้ได้ $\alpha(k) = \alpha(e)$ แต่ α เป็นฟังก์ชันหนึ่งต่อหนึ่ง เพราะฉะนั้น $k = e$

ในทางกลับกัน เพราะว่า H_1, H_2, \dots, H_n เป็นกรุปย่อยปกติของ G

ดังนั้น $H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n$ เป็นกรุปย่อยของ G ทำให้ได้ $e \in H_i$ และ $e \in H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n$

เพราะฉะนั้น $H_i \cap (H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_n) = e$

ดังนั้น G เป็นผลคูณภายในของ H_1, H_2, \dots, H_n

(\leftarrow) ให้ H_1, H_2, \dots, H_n เป็นกรุปย่อยปกติของ G ซึ่ง G_i สมมติฐานกันกับ H_i โดย
 สหสัมพันธ์ฐาน α_i สำหรับแต่ละ $1 \leq i \leq n$ และให้ G เป็นผลคูณภายในของ H_1, H_2, \dots, H_n จะ

แสดงว่า G เป็นผลคูณภายนอกของ G_1, G_2, \dots, G_n นั่นคือจะแสดงว่า $G \cong G_1 \times G_2 \times \dots \times G_n$

ให้ $\alpha: G \rightarrow G_1 \times G_2 \times \dots \times G_n$ นิยามโดย $\alpha(g) = (g_1, g_2, \dots, g_n)$ สำหรับแต่ละ
 $g \in G$ โดยที่ $g = h_1 h_2 \dots h_n$ โดยที่ $h_i \in H_i$ และ $\alpha_i(h_i) = g_i$ ทุกๆ $1 \leq i \leq n$

1. ให้ $g, q \in G$ ซึ่ง $g = q$ เมื่อ $g = h_1 h_2 \dots h_n$ โดยที่ $h_i \in H_i$ และ $\alpha_i(h_i) = g_i$ ทุกๆ $1 \leq i \leq n$

และ $q = k_1 k_2 \dots k_n$ โดยที่ $k_i \in H_i$ และ $\alpha_i(k_i) = q_i$ ทุกๆ $1 \leq i \leq n$

แล้ว $g = h_1 h_2 \dots h_n = q = k_1 k_2 \dots k_n$ จากทฤษฎีบท 3.13 จะได้ว่า $h_i = k_i$ ทุกๆ $1 \leq i \leq n$

$$\begin{aligned} \text{แล้ว} \quad \alpha(g) &= \alpha(h_1 h_2 \dots h_n) \\ &= (\alpha_1(h_1), \alpha_2(h_2), \dots, \alpha_n(h_n)) \\ &= (\alpha_1(k_1), \alpha_2(k_2), \dots, \alpha_n(k_n)) \\ &= \alpha(k_1 k_2 \dots k_n) \\ &= \alpha(q) \end{aligned}$$

เพราะฉะนั้น α เป็นฟังก์ชัน

2. ให้ $g, q \in G$ เมื่อ $g = h_1 h_2 \dots h_n$ โดยที่ $h_i \in H_i$ และ $\alpha_i(h_i) = g_i$ ทุกๆ $1 \leq i \leq n$

และ $q = k_1 k_2 \dots k_n$ โดยที่ $k_i \in H_i$ และ $\alpha_i(k_i) = q_i$ ทุกๆ $1 \leq i \leq n$

$$\begin{aligned} \text{แล้ว } \alpha(gq) &= \alpha(h_1 h_2 \dots h_n k_1 k_2 \dots k_n) \\ &= \alpha(h_1 k_1 h_2 k_2 \dots h_n k_n) \\ &= (\alpha_1(h_1 k_1), \alpha_2(h_2 k_2), \dots, \alpha_n(h_n k_n)) \\ &= (\alpha_1(h_1)\alpha_1(k_1), \alpha_2(h_2)\alpha_2(k_2), \dots, \alpha_n(h_n)\alpha_n(k_n)) \\ &= (g_1 q_1, g_2 q_2, \dots, g_n q_n) \end{aligned}$$

$$\text{และ } \alpha(g)\alpha(q) = (g_1, g_2, \dots, g_n)(q_1, q_2, \dots, q_n) = (g_1 q_1, g_2 q_2, \dots, g_n q_n)$$

ดังนั้น α เป็นสัทิสต์ฐาน

3. ให้ $g, q \in G$ ซึ่ง $\alpha(g) = \alpha(q)$ เมื่อ $g = h_1 h_2 \dots h_n$ โดยที่ $h_i \in H_i$ และ $\alpha_i(h_i) = g_i$

ทุกๆ $1 \leq i \leq n$ และ $q = k_1 k_2 \dots k_n$ โดยที่ $k_i \in H_i$ และ $\alpha_i(k_i) = q_i$ ทุกๆ $1 \leq i \leq n$

$$\begin{aligned} \text{แล้ว } \alpha(h_1 h_2 \dots h_n) &= \alpha(k_1 k_2 \dots k_n) \\ (\alpha_1(h_1), \alpha_2(h_2), \dots, \alpha_n(h_n)) &= (\alpha_1(k_1), \alpha_2(k_2), \dots, \alpha_n(k_n)) \end{aligned}$$

ดังนั้น $\alpha_i(h_i) = \alpha_i(k_i)$ ทุกๆ $1 \leq i \leq n$

แล้ว $h_i = k_i$ ทุกๆ $1 \leq i \leq n$ เพราะฉะนั้น $g = q$

เพราะฉะนั้น α เป็นฟังก์ชันหนึ่งต่อหนึ่ง

4. ให้ $(g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n$ แล้ว $g_i \in G_i$ ทำให้ $\alpha_i(g_i) = h_i \in H_i$ สำหรับแต่ละ $1 \leq i \leq n$ เลือก $g = h_1 h_2 \dots h_n$ แล้ว

$$\alpha(g) = \alpha(h_1 h_2 \dots h_n) = (\alpha_1(h_1), \alpha_2(h_2), \dots, \alpha_n(h_n)) = (g_1, g_2, \dots, g_n)$$

ดังนั้น α เป็นฟังก์ชันทั่วถึง

เพราะฉะนั้น α เป็นสมสัฐาน เพราะฉะนั้น $G \cong G_1 \times G_2 \times \dots \times G_n$ ●

3.15 ทฤษฎีบท ให้ G เป็นกรุปและให้ G_1, G_2, \dots, G_n เป็นกรุปย่อยของ G ซึ่ง G เป็นผลคูณภายในของ G_1, G_2, \dots, G_n ถ้า H_1, H_2, \dots, H_n เป็นกรุปซึ่ง $H_i \cong G_i$ สำหรับแต่ละ $i = 1, 2, \dots, n$ และ H เป็นผลคูณภายนอกของ H_1, H_2, \dots, H_n แล้ว $G \cong H$

บทพิสูจน์ ให้ G เป็นกรุป และให้ G_1, G_2, \dots, G_n เป็นกรุปย่อยของ G ซึ่ง G เป็นผลคูณภายในของ G_1, G_2, \dots, G_n และให้ H_1, H_2, \dots, H_n เป็นกรุปซึ่ง $H_i \cong G_i$ สำหรับแต่ละ $i = 1, 2, \dots, n$ และ H เป็นผลคูณภายนอกของ H_1, H_2, \dots, H_n

ให้ $f_i : H_i \rightarrow G_i$ เป็นสมสัณฐานจาก H_i ไปยัง G_i

ให้ $f : H \rightarrow G$ นิยามโดย $f((h_1, h_2, \dots, h_n)) = f_1(h_1)f_2(h_2)\dots f_n(h_n)$

1. ให้ (h_1, h_2, \dots, h_n) และ (a_1, a_2, \dots, a_n) เป็นสมาชิกของ $H_1 \times H_2 \times \dots \times H_n$ ซึ่ง $(h_1, h_2, \dots, h_n) = (a_1, a_2, \dots, a_n)$ แล้ว $h_i = a_i$ สำหรับแต่ละ $i = 1, 2, \dots, n$ แล้ว

$$f((h_1, h_2, \dots, h_n)) = f_1(h_1)f_2(h_2)\dots f_n(h_n) = f_1(a_1)f_2(a_2)\dots f_n(a_n) = f((a_1, a_2, \dots, a_n))$$

เพราะฉะนั้น f เป็นฟังก์ชัน

2. ให้ (h_1, h_2, \dots, h_n) และ (a_1, a_2, \dots, a_n) เป็นสมาชิกของ $H_1 \times H_2 \times \dots \times H_n$

$$\begin{aligned} f((h_1, h_2, \dots, h_n)(a_1, a_2, \dots, a_n)) &= f((h_1a_1, h_2a_2, \dots, h_na_n)) \\ &= f_1(h_1a_1)f_2(h_2a_2)\dots f_n(h_na_n) \\ &= f_1(h_1)f_1(a_1)f_2(h_2)f_2(a_2)\dots f_n(h_n)f_n(a_n) \\ &= (f_1(h_1)f_2(h_2)\dots f_n(h_n))(f_1(a_1)f_2(a_2)\dots f_n(a_n)) \\ &= f(h_1, h_2, \dots, h_n) f(a_1, a_2, \dots, a_n) \end{aligned}$$

เพราะฉะนั้น f เป็นสัทิสสัณฐาน

3. ให้ (a_1, a_2, \dots, a_n) เป็นสมาชิกของ $H_1 \times H_2 \times \dots \times H_n$ ซึ่ง $f((a_1, a_2, \dots, a_n)) = e$

แล้ว $(a_1, a_2, \dots, a_n) \in \ker(f)$ แล้ว $f((a_1, a_2, \dots, a_n)) = e$ แล้ว

$$f_1(a_1)f_2(a_2)\dots f_n(a_n) = e_1e_2\dots e_n \text{ จะได้ว่า } f_i(a_i) = e_i \text{ สำหรับ } i=1,2,\dots,n$$

เพราะว่า f_i เป็นฟังก์ชันหนึ่งต่อหนึ่ง ดังนั้น $a_i = e_i$ สำหรับ $i=1,2,\dots,n$ แล้ว

$$(a_1, a_2, \dots, a_n) = (e_1, e_2, \dots, e_n) \text{ ซึ่งก็คือเอกลักษณ์ของ } H$$

เพราะฉะนั้น f เป็นฟังก์ชันหนึ่งต่อหนึ่ง

4. ให้ g เป็นสมาชิกของ G ซึ่ง $g = b_1b_2\dots b_n \mid b_i \in G_i$

เนื่องจาก f_i เป็นฟังก์ชันทั่วถึง จะมี $a_i \in H_i$ ซึ่ง $f_i(a_i) = b_i$

$$\text{แล้ว } (a_1, a_2, \dots, a_n) \in H \text{ ซึ่ง } f((a_1, a_2, \dots, a_n)) = f_1(a_1)f_2(a_2)\dots f_n(a_n) = b_1b_2\dots b_n = g$$

เพราะฉะนั้น f เป็นฟังก์ชันทั่วถึง

เพราะฉะนั้น f เป็นสมสัณฐาน ดังนั้น $G \cong H$ ●

ถ้าไม่เน้นการสมสัณฐานกัน เราอาจกล่าวบทแทรกต่อไปนี้

3.16 บทแทรก ให้ G เป็นกรุป และให้ G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของ G

แล้ว G เป็นผลคูณภายนอกของ G_1, G_2, \dots, G_n ก็ต่อเมื่อ G เป็นผลคูณภายในของ

G_1, G_2, \dots, G_n

บทพิสูจน์ ให้ G เป็นกรุปและให้ G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของ G

(\rightarrow) ให้ G เป็นผลคูณภายนอกของ G_1, G_2, \dots, G_n

เราจะแสดงว่า G เป็นผลคูณภายในของ G_1, G_2, \dots, G_n

1. ให้ $g \in G_1 \times G_2 \times \dots \times G_n$ และโดยทฤษฎีบท 3.10(3) จะมี $\bar{g}_i \in \bar{G}_i$ สำหรับ

แต่ละ $1 \leq i \leq n$ ที่ทำให้ $g = \bar{g}_1 \bar{g}_2 \dots \bar{g}_n$ แต่ $\bar{g}_i \in \bar{G}_i$ และ \bar{G}_i สมสัณฐานกัน กับ G_i สำหรับแต่

ละ $1 \leq i \leq n$ ทำให้ได้ $g = g_1 g_2 \dots g_n$ เพราะฉะนั้น $G = G_1 G_2 \dots G_n$

2. ให้ $1 \leq i \leq n$ และให้ $k \in G_i \cap (G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n)$ แล้ว $k \in G_i$ และ

$k \in G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n$ เพราะว่า $k \in G_i$ แล้วจะมี $g_i \in G_i$ ที่ทำให้ $k = g_i = \bar{g}_i$

เพราะฉะนั้น $k \in \bar{G}_i$ และเพราะว่า $k \in G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n$ แล้วจะมี $g_j \in G_j$ สำหรับ

$1 \leq j \neq i \leq n$ ที่ทำให้ $k = g_1 g_2 \dots g_{i-1} g_{i+1} \dots g_n = \bar{g}_1 \bar{g}_2 \dots \bar{g}_{i-1} \bar{g}_{i+1} \dots \bar{g}_n$

เพราะฉะนั้น $k \in \bar{G}_1 \bar{G}_2 \dots \bar{G}_{i-1} \bar{G}_{i+1} \dots \bar{G}_n$

เพราะฉะนั้น $k \in \bar{G}_i \cap (\bar{G}_1 \bar{G}_2 \dots \bar{G}_{i-1} \bar{G}_{i+1} \dots \bar{G}_n) = \{(e_1, e_2, \dots, e_n)\}$ โดยที่ e_i

เป็นเอกลักษณ์ของ G_i สำหรับ $1 \leq i \leq n$

เพราะฉะนั้น $k = (e_1, e_2, \dots, e_n)$ เป็นเอกลักษณ์ใน $G_1 \times G_2 \times \dots \times G_n$ เพราะฉะนั้น $k = e$

ในทางกลับกัน เพราะว่า G_1, G_2, \dots, G_n เป็นกรุปย่อยปกติของ G

ดังนั้น $k \in G_i \cap (G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n)$ เป็นกรุปย่อยของ G ทำให้ได้ $e \in G_i$

และ $e \in G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n$

เพราะฉะนั้น $G_i \cap (G_1 G_2 \dots G_{i-1} G_{i+1} \dots G_n) = e$

ดังนั้น G เป็นผลคูณภายในของ G_1, G_2, \dots, G_n

(\leftarrow) ให้ G เป็นผลคูณภายในของ G_1, G_2, \dots, G_n จะแสดงว่า G เป็นผลคูณภายนอกของ

G_1, G_2, \dots, G_n นั่นคือจะแสดงว่า $G = G_1 \times G_2 \times \dots \times G_n$

ให้ $g \in G_1 G_2 \dots G_n$ จากทฤษฎีบท 3.10(1) ทำให้ได้ $g \in \bar{G}_1 \bar{G}_2 \dots \bar{G}_n$

และ $G_1 \times G_2 \times \dots \times G_n = \bar{G}_1 \bar{G}_2 \dots \bar{G}_n$ ดังนั้น $g \in G_1 \times G_2 \times \dots \times G_n$

เพราะฉะนั้น $G = G_1 \times G_2 \times \dots \times G_n$

ดังนั้น G เป็นผลคูณภายนอกของ G_1, G_2, \dots, G_n ●

บทที่ 4
ผลคูณอนันต์และผลคูณอิสระของกรุป

จากบทที่ 3 เราได้สร้างผลคูณภายนอกและผลคูณภายในขึ้นมาจากกรุปต่างๆจำนวนจำกัดกรุป ในบทนี้จะศึกษาผลคูณของกรุปจำนวนอนันต์กรุปตลอดจนศึกษาสมบัติที่สำคัญของผลคูณอนันต์ของกรุปและแสดงว่าผลคูณอนันต์ของกรุปสอดคล้องกับบทนิยาม 2.40 นอกจากนี้ยังจะแสดงการสร้างกรุปที่สอดคล้องกับบทนิยาม 2.41 และ บทนิยาม 2.42 ซึ่งทำให้เราได้ผลคูณอิสระของกรุป

4.1 บทนิยาม ให้ $\{G_i | i \in I\}$ เป็นวงศ์ของเซตโดยที่ I เป็นเซตคอร์ดอร์ชนี และให้ $G = \bigcup_{i \in I} G_i$ **ผลคูณคาร์ทีเซียน** (Cartesian product) หรือ**ผลคูณ** (product) ของ $\{G_i | i \in I\}$ เขียนแทนด้วย $\prod_{i \in I} G_i$ กำหนดโดย

$$\prod_{i \in I} G_i = \{ f | f: I \rightarrow G \text{ โดยที่ } f(i) \in G_i \text{ สำหรับทุก } i \in I \}$$

4.2 ทฤษฎีบท ให้ $\{G_i | i \in I\}$ เป็นวงศ์ของกรุปโดยที่ I เป็นเซตคอร์ดอร์ชนี และให้ $o: \prod_{i \in I} G_i \times \prod_{i \in I} G_i \rightarrow \prod_{i \in I} G_i$ นิยามโดย $f \circ g = f \cdot g$ สำหรับทุกๆ f และ g ใน $\prod_{i \in I} G_i$ โดยที่ $f \cdot g(i) = f(i) \cdot g(i)$ สำหรับทุก $i \in I$ แล้ว $(\prod_{i \in I} G_i; o)$ เป็นกรุป

บทพิสูจน์ ให้ $\{G_i | i \in I\}$ เป็นวงศ์ของกรุปโดยที่ I เป็นเซตคอร์ดอร์ชนี

1. ให้ f, g และ h เป็นสมาชิกของ $\prod_{i \in I} G_i$ แล้ว

$$(f \circ g) \circ h = (f \cdot g) \circ h = f \cdot g = f \circ (g \cdot h) = f \circ (g \circ h)$$

ดังนั้น o มีสมบัติการเปลี่ยนหมู่บน $\prod_{i \in I} G_i$

2. ให้ $f \in \prod_{i \in I} G_i$ เพราะว่า G_i เป็นกรุปสำหรับแต่ละ $i \in I$ ให้ e_i เป็นเอกลักษณ์บน G_i สำหรับแต่ละ $i \in I$ ดังนั้นจะมี $e \in \prod_{i \in I} G_i$ ซึ่ง $e(i) = e_i$ แล้ว

$$(f \circ e)(i) = (f \epsilon)(i) = f(i) e(i) = f(i) e_i = f(i) \text{ และ}$$

$$(e \circ f)(i) = (e f)(i) = e(i) f(i) = e_i f(i) = f(i)$$

ดังนั้น e เป็นเอกลักษณ์ของ $\prod_{i \in I} G_i$ ภายใต้ \circ

3. ให้ $f \in \prod_{i \in I} G_i$ และ $f(i) \in G_i$ เพราะว่า G_i เป็นกรุปสำหรับทุกๆ $i \in I$ ดังนั้นสำหรับแต่ละ

$i \in I$ จะมี $g(i) \in G_i$ ซึ่ง $f(i)g(i) = e(i) = g(i)f(i)$ ทำให้ได้

$$(f \circ g)(i) = (f g)(i) = f(i)g(i) = e(i) \text{ และ}$$

$$(g \circ f)(i) = (g f)(i) = g(i)f(i) = e(i)$$

ดังนั้น g เป็นตัวผกผันของ f ภายใต้ \circ

เพราะฉะนั้น $\prod_{i \in I} G_i$ เป็นกรุป

4.3 บทนิยาม เราเรียกรูป $(\prod_{i \in I} G_i; \circ)$ โดยที่ I เป็นเซตคอร์ดานี้ ในทฤษฎีบท 4.2 ว่าผลคูณตรง

(direct product) ของวงศ์ของกรุป $\{G_i | i \in I\}$

ขอให้สังเกตว่าถ้า I เป็นเซตจำกัดแล้ว $(\prod_{i \in I} G_i; \circ)$ ก็คือผลคูณภายนอกในบทที่ 3 และ

ถ้า I เป็นเซตอนันต์เราจะเรียก $(\prod_{i \in I} G_i; \circ)$ ว่าผลคูณอนันต์ (infinite product) ของกรุป

4.4 ทฤษฎีบท ให้ $\{G_i | i \in I\}$ เป็นวงศ์ของกรุป โดยที่ I เป็นเซตคอร์ดานี้ สำหรับแต่ละ $k \in I$

นิยาม $\pi_k : \prod_{i \in I} G_i \rightarrow G_k$ โดย $\pi_k(f) = f(k)$ แล้ว π_k เป็นอูปริสรฐานทุกๆ $k \in I$

บทพิสูจน์ ให้ $\{G_i | i \in I\}$ เป็นวงศ์ของกรุป โดยที่ I เป็นเซตคอร์ดานี้และสำหรับแต่ละ $k \in I$

นิยาม $\pi_k : \prod_{i \in I} G_i \rightarrow G_k$ โดย $\pi_k(f) = f(k)$

1. ให้ f และ g เป็นสมาชิกของ $\prod_{i \in I} G_i$ โดยที่ $f=g$ เพราะฉะนั้น $f(k) = g(k)$ สำหรับแต่ละ

$k \in I$ เพราะฉะนั้น $\pi_k(f) = f(k) = g(k) = \pi_k(g)$

ดังนั้น π_k เป็นฟังก์ชัน

2. ให้ f และ g เป็นสมาชิกของ $\prod_{i \in I} G_i$ จะได้ว่า

$$\pi_k(f \circ g) = \pi_k(f g) = (f g)(k) = f(k)g(k) = \pi_k(f) \pi_k(g) \text{ สำหรับทุก } k \in I$$

ดังนั้น π_k เป็นสาคทิสต์ฐาน

3. ให้ $g_k \in G_k$ จะมี $f \in \prod_{i \in I} G_i$ ซึ่ง $f: I \rightarrow G$ โดยที่ $f(k) = g_k \in G_k$ ที่ทำให้

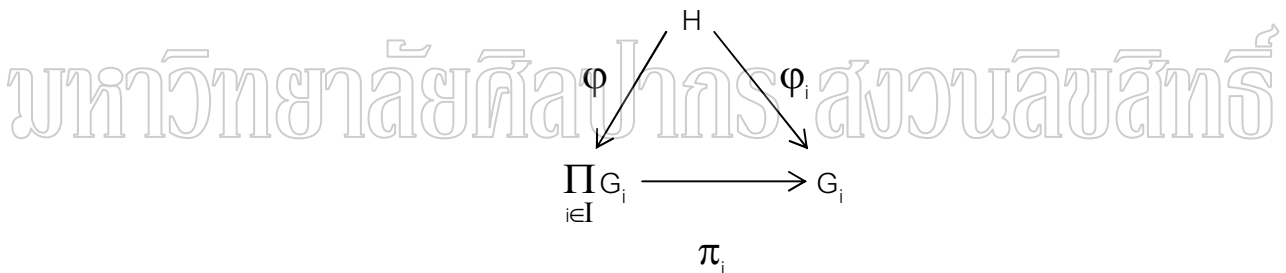
$$\pi_k(f) = f(k) = g_k$$

ดังนั้น π_k เป็นฟังก์ชันทั่วถึง

จากการพิสูจน์ข้างต้นทำให้สรุปได้ว่า π_k เป็นอูปริสต์ฐาน ●

ต่อไปจะแสดงความสัมพันธ์ของ $\prod_{i \in I} G_i$ กับกรุป H ใดๆโดยพิสูจน์ว่า $\prod_{i \in I} G_i$ สอดคล้องคุณสมบัติการเป็นผลคูณสำหรับวงศ์ $\{G_i | i \in I\}$ ตามบทแทรก 2.39

4.5 ทฤษฎีบท ให้ $\{G_i | i \in I\}$ เป็นวงศ์ของกรุปโดยที่ I เป็นเซตดรรชนี และให้ H เป็นกรุปและ $\{\varphi_i : H \rightarrow G_i | i \in I\}$ เป็นวงศ์ของสาคทิสต์ฐานแล้วจะมีสาคทิสต์ฐาน $\varphi: H \rightarrow \prod_{i \in I} G_i$ เพียงหนึ่งเดียวซึ่ง $\pi_i \varphi = \varphi_i$ สำหรับทุกๆ $i \in I$



บทพิสูจน์ เราจะต้องแสดงให้เห็นว่า $\prod_{i \in I} G_i$ โดยที่ I เป็นเซตดรรชนีมีคุณสมบัติเป็นผลคูณของวงศ์ $\{G_i | i \in I\}$ ดังนี้ ให้ H เป็นกรุปและ $\{\varphi_i : H \rightarrow G_i | i \in I\}$ เป็นวงศ์ของสาคทิสต์ฐานและเรานิยาม $\varphi: H \rightarrow \prod_{i \in I} G_i$ โดย $\varphi(a)(i) = \varphi_i(a)$ สำหรับทุกๆ $i \in I$ และทุกๆ $a \in H$

1. ให้ a และ b เป็นสมาชิกของ H โดยที่ $a=b$ แล้วจะพิสูจน์ว่า $\varphi(a) = \varphi(b)$
ให้ $i \in I$ เพราะว่า $\varphi_i : H \rightarrow G_i$ เป็นสาคทิสต์ฐาน เพราะฉะนั้น $\varphi_i(a) = \varphi_i(b)$ ทุกๆ $i \in I$ ทำให้ได้ว่า $\varphi(a)(i) = \varphi(b)(i)$ สำหรับทุกๆ $i \in I$ ซึ่งแสดงว่า $\varphi(a) = \varphi(b)$
ดังนั้น φ เป็นฟังก์ชัน
2. ให้ a และ b เป็นสมาชิกของ H แล้วสำหรับแต่ละ $i \in I$ จะได้ว่า $\varphi(ab)(i) = \varphi_i(ab)$
เนื่องจาก $\varphi_i : H \rightarrow G_i$ เป็นสาคทิสต์ฐานสำหรับทุกๆ $i \in I$ เพราะฉะนั้น $\varphi_i(ab) = \varphi_i(a)\varphi_i(b)$ สำหรับทุกๆ $i \in I$ ดังนั้น

$$\varphi(ab)(i) = \varphi_i(ab) = \varphi_i(a)\varphi_i(b) = (\varphi(a)\varphi(b))(i)$$

ดังนั้น $\varphi(ab) = \varphi(a)\varphi(b)$ ซึ่งแสดงว่า φ เป็นสัทิสต์ฐาน

3. ให้ $a \in H$ จะได้ว่า $\pi_i\varphi(a) = \varphi(a)(i) = \varphi_i(a)$ สำหรับทุกๆ $i \in I$ ดังนั้น $\pi_i\varphi = \varphi_i$ สำหรับทุกๆ $i \in I$

4. ให้ $\beta: H \rightarrow \prod_{i \in I} G_i$ เป็นสัทิสต์ฐานซึ่ง $\pi_i\beta = \varphi_i$ สำหรับทุกๆ $i \in I$ ให้ $a \in H$ และ $i \in I$ จะได้ว่า

$$\varphi(a)(i) = \varphi_i(a) = \pi_i\beta(a) = \beta(a)(i)$$

เพราะฉะนั้น $\varphi(a) = \beta(a)$ ดังนั้น $\varphi = \beta$

เพราะฉะนั้น φ เป็นสัทิสต์ฐานเพียงหนึ่งเดียวซึ่ง $\pi_i\varphi = \varphi_i$ สำหรับทุก $i \in I$ ●

ต่อไปเราจะแสดงวิธีการสร้างกรุปที่จะสอดคล้องตามบทแทรก 2.41 ดังนี้ ให้ X เป็นเซตใดๆ ให้ X^{-1} เป็นเซตต่างสมาชิกของ X โดยที่ $|X| = |X^{-1}|$ จากนั้นเลือกฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก X ไปยัง X^{-1} โดยใช้สัญลักษณ์ x^{-1} แทนภาพของ $x \in X$ และเลือกเซตที่

ประกอบด้วยสมาชิกที่ต่างจากสมาชิกใน X และ X^{-1} โดยมีสมาชิกเพียงตัวเดียว เราแทนสมาชิกเพียงตัวเดียวนั้นด้วยสัญลักษณ์ 1

เราเรียกลำดับ (a_1, a_2, \dots) โดยที่ a_i เป็นสมาชิกของ $X \cup X^{-1} \cup \{1\}$ สำหรับแต่ละ $i \in \{1, 2, \dots\}$ ว่าคำ (word) และถ้าคำสอดคล้องกับเงื่อนไขต่อไปนี้

- 1) ถ้า x เป็นสมาชิกของ X แล้ว x และ x^{-1} ไม่ประชิดกัน
- 2) มี $i \geq 1$ ซึ่ง $a_i = 1$
- 3) สำหรับแต่ละ $k \geq 1$ ถ้า $a_k = 1$ แล้ว $a_i = 1$ สำหรับทุกๆ $i \geq k$

จะเรียกว่าคำลดทอน (reduce word) โดยแทนคำลดทอน $(a_1, a_2, \dots, a_n, 1, 1, \dots)$ เมื่อ $n \geq 1$ ด้วย (a_1, a_2, \dots, a_n) และคำลดทอน $(1, 1, \dots)$ เรียกว่าคำว่าง (empty word) และใช้ 1 เป็นสัญลักษณ์แทนคำว่าง

ให้ F เป็นเซตของคำลดทอนทั้งหมดบน $X \cup X^{-1} \cup \{1\}$ รวมกับคำว่างและเราจะแทนลำดับ (a_1, a_2, \dots, a_n) ด้วย $a_1 a_2 \dots a_n$ และนิยามการดำเนินการ $*$ บน F โดยวิธีการวางเคียงกัน (juxtaposition) ดังนี้

$$(a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m) = \begin{cases} a_1 a_2 \dots a_n b_1 b_2 \dots b_m & \text{เมื่อ } a_n \neq b_1^{-1} \\ a_1 a_2 \dots a_{n-k} b_{k+1} \dots b_m & \text{เมื่อ } k \text{ เป็นจำนวนเต็มบวกที่มากที่สุดซึ่ง } a_{n-j} = b_{j+1}^{-1} \text{ สำหรับ } j=0, 1, \dots, k-1 \\ b_{n+1} \dots b_m & \text{เมื่อ } a_{n-i+1} = b_i^{-1} \text{ สำหรับ } i=1, 2, \dots, n \text{ และ } n < m \\ a_1 a_2 \dots a_{n-m} & \text{เมื่อ } a_{n-i+1} = b_i^{-1} \text{ สำหรับ } i=1, 2, \dots, n \text{ และ } m < n \\ 1 & \text{เมื่อ } a_{n-i+1} = b_i^{-1} \text{ สำหรับ } i=1, 2, \dots, n \text{ และ } m=n \\ a_1 a_2 \dots a_n & \text{เมื่อ } b_i = 1 \text{ สำหรับทุกๆ } 1 \leq i \leq m \\ b_1 b_2 \dots b_m & \text{เมื่อ } a_i = 1 \text{ สำหรับทุกๆ } 1 \leq i \leq n \\ 1 & \text{เมื่อ } a_i = 1 \text{ สำหรับทุกๆ } 1 \leq i \leq n \text{ และ } b_i = 1 \text{ สำหรับทุกๆ } 1 \leq i \leq m \end{cases}$$

จากการนิยามการดำเนินการ * บน F ข้างต้น จะเห็นว่าสำหรับทุกๆ $(a_1, a_2, \dots, a_n) \in F$

จะมี $(1, 1, \dots) \in F$ ซึ่ง $(a_1, a_2, \dots, a_n) * (1, 1, \dots) = (a_1, a_2, \dots, a_n) = (1, 1, \dots) * (a_1, a_2, \dots, a_n)$

นั่นคือ $(1, 1, \dots)$ เป็นเอกลักษณ์ของ F ภายใต้การดำเนินการ * และสำหรับทุกๆ

$(a_1, a_2, \dots, a_n) \in F$ จะมี $(a_n^{-1}, a_{n-1}^{-1}, \dots, a_1^{-1}) \in F$ ซึ่ง

$(a_1, a_2, \dots, a_n) * (a_n^{-1}, a_{n-1}^{-1}, \dots, a_1^{-1}) = (1, 1, \dots) = 1 = (a_n^{-1}, a_{n-1}^{-1}, \dots, a_1^{-1}) * (a_1, a_2, \dots, a_n)$

นั่นคือ $(a_n^{-1}, a_{n-1}^{-1}, \dots, a_1^{-1})$ เป็นตัวผกผันของ (a_1, a_2, \dots, a_n) ภายใต้การดำเนินการ * บน F

ต่อไปจะแสดงให้เห็นว่าเซต F ภายใต้การดำเนินการ * เป็นกรุปโดยแสดงให้เห็นว่า

$(F; \cdot)$ สมบัติฐานกันกับกรุปที่เราสร้างขึ้นมาซึ่งก็คือกรุปย่อยของกรุปการเรียงสับเปลี่ยน

4.6 ทฤษฎีบท $(F; \cdot)$ เป็นกรุป

บทพิสูจน์ ให้ $A(F)$ แทนเซตของฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึงทั้งหมดบนเซต F แล้ว $A(F)$ จะเป็นกรุปการเรียงสับเปลี่ยนบน F ภายใต้ผลประกอบ \circ ของฟังก์ชัน

ให้ $x \in X$ และให้ $|x|$ เป็นฟังก์ชันจาก F ไปยัง F นิยามสำหรับแต่ละ

$(a_1, a_2, \dots, a_n) \in F$ นิยามโดย

$$|x|(a_1, a_2, \dots, a_n) = \begin{cases} xa_1a_2\dots a_n & \text{เมื่อ } x \neq a_1^{-1} \\ a_2\dots a_n & \text{เมื่อ } x = a_1^{-1} \\ x & \text{เมื่อ } (a_1, a_2, \dots, a_n) = 1 \\ 1 & \text{เมื่อ } x = a_1^{-1} \text{ และ } n=1 \end{cases}$$

1) ให้ (a_1, a_2, \dots, a_n) และ $(b_1, b_2, \dots, b_m) \in F$ สำหรับทุก $n, m \in \mathbf{I}$ ซึ่ง

$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_m)$ เนื่องจาก (a_1, a_2, \dots, a_n) และ (b_1, b_2, \dots, b_m) เป็นลำดับ

ดังนั้น $n=m$ และ $a_i = b_i$ สำหรับทุก $i, 1 \leq i \leq n$

กรณีที่ 1 เมื่อ $x \neq a_1^{-1}$ จะได้ว่า $x \neq b_1^{-1}$ เพราะฉะนั้น

$$|x|(a_1, a_2, \dots, a_n) = xa_1a_2\dots a_n = xb_1b_2\dots b_n = xb_1b_2\dots b_m = |x|(b_1, b_2, \dots, b_m)$$

กรณีที่ 2 เมื่อ $x = a_1^{-1}$ จะได้ว่า $x = b_1^{-1}$ เพราะฉะนั้น

$$|x|(a_1, a_2, \dots, a_n) = a_2\dots a_n = b_2\dots b_n = b_2\dots b_m = |x|(b_1, b_2, \dots, b_m)$$

กรณีที่ 3 เมื่อ $(a_1, a_2, \dots, a_n) = 1$ จะได้ว่า $(b_1, b_2, \dots, b_m) = 1$ เพราะฉะนั้น

$$|x|(a_1, a_2, \dots, a_n) = x = |x|(b_1, b_2, \dots, b_m)$$

กรณีที่ 4 เมื่อ $x = a_1^{-1}$ และ $n=1$ จะได้ว่า $x = b_1^{-1}$ เพราะฉะนั้น

$$|x|(a_1, a_2, \dots, a_n) = 1 = |x|(b_1, b_2, \dots, b_m)$$

จากทุกกรณีข้างต้นทำให้สรุปได้ว่า ถ้า $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_m)$ แล้ว

$$|x|(a_1, a_2, \dots, a_n) = |x|(b_1, b_2, \dots, b_m)$$

เพราะฉะนั้น $|x|$ เป็นฟังก์ชัน

2) ให้ (a_1, a_2, \dots, a_n) และ $(b_1, b_2, \dots, b_m) \in F$ โดยที่ $|x|(a_1, a_2, \dots, a_n) = |x|(b_1, b_2, \dots, b_m)$

ดังนั้น $xa_1a_2\dots a_n = xb_1b_2\dots b_m$

กรณีที่ 1 เมื่อ $x = a_1^{-1}$ และ $x = b_1^{-1}$ เนื่องจาก $xa_1a_2\dots a_n = xb_1b_2\dots b_m$ จะได้ว่า

$$a_1^{-1}a_1a_2\dots a_n = b_1^{-1}b_1b_2\dots b_m \text{ ดังนั้น } a_2\dots a_n = b_2\dots b_m \text{ จะได้ว่า } n=m$$

และ $a_i = b_i$ สำหรับทุกๆ $1 \leq i \leq m = n$ เพราะฉะนั้น $a_1 a_2 \dots a_n = b_1 b_2 \dots b_m$
 กรณีที่ 2 เมื่อ $x \neq a_1^{-1}$ และ $x = b_1^{-1}$ ดังนั้น $b_1 = x^{-1}$ เนื่องจาก $x a_1 a_2 \dots a_n = x b_1 b_2 \dots b_m$
 จะได้ว่า $x a_1 a_2 \dots a_n = b_1^{-1} b_1 b_2 \dots b_m$ ดังนั้น $x a_1 a_2 \dots a_n = b_2 \dots b_m$ จะได้ว่า
 $b_2 = x$ ซึ่งขัดแย้งกับ $(b_1, b_2, \dots, b_m) \in F$ ดังนั้นกรณีนี้ไม่สามารถเกิดขึ้นได้
 กรณีที่ 3 เมื่อ $x = a_1^{-1}$ และ $x \neq b_1^{-1}$ ดังนั้น $a_1 = x^{-1}$ เนื่องจาก $x a_1 a_2 \dots a_n = x b_1 b_2 \dots b_m$
 จะได้ว่า $a_1^{-1} a_1 a_2 \dots a_n = x b_1 b_2 \dots b_m$ ดังนั้น $a_2 \dots a_n = x b_1 b_2 \dots b_m$ จะได้ว่า
 $a_2 = x$ ซึ่งขัดแย้งกับ $(a_1, a_2, \dots, a_n) \in F$ ดังนั้นกรณีนี้ไม่สามารถเกิดขึ้นได้
 กรณีที่ 4 เมื่อ $x \neq a_1^{-1}$ และ $x \neq b_1^{-1}$

เนื่องจาก $x a_1 a_2 \dots a_n = x b_1 b_2 \dots b_m$ ดังนั้น $x a_1 = x b_1$ ทำให้ $a_1 = b_1$ ดังนั้น
 $n = m$ และ $a_i = b_i$ สำหรับทุกๆ $1 \leq i \leq m = n$ นั่นคือ $a_1 a_2 \dots a_n = b_1 b_2 \dots b_m$

จากทุกกรณีข้างต้นทำให้สรุปได้ว่าถ้า $|x|(a_1, a_2, \dots, a_n) = |x|(b_1, b_2, \dots, b_m)$
 แล้ว $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_m)$ เพราะฉะนั้น $|x|$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

3) ให้ $a_1 a_2 \dots a_n \in F$

กรณีที่ 1 เมื่อ $x = a_1^{-1}$ จะมี $a_2 \dots a_n \in F$ ที่ทำให้ $|x|(a_2, \dots, a_n) = (x, a_2, \dots, a_n) = (a_1, a_2, \dots, a_n)$

กรณีที่ 2 เมื่อ $x \neq a_1^{-1}$ จะมี $x^{-1} a_1 a_2 \dots a_n \in F$ ที่ทำให้

$$|x|(x^{-1}, a_1, a_2, \dots, a_n) = x x^{-1} (a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_n)$$

จากทุกกรณีข้างต้นทำให้สรุปได้ว่า $|x|$ เป็นฟังก์ชันทั่วถึง

ดังนั้น $|x|$ เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก F ไปยัง F นั่นคือ $|x| \in A(F)$

4) ให้ $(a_1, a_2, \dots, a_n) \in F$

กรณีที่ 1 เมื่อ $x \neq a_1^{-1}$ จะได้ว่า $|x^{-1}|(x a_1 a_2 \dots a_n) = a_1 a_2 \dots a_n$

กรณีที่ 2 เมื่อ $x = a_1^{-1}$ จะได้ว่า $|x^{-1}| \circ |x|(a_1, a_2, \dots, a_n) = |x^{-1}|(a_2 \dots a_n) = x^{-1} a_2 \dots a_n$
 $= x^{-1} (x a_1) a_2 \dots a_n = a_1 a_2 \dots a_n$

กรณีที่ 3 เมื่อ $(a_1, a_2, \dots, a_n) = 1$ จะได้ว่า $|x^{-1}| \circ |x|(a_1, a_2, \dots, a_n) = 1 = a_1 a_2 \dots a_n$

จากทุกกรณีข้างต้น สามารถสรุปได้ว่า $|x^{-1}| \circ |x|(a_1, a_2, \dots, a_n) = a_1 a_2 \dots a_n$

ดังนั้น $|x^{-1}| \circ |x| = 1_F$ นั่นคือ $|x^{-1}|$ เป็นตัวผกผันของ $|x|$

5) ให้ $S = \{|x| \mid x \in X\}$ แล้ว $\langle S \rangle$ เป็นกรุปที่เล็กที่สุดซึ่งมี S เป็นสับเซต ดังนั้น $(\langle S \rangle; \circ)$ เป็น
 กรุปย่อยของ $(A(F); \circ)$

6) ให้ $\varphi: (F; \circ) \rightarrow (\langle S \rangle; \circ)$ นิยามสำหรับ $(a_1, a_2, \dots, a_n) \in F$ นิยามโดย

$$\varphi(a_1, a_2, \dots, a_n) = |a_1| \circ |a_2| \circ \dots \circ |a_n| \text{ และ } \varphi(1) = 1_F$$

ให้ (a_1, a_2, \dots, a_n) และ $(b_1, b_2, \dots, b_m) \in F$ โดยที่ $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_m)$

เนื่องจาก (a_1, a_2, \dots, a_n) และ (b_1, b_2, \dots, b_m) เป็นลำดับตั้งนั้น $n=m$ และ $a_i = b_i$

สำหรับทุกๆ $1 \leq i \leq n$ จะได้ว่า $|a_i| = |b_i|$ ทำให้ได้ว่า

$$\begin{aligned} \varphi(a_1, a_2, \dots, a_n) &= |a_1| \circ |a_2| \circ \dots \circ |a_n| = |b_1| \circ |b_2| \circ \dots \circ |b_n| = |b_1| \circ |b_2| \circ \dots \circ |b_m| \\ &= \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

ดังนั้น φ เป็นฟังก์ชัน

7) ให้ (a_1, a_2, \dots, a_n) และ $(b_1, b_2, \dots, b_m) \in F$

กรณีนี้ที่ 1 เมื่อ $a_n \neq b_1^{-1}$ จะได้ว่า

$$\begin{aligned} \varphi((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \varphi(a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m) \\ &= |a_1| \circ |a_2| \circ \dots \circ |a_n| \circ |b_1| \circ |b_2| \circ \dots \circ |b_m| \\ &= (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_m|) \\ &= \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 2 เมื่อ k เป็นจำนวนเต็มบวกที่มากที่สุดซึ่ง $a_{n-j} = b_{j+1}^{-1}$ สำหรับ $j = 0, 1, \dots, k-1$ จะได้ว่า

$$\begin{aligned} \varphi((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \varphi(a_1, a_2, \dots, a_{n-k} b_{k+1}, \dots, b_m) \\ &= |a_1| \circ |a_2| \circ \dots \circ |a_{n-k}| \circ |b_{k+1}| \circ \dots \circ |b_m| \\ &= |a_1| \circ |a_2| \circ \dots \circ |a_{n-k}| \circ (|a_{n-k+1}| \circ \dots \circ |a_n|) \circ (|b_1| \circ \dots \circ |b_k|) \circ |b_{k+1}| \circ \dots \circ |b_m| \\ &= (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_m|) \\ &= \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 3 เมื่อ $a_{n-i+1} = b_i^{-1}$ สำหรับ $i = 1, 2, \dots, n$ และ $n < m$ จะได้ว่า

$$\begin{aligned} \varphi((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \varphi(b_{n+1}, \dots, b_m) = |b_{n+1}| \circ \dots \circ |b_m| \\ &= (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_n|) \circ (|b_{n+1}| \circ \dots \circ |b_m|) \\ &= |a_1| \circ |a_2| \circ \dots \circ |a_n| \circ |b_1| \circ |b_2| \circ \dots \circ |b_n| \circ |b_{n+1}| \circ \dots \circ |b_m| \\ &= (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_n| \circ |b_{n+1}| \circ \dots \circ |b_m|) \\ &= \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 4 เมื่อ $a_{n-i+1} = b_i^{-1}$ สำหรับ $i=1,2,\dots,m$ และ $m < n$ จะได้ว่า

$$\begin{aligned} \varphi((a_1, a_2, \dots, a_n)^*(b_1, b_2, \dots, b_m)) &= \varphi(a_1, a_2, \dots, a_{n-m}) = |a_1| \circ |a_2| \circ \dots \circ |a_{n-m}| \\ &= (|a_1| \circ |a_2| \circ \dots \circ |a_{n-m}|) \circ (|a_{n-m+1}| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_m|) \\ &= |a_1| \circ |a_2| \circ \dots \circ |a_{n-m}| \circ |a_{n-m+1}| \circ \dots \circ |a_n| \circ |b_1| \circ |b_2| \circ \dots \circ |b_m| \\ &= (|a_1| \circ |a_2| \circ \dots \circ |a_{n-m}| \circ |a_{n-m+1}| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_m|) \\ &= \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 5 เมื่อ $a_{n-i+1} = b_i^{-1}$ สำหรับ $i=1,2,\dots,n$ และ $m=n$ จะได้ว่า

$$\begin{aligned} \varphi((a_1, a_2, \dots, a_n)^*(b_1, b_2, \dots, b_m)) &= \varphi(1) = 1_F \\ &= 1_F \circ (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_n|) \\ &= (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_n|) \\ &= \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 6 เมื่อ $b_i = 1$ สำหรับทุกๆ $1 \leq i \leq m$ จะได้ว่า

$$\begin{aligned} \varphi((a_1, a_2, \dots, a_n)^*(b_1, b_2, \dots, b_m)) &= \varphi((a_1, a_2, \dots, a_n)^*(1)) = \varphi(a_1, a_2, \dots, a_n) \\ &= |a_1| \circ |a_2| \circ \dots \circ |a_n| = |a_1| \circ |a_2| \circ \dots \circ |a_n| \circ 1_F = (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (1_F) \\ &= \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 7 เมื่อ $a_i = 1$ สำหรับทุกๆ $1 \leq i \leq n$ จะได้ว่า

$$\begin{aligned} \varphi((a_1, a_2, \dots, a_n)^*(b_1, b_2, \dots, b_m)) &= \varphi(1)^*(b_1, b_2, \dots, b_m) \\ &= \varphi(b_1, b_2, \dots, b_m) = |b_1| \circ |b_2| \circ \dots \circ |b_m| = 1_F \circ |b_1| \circ |b_2| \circ \dots \circ |b_m| \\ &= (1_F) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_m|) \\ &= \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 8 เมื่อ $a_i = 1$ สำหรับทุกๆ $1 \leq i \leq n$ และ $b_i = 1$ สำหรับทุกๆ $1 \leq i \leq m$ จะได้ว่า

$$\begin{aligned} \varphi((a_1, a_2, \dots, a_n)^*(b_1, b_2, \dots, b_m)) &= \varphi(1) = 1_F \\ &= 1_F \circ (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_m|) \\ &= (|a_1| \circ |a_2| \circ \dots \circ |a_n|) \circ (|b_1| \circ |b_2| \circ \dots \circ |b_m|) \\ &= \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m) \end{aligned}$$

จากทุกกรณีข้างต้นทำให้สรุปได้ว่า

$$\varphi((a_1, a_2, \dots, a_n)^*(b_1, b_2, \dots, b_m)) = \varphi(a_1, a_2, \dots, a_n) \circ \varphi(b_1, b_2, \dots, b_m)$$

นั่นคือ φ เป็นสาทิสต์พื้นฐาน

8) ให้ (a_1, a_2, \dots, a_n) และ $(b_1, b_2, \dots, b_m) \in F$ โดยที่ $\varphi(a_1, a_2, \dots, a_n) = \varphi(b_1, b_2, \dots, b_m)$

ดังนั้น $|a_1| \circ |a_2| \circ \dots \circ |a_n| = |b_1| \circ |b_2| \circ \dots \circ |b_m|$ ให้ $x \neq y$ ดังนั้น

กรณีที่ 1 เมื่อ $x \neq a_1^{-1}$ จะได้ว่า $|y| \circ |x| (a_1 a_2 \dots a_n) = y x a_1 a_2 \dots a_n = |y x| (a_1 a_2 \dots a_n)$

กรณีที่ 2 เมื่อ $x = a_1^{-1}$ จะได้ว่า $|y| \circ |x| (a_1 a_2 \dots a_n) = y a_2 \dots a_n = |y x| (a_1 a_2 \dots a_n)$

จากทุกกรณีข้างต้นทำให้สรุปได้ว่า $|y| \circ |x| = |y x|$ ดังนั้น

$$\begin{aligned} |a_1| \circ |a_2| \circ \dots \circ |a_n| &= |b_1| \circ |b_2| \circ \dots \circ |b_m| \\ |a_1| \circ |a_2| \circ \dots \circ |a_{n-1} a_n| &= |b_1| \circ |b_2| \circ \dots \circ |b_{m-1} b_m| \\ \cap \quad \cap \\ |a_1 a_2 \dots a_n| &= |b_1 b_2 \dots b_m| \end{aligned}$$

เนื่องจาก $a_1 a_2 \dots a_n$ และ $b_1 b_2 \dots b_m$ เป็นลำดับ จะได้ว่า $n = m$ และ $a_i = b_i$ สำหรับทุกๆ

$1 \leq i \leq m = n$ นั่นคือ $a_1 a_2 \dots a_n = b_1 b_2 \dots b_m$

ดังนั้น φ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

9) ให้ $f \in \langle S \rangle$ ดังนั้นจะมี $(a_1, a_2, \dots, a_n) \in F$ ซึ่ง $|a_1|, |a_2|, \dots, |a_n| \in S$ และ

$f = |a_1| \circ |a_2| \circ \dots \circ |a_n|$ ซึ่งทำให้ $\varphi(a_1, a_2, \dots, a_n) = f = |a_1| \circ |a_2| \circ \dots \circ |a_n| \in \langle S \rangle$

หรือถ้า $f = 1_F$ ก็จะมี $(a_1, a_2, \dots, a_n) = (1) \in F$ ที่ทำให้ $\varphi(a_1, a_2, \dots, a_n) = 1_F = f$

ดังนั้น φ เป็นฟังก์ชันทั่วถึง

จากการพิสูจน์ข้างต้นทำให้สรุปได้ว่า φ เป็นสมสัณฐาน เพราะฉะนั้น $(F; \circ)$ สมสัณฐานกันกับ

$(\langle S \rangle; \circ)$ และเนื่องจาก $(\langle S \rangle; \circ)$ เป็นกรุป ดังนั้น $(F; \circ)$ เป็นกรุป ●

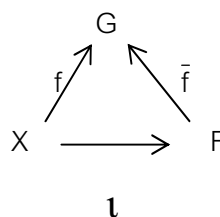
ต่อไปจะแสดงความสัมพันธ์ของกรุป $(F; \circ)$ กับกรุป G ใดๆ โดยพิสูจน์ว่ากรุป $(F; \circ)$

เป็นกรุปอิสระตามบทแทรก 2.41

4.7 ทฤษฎีบท ให้ F เป็นกรุปในทฤษฎีบท 4.6 ถ้า G เป็นกรุปใดๆ และ $f: X \rightarrow G$ แล้วจะมี

สัทิสสัณฐาน $\bar{f}: F \rightarrow G$ เพียงหนึ่งเดียวซึ่ง $\bar{f} \circ \iota = f$ โดยที่ $\iota: X \rightarrow F$ นิยามโดย

$\iota(a) = (a, 1, 1, \dots)$ สำหรับทุกๆ $a \in X$



บทพิสูจน์ เราจะต้องแสดงให้เห็นว่า $(F; \cdot)$ เป็นกรุปอิสระดังนี้ ให้ $\iota: X \rightarrow F$ นิยามโดย

$\iota(a) = (a, 1, 1, \dots)$ ให้ G เป็นกรุป และ $f: X \rightarrow G$ ให้ $\bar{f}: F \rightarrow G$ นิยามโดย $\bar{f}(\iota(a)) = e$ และ $\bar{f}(a_1 a_2 \dots a_n) = f(a_1) f(a_2) \dots f(a_n)$ สำหรับ $a_1, a_2, \dots, a_n \in X$

1) ให้ (a_1, a_2, \dots, a_n) , (b_1, b_2, \dots, b_m) และ $1 \in F$

กรณีที่ 1 ให้ $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_m)$

เนื่องจาก (a_1, a_2, \dots, a_n) และ (b_1, b_2, \dots, b_m) เป็นลำดับ ดังนั้น $n=m$ และ $a_i = b_i$ สำหรับทุก i

$1 \leq i \leq n$ จะได้ว่า $f(a_i) = f(b_i)$ ทำให้ได้ว่า

$$\begin{aligned} \bar{f}(a_1, a_2, \dots, a_n) &= f(a_1) f(a_2) \dots f(a_n) = f(b_1) f(b_2) \dots f(b_n) = f(b_1) f(b_2) \dots f(b_m) \\ &= \bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีที่ 2 ให้ $(a_1, a_2, \dots, a_n) = 1$ จะได้ว่า $\bar{f}(a_1, a_2, \dots, a_n) = e = \bar{f}(1)$

ดังนั้น \bar{f} เป็นฟังก์ชัน

2) ให้ (a_1, a_2, \dots, a_n) และ $(b_1, b_2, \dots, b_m) \in F$

กรณีที่ 1 เมื่อ $a_n \neq b_1^{-1}$ จะได้ว่า

$$\begin{aligned} \bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \bar{f}(a_1 a_2 \dots a_n b_1 b_2 \dots b_m) \\ &= f(a_1) f(a_2) \dots f(a_n) f(b_1) f(b_2) \dots f(b_m) \\ &= (f(a_1) f(a_2) \dots f(a_n)) (f(b_1) f(b_2) \dots f(b_m)) \\ &= \bar{f}(a_1, a_2, \dots, a_n) \bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีที่ 2 เมื่อ k เป็นจำนวนเต็มบวกที่มากที่สุดซึ่ง $a_{n-j} = b_{j+1}^{-1}$ สำหรับ $j=0, 1, \dots, k-1$ จะได้ว่า

$$\begin{aligned} \bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \bar{f}(a_1 a_2 \dots a_{n-k} b_{k+1} \dots b_m) \\ &= f(a_1) f(a_2) \dots f(a_{n-k}) f(b_{k+1}) \dots f(b_m) \\ &= f(a_1) f(a_2) \dots f(a_{n-k}) (e) f(b_{k+1}) \dots f(b_m) \\ &= f(a_1) f(a_2) \dots f(a_{n-k}) \bar{f}(1) f(b_{k+1}) \dots f(b_m) \\ &= f(a_1) f(a_2) \dots f(a_{n-k}) \bar{f}(a_{n-k+1} \dots a_n b_1 \dots b_k) f(b_{k+1}) \dots f(b_m) \\ &= f(a_1) f(a_2) \dots f(a_{n-k}) f(b_{k+1}) \dots f(b_m) f(a_{n-k+1}) \dots f(a_n) f(b_1) \dots f(b_k) \\ &= f(a_1) f(a_2) \dots f(a_n) f(b_1) f(b_2) \dots f(b_m) \\ &= (f(a_1) f(a_2) \dots f(a_n)) (f(b_1) f(b_2) \dots f(b_m)) \\ &= \bar{f}(a_1, a_2, \dots, a_n) \bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 3 เมื่อ $a_{n-i+1} = b_i^{-1}$ สำหรับ $i=1,2,\dots,n$ และ $n < m$ จะได้ว่า

$$\begin{aligned} \bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \bar{f}(b_{n+1}, \dots, b_m) = f(b_{n+1}) \dots f(b_m) \\ &= (e) f(b_{n+1}) \dots f(b_m) \\ &= \bar{f}(1) f(b_{n+1}) \dots f(b_m) \\ &= \bar{f}(a_1 \dots a_n b_1 \dots b_n) f(b_{n+1}) \dots f(b_m) \\ &= f(a_1) f(a_2) \dots f(a_n) f(b_1) f(b_2) \dots f(b_m) \\ &= (f(a_1) f(a_2) \dots f(a_n)) (f(b_1) f(b_2) \dots f(b_m)) \\ &= \bar{f}(a_1, a_2, \dots, a_n) \bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 4 เมื่อ $a_{n-i+1} = b_i^{-1}$ สำหรับ $i=1,2,\dots,m$ และ $m < n$ จะได้ว่า

$$\begin{aligned} \bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \bar{f}(a_1, \dots, a_{n-m}) = f(a_1) \dots f(a_{n-m}) \\ &= f(a_1) \dots f(a_{n-m}) (e) \\ &= f(a_1) \dots f(a_{n-m}) \bar{f}(1) \\ &= f(a_1) \dots f(a_{n-m}) \bar{f}(a_{n-m+1} \dots a_n b_1 \dots b_m) \\ &= f(a_1) \dots f(a_{n-m}) f(a_{n-m+1}) \dots f(a_n) f(b_1) \dots f(b_m) \\ &= (f(a_1) f(a_2) \dots f(a_n)) (f(b_1) f(b_2) \dots f(b_m)) \\ &= \bar{f}(a_1, a_2, \dots, a_n) \bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 5 เมื่อ $a_{n-i+1} = b_i^{-1}$ สำหรับ $i=1,2,\dots,n$ และ $m=n$ จะได้ว่า

$$\begin{aligned} \bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \bar{f}(1) \\ &= \bar{f}(a_1 a_2 \dots a_n b_1 b_2 \dots b_m) \\ &= (f(a_1) f(a_2) \dots f(a_n)) (f(b_1) f(b_2) \dots f(b_m)) \\ &= \bar{f}(a_1, a_2, \dots, a_n) \bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณีนี้ที่ 6 เมื่อ $b_i = 1$ สำหรับทุกๆ $1 \leq i \leq m$ จะได้ว่า

$$\begin{aligned} \bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \bar{f}((a_1, a_2, \dots, a_n) * (1)) = \bar{f}(a_1, a_2, \dots, a_n) \\ &= f(a_1) f(a_2) \dots f(a_n) = f(a_1) f(a_2) \dots f(a_n) (e) = f(a_1) f(a_2) \dots f(a_n) \bar{f}(1) \\ &= (f(a_1) f(a_2) \dots f(a_n)) \bar{f}(b_1 \dots b_m) \\ &= (f(a_1) f(a_2) \dots f(a_n)) (f(b_1) f(b_2) \dots f(b_m)) \\ &= \bar{f}(a_1, a_2, \dots, a_n) \bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณี 7 เมื่อ $a_i = 1$ สำหรับทุกๆ $1 \leq i \leq n$ จะได้ว่า

$$\begin{aligned} \bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \bar{f}((1, 1, \dots, 1) * (b_1, b_2, \dots, b_m)) = \bar{f}(b_1, b_2, \dots, b_m) \\ &= f(b_1)f(b_2)\dots f(b_m) = (e)f(b_1)f(b_2)\dots f(b_m) = \bar{f}(1)f(b_1)f(b_2)\dots f(b_m) \\ &= \bar{f}(a_1, a_2, \dots, a_n)(f(b_1)f(b_2)\dots f(b_m)) \\ &= (f(a_1)f(a_2)\dots f(a_n))(f(b_1)f(b_2)\dots f(b_m)) \\ &= \bar{f}(a_1, a_2, \dots, a_n)\bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

กรณี 8 เมื่อ $a_i = 1$ สำหรับทุกๆ $1 \leq i \leq n$ และ $b_i = 1$ สำหรับทุกๆ $1 \leq i \leq m$ จะได้ว่า

$$\begin{aligned} \bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) &= \bar{f}(1) \\ &= \bar{f}(a_1 a_2 \dots a_n b_1 b_2 \dots b_m) \\ &= (f(a_1)f(a_2)\dots f(a_n))(f(b_1)f(b_2)\dots f(b_m)) \\ &= \bar{f}(a_1, a_2, \dots, a_n)\bar{f}(b_1, b_2, \dots, b_m) \end{aligned}$$

จากทุกกรณีข้างต้นทำให้สรุปได้ว่า

$$\bar{f}((a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_m)) = \bar{f}(a_1, a_2, \dots, a_n)\bar{f}(b_1, b_2, \dots, b_m)$$

นั่นคือ \bar{f} เป็นสาคทิสต์ฐาน

3) ให้ $a_i \in X$ จะได้ว่า $\bar{f}(a_i) = \bar{f}(1(a_i)) = \bar{f}(a_i, 1, 1, \dots) = \bar{f}(a_i)$ เพราะฉะนั้น $\bar{f}1 = f$

4) เพราะว่า $\bar{f}: F \rightarrow G$ เป็นสาคทิสต์ฐาน โดยที่ $\bar{f}1 = f$

ให้ $g: F \rightarrow G$ เป็นสาคทิสต์ฐาน ดังนั้น $g1 = f$ จะได้ว่า

$$\begin{aligned} g(a_1 a_2 \dots a_n) &= g(a_1)g(a_2)\dots g(a_n) = g1(a_1)g1(a_2)\dots g1(a_n) = f(a_1)f(a_2)\dots f(a_n) \\ &= \bar{f}(a_1 a_2 \dots a_n) \end{aligned}$$

เพราะฉะนั้น $\bar{f} = g$ นั่นคือมีสาคทิสต์ฐาน $\bar{f}: F \rightarrow G$ เพียงหนึ่งเดียว



บรรณานุกรม

- [1] ช่อฟ้า นิลรัตน์ , **พีชคณิตนามธรรม** , มหาวิทยาลัยสงขลานครินทร์ สงขลา 2533
- [2] Hilton,Peter John , **A Course in Modern Algebra** , Library of Congress Cataloging-inPublication Data ,1974.
- [3] Thomas W. Judson , **Abstract Algebra : theory and applications** , Library of Congress Cataloging-inPublication Data ,1993.
- [4] John B. Fraleigh , **A First Course In Abstract Algebra** , Department of Mathematics University of Rhode Island ,1971.
- [5] M.A. Armstrong , **Groups and Symmetry** , Library of Congress Cataloging-inPublication Data ,1988.
- [6] EUGENE SCHENKMAN , **Group Theory** , K.S. Padmanabhan for AFFILIATED EAST-WEST PRESS PRIVATE LTD. ,1965.

มหาวิทยาลัยศิลปากร สงวนลิขสิทธิ์

ประวัติผู้วิจัย

ชื่อ-สกุล	นายไอลัน น้าวไกรศร
ที่อยู่	118 หมู่ 1 ต.วังเย็น อ.บางแพ จ.ราชบุรี 70160
ประวัติการศึกษา	
พ.ศ. 2544	สำเร็จการศึกษาปริญญาวิทยาศาสตรบัณฑิต สาขาคณิตศาสตร์ จากมหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ จังหวัดสงขลา
พ.ศ. 2547	ศึกษาต่อระดับปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาคณิตศาสตร์และเทคโนโลยีสารสนเทศ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร
ประวัติการทำงาน	
พ.ศ. 2544-2545	ครูสอนวิชาคณิตศาสตร์ และ วิชาสถิติ ระดับประกาศนียบัตร วิชาชีพชั้นสูง โรงเรียนหาดใหญ่อำนวยวิทยบริหารธุรกิจ จังหวัดสงขลา
พ.ศ. 2545-2551	ครูสอนวิชาคณิตศาสตร์ ระดับประกาศนียบัตรวิชาชีพและ ระดับประกาศนียบัตรวิชาชีพชั้นสูง โรงเรียนดรุณราชบุรีโปลี เทคนิค จังหวัดราชบุรี